Risiken und Chancen in der Cloud

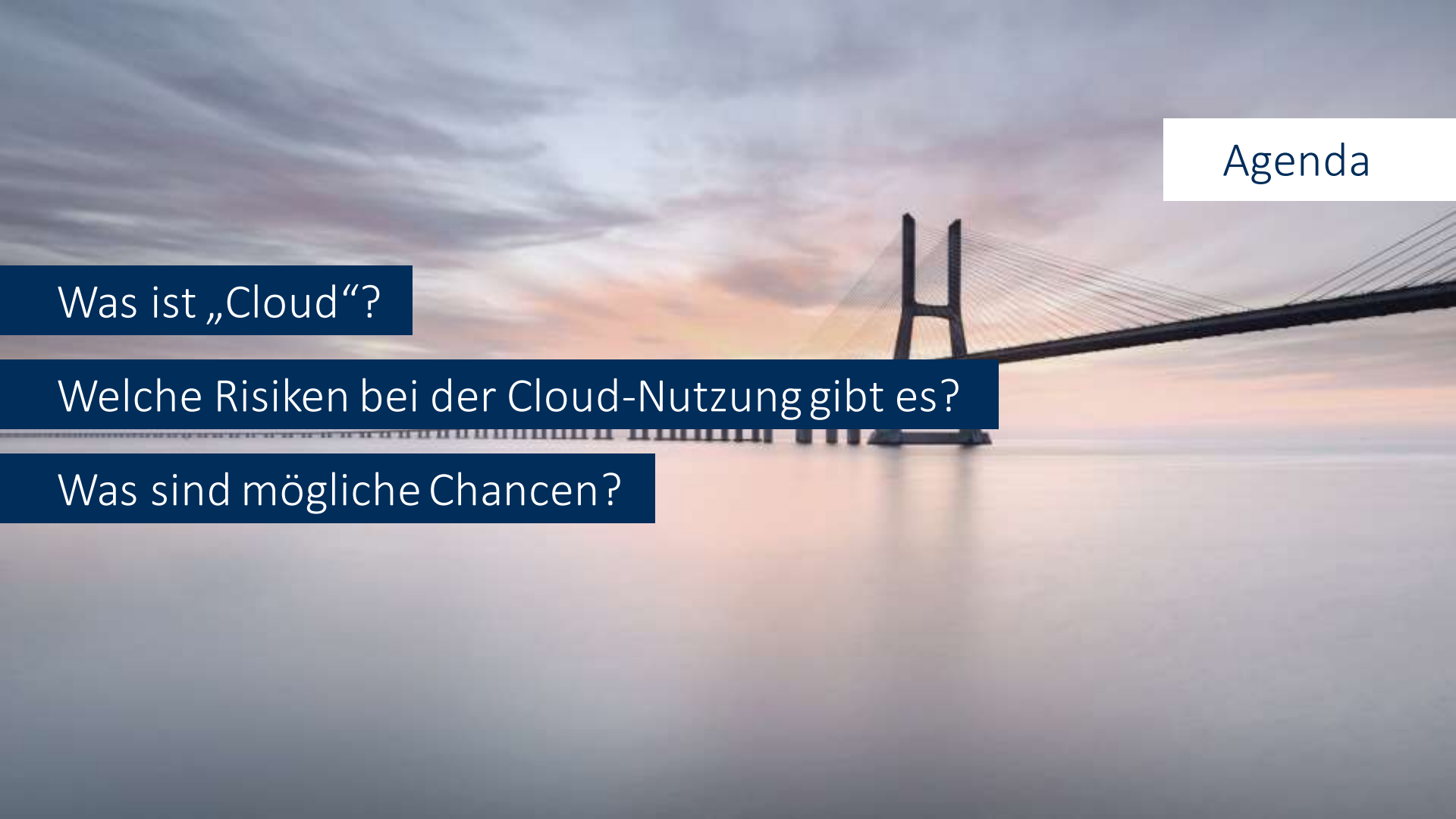
HiSolutions Know-how to go

HiSolutions AG

Michael Sehring

Michael Sehring
Senior Consultant

- Technische IT-Sicherheitsberatung
  - Beratung zur sicheren Inbetriebnahme neuer Anwendungen und Systeme
  - Beratung zu Security-Aspekten bei Cloud-Migrationen
- Aufbau von Informationssicherheitsmanagementsystemen nach ISO 27001 und IT-Grundschutz
- Cloud-Sicherheit
- Kryptographie



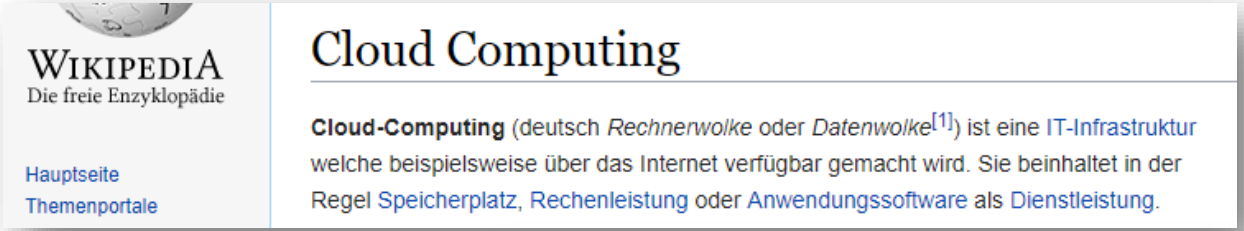
Agenda

- Was ist „Cloud“?
- Welche Risiken bei der Cloud-Nutzung gibt es?
- Was sind mögliche Chancen?

Was ist „Cloud“?

Quelle: Cloud-Monitor 2023, https://kpmg.com/de/de/home/themen/2023/09/cloud-monitor-2023.html

Cloud Computing: Was steckt dahinter?



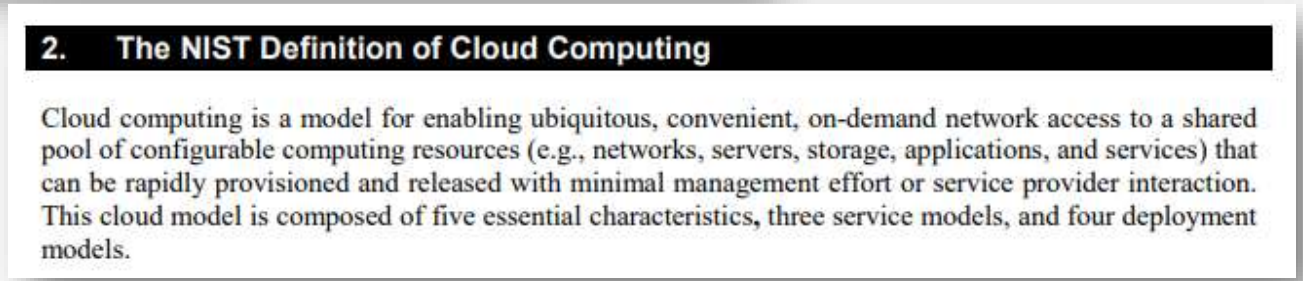
WIKIPEDIA
Die freie Enzyklopädie

Hauptseite
Themenportale

Cloud Computing

Cloud-Computing (deutsch *Rechnerwolke* oder *Datenwolke*[1]) ist eine IT-Infrastruktur welche beispielsweise über das Internet verfügbar gemacht wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung.

Quelle:
https://de.w ikipedia.org/w iki/Cloud_Computing



2. The NIST Definition of Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Quelle:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

"Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."

Quelle:
https://w ww.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html

Was ist Cloud-Computing?

NIST definiert Cloud-Computing als eine Menge an Charakteristiken, Cloud-Bereitstellungsmodellen und Cloud-Service-Modellen.

5 Charakteristiken

- **On-demand Self Service:** Die Zuteilung der Ressourcen erfolgt automatisiert, ohne dass ein Mitarbeiter-Interaktion notwendig ist.
- **Broad Network Access:** Die Cloud-Dienste stehen über das Netz zur Verfügung und sind nicht an bestimmte Clients gebunden.
- **Resource Pooling:** Die Ressourcen des Cloud-Anbieters liegen in einem Pool vor, aus dem sich viele Cloud-Kunden bedienen können (Multi-Tenant Modell). Dabei wissen die Cloud-Kunden nicht, welche Ressourcen genau verwendet werden. Die Verarbeitung und Speicherung kann aber vertraglich festlegt werden, z. B. auf ein Land oder eine Region).
- **Rapid Elasticity:** Die Cloud-Dienste können schnell und elastisch zur Verfügung gestellt werden.
- **Measured Services:** Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Kunden zur Verfügung gestellt werden.

4 Bereitstellungsmodelle

- **Private Cloud:** Die Cloud-Infrastruktur wird durch ein Unternehmen genutzt.
- **Community Cloud:** Die Cloud-Infrastruktur wird durch mehrere Institutionen, z. B. einer Branche, genutzt.
- **Public Cloud:** Die Cloud-Infrastruktur wird von beliebigen Cloud-Kunden genutzt.
- **Hybrid Cloud:** Es kommen zwei oder mehr Bereitstellungs-modelle zum Einsatz, die miteinander verbunden sind.

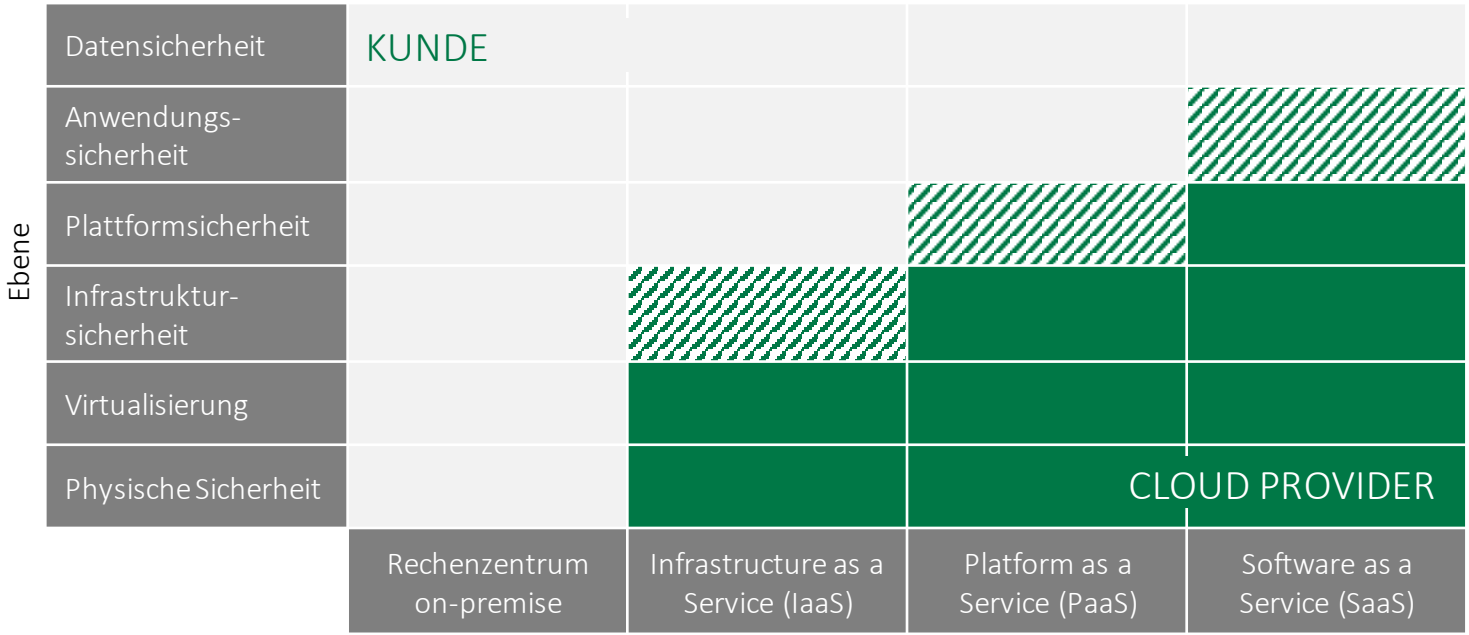
3 Service-Modelle

- **Infrastructure-as-a-Service (IaaS):** Es werden Infrastrukturkomponenten, wie virtuelle Maschinen, Netzwerkverbindungen und Speicherplatz in einem Rechenzentrum, bereitgestellt.
- **Platform-as-a-Service (PaaS):** Zusätzlich zu IaaS werden Dienste für die Entwicklung, Middleware, Datenbanken uvm. bereitgestellt.
- **Software-as-a-Service (SaaS):** Über das Internet bereitgestellte Anwendungen.

Welche Risiken bei der Cloud-Nutzung gibt es?

Shared Responsibility

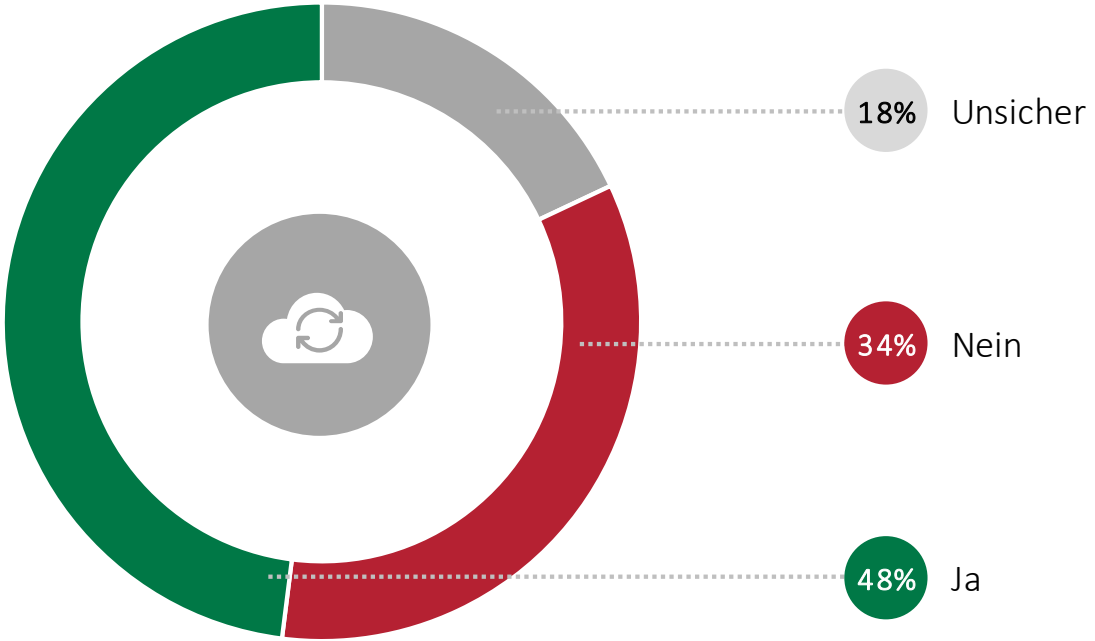
Shared Responsibility



Frage: Werden bei Ihnen Risiken für Cloud-Dienste wiederholt bewertet?

Evergreen

Frage: Werden bei Ihnen Risiken für Cloud-Dienste wiederholt bewertet?



Evergreen

Quelle: Cloud Security Alliance 2022, https://cloudsecurityalliance.org/artifacts/measuring-risk-and-risk-governance

Vendor Lock

Vendor Lock

Vendor Lock-Out

- Eingeschränkter Zugriff auf (eigene) Daten
- Möglicher Verlust von Daten

Vendor Lock

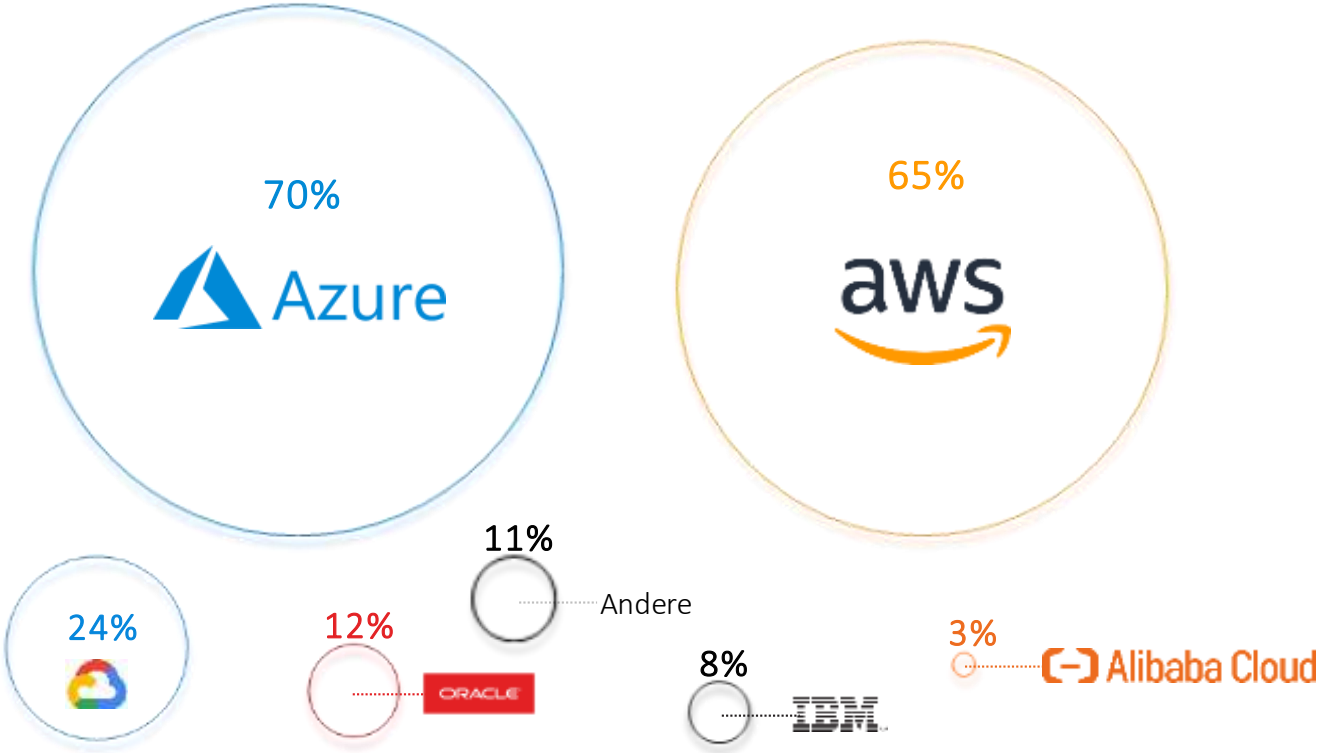
Vendor Lock-Out

- Eingeschränkter Zugriff auf (eigene) Daten
- Möglicher Verlust von Daten

Vendor Lock-In

- Hohe Abhängigkeit zum Cloud-Anbieter
- Wechsel des Cloud-Anbieters ist mit hohen Kosten verbunden
- Cloud-Anbieter steigert langsam die Servicekosten

Frage: Welche IaaS Plattform wird genutzt?



Quelle: Cloud Security Alliance 2022, https://cloudsecurityalliance.org/artifacts/measuring-risk-and-risk-governance

Unzureichende Exit-Strategie

Unzureichende Cloud-Strategie

Unzureichende Cloud-Strategie

Cloud-Too-Strategie

- Vereinzelte **Ergänzung** um Cloud-Dienste

Unzureichende Cloud-Strategie

Cloud-Too-Strategie

- Vereinzelte **Ergänzung** um Cloud-Dienste

Cloud-First-Strategie

- Neue Entwicklungen **bevorzugt** in der Cloud

Unzureichende Cloud-Strategie

Cloud-Too-Strategie

- Vereinzelte **Ergänzung** um Cloud-Dienste

Cloud-First-Strategie

- Neue Entwicklungen **bevorzugt** in der Cloud

Cloud-Only-Strategie

- Cloud-Dienste für **alle** Systeme / Anwendungen

Unzureichendes Notfallkonzept

Unzureichendes Notfallkonzept

- Haben Sie Break-Glass Accounts?
- Haben Sie einen direkten Kontakt zum Cloud-Provider?
- Haben Sie Off-Site Backups?

Großbrand im OVH Rechenzentrum

Im März 2021 führte ein Großbrand bei der OVHcloud zu einem riesigen Datenverlust.

Ursache:

- Ein elektrischer Fehler hat zu einem Brand geführt. In Folge des Brandes ist ein Rechenzentrum vollständig abgebrannt und zwei weitere sind beschädigt worden.

Folgen / Auswirkungen:

- Weltweit waren Webseiten und Dienstleistungen nicht erreichbar.
- Der durch den Brand in Kritik geratene Anbieter, erscheint mit Negativ-Schlagzeilen in der Presse.

Störung bei Google Cloud Platform

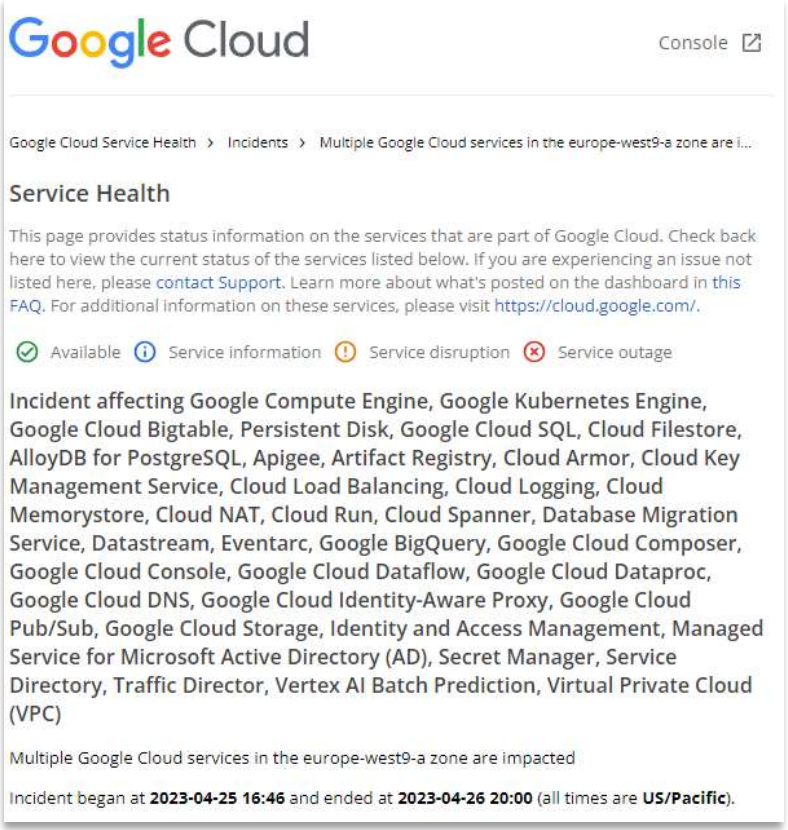
Im April 2023 gab es einen 20-stündigen Ausfall in der GCP Region europe-9.

Ursache:

- Leck in der Wasserleitung des Kühlsystems eines Rechenzentrums. Das Wasser ist in einen Raum für die unterbrechungsfreie Stromversorgung (USV) eingedrungen und hat dort zu einem Brand geführt.
- Zusätzlich wurden die Replikate des regionalen Spanners nicht korrekt auf die drei Gebäude in der Region verteilt

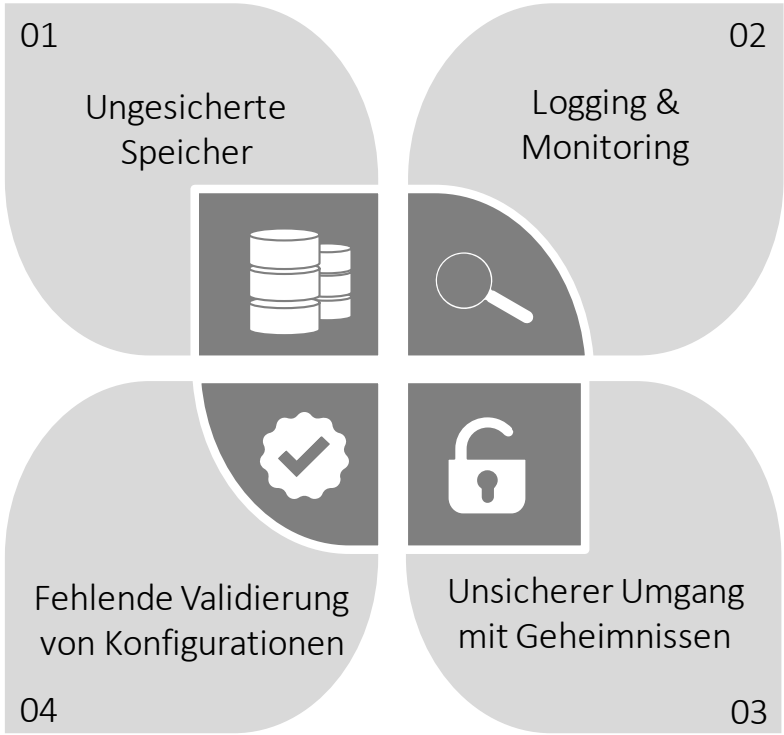
Folgen / Auswirkungen:

- Einige Dienste in GCP waren nicht erreichbar.

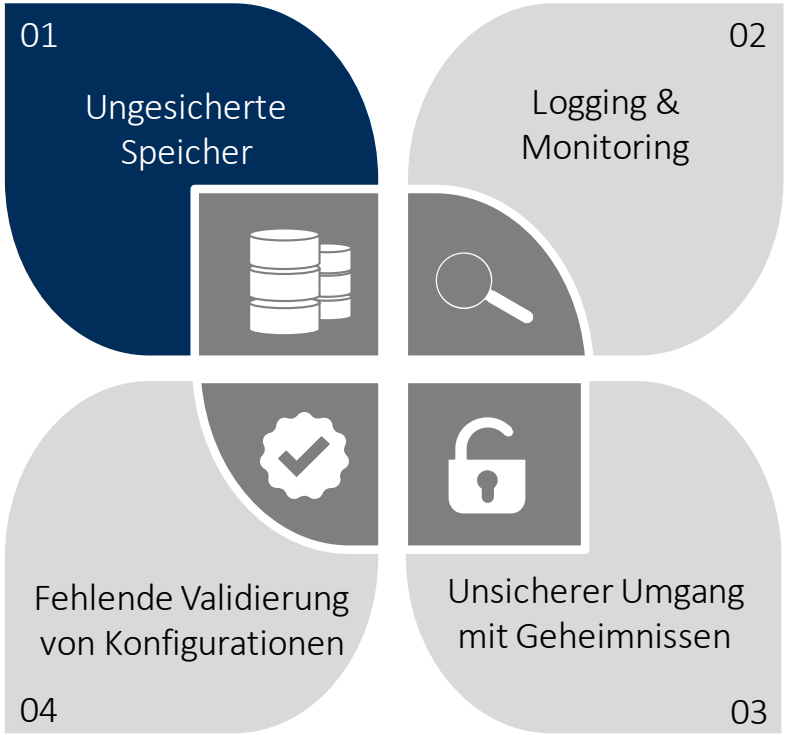


Quelle: Google Cloud Service Health, https://status.cloud.google.com/incidents/dS9ps52MUnxQfyDGPfkY

Unzureichende Konfiguration



Unzureichende Konfiguration



Unzureichende Konfiguration

01

02

Logging &

Vordefinierte Gruppen in Amazon S3

Amazon S3 besitzt mehrere vordefinierte Gruppen. Wenn Sie einem Konto Zugriff auf eine Gruppe erteilen, geben Sie eine der Amazon-S3-URIs statt einer kanonischen Benutzer-ID an. Amazon S3 stellt die folgenden vordefinierten Gruppen bereit:

- **Gruppe „Authentifizierte Benutzer“** – Repräsentiert durch `http://acs.amazonaws.com/groups/global/AuthenticatedUsers`.

  Diese Gruppe stellt alle AWS-Konten dar. **Die Zugriffsberechtigung für diese Gruppe gestattet jedem AWS-Konto, auf die Ressource zuzugreifen.** Alle Anfragen müssen jedoch signiert (authentifiziert) sein.

  > ⚠ **Warnung**
  >
  > Wenn Sie einen Zugriff auf die **Gruppe „Authentifizierte Benutzer“** erteilen, hat jeder AWS-authentifizierte Benutzer weltweit Zugriff auf Ihre Ressource.

von Konfigurationen

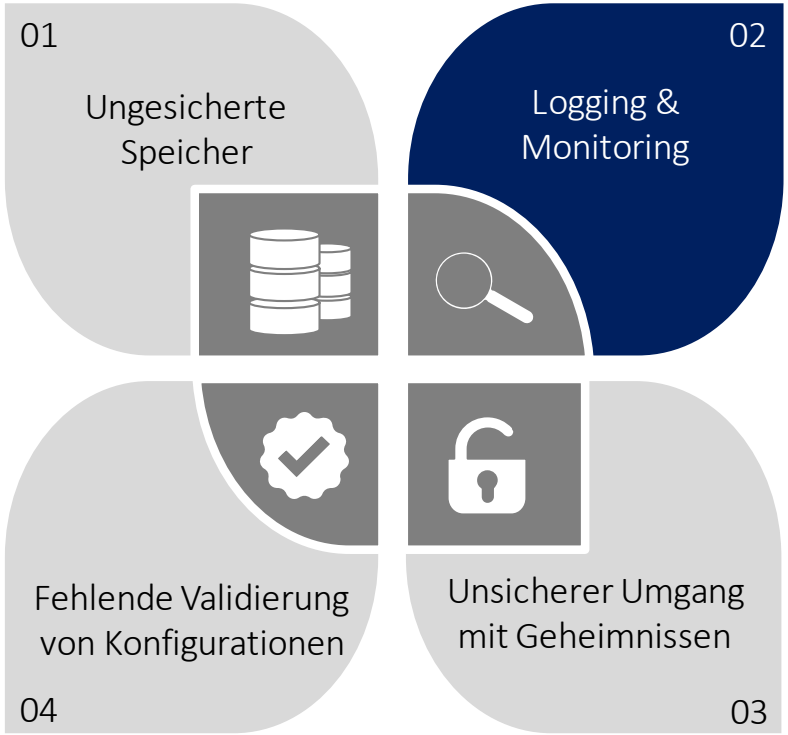
mit Geheimnissen

04

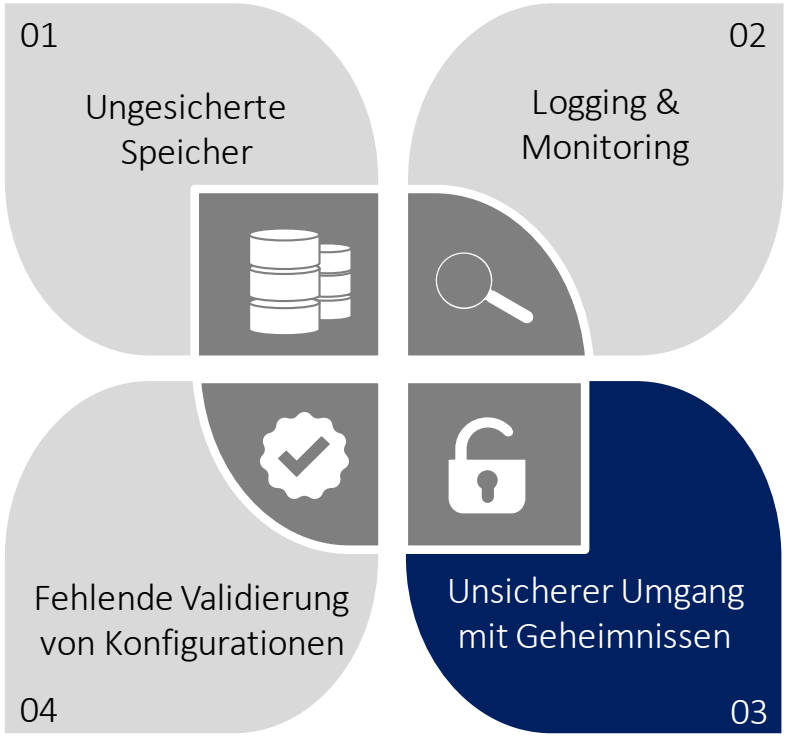
03

Quelle: AWS Zugriffskontrolllisten (ACL), https://docs.aws.amazon.com/de_de/AmazonS3/latest/userguide/acl-overview.html

Unzureichende Konfiguration



Unzureichende Konfiguration



Unzureichende Konfiguration

Security

Microsoft lost its keys, and the government got hacked

Zack Whittaker

@zackwhittaker / 4:05 PM GMT+2 • July 17, 2023

Comment

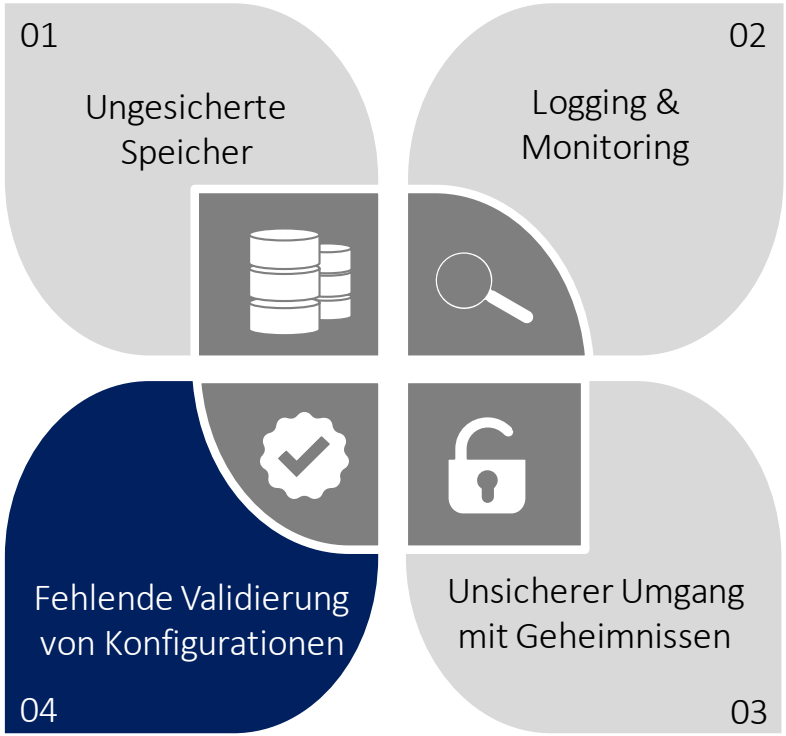
Microsoft still doesn't know — or want to share — how China-backed hackers stole a key that allowed them to stealthily break into dozens of email inboxes, including those belonging to several federal government agencies.

04

03

Quelle: Techcrunch, https://techcrunch.com/2023/07/17/microsoft-lost-keys-government-hacked/

Unzureichende Konfiguration



Angreifer schürfen Kryptocoins auf ungeschütztem AWS Account

Im Januar 2018 wurde durch Sicherheitsforscher entdeckt, dass Teslas AWS Account zum Kryptocoins schürfen genutzt wurde.

Ursache:

- Eine Kubernetes Konsole war offen zugängig und hierrüber konnten die Angreifer AWS Zugangsdaten auslesen und ihren Angriff ausweiten.

Folgen / Auswirkungen:

- Die Angreifer installierten eine Kryptomining-Software in Teslas AWS Account und nutzten Ressourcen, für die Tesla bezahlte.
- Laut Tesla waren keine Kundendaten betroffen.


MILLIONENBEUTE

Hacker kapern Tesla-Cloud für Krypto-Mining

Hacker haben eine Sicherheitslücke bei Tesla ausgenutzt, um Krypto-Währung zu schürfen. Die Beute soll mehrere Millionen Dollar betragen.

Was sind mögliche Chancen?

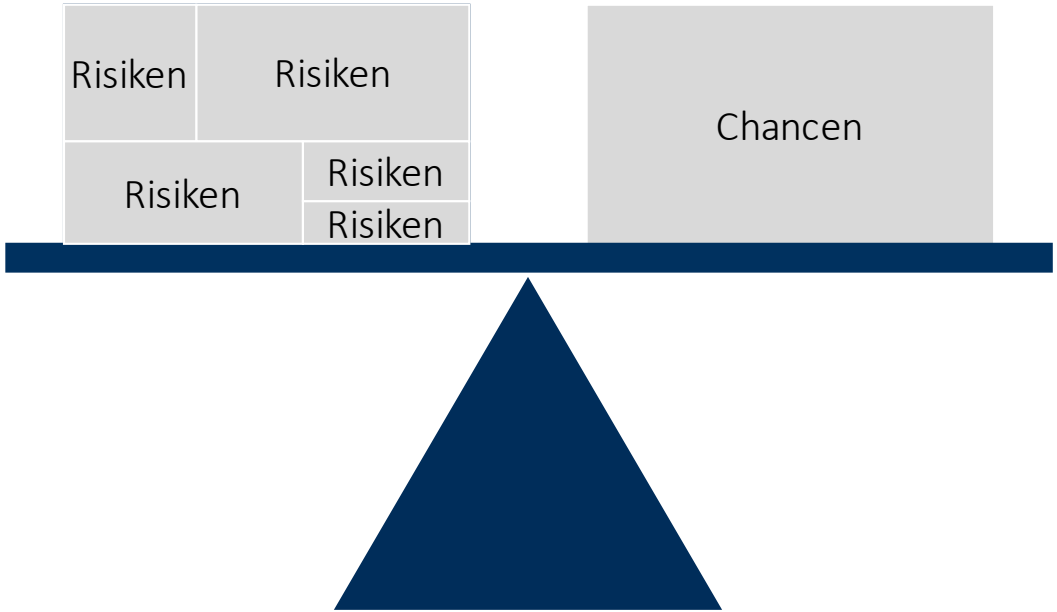
Vorteile und Chancen der Cloud nutzen…

- **Flexibilität**
- **Zeit- und ortsunabhängige Zusammenarbeit**
- **Skalierbarkeit**

Vorteile und Chancen der Cloud nutzen…

- **Flexibilität**
- **Zeit- und ortsunabhängige Zusammenarbeit**
- **Skalierbarkeit**
- **Transparente monatliche Kosten**
- **Automatische Updates**
- **Verfügbarkeit**

Fazit: Risiken und Chancen angemessen abwägen



Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com