Informationssicherheit in der Cloud

Know-how to go – ISO 27001 Novellierung

HiSolutions AG

Matthias P. Reintges

Matthias P. Reintges

Senior Consultant

Fachliche Schwerpunkte

- Beratung zu Themen der operativen IT-Sicherheit
  - Security Monitoring
  - Cloud Security
  - Active Directory Security
- Durchführung von Konfigurationsaudits

Qualifikationen

- zertifizierter IT-Security-Manager (TÜV Rheinland)
- zertifizierter IT-Security Beauftragter (TÜV Rheinland)
- ITIL 3 - Foundation Certificate IT Service Management
- BSI IT-Grundschutz Praktiker

Agenda

1. Ausgangslage
2. Cloud Strategie
3. (Neue) Gefährdungslagen
4. Sicherheit

1. Ausgangslage

Ausgangslage – Cloud-Nutzung ist auch in Deutschland angekommen

2012 nutzten **37 %** der Unternehmen in Deutschland Cloud Computing. **2021** nutzen bereits **82** % der Unternehmen in Deutschland die Cloud.

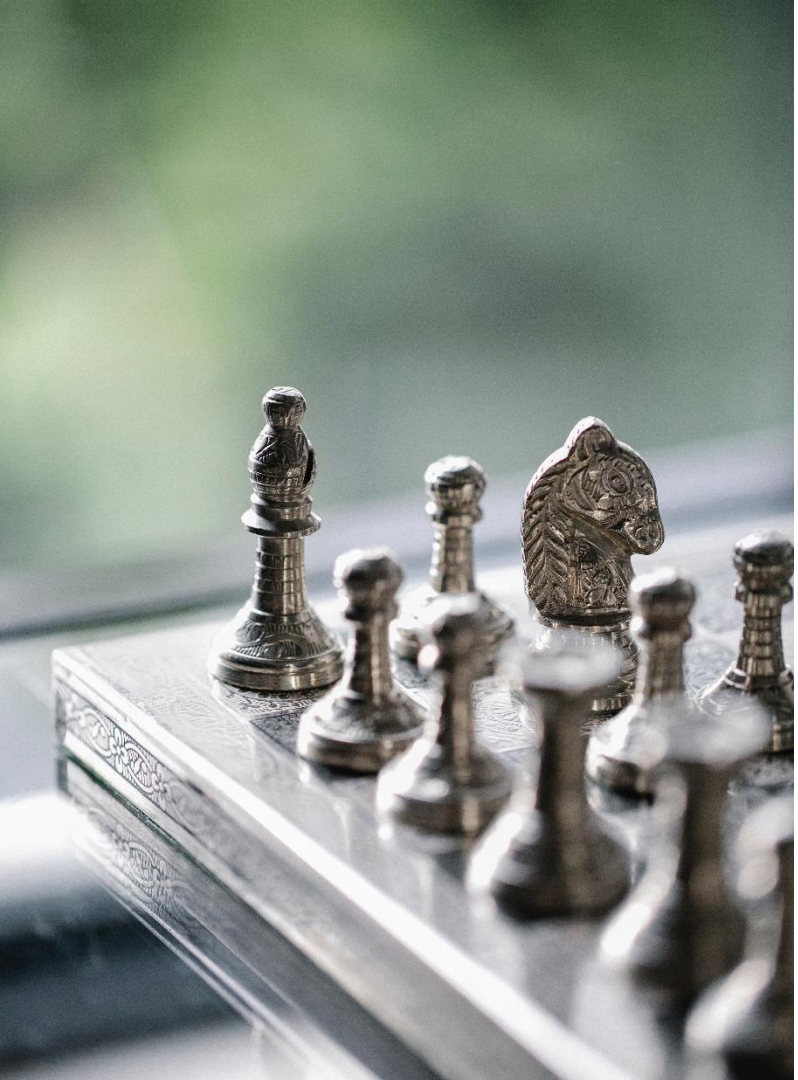
Die Nutzung der Public Cloud ist von **10 %** (**2012**) auf **46%** (**2021**) angestiegen, während die Nutzung der Private Cloud sich von **34 %** (**2012**) auf **63 %** (**2021**) erhöhte.

Quellen: Cloud-Monitor 2021, https://hub.kpmg.de/cloud-monitor-2021

Information security for use of cloud services

Cloud-Dienste müssen ganzheitlich betrachtet werden. Beginnend bei der Einführung über den Betrieb bis hin zur Exit-Strategie.

2. Cloud-Strategie



Cloud-Strategie

- Ziele, Chancen und Risiken der Cloud-Nutzung in der eigenen Organisation bestimmen
- Daraus ableiten, welche Cloud-Bereitstellungs- und -Service-Modelle in Frage kommen

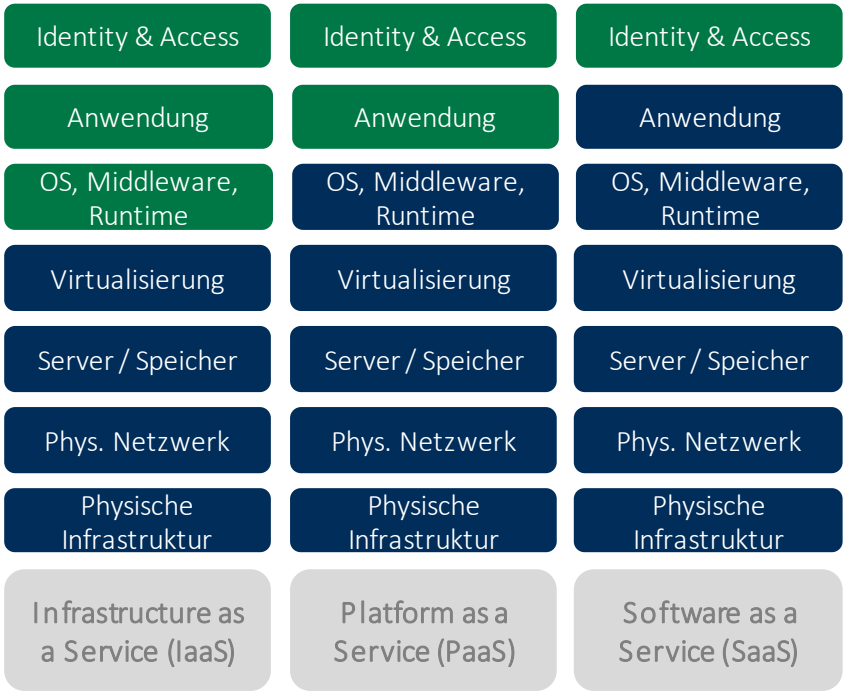
Bereitstellungs- und Service-Modelle

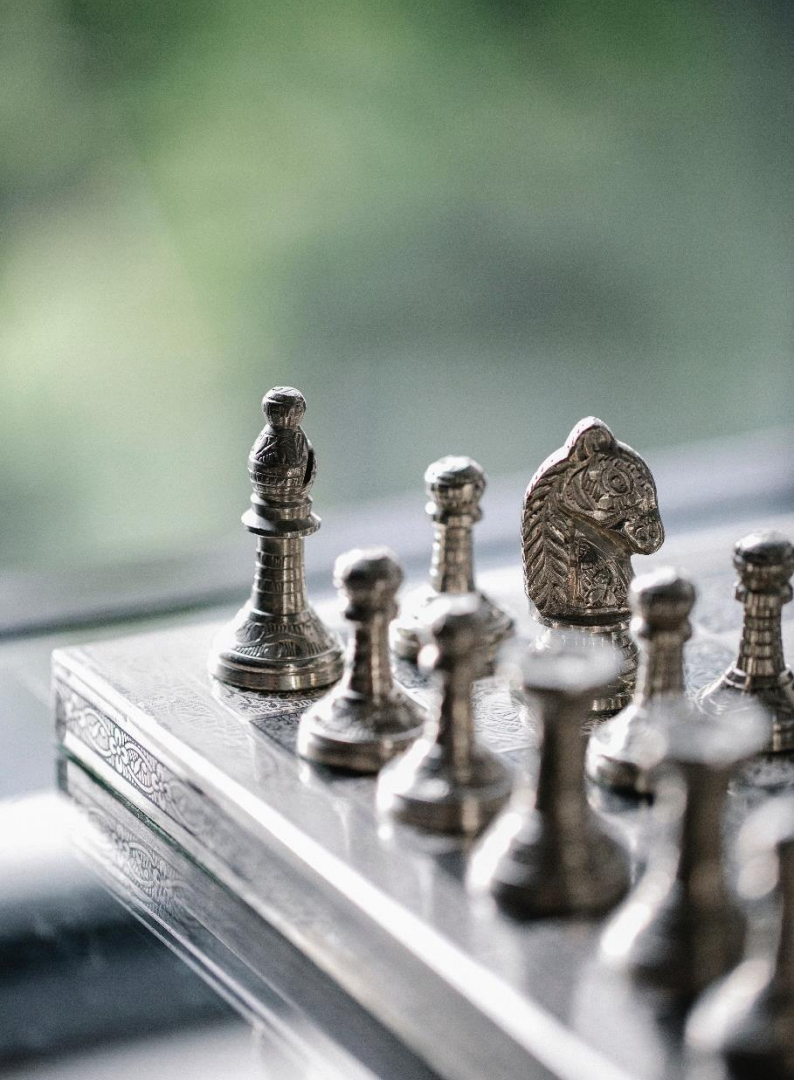
4 Bereitstellungsmodelle

- **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 vielen verschiedenen Cloud-Kunden genutzt.
- **Hybrid Cloud:** Es kommen zwei oder mehr Bereitstellungsmodelle 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.

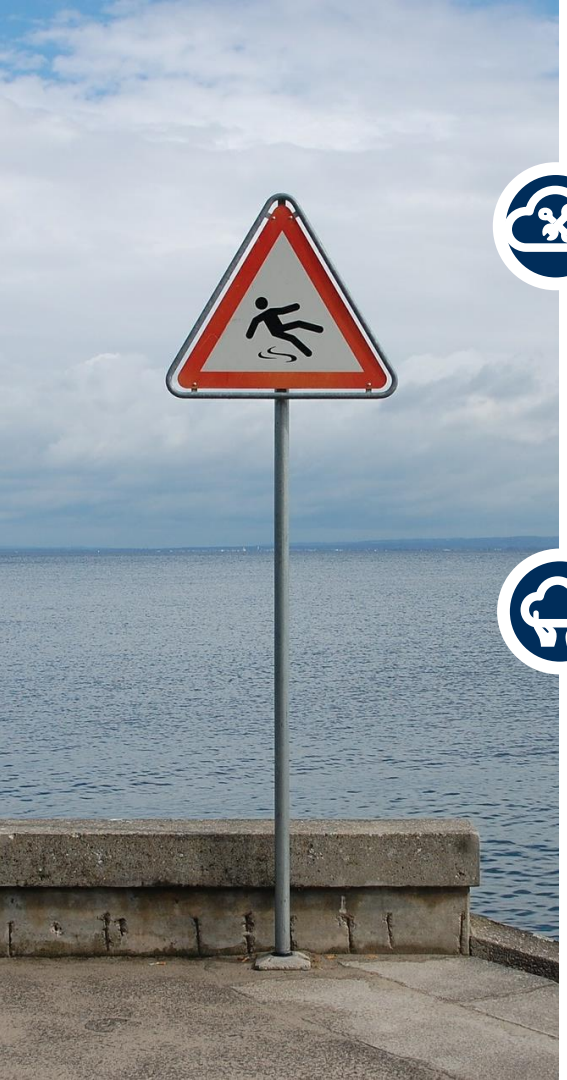




Cloud-Strategie

- Ziele, Chancen und Risiken der Cloud-Nutzung in der eigenen Organisation bestimmen
- Daraus ableiten, welche Cloud-Bereitstellungs- und -Service-Modelle in Frage kommen
- Mögliche Ergebnisse:
  - Cloud-only
  - Cloud-first (für Testumgebungen)
  - On-premise-first (für Kernsysteme)
  - Etc.

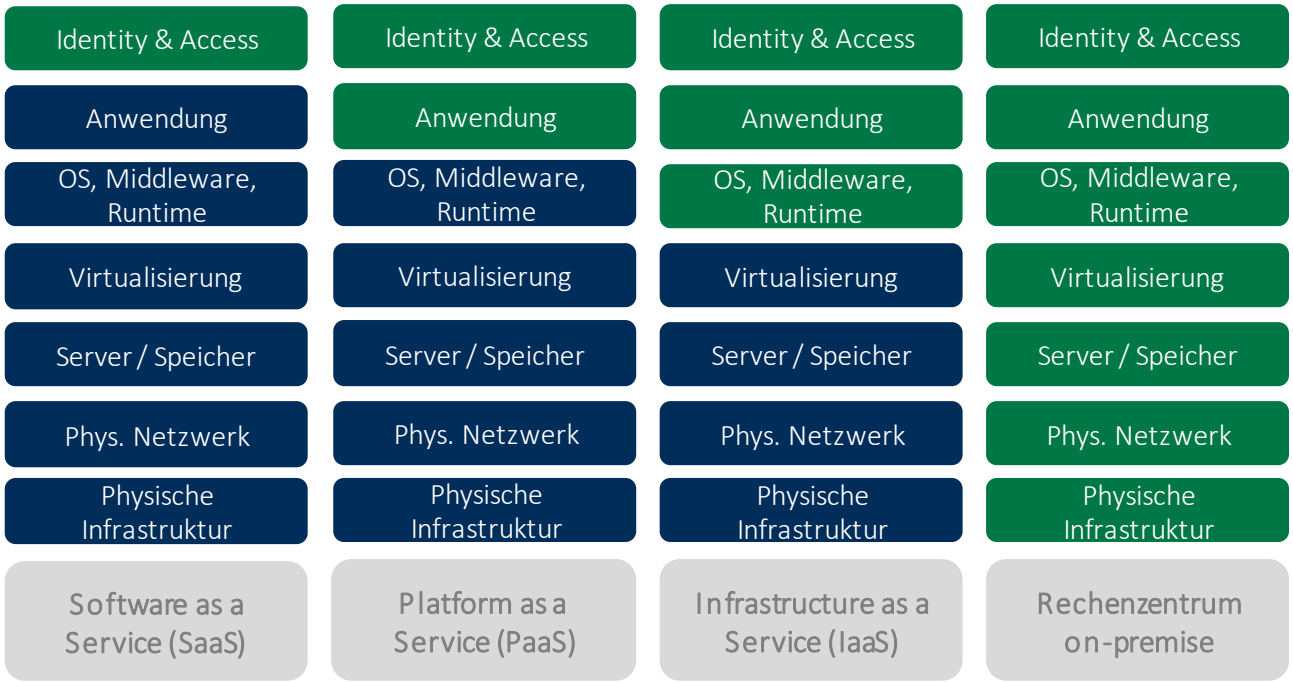
3. (Neue) Gefährdungslage



(Neue) Gefährdungen

- **Unzureichende Härtung/Konfiguration**
  - Häufige Ursache für erfolgreiche Angriffe
  - Cloud-Dienste sind per Default meistens auf Funktionalität getrimmt
  - Ungenutzte Dienste, welche jedoch nicht deaktiviert werden können
- **Unklare Verantwortlichkeiten**
  - Die Verantwortung für die Sicherheit des Cloud-Dienstes verteilt sich auf den Cloud-Anbieter und den Cloud-Nutzer
  - Missverständnisse bzw. mangelndes Bewusstsein können zu einem falschen Gefühl von Sicherheit führen

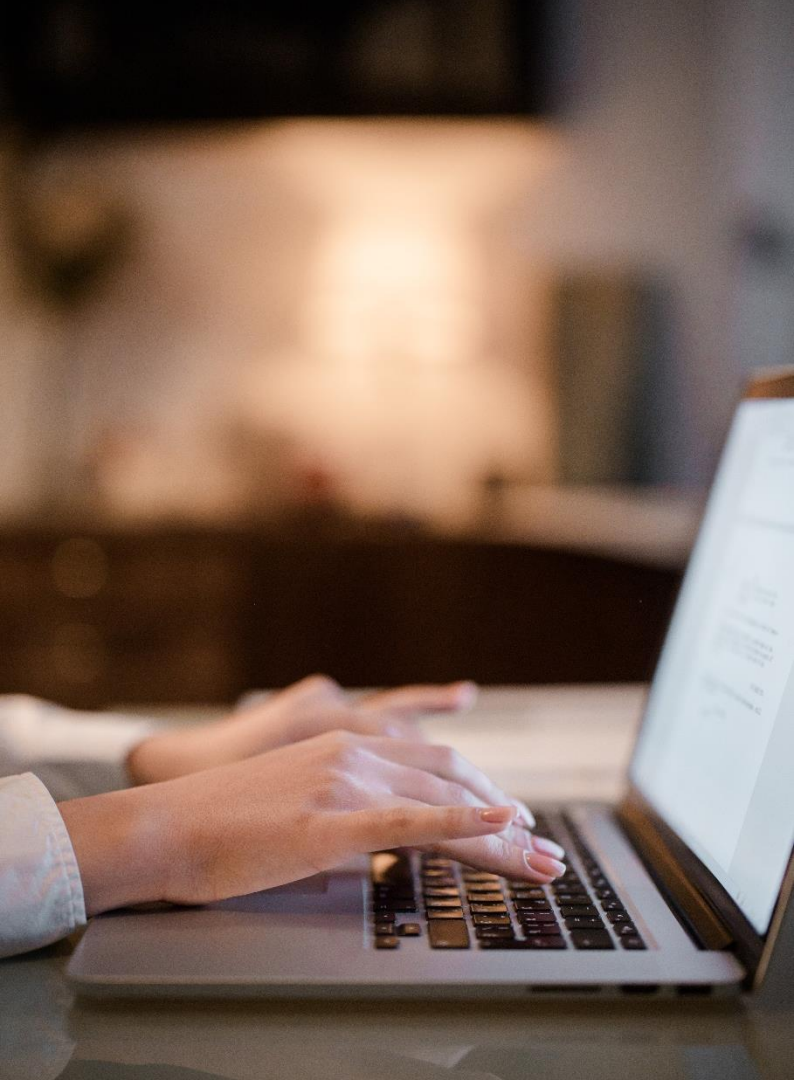
Geteilte Verantwortung



(Neue) Gefährdungen

- **Vendor Lock-In**
  - Finanzielle Auswirkungen aufgrund steigender Servicekosten, die nicht vermieden werden können
  - Verlust von Daten beim Anbieterwechsel
  - Schlechter oder langsamer Support, einschließlich beim Schließen von Schwachstellen
- **Vendor Lock-Out**
  - Beim Cloud Vendor Lock-Out ist der Cloud-Anbieter insolvent und ein Zugriff auf Daten / Anwendungen ist nicht oder nur eingeschränkt möglich.

4. Sicherheit



Sicherheitsrichtlinie für die Cloud-Nutzung (Cloud-Policy)

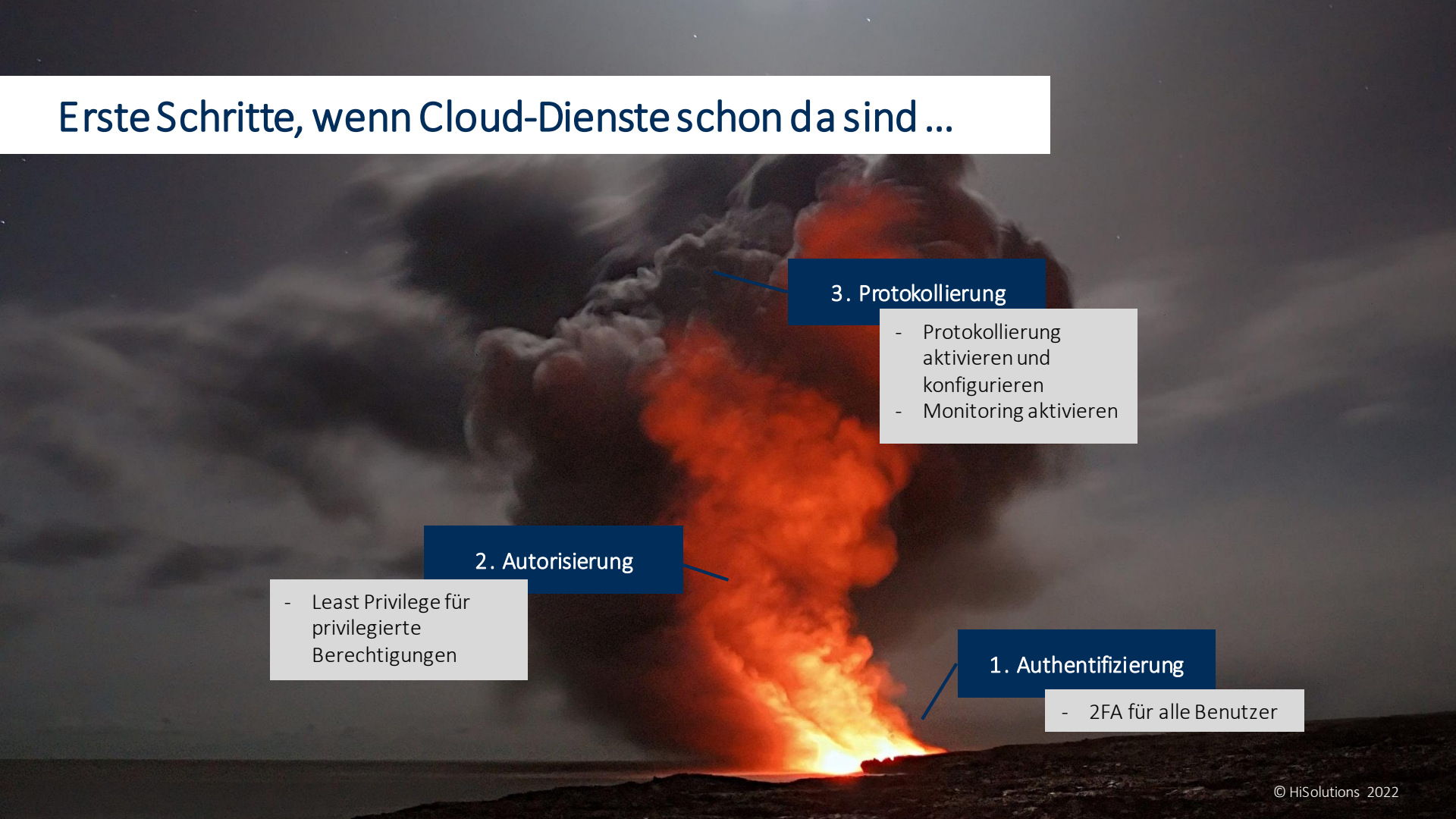
- Anforderungen an sich selbst
  - Übersicht der eingesetzten Cloud-Dienste
  - Einbindung bestimmter Rollen (Informationssicherheit, Datenschutz, Betriebsrat und etc.)
  - Erstellung einer Exit-Strategie
  - Regelmäßige Prüfung der Zertifizierungen
  - Vertragsgestaltung

- Anforderungen an den Cloud-Dienst
  - Abhängig vom Risikoappetit bzw. Schutzbedarf

Typische Anforderungen

- Zwei-Faktor-Authentifizierung für Nutzung und Administration
- Verschlüsselung der Kommunikation
- Nachweis über Einhaltung gängiger Sicherheitsstandards
  - ISO 27001
  - BSI C5
  - ISO 22301
- Zentrale Benutzerverwaltung
- Zentrale Berechtigungsverwaltung
- Zentrale Protokollierung

Erste Schritte, wenn Cloud-Dienste schon da sind …



3. Protokollierung

- Protokollierung aktivieren und konfigurieren
- Monitoring aktivieren

2. Autorisierung

- Least Privilege für privilegierte Berechtigungen

1. Authentifizierung

- 2FA für alle Benutzer

Schloßstraße 1 | 12163 Berlin

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

www.hisolutions.com