
CLOUD
INSIGHTS
02. Februar 2022

ORGANISATORISCHES

Diese Online-Veranstaltung wird aufgezeichnet.

Wir nutzen das freundliche „DU“ ☺

Nutzt den Chat-Bereich (auch anonym), um eure Fragen zu stellen.

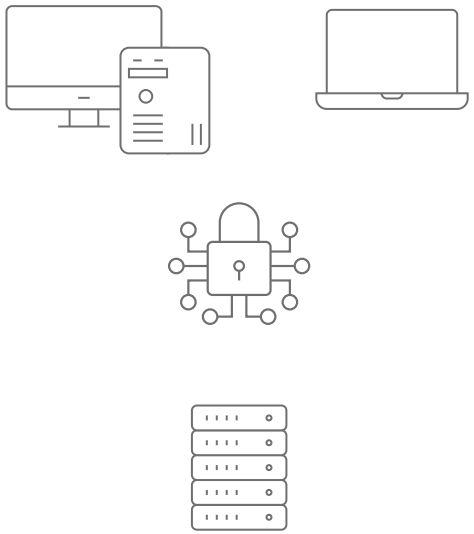
Im Nachgang erhaltet ihr einen Link zur Aufzeichnung und Präsentation.

Cloud Security:
Wie sicher ist die Cloud?

Tomasz Lawicki
m3 management consulting GmbH

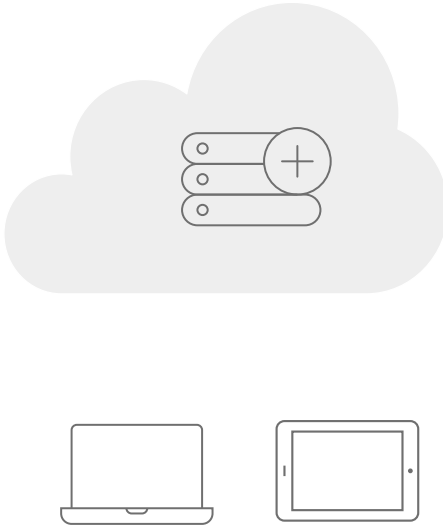
On-Premises oder Cloud: was ist sicherer?

On-premises



VS.

Cloud

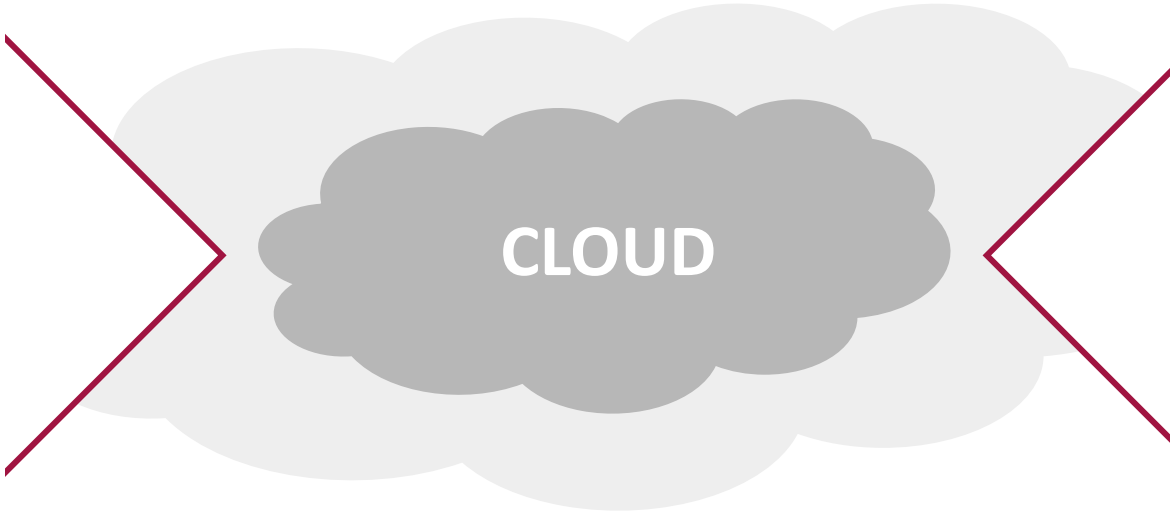


Allgemein betrachtet bietet die „Cloud“-Welt eine höhere Sicherheit
im Vergleich mit der „on-premises“-Welt eines durchschnittlichen KMUs.

Risiken verbunden mit der Nutzung der Cloud-Dienste

Allgemeine Risiken

- Cyber-Risiken
- Menschliche Handlung
- Technische Risiken
- Naturgewalt-Risiken
- Rechtliche Risiken



Erhöhtes Risiko bei der Cloud-Nutzung

- Verfügbarkeit
- Cyber-Kriminalität
- IT-Compliance

Die Nutzung der Cloud-Dienste bietet neben Chancen auch Risiken,
die aber durch geeignete Sicherheitsmaßnahmen mitigiert werden können.

Anforderungen an die IT-Compliance

DSGVO

IT-SiG

NIS-RL

GeschGehG

...

Die Cloud Service Provider (CSP) bieten bereits vorbereitete Dokumentation und eine automatisierte Prüfung der Konfiguration gegen die gängigen Compliance-Vorgaben an. Diese müssen gegen die individuellen Vorgaben des Unternehmens validiert und ggf. entsprechend erweitert werden.

Datenschutzbestimmungen & Fallstricke

- Seit 25. Mai 2018 gilt europaweit die EU-Datenschutzgrundverordnung (DSGVO; eng: GDPR). Übrigens gilt sie für alle EU-Mitglieder sowie alle Unternehmen, die ihr Geschäfte mit oder in der EU betreiben. Die DSGVO regelt den Schutz personenbezogener Daten.
- Gem. Art 32 DSGVO sind der Verantwortliche und der Verarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um dem Risiko angemessenes Schutzniveau zu gewährleisten.
- In Zusammenhang mit der Cloud wird der Cloud-Anwender (Nutzer der Cloud-Dienste) seitens der Aufsichtsbehörden als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO verstanden. Der Cloud-Anbieter (z.B. CSP) ist der Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO.
- Zwischen dem Anwender und dem Anbieter ist ein Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 Satz 1 DSGVO zu schließen.

Datenschutzbestimmungen & Fallstricke

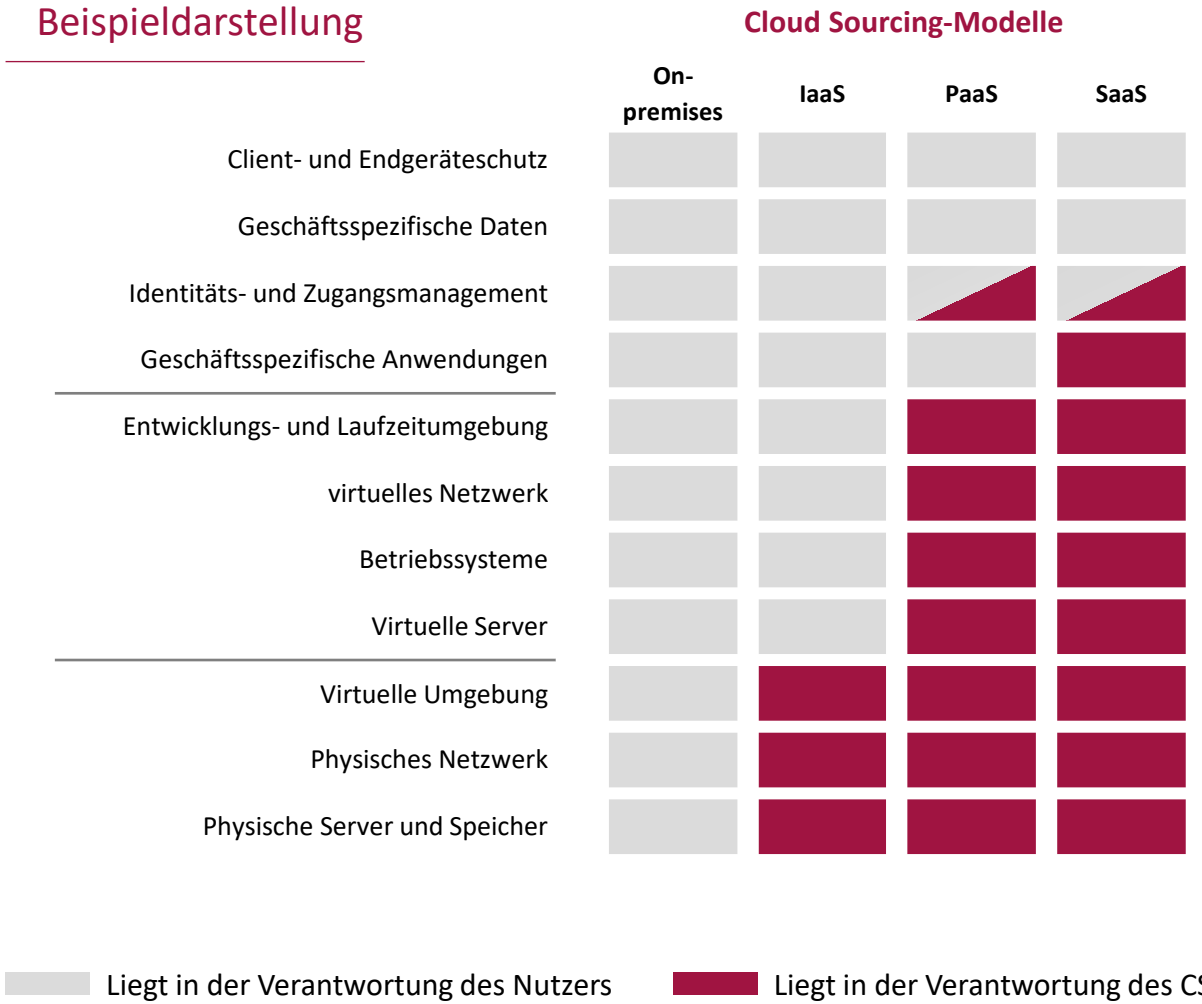
Privacy shield

EU-Standardvertragsklauseln

- Da insbesondere die s.g. Hyperscaler (Ms Azure, AWS, Google) ihre Daten nicht zwingend in der EU speichern, reicht der Abschluss von Auftragsverarbeitungsverträgen für den Datentransfer (personenbezogener Daten) in ein Drittland (in diesem Fall USA) nicht aus.
- Auch können sich die Anbieter aus den USA seit der Entscheidung des EuGH (vg. Schremps II Urteil, 07/2020) nicht mehr auf Privacy Shield berufen.
- Hierfür werden seitens der EU-Kommission die s.g. EU-Standarddatenschutzklauseln (SCC) empfohlen.

Geteilte Verantwortung oder doch nicht…

Beispieldarstellung



Die Verantwortung hängt immer von den Komponenten/Assets ab, die der jeweilige Beteiligte bereitstellt und in seinem unmittelbaren Zugriff hat.

Aus Sicht der Cloud Security ist es existenziell, sich im Vorwege der Cloud Nutzung klar zu machen, wie die Verantwortung für einzelnen Elemente geregelt ist.

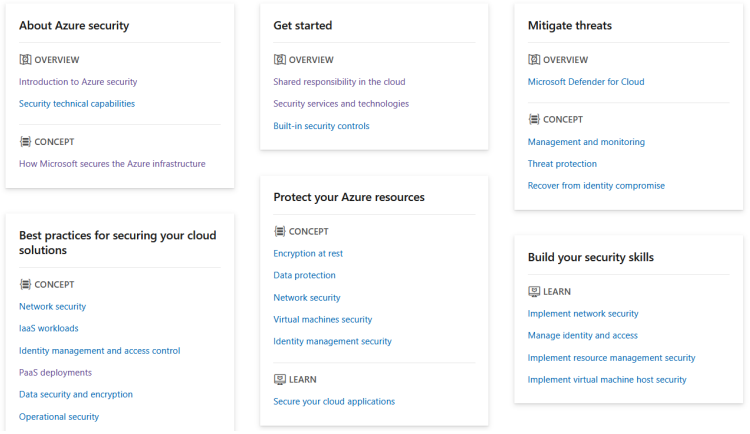
Wer ist zuständig für was?

In Abhängigkeit davon müssen Sicherheitsmaßnahmen gezielt aufgesetzt werden.

Technische Sicherheitsmaßnahmen bei den CSPs

Azure Security Center

https://docs.microsoft.com/en-us/azure/security/fundamentals/



AWS Cloud Security

https://aws.amazon.com/de/products/security/

Kategorie	Anwendungsfälle	AWS Service
Identity and Access Management	Sichere Verwaltung des Zugriffs auf Services und Ressourcen	**AWS Identity and Access Management (IAM)**
	Single Sign-On (SSO)-Service für die Cloud	**AWS Single Sign-On**
	Identitätsverwaltung für Ihre Apps	**Amazon Cognito**
	Verwaltetes Microsoft Active Directory	**AWS Directory Service**
	Einfacher und sicherer Service zum Teilen von AWS-Ressourcen	**AWS Resource Access Manager**
	Zentrale Steuerung und Verwaltung über AWS-Konten hinweg	**AWS Organizations**
Erkennung	Einheitliches Sicherheits- und Compliance-Zentrum	**AWS Security Hub**
	Verwalteter Service zur Bedrohungserkennung	**Amazon GuardDuty**
	Analysieren der Anwendungssicherheit	**Amazon Inspector**
	Aufzeichnen und Beurteilen der Konfigurationen Ihrer AWS-Ressourcen	**AWS Config**
	Nachverfolgen der Benutzeraktivität und API-Nutzung	**AWS CloudTrail**
	Sicherheitsverwaltung für IoT-Geräte	**AWS IoT Device Defender**

Google Cloud Armor

https://cloud.google.com/armor

Vordefinierte WAF-Regeln zur Minderung der OWASP-Top-10-Risiken	Sofort einsatzbereite Regeln basierend auf Branchenstandards, um gängige Sicherheitslücken in Webanwendungen zu vermeiden und Schutz für die OWASP Top 10 zu gewährleisten.
Umfassende Regelsprache für Web Application Firewall	Erstellen Sie benutzerdefinierte Regeln mit einer Kombination aus L3- bis L7-Parametern und Standortbestimmung, um Ihre Bereitstellung mit einer flexiblen Regelsprache zu schützen.
Transparenz und Monitoring	Behalten Sie die Messwerte, die mit Ihren Sicherheitsrichtlinien zusammenhängen, auf dem Cloud Monitoring-Dashboard im Blick. Sie können sich auch verdächtige Muster im Anwendungstraffic aus Cloud Armor direkt im Security Command Center-Dashboard anzeigen lassen.

Jeder CSP bietet in seinem Angebot viele technische Sicherheitsmaßnahmen an, die individuell für den Cloud Nutzer auf seinen Bedarf konfiguriert werden müssen.

Technische Sicherheitsmaßnahmen

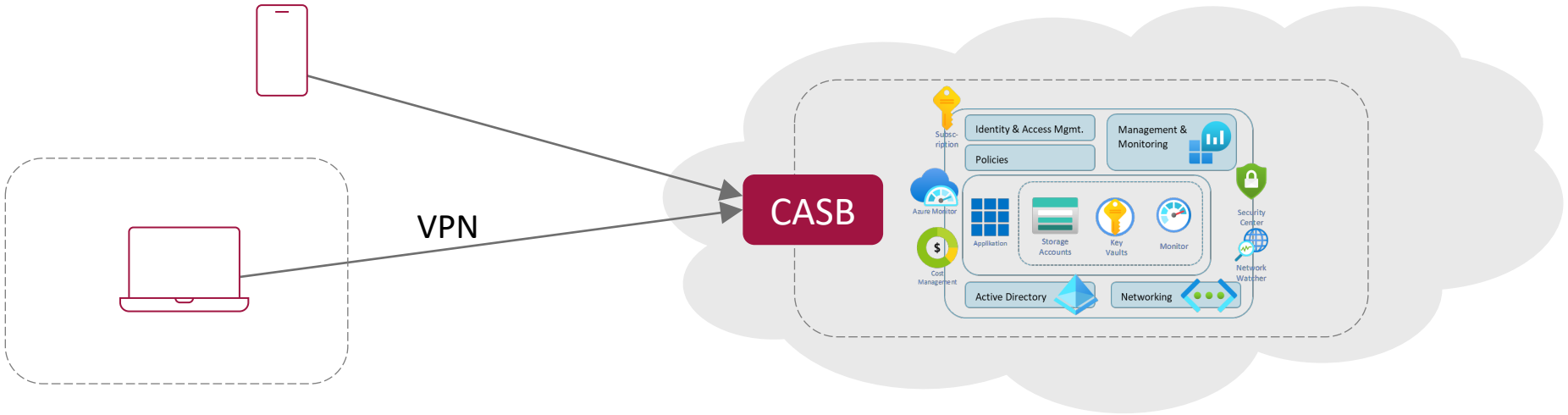
Auswahl

Vergleich mit on-premises	Microsoft Azure	aws	Google Cloud
Firewall & ACL	Network Security Groups/ Azure Firewall	Security Groups AWS Network ACLs	Cloud Armor VPC Firewall
Web Application Firewall (WAF)	Azure Application Gateway	AWS WAF AWS Firewall Manager	nur 3. Anbieter
Data Loss Prevention	Azure Information Protection (AIP)	Amazon Macie	Cloud Data Loss Prevention API
Endpoint Protection	Microsoft Defender ATP	nur 3. Anbieter	nur 3. Anbieter
DDoS Protection	Azure DDoS	Cloud Shield	Cloud Armor
Governance, Risk and Compliance	Azure Security Center	AWS Compliance Center	Cloud Security Command Center
...	...	...	...

Manche Sicherheitsmaßnahmen sind bereits standardmäßig verfügbar. Andere müssen gezielt konfiguriert werden und sie sind nur entgeltlich verfügbar.

Je nach Sourcing-Modell und den Schutzbedarf ist eine Erweiterung durch externe technische Sicherheitsmaßnahmen sinnvoll.

Cloud Access Security Broker (CASB)

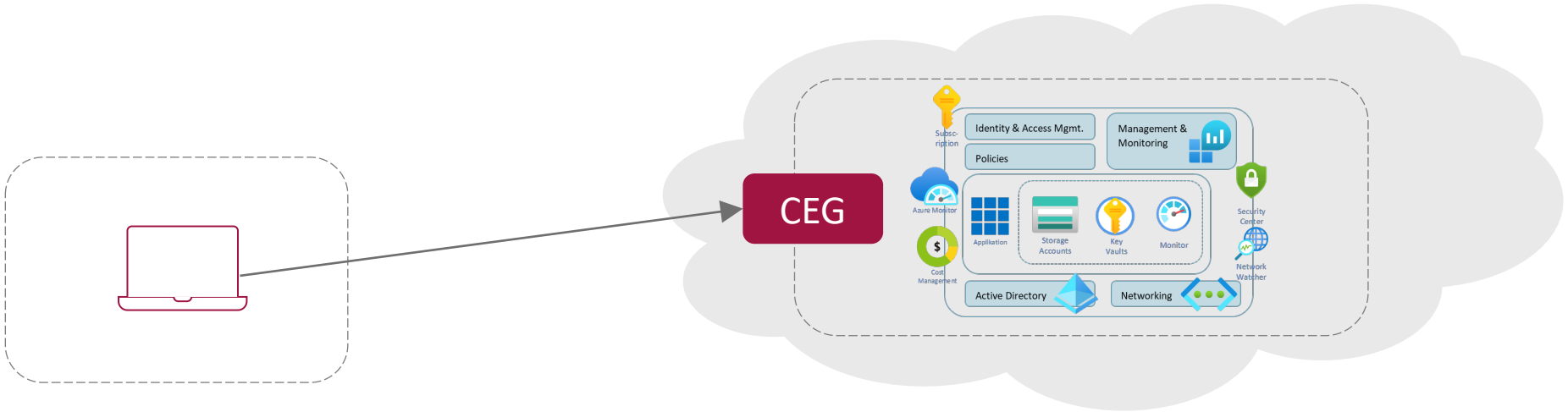


CASB erfasst, überwacht und kontrolliert den Zugriff der Anwender eigener Organisation auf die genutzten Cloud-Dienste.

Damit ermöglicht es Nutzungsrichtlinien (Policies) zu definieren und zu überwachen.

CASB kann ebenfalls Funktionalitäten zu Data Loss Prevention enthalten, eine automatisierte Klassifizierung der Daten durchführen sowie das ungewollte Verhalten (durch Dritte) in den Anwendungen und Datenbeständen identifizieren und melden.

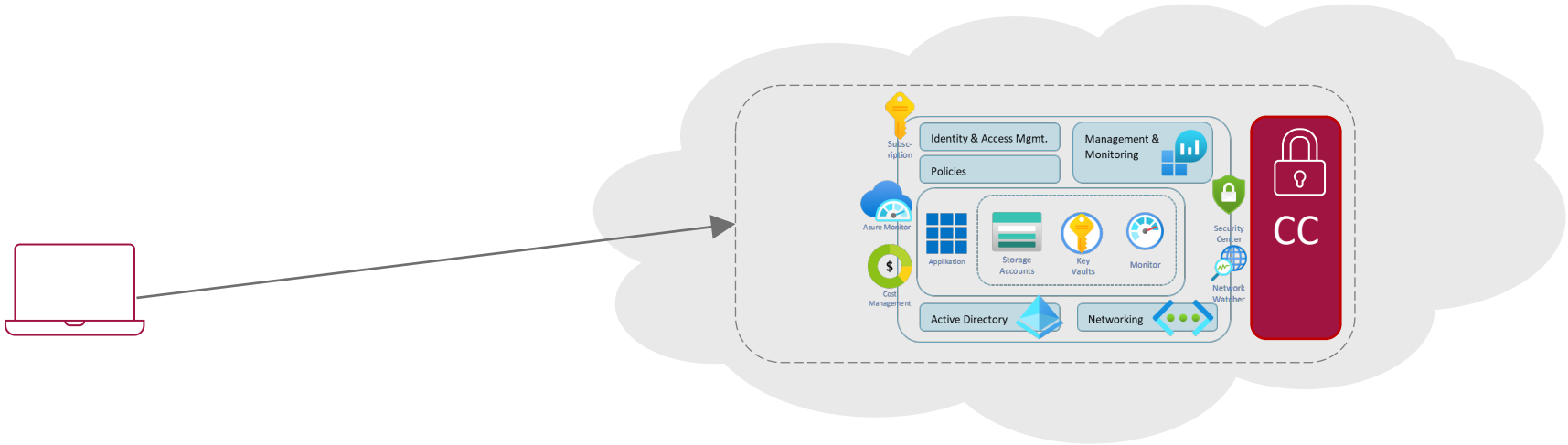
Cloud Encryption Gateway (CEG)



Wenn beispielsweise sensible Daten in einer Cloud Umgebung abgelegt werden sollen, kann die Sicherheit durch den Einsatz von sogenannten Cloud Encryption Gateways (CEG) erhöht werden.

Diese sorgen dafür, dass die Daten noch vor Verlassen der internen Umgebung verschlüsselt werden. Besonders Rolle spielt hierbei das Schlüsselmanagement, das ausschließlich unter der Kontrolle des Anwenderunternehmens liegen muss.

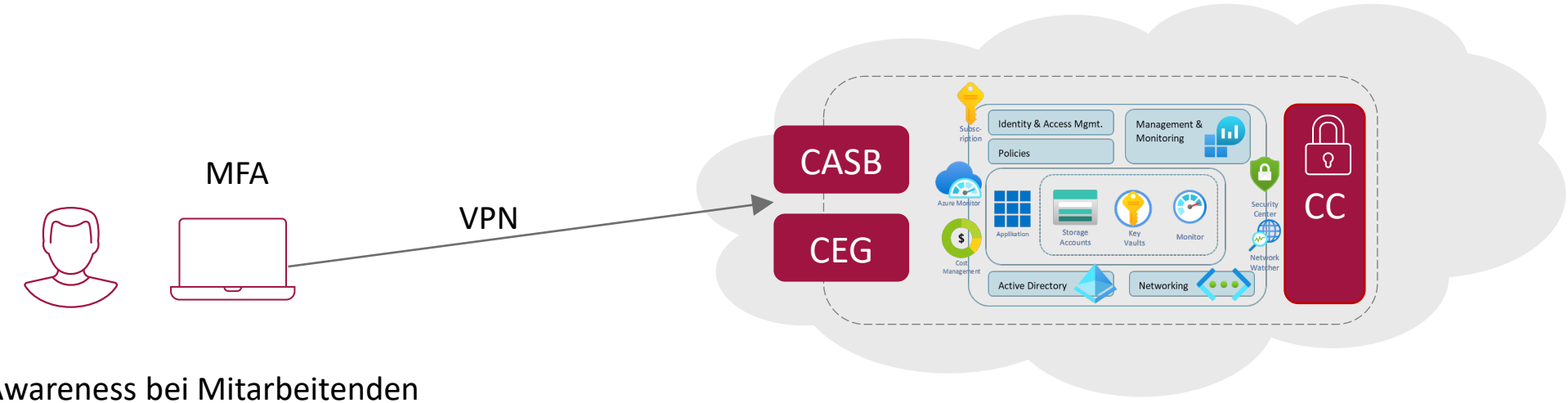
Confidential computing (CC)



Während der Verarbeitung können besonders sensible Daten (z.B. KRITIS Daten) mit Hilfe von s.g. confidential computing vom (bewussten oder unbewussten) Zugriffen durch die Admins geschützt werden.

Dabei handelt es sich um einen von der Außenwelt abgeschirmten Bereich oder Kapsel, in dem die komplette Datenverarbeitung im unverschlüsselten Zustand stattfindet. Diese Abschirmung kann entweder direkt auf dem Prozessorchip der Server und/oder gleich über mehrere Server umgesetzt werden.

Best practises für eine sichere Cloud



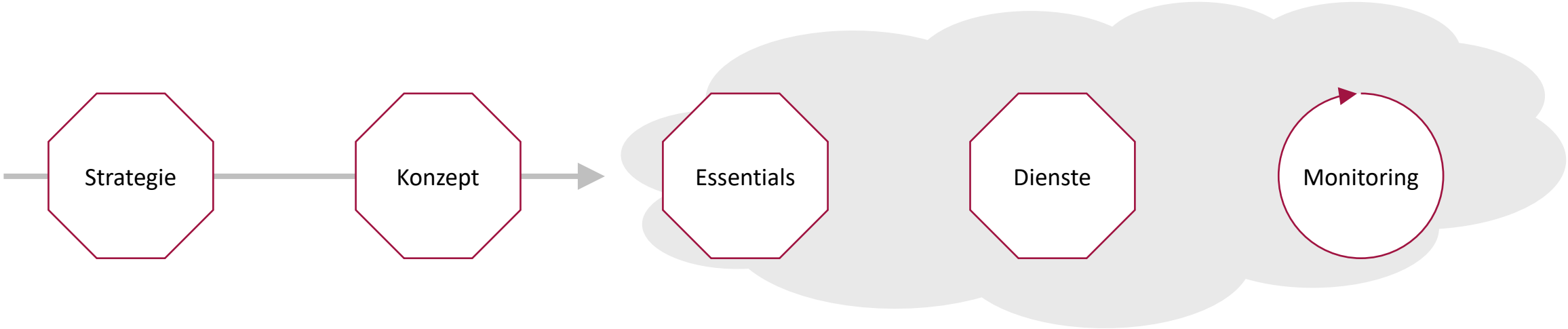
- Awareness bei Mitarbeitenden
- Endgeräteschutz

Cloud Security muss gesamtheitlich betrachtet werden. Ein zentraler Bestandteil ist dabei die Identitäts- und Datensicherheit.

- MFA
- Rechtemanagement (RBAC)
- Single Sign-On
- CASB
- CSP Tools

- WAF
- Cloud Netzwerk Segmentierung
- Datenverschlüsselung
- Backup-Strategie / Notfallplanung
- Confidential computing (b. B.)

Der Weg in die Cloud beginnt lange bevor die Cloud-Dienste genutzt werden



- Eigenen Bedarf kennen
- Übergreifende Cloud Strategie festlegen
- Kritische Daten und Prozesse kennen
- Schutzbedarf analysieren

- Cloud Konzept erstellen
- CSP auswählen
- Aufgabenverantwortung klären
- CSP Sicherheitsmaßnahmen kennen und Lücken identifizieren
- Ergänzende externe Sicherheits-Maßnahmen identifizieren
- Vertragliche Themen klären

- Cloud Umgebung konfigurieren (Security Essentials)
- CSP Sicherheitsmaßnahmen aktivieren
- Bei Bedarf durch externe technische Maßnahmen ergänzen
- Monitoring aktivieren

- Erst jetzt werden die ersten Dienste/Services genutzt oder bestehende Apps umgezogen.

- Cloud Security ist ein Prozess.
- Es genügt nicht, die Maßnahmen einmalig aufzusetzen. Sie müssen überwacht und ggfs. angepasst werden.

Fazit

- Die Cloud kann durch geeignete Maßnahmen sicher aufgesetzt und betrieben werden.
- Für viele Unternehmen bedeutet der Umstieg von der on-premises Welt in die Cloud-Welt eine Verbesserung der IT-Sicherheit.
- Dennoch muss die Cloud-Umgebung gut vorbereitet sein, bevor die ersten Dienste genutzt werden.

Vielen Dank!

Q & A

CLOUD INSIGHTS

Kommende Online-Seminare

#digitalisierenmitmehrwert

16.02.2022 I Michael Schäfer

Cloud-Native Architecture – Wie können wir die Vorteile der Cloud optimal nutzen?

09.03.2022 I Philipp Dühring & Stefan Kurz

Cloud Security in der Praxis – am Beispiel von AWS

23.03.2022 I Matthias Meyer

Hochskalierbare Cloud-Architekturen am Beispiel von Cassandra

06.04.2022 I Victor Ionescu & Walter Knaub

Azure DevOps services: From Dev to DevOps – Let the journey begin

....

Registrierungslink:

www.msg.group/cloud#events

Kontakt

Tomasz Lawicki
Senior Manager

Tomasz.Lawicki@m3maco.com

msg systems ag
Robert-Bürkle-Straße 1
85737 Ismaning

+49 89 96101-0
+49 89 96101-1113

info@msg.group

value – inspired by people