Dipl. Ing. Uwe Irmer

Cloud Security Band 2

Best Practice 2. Auflage 2021

Was du siehst, ist nicht das,
was die Cloud von dir weiss.

Uwe Irmer, März 2020

Inhaltsverzeichnis

VORWORT

ABKÜRZUNGEN UND BEGRIFFE

ABBILDUNGSVERZEICHNIS

DEFINITIONEN

EINLEITUNG

Best Practice zur Einführung von Cloud Technologie

Technische Massnahmen

Organisatorische Massnahmen

Warum scheitern Migrationsprojekte?

CLOUD SERVICE MODELLE

Infrastructure as a Service IaaS

Plattform as a Service PaaS

Software as a Service SaaS

Container as a Service CaaS

Verantwortlichkeiten für die Sicherstellung der Informationssicherheit

Eingriffsmöglichkeiten des Consumers

Zusammenfassung zur Informationssicherheit

FRAMEWORKS

Jericho

NIST Cybersecurity Framework

OWASP Software Security

ISO 27017 und 27018

TECHNISCHE MASSNAHMEN

Cloud Provider Modelle

- Amazon
- Azure
- Google

Key Management

Datenverschlüsselung

Verschlüsselung von Datenbanken

Absicherung der Endpoints

Container

Security Modelle für Container Technologie

- Aktuelle Versionen der eingesetzten Betriebssysteme und Frameworks
- Kontrolle der Zugriffe
- Deployment von Containern und der CI/ CD Prozess
- Logging und Monitoring
- Weitere Massnahmen

ORGANISATORISCHE MASSNAHMEN

Exit Strategie

Multi Cloud Strategie

Extreme Dynamic in Cloud Services

Agile

DevOps

- Continuous Monitoring CM
- CI/ CD

Microservices
Infrastructure as Code
Überwachung und Logging
Kommunikation und Zusammenarbeit

BENEFITS UND MEHR

Vorteile
Risiken

QUO VADIS

QUELLENVERZEICHNIS

Vorwort

Gemäss den Analysen von IDC in Zusammenarbeit mit der Swisscom [1] befassen sich über 70% der Schweizer Unternehmen mit dem Gedanken, Cloud Technologie zu nutzen. Gleiches gilt für Unternehmen in der Europäischen Union EU, wie Analysen von Forrester [2] zeigen.

Als Hauptgrund für den Wechsel in die Cloud nennen die befragten Unternehmen die Einsparungen für die Betriebskosten und Kosten für das Operating. Die Erwartung sind die Verschiebung von Investitionsaufwendungen (CapEx) zu Betriebsausgaben (OpEx), die Verlagerung operativer Risiken sowie die Steigerung der Flexibilität bei reduziertem Aufwand.

Zum Zeitpunkt der Veröffentlichung dieses Buches kommt noch ein weiterer Aspekt hinzu. Die Corona Krise, die seit März 2020 die gesamte Welt beeinflusst. Vor diesem Hintergrund suchen die Unternehmen dringend nach Lösungen ausserhalb der eigenen IT Infrastruktur in der Absicht, Services verlagern zu können. Dies, um so den Betrieb aufrecht erhalten zu können, sollte eigenes Personal zum Unterhalt der IT Infrastruktur ausfallen.

Doch wie ist der Weg in die Cloud?

Wie kann ein Unternehmen seine bestehende IT Infrastruktur in die Cloud verlagern unter Einhaltung der geltenden Regularien sowie unter Sicherstellung der Schutzbedürfnisse?

Welche Risiken entstehen und welche Veränderungen bedeutet der Wechsel zur Cloud Technologie?

In vielen Unternehmen, hauptsächlich im Bereich Software Entwicklung und Services, überwiegt die Motivation, mittels Cloud Technologie kürzere Bereitstellungszeiten für neue Produkte oder Produktversionen zu erreichen. Hierfür werden neue Prozesse wie CI/ CD (Continuous Integration/ Continuous Delivery) eingeführt in der Überzeugung, alles Erforderliche im Bereich Produkt und Service Erstellung unternommen zu haben. Die Praxis zeigt jedoch, dass derartige Vorhaben oftmals scheitern.

Eine wichtige Erkenntnis ist, dass es kein Umsetzungsvorhaben zur Cloud Technologie ohne grundlegende organisatorische Änderungen im Unternehmen gibt. So sind nicht nur die Unternehmensbereiche von Änderungen betroffen, die unmittelbar im Zusammenhang mit Produkten oder Services stehen. Vielmehr benötigt das gesamte Unternehmen eine neue Kultur, neue Vorgehensweisen, neue Prozesse oder kurzgefasst, eine neue Governance.

Im Band 1 dieser Buchreihe Cloud Security wurden die grundlegenden organisatorischen Aspekte erörtert, die bei einem Wechsel hin zur Cloud Technologie zu beachten sind. Zudem wurden dort die Grundlagen der Cloud Technologie beschrieben.

Der vorliegende Band 2 der Buchreihe befasst sich vertiefend mit den möglichen Cloud Architekturen und Delivery Modellen sowie technischen und organisatorischen Massnahmen, um einen best practice Weg zu beschreiben, anhand dessen Unternehmen zielgerichtet und dauerhaft erfolgreich die Cloud Technologie nutzen können.

Abkürzungen und Begriffe

CaaS	Container as a Service
CDN	Content Delivery Network
CI/ CD	Continuous Integration/ Continuous Deployment
CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
deploy	Verteilen, zum Beispiel ein Artefakt in die Produktionsumgebung installieren.
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IoT	Internet of Things
ISMS	Information Sicherheit Management System
IT	Informationstechnologie
KI	Künstliche Intelligenz
Major Release	Haupt Version
PaaS	Plattform as a Service
PC	Personal Computer
SaaS	Software as a Service
VPN	Virtuelles Privates Netzwerk
WAF	Web Application Firewall
WLAN	Wireless Local Area Network

Abbildungsverzeichnis

Nummer	Titel
1	Migration zur Cloud Technologie
2	Verantwortlichkeiten nach Servicemodell
3	Cloud Modelle und Einflussnahme
4	Cloud Kube Modell
5	Daten Life Cycle
6	Containerisierung
7	Einsatz unterschiedlicher Container Orchestratoren
8	Vorgehen agiler Teams nach Scrum
9	Kanban Board
10	DevOps

Definitionen

[i]	Asset	Die Werte des Unternehmens, dies können neben monetären Grössen auch Reputation, Patente, Prozesse, die Mitarbeitenden etc. sein.
[ii]	Entität	Die Entität ist ein Objekt innerhalb der Information Technologie und beschreibt, wie Beziehungen in den Prozessen der Information Technologie hergestellt werden. Entitäten sind natürliche Personen, Prozesse oder Services.
[iii]	leased privilege	Dieses Prinzip stellt sicher, dass Entitäten nur mit den Berechtigungen ausgestattet werden, die diese mindesten benötigen. Weitergehende Privilegien werden nicht erteilt.
[iv]	Artefakt	Ergebnis aus einem Arbeitsprozess, zum Beispiel ein neuer Service in der Informationstechnologie
[v]	Deploy	Verteilen, ein Artefakt in eine Betriebsumgebung bringen um den Service bereitzustellen.
[vi]	Ressource	Eine Ressource im Zusammenhang mit der Cloud Technologie ist eine Komponente, die aus der Cloud bezogen wird und die kombinierbar ist. Beispiele für Ressourcen sind virtuelle Netzwerke, Storage oder virtuelle Server [3].
[vii]	Service	Ein Service ist die Kombination von Ressourcen, die für geschäftsrelevante Prozesse benötigt werden. Ein Beispiel hierfür ist das Customer Relationsship Management System CRM. Dieses besteht

		aus der Kombination von virtuellen Netzwerken, virtuellen Anwendungsservern, Datenbankservern, Benutzerauthentifizierung etc. [3].
[viii]	Provider	Ein Provider stellt Services für Dritte zur Verfügung. Je nach Ausprägung der Verträge nimmt der Provider mit mehr oder weniger Umfang den Betrieb und die Wartung der zugehörigen Ressourcen. [3]
[ix]	Consumer	Der Consumer bezieht Services von einem Provider. [3]
[x]	Epic	Epic ist eine user Story, die in weitere user Stories strukturiert wird. Dabei beschreibt das Epic Anforderungen an ein Produkt in einer allgemeinen Weise, die zu einem späteren Zeitpunkt genauer definiert werden sollen.
[xi]	Item	Bestandteil oder Element