MASTERARBEIT

Herausforderungen bei der Transformation von Unternehmensprozessen in die Cloud

ausgeführt am

am Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Armin Hirsch

Personenkennzeichen: 2010320020

Graz, am 13.12.2021 .....

Unterschrift

Ehrenwörtliche Erklärung

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

Kurzfassung

Auch heutzutage vertrauen noch viele Unternehmen auf eigene IT-Infrastruktur und veraltete Legacy-Anwendungen, um ihre geschäftskritischen Prozesse zu unterstützen. Allerdings gibt es mehrere kritische Bedenken, wie Wartbarkeit, Skalierbarkeit und Sicherheit, die mit dem Fortbestand eines Legacy-Systems und eigenständig verwalteter Infrastruktur verbunden sind. Vor diesem Hintergrund bieten Cloud-Services eine agilere und kostengünstigere Plattform, um Geschäftsprozesse zu unterstützen. Da die Akzeptanz von Cloud-Diensten in letzter Zeit zugenommen hat, hat auch die akademische Forschung im Bereich des Einsatzes von Cloud-Diensten zugenommen. Es besteht jedoch ein Bedarf an Sekundärstudien, um diese Forschung weiter zu stärken. Das primäre Ziel dieser Arbeit ist es, die prioritären Herausforderungen bei der Transformation von Geschäftsprozessen in die Cloud aufzuzeigen, und eine Übersicht über Migrationsstrategien zu liefern. Da der Wechsel von einer On-Premise-Lösung hin zu einer Cloud-Lösung durch technische und nicht-technische Faktoren beeinflusst wird, soll erörtert werden, worauf im Sinne einer erfolgreichen Migration besonders Wert gelegt werden muss. Im Rahmen dieser Untersuchung konnte gezeigt werden, dass die Faktoren Change-Management und Cybersecurity die größte Herausforderung für eine erfolgreiche Transformation von Geschäftsprozessen in die Cloud darstellen, und aktiv gemanagt, respektive sichergestellt werden müssen.

Abstract

Today, many organizations still rely on their own IT infrastructure and outdated legacy applications to support their business-critical processes. However, there are several critical concerns, such as maintainability, scalability, and security, associated with the continued existence of a legacy system and independently managed infrastructure. Cloud services offer a more agile and cost-effective platform to support business processes. As the adoption of cloud services has recently increased, academic research in the area of cloud service deployment has also increased. However, there is a need for secondary studies to further strengthen this research. The primary objective of this paper is to highlight the priority challenges in transforming business processes to the cloud, as well as to provide an overview of migration strategies. Since the change from an on-premise solution to a cloud solution is influenced by technical and non-technical factors, it will be discussed what must be given particular attention to achieve a successful migration. In the course of this study, it was shown that the factors of change management and cybersecurity represent the greatest challenge for a successful transformation of business processes to the cloud and they must be actively managed and ensured.

INHALTSVERZEICHNIS

1 EINLEITUNG

Das Thema Cloud-Computing hat im letzten Jahrzehnt einen kometenhaften Aufstieg durchlaufen, und ist zu einer der meistdiskutierten Technologien der letzten Zeit geworden. Und dieser Höhenflug neigt sich noch lange nicht dem Ende entgegen, was prognostizierte jährliche Wachstumsraten von 14.9% in den Jahren 2020 bis 2027 verdeutlichen. So hat sich die Diskussion um die Cloud-Einführung von „ob“ hin zu „wann“ und „wie“ gewandelt.

Für ein Unternehmen stellt Cloud-Computing nicht nur eine Möglichkeit dar, auf einen Hype zur Ressourcenbeschaffung aufzuspringen, sondern eröffnet neben neuen Geschäftsmodellen auch eine exzellente Möglichkeit, Kosten zu sparen. Wie Daten aus einer Analyse von Grand View Research zeigen, lassen sich die jährlichen Betriebskosten durch den Einsatz von Cloud-Computing um bis zu 35% reduzieren. Mitunter ein Grund, der verdeutlicht, wie eine Verdopplung des Cloud-Einsatzes innerhalb der Unternehmen im Jahr 2022, in Bezug auf 2018er Zahlen, zu Stande kommt. Damit würden rund 60% aller Unternehmen auf einen externen Cloud-Service-Anbieter zurückgreifen. (Grand View Research, 2020)

Der Begriff Cloud ist eine Metapher für das Internet und ist eine Abstraktion für die komplexe Infrastruktur, die sie verbirgt. Es gibt einige wichtige Punkte in der Definition, die in Bezug auf Cloud-Computing diskutiert werden. Cloud-Computing unterscheidet sich von traditionellen Computing-Paradigmen, da es skalierbar ist und als abstrakte Einheit gekapselt werden kann. Zusätzlich besteht die Möglichkeit zur Nutzung weiterer Dienste des Cloud Anbieters, sowie des Einsatzes dynamischer Konfigurationen.

Das Wertversprechen ist dabei vielschichtig, und umfasst neben signifikanten Kosteneinsparungen gegenüber einem traditionellen Rechenzentrumsansatz auch Möglichkeiten, schnelle, robuste, widerstandsfähige Anwendungen zu erstellen, die bei einem Anstieg des Datenverkehrs entsprechend skalieren, und bei einem Rückgang des Datenverkehrs wieder zurückgefahren werden können. Der Wechsel zu Cloud-Diensten kann damit eine dynamische und schnelle Möglichkeit sein, IT-Dienste nicht nur kosteneffizient zu betreiben, sondern auch Energie- und Administrationseinsparungen zu realisieren.

Organisationen, sowie auch Nutzer von Cloud-Diensten, sind allerdings auch mit Herausforderungen und Risiken konfrontiert. Da Organisationen von Natur aus komplexer werden, je größer sie sind, ist es sehr wichtig, dass Cloud-Computing einen echten Mehrwert liefert, und nicht nur

eine Plattform für einfache Aufgaben darstellt (wie z.B. das Speichern von Dateien und Dokumenten zum stetigen Zugriff aller).

Unternehmen müssen die Vorteile, Nachteile und die Auswirkungen von Cloud-Computing auf ihre Organisationen, sowie den geplanten Einsatzzweck, genauestens abwägen, um eine Entscheidungsbasis für eine etwaige Transformation in die Cloud zu schaffen. Für Unternehmen ist die Wirtschaftlichkeit oder der Kostenfaktor oftmals das oberste Kriterium, aber gleichzeitig sind Einfachheit, Akzeptanz, Flexibilität, Geschäftskontinuität und Compliance von ebenso hoher Bedeutung. Folglich müssen Unternehmen verstehen, wie sich Cloud-Computing auf all diese Aspekte auswirkt.

So ist die Akzeptanz innerhalb der Unternehmen zum Einsatz von Cloud-Computing bedeutend abhängiger vom Reifegrad der organisatorischen und kulturellen, einschließlich gesetzgeberischen, Prozesse als von der Technologie per se (Fellows, 2008).

Trotz einiger Vorteile von Cloud-Computing, und den erstaunlichen Wachstumsraten der letzten Jahre, zeigt sich, dass Unternehmen teilweise gezögert haben, auf Cloud-basierte Lösungen zu wechseln.

Es gibt verschiedene Faktoren, die diese Adoptionsraten beeinflusst haben. Die Arbeit versucht daher, die Herausforderungen, denen sich Unternehmen zur Transformation ihrer Unternehmensprozesse in die Cloud stellen müssen, aufzuzeigen, und Best-Practice Empfehlungen daraus abzuleiten.

1.1 Problemstellung und Zielsetzung

Traditionell beschaffen Unternehmen und Organisationen physische Hardware, um ihre IT-Infrastruktur zu betreiben. Allerdings hat die Verfügbarkeit von hoch performanten Mehrkernprozessor-Plattformen in Kombination mit Virtualisierungstechnologien und Hochgeschwindigkeits-Datennetzen dazu geführt, dass neue Möglichkeiten der Ressourcenbeschaffung etabliert wurden. Diese werden üblicherweise unter dem Begriff des Cloud-Computing zusammengefasst. Eine entsprechende Cloud Strategie muss jedoch gründlich vorbereitet werden.

Ziel dieser Masterarbeit ist es, zu den Kernproblemen und Herausforderungen erfolgreicher Transformation in die Cloud Stellung zu beziehen, vor allem aber die Faktoren aufzuzeigen, die sich in technische und nicht-technische gliedern lassen, und essenziell für die erfolgreiche Durchführung sind.

Die Hauptziele dieser Arbeit liegen dahingehend auf einer detaillierten Betrachtung des Cloud-Computing Konzeptes und die damit verbundenen Herausforderungen, Chancen, und Sicherheitsrisiken für kleine und mittlere Unternehmen sowie Großkonzernen.

1.2 Forschungsfrage und Hypothesen

Aus Kapitel 1.1 abgeleitet lässt sich folgende Forschungsfrage definieren: „Welche Faktoren müssen Unternehmen beim Einsatz von Cloud-Computing prioritär behandeln, und welchen Einfluss haben diese auf eine erfolgreiche Transformation?“

Aus der Forschungsfrage abgeleitet können folgende statistische Hypothesen formuliert werden:

- H1: Effektives Change-Management ist der wichtigste Faktor für eine erfolgreiche Transformation.
- H0: Effektives Change-Management spielt keine Rolle für eine erfolgreiche Transformation.

- H1: Die benötigten Fähigkeiten und Qualifikationen von Mitarbeitern zu effektiver Cloud Nutzung unterscheiden sich deutlich von jenen traditioneller On-Premise-Lösungen.
- H0: Die benötigten Fähigkeiten und Qualifikationen zu effektiver Cloud Nutzung sind dieselben wie bei traditionellen On-Premise-Lösungen.

- H1: Cybersecurity stellt die größte nicht-organisatorische Herausforderung dar.
- H0: Cybersecurity stellt eine vernachlässigbare nicht-organisatorische Herausforderung dar.

- H1: Cloud ermöglicht Veränderung von Freigabeprozessen hin zu Servicekatalogen.
- H0: Cloud ermöglicht keine Umstellung des Freigabeprozesses.

- H1: Cloudcomputing reduziert die Größe von IT-Teams.
- H0: Cloudcomputing hat keinen Einfluss auf die Größe von IT-Teams.

- H1: Mittels Cloud-Computing wird schneller auf Sicherheitslücken reagiert als bei traditionellen On-Premise-Lösungen.
- H0: Mittels Cloud-Computing realisierte und traditionelle On-Premise-Lösungen reagieren in gleicher Geschwindigkeit auf Sicherheitslücken.

1.3 Aufbau der Arbeit

Zur Beantwortung der Forschungsfragen wurde eine Unterteilung der hier vorliegenden Arbeit in 8 Kapitel vorgenommen. In Kapitel 2 werden die theoretischen Grundlagen und Definitionen im

Zusammenhang mit dem Begriff der Cloud erörtert, die für ein Verständnis dieser Arbeit von essenzieller Bedeutung und daher unbedingt erforderlich sind.

Im Empirie-Teil wird das methodische Vorgehen bei den Experten- und Expertinnen Befragungen erläutert, und kurz zusammengefasst, wie dieser Prozess auf Grundlage der Erkenntnisse der Theorie vollzogen wurde. Auf diese Erläuterungen aufbauend, folgt die Analyse und Ausarbeitung der Experten- und Expertinnen Befragungen, bevor diese in eine Zusammenfassung münden.

2 GRUNDLAGEN UND DEFINITIONEN

Um das Thema Cloud-Computing in seiner Gänze zu verstehen, muss zuerst definiert werden, worum es sich bei Cloud-Computing handelt. Ersteres wird im nachfolgenden Kapitel prioritär behandelt, um danach die Vorteile und Limitierungen von Cloud-Diensten darzulegen, bevor eine Übersicht über die relevantesten Cloud Service Modelle das Kapitel abschließt.

2.1 Cloud-Computing

Obwohl der Begriff mittlerweile im Fachjargon der IT-Branche angekommen ist, gibt es immer wieder Missverständnisse, wie der Begriff zu definieren ist, und was er in seiner Gesamtheit beinhaltet. Die nachfolgenden Kapitel sollen darüber Aufschluss geben.

2.1.1 Definition

Bevor der Begriff Cloud-Computing erörtert wird, muss zuerst eine Abgrenzung der unterschiedlichen Arten von IT-Lösungen, die einem Unternehmen prinzipiell zur Verfügung stehen, gezogen werden. Unternehmen haben generell die Möglichkeit, auf drei Varianten von IT-Lösungen zurückzugreifen:

1.) On-Premise-Hosting

2.) Managed Hosting

3.) Cloud-Computing

Der hierbei traditionelle Ansatz spiegelt sich im On-Premise-Hosting wider. Dabei erwirbt ein Unternehmen die benötigte IT-Infrastruktur, wie z.B. Server, Betriebssysteme, Netzwerkinfrastruktur, selbst, und betreibt diese auf dem firmeneigenen Gelände. Zu Betrieb und Wartung wird eine eigene IT-Abteilung benötigt, die auch die Skalierung der IT-Infrastruktur durch Beschaffung neuer Hardware sicherstellt. (IONOS, 2020)

Als eine Stufe zwischen On-Premise-Hosting und Cloud-Computing kann das Managed Hosting verstanden werden. Hierbei übernimmt ein Anbieter, der sich auf das Hosting spezialisiert hat, den Betrieb und die Wartung der IT-Infrastruktur in einem dafür bereitgestellten Rechenzentrum. Der Einsatz von Virtualisierungslösungen erlaubt dem Anbieter hierbei, mehrere Unternehmen auf einer größeren IT-Infrastruktur zu platzieren. Im Gegensatz zu On-Premise-Hosting sind Managed Hosting Lösungen in der Regel bereits redundant ausgeführt, wodurch eine Nichtverfügbarkeit der Systeme vermieden werden soll. (INAP, 2017)

Eine allgemeingültige Definition von Cloud-Computing wurde am National Institute of Standards and Technology (NIST) entwickelt. Das NIST definiert Cloud-Computing als: „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" (Mell & Grance, 2011).

Der Begriff Cloud-Computing kann in der gelebten Praxis jedoch sowohl eine Plattform als auch eine spezielle Art von Anwendung umfassen.

Wird darunter eine Plattform verstanden, so mietet ein Unternehmen im Grunde nur einen kleinen Teil einer riesigen IT-Infrastruktur aus Rechenzentren, Servern, Speicher- und Netzwerkkapazitäten, die als physische Geräte, oder durch Einsatz von Virtualisierungstechnologien zur Verfügung gestellt werden, und untereinander verknüpft sind. Dies ermöglicht einfache Skalierbarkeit und entsprechende Ausfallsicherheit durch Redundanz. So wird zur Bereitstellung weiterer Rechenleistung kein Ankauf neuer Hardware benötigt, sondern kann innerhalb weniger Minuten durch eine Bestellung von Mehrleistung bewerkstelligt werden.

Dieser Prozess lässt sich auch so weit automatisieren, dass Leistungsspitzen durch Skalierung der IT-Infrastruktur nur für jenen Zeitraum abgefangen werden, in welchem auch die entsprechende Leistung benötigt wird. Die Mehrkosten für das Bereitstellen weiterer Ressourcen fallen in dieser Konstellation nur für den Zeitraum der Leistungsspitze an.

Im Sinne von Anwendungen spricht man von internetbasierter Websoftware, die mittels meist redundanter Rechenzentren und entsprechend leistungsstarken, sowie skalierbaren Servern, zugänglich gemacht wird. Diese Websoftware wird in der Regel von Unternehmen bzw. Anwendern nur angemietet („Subscription-based Licensing"-Modell) und nicht angekauft, wie es beim traditionellen Ansatz, in welchem die Software nach dem Kauf für immer genutzt werden kann, der Fall ist („Perpetual Licensing"-Modell).

2.1.2 Cloud-Computing Bereitstellungsmodelle

Bereitstellungsmodelle für Cloud-Computing lassen sich vorrangig in 3 Kategorien gliedern:

1.) Private Clouds

2.) Öffentliche Clouds

3.) Hybride Clouds

Eine private Cloud wird dabei normalerweise innerhalb eines Unternehmens etabliert, und stellt darin verfügbare Dienste jenen Benutzern zur Verfügung, die auch dem Unternehmen zuzuordnen sind. (Balasubramanian & Aramudhan, 2012)

Konträr dazu werden in einer öffentlichen Cloud Ressourcen durch einen Cloud Service Provider (CSP) zur Verfügung gestellt, der mehrere Organisationen bedient. Entsprechende Ressourcen werden dahingehend unter den Organisationen aufgeteilt. Dies stellt einen entscheidenden Vorteil der öffentlichen Cloud im Vergleich zur privaten Cloud dar. Unternehmen sind so in der Lage, Ressourcen dynamisch und nur bei anstehendem Bedarf zu akquirieren, ohne entsprechende Hardwareanschaffungen im Vorfeld zu betreiben. (Goyal, 2014)

Bei der hybriden Cloud werden die private, sowie die öffentliche Cloud miteinander kombiniert. Hiermit soll erreicht werden, dass die limitierten Kapazitäten einer unternehmensinternen, privaten Cloud bei Lastspitzen durch zusätzliche Ressourcen aus einer öffentlichen Cloud erweitert werden können. (Jin, et al., 2010)

In Kapitel 2.2 wird näher auf die Vorteile der öffentlichen Cloud im Vergleich zur privaten Cloud eingegangen. Auf die hybride Cloud wird in dieser wissenschaftlichen Arbeit auf Grund ihrer geringen Verbreitung nicht näher eingegangen.

2.1.3 Cloud-Computing Architektur

Die Cloud-Computing Architektur lässt sich in zwei Bestandsteile unterteilen: Frontend und Backend. Die Kommunikation zwischen Frontend und Backend findet dabei über ein Netzwerk oder das Internet statt. Hierbei wird das Frontend von Kunden oder Dienstleistungsunternehmen benutzt. Das Frontend greift dabei die im Optimalfall mittels Schnittstellen auf das Backend zu. Es stellt somit eine Arbeitsumgebung dar. Im Gegensatz dazu befasst sich das Backend mit der eigentlichen Applikation, die über das Internet zur Verfügung gestellt wird. Es ist weiters für die Speicherung der Informationen verantwortlich. Die unterschiedlichen Bestandteile eines Backends lassen sich, wie in Abbildung 1 ersichtlich, in folgende Komponenten gliedern:

- Anwendung
- Service
- Storage
- Management
- Sicherheit

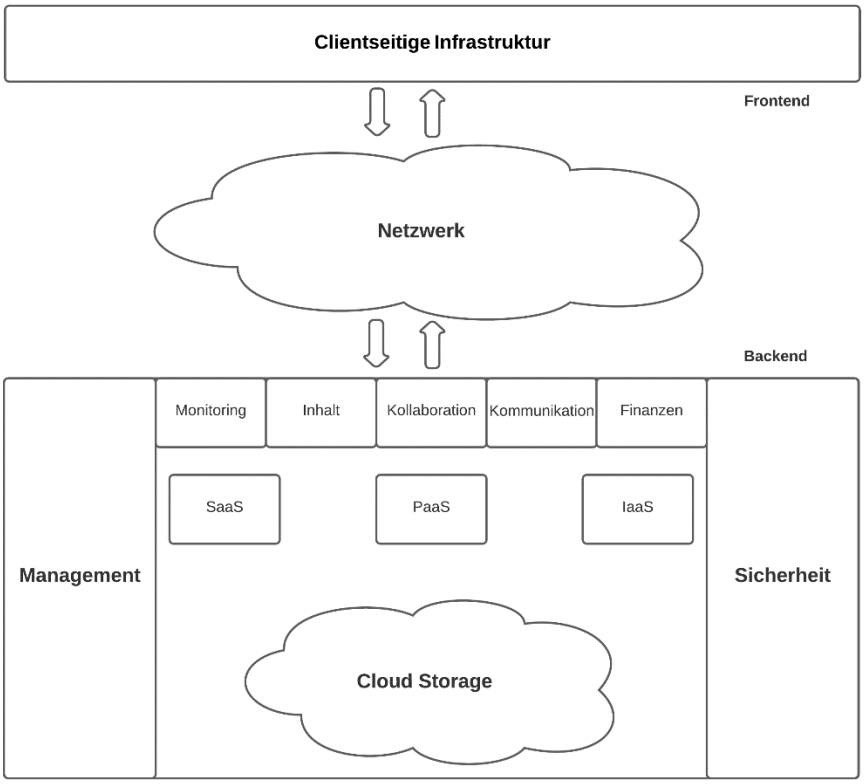

Abbildung 1: Cloud-Computing Architektur (eigene Darstellung nach Rangwani D., & Om, H. (2021))

2.1.4 Cloud-Computing Charakteristika

Cloud-Computing wird von Tag zu Tag beliebter. Es kann Unternehmen dabei helfen zu expandieren und Daten sicher von physischen Standorten in die Cloud zu übertragen. Somit kann darauf von überall aus zugegriffen werden. Die Flexibilität, die Cloud-Dienste in Form einer ständig wachsenden Anzahl von Anwendungen und Techniken bieten, hat ihre Verbreitung in allen Branchen beschleunigt. Das NIST beschreibt ein Cloud-Modell anhand von fünf wesentlichen Merkmalen:

- On-Demand Self-Service
- Broad Network Access
- Ressource Pooling
- Rapid Elasticity
- Measured Service

(Mell & Grance, 2011)

On-Demand Self-Service bedeutet, dass ein Kunde Rechenzeit beantragen kann, ohne dass ein Administrator oder Support-Mitarbeiter die Anfrage manuell bearbeiten muss. Der ganze Prozess ist automatisiert, was nicht nur Vorteile für den Anbieter, sondern auch für den Kunden bietet. (Lisdorf, 2021)

Unter Broad Network Access versteht man die Eigenschaft, dass nahezu alle Funktionen von Datenbanken bis hin zu den Anwendungen, die vom Kunden erstellt und verarbeitet werden, über ein Netzwerk verfügbar sind. Der Zugriff erfolgt hierbei über Standardmechanismen und -protokolle und es kommen sogenannte Thick- oder Thin-Clients zur Anwendung. (Manvi & Shyam, 2021)

Unter Thin-Clients versteht man Netzwerkcomputer ohne Festplattenlaufwerk, die eine ständige Kommunikation mit dem Server benötigen. Im Gegensatz dazu führt ein Thick-Client den Großteil der Verarbeitung in den Client/Server-Anwendungen selbst durch. Hierdurch entfällt die Notwendigkeit für eine ständige Kommunikation mit dem Server. Der Großteil - von Datenbanken bis hin zu den Anwendungen, die sie erstellen und verarbeiten - ist über das Netz verfügbar (GoCloud, 2021). In Zusammenhang mit Cloud-Computing stellt der Webbrowser eine Art von universellem Client dar.

Beim Ressourcen-Pooling werden die Rechenressourcen des Dienstanbieters gepoolt, um mehrere Nutzer zu bedienen. Dadurch können viele Nutzer gleichzeitig auf die Ressourcen desselben Standortes zugreifen. Weiters werden die benötigten Ressourcen dynamisch an den Bedarf des Kunden angepasst. (Rountree & Castrillo, 2014)

Rapid Elasticity ermöglicht es den Nutzern, automatisch zusätzlichen Speicherplatz in der Cloud oder andere Arten von Diensten anzufordern. Aufgrund des Aufbaus von Cloud-Computing-Diensten kann die Bereitstellung für den Kunden oder Nutzer nahtlos erfolgen. Die Tatsache, dass hierbei im Hintergrund immer noch Ressourcen zugewiesen und freigegeben werden müssen, spielt für den Kunden oder Nutzer oftmals keine Rolle (Schouten, 2012).

Dies stellt einen wesentlichen Aspekt der Cloud-Technologie dar. Hierdurch scheinen die Ressourcen des Cloud-Computing unendlich oder automatisch verfügbar zu sein, was einen großen Unterschied zu älteren Systemen darstellt. Letztgenannte haben durch ihre natürliche Limitation von Speicherplatz und Arbeitsspeicher oftmals spürbare Auswirkungen auf die Nutzbarkeit einer Applikation oder dessen Leistungsfähigkeit.

Beim Measured Service werden die verbrauchten Ressourcen gemessen und anschließend auch nur diese in Rechnung gestellt. Um die Transparenz dieser Abrechnung zu garantieren, werden die Daten der Nutzung auch dem Kunden zur Verfügung gestellt. Die verrechneten Kosten können variieren, da sie von der Nutzung des Kunden abhängig sind. Dies erschwert eine Kostenvorkalkulation und damit eine entsprechende Budgetierung. (REHMAN, 2019)

2.1.5 Cloud Service Modelle

Die am häufigsten auftretenden Cloud-Service Modelle lassen sich durch das Akronym SPI beschreiben. Dabei handelt es sich um **S**oftware-as-a-Service (SaaS), **P**latform-as-a-Service (PaaS) und **I**nfrastructure-as-a-Service (IaaS). Abbildung 2 stellt hierzu die Unterschiede im Vergleich zu traditionellem On-Premise-Hosting schematisch dar.

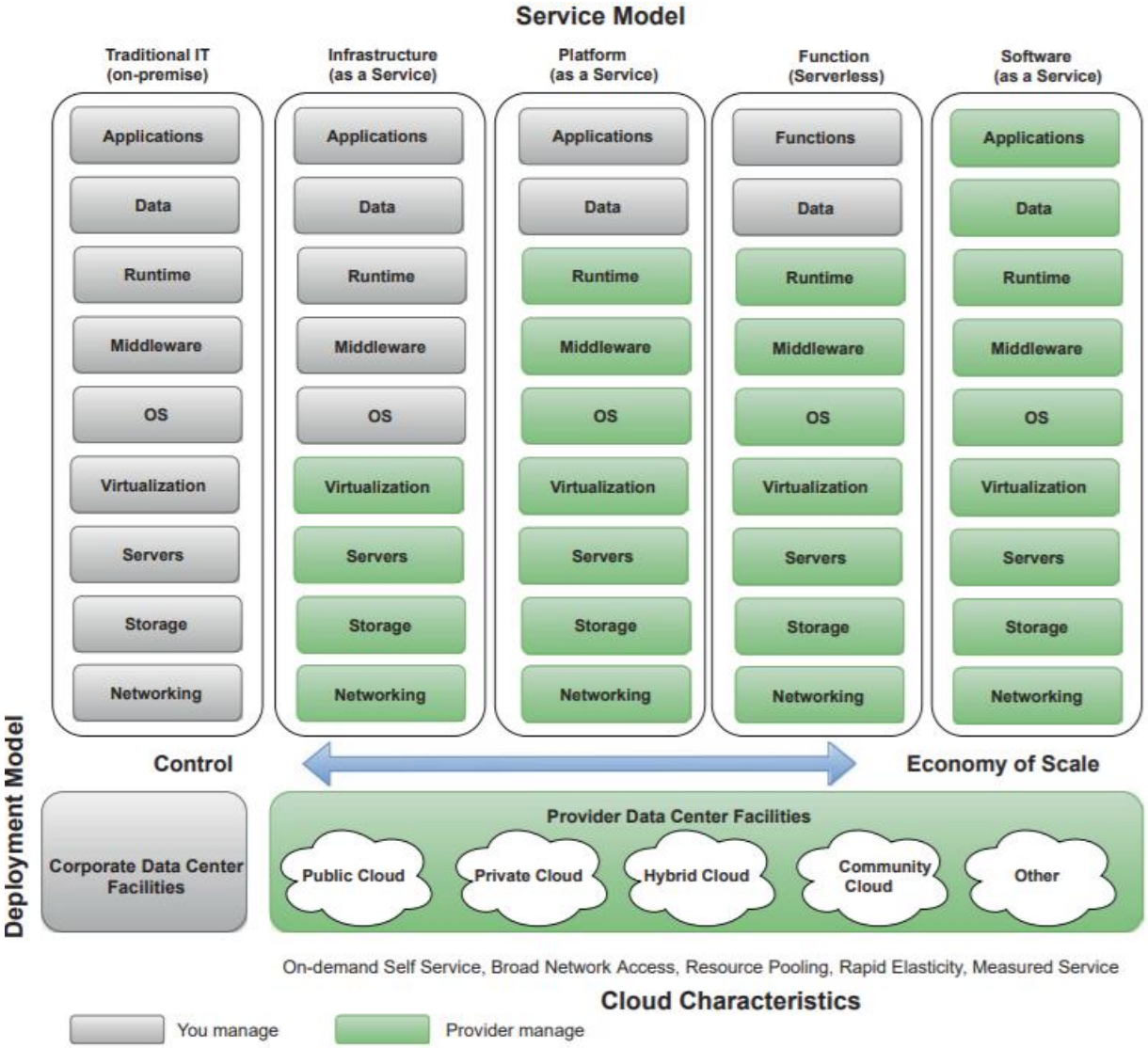

Abbildung 2: Cloud-Computing Servicemodelle (Gleb, 2021)

IaaS beschreibt das komplette Auslagern der Datenzentrums-Infrastruktur zu einem CSP und umfasst hierbei hauptsächlich Hardware wie Server- und Netzwerkkomponenten oder auch Speicher. Die entsprechenden Ressourcen werden dabei meist durch Virtualisierungstechnologien über das Internet zur Verfügung gestellt. (Comer, 2021)

Hierbei werden unter dem Einsatz eines Hypervisors, oder auch Virtual-Machine-Monitor (VMM) genannt, mehrere virtuelle Maschinen (VM) mit Hardwareressourcen, verfügbarer Peripherie und

bei Bedarf unterschiedlichen Konfigurationen geschaffen, die unabhängig von der tatsächlich zur Verfügung stehenden Serverhardware operieren. Bekannte Hypervisor Applikationen sind u.a. Citrix Hypervisor, Red Hat Virtualization, VMware vSphere, Microsoft Hyper-V und Oracle VM Server.

Bei PaaS handelt es sich um eine komplette Entwicklungs- und Bereitstellungsumgebung in der Cloud, die es ermöglicht, Cloud-basierte Applikationen zu erstellen. Die entsprechenden Ressourcen werden hierzu vom Cloud-Service-Anbieter zur Verfügung gestellt, und zum Großteil mittels eines „Pay-as-You-Go (PAYG)“ Geschäftsmodells verrechnet, in welchem nur jene Ressourcen zu bezahlen sind, die auch tatsächlich benötigt wurden. (Srinivasan, 2014)

Wie IaaS umfasst PaaS die Infrastruktur (Server, Speicher und Netzwerke), aber auch Middleware und Schnittstellen, Entwicklungstools, Auswertungs- und Analysetools wie z.B. Business-Intelligence (BI) Lösungen, sowie Datenbankmanagementsysteme. PaaS ist darauf ausgelegt, den gesamten Lebenszyklus von Webanwendungen zu unterstützen: Erstellen, Testen, Bereitstellen, Verwalten und Aktualisieren.

SaaS beschreibt ein Software-Distributions-Modell, in welchem der Anwender eine entsprechende Software über das Internet nutzt, welche vom Anbieter direkt, oder ausgelagert durch einen Service-Provider, gehostet wird. (Rittinghouse & Ransome, 2010)

Die in ihrer Vielzahl zur Verfügung stehenden Bereitstellungsmodelle, die über das Internet ausgeliefert werden, können auch als Anything-as-a-Service (XaaS) bezeichnet werden. XaaS umfasst dabei Konzepte wie Security-as-a-Service, Storage-as-a-Service oder auch Database-as-a-Service.

Das ultimative Ziel des Cloud-Computing, unabhängig von IaaS, PaaS, oder SaaS, ist die Bereitstellung effizienter Dienste für die Nutzer und die Erfüllung ihrer Anforderungen. Dennoch gibt es viele Fälle, in denen es zu Ausfällen oder Verletzungen der Sicherheits- oder Verfügbarkeitsgarantien kommt. Darüber hinaus können massive Änderungen in der Cloud-Struktur auch erhebliche Leistungsprobleme mit sich bringen.
Diese Herausforderungen machen die Entwicklung von adaptiven Mustern erforderlich, die auch die zunehmende Komplexität der Cloud bewältigen können. Techniken zur Selbstverwaltung bieten hier ein probates Mittel für die zunehmende Komplexität, da sie dazu neigen, sowohl mit internen als auch mit externen Reizen zu interagieren, ohne dass ein Mensch eingreifen muss.

Diese Techniken lassen sich in vier Aspekte des Selbstmanagements unterteilen:

1.) Selbstkonfiguration - das System verwaltet den Einsatz von neu hinzukommenden oder verschwindenden Cloud-Knoten selbst.
2.) Selbstoptimierung - stößt ein Cloud-Knoten oder eine Netzverbindung an ihre Kapazitätsgrenzen, muss sie in der Lage sein, einen Teil der Aufgaben an einen anderen (optimal zusammengesetzten) Knoten/eine andere Netzverbindung abzugeben.
3.) Selbstschutz - die Fähigkeit, sich gegen Angriffe von Dritten zu schützen, wie z. B. Distributed-Denial-of-Service (DDoS).
4.) Selbstheilung - im Falle eines Ausfalls müssen die aktiven und ausgeführten Anwendungen migriert und an anderer Stelle wieder verfügbar gemacht werden. (Lynn T. , Mooney, Lee, & Endo, 2020)

Generell muss jedes Cloud-System seine Anpassungsfähigkeit gewährleisten und die oben genannten Herausforderungen bewältigen, d. h. kontinuierlicher Betrieb unter allen Umständen, Lastausgleich, Sicherheit, Interoperabilität und Energieeffizienz.

2.2 Vorteile der öffentlichen Cloud

Dieses Kapitel legt die Vorteile der Cloud im Vergleich zu einer privaten Cloud dar. Es wird auf einen Vergleich mit der hybriden Cloud verzichtet, da auch hier ein Teil durch eine öffentliche Cloud bereitgestellt wird, und somit viele der nachfolgend genannten Punkte ident zu bewerten sind.

2.2.1 Sicherheit und Skalierung

Maßnahmen zur Absicherung einer IT-Infrastruktur lassen sich effizienter und kosteneffektiver umsetzen, wenn diese in größerem Maßstab etabliert werden. Mit dem gleichen Betrag an Investitionen lassen sich dahingehend auch bessere Schutzgrade erzielen. Dies lässt sich auf alle Arten von Schutzmaßnahmen, die nachfolgend kurz benannt werden, übertragen: Firewalls, Management von Sicherheitspatches, entsprechende Verwaltung und Überprüfung von Personalressourcen, Zugriff- und Zutrittskontrollen, Identitätsmanagement und Authentifizierung, Absicherung von virtuellen Maschinen und Hypervisoren, oder auch redundante Ausführungen von Software und Hardware. (Comer, 2021)

Zusätzlich haben Cloud-Lösungen den Vorteil, dass vor allem CSP über mehrere Standorte verfügen, und Daten bzw. Applikationen hierbei zur Schaffung von Redundanz repliziert werden können, um bei Ausfall einzelner Komponenten gewappnet zu sein. Auch eine Bereitstellung näher

am Standort des Nutzers oder des Unternehmens (Edge-Netzwerke) zu Zwecken der Latenzminimierung und zur Minimierung von Netzwerkproblemen durch globale Nebeneffekte, kann im Regelfall einfach durchgeführt werden.

Des Weiteren können gut geführte Systeme in größerem Maßstab Sicherheitsprobleme frühzeitig erkennen, und eine bessere Reaktionszeit zur Bewältigung dieser liefern, da hier auf Sicherheitsspezialisten zurückgegriffen werden kann, die für ein normales KMU mitunter zu kostspielig wären.

2.2.2 Sicherheit als Differenzierungsmerkmal

Für viele Organisationen ist das Thema Sicherheit ein vorrangiger Aspekt, um eine Kaufentscheidung zu treffen. Hierbei fließen Elemente wie der Ruf eines Anbieters, dessen Sicherheitsstandards, oder auch die vertraglich geregelten Absicherungen mit ein. Dahingehend stellt Sicherheit ein Differenzierungsmerkmal zwischen den CSPs im Markt dar und hat dazu geführt, dass öffentliche Clouds hohe Investitionen in die Erhaltung von Sicherheitsstandards tätigen. Diese lassen sich im Regelfall für KMUs, die eine private Cloud betreiben, wirtschaftlich nicht darstellen. (Sehgal, Bhatt, & Acken, 2020)

2.2.3 Rechtzeitigere, effektivere und effizientere Updates, sowie Voreinstellungen

Durch den Einsatz virtueller Maschinen können Abbildungen eines Betriebssystems im Vorfeld bereits durch entsprechendes Personal mit neuesten Updates und Sicherheitsbeschränkungen ausgestattet werden. Ein Abgleich mit anderen virtuellen Maschinen ermöglicht so das rasche Erkennen von Diskrepanzen in Sicherheitspatches und Firewall-Regeln. Des Weiteren ermöglichen die homogenen Plattformen der CSPs ein vielfach schnelleres Ausrollen von Updates konträr zu traditionellen IT-Systemen, die auf einem Patching-Modell basieren. Die seitens des CSPs eingesetzten Softwarelösungen sind weiters auf den Betrieb außerhalb von Unternehmensumgebungen ausgerichtet, wodurch die Wahrscheinlichkeit einer höheren Abhärtung gegenüber Angriffen anzunehmen ist. (Sehgal, Bhatt, & Acken, 2020)

2.2.4 Schnelle, intelligente Skalierung von Ressourcen

Die öffentliche Cloud bringt den Vorteil mit sich, dass entsprechende Ressourcen bei Bedarf dynamisch skaliert werden können. Mittlerweile lässt sich dies nicht mehr nur auf die Nutzung einzelner oder mehrerer Kerne einer zentralen Recheneinheit, allgemein unter Central Processing Unit (CPU) bekannt, übertragen, sondern umfasst Komponenten wie Festplatten- und Arbeitsspeicher, Web-Service Anfragen, oder auch virtuellen Maschinen. Dabei nimmt der Grad

granularer Ressourcenverbrauchskontrolle mit der Technologiereife zu. (Lorido-Botran, Miguel-Alonso, & Lozano, 2014)

Dies zeigen auch die Möglichkeiten der CSPs, gezielt und dynamisch neue Ressourcen für Verschlüsselungstechnologien, Filterungen, und Bandbreitenverwaltungen zuzuweisen, um den Schutz vor laufenden oder potenziell anstehenden Angriffen, z.B. Distributed Denial-of-Service (DDoS) Attacken, zu erhöhen. (Amazon Web Services, 2021)

Aber auch Kostenfaktoren spielen eine Rolle, da die bedarfsgerechte Bereitstellung von Ressourcen umso effizienter umgesetzt werden kann, je granularer Einzelressourcen skaliert werden können, ohne dabei die gesamten Systemressourcen anheben zu müssen.

2.2.5 Audit und Beweissicherung

Wurde ein potenzieller Angriff oder ein Sicherheitsleck entdeckt, kann im Regelfall durch das auf Abruf verfügbare Klonen von virtuellen Maschinen oder virtueller Komponenten davon ein Offline-Image für die forensische Analyse erstellt werden, ohne dabei das Live-System für längere Zeit vom Netz zu nehmen, sofern dies der Abwendung größeren Schadens durch den Ausfall dienlich ist.
Durch den Einsatz von Software wie Open Network Technology for Appliance Products (ONTAP), ein proprietäres Betriebssystem von NetApp, können weiters mehrere Klone erstellt, und die Analyseaktivitäten somit parallelisiert werden. Dies führt nicht nur zu einer Reduktion der Untersuchungszeit, sondern verbessert auch die Wahrscheinlichkeit Angreifer aufzuspüren und die Schwachstellen zu schließen. (Lynn T. , Mooney, van der Werff, & Fox, 2021)

2.2.6 Audits und SLAs für besseres Risikomanagement

Der Großteil der CSP bietet ihren Kunden mittlerweile Service Level Agreements (SLAs) an. Diese definieren den Grad an Dienstleistungen, den ein Kunde vom CSP erwarten darf, und legt dafür relevante Messgrößen fest, an denen die Einhaltung gemessen wird. Für die Nichteinhaltung definieren SLAs u.a. Abhilfemaßnahmen oder Strafen, die der CSP dem Kunden zu leisten hat. Wie in Kapitel 2.2.2 dargelegt, ist durch das Differenzierungsmerkmal Sicherheit im Markt, die Notwendigkeit Strafen, im Falle verschiedenster Risikoszenarien in SLAs zu quantifizieren, als gesetzt anzusehen. Dies führt mitunter zu strengeren internen Audit- und Risikobewertungsverfahren, als dies sonst der Fall wäre, und damit unweigerlich zu einer höheren Erkennungsrate von Risiken. (McHaney, 2021)

2.3 Limitierungen der öffentlichen Cloud

Multi-Tenancy, also die Fähigkeit, mehrere Mandaten auf einem System softwareseitig und nicht physikalisch zu trennen, kann für Unternehmen, die strenge gesetzliche Vorschriften einhalten müssen, ein Problem darstellen. Durch die Nutzung eines Datenbankservers und durch die Unterteilung der Datenbank in mehrere Kundensegmente kann bei einem Sicherheitsleck die komplette Kompromittierung des Servers stattfinden. Hierdurch steigt das Risiko, dass mehrere Kunden von einem Sicherheitsvergehen betroffen sind. Im Regelfall ist das Risiko minimal, da die meisten Cloud-Anbieter hohe Sicherheitsstandards verfolgen, aber je nach Unternehmen kann bereits die Risikotoleranzgrenze des Hinnehmbaren übertroffen werden.

Es kann auch schwierig sein, dieselben Sicherheitsrichtlinien für die internen Ressourcen eines Unternehmens, als auch für eine öffentliche Cloud einzusetzen. Besonders wenn Unternehmen an einen gesetzlichen Rahmen gebunden sind und einen gewissen Sicherheitsstandart garantieren müssen, kann dies problematisch sein, auch wenn die großen Cloud Anbieter dieses Problem durch facheinschlägige Zertifikate zu lösen versuchen. Wenn ein Unternehmen spezielle Anforderungen hat, können diese möglicherweise nicht erfüllt werden, da CSP dazu neigen, einen Einheitsansatz zu verfolgen.

Dies kann für Unternehmen mit einer komplexen Netzwerkarchitektur oder komplizierten Anwendungsprozessen ein Ausschlussgrund einer öffentlichen Cloud sein, besonders wenn die Integration älterer Plattformen dabei in Betracht gezogen werden muss. Die öffentliche Cloud erfüllt dann möglicherweise nicht den Bedarf für die Integration aller Facetten der IT-Infrastruktur solcher Unternehmen. Eine interne Überprüfung der Anforderungen ist somit vor der Auswahl des Cloud Bereitstellungsmodells essenziell, damit die rechtlichen Pflichten und die wirtschaftlichen Interessen mit der gewählten Umgebung vereinbar sind.

3 TECHNISCHE HERAUSFORDERUNGEN

Unternehmen gehen oft davon aus, dass die Migration in die Cloud ein einfacher Prozess ist, bei dem die bestehende Infrastruktur migriert wird. Aus diesem Grund versäumen es viele Unternehmen, für eine reibungslose Migration erforderlichen Analyse- und Planungsprozesse durchzuführen, die technische Herausforderungen berücksichtigen. In diesem Abschnitt werden die verschiedenen Strategien, welche bei einer Cloud-Migration in Betracht gezogen werden müssen, beschrieben. Einleitend ergänzt wird dies durch die Vorstellung marktführender CSP, bevor zum Abschluss des Kapitels auf Cybersecurity Aspekte eingegangen wird.

3.1 Legacy Systeme

Um zu entscheiden, ob eine Cloud Lösung für ein Unternehmen in Betracht kommt, ist es wichtig, das Ökosystem an bestehenden Systemen als Ganzes zu sehen. Hierbei muss bestimmt werden, wie diese in Zukunft in einer neuen Umgebung betrieben werden sollen. So sollte abgeklärt werden, ob eine Investition in bestimmte Anwendungen weiterhin gerechtfertigt ist, oder ob diese stillgelegt werden sollten. Viele Unternehmen haben ihre Anwendungen viel zu lange behalten, ohne einen entsprechenden Wartungs- oder Ablösungsplan auszuarbeiten. Dies lässt sich oftmals auf die Komplexität einer Anwendung, fehlende Dokumentation, ein Abhandenkommen des Quellcodes, sowie auf weitere Hindernisse zurückführen.

Dadurch bleiben Anwendungen über Jahre bzw. Jahrzehnte unangetastet. Ein Beispiel hierzu sind Anwendungen, die in einer im Jahr 1959 eingeführten Programmiersprache Common Business-Oriented Language (COBOL) entwickelt wurden, und bis heute vor allem im Banken- und Versicherungswesen zu finden sind. Dabei wurde COBOL bereits in den 70er Jahren für tot erklärt, und verschwand so allmählich aus den Studienplänen von Universitäten. Und dennoch feierte diese Programmiersprache erst kürzlich ihren 60sten Geburtstag. Das COBOL uns auch noch längere Zeit erhalten bleiben wird, zeigt eine Statistik von Micro Focus, einem der marktdominierenden Anbieter von COBOL-Compilern, die besagt, dass 70% aller Transaktionsverarbeitungssysteme weiterhin auf COBOL aufbauen und sogar 95% der bestehenden Magnetkarten-Lesegeräte nicht ohne COBOL auskommen. Dabei erstaunt es nicht, dass 220 Milliarden Zeilen an COBOL Code heutzutage weiterhin genutzt werden, und diese Anzahl jährlich um weitere 5 Milliarden steigt (Mangus, 2019).

Falls Unternehmen die Entscheidung treffen, diese Systeme in die Cloud zu verlegen, können mehrere Strategien angewandt werden. Nicht jede davon eignet sich jedoch für alte, bestehende Systeme, da sie viele Vorteile der Cloud, ohne entsprechende Adaptierung des

Programmiercodes, nicht nutzen können. In Kapitel 3.3 wird daher näher auf diese Migrationsstrategien, und deren Einsatzzweck, eingegangen.

3.2 Anbieter von Cloud-Computing

CSP sind multinationale Organisationen, die verschiedene Cloud-Dienste anbieten. Sie sind in Regionen rund um den Globus angesiedelt, und verfügen über private Rechenzentren (zur Verwaltung der Server), auf die ihre jeweiligen Kunden zugreifen. Da die Anzahl der Cloud Anbieter ständig wächst, konzentriert sich diese wissenschaftliche Arbeit auf die marktdominierenden drei Anbieter. In den nachfolgenden Kapiteln werden die Unterschiede zwischen den Anbietern genauer betrachtet, um die Vor- und Nachteile besser beurteilen zu können.

3.2.1 Amazon Web Services

Amazon Web Services (AWS) ist eine 2006 gegründete Tochtergesellschaft von Amazon, und der führende Anbieter von Cloud-Diensten. Die größte Stärke von AWS ist die Dominanz auf dem Markt für öffentliche Clouds. Dies belegt ein Marktanteil von 31% im Ranking der Cloud-Computing Marktführer (Canalys, 2021).

AWS ist der ausgereifteste und unternehmenstauglichste Anbieter mit einer beeindruckenden Erfolgsbilanz bei Kunden, die eine Bandbreite von kleinen und mittleren Unternehmen bis hin zu Großunternehmen abdecken. Diese Reife kommt daher, dass AWS der älteste Cloud Anbieter auf dem Markt ist und so eine große Unterstützung aus der Nutzerbasis erfährt, da viele Unternehmen wie Netflix, BMW, oder auch Samsung stark von AWS abhängig sind.

Die große Schwäche von Amazon sind die Kosten. AWS senkt zwar regelmäßig seine Preise, aber viele Unternehmen finden es schwierig, die Kostenstruktur des Unternehmens zu verstehen, und diese Kosten effektiv zu verwalten. Dies führt vor allem dann zu einem Problem, wenn ein hohes Arbeitslastvolumen durch den Cloud-Dienst in Anspruch genommen wird.

Bei den meisten Diensten spielen die Rechenleistung, der Speicherplatz und der ausgehende Datentransfer eine entscheidende Rolle bei der Einschätzung des Gesamtpreises für den Nutzer. Für die Integration von Daten in die nativen AWS-Anwendungen werden keine Gebühren erhoben, aber es fallen Kosten für jeden festgestellten, ausgehenden Datenverkehr an. Der Speicherplatz wird pro Gigabyte (GB) bezahlt, während die Datenverarbeitung stundenweise abgerechnet wird. Das führt dazu, dass die Kosten bei AWS schwer im Vorfeld abzuschätzen sind, und dies für kleine Unternehmen im Budgetplanungsprozess eine risikobehaftete Variable darstellt.

3.2.2 Microsoft Azure

Microsoft Azure wurde 2010 eingeführt und hat sich zu einem der größten kommerziellen Cloud-Service-Anbieter entwickelt. Es bietet eine breite Palette integrierter Cloud-Dienste und Funktionen, die sich nahtlos in Unternehmensumgebungen integrieren lassen. AWS und Azure bieten weitgehend dieselben grundlegenden Funktionen in Bezug auf flexible Rechenleistung, Speicherung, Vernetzung und Preisgestaltung.

Beide Anbieter bieten auch weitgehend ähnliche IaaS-Funktionen, Azure hat sich jedoch stärker auf PaaS-Funktionen fokussiert, die heute ein wichtiger Bestandteil der Cloud-Infrastruktur sind. Die Kompatibilität von Azure mit der Programmiersprache .NET ist jedoch einer der größten Vorteile von Azure, die Microsoft einen klaren Vorsprung gegenüber den übrigen Wettbewerbern verschafft. Azure wurde so entwickelt und optimiert, dass es sowohl mit alten als auch mit neuen Anwendungen, die in der .NET-Umgebung entwickelt wurden, konsistent funktioniert. Für Unternehmen ist es dadurch viel einfacher und unkomplizierter, ihre Windows-Anwendungen in die Azure Cloud zu verlagern. Generell entsteht für Unternehmen mit bestehendem Microsoft Enterprise-Agreement ein erheblicher Anreiz, Azure zu verwenden, da Microsoft diese Vereinbarungen in der Regel so gestaltet, dass die Preise für Azure reduziert sind.

Weiters war Microsoft mit Azure der erste Cloud-Anbieter, der von den Datenschutzbehörden der Europäischen Union und der Artikel-29-Datenschutzgruppe zugelassen wurde, und den internationalen Standard für Cloud-Datenschutz, ISO 27018, eingeführt hat. (Atmosera, 2021) Auf diesen Standard wird im Kapitel 3.4.4 noch genauer eingegangen.

3.2.3 Google Cloud Plattform

Die von Google angebotene Google Cloud Plattform (GCP), ist eine Reihe von Cloud-Diensten, die auf derselben Infrastruktur laufen, die Google intern für seine Endnutzerprodukte verwendet. Ein großer Vorteil von GCP ist die Preisgestaltung, wodurch Google die Komplexität der AWS- und Azure-Preismodelle in Frage stellt. Gepaart wird dies mit der Fähigkeit von Google, Preise anzubieten, die niedriger und einfacher zu kalkulieren sind als jene der Konkurrenz.

GCP bietet vergleichbare Cloud-Computing-Kernlösungen wie AWS, obwohl diese zwei Dienste in ihrer gesamten Funktionalität konträr zueinanderstehen. Dennoch ermöglicht GCP im Normalfall niedrigere Kosten als die Konkurrenzprodukte. Dies ist durch die Rabattprogramme von Google möglich, und kann zu erheblichen Preisvorteilen führen. (Jackson, 2021)

Die Kosten spiegeln jedoch nur einen Teil des Ganzen wider. Die Entscheidung für einen Cloud-Anbieter sollte nicht an reinen Betriebskosten festgemacht werden. Flexibilität, Zuverlässigkeit,

und das angebotene Leistungsniveau sollten jedenfalls miteinbezogen werden, um die Anforderungen des Unternehmens zur Gänze zu erfüllen.

GCP hat durch entsprechende Flexibilität mit Sicherheit einen Vorteil zur Konkurrenz, da die Möglichkeiten zur Anpassung von Recheninstanzen weitaus größer sind, als dies AWS oder Azure dem Nutzer anbieten. Alle Plattformen bieten vordefinierte Instanzen, die den Anforderungen der meisten Unternehmen entsprechen. Wenn die Rechenanforderungen jedoch nicht mit den vordefinierten Instanzen übereinstimmen, ist es bei GCP möglich, benutzerdefinierte virtuelle Maschinen zu erstellen, um ungenutzte Ressourcen-Kapazitäten auch nicht bezahlen zu müssen. (Ozer, 2018)

3.3 Migrationsstrategien

Cloud-Migration ist ein Prozess der Verlagerung digitaler Geschäftsabläufe. Meistens beschreibt der Begriff den Umzug von einer lokalen Infrastruktur in die Cloud. Der Begriff kann sich aber auch auf eine Migration von einer Cloud in eine andere beziehen. Die Verlagerung in die Cloud erfordert eine gut durchdachte Strategie. Diese sollte technologische Herausforderungen und eine Neuausrichtung des Personals bzw. der Ressourcen, umfassen. Zunächst muss die Art der Anwendung und dessen aktuelle Limitierungen bestimmt werden, da jedes Unternehmen einen anderen Grund hat, seine Arbeitslast in die Cloud zu verlagern. Besonders bei geschäftskritischen Anwendungen ist es wichtig, eine entsprechende Strategie auszuarbeiten, die auch Risikobewertungen und Sicherheitsaspekte miteinbezieht.

Vor der Migration sollte eine Evaluierung der Anwendung in Bezug auf bestehende Funktionalitäten vorgenommen werden, da oftmals einige Funktionen keine Verwendung mehr finden. In diesem Zusammenhang kann ein entsprechender Migrationsplan zur Unterstützung erstellt werden. Folgende Strategien, auch „6 R“ genannt, kommen bei der tatsächlichen Verlagerung zum Einsatz: (Amazon Web Services, 2018)

3.3.1 Rehost

Beim Rehosting, auch bekannt als Lift & Shift, werden Server oder Anwendungen aus der aktuellen Hosting-Umgebung in eine Cloud-Infrastruktur verlagert. Es ist daher eine gängige Strategie für Unternehmen, die gerade erst mit der Migration beginnen. Die Kerninfrastruktur bleibt dabei bestehen, kann nun aber die Vorteile der Cloud nutzen. Einer der wichtigsten Schritte, erfolgreiches Rehosting zu gewährleisten, ist das Sicherstellen von reibungslosem Datenzugriff der Anwendung auch nach dem Wechsel in die Cloud. Der Rehosting-Ansatz ist sehr risikoarm und bringt zusätzliche Vorteile wie Kosten- und Zeiteffizienz mit sich. Mitunter lässt sich durch den Einsatz einer Rehosting-Strategie auch eine einfachere Optimierung einer Anwendung an die

Cloudinfrastruktur vollziehen. Dies stellt daher oftmals den nächsten Schritt nach dem Rehosting dar. (Surianarayanan & Pethuru, 2019)

3.3.2 Refactor

Refactoring ist die ressourcenintensivste Option der Cloud-Migration. Dabei handelt es sich um einen disziplinierten Prozess, in dem die Architektur und Komponenten der Applikation überprüft, und anschließend neu programmiert werden. Dieser Ansatz wird gewählt, um die nativen Funktionen der Cloud und die zusätzliche Flexibilität, die sie ermöglicht, vollständig nutzbar zu machen. (NetApp, 2019)

Trotz der anfänglichen Kosten und des Ressourcenaufwands ist es wahrscheinlicher, dass das Refactoring auf lange Sicht eine bessere Rendite abwirft, besonders da es sich hier um eine Cloud-native Applikation handelt und somit das kontinuierliche Cloud-Innovationsmodell zum Einsatz kommt.

3.3.3 Replatform

Eine Replatform-Migration ist der Mittelweg zwischen den beiden in Kapiteln 3.3.1 und 3.3.2 beschriebenen Strategien. Sie ähnelt dem Rehosting von Anwendungen in der Cloud, erfordert aber eine gewisse Modifikation der Applikation, um die Vorteile der neuen Cloud-Infrastruktur zu nutzen. (NetApp, 2019)

Der Hauptvorteil von Replatforming ist die unmittelbare, wenn auch bescheidene, Nutzung der Cloud durch den Austausch gemeinsamer Komponenten und damit die Nutzung von Kosten- und Leistungsverbesserungen ohne die Risiken der Komplexität, der Kosten, und des Zeitaufwandes eines vollständigen Refactorings. Der Replatform-Ansatz kann die Kosten für die Migration und weiters auch für den laufenden Betrieb einer Anwendung stark senken. Gleichzeitig werden Risiken minimiert, wodurch es von vielen Unternehmen als „Sweet Spot“ der Migrationsstrategien gesehen wird.

3.3.4 Repurchase

Beim Repurchase, auch bekannt als „Drop & Shop“, wird die On-Premise-Anwendung durch ein Cloud-natives Paket eines Anbieters ersetzt. In der Regel bedeutet dies den Wechsel zu einer SaaS-Anwendung mit den gleichen Funktionen. Bei diesem Wechsel können extra Kosten anfallen, da Mitarbeiter neu eingeschult werden müssen, und SaaS-Plattformen, im Vergleich zu maßgeschneiderten Lösungen, oftmals weniger Anpassungsmöglichkeiten bieten. Aus diesem Grund wird diese Strategie meist mit anderen Migrationsmethoden kombiniert. Hierfür wird die

Anwendungslandschaft eines Unternehmens im Vorfeld evaluiert, und dann pro Anwendung eine entsprechende Migrationsstrategie festgelegt. (Sage, Cloudsoft, 2021)

3.3.5 Retire

Im Laufe der Migration in die Cloud muss festgestellt werden, welche Anwendungen tatsächlich noch innerhalb eines Unternehmens im Einsatz sind, um unnötigen Ballast zu vermeiden. Aus diesem Grund ist eine Cloud-Migration eine großartige Gelegenheit, alte und funktionsidente Anwendungen zu identifizieren, und festzulegen, welche davon die Voraussetzungen für eine Migration erfüllen, und welche für eine zukunftsorientierte Ausrichtung des Unternehmens besser ausgemustert werden. AWS schätzt das 10-20% des IT-Portfolios eines Unternehmens abgeschaltet werden können. Durch diese Reduktion können Unternehmen den Fokus auf jene Anwendungen legen, die auch tatsächlich genutzt werden. (Amazon Web Services, 2018)

3.3.6 Retain

Beim Einsatz der Retain-Strategie wird die Anwendung zum aktuellen Zeitpunkt nicht migriert, da wichtige Informationen, Fehler, oder andere Faktoren eine Migration behindern. Für einige Anwendungen ist eine Verlagerung auch generell nicht sinnvoll, da der Aufwand der Migration, im Vergleich zu den Vorteilen, zu hoch ausfällt. Dies bedeutet jedoch nicht, dass diese Anwendung nie in die Cloud migriert werden kann. Aufgrund neuer technischer Gegebenheiten oder Vorschriften kann eine Migration in Zukunft durchaus Nutzen generieren. (Amazon Web Services, 2018)

3.4 Cybersecurity

Die Einführung der Cloud-Technologie hat Unternehmen in die Pflicht genommen, auch die Cybersicherheit neu zu bewerten. Daten und Anwendungen können zwischen lokalen und entfernten Systemen hin- und hergeschoben werden. Daher ist es schwieriger geworden, diese zu schützen. Heutzutage geht es nicht mehr nur darum, unerwünschten Nutzern den Zugang zu einem Unternehmensnetzwerk zu verwehren. Die Cloud-Sicherheit erfordert die Anpassung früherer IT-Praktiken. In diesem Kapitel werden aktuelle Sicherheitsgefahren, und der bedeutende Nutzen gelebter Cybersecurity genauer erklärt.

3.4.1 Definition

Cybersecurity und Information Security haben einen starken Zusammenhang, sodass sie oftmals als Synonym verwendet werden. Die beiden Begriffe sind jedoch nicht synonym zu verwenden. Sie adressieren jeweils unterschiedliche Arten von Sicherheit, und es ist für jede Organisation,

die in ein angemessenes Sicherheits-Framework investiert, wichtig, den Begriff und seine Bedeutung zu verstehen, sowie die Unterschiede zwischen den beiden festzumachen.

Unter Cybersecurity wird laut NIST die Fähigkeit verstanden, den Cyberspace vor Cyberangriffen zu schützen und zu verteidigen. (Richard, 2013).

Die Definitionen von anderen Organisationen weichen teilweise von dieser Erörterung ab, die Kernaussage bleibt jedoch intakt. Cybersecurity bezieht sich somit auf Angriffe auf eine Organisation, und bietet den Rahmen für den Schutz gegen entsprechende Angriffspunkte.

Im Vergleich dazu dient Information Security dem Schutz von Informationen und Informationssystemen und gewährleistet die Sicherheit dieser (NIST, 2011). Das bezieht sich dabei sowohl auf elektronische, aber auch physikalische Daten.

3.4.2 Datensicherheit in der Cloud

Bei der Datensicherheit geht es darum, die Daten eines Unternehmens in einer Cloud-Umgebung zu sichern, unabhängig davon, wo sich diese Daten befinden und ob sie intern vom Unternehmen oder extern von einem Dritten verwaltet werden. Diese Praxis hat zunehmend an Bedeutung gewonnen, da immer mehr Unternehmen vom Aufbau und der Verwaltung eigener Rechenzentren zur Speicherung ihrer Anwendungen und Daten in der Cloud übergegangen sind. Laut einer Umfrage von IDG benutzen bereits 81% der Befragten Cloud-Computing und weitere 12% planen eine Einführung von Cloud-basierten Anwendungen innerhalb der nächsten 12 Monate. (IDG, 2020).

Auch wenn öffentliche und private Clouds hochsichere Umgebungen für Daten und Anwendungen sind, bedeutet das nicht, dass Unternehmen die gesamte Verantwortung für die Datensicherheit an ihren Cloud-Anbieter abtreten können. Es gibt noch viele grundlegende Sicherheitsmaßnahmen, die Unternehmen ergreifen müssen, angefangen bei der Authentifizierung. Für Administratoren sind Verfahren zur Multifaktor-Authentifizierung entscheidend für einen sicheren Betrieb. Das Hinzufügen biometrischer Daten als Teil der Multifaktor-Authentifizierung wird in Unternehmen immer beliebter, womit der Zugriff auf Daten stärker abgesichert wird.

Zusätzlich zum Datenzugriff sollten auch die Daten selbst geschützt werden. Aus diesem Grund empfiehlt es sich, eine Verschlüsselung einzusetzen, bevor Daten in die Cloud verschoben werden. In der Regel bieten Cloud-Service-Anbieter eine Reihe von Verschlüsselungsverfahren an. Auch wenn Daten selbst nun sicher gespeichert werden, müssen diese vom Unternehmen verwaltet, und sofern notwendig gelöscht werden. (Manvi & Shyam, 2021)

Der erste Schritt zur Verwaltung und Löschung alter Daten besteht darin, zu entscheiden, wie lange die Daten auf Grund rechtlicher oder interner Vorgaben aufbewahrt, und wann sie gelöscht werden müssen. Unternehmen sollten für alle Arten von Daten, die sie speichern, einen

Datenlebenszyklus festlegen. Wie dieser festgelegt wird, hängt nicht nur davon ab, wie lange das Unternehmen selbst diese Daten benötigt, sondern kann auch durch Regularien beeinflusst werden.

Wie wichtig es ist, diese Maßnahmen im Unternehmen umzusetzen, hängt nicht nur von der Art der Daten ab, sondern auch von den Kunden, die das Unternehmen bedient. Besonders bei sensiblen Daten ist es nicht unüblich, dass gewisse Sicherheitszertifikate vorhanden sein müssen, bevor die Daten in die Cloud migriert werden können. (Potluri, Rao, & Moh, 2021)

3.4.3 Angriffsmethoden

3.4.3.1. Denial-of-Service (DoS) und Distributed-Denial-of-Service (DDoS)

Da sich immer mehr Unternehmen auf die Cloud-basierten Dienste verlassen, werden DoS- und DDoS-Angriffe zu einem allgemeinen und kritischen Angriff auf die Cloud, der sich als äußerst schädlich erweist. Es lässt sich dabei zwischen zwei Formen von DoS-Angriffen unterscheiden:

Solche, die Dienste zum Absturz bringen, und solche, die Dienste überfluten. Die schwerwiegendsten Angriffe sind dabei DDoS-Attacken. An einem DDoS-Angriff sind in der Regel mindestens 3-5 Knoten in verschiedenen Netzen beteiligt. Liegt die Anzahl der Knoten darunter, wird von einem DoS-Angriff gesprochen.
Das Ziel von DoS- und DDoS-Angriffen besteht darin, die Verfügbarkeit eines Zielsystems, durch Überlastung dessen Bandbreite oder Ressourcen, zu unterbrechen und die Kundenerfahrung zu beeinträchtigen. In der Regel betrifft dies einzelne oder mehrere Webserver, die über unterschiedliche IP-Adresse oder ein Rechner geflutet werden. Zum Großteil findet dies über sogenannte Bot-Netzwerke statt, die aus Tausenden von mit Malware infizierten Rechnern bestehen. Ohne Cloud-DDoS-Abwehr, die gültigen Datenverkehr von bösartigem unterscheiden kann, sind Anbieter oder Kunden einem DDoS-Angriff schutzlos ausgeliefert. Die Cloud-Infrastruktur bietet Unternehmen zwar eine Fülle von Vorteilen und Möglichkeiten, jedoch sind diese auch für Angreifer ausnutzbar.
Automatische Skalierung und Pay-as-You-Go (PAYG) sind Hauptmerkmale des Cloud-Computings. Diesen Umstand können sich Angreifer bei DoS-Angriffen auf die Cloud zu Nutze machen, indem darauf abgezielt wird, die wirtschaftliche Nachhaltigkeit des Nutzers und die Performance eines Systems anzugreifen. Diese Form von Angriffen werden auch als EDoS (Economic Denial of Sustainability) bezeichnet. Sendet ein Angreifer genügend gefälschte Anfragen, führt dies bei einer Cloud-Umgebung zu einer starken Auslastung der Ressourcen auf dem Zielserver. Die automatische Skalierungsfunktion der Cloud nimmt diese Überlastung als Rückmeldung des

Systems an, und fügt dem bestehenden Pool der VM-Komponenten weitere Ressourcen wie CPUs, Speicher, etc. hinzu. (Chowdhury, Kiah, Ahsan, & Idris, 2017)
Wenn kein Cloud-basiertes DoS-Schutzsystem vorhanden ist, wird dieser Prozess so lange fortgesetzt, bis das Budget des Kunden aufgebraucht ist oder keine weiteren Ressourcen zur Verfügung stehen. Werden die Ressourcen des Systems reduziert, führt diese Art des Angriffs automatisch eine erneute Skalierung nach oben hin aus, bis schließlich die Verfügbarkeit der Dienste oder Anwendungen unter der Belastung einbricht.
Diese Art von Überflutung führt auch zu einer drastischen Kostenexplosion beim Nutzer und damit zu enormen wirtschaftlichen Verlusten. DoS-Schutzlösungen, die vor Ort im Rechenzentrum des Unternehmens installiert werden, sind zwar leistungsstark genug, um DoS-Angriffe auf der Netzwerk-, Anwendungs- und SSL-Ebene zu erkennen und abzuschwächen. Sie sind jedoch nicht ausreichend, um riesige volumetrische DoS-Angriffe abzuwehren, die auf eine Überflutung des Internetverkehrs abzielen. (Radware, 2016)
Daher sollten Unternehmen auf die bereits erwähnte Cloud-DDoS-Abwehr setzen, um größere Massen an Angriffen absorbieren zu können.

3.4.3.2. Permanent-Denial-of-Service (PDoS)

Ein PDoS-Angriff ist eine Dienstverweigerung durch Hardware-Sabotage. Diese Angriffe erfreuen sich bei Hackern immer größerer Beliebtheit. Es ist daher wichtig, dass Unternehmen sich den Gefahren bewusst sind, da sie die Infrastruktur nachhaltig schädigen können. Diese Angriffsart ist in gewissen Kreisen auch unter „Phlashing“ bekannt. Der Angreifer versucht dabei, ein Gerät oder dessen Firmware zu zerstören, um damit ein ganzes System unbrauchbar zu machen.

Hierzu werden Schwachstellen und Sicherheitslücken ausgenutzt, um die vorinstallierte und in Betrieb befindliche Basissoftware durch ein beschädigtes Firmware-Abbild zu ersetzen. In solch einem Szenario bleibt keine andere Wahl, als das Gerät zu reparieren oder komplett zu ersetzen, um den Betrieb wieder aufnehmen zu können.

Radware sagte bereits 2017 im Global Application & Network Security Report voraus, dass diese Art der Angriffe zunehmen wird. (Radware, 2017)

Leider ist es nicht möglich, eine 100%ige Sicherheit vor diesem Angriffstyp zu bieten. Es lässt sich jedoch das Risiko für ein Unternehmen minimieren, indem einige Sicherheitsaspekte berücksichtigt werden. So kann das Bespielen von Geräten mit Firmware durch eine Authentifizierung geschützt werden, um das schadhafte Ändern der Basissoftware zu erschweren. Weiters sollten regelmäßige Sicherheitsupdates zum Einsatz kommen, um bekannte Sicherheitslücken zu schließen.

3.4.3.3. Session-Hijacking

Wenn sich ein Benutzer in der Cloud anmeldet, wird eine sogenannte „Session“ erstellt, die Benutzerinformationen und die Session-ID enthält. Letztere wird dabei für die Authentifizierung von Anfragen verwendet. Meldet sich der Benutzer aus dem System ab, so erlischt auch die Session-ID, und es können keine gültigen Anfragen mehr ausgeführt werden.
Diese Daten werden normalerweise als Cookie, einem kleinen Datenblock, der auf dem Gerät des Nutzers gespeichert wird, oder in einem URL Parameter übergeben. Im Falle des Session-Hijacking wird eine gütige Session-ID von einem Angreifer übernommen. Dieser ist dadurch in der Lage sich als autorisierter Benutzer auszugeben und auf Daten zuzugreifen.
Grundsätzlich erfolgen Hijacking-Attacken folgendem Muster: Ein Benutzer erstellt eine gültige Session durch eine legitime Anmeldung. Der Angreifer führt eine Scan- oder Sniffing-Attacke durch, um an die Session-Daten zu gelangen. Sobald diese Daten dem Angreifer bekannt sind, erzwingt er mittels eines „Disassociation Management Frames“ die Umleitung der HTTP-Kommunikation an sein Gerät und unterbricht damit die Verbindung des eigentlichen Nutzers. Nun hat der Angreifer vollen Zugriff auf jene Dateien in der Cloud, die der kompromittierte Nutzer einsehen darf. (Gowrie, 2014)
Um sich vor Session-Hijacking-Attacken zu schützen, sollten Webanwendungen zusätzlich abgesichert werden. Dies kann mittels einfacher Verfahren wie dem Einsatz des HTTPS-Protokolls geschehen, welches den Datenverkehr des Nutzers verschlüsselt. Allerdings sollte zu weiteren Absicherungszwecken hierbei auf „HTTP Strict Transport Security“ (HSTS) zurückgegriffen werden. Weitere Möglichkeiten stellen der Einsatz von virtuellen privaten Netzwerken (VPN) und Session-Keys dar. (Baig, 2021)

3.4.3.4. Account-Hijacking

Bei Account-Hijacking-Attacken wird versucht, jenes Konto eines Nutzers zu übernehmen, welches mit einem Computergerät oder Computerdienst verbunden ist. Grundsätzlich handelt es sich hier um eine Art von Identitätsdiebstahl, da der Angreifer versucht, mit den gestohlenen Daten böswillige oder unbefugte Aktivitäten durchzuführen. Bei diesem Angriff gibt sich der Hacker als rechtlicher Besitzer des Kontos aus, was oftmals über ein kompromittiertes E-Mail-Konto bewerkstelligt wird. Das eigentliche Account-Hijacking wird meist durch Phishing E-Mails oder Brute-Force-Attacken durchgeführt. Durch die weitverbreitete Verknüpfung der Nutzerkonten mit unterschiedlichen Diensten kann ein komprimierter Account einen großen Schaden anrichten. Mitunter ein Grund warum Account-Hijacking in den Listen der größten Sicherheitsrisiken für Cloud-Computing meist in den Top-5 zu finden ist. Erwirbt ein Angreifer Zugang zu privilegierten Konten, kann dies desaströse Auswirkungen auf das Unternehmen haben. So kann der Angreifer die Zugänge dafür nützen, um die Geschäftsprozesse des Unternehmens zu unterbinden,

Lösegeldforderungen zu stellen, oder das Gerät als Quelle für weitere Angriffe nutzen. Auch nach dem eigentlichen Angriff fällt es Unternehmen oftmals schwer, sich von diesem zu erholen, da Angreifer aufgrund erworbener Systemrechte subtile Änderungen vornehmen, und so weitere Hintertüren öffnen. Diese lassen sich allerdings nur schwer erkennen, wodurch es IT-Sicherheitsbeauftragten in Unternehmen kaum möglich ist, eine kompromittierte Systemumgebung, ohne vollkommenen Ersatz durch ein Backup, sicher wieder zur Verfügung zu stellen.

Um sich vor diesen Angriffen zu schützen, empfiehlt Brown folgende Ansätze zur Umsetzung im Unternehmen:

1) Multifaktor Authentifikationen benutzen.
2) IP-Adressen einschränken, die auf eine Cloud-Anwendung zugreifen dürfen.
3) Verschlüsselung sensibler Daten, bevor sie in der Cloud gespeichert werden.
4) Verfolgung eines mehrschichtigen Sicherheitsansatzes.
   (Brown, 2016)

3.4.4 Internationale Standards und Regularien

Unternehmen müssen zahlreiche globale Vorschriften einhalten. In vielen Fällen gelten dieselben Vorschriften, die für lokale Umgebungen heranzuziehen sind, auch für die Cloud-Umgebung. Die führenden Cloud-Anbieter verfügen über zahlreiche Zertifizierungen, die belegen, dass sie die globalen Compliance-Anforderungen erfüllen. Aber die Einhaltung der Vorschriften in der Cloud liegt nicht nur in der Verantwortung der Cloud-Anbieter. Anbieter wie AWS und Azure geben Unternehmen Kontrollmöglichkeiten für ihre Sicherheit. Unternehmen tragen daher ebenso eine Verantwortung für die Gewährleistung der Compliance innerhalb des Cloud-Netzwerkes wie Cloud-Anbieter. In den nachfolgenden Kapiteln wird daher näher auf relevante Zertifikate und Regularien eingegangen, die Cloud-Anbieter, aber auch Unternehmen betreffen.

3.4.4.1. ISO/IEC 27001

Die Internationale Organisation für Normung (ISO) ist ein weltweites Gremium, das verschiedene Normen für unterschiedliche Bereiche sammelt und verwaltet. Dazu gehören alle Richtlinien und Prozesse, die für die Kontrolle und Verwendung von Daten relevant sind. Für den Schutz von Informationen und Informationssystemen bieten die Normen ISO 27001 und ISO 27002 Kontrollziele, spezifische Kontrollen, Anforderungen und Richtlinien, mit denen das Unternehmen eine angemessene Informationssicherheit erreichen kann. Dabei ermöglicht die ISO 27001 Norm die Zertifizierung des Unternehmens in Übereinstimmung mit einem international anerkannten Organisationsstandard für Informationssicherheit zur Dokumentation und zum Beweis konsequent

angewendeter Prozesse. Mit einer Zertifizierung nach ISO 27001 bestätigt ein Unternehmen die Erfüllung bekannter und anerkannter Sicherheitsstandards und fördert so das Vertrauen bei den Kunden. Ebenso reduziert der Nachweis der Einhaltung eines internationalen Standards das Risiko von Bußgeldern oder Schadensersatzzahlungen infolge von Rechtsstreitigkeiten, da gesetzlichen Anforderungen mit der Einhaltung von Standards begegnet werden kann.

Im Mittelpunkt der ISO 27001, die sich gerade in einer Neuauflage für das Jahr 2021/2022 befindet, steht die Forderung nach Planung, Implementierung, Betrieb und kontinuierliches Monitoring und Verbesserung eines prozessorientierten Informationssicherheitsmanagementsystems (ISMS). Der Geltungsbereich und der Umfang eines ISMS sollten für die Planung und Umsetzung definiert, Risiken sollten identifiziert sowie bewertet, und Kontrollziele für die Informationen und Informationssysteme ausgearbeitet werden. Daraus werden geeignete Maßnahmen zum Schutz des Betriebs abgeleitet.

Im Annex A der Norm sind insgesamt 39 Kontrollziele und 134 Maßnahmen für das Sicherheitsmanagement aufgeführt und damit ausdrücklich vorgeschrieben. Um die Übereinstimmung des ISMS mit der ISO 27001 zu überprüfen, muss ein Unternehmen ein Zertifizierungsverfahren von einer autorisierten Zertifizierungsorganisation durchlaufen. Die kodifizierten Anforderungen der ISO 27001 werden in ISO 27002 in Form eines Leitfadens erweitert und genaustens erläutert. In diesem werden gemeinsame Praktiken - oft auch als Best Practices bezeichnet - als Verfahren und Methoden angeboten, die sich in der Praxis bewährt haben. (Disterer, 2013)

3.4.4.2. ISO/IEC 27018

Wie wichtig eine Zertifizierung sein kann, zeigt die ISO 27018. Dies ist die erste internationale Norm, die speziell für den Datenschutz beim Einsatz von Cloud-Computing geschaffen wurde. ISO 27018 ist Teil der ISO 27000-Normenfamilie, die bewährte Verfahren für das Informationssicherheitsmanagement definiert, und ergänzt dabei die ISO/IEC 27002 um zusätzliche Sicherheitskontrollen, die bei der Verarbeitung personenbezogener Daten in öffentlichen Clouds anwendbar sind. Sie soll den Anbietern von Cloud-Diensten dabei helfen, die für personenbezogene Daten im Cloud-Computing typischen Sicherheitsrisiken besser zu bewältigen. Der Standard liegt in der aktuellen Fassung als ISO/IEC 27018:2019 vor.

Die Einhaltung der ISO 27018 stellt weiters einen Wettbewerbsvorteil, sowohl für Anbieter von Cloud-Diensten als auch für deren Kunden dar. Wenn Unternehmen den Verbrauchern zeigen können, dass ihre Daten durch etablierte Standards zum Schutz von personenbezogenen Daten geschützt sind, werden sie eher bereit sein, Geschäfte mit diesen Unternehmen abzuschließen. Zusätzlichen Nutzen generieren die Implementierung von ISO 27018-Kontrollmechanismen und

die Erlangung einer Zertifizierung beim Schutz des Unternehmens vor dem groben Fahrlässigkeitsvorwurf. Bei einem Verstoß und einer Klage wegen grober Fahrlässigkeit, die eine Steigerung der leichten Fahrlässigkeit darstellt, drohen deutlich härtere Strafe. Kann ein Unternehmen jedoch einen klar definierten Ansatz zum Schutz personenbezogener Daten vorweisen, sinkt die Wahrscheinlichkeit, dass grobe Fahrlässigkeit vorliegt. (Nunn, 2021)

3.4.4.3. DSGVO (Datenschutz Grundverordnung 2018)

Die Datenschutz-Grundverordnung ist ein rechtlicher Rahmen, der Richtlinien für die Erhebung und Verarbeitung personenbezogener Daten von in der Europäischen Union lebenden Personen festlegt. Da die Verordnung unabhängig davon gilt, wo Unternehmen Ihren Sitz haben, muss sie von allen Unternehmen beachtet werden, die europäische Kunden adressieren, auch wenn sie nicht explizit Waren oder Dienstleistungen für EU-Bürger anbieten.

Die Maßnahmen der Verordnung stellen sicher, dass personenbezogene Daten nicht standardmäßig einer unbestimmten Anzahl von Personen zugänglich gemacht werden. Damit diese Regelung in der öffentlichen Cloud befolgt wird, können Unternehmen Tools wie AWS Identity and Access Management und Azure Active Directory verwenden. Hiermit sind Datenzugriffe auf Nutzerebene verwaltbar. Die Cloud-Provider bieten diese Tools zwar an, es obliegt jedoch den Unternehmen selbst, diese auch entsprechend einzusetzen und zu konfigurieren. Dasselbe gilt für die Verschlüsselung und Löschung der Daten, die von der DSGVO gefordert werden. Findet ein Bruch der Regularien statt, kann dies mitunter zu hohen Strafen für ein Unternehmen führen, und gleichzeitig das Image des Unternehmens nachhaltig schädigen. (Selzer, 2020)

3.4.4.4. SOC-Audit

Anfang 2011 veröffentlichte das American Institute of Certified Public Accountants (AICPA) sein Rahmenwerk für die Berichterstattung über die Kontrolle von Service Organization Control (SOC), welches zuletzt 2018 überarbeitet wurde. Der Zweck dieses Rahmens ist es, zwischen den gängigen Arten von AICPA-Berichten zu unterscheiden, die Dienstleistungsunternehmen ihren Kunden vorlegen müssen. Bei SOC handelt es sich um keine klassische Zertifizierung, sondern um ein von einem zugelassenen Prüfer durchgeführtes Audit einer Unternehmung. Der Umfang eines SOC 2-Berichts wird vom Kunden und dem Prüfer unter Verwendung eines oder mehrerer Trust Service Principals (TSP) festgelegt. Diese werden vom Kunden spezifiziert, um festzustellen, ob ein vom Kunden betriebenes Informationssystem ausreichende Kontrollaktivitäten einsetzt, und die festgelegten Kriterien für die ausgewählten Prinzipien erfüllt. Der Kunde legt auch fest, ob für den SOC 2-Bericht eine "Typ 1"- oder "Typ 2"-Prüfung durchgeführt werden soll.

Beide Berichte befassen sich mit den Berichterstattungskontrollen und -prozessen einer Dienstleistungsorganisation im Zusammenhang mit den fünf Vertrauensgrundsätzen für Daten, wobei die Einhaltung von SOC 2, egal ob Typ 1 oder Typ 2, freiwillig ist. Bei einer Prüfung des Typ 1 deckt der Bericht die Wirksamkeit der internen Kontrollen zu einem bestimmten Zeitpunkt ab, z. B. Stichtag 30. November. Der Bericht bezieht sich nur auf die Wirksamkeit der internen Kontrollen, die zur Erreichung der Ziele des Dienstleisters entwickelt wurden, und bestätigt auch die Eignung der besagten Kontrollen für die Erreichung der Ziele. Ein SOC-2-Typ-2-Auditbericht deckt dagegen einen längeren Zeitraum ab. Dieser kann zwischen sechs und zwölf Monaten liegen, wobei der häufigste Zeitraum zwölf Monate beträgt. Er befasst sich mit der Gestaltung der internen Kontrollen und ihrer operativen Wirksamkeit im Hinblick auf die Erreichung der festgelegten Ziele. Aus diesem Grund wird im Regelfall ein SOC-2-Typ-2-Auditbericht von Kundenseite verlangt. (RSI Security, 2019)

4 NICHT-TECHNISCHE HERAUSFORDERUNGEN

Viele Unternehmen planen ihre Transformation in die Cloud unter der Annahme, dass sich die bestehenden Prozesse dadurch nur marginal oder gar nicht ändern, da nur eine lokale Veränderung des Speicherortes bzw. der Ausführung von IT-Systemen vollzogen wird. Des Weiteren herrscht die Meinung vor, dass bestehende Fähigkeiten und Qualifikationen nur einfachen Erweiterungen bedürfen. Dabei sind es in der Regel menschliche Verhaltensweisen und organisatorischer Reibung, die für Probleme sorgen. Die nachfolgenden Kapitel gehen näher auf diese nicht-technischen Faktoren ein.

4.1 Unternehmerischer Wandel

Wird die Cloud wie vorherige Outsourcing-Projekte behandelt, so manifestieren sich gewisse Probleme zwar nicht von Anfang an, jedoch kommen diese letztlich doch zum Vorschein. Das neue Potenzial der Cloud, und die damit einhergehende Transformation des Unternehmens, bringt eine Vielzahl disruptiver Veränderungen innerhalb einer IT-Organisation mit sich.

Anders ausgedrückt, Unternehmen müssen einen Change-Management-Prozess durchlaufen. Dies wirkt sich insbesondere auf traditionelle IT-Strukturen aus, um für Cloud-Modelle gewappnet zu sein. Da die Cloud immer mehr an Bedeutung gewinnt und die On-Premise-Infrastruktur in den Hintergrund rückt, verlieren auch die traditionellen Aufgaben der sogenannten „Infrastructure and Operations (I&O)“ Teams an Bedeutung für die Organisation.

Die I&O-Teams müssen sich daher weiterentwickeln, um weiterhin eine Relevanz für das Unternehmen zu bieten. In der Vergangenheit hatten I&O-Teams die Aufgabe, große Rechenzentren zu bauen, in denen Backend-Systeme verwaltet wurden. Diese Teams wurden auch damit betreut, auf Warnungen bei Vorfällen zu reagieren, diese vorab zu sortieren, und erst dann zu eskalieren, wenn es angebracht ist. Ihre Aufgabe als Ersthelfer ließ sich dahingehend als eine laufende Bewertung von geschäftlichen Vorfällen definieren, da für die betrieblichen Abläufe unterschiedliche Berechtigungen und Spezialanwendungen erforderlich sind, die rein von den I&O Teams verwaltet wurden. Diese traditionellen Arbeitsweisen bedürfen in der Cloud jedoch einem völlig neuen Ansatz. (Passmore, 2016)

Die meist sehr starren Arbeitsabläufe, die langen Umsetzungszyklen, und die Vorgaben, eine einheitliche Umgebung innerhalb des Unternehmens zu implementieren, um die Kosten niedrig und die Stabilität hochzuhalten, brachte vielen IT-Abteilungen den Stereotyp des Nein-Sagens bzw. Abblockens ein. Durch den Einsatz von Cloud-Lösungen ist es nun jedoch möglich, das zentrale Rechenzentrum durch einen Cloud-Service-Katalog zu ersetzen, und so Unternehmensmitarbeitern die Selbstbedienung daraus zu ermöglichen. Langwierige Umsetzungszyklen und

manuelle Genehmigungsprozesse gehören so der Vergangenheit an, es bedeutet allerdings auch große Veränderungen für die Rollen und Rollenbeschreibungen der Mitarbeiter sowie die Art und Weise, wie diese zusammenarbeiten.

4.2 Akzeptanz von Cloud-Computing

Die Umstellung auf Cloud-Computing ist einer der wichtigsten Techniktrends der letzten Jahre. Während es früher die Norm war, dass Unternehmen ihre eigenen Rechenzentren besessen und betrieben haben, geht die Tendenz immer weiter in Richtung Cloud-Computing. Es wird erwartet, dass der weltweite Markt für Cloud-Computing von 445,3 Milliarden US-Dollar im Jahr 2021 auf 947,3 Milliarden US-Dollar im Jahr 2026 ansteigen wird.

Cloud-Computing unterstützt Unternehmen bei der Nutzung von im Internet gehosteten Remote-Servern zur Speicherung, Verwaltung und Verarbeitung wichtiger Daten. Das zunehmende Datenaufkommen auf Websites und in mobilen Apps, der steigende Fokus auf die Bereitstellung kundenorientierter Anwendungen zur Steigerung der Kundenzufriedenheit und die wachsende Notwendigkeit, Investitionsausgaben und Betriebsausgaben zu kontrollieren und zu reduzieren, sind einige der Faktoren, die das Wachstum der neuen Technologien vorantreiben.

Diese Faktoren steigern auch die allgemeine Akzeptanz von Cloud-Computing. Waren früher IT-Verantwortliche oftmals skeptisch der Cloud gegenüber, haben die neuen Herausforderungen, denen sie sich ausgesetzt sehen, ein Umdenken herbeigeführt. Aufgrund von Covid-19 haben viele Unternehmen in allen Branchen das Modell der Heimarbeit eingeführt, um das Wohlergehen der Mitarbeiter zu sichern, und die betriebliche Effizienz aufrechtzuerhalten. Dies führte zu einer erhöhten Nachfrage an cloudbasierten Kollaborationslösungen.

So ist beispielsweise die Nutzeranzahl der Microsoft Teams-Plattform aufgrund der hohen Nachfrage nach Kollaborationslösungen weltweit auf 44 Millionen gestiegen. Die eigenständige Cloud-Lösung 8x8 Video Meetings verzeichnete Anfang 2020 sogar einen Anstieg registrierter Nutzer um mehr als 300%, und das in rund 150 Ländern. Andere beliebte cloudbasierten Kollaborationslösungen, die an Zugkraft gewonnen haben, sind unter anderem Google Hangouts, Cisco Webex, Slack und Zoom. (MarketsAndMarkets, 2021)

Cloud-Computing ist somit im Mainstream angekommen. Besonders die Covid-19 Pandemie hat die Akzeptanz cloudbasierter Lösungen um ein Vielfaches beschleunigt. Wo früher langwierige Implementierungsdiskussionen geführt wurden, mussten nun in kürzester Zeit Entscheidungen gefällt, und Cloudlösungen integriert werden.

4.3 Kosten des Cloud-Computing

Die Kostenvorteile der Cloud ergeben sich zu einem großen Teil aus der Hardwareverantwortung. Wenn Hardware vor Ort ausfällt, bedeutet das hohe Kosten für Unternehmen. In der Cloud liegt die Verantwortung für den Ausfall eines Servers oder eines ganzen Rechenzentrums beim Cloud-Anbieter. Diese Verschiebung der Kosten führt zu einem der großen Vorteile des Cloud-Computing: gleichbleibende, vorhersehbaren Kosten, sofern Ressourcen konstant bleiben. Diese Konsistenz der monatlichen Fixkosten wird von Unternehmen sehr geschätzt.

Ein wichtiger Aspekt ist hier, dass nur für Dienste bezahlt wird, die auch wirklich in Anspruch genommen werden. Auch die Betriebskosten können aufgrund des „Pay-as-You-Go“ Modells und der elastischen Skalierungsfunktionen in der Cloud viel günstiger umgesetzt werden als in klassischen On-Premise Varianten. Weiters werden die Kosten des typischen IT-Supportmodells von Unternehmensleitern und -eigentümern oft nicht klar verstanden. Die Personalkosten in der IT-Abteilung oder für den ausgelagerten IT-Support für die Bereitstellung, den Betrieb und die Wartung von Anwendungen und der zugrunde liegenden Infrastruktur können teuer sein.

Viele dieser Kosten werden in einer Cloud-Umgebung stark reduziert, da Cloud-Anbieter fast alle Kosten, die mit der Installation, dem Betrieb und der Wartung der Anwendungen der zugrunde liegenden Software-Infrastruktur und der zugehörigen Hardware verbunden sind, übernehmen. (Lynn T. , Mooney, Rosati, & Fox, 2020)

Dies führt oftmals dazu, dass Unternehmen Arbeiten im Ausmaß einiger Vollzeitäquivalenten einsparen können. Es bedeutet jedoch nicht, dass dadurch auch tatsächlich Stellen gestrichen werden müssen. Das Entfernen unnötiger Arbeiten mit geringem Mehrwert kann es dem IT-Team ermöglichen, sich auf strategische und wertschöpfende Dienstleistungen zu fokussieren. Dies führt weiters auch dazu, dass eine gut konzipierte Cloud-Plattform den Mitarbeitern ermöglicht, ihre Arbeit von überall und jederzeit zu erledigen.

Besonders die Covid-19 Krise hat gezeigt, wie wichtig es ist, dass Unternehmen flexibel sind und schnell reagieren können. Cloud-Computing kann jedoch auch höhere Betriebskosten verursachen, besonders dann, wenn Applikationen, die nicht ausdrücklich für den Einsatz in der Cloud konzipiert wurden und nicht ressourcenschonend sind, zum Einsatz kommen. Dies ist häufig bei „Legacy“-Anwendungen der Fall, die in ihrem aktuellen Zustand migriert werden. Die genauen Kosten von Cloud-Computing sind daher oftmals vorab schwer einzuschätzen.

Aus diesem Grund empfiehlt es sich, vor einer anstehenden Migration eine Prüfung und Einstufung der Anwendungen auf Kompatibilität zu Cloudtechnologien und die Häufigkeit der Verwendung im Unternehmen durchzuführen. Sollte diese Prüfung ergeben, dass einige Anwendungen nicht genutzt werden, ist eine Ausscheidung dieser Applikationen die bessere Wahl. Ein weiterer Aspekt, der berücksichtigt werden muss, ist der Kostenunterschied, der sich auf Grund von

unterschiedlichen Infrastrukturausbauten von Region zu Region ergeben kann. So kann das Nutzen eines anderen Standortes, der sich einige hundert Kilometer vom gewünschten Standort befindet, oftmals bereits eine Kostenreduktion herbeiführen. (Marquez, 2021)

4.4 Freigabe- und Genehmigungsprozesse

Freigabe- und Genehmigungsprozesse sind das A und O des IT-Service-Management (ITSM). Diese sind essenziell für eine adäquate Änderungskontrolle, z. B. für die Bereitstellung von Cloud-Ressourcen. Um eine entsprechende Governance im Unternehmen zu erreichen und sicherzustellen, dass Vorschriften und Gesetze eingehalten werden, muss die unrechtmäßige Nutzung der IT im gesamten Unternehmen verhindert werden. Hierzu können Freigabe- und Genehmigungsprozesse eingesetzt werden, die z.B. Mitarbeiter daran hindern eine riesige virtuelle Maschine bereitzustellen, ohne dass jemand davon weiß, oder eine Firewall-Änderung durchzuführen, die das ganze Netzwerk lahmlegt.

Da diese Prozesse komplexe Strukturen aufweisen können, und sich im Laufe ihres Zyklus häufig ändern, sind Unternehmen gut darin beraten, Workflow-Software einzusetzen. Somit können Freigabe- und Genehmigungsprozesse konsolidiert, bei Bedarf leicht geändert, und entsprechend aktualisiert werden.

4.5 Rechtliche Aspekte

Immer mehr Unternehmen entscheiden sich, ihre Systeme in die Cloud zu verlagern. Hierbei kommen jedoch rechtliche Aspekte zu tragen, die einige Unternehmen vor Herausforderungen stellen. Durch sich ständig weiterentwickelnde, rechtliche Standards, Vorschriften und Normen in Bezug auf Cloud-Computing müssen stetige Anpassungen vorgenommen werden.

Erschwerend kommt hinzu, dass in den Vereinigten Staaten, in Europa, in China und in anderen Ländern rechtliche Vorgaben komplett unterschiedlicher Umsetzung bedürfen. Dies gilt ebenso für die unterschiedlichen Märkte, in denen sich Unternehmen bewegen.

Branchen wie Gesundheitswesen oder Fintech- bzw. Banken-/Finanzdienstleistungen bieten ihren Kunden cloudbasierte Produkte und Dienstleistungen an, die eine noch nie dagewesene Bequemlichkeit und Mobilität bieten. Allerdings gehen damit auch noch nie dagewesene Risiken einher. Viele Unternehmen gehen davon aus, dass Lieferanten von cloudbasierten Lösungen die notwendigen Schritte unternehmen, um die Datensicherheit zu gewährleisten, und die vielen potenziellen rechtlichen Probleme zu lösen.

Die Realität zeigt jedoch, dass die Anbieter von Cloud-Diensten nicht alle rechtlichen Anforderungen jedes Marktsegmentes kennen, und diese somit umsetzen können. Cloud-Dienst-Anbieter und Nutzer müssen daher eng zusammenarbeiten, um festzulegen, welche Maßnahmen getroffen werden müssen. (Gordon, 2016)

Der geografische Standort der Ressourcen des Cloud-Anbieters variiert zunehmend, da Cloud-Anbieter ihr Angebot auf Kunden in der ganzen Welt ausweiten. Aufgrund des Ressourcen Poolings, das vielen Cloud-Diensten zugrunde liegt, wissen viele Nutzer unter Umständen nicht genau, auf welchen Servern des Cloud-Anbieters ihre Daten gespeichert sind, und wo sich diese Server befinden. Für eine feinere Kontrolle über Unternehmensdaten, einschließlich spezifischer geografischer Beschränkungen, sind viele Cloud-Anbieter bereit, Individuallösungen auf Basis der gewünschten Anforderungen zu entwickeln.

5 METHODISCHES VORGEHEN

Um die Forschungsfrage zu beantworten, wird in der vorliegenden Arbeit die qualitative Forschung gewählt. Hierbei werden die untersuchten Aspekte im Gegensatz zur quantitativen Forschung nicht gemessen und ausgewertet, sondern in ihrer ganzen Komplexität betrachtet (Flick, 2005).

Dazu passend wird für die Befragung der Experten und Expertinnen eine teilstandardisierte, qualitative Befragungsmethode gewählt. Die Befragung wird anhand eines Interviews digital durchgeführt. Für den Interviewleitfaden wurden die aus der Theorie gewonnen Erkenntnisse als Basis für die qualitative Befragung herangezogen. Der Interviewleitfaden lässt sich in folgende Dimensionen bzw. Kategorien einteilen:

- Qualifikation und Profil der Experten und Expertinnen: In diesem einleitenden Teil sollen in erster Linie Rollenbezeichnung, sowie die Berufserfahrung der befragten Personen abgefragt werden. Dies dient dazu, den Aussagen der Befragten entsprechende Relevanz zu verleihen.
- Einflussfaktoren: Dies ist der Beginn des Hauptteils des Experteninterviews und es soll die Meinungen der Experten zu den Einflussfaktoren erhobenwerden, die bei der Transformation der Geschäftsprozesse in die Cloud prioritär zu berücksichtigen sind. Hierzu wird auf folgende Kriterien genauer abgefragt:
    - Change-Management
    - Mitarbeiter Qualifikationen
    - IT-Teams und Organisation
    - Cybersecurity
    - Zertifizierungen

Das Ziel ist es, Erfahrungen und Meinungen von Experten und Expertinnen zu diesem Themengebiet zu erforschen, und diese systematisch auszuwerten, um daraus ein Gesamtbild für die Transformation von Geschäftsprozessen in die Cloud zu kreieren. Tabelle 1 zeigt hierzu das Qualifikationsprofil der Experten und Expertinnen.

Experte/ Expertin	**Rollenbezeichnung**	**Berufserfahrung**
1	Chief Strategy Officer	13 Jahre
2	Head of IT	6 Jahre
3	Chief Information Officer	5-6 Jahre
4	Cloud Migration Consultant	4 Jahre

Tabelle 1: Qualifikationsprofil der Experten und Expertinnen

Die zur Durchführung einer empirischen Forschung gestellten Fragen können grundsätzlich in nicht strukturierte, halb strukturierte und vollstrukturierte Befragungen kategorisiert werden. Im Zuge dieser Arbeit wurde rein auf nicht strukturierte Fragestellungen zurückgegriffen.

Die nicht strukturierte Befragung zielt darauf ab, eine frei formulierte Antwort der Experten und Expertinnen zu erhalten, wohingegen in der halb strukturierten Befragung nicht standardisierte Fragen verwendet werden. Bei der vollstrukturierten Befragung werden den Experten- und Expertinnen Aussagen mit Antwortvorgaben zur Verfügung gestellt, um hier bereits passende Antwortmöglichkeiten wählen zu können. Die qualitative Befragung bringt den Vorteil der offenen Fragestellung mit sich, wodurch die Antworten der Experten und Expertinnen nicht eingeschränkt werden. Dies erlaubt der Forschung, ihre Werte und Ziele zu erfassen (Mayring P. , 2016). Für die in dieser Arbeit geplante qualitative Befragung müssen, im Gegensatz zur quantitativen Befragung, zusätzlich eigene Kriterien entwickelt werden:

- Verfahrensdokumentation: Die Ergebnisse müssen zur weiteren Verwendung in ihrer Gänze nachvollziehbar sein. Dahingehend muss eine Dokumentation des eingesetzten Verfahrens durchgeführt werden.
- Argumentative Interpretationsabsicherung: Im Gegenzug zu rein quantitativen Methoden, die mittels mathematischer Daten erhoben werden, basieren die Ergebnisse in der qualitativen Forschung auf den Interpretationen sprachlicher und textlicher Formen. Um entsprechende Nachvollziehbarkeit zu gewährleisten, muss die Herleitung der Ergebnisse für andere Personen schlüssig sein.

- Regelgeleitetheit: Eine zentrale Komponente der qualitativen Forschung ist deren offene und individuelle Form. Um allerdings einen klaren und strukturierten Rahmen zu gewährleisten, muss der Forschungsprozess entsprechend geplant werden.
- Nähe zum Gegenstand: Die qualitative Forschung setzt an sozialen Phänomenen an, deren Ziel es ist, Forschung im Sinne einer gleichberechtigten Beziehungssituation, mit den involvierten Personen, durchzuführen. Da die Forschung nicht unter Laborbedingungen durchgeführt wird, ist diese der Alltagssituation der beforschten Personen so nahe wie möglich.
- Kommunikative Validierung: Um Missverständnisse zu vermeiden ist es wichtig, einen Dialog zwischen dem Forscher und den involvierten Personen anzustreben. Dadurch kann auch die Relevanz entsprechender Ergebnisse durch wichtige Argumentationen gewonnen, und die Interpretation der Daten sowie die Gültigkeit der Ergebnisse bestätigt werden.
- Triangulation: Um die Qualität der qualitativen Forschung zu steigern, können mehrere Forschungsmethoden miteinander kombiniert werden (Mayring P. , 2016).

Zusätzlich zu den angeführten Richtlinien müssen laut (Bortz & Döring, 2016) folgende Kriterien erfüllt werden:

- Formulierung von möglichst offenen Fragen (W-Fragen); verständliche und eindeutige Formulierung; Offenheit der Fragen beachten und Experten bzw. Expertinnen nicht in ihren Antworten einschränken
- Die Beantwortung des Fragebogens durch die Experten und Expertinnen darf nicht durch den Forschenden beeinflusst werden; bei Fragen gibt es jedoch die Möglichkeit, dass Experten und Expertinnen sich schriftlich oder telefonisch an den Forschenden wenden können
- Fragen müssen neutral, und nicht suggestiv formuliert sein
- Faktenfragen müssen am Anfang stehen
- Geschlossene Fragen (Ja/Nein-Fragen) können zur Vorabfilterung eingesetzt werden

Um eine möglichst breite und qualitativ hochwertige Auswertung zu erreichen, wurden 4 Experten und Expertinnen ausgewählt, wobei die Fachkenntnisse eine prioritäre Rolle gespielt haben. Die Auswertung des Interviews fand mittels der Inhaltsanalyse nach Mayring statt, wobei hier eine Reduktion von 7 auf 4 Schritten auf Grund der kleineren Datenmenge vollzogen wurde. (Mayring P. , 2015) Die angewandten Schritte werden in folgender Abbildung dargestellt, um einen Überblick über die Auswertungsmethodik zu erlauben.

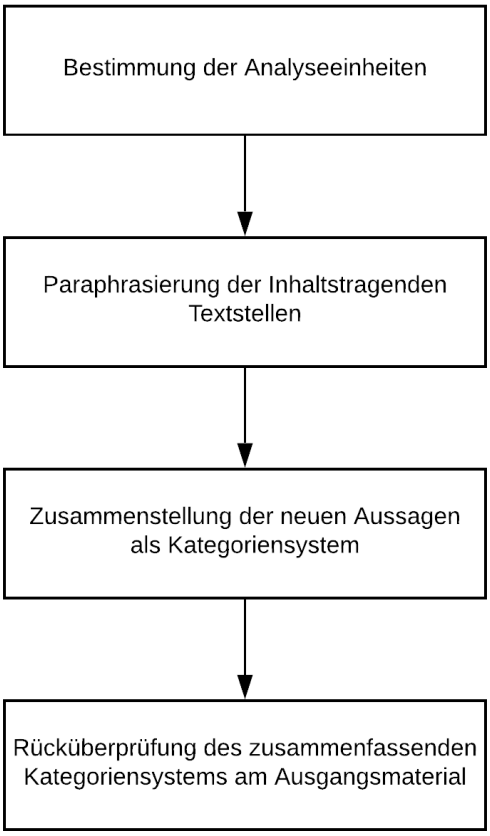

Abbildung 3: Inhaltsanalyse nach Mayring (eigene Darstellung nach Mayring, 2015)

Diese Darstellung stellt das Vorgehen des empirischen Teiles dar. Hierzu werden die Aussagen der Experten und Expertinnen paraphrasiert und einander gegenübergestellt. Dazu wird je ein Unterkapitel pro Frage zur Verfügung gestellt und die Frage anschließend im Detail ausgewertet.

6 EMPIRISCHE ERGEBNISSE

Die genaue Beschreibung der eingesetzten Methoden wurde in Kapitel 5 durchgeführt. Es haben sich 4 Experten und Expertinnen bereit erklärt, an der empirischen Forschung teilzunehmen. In diesem Kapitel werden Antworten nach zuvor durchgeführter Paraphrasierung analysiert und ausgewertet.

6.1 Ergebnisse

In diesem Teil des Abschnittes werden die Aussagen der Experten paraphrasiert und den verschieden Themengebieten zugeordnet und damit eine Basis für die Diskussion in Kapitel 7 geschaffen.

6.1.1 Einflussfaktoren

In diesem Abschnitt des Interviews wurden die Meinungen der Experten zu den Einflussfaktoren erhoben, die bei der Transformation der Geschäftsprozesse in die Cloud prioritär zu berücksichtigen sind. Experte 1 war der Meinung, dass es „ein großer Einflussfaktor ist, dass Personen, die mit dem Thema Cloud aufgewachsen sind, mittlerweile die Entscheidungsträger von heute und morgen sind. […] Für diese Personen ist Cloud zum Standard geworden, wodurch das Herausgeben von Daten deutlich leichter fällt. Ein weiterer Faktor ist der Bereich des Change-Managements, um die Ängste der Mitarbeiter aufzufangen und die Prozesse des Unternehmens an die Cloud anzupassen […]“.

Diese Meinung konnte auch von Experte 3 beobachtet werden, der es wichtig fand, dass „[…] Change-Management in einem Unternehmen betrieben wird, um die Mitarbeiter zu überzeugen und den Sinn der Veränderung zu erläutern.“ Einen zusätzlichen Faktor sah Experte 3 in „[…] Technik denn wenn Mitarbeiter mit dieser nicht vertraut sind besteht die Angst vor der Veränderung, die die Cloud mit sich bringt“.

Eingehend auf die Einflussfaktoren kommentierte Experte 2: “Ein Einflussfaktor ist sicherlich, ob es erlaubt ist in die Cloud zu wechseln, im Gesundheitsbereich oder öffentlichen Bereichen ist dies ja teilweise verboten beziehungsweise nur spezialisierte Cloud Lösungen erlaubt. [...] Weitere Faktoren sind natürlich die Kosten, meiner Erfahrung nach ist Cloud teurer als On-Premise, hat aber andere Vorteile und natürlich, wie die IT diese Umstellung organisatorisch bewältigt“.

Experte 4 vertrat die Meinung, dass „es wichtig ist, dass die Unternehmen bereit sind ihre internen Prozesse zu verändern, da im Vergleich zu On-Premise-Lösungen andere Prozesse benötigt werden.“ Auch sei dies wichtig, „[…] um die Kosten stabil zu halten. Die Mitarbeiter müssen auch

über die Vorteile aufgeklärt werden und wie sich die Veränderung der Prozesse auf sie auswirkt.“ Als weiteren Faktor sah Experte 4 die „[…] Sicherheit, da in diesem Bereich oft Überzeugungsarbeit notwendig ist, besonders wenn sich die Sicherheitsvorkehrungen im Unternehmen ändern.“

Weiters wurde erhoben, wie diese Einflussfaktoren aktiv gesteuert werden können. Experte 1 antwortete wie folgt: „Es kommt natürlich auf die Einflussfaktoren an, zusätzlich zu den von mir erwähnten Faktoren gibt es ja noch andere Faktoren, wie Flexibilität schaffen, Kosten senken etc. Diese kann man aktiv steuern. […] Ich glaube, das Wichtigste ist einfach, wenn Prozesse in die Cloud ausgelagert werden und dass neben dem Change-Management darauf geachtet wird, dass es sich um ein Projekt handelt, und deswegen aktives Projektmanagement, eine Planung und eine Strategie benötigt wird.“

Experten 3 und 4 sahen dies ähnlich, da Experte 3 meinte: “Hier kommt definitiv Management ins Spiel, Change-Management wurde ja schon angesprochen, es ist aber auch wichtig, dass Projektmanagement eingebunden wird, damit eine Struktur vorhanden ist.“ Experte 4 ergänzte, dass „dafür einfach ein gutes Management benötigt wird und eine Übersicht über die Firmenprozesse damit Projektmanagement betrieben werden kann.“

Experte 2 fiel hier aus der Rolle und kommentierte: „Was den Preis angeht kann man natürlich Anbieter vergleichen.“

3 von 4 Experten gaben auch ihre Meinung zu der Frage, welche Faktoren in der Zukunft die größte Rolle spielen werden, zu ihrem Besten. Experte 1 meinte, „wenn man über Cloud-Computing spricht, wird in Zukunft sicherlich das Wichtigste sein, dass es sicher ist.“ Dem stimmte auch Experte 4 zu, der „[…] glaubt, dass es die Sicherheit sein wird. […] die Sicherheut und Cybersecurity im Unternehmen ist einfach so wichtig. Und wird auch wichtiger durch Internet of Things, Bring-your-own-device, etc.“

Experte 3 hingegen „[…] würde auf Change-Management tippen, da die Überzeugung der Mitarbeiter immer einer der größten Aufgaben im Unternehmen ist.“

6.1.2 Change-Management

In diesem Kapitel wurde die Meinung der Experten zum Einfluss des Change-Managements bei der Transformation von Geschäftsprozessen in die Cloud erhoben. Experte 1 sah dies als „[…] einer der wichtigsten Komponenten, nur wenn User die Änderung der Prozesse akzeptieren, kann man es entsprechend umsetzen. […] Wenn Change-Management nicht aktiv gemanagt wird, dann hat man ein großes Problem, man muss die Ängste vom Anfang an adressieren."

In Bezug auf Change-Management sagte Experte 2, dass „[…] eine gute Vorbereitung wichtig ist und es muss wie immer im Change-Management Projektmanagement betrieben werden. Es müssen die Folgen abgeschätzt werden und die Vor- und Nachteile erwogen werden. Aus meiner Sicht ist es auch wichtig zu berücksichtigen wie die Gesamt IT-Lösungen eingebunden wird, die Sicherung, das Zugriffssystem, Desaster Management etc. muss ein großes Ganzes ergeben."

Experte 3 und 4 gaben sich fast unisono, wobei Ersterer meinte „Change-Management ist eine sehr wichtige Komponente, wenn nicht sogar die wichtigste. Denn auch wenn ein System gut funktioniert und alles gut geplant wurde, wenn man die Mitarbeiter nicht vom Nutzen der Transformation überzeugen kann, wird es im Unternehmen nicht funktionieren. Man sieht das immer wieder bei Bestellungen wo Kunden ein bereits bestelltes Produkt stornieren da die Überzeugung der Mitarbeiter nicht funktioniert hat" und Letzterer meinte, es sei „[…] der wahrscheinlich wichtigste Bestandteil und muss bei der Transformation in die Cloud definitiv existieren."

Wie auch schon in Kapitel 6.1.1, wurden die Experten befragt, wie hier aktiv gesteuert werden kann. Experte 1 hat dazu keine Meinung abgegeben.

Experte 2 sagt dazu aus, aktive Beeinflussung wäre möglich mit „gutem Projektmanagement, und man muss auch die Stakeholder einbeziehen."

Experte 3 vertrat hier die Meinung, es sei „[…] einfach Management, man kann dies durch Projektmanagement umsetzen aber man benötigt einfach Managementkonzepte."

Experte 4 hingegen führte aus, Change-Management sei „[…] an sich ist ja schon etwas Aktives, da es im Unternehmen betrieben werden muss. Es gibt verschiedene Methoden, aber es ist wichtig, dass die Mitarbeiter informiert werden, es klare Ziele gibt, und dass die Entscheidungen nachvollziehbar sind."

Schlussendlich wurden auch noch Informationen zu den Unterschieden zwischen der jetzigen Generation und der zukünftigen Generation Beta, also die Generation zwischen 2025 und 2039, erhoben. Experte 1 glaubt „[…] diese Generation wird sich keine Gedanken mehr machen, ob etwas in der Cloud gehostet wird, Cloud-Computing wird hier der Standard sein. […] Diese Personen werden sich über Datenschutz weniger Gedanken machen da es viel wichtiger ist das eine Vernetzung untereinander vorhanden ist. Das sieht man schon jetzt. Es geht immer mehr

Richtung Remote, das Verlangen nach Home-Office steigt. Dies ist zwar auch mit On-Premise-Lösungen möglich, führt aber zu einer erhöhten Komplexität."

Experte 2 stimmte dem zu und meinte, „diese Generation wird vermutlich aufgeschlossener sein, es ist schwierig die Zukunft zu projizieren, aber ich gehe davon aus das das Wachstum beschleunigt wird und diese Generation noch offener ist." Auch Experte 3 konnte sich dieser Meinung anschließen, und findet, es sei „jetzt natürlich eine Prognose, aber wenn sich die jetzige Entwicklung fortführt, dann glaube ich, diese Generation wird viel offener für Cloud-Computing sein, da sie damit aufwächst." Dem schließt sich Experte 4 unisono an und kommentiert: „Change-Management wird für diese Generation leichter sein da Cloud-Computing weiter verbreitet sein wird und diese Generation offener gegenüber dem Thema Cloud sein wird. Auch Home-Office wird eine größere Rolle spielen und die Umsetzung ist leichter mittels einer Cloud Lösung."

6.1.3 Mitarbeiter Qualifikationen

In diesem Abschnitt wurden die Experten zu den Fähigkeiten und Qualifikationen der Mitarbeiter und Mitarbeiterinnen befragt wobei hier der Unterschied zwischen On-Premise und Cloud im Vordergrund stand.

Alle Experten und Expertinnen waren sich einig, dass es hier zu Veränderungen in der benötigten Mitarbeiterqualifikation kommen wird. Experte 1 äußerte sich folgendermaßen: „Bei On-Premise versucht man alles zu handhaben, die Hardware wird gekauft, installiert und gewartet. In der Cloud existieren diese Aspekte nicht, sondern es werden spezialisierte Ressourcen benötigt, welche natürlich vom Cloud Anbieter abhängig sind. […] Bei On-Premise mussten die Mitarbeiter sich weniger Gedanken machen, wie die Prozesse im Unternehmen zusammenspielen, und wie diese unterstützt werden können. In der Cloud ist mehr analytisches und strategisches Denken in diesem Bereich notwendig, man benötigt hier das Wissen, wie man ein Data Warehouse oder eine Business Intelligence schaffen kann, und die Flut der Daten müssen ausgewertet werden. Technisches Wissen wird weiterhin notwendig sein, aber es wird sich dahingehend abwandeln, dass Mitarbeiter verschiedene Zertifizierungen für die unterschiedlichen Cloud Anbieter benötigen werden."

Experte 2 gab zu verstehen, dass „[…] beim Endbenutzer sich wenig ändern wird, bei den Technikern gibt es natürlich Änderungen es müssen jetzt keine lokalen Server mehr gewartet werden, aber es muss Wissen über die Cloud bestehen. Das Ganze wird vielleicht auch etwas schlanker, die unternehmenseigenen Techniker werden aber trotzdem benötigt. Auch wenn das Warten der lokalen Server wegfällt, müssen nun Userkonten angelegt werden und Konfigurationen vorgenommen werden."

Experte 3 sah bei den benötigten Qualifikationen große Änderungen, denn „[…] bei On-Premise-Lösungen wurde detailliertes Wissen bezüglich der Server und der grundsätzlichen Technik benötigt. Bei Cloud-Computing ist dies anders, es wird zwar noch immer technisches Wissen benötigt, aber dies richtet sich auf den Bereich des Cloud-Computings. Mitarbeiter müssen die Fähigkeit besitzen, mit Daten umzugehen und diese zu interpretieren. Mitarbeiter müssen auch die Unternehmensprozesse verstehen und diese in einen Cloud-Computing Ansatz einbinden."

Die Meinung von Experte 3 konnte auch durch Experte 4 gestützt werden, der angab, „[…] bei Cloud-Computing wird ein anderes Fähigkeiten-Set benötigt, Mitarbeiten müssen mit Daten arbeiten können, denn oft wird in diesem Bereich Informationsmanagement betrieben. Die besten Tools sind nutzlos, wenn man diese nicht interpretieren kann, um die Prozesse zu optimieren. Das war bei On-Premise-Lösungen teilweise nicht notwendig, dort war es wichtig, dass Mitarbeiter die Hardware verwalten und warten konnten."

6.1.4 IT-Teams und Organisation

In diesem Abschnitt wurden die Auswirkungen von Cloud-Computing auf IT-Teams und die Organisation erfragt. Die Meinung von Experte 1 dazu war: „Neben den Qualifikationen muss sich auch der tägliche Ablauf verändern, da einige Aufgaben wie Beschaffung von Hardware wegfallen. Dieser Bereich wird völlig ausgelagert, in unserem Unternehmen ist der Head of IT für einige dieser Aufgaben zuständig, der Rest wurde aber ausgelagert an eine IT-Dienstleistungsfirma. Diese warten die Computer und Server, da sie sowieso nicht mehr On-Premise sind. Es gibt daher definitiv mehr Dienstleistungsgeschäft und Lieferantenprüfungen werden benötigt. […] Die Reduzierung der IT-Teams findet dann natürlich statt, da gewisse Aufgaben nicht mehr benötigt werden, und es keinen Sinn macht, jemanden vor Ort anzustellen, wenn diese Dienstleistung nur für 2 Monate im Jahr in Anspruch genommen wird. […] Bei einer Transformation in die Cloud müssen auch die Prozesse überprüft werden, ob diese noch sinnvoll für das Unternehmen sind. Prozesse müssen dann aber, falls notwendig, auch wirklich abgeändert werden."

Experte 2 tat sich schwer, hier eine konkrete Aussage zu treffen, und konnte nur eine Schätzung abgeben, da er „[…] den Einfluss auf die IT-Teams schwer beurteilen kann, unsere Firma ist dafür zu klein, um eine Aussage dazu zu treffen, ob die IT-Teams wachsen oder schrumpfen. Theoretisch müssten sie kleiner werden, praktisch kann ich es nicht beurteilen, denn in unserer Firma ist gleichzeitig ein Unternehmenswachstum einhergegangen, und wir sind in der gleichen Zeit um das Vierfache gewachsen. Die Prozesse müssen gleich wie bei jeder Softwareeinführung adaptiert werden, da sehe ich keinen großen Unterschied."

Experte 3 und 4 stimmten mit der Meinung von Experte 1 überein, dass es deutliche Änderungen geben wird. Experte 3 meinte „es verändert sich sehr viel, meiner Meinung nach führt es zu einer

Reduktion der IT-Teams und es gibt eine Änderung wie diese zu funktionieren haben. Wenn diese sich vorher eher auf die Hardware fokussiert haben, ist es danach notwendig, die Unternehmensprozesse einzubinden, und hierfür wird eine andere Struktur benötigt, und das Unternehmen muss sich wandeln." Experte 4 stimmt dahingehend zu, dass IT-Teams „[…] sich verändern, die IT-Teams werden sich reduzieren, da unternehmenseigene Techniker nicht mehr notwendig sein werden. Es ist leichter, die verbliebene Hardware auszulagern, als ein eigenes Team dafür zu betreiben. Auch die Strukturen im Unternehmen müssen sich anpassen, da Cloud-Computing abgeänderte Prozesse benötigt. Der Grad der Veränderung hängt davon ab, wie die Strukturen davor aufgebaut waren."

6.1.5 Freigabeprozesse und Servicekatalog

In diesem Unterkapitel wurden die Experten befragt, wie sich Freigabeprozesse bei Cloud Lösungen verändern, und ob es zu einem Wandel hin zu Servicekatalogen kommt. Experte 1 hatte dazu folgende Meinung: „Natürlich ist es wichtig, dass bei Cloud-Lösungen Freigabeprozesse existieren. Man braucht sich nur einmal vorstellen, wie viel Schaden jemand anrichten kann, wenn Änderungen einfach so durchgeführt werden, ohne dass jemand die Hand darüber hat. Das wird bei Cloud-Computing umso wichtiger sein, da hier immer mehr Dienste verwendet werden."

Zum Thema Servicekatalog meinte Experte 2, dass „[…] dies für ein Unternehmen deutliche Änderungen bringt. Es ist de facto eine Liste von möglichen Diensten. Also wie eine Menükarte aus der man mittels „Pick and Choose" seine gewünschten Dienste wählt, die vorab von der IT und ggf. dem Management freigegeben wurden, vor allem in Bezug auf datenschutzrechtliche Aspekte. Oftmals funktionieren die Aufnahmen von Diensten in den Servicekatalog auch deutlich schneller als das bei selbst installierten Anwendungen der Fall war, da hier entsprechende Absicherungen wie Zertifikate oder Service Level Agreements bei den Anbietern schon vorliegen."

Experte 3 meinte, es sei „[…] definitiv anders. In der Cloud ist es eher üblich, schon bestehende Services zu wählen, damit kein gesonderter Freigabeprozess notwendig ist. Da diese Prozesse bei On-Premise-Lösungen dafür gesorgt haben, das schnelle Reaktionen auf neue Firmeneinflüsse oftmals langwierig waren, gibt es schon Bedarf. Wenn bei Cloud Lösungen ein File-System benötigt wird, ist es möglich, zum Beispiel SharePoint einzuführen, ohne dass eine Überprüfung notwendig ist. Denn man weiß, die benötigten Zertifikate existieren. Aus diesem Grund bin ich der Meinung, dass es Richtung Servicekatalogen geht, weil es auch effizienter ist."

Experte 4 stimmte den anderen Experten dahingehend zu, und meinte „die ändern sich auf jeden Fall, der Vorteil von Cloud-Computing ist, dass im Unterschied zu On-Premise-Lösungen Freigabeprozesse nicht bei jedem Produkt mehr so langwierig sind. Dort gibt es Produkte, die funktionieren mit den gewissen Anbietern, man weiß diese sind sicher, und fügt sie einfach hinzu." Auf

Rückfrage ob hier ein Wechsel auf Servicekataloge stattfindet, antworte Experte 4 folgendermaßen: „Genau so ist es, man nimmt einen Service aus dem Katalog und baut ihn ein“.

Experte 2 konnte zu diesem Thema leider keine Antwort geben, da er „hier zu wenig Bezugspunkte hat“.

6.1.6 Cybersecurity

In diesem Unterkapitel wurden die Meinungen der Experten zu den Herausforderungen der Cybersecurity eingeholt. Experte 1 kommentierte dies folgendermaßen: „Die größte Herausforderung ist sicherlich, die Security jetzt sicherzustellen. Denn es gibt momentan viele Attacken, und das bekommen wir auch durch unsere Lieferanten mit, wo es jede Woche mehrere hundert Angriffe gibt, die Firmen aber Angst haben, dies öffentlich zu kommunizieren. […] Es zeigt auch, dass Zertifizierungen nichts mit Cybersecurity zu tun haben, denn die Zertifizierung sagt nichts darüber aus, wie sicher die Systeme wirklich sind. Eine uns bekannte Firma hatte eine ISO 27001 Zertifizierung, wurde gehackt, und hat sich geweigert, das Lösegeld zu zahlen. Kritische Kundendaten sind nun im Darknet veröffentlicht.“

Experte 2 fand: „Die Herausforderung ist, dass die Software von überall aus erreichbar ist. Aus diesem Grund ist eine Einschränkung notwendig, und ich muss mir überlegen, wie ich diese gestalte. Verwende ich Multifaktor-Authentifizierungen, oder erlaube ich nur Firmengeräte den Zugang. […] Eine weitere Herausforderung ist das Backup. Bei On-Premise ist das zu 100 Prozent unter eigener Kontrolle. Bei der Cloud gilt der Ansatz „Trust the Cloud“. Es ist aber wichtig, sich unbedingt auch selbst Gedanken über das Backup zu machen. Natürlich wird die Cloud nicht wegbrechen, da diese redundante Systeme betreiben. Aber einfache Sachen, wie überschriebene Daten, sind schwer wiederherzustellen. Aus diesem Grund haben wir uns entschieden, bei geschäftskritischen Systemen ein zusätzliches Onsite Backup zu machen.“

Experte 3 vertrat die Meinung, Cybersecurity rücke „[…] natürlich in den Fokus, da die Daten im öffentlichen Internet sind, und es auch öfter der Fall sein wird, dass Mitarbeiter nicht nur vom Firmenstandort aus auf Daten zugreifen. Sicherheitsstandards im Unternehmen müssen deswegen angepasst werden. Der Vorteil ist, dass man von der Cybersecurity der Großen geschützt wird. Anbieter wie Amazon, Google oder Microsoft haben hier ganz andere Budgets für Cybersecurity. […] Auf diese Struktur darf man sich natürlich nicht verlassen und man muss auch im Unternehmen Vorkehrungen treffen. Mit Multifaktor-Authentifizierung zum Beispiel.“

Dass die Herausforderungen in Bezug auf Cybersecurity anders werden, vertrat auch Experte 4 und „[…] deswegen benötigt man andere Sicherheitsvorkehrungen. Zugänge müssen geregelt werden und es muss eine Entscheidung getroffen werden, welche und wie viele Authentifizierungsmethoden genutzt werden. Auch die Mitarbeiter müssen sich anders verhalten, wodurch

Schulungen in diesem Bereich notwendig sind. Wobei hier auch der Sinn der Schulung den Mitarbeitern gezeigt werden muss. […] Auch bei den Cloud-Anbietern muss man auf die Sicherheit achten. Auch wenn diese mehr Budget für Sicherheit aufwenden können, sind nicht alle Anbieter gleich gut aufgestellt."

Weiters wurde die Frage gestellt, ob Cloud- oder On-Premise-Lösungen schneller auf Sicherheitslücken und sicherheitsrelevante Aspekte reagieren. Alle Experten waren sich dahingehend einig, dass Cloud-Anbieter deutlich schneller auf sicherheitsrelevante Aspekte reagieren. So meinte Experte 1, dass „[…] Cloud Lösungen mit Sicherheit schneller reagieren, da die großen Anbieter, bevor die Lücken öffentlich werden, diese schon schließen. Weiters haben diese Anbieter Teams die gezielt nach Zero-Day-Exploits suchen und Sicherheitslücken schließen. Das kann man sich als Unternehmen mit On-Premise-Hosting nicht leisten. Da wird man erst auf Sicherheitslücken aufmerksam, wenn diese veröffentlicht werden. Man ist deswegen erst viel später in der Lage diese Lücke zu schließen."

Die Äußerungen von Experte 1 konnte auch Experte 2 teilen, denn das Schließen von Sicherheitslücken „[…] funktioniert in der Cloud besser. So werden Security Bulletins herausgegeben, womit On-Premise-Lösungen die Sicherheitslücken patchen müssen. In der Cloud ist es aber schon erledigt. Das ist in der Cloud besser gesteuert. Die schließen diese Lücke bevor sie es veröffentlichen."

Auch Experte 3 und 4 sahen Geschwindigkeitsvorteile bei den Cloud-Anbietern. Experte 3 sagte, „Cloud Lösungen sind definitiv schneller, die Anbieter haben ein Budget für Cybersecurity, da kann man nicht mitspielen. Die Sicherheitslücken werden meistens auch schon vor dem Veröffentlichen geschlossen, während man bei einer On-Premise-Lösung auf die Veröffentlichung warten muss, und erst dann anfangen kann, die Lücke zu schließen." Experte 4 sah den Grund für Geschwindigkeitsvorteile in darin, dass „[…] die Anbieter eigene Teams haben, die nach Sicherheitslücken suchen." Wie drei von vier Experten auch, sah Experte 4 die unterschiedlich zur Verfügung stehenden Budgets als Grund, dass hier solch eine Lücke zwischen On-Premise und Cloud klafft, denn „[…] die Budgets, die hier zur Verfügung stehen, kann man sich als kleineres Unternehmen nie leisten, gleichzeitig erfährt man in der Cloud auch früher von den Sicherheitslücken, da die Anbieter diese gleich schließen. Bei On-Premise ist man selbst dafür verantwortlich zu überprüfen, ob neue Sicherheitslücken veröffentlicht wurden."

6.1.7 Zertifizierungen

In diesem Abschnitt wurden die Experten zu dem Nutzen von Zertifikaten bei der Umsetzung von Cybersecurity in der Cloud befragt. Experte 1 fand, dass „[…] regelmäßige Audits und Zertifikate bedeutet, dass Unternehmen sich mit dem Thema Cybersecurity befassen. Dadurch hat man die

Absicherung, dass Unternehmen sich mit dem Thema beschäftigt haben, wie stark das Unternehmen, das im täglichen Tun umsetzt, sei dahingestellt, da Audits nicht täglich stattfinden. Wenn die Zertifizierung existiert, gibt es zumindest einmal ein Minimum. Es gibt ein Qualitätsmanagement System, und ggf. ein Informationssicherheitssystem. Das muss ich zumindest etablieren, um zur Zertifizierung zu kommen. Auch in der durchzuführenden Risikoevaluierung wird man vielleicht auf Probleme aufmerksam, die sonst untergehen würden, und vielleicht löst man diese einfach mit."

Experte 2 berichtete aus der Praxis, denn sein Unternehmen „[…] besitzt eine ISO 9001 Zertifizierung, welche schon einige Vorgaben enthält. Diese bezieht sich auf die Geschäftsprozesse unser nächster Schritt ist die ISO 27001. Diese Zertifizierung ist ein Baukasten mit Tool Sets, denen man sich bedienen kann, und wenn man diese umsetzt, ist man Recht gut geschützt was Informationssicherheit und Datenschutz betrifft."

Experte 3 führte aus, dass es hier „[…] verschiedene Seiten gibt, einerseits die Cloud-Anbieter Ebene, wo gewisse Zertifizierungen gefordert sind, damit manche Branchen überhaupt in die Cloud wechseln können. Auf der anderen Seite gibt es Zertifizierungen für Unternehmen, wobei ich das hier eher als Leitfaden sehe, denn eine Zertifizierung bedeutet nicht immer, dass dieses Unternehmen auch sicher ist. Das hängt nämlich von der Umsetzung ab. Die ISO 27001 ist hier ein guter Start und dient als Leitfaden, die ISO 27002 erweitert die ISO 27001 in dem sie einen Leitfaden zur Umsetzung liefert."

Den großen Nutzen von Zertifizierungen sah Experte 4 dahingehend, dass „[…] man eine Vorgabe hat und man sich informieren muss. Bedeutet jedoch nicht, dass das Unternehmen sicher ist. Regelmäßige Audits helfen, da so aufgezeigt wird, ob das Unternehmen die Zertifizierung auch wirklich lebt."

Weiters wurde den Experten die Frage gestellt, welche Zertifikate Ihrer Meinung nach die größte Relevanz aufweisen.

Experte 1 meinte, es gäbe „[…] mehrere Zertifikate in diesem Bereich. Es gibt die verschiedensten ISO Normen für Datenzentren, ich glaube es ist wichtig, dass diese jene Zertifizierungen haben. Besonders die DIN EN 50600 ist für Datenzentren relevant. Wichtig in diesem Bereich ist auf jeden Fall die ISO 27001 Zertifizierung, die zwar generell international relevant, aber besonders in Europa sehr wichtig ist. In den USA ist noch SOC 2 Typ 2 sehr wichtig, auch wenn es nur ein Audit Report und keine echte Zertifizierung ist."

Der Meinung von Experte 1 stimmte auch die übrigen Experten zu. So schilderte Experte 2, „[…] die Kundenanforderung ist bei uns definitiv die ISO 27001 und aus den USA SOC 2 TYP 2." Auch Experte 3 und 4 sahen hier unisono ISO 27001 und SOC 2 Typ 2 als relevant an. So meinte Experte 3, „[..] die ISO 27001 ist hier ein guter Start, beziehungsweise ISO 27002 das noch etwas

ausführlicher auf die Umsetzung eingeht. Sonst gibt es noch sicherheitstechnisch die SOC 2 TYP 2 Zertifizierung, und recht viele Zertifizierungen für Datenzentren selbst, wobei ich jedoch die genauen Namen jetzt nicht parat habe.“ Auch Experte 4 fand, dass „[…] die ISO 27001 von den Kunden am meisten gewünscht ist und natürlich auch SOC 2 Typ 2. Es gibt auch noch Zertifizierungen direkt für Cloud-Anbieter, wobei ich die genaue Bezeichnung dafür jetzt nicht bei der Hand hätte.“

Weiters führte Experte 2 aus, dass es „[…] für die ISO 27001 noch TISAX gibt. Das ist eine Erweiterung für die Automobilindustrie. Und intern gibt es noch die ISO 9001.“

7 DISKUSSION

In diesem Kapitel werden die gewonnenen Informationen aus dem empirischen Teil entsprechend interpretiert, und die Forschungsfrage: „Welche Faktoren müssen Unternehmen beim Einsatz von Cloud-Computing prioritär behandeln, und welchen Einfluss haben diese auf eine erfolgreiche Transformation?“, sowie die zuvor aufgestellten Hypothesen, anhand der Erfahrungen und Meinungen der Experten und Expertinnen beantwortet.

7.1 Interpretation der Ergebnisse

In der Befragung legten die Experten und Expertinnen ihre Standpunkte nahe, anhand dieser Antworten werden die in Kapitel 1.2 aufgestellten Hypothesen bestätigt oder für ungültig erklärt. Anhand dieser wird schlussendlich die Forschungsfrage beantwortet.

7.1.1 Hypothese 1: Change-Management

Dieses Unterkapitel behandelt die H1 Hypothese: „Effektives Change-Management ist der wichtigste Faktor für eine erfolgreiche Transformation“ Zwei der vier befragten Experten gaben an, dass Change-Management der wichtigste Faktor bei der Transformation von Geschäftsprozessen in die Cloud sei. Für Experte 1 war es sogar einer der wichtigsten Komponenten, für Experte 2 war Changemanagement wichtig, es wurde jedoch keine Reihung in der Aussage getätigt. Es bestehen keine Aussagen, die diese Hypothese widerlegen und 50% der Befragten haben explizit Change-Management als wichtigste Komponente erwähnt, aus diesem Grund sieht der Autor dieser Arbeit die H1 Hypothese „Effektives Change-Management ist der wichtigste Faktor für eine erfolgreiche Transformation“ als bestätigt an.

7.1.2 Hypothese 2: Qualifikationen von Mitarbeitern

In diesem Kapitel wird die H1 Hypothese „Die benötigten Fähigkeiten und Qualifikationen von Mitarbeitern zu effektiver Cloud Nutzung unterscheiden sich deutlich von jenen traditioneller On-Premise-Lösungen“ genauer betrachtet und es wird anhand der Expertenmeinung entschieden, ob die Hypothese korrekt ist. Experte 3 und 4 waren der Meinung, dass es zu deutlichen Änderungen in den benötigten Fähigkeiten kommen wird, wenn mehr und mehr Cloud-Lösungen zum Einsatz kommen. Experte 1 gab Beispiele an, in welchen verdeutlicht wurde, dass andere Fähigkeiten benötigt wurden. Im Gegensatz dazu gab Experte 2 an, dass nur Techniker neue Fähigkeiten benötigen. Alle Experten haben in ihren Interviews also dargelegt, dass es Unterschiede

gibt. Hierbei zeigten 75% deutliche Unterschiede auf, und keiner der Experten bestätigte die Gegenhypothese. Daraus abgeleitet wird die H1 Hypothese als bestätigt angesehen.

7.1.3 Hypothese 3: Freigabeprozesse und Servicekatalog

In diesem Unterkapiteln wurden die Experten zur Veränderung der Freigabeprozesse bei Cloud Lösungen befragt. Es wurde dazu bewusst in der gestellten Frage der eigentliche Servicekatalog nicht erwähnt, um die Meinung der Experten nicht vorab zu beeinflussen. Daher wurde, sofern notwendig, der Servicekatalog in einer nachgestellten Frage erörtert. Experte 2 konnte zu diesem Thema keine Antwort geben, jedoch waren die restlichen Experten einig, dass Freigabeprozesse in der Cloud umso wichtiger sind, und es auch zu einer Verschiebung hin zu vermehrten Servicekatalogen kommt. Aus den genannten Gründen ist die Hypothese H1 „Cloud ermöglicht Veränderung von Freigabeprozessen hin zu Servicekatalogen“ als bestätigt anzusehen.

7.1.4 Hypothese 4: IT-Teams

In diesem Abschnitt werden die Meinungen der Experten mit der H1 und H0 Hypothese zum Thema Reduzierung der IT-Teams verglichen. Aus der Erfahrung von 3 der 4 Experten reduzieren sich IT-Teams aufgrund von Cloud-Computing-Lösungen. Experte 2 war der Meinung, dass sich die Mitarbeiterzahl in der Theorie reduzieren müsste. Aufgrund des Unternehmenswachstums konnte er dies jedoch nicht durch Praxiswissen bestätigen. Dennoch geben 75% an, dass es zu einer Reduktion kommt. Auch die Aussage von Experten 2 weist eine entsprechende Tendenz auf. Daher ist die Hypothese H1: „Cloudcomputing reduziert die Größe von IT-Teams“ aus Sicht des Autors bestätigt.

7.1.5 Hypothese 5: Einflussfaktoren

In diesem Abschnitt wird versucht, die Hypothese H1 „Cybersecurity stellt die größte nicht-organisatorische Herausforderung dar“ oder ihre Gegenhypothese H0 „Cybersecurity stellt eine vernachlässigbare nicht-organisatorische Herausforderung dar“ zu bestätigen. Experte 4 erwähnte die Sicherheit als einer der prioritär zu berücksichtigten Einflussfaktoren. Diesem Thema konnte auch die Meinungen von Experte 1 und 3 zugeordnet werden. Experte 3 fand dabei, dass neben Cybersecurity auch Changemanagement der wichtigste zukünftige Faktor sein wird. Daraus lässt sich schließen, dass die Berücksichtigung der Cybersecurity für eine erfolgreiche Transformation wichtig ist. Die Gegenhypothese H0 kann somit nicht bestätigt werden, da 75% der Experten Cybersecurity als einer der wichtigsten Einflussfaktoren anerkannten. Experte 2 erwähnte hier zusätzlich noch die Kosten, die jedoch eine nicht-organisatorische Herausforderung darstellen, und ist der Einzige mit dieser Meinung. Experten 1, 3 und 4 nannten neben der Cybersecurity

zwar auch das Change-Management, dies stellt jedoch eine organisatorische Herausforderung dar. Aus diesem Grund gilt die Hypothese H1 als bestätigt.

7.1.6 Hypothese 6: Cybersecurity

In diesem Kapitel wird die letzte der in dieser Arbeit angeführten Hypothesen bearbeitet. Hierbei wurde die Hypothese, dass die Reaktionszeiten auf Sicherheitslücken zwischen On-Premise- und Cloud-Lösungen unterschiedlich sind, untersucht. Die Antworten der Experten zu dieser Frage waren sehr deutlich. 100% der Experten gaben an, dass Cloud-Lösungen deutlich schneller auf Sicherheitslücken reagieren. Aus diesem Grund gilt die Hypothese H1 „Mittels Cloud-Computing wird schneller auf Sicherheitslücken reagiert als bei traditionellen On-Premise-Lösungen“ als bestätigt.

7.2 Forschungsfrage

Schlussendlich muss noch die Forschungsfrage: „Welche Faktoren müssen Unternehmen beim Einsatz von Cloud-Computing prioritär behandeln, und welchen Einfluss haben diese auf eine erfolgreiche Transformation?“ beantwortet werden. Die Beantwortung dieser Frage gliedert sich in zwei Teile. Die Aufzählung der von den Experten angesprochenen Faktoren, und der damit verbundene Einfluss auf eine erfolgreiche Transformation. Folgende Faktoren wurden von den Experten prioritär adressiert:

- Change-Management
- Kosten
- Technik
- Rechtliche Aspekte
- Cybersecurity

Hierbei ist anzumerken, dass die Experten Change-Management und Cybersecurity als die wichtigsten Faktoren sahen. Dies lässt sich auch durch die Hypothesen in Kapitel 7.1.1 und 7.1.5 bestätigen. Um eine erfolgreiche Migration in die Cloud durchzuführen, sind diese Aspekte daher prioritär zu adressieren. Die Befragung der Experten zeigte, dass dem Faktor Change-Management vor allem mit effektivem und effizientem Projektmanagement begegnet werden kann, und auch Managementkonzepte eine wichtige Rolle spielen. Diese beiden Elemente sind unabdingbar, um aktiv eine Steuerung vorzunehmen. Im Bereich der Cybersecurity kann mit Zertifikaten ein gewisses Maß an Grundsicherheit gewährleistet werden, da hier zur Erreichung der Zertifizierung ein Mindestmaß erfüllt sein muss, und die entsprechenden Standards einen Leitfaden für

eine erfolgreiche Umsetzung liefern. Allerdings hat sich auch gezeigt, dass Zertifikaten nicht uneingeschränkt vertraut werden kann. Eine erfolgreiche Zertifizierung hält nämlich nur eine Überprüfung zu einem gewissen Zeitpunkt fest, und zeigt nicht, dass die entsprechenden Regularien und Vorgaben auch dauerhaft eingehalten werden. Nur wenn die Prozesse und Sicherheitsvorkehrungen im Unternehmen auch gelebt werden, kann effektive Cybersecurity betrieben werden.

8 ZUSAMMENFASSUNG

Im letzten Kapitel werden die Erkenntnisse der Arbeit noch einmal zusammengefasst. Des Weiteren wird kurz auf die Limitierungen dieser wissenschaftlichen Arbeit eingegangen, um die Aussagekraft der Arbeit zu erörtern.

8.1 Schlussfolgerungen

Das Ziel der vorliegenden wissenschaftlichen Arbeit war es, jene Faktoren zu ermitteln, die für den erfolgreichen Einsatz von Cloud-Computing in Unternehmen als größte Herausforderungen gelten, und wie diese prioritär behandelt werden müssen.

Des Weiteren sollten die grundlegenden Aspekte der Transformation beschrieben werden, um eine grundlegende Basis für Verantwortliche zu legen, die eine Cloud-Migration anstreben. Hierzu wurde die Forschungsfrage: „Welche Faktoren müssen Unternehmen beim Einsatz von Cloud-Computing prioritär behandeln, und welchen Einfluss haben diese auf eine erfolgreiche Transformation?“ anhand qualitativer Experteninterviews beantwortet. Trotz andauernder Covid-19-Krise und den damit verbunden Lockdowns haben sich vier Experten bereit erklärt, ein persönliches Interview zu führen. Anhand ihres Wissensschatzes wurden die zuvor aufgestellten Hypothesen beantwortet. Daraus abgeleitet lassen sich folgende Hypothesen als bestätigt ansehen:

(1) Effektives Change-Management ist der wichtigste Faktor für eine erfolgreiche Transformation.

(2) Die benötigten Fähigkeiten und Qualifikationen von Mitarbeitern zu effektiver Cloud-Nutzung unterscheiden sich deutlich von jenen traditioneller On-Premise-Lösungen.

(3) Cloud ermöglicht eine Veränderung von Freigabeprozessen hin zu Servicekatalogen.
(4) Cloudcomputing reduziert die Größe von IT-Teams.
(5) Cybersecurity stellt die größte nicht-organisatorische Herausforderung dar.
(6) Mittels Cloud-Computing wird schneller auf Sicherheitslücken reagiert als bei traditionellen On-Premise-Lösungen.

Aufgrund des technologischen Fortschrittes und der damit verbunden Änderungen der Prozesse, ist die Einführung von Cloud-Lösungen oft besonders für kleine Unternehmen schwer zu bewerkstelligen. Diese Arbeit stellt daher eine Sammlung der aktuellen Technologien und der Expertenerfahrungen dar, und soll so Unternehmen in den Anfangsstadien einer Cloud-Transformation unterstützen.

8.2 Limitierungen

Aufgrund der Covid-19-Pandemie und dem damit verordneten Lockdown wurde die Anzahl der geplanten Experten auf vier verringert. Um eine höhere Aussagekraft zu bewerkstelligen, sollte für die weitere Forschung die Anzahl der Experten erhöht werden. Die Erkenntnisse dieser Arbeit können auch genutzt werden, um eine quantitative Befragung durchzuführen. Weiters stammen alle befragten Experten aus dem DACH-Raum, was die Reichweite der Aussagen in dieser Arbeit vermindert. Für weitere Befragungen sollten globale Experten ihr Wissen teilen, um überprüfen zu können, ob den gewonnenen Erkenntnissen globale Aussagekraft zukommt.

ABKÜRZUNGSVERZEICHNIS

AWS	Amazon Web Services
BI	Business-Intelligence
COBOL	Common Business-Oriented Language
CPU	Central Processing Unit
CSP	Cloud-Service-Provider
DDoS	Distributed Denial-of-Service
DoS	Denial of Service
EDoS	*Economical Denial of Sustainability*
GB	Gigabyte
GCP	Google Cloud Plattform
ggf.	*gegebenenfalls*
HTTPS	*HyperText Transfer Protocol Secure*
I&O	*Infrastructure and Operations*
IaaS	Infrastructure-as-a-Service
ITSM	*IT-Service-Management*
KMU	*Klein- und Mittelbetriebe*
NIST	*National Institute of Standards and Technology*
ONTAP	Open Network Technology for Appliance Products
PaaS	Platform-as-a-Service
PAYG	*PAY-as-You-Go*
PDoS	Permanent Denial of Service
SaaS	Software-as-a-Service
SLAs	Service Level Agreements
SSL	*Secure Sockets Layer*
u.a.	*unter anderem*
VM	Virtual Machine
VMM	Virtual-Machine-Monitor
XaaS	Anything-as-a-Service
z.B.	*zum Beispiel*

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Amazon Web Services. (März 2018). AWS Migration Whitepaper. Abgerufen am 10. Juli 2021 von https://d1.awsstatic.com/whitepapers/Migration/aws-migration-whitepaper.pdf

Amazon Web Services. (2021). *AWS Best Practices for DDoS Resiliency.* Amazon Web Services.

Atmosera. (25. Oktober 2021). *Atmosera*. Abgerufen am 25. Oktober 2021 von https://www.atmosera.com/resources/glossary/azure/

Baig, A. (09. Juli 2021). *GlobalSign*. Abgerufen am 9. Dezember 2021 von https://www.globalsign.com/en/blog/session-hijacking-and-how-to-prevent-it

Balasubramanian, R., & Aramudhan, M. (13. Oktober 2012). Security Issues: Public vs Private vs Hybrid. *International Journal of Computer Application*, S. 35-41.

Bortz, J., & Döring, N. (2016). *Forschungsmethoden und Evaluation in den Sozial- und Human-wissenschaften.* Heidelberg: Springer Verlag.

Brown, L. (16. Mai 2016). *ITProPortal*. Abgerufen am 30. August 2021 von https://www.itproportal.com/2016/05/16/four-steps-to-protect-against-cloud-account-hijacking/

Canalys. (2. Februar 2021). *Canalys*. Abgerufen am 12. Dezember 2021 von https://www.canalys.com/newsroom/global-cloud-market-q4-2020

Chowdhury, F. Z., Kiah, L. B., Ahsan, M., & Idris, M. Y. (2017). Economic denial of sustainability (EDoS) mitigation approaches in cloud: Analysis and open challenges. Palembang: IEEE.

Comer, D. E. (2021). *The Cloud Computing Book: The Future Of Computing Explained.* Boca Raton: CRC Press.

Disterer, G. (April 2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, S. 92-100.

Fellows, W. (2008). *Partly Cloudy – Blue-Sky Thinking About Cloud Computing.* 451Group.

Gleb, T. (2021). *Systematic Cloud Migration - A Hands-On Guide to Architecture, Design, and Technical Implementation.* Berkeley, CA: Apress.

GoCloud. (2021). *GoCloud*. Abgerufen am 17. 10 2021 von https://www.gocloud.co.uk/glossary/thin-client-vs-thick-client-the-pros-and-cons

Gordon, D. G. (2016). Legal Aspects of Cloud Computing. In S. Murugesan, & I. Bojanova, *Encyclopedia of Cloud Computing.* John Wiley & Sons, Ltd.

Gowrie, C. (2014). *Session Hijacking and the Cloud.*

Goyal, S. (3. Februar 2014). Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *I.J. Computer Network and Information Security*, S. 20-29.

Grand View Research. (2020). *Cloud Computing Market Size, Share & Trends Analysis Report By Service (SaaS, PaaS, IaaS), By Workload, By Deployment, By Enterprise Size, By End-use, By Region, And Segment Forecasts, 2020 - 2027.* Grand View Research.

IDG. (2020). IDG Cloud Computing Survey.

INAP. (21. Juni 2017). *INAP*. Abgerufen am 16. Oktober 2021 von INAP: https://www.inap.com/blog/what-is-managed-hosting/

IONOS. (23. September 2020). *IONOS*. Abgerufen am 16. Oktober 2021 von IONOS: https://www.ionos.at/digitalguide/server/knowhow/was-ist-on-premises/

Jackson, B. (11. März 2021). *Kinsta*. Abgerufen am 25. 10 2021 von https://kinsta.com/blog/google-cloud-hosting/

Jin, H., Ibreahim, S., Bell, T., Gao, W., Huang, D., & Wu, S. (2010). Cloud Types and Services. In *Handbook of Cloud Computing* (S. 335-355). Boston: Springer.

Lisdorf, A. (2021). *Cloud Computing Basics A Non-Technical Introduction.* New York City: Apress.

Lorido-Botran, T., Miguel-Alonso, J., & Lozano, J. A. (Dezember 2014). A Review of Auto-scaling Techniques for Elastic. *Journal of Grid Computing*, S. 559–592.

Lynn, T., Mooney, J. G., van der Werff, L., & Fox, G. (2021). Data Privacy and Trust in Cloud Computing - Building trust in the cloud through assurance and accountability. In P. Macmillan, *Palgrave Studies in Digital Business & Enabling Technologies.* Cham: Palgrave Macmillan.

Lynn, T., Mooney, J., Lee, B., & Endo, P. (2020). The Cloud-to-Thing Continuum - Opportunities and Challenges in Cloud, Fog and Edge Computing. In P. Macmillan, *Palgrave Studies in Digital Business & Enabling.* Cham: Palgrave Macmillan.

Lynn, T., Mooney, J., Rosati, P., & Fox, G. (2020). Measuring the Business Value of Cloud Computing. In P. Macmillan, *Palgrave Studies in Digital Business & Enabling Technologies.* Cham: Palgrave Macmillan.

Mangus, Q. (09. 10 2019). *Micro Focus Blog*. Abgerufen am 20. 06 2021 von Micro Focus: https://blog.microfocus.com/cobol-is-60/

Manvi, S., & Shyam, G. K. (2021). *Cloud Computing Concepts and Techlologies.* Boca Raton: CRC Press.

MarketsAndMarkets. (2021). *Cloud Computing Market by Service Model (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), Deployment Model (Public and Private), Organization Size, Vertical, and Region - Global Forecast to 2026.* Markets and Markets.

Marquez, E. (8. Dezember 2021). *Concurrency Labs*. Abgerufen am 12. Dezember 2021 von https://www.concurrencylabs.com/blog/choose-your-aws-region-wisely/

Mayring, P. (2015). *Qualitative Inhaltsanalyse.* Weinheim: Beltz Verlag.

Mayring, P. (2016). *Einführung in die qualitative Sozialforschung.* Weinheim: Beltz Verlag.

McHaney, R. (2021). *Cloud Technologies - An Overview of Cloud Computing Technologies for Managers.* New Jersey: John Wiley & Sons, Ltd.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology.* Abgerufen am 25. März 2021 von https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NetApp. (25. Juli 2019). *NetApp*. Abgerufen am 25. Oktober 2021 von https://cloud.netapp.com/blog/aws-migration-strategy-the-6-rs-in-depth

NIST. (2011). *Guide for Security-Focused Configuration Management of Information Systems.*

Nunn, A. (27. Jänner 2021). *Auth0*. Abgerufen am 12. Dezember 2021 von https://auth0.com/blog/what-is-iso-27018-2019-everything-executives-need-to-know/

Ozer, Y. (1. August 2018). *Revolgy*. Abgerufen am 11. Dezember 2021 von https://www.revolgy.com/insights/blog/customising-virtual-machines

Passmore, E. (2016). *Migrating Large-Scale Services to the Cloud.* Berkeley, CA: Apress.

Potluri, S., Rao, K., & Moh, S. (2021). *Cloud Security - Techniques and Applications.* Berlin/Boston: Walter de Gruyter GmbH.

Radware. (2016). *On-Demand, Always-on, or Hybrid? Choosing an Optimal Solution for DDoS Protection.*

Radware. (2017). *Global Application & Network Security Report.*

Rangwani, D., & Om, H. (2021). A Secure User Authentication Protocol Based on ECC for Cloud Computing Environment. *Arabian Journal for Science and Engineering*, S. 3865-3888.

REHMAN, T. B. (2019). *Cloud Computing Basics.* Dulles: MERCURY LEARNING AND INFORMATION.

Richard, K. (2013). *Glossary of Key Information Security Terms.*

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud Computing Implementation, Management, and Security.* Boca Raton: CRC Press.

Rountree, D., & Castrillo, I. (2014). *The Basics of Cloud Computing.* Waltham: Syngress Publishing.

RSI Security. (5. Juni 2019). *RSI Security*. Abgerufen am 5. Dezember 2021 von https://blog.rsisecurity.com/soc-2-type-1-vs-type-2-whats-the-difference/

Sage, A. (3. Februar 2021). *Cloudsoft*. Abgerufen am 25. Oktober 2021 von https://cloudsoft.io/blog/cloud-migration-strategies-5-repurchase

Schouten, E. (12. September 2012). *IBM*. Von https://www.ibm.com/blogs/cloud-computing/2012/09/12/rapid-elasticity-and-the-cloud/ abgerufen

Sehgal, N., Bhatt, P., & Acken, J. (2020). *Cloud Computing with Security - Concepts and Practices.* Cham: Springer.

Selzer, A. (2020). *Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit.* Wiesbaden: Springer Vieweg.

Srinivasan, S. (2014). *Cloud Computing Basics.* New York: Springer.

Surianarayanan, C., & Pethuru, R. (2019). *Essentials of Cloud Computing.* Cham: Springer Nature Switzerland.