HAW HAMBURG

MASTERTHESIS
Flah-Uddin Ahmad

Realisierung einer Landing Zone in Amazon Web Services zur Steuerung einer sicheren Umgebung in der Cloud

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Flah-Uddin Ahmad

Realisierung einer Landing Zone in Amazon Web Services zur Steuerung einer sicheren Umgebung in der Cloud

Masterarbeit eingereicht im Rahmen der Masterprüfung
im Studiengang *Master of Science Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Stefan Sarstedt
Zweitgutachter: Prof. Dr. Marina Tropmann-Frick

Eingereicht am: 02.08.2022

Flah-Uddin Ahmad

Thema der Arbeit

Realisierung einer Landing Zone in Amazon Web Services zur Steuerung einer sicheren Umgebung in der Cloud

Stichworte

Cloud Computing, Account-Management, Cloud Governance, Infrastructure as Code, Landing Zone, Cloud Adoption Framework, Amazon Web Services

Kurzzusammenfassung

Die IT hat in den vergangenen Jahren einen starken Wandel durchlebt und beeinflusst viele Bereiche des alltäglichen Lebens. Unternehmen verlagern ihre Aktivitäten immer mehr in die digitale Welt und die Cloud. Diese Arbeit zielt darauf ab, die Technologie des Cloud Computing näher zu beleuchten, und herauszufiltern, wie der größte Nutzen aus der Technik gezogen werden kann. Schlussendlich soll die Entwicklung einer zentralen Account-Management Lösung vorgestellt werden.

Flah-Uddin Ahmad

Title of Thesis

Realization of a Landing Zone in Amazon Web Services for managing a safe environment in the cloud

Keywords

Cloud Computing, Account-Management, Cloud Governance, Infrastructure as Code, Landing Zone, Cloud Adoption Framework, Amazon Web Services

Abstract

IT has undergone major changes in the past few years and influences everyday life nowadays. Companies are increasingly shifting their activities to the cloud. This thesis aims to shed more light on cloud computing and to show how to get the most benefit from the technology. Finally, the development of a central account management solution will be presented.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Zu Beginn dieser Arbeit soll der Kontext sowie die Relevanz des Themas Cloud Computing aufgezeigt werden. Darüber hinaus soll die persönliche Motivation, die Fragestellung und auch das angestrebte Ziel dieser Ausarbeitung verdeutlicht werden.

1.1 Kontext und Motivation

Die Informations- und Kommunikationstechnologie hat in den vergangenen Jahren einen steilen Wandel durchlebt und übt einen großen Einfluss auf fast alle Bereiche des alltäglichen Lebens aus. Unternehmen und auch Privatpersonen verlagern ihre Aktivitäten immer mehr in die digitale Welt. Durch die rasante Zunahme der Digitalisierung im Alltag entstehen neue und größere Anforderungen an Informationssysteme. Der Bedarf an Rechenleistung und Speicherkapazität steigt parallel dazu an. Die manuelle Installation und Konfiguration von IT-Infrastruktur ist ein sehr zeitaufwendiger Prozess und auch die Wartung und Instandhaltung der Infrastruktur stellt Unternehmen immer wieder vor Herausforderungen. Der Markt schreit förmlich nach neuen Möglichkeiten, um all diese Prozesse schneller, strukturierter und konsistenter umzusetzen. Cloud Computing bietet hierfür einen möglichen Lösungsansatz. Die Nutzung von Cloud ist heutzutage für viele Unternehmen nicht mehr nur eine gute Alternative zur statischen IT-Infrastruktur, sie ist vielmehr zu einer obligatorischen Gegebenheit geworden. Zumindest dann, wenn man als Unternehmen konkurrenzfähig bleiben möchte, sich voll und ganz auf das Hauptgeschäft fokussieren möchte und gleichermaßen unnötige IT-Kosten und Managementverantwortlichkeiten vermeiden will. IT-Ressourcen, die nicht zur Neige gehen und auf Abruf bereitgestellt werden klingen an dieser Stelle überaus attraktiv und bilden für Unternehmen eine flexible und skalierbare Soft- und Hardwareinfrastruktur. Die Cloud ist in aller Munde – aber, was steckt dahinter? Und wie kann der größte Nutzen aus der Technik gezogen werden? Dieser und mehr Fragestellungen soll in dieser Arbeit Beachtung geschenkt

werden. Zu Beginn soll sich mit der Cloud im Allgemeinen beschäftigt werden, ehe es einen vertiefenden Einblick in die verschiedenen Service- und Liefermodelle der Cloud gibt. Anschließend werden die Chancen und Risiken von Cloud Computing ausgearbeitet und es wird ein Blick auf die Sicherheitsfragen von Cloud geworfen. Danach folgt ein Einstieg in das Thema Landing Zone in der Cloud. Abschließend steht die Entwicklung einer zentralen Account Management Lösung, basierend auf AWS Organizations, im Fokus der Arbeit.

1.2 Fragestellung und Zielsetzung

In meiner Masterarbeit möchte ich mich mit Cloud Computing beschäftigen. Hierbei sollen unter anderem die Optimierungsmöglichkeiten durch die Cloud beleuchtet werden. Diese werden durch einen Blick auf die vielfältigen Möglichkeiten in der Cloud verdeutlicht. Gerne würde ich dabei sowohl auf die Kostenoptimierung als auch auf die Effizienzsteigerung für Unternehmen durch die Nutzung von Cloud Technologien eingehen. Im praktischen Teil meiner Arbeit soll eine zentrale Account Management Lösung entwickelt werden, die auf einer Serverless Architektur basiert und über APIs konsumiert werden kann. Durch ein zentrales Management können alle Accounts einer Organisation an einem Ort gemanaged werden Accounts können gruppiert und Hierarchien abgebildet werden. Regeln für die Nutzung der Accounts können auf Accountgruppen oder einzelne Accounts angewandt werden. Die Einführung von Cloud in Unternehmen ist komplex und zeitaufwendig. Dadurch rücken die vielen Vorteile, die Cloud Computing mit sich bringt, oft in den Hintergrund. Es gibt viele Fragen aus verschiedenen Perspektiven, die beantwortet werden müssen. Die Einrichtung einer Multi Account Landing Zone kann Governance, Compliance, Security und vieles mehr für Unternehmen vereinfachen. Durch klar definierte Grenzen und Verantwortlichkeiten für Identitäten und Dienste, können Unternehmen sich auf ihr jeweiliges Kerngeschäft konzentrieren. Ziel dieser Arbeit ist es, sich dem Thema Landing Zone anzunähern und als Anfang eine zentrale Account Management Lösung auszuarbeiten. Um dieses Ziel zu erreichen, soll sich an den folgenden Fragestellungen orientiert werden:

- Wie wird Cloud in Unternehmen gemanaged und strukturiert?
- Welche Potenziale und Hindernisse birgt der Einsatz der Cloud für Unternehmen?
- Wie kann die Cloud Technologie effizient und gewinnbringend in Unternehmen eingesetzt werden?
- Wie kann mit einer zentralen Account Management Lösung ein Mehrwert für die Nutzer von Cloud Services erreicht werden?
- Wie kann eine Landing Zone in der Cloud aussehen?
- Welche Vorteile bringt eine Landing Zone für die Cloud?
- Wie kann eine Landing Zone dazu beitragen, dass die Sicherheit in der Cloud erhöht wird?
- Wie kann eine Landing Zone dazu beitragen, dass Compliance Richtlinien eingehalten werden?

An dieser Stelle soll noch erwähnt werden, dass in dieser Arbeit einige englischsprachige Begriffe ohne Übersetzung verwendet werden. Viele Begriffe werden in der IT nicht mehr ins Deutsche übersetzt und der englische Gebrauch hat sich auch in Deutschland durchgesetzt. Um dem realitätsnahen Sprachgebrauch nachzukommen, wird daher in dieser Arbeit von überflüssigen Übersetzungen abgesehen.

2 Einführung Cloud Computing

In den folgenden Abschnitten erfolgt ein thematischer Einstieg in die Technologie des Cloud Computing. Dazu dient zunächst eine Begriffsklärung, ehe auf die Anwendungsbereiche, den geschichtlichen Hintergrund, die aktuellen Tendenzen sowie die Schlüsselcharakteristika von Cloud Computing eingegangen wird.

2.1 Begriffliche Annäherung

In der aktuellen Forschung ist man sich einig, dass es bislang noch keine allgemeingültige Definition für Cloud Computing gibt. Es wird sich an dieser Stelle oftmals an dem Definitionsversuch des National Institute of Standards and Technology (NIST) aus dem Jahr 2011 bedient:

> *„Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.“* (Mell et. al., 2011, p. 2)

Das NIST bezeichnet Cloud Computing also als ein Modell, welches über ein Netzwerk einen komfortablen Zugriff auf einen Ressourcenpool ermöglicht. Zu diesen Ressourcen gehören Netzwerk, Speicherkapazität, Rechenleistung, Anwendungen und weitere Dienste. Die Haupteigenschaft aller Ressourcen ist, dass sie ohne direkte Interaktion zwischen Anbieter und Kunden an den tatsächlichen Bedarf angepasst werden und jederzeit verfügbar sind.

Hentschel et. al. nutzen für die begriffliche Definition darüber hinaus die verschiedenen Ebenen, auf denen die Cloud Anwendung findet. Auf technischer Ebene stehe Cloud im

Zusammenhang mit der Virtualisierung von Hardware, virtuellen Rechenzentren und den Service Ebenen des Cloud Computing (siehe Abschnitt 3): Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Wirtschaftlich betrachtet könne Cloud Computing als spezielle Form des Outsourcings von IT-basierten Funktionen bezeichnet werden. Hierbei erfolge der Betrieb und die Wartung der jeweiligen Dienste durch spezialisierte Drittanbieter (Hentschel et. al., 2018).

Weitere begriffliche Annäherungen arbeiten meist mit den typischen Charakteristika der Cloud. So zum Beispiel hier:

> *„Cloud Computing selbst stellt eine Ansammlung von Diensten, Anwendungen & Ressourcen dar, die dem Nutzer flexibel und skalierbar über das Internet angeboten werden, ohne eine langfristige Kapitalbindung und IT-spezifisches Know-how vorauszusetzen.“* (Repschläger et. al., 2014, p. 6).

Es handele sich bei der Cloud um eine IT-Technologie, bei der der Kunde keinerlei Wartungsarbeiten auf sich nehmen müsse, da der gesamte Betrieb vom Anbieter verwaltet werde. Der Kunde mietet eine Leistung an und zahlt diese seinem Verbrauch entsprechend ab. Der Kunde kann meist zwischen verschiedenen Modellen wählen und so beispielsweise entscheiden, ob er den Service einer kompletten Softwareanwendung beziehen möchte oder lediglich die oberflächige IT-Infrastruktur nutzen will (Repschläger et. al., 2014).

Cloud Computing kann also als ein Modell beschrieben werden, durch welches dynamische, flexible und skalierbare Ressourcen und Services über ein Netzwerk als Service an den Kunden ausgeliefert werden.

2.2 Anwendungsgebiete

Cloud Computing findet sowohl in der globalen Wirtschaft als auch im behördlichen und privaten Sektor Anwendung. Eine Umfrage aus dem Jahre 2010 habe ergeben, dass bereits dreiviertel aller Unternehmen die Cloud nutzen. Diese Zahl dürfte bis heute weiter angestiegen sein (siehe Abschnitt 2.4). Neben Unternehmen wird Cloud Computing auch im E-Commerce in der Agrarkultur, der Nuklearwissenschaft oder dem Gesundheitswesen genutzt. Auch beispielsweise die US-Regierung nutze die Cloud, um die bisherigen jährlichen Ausgaben von 76

Mrd. Dollar (Stand 2010) für IT zu reduzieren. Aus ökonomischer Sicht befähigt das Cloud Computing Unternehmen und Organisationen dazu, große Einsparungen dadurch einzufahren, dass sie nicht für ungenutzte und begrenzte Ressourcen zahlen müssen. Dies ist im Vergleich zu der Verwendung von traditioneller IT-Technologie der Fall. Neben den Verbesserungen für Unternehmen ist Cloud Computing auch dazu in der Lage, das private Sozialleben zu verändern. So hat beispielsweise das Arbeiten mit sozialen Netzwerken die Kommunikationslücke gefüllt und hilft Nutzern dabei, sich nahtlos über die Cloud miteinander zu verbinden. Darüber hinaus erlaubt die Cloud den Nutzern, Fotos, Videos und andere Dateien unkompliziert zu versenden oder beispielsweise das Downloaden und Updaten von mobilen Applikationen auf Smartphones. Auch Spielprozesse werden mithilfe der Cloud in Echtzeit abgebildet. So wird ermöglicht, dass Nutzer über verschiedenste Endgeräte hochauflösende Onlinespiele gegen reale andere Gegner spielen können (Khan, 2014).

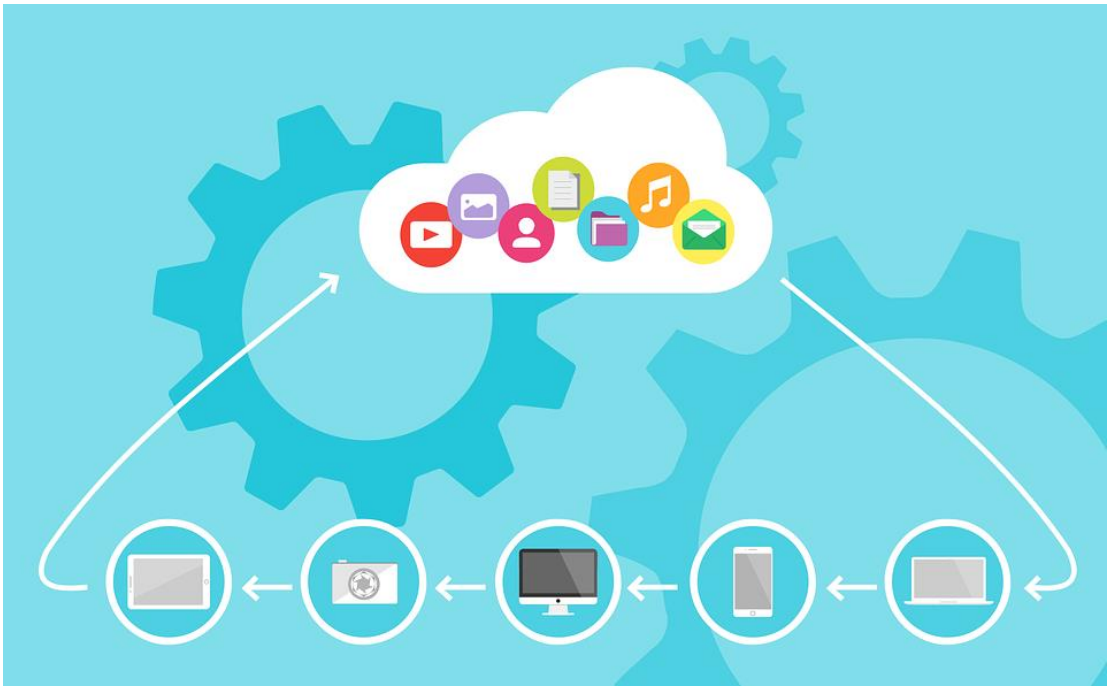

Abbildung 1: Cloud Computing Anwendungsgebiete

Barton geht in seinem Buch *„E-Business mit Cloud Computing. Grundlagen – Praktische Anwendungen – verständliche Lösungsansätze“* detailliert auf die Verbindung zwischen Cloud Computing und E-Business ein. E-Business stehe demnach in engem Zusammenhang mit

Cloud Computing. E-Business dient als Abkürzung für Electronic Business. Der Ursprung des Begriffs liegt in einer Werbekampagne der Firma IBM aus dem Jahre 1997. Die Kombination der beiden Wörter „Electronic“ und „Business“ sollte damals verdeutlichen, dass der Gebrauch des Internets die Art, wie Unternehmen arbeiten, beeinflussen wird. E-Business steht für einen Leistungsaustausch zwischen Marktteilnehmern, um eine Wertschöpfung zu erzielen oder, um eine Gesellschaft anhand von Informations- und Kommunikationstechnologien zu organisieren. Die Marktteilnehmer lassen sich Barton zufolge in drei Gruppen zusammenfassen: Business (B): Unternehmen; Consumer (C): Konsumenten beziehungsweise Bürger sowie Administration (A): andere Organisationen (non-profit), wie zum Beispiel öffentliche Verwaltungen. Alle drei Gruppen von Teilnehmern können am Markt sowohl als Leistungsanbieter als auch als Leistungsabnehmer fungieren. Daraus ergeben sich neun verschiedene Arten des Leistungsaustauschs, die in Abbildung 1 dargestellt werden (Barton, 2014):

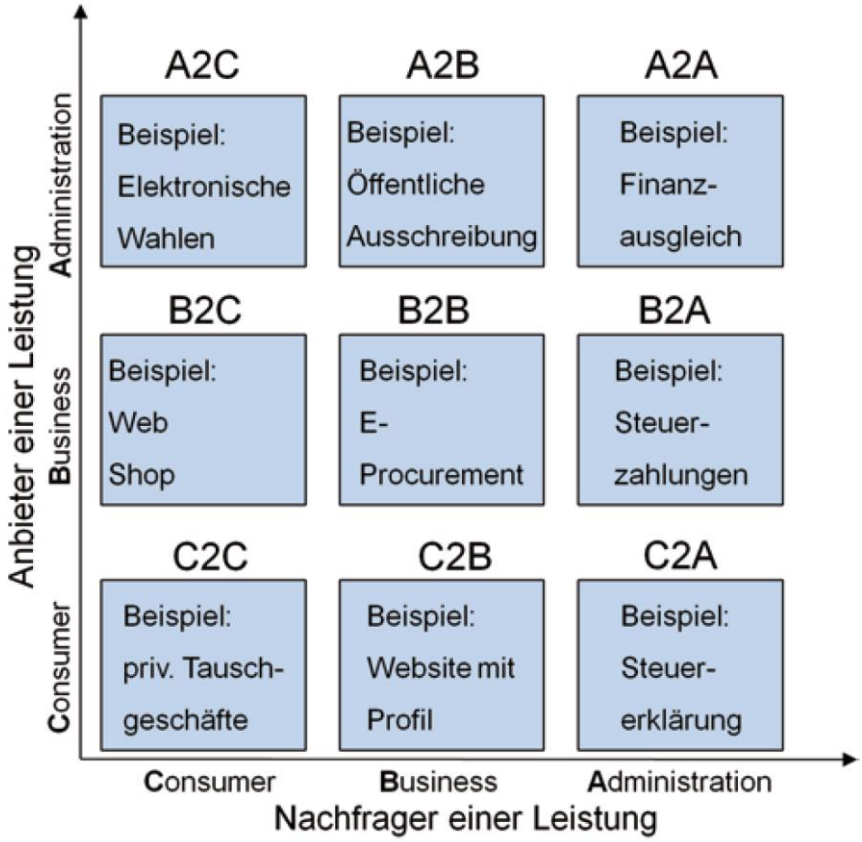

Abbildung 2: Leistungsarten E-Business

Bietet ein Unternehmen (B) eine Leistung für Konsumenten (C) an, so wird diese Geschäftsbezeichnung als B2C (Business-to-Consumer) bezeichnet. Diese Art der Geschäftsbeziehung sowie die B2B (Business-to-Business) Variante gehören zu dem Bereich E-Commerce. Geschäftsbeziehungen der Art A2C (Administration-to-Consumer), A2B (Administration-to-Business) und A2A (Administration-to-Administration) fallen in den Bereich des E-Government. E-Commerce und E-Government sind jeweils als Unterkategorien des E-Business zu klassifizieren. Zu Beginn stand im Rahmen des E-Business die Nutzung von unternehmensinternen Systemen und die Ausführung von Geschäftsprozessen mithilfe eines Webbrowsers im Vordergrund. Heutzutage umfasst es darüber hinaus aber auch beispielsweise die Nutzung von Anwendungen auf mobilen Endgeräten. Im weiteren Verlauf geht Barton noch auf einige Praxisbeispiele zum Einsatz von Services in Cloud Computing und E-Business ein. Die Internetplattform YouTube kann beispielsweise dafür genutzt werden, um für Produkte oder Dienstleistungen im Bereich B2C oder A2C zu werben. Hierbei wird ein YouTube Video in eine Website eingebettet. Über den Kurznachrichtendienst Twitter lassen sich kurze Informationen Einzelner (C2C) oder von Unternehmen (B2C) beziehungsweise anderen Organisationen (A2C) versenden. Für die Versendung der Nachrichten stellt Twitter den Programmcode zur Verfügung, um die abgesetzte Nachricht (Tweet) in eine Website mithilfe von JavaScript einzubetten. Ein weiteres Beispiel bietet der Simple Storage Service (S3) von AWS. Er dient der Datenspeicherung und verwandelt Dateien aus einem Massenspeicher in sogenannte Buckets. Um AWS S3 nutzen zu können, müssen sich Kunden registrieren. Im Anschluss daran wird dann ein Bucket erstellt. Um den Bucket verwalten zu können, steht eine grafische Benutzeroberfläche (AWS Konsole) zur Verfügung. Der Besitzer des Buckets erhält automatisch die Berechtigung, auf die im Bucket gespeicherten Dateien zuzugreifen, sie herunterzuladen oder anzupassen. Darüber hinaus kann er diese Berechtigung auch für andere Nutzer einrichten. Die Nutzung von AWS S3 ist zunächst kostenlos, es müssen aber einige Bedingungen dafür erfüllt werden. So sind beispielsweise die Größe des Datenspeichers und die Datenmenge für ausgehende Daten begrenzt. Wenn die Nutzung über diese Einschränkungen hinausgeht, entstehen für den Kunden Kosten, die monatlich berechnet werden (Barton, 2014).

2.3 Historie

Cloud Computing baut teils auf bereits existierenden IT-Technologien auf. Aus diesem Grund ist es besonders schwierig, den genauen Ursprung der Cloud Technologie zu benennen. So werden im aktuellen Konsens der Forschung verschiedenste Szenarien zur Geschichte des Cloud Computing benannt. Einige sollen an dieser Stelle näher beleuchtet werden.

Repschläger geht in seinem Text „*Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale*“ beispielsweise davon aus, dass Application Service Providing (ASP) als einer der Vorgänger von Cloud Computing bezeichnet werden kann. Dies wäre im Rahmen der Cloud zu dem Modell Software as a Service (SaaS) weiterentwickelt worden. Weiterhin könne ihm zufolge das Grid Computing als einer der Wegbereiter für die Cloud bezeichnet werden. Es wurde im Forschungskontext entwickelt und brachte für die Cloud, wie wir sie heute kennen, wichtige Erkenntnisse in Bezug auf die verteilte Nutzung von Ressourcen. Bei dem ASP-Modell handelt es sich um eine Form von IT-Outsourcing, bei der der Anbieter bestimmte Leistungen, wie zum Beispiel Administration oder Hosting, für den Kunden übernimmt. Der Kunde hat dann über das Internet Zugriff auf seine Anwendungen. ASP-Modelle sind aber kaum individualisierbar und meist Standardlösungen. Das SaaS Konzept ist im Gegenzug in einem hohen Maß individualisierbar. Aufgrund dessen ist es besonders geeignet für die Abwicklung komplexer Geschäftsprozesse. Bei diesem Modell zahlt der Nutzer nur für die tatsächlich verbrauchten Ressourcen. Als Basis für dieses flexibel abrechenbare Modell dient eine Multi-Tenancy-Architektur, die es ermöglicht, mehrere Nutzer gleichzeitig mit denselben IT-Ressourcen zu versorgen. Das SaaS Modell beruht ebenfalls auf standardisierten Konzepten, welche allerdings im Gegensatz zum ASP-Modell für jeden Kunden individuell angepasst und konfiguriert werden können, ohne dabei die komplette Architektur des Systems verändern zu müssen. Darüber hinaus gilt auch das Grid Computing als einer der Vorgänger von Cloud Computing. Durch den Einsatz von Grid Computing können Daten und Rechenkapazitäten über mehrere (z.B. Unternehmens-) Standorte hinweg gemeinsam genutzt werden. Die dazu genutzten verteilten Ressourcen werden hierzu zu einem virtuellen Hochleistungscomputer verbunden, um die rechenintensiven Prozesse und Abläufe effektiv bewältigen zu können. Eine wichtige Aufgabe im Rahmen des Grid Computing ist hierbei die Kontrolle und Koordination der Ressourcennutzung. Cloud Computing und Grid Computing unterscheiden sich in der

Bereitstellung und Nutzung von Ressourcen. Im Cloud Computing wird ein zentraler Ressourcenbestand von einem Anbieter bereitgestellt und verwaltet. Beim Grid Computing wird eine dezentrale Zusammenführung verschiedener Ressourcen vorgenommen. Grid Computing Nutzer sind vorrangig Einzelkunden, wie beispielsweise Forschungseinrichtungen von Universitäten, die viele kleine IT-Ressourcen beziehen (z.B. von privaten Rechnern). Cloud Computing Nutzer hingegen sind Privat- oder Geschäftskunden, die ausschließlich von einem Anbieter eine einzige Leistung erwerben (Repschläger et. al., 2014).

Hentschel und Leyh beschreiben in ihrer Ausarbeitung „*Cloud Computing: Status quo, aktuelle Entwicklungen und Herausforderungen*“ den Begriffsursprung des Cloud Computing folgendermaßen: Der Begriff „Cloud Computing“ gehe demnach auf Ramnath K. Chellappa (Professor für Informationstechnologie) zurück. Er habe den Begriff auf einer Konferenz in Dallas 1997 geprägt. Historisch ist das Bild der Wolke eine Metapher für das Internet, was darauf hindeutet, dass alle Cloud Dienste von einem Anbieter im Internet beziehungsweise Intranet geleistet werden (Hentschel et. al., 2018).

Barton wiederum benennt in seinem Werk „*E-Business mit Cloud Computing. Grundlagen – Praktische Anwendungen – verständliche Lösungsansätze*“ Eric Schmidt als den Urheber des Begriffs „Cloud“. In den 90er Jahren habe dieser als CTO eines Technikkonzerns den Begriff „Computer in der Cloud“ geprägt. Unter dem Begriff werden heute verschiedene Fortschritte der Informationstechnik und der Internettechnologien zusammengefasst. Diese Fortschritte sind sowohl bedingt durch die rasanten Entwicklungen der Technik als auch durch das Verhalten und die Erwartungen der vielen Nutzer. Viele verschiedene Faktoren haben zur Entstehung des Cloud Computing beigetragen. So zum einen das Internet in seiner Funktion als globale Kommunikationsstruktur. Es ist weltweit verbreitet und bietet dank der Internettechnologie einen universellen Zugriff auf Informationstechnik von den verschiedensten Endgeräten. Weiterhin ist als ein Faktor die kontinuierlichen Verbesserungen in der Prozessorleistung zu nennen. Auch die fortschreitende Miniaturisierung und die immer günstiger werdenden Speicherlösungen haben zur Entstehung des Cloud Computing beigetragen. Den wichtigsten Faktor aber bildet die geänderte Verhaltensweise der Nutzer von Informationstechnologien. Nutzer haben heutzutage den Anspruch, zu jeder Zeit und von überall aus mit einem beliebigen

mobilen Endgerät Zugriff auf private und/oder geschäftliche Anwendungen zu haben (Barton, 2014).

Die Cloud Technologie hat schon einen langen Weg hinter sich gebracht. Liu beschreibt die ersten Anfänge der Cloud im Jahre 2006. Bei Amazon Web Services (AWS) wurden die Services „Simple Storage Service“ (S3) und „Elastic Compute“ (EC2) vorgestellt. Damals war Cloud noch etwas Unbekanntes. Heute reicht die Spannweite von Cloud Technologien von der Lagerung und Berechnung bis hin zu Daten- und Applikationsservices. Anhand des Wachstums von AWS‘ S3-Technologie kann man ablesen, wie stark der Cloud Markt allgemein gewachsen ist. Innerhalb von 6 Jahren ist die Anzahl an Objekten, die AWS S3-Services hostet von 200.000 auf eine Billion angestiegen (Stand 2013, aktuellere Angaben siehe Abschnitt 2.4 und 7.1.1). Das frühe und schnelle Wachstum von Cloud Technologien wurde vor allem durch kleine Start-Up Unternehmen vorangetrieben, die sich oftmals aufgrund des begrenzten Budgets keine hauseigene IT-Infrastruktur leisten konnten. Daher greifen sie bevorzugt auf mietbare Cloud Lösungen zurück. So können sie zunächst die benötigte Menge an Speicherplatz und den Server mieten, um die Effektivität ihres neuen Unternehmens erproben zu können (Liu, 2013).

2.4 Aktuelles

Heutzutage ist die Cloud aus den IT-Infrastrukturen großer Unternehmen und auch aus Privathaushalten nicht mehr wegzudenken. Im letzten Jahrzehnt ist die Nutzung von Cloud Computing stark angestiegen. Nahezu jede Firma nutzt die Cloud mit den verschiedenen Services, die sie zu bieten hat, beispielsweise um Kosten zu sparen oder auch wegen der gesteigerten Rechenstärke und Speicherkapazitäten (Thuraisingham, 2020). Die vielen Vorteile, die Cloud Computing mit sich bringt (siehe Abschnitt 5.1) haben in den vergangenen Jahren dazu geführt, dass immer mehr Unternehmen auf Cloud Computing bauen. 33% der deutschen Unternehmen würden PaaS Dienste und 47% IaaS Dienste verwenden und weitere 73% würden standardisierte Software in Form von SaaS Angeboten beziehen. Für diese Zahlen bezieht sich Hentschel auf eine Studie von Gartner aus dem Jahr 2015. Gemäß einer weiteren Studie aus 2016 verwenden bereits 65% der Unternehmen Cloud Computing und bereits 18% haben die Migration in die Cloud zukünftig geplant (Hentschel et. al., 2018).

Im Jahr 2020 ergab eine globale Umfrage, dass für 61% der Befragten die Cloud Nutzung aufgrund von COVID-19 höher war als erwartet. Es liegt nahe, dass dieser Anstieg daran liegt, dass Unternehmen auf der ganzen Welt viele ihrer Mitarbeiter zur Arbeit ins Homeoffice schicken mussten. Hierfür sind Unternehmen stark auf Cloud Dienste angewiesen. Nur mithilfe von Cloud kann eine Vielzahl an Mitarbeitern parallel von zu Hause aus arbeiten, da sie von verschiedenen Standorten aus auf Anwendungen und Daten zugreifen müssen (Internetquelle Statista Covid & Cloud). In Deutschland haben bis Ende Januar 2021 24% der befragten Erwerbstätigen einer Umfrage ausschließlich oder überwiegend im Homeoffice gearbeitet. Im ersten Lockdown im April 2020 lag diese Zahl bei 27%. Insgesamt ist erkennbar, dass die Homeoffice Nutzung seit Beginn der Pandemie deutlich zugenommen hat (Internetquelle Statista Corona & Homeoffice).

Für 2022 wird ein Umsatz von schätzungsweise 495 Milliarden US-Dollar für die Cloud prognostiziert. Dies umfasst Geschäftsprozesse, Plattformen, Infrastruktur, Software, Management, Sicherheit und Werbedienste, die von den verschiedenen Cloud Anbietern bereitgestellt werden (siehe Internetquelle Statista Umsatz Cloud Computing). Im vierten Quartal 2021 kontrollierte der stärkste Cloud Anbieter auf dem Markt, Amazon Web Services (AWS), 33% des gesamten Marktes. Microsoft Azure belegt mit 22% Marktanteil den zweiten Platz, gefolgt von Google Cloud mit 9% Marktanteil (siehe Internetquelle Statista Cloud Marktanteile). Im ersten Quartal 2022 wuchs der Umsatz von Amazon Web Services um 37% im Vergleich zum Vorquartal. AWS erwirtschaftete 2021 einen Nettoumsatz von 62 Milliarden US-Dollar, gegenüber 45 Milliarden US-Dollar im Jahr 2020 (Internetquelle Statista AWS).

2.5 Charakteristika

Das NIST nennt einige grundlegende Eigenschaften von Cloud Computing: Dazu gehören die fünf Charakteristika On-Demand, Self-Service, breiter Netzwerkzugriff, Ressourcen pooling und Elastizität sowie die drei Service Modelle „Infrastructure as a Service“ (IaaS), „Platform as a Service“ (PaaS) und „Software as a Service“ (SaaS) (siehe Abschnitt 3.1 – 3.3). Als weitere Kernelemente von Cloud werden zudem die verschiedenen Organisationsformen „Private Cloud“, „Public Cloud“ und „Hybrid Cloud“ genannt (siehe Abschnitt 4.1 – 4.3) (Bounagui et. Al., 2015).

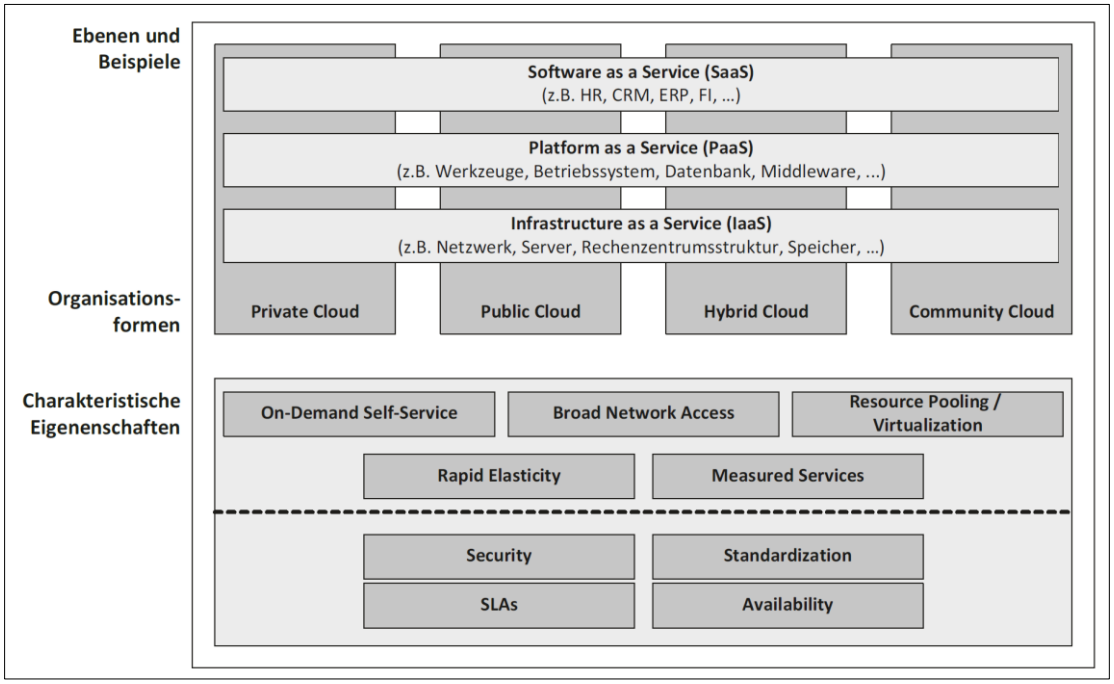

Abbildung 3: Charakteristika der Cloud

Die unterschiedlichen Organisationsformen geben Aufschluss darüber, ob die Cloud innerhalb des Unternehmens im Eigenbetrieb (insourced) oder außerhalb des Unternehmens von Drittanbietern (outsourced) betrieben werden soll. Die immer weiter steigenden Nutzerzahlen und die zunehmende Digitalisierung der Gesellschaft bringen einen wachsenden Bedarf an Rechenleistungen und Speicherkapazitäten mit sich. Klassische Modelle der Datenverarbeitung können diesem Andrang teils nicht mehr gerecht werden. Cloud Computing hingegen ist dazu sehr wohl in der Lage. In erster Linie steht hier der Einsatz von Virtualisierungstechnologien im Vordergrund. Die serviceorientierten Architekturen des Cloud Computing ermöglichen es Unternehmen, einzelne Dienste getrennt voneinander zu nutzen und miteinander zu kombinieren. Dies steigert nicht nur die Agilität und Flexibilität in Unternehmen, sondern erlaubt es ihnen auch, bestimmte Funktionen an externe Dienstleister auszulagern (Hentschel et. al., 2018).

Cloud Computing basiert auf verschiedenen Services, die dem Nutzer angeboten werden. Darunter fallen Services der Bereiche Rechenzeit, Netzwerkkapazität, Speicher und Datenbanken. Auch ganze Anwendungen werden als Services angeboten. Alle Services versprechen eine schnelle und flexible Verfügbarkeit bei geringen Vorabinvestitionen. Die Abrechnung erfolgt

in Abhängigkeit des Nutzungsvolumens. Der Zugriff auf einen Service beziehungsweise eine Anwendung in der Cloud erfolgt webbasiert, was eine hohe Standardisierung mit sich bringt. Für die hohen Anforderungen von Cloud Computing eignet sich eine zentrale Infrastruktur, die ihre Ressourcen aufteilt (Virtualisierung). Damit die verschiedenen Services dieselbe Infrastruktur zur selben Zeit nutzen können, muss diese dazu in der Lage sein, verschiedene Szenarien abzubilden. Um Lastspitzen auffangen zu können, muss das System zudem eine sehr hohe Skalierbarkeit aufweisen (Barton, 2014).

Das Kostenmodell im Cloud Computing beruht auf einem nachfrageabhängigen Mietmodell (On-Demand). Es entstehen also nur Kosten für die direkte Nutzung der angebotenen Dienstleistungen. Hierbei kann entweder auf Grundlage von Zeiträumen oder Verbrauchsmengen abgerechnet werden. Im Gegensatz zu klassischen IT-Lösungen fallen für den Kunden somit keine langfristigen Kosten für Lizensierungen oder Hardware an. Die Cloud Verträge haben meist recht kurze Laufzeiten, wodurch die Kunden an Flexibilität gewinnen (Repschläger et. al., 2014).

3 Servicemodelle in der Cloud

Cloud Computing basiert auf einem serviceorientierten Modell und bietet den Nutzern unterschiedliche Services an. Es gibt verschiedene Arten von Clouds: Cloud, die Infrastruktur zur Verfügung stellt, Cloud, die Infrastruktur und Plattform zur Verfügung stellt (z.B. Datenbanken und Programmierumgebungen) und eine Cloud, die Infrastruktur, Plattform und Software zur Verfügung stellt (Thuraisingham, 2020). Diese verschiedenen Arten von Clouds werden als unterschiedliche Servicemodelle beziehungsweise Abstraktionsebenen von Cloud Services benannt.

Die drei bekanntesten und meistgenutzten Service Ebenen sind „Infrastructure as a Service" (IaaS), „Platform as a Service" (PaaS) und „Software as a Service" (SaaS). Sie umfassen in der Regel alle vorhandenen Geschäftsmodelle der Cloud. Darüber hinaus gibt es noch weitere Service Ebenen, wie beispielsweise „Function as a Service" (auch: FaaS, Serverless Computing), welches als Erweiterung von PaaS verstanden werden kann. Anhand der Service Ebenen kann eine Unterscheidung nach Funktionalität und Zielsetzung erfolgen. Die drei Ebenen werden nach dem Abstraktionsgrad angeordnet. So kann die jeweilige Schicht mit höherem Abstraktionsgrad auf eine der unteren Schichten zurückgreifen und darauf aufgebaut werden. Je abstrakter die Ebene, desto komplexer ist der jeweilige auf der Ebene bereitgestellte Service (Hentschel et. al., 2018).

Mit der Eselsbrücke „Pizza as a Service" lässt sich leicht veranschaulichen, in welchem Rahmen die Beteiligung des Nutzers bei dem jeweiligen Service stattfindet.

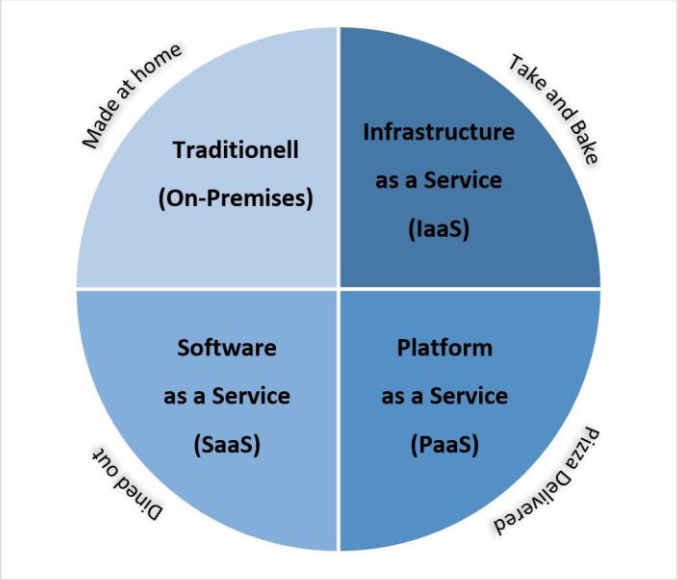

Abbildung 4: Pizza as a Service

Hier werden Analogien zwischen den verschiedenen Art und Weisen, Pizza zu konsumieren, und den unterschiedlichen Cloud Servicelevels hergestellt:

Made at home

Möchte ein Unternehmen die eigene IT-Infrastruktur sowie das Betriebssystem und Anwendungen in einem eigenen Rechenzentrum selbst betreiben, spricht man von „Traditionell On-Premises“. Bezogen auf das Pizzabeispiel bedeutet dies, dass die Zutaten für die Pizza selbst eingekauft werden, ein eigener Teig hergestellt wird, sie im eigenen Ofen gebacken wird und abschließend Zuhause verzehrt wird. In solch einem Konzept muss ein Unternehmen regelmäßig in neue Hardware investieren, da nach bestimmten Zeiträumen der Service und Support bei den entsprechenden Herstellern ausläuft. Genauso wird nach gewisser Zeit auch der Pizzateig und die gewählten Zutaten verderben. Ist die Haltbarkeit überschritten, muss ein neuer Pizzateig hergestellt werden.

Take & Bake

Im Cloud Servicemodell „Infrastructure as a Service“ kümmert sich der Cloud Anbieter um die benötigte Infrastruktur und ist für dessen Betrieb verantwortlich. Das Unternehmen ist nur noch

für die Betriebssysteme und Anwendungen selbst verantwortlich. Übertragen auf das Pizzakonzept bedeutet dies, dass Konsumenten sich eine Fertigpizza kaufen, diese dann im eigenen Ofen backen und am eigenen Tisch verzehren.

Pizza Delivered

Das Cloud Servicemodell „Platform as a Service“ geht noch einen Schritt weiter. Der Cloud Anbieter ist hierbei sowohl für den Betrieb der Infrastruktur, als auch für den Betrieb der Betriebssysteme (z.B. Updates) und Basisapplikationen (z.B. ein Datenbanksystem) verantwortlich. Das Unternehmen kann sich in diesem Modell dann voll auf die Anwendungen für die Nutzer fokussieren. Im Pizzabeispiel bedeutet dies, dass die Pizza ofenfrisch nach Hause geliefert wird und der Konsument nur noch Tisch und Getränk bereitstellen muss.

Dined out

In diesem Fall liegt die Verantwortung komplett beim Cloud Anbieter. Ein Beispiel dafür wäre der Konsum von Apps auf einem Smartphone. Hier sprechen wir von dem Cloud Servicemodell „Software as a Service“. Bezogen auf das Pizzabeispiel steht hierfür stellvertretend ein Restaurantbesuch. Der Konsument isst eine fremdgebackene Pizza an einem fremden Tisch und bezahlt am Ende für die Gastwirtschaft.

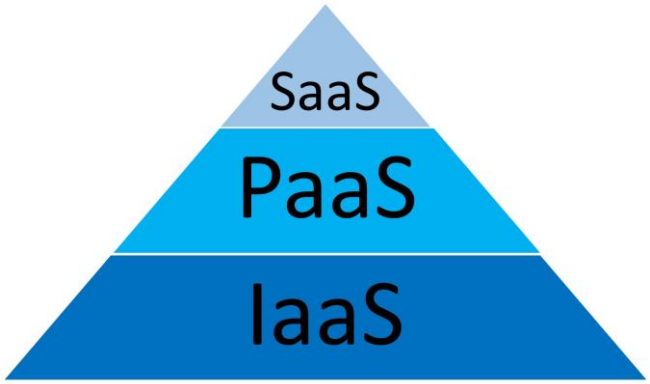

Abbildung 5: Service Ebenen der Cloud

Die unterste Service Ebene des Cloud Computing stellt Services für den Aufbau einer Infrastruktur zur Verfügung (IaaS). Dem Nutzer wird auf dieser Ebene Rechen-, Speicher- und/oder Netzkapazität zur Verfügung gestellt. Bekannte Services auf der Ebene IaaS für den B2B

Geschäftsbereich sind beispielsweise verschiedenste Dienste von Amazon Web Services (AWS). Für den privaten Bereich gibt es hier Produkte wie zum Beispiel Dropbox. Die zweite Ebene wendet sich an Softwarearchitekten und Anwendungsentwickler und stellt ihnen Entwicklungsplattformen (PaaS) zur Verfügung. Auf der Plattform können die Nutzer neue Anwendungen entwickeln oder bereits bestehende Anwendungen individuell unternehmensspezifisch anpassen. Beispiele für PaaS Anbieter sind AWS, Microsoft Azure oder die Google Cloud. Auf der obersten Ebene werden ganze Anwendungen als Software in einer standardisierten Form zur Verfügung gestellt (SaaS). Der Nutzer erwirbt hierbei kein individuelles Nutzungsrecht an der Anwendung, sondern die Anwendung wird ihm als Dienstleistung für einen festgelegten Zeitraum zur Verfügung gestellt. Die Abrechnung erfolgt auch hier nach Nutzungsumfang. Beispiele für solche Anwendungen sind Salesforce.com, Office 365 von Microsoft oder Google Apps for Business (Barton, 2014).

3.1 Infrastructure as a Service

Infrastructure as a Service (IaaS) bildet die niedrigste Abstraktionsschicht und stellt eine physikalische IT-Infrastruktur in Form von verschiedenen Diensten bereit. Der Schwerpunkt liegt auf dieser Ebene in der dynamischen Zuweisung von IT-Ressourcen (Speicher-, Prozessor- & Netzkapazitäten), um dem Nutzer auf Abruf zur Verfügung stehen zu können. Das IaaS Modell findet dann Verwendung, wenn komplexe Anwendungen vorliegen, die von einer klassischen Hardware nicht mehr bewältigt werden können. Infrastrukturkomponenten wie Rechenleistung oder Speicher müssen vom Kunden nicht kostspielig erworben werden, sondern werden von einem externen Dienstleister angemietet. Bekannte Dienstleister für IaaS sind zum Beispiel Amazon Web Services (AWS) oder T-Systems. Dem Nutzer wird eine uneingeschränkte Skalierbarkeit der Kapazitäten zur Verfügung gestellt. Bei erhöhtem Bedarf können immer weitere Ressourcen aus einer Art Hardware-Pool dynamisch hinzugezogen werden. Dieser Pool wird mithilfe einer Programmierschnittstelle (API) angesprochen und ermöglicht die flexible Skalierung der vorhandenen Infrastruktur. Typische Kunden von IaaS Leistungen sind zum Beispiel IT-Dienstleister, Cloud Anbieter oder Fachabteilungen (Hentschel et. al., 2018).

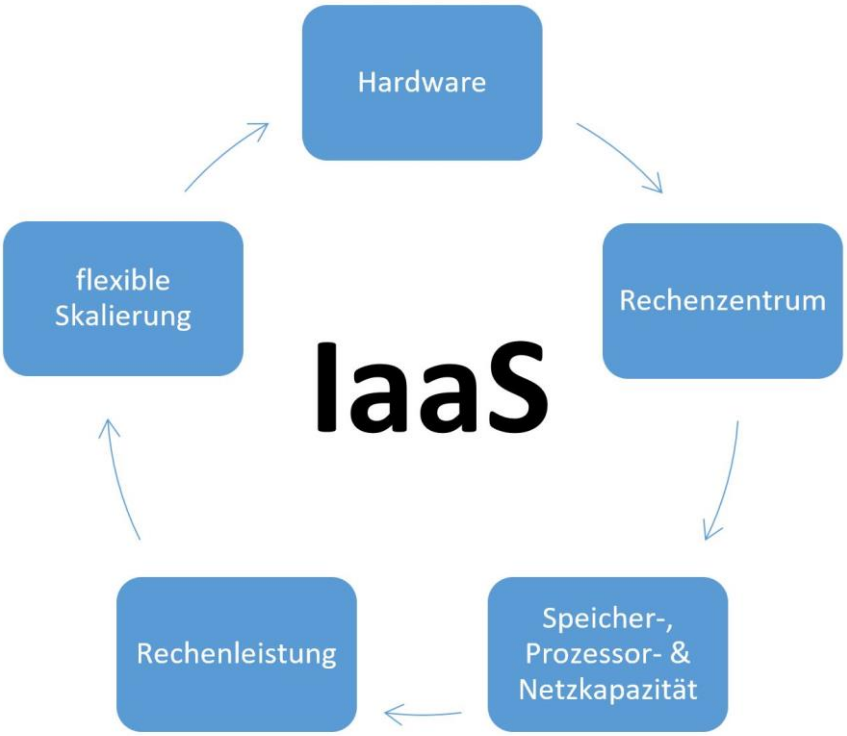

Abbildung 6: Infrastructure as a Service

Bei dem IaaS Geschäftsmodell ist also eine Infrastruktur notwendig, die an den wechselnden Ressourcenbedarf angepasst werden kann. Dazu werden eigenständige virtualisierte Instanzen und dazugehörige Betriebssysteme inklusive Rechenleistung genutzt. Die dazu benötigten Leistungen (Arbeitsspeicher, Speicherkapazität der Festplatte, Leistung des Prozessors) können flexibel angepasst werden. Diese Art von Infrastruktur kann nicht nur über Cloud Anbieter als IaaS Leistung erworben werden, sondern alternativ auch in eigenen Rechenzentren betrieben werden oder extern gemanaged werden.

An dieser Stelle soll auf das IaaS Angebot von Amazon Web Services (AWS) eingegangen werden. Die Amazon Web Services umfassen viele verschiedene Dienstleistungen in den folgenden Bereichen: Rechenleistung, Datenspeicherung, Messaging und Content Distribution Network. Speziell für den Bereich Infrastructure as Service gibt es die „Amazon Elastic Compute Cloud“ (EC2). Sie bietet den Kunden eine virtuelle Rechenumgebung, dessen Kapazität sich skalierbar an den Bedarf des Kunden anpasst. Der „Amazon Simple Storage Service“ (S3)

ermöglicht es, Daten dynamisch und ortsunabhängig zu speichern und eine beliebige Anzahl an Daten, die auf mehreren verteilten Amazon Servern gespeichert sind, abzurufen. Zudem bietet Amazon unter anderem zwei webbasierte Datenbanken an: „Amazon Simple DB“ (verteilte Datenbank) und „Amazon Relational Database Service“ (relationale Datenbank). Die „Amazon Cloud Front“ ist besonders für den Bereich Quality of Service interessant und ermöglicht die Bereitstellung von Inhalten über ein globales Netzwerk aus verschiedenen Serverstandorten. In den weltweit betriebenen Amazon internen Rechenzentren spielen Merkmale wie Ausfallsicherheit, skalierbare Rechenleistung und variable Speicherkapazität eine wichtige Rolle. Amazon arbeitet ebenfalls mit unabhängigen Softwareanbietern im Rahmen eines Partnerprogramms zusammen. Drittanbieter können ihre Leistungen so in einem öffentlichen Verzeichnis auflisten und für ihre Kunden präsentieren. Eine Entwicklungsplattform wird hier allerdings nicht angeboten, sondern es können lediglich die o.g. Dienste verwendet werden um beispielsweise darauf aufbauend eine Anwendung zu entwickeln. Um die AWS Leistungen mit bereits existierenden Programmierumgebungen (z.B. Java, PHP) verknüpfen zu können, stellt Amazon passende Schnittstellen zur Verfügung. Die AWS Cloud Modelle machen es möglich, die genutzten Ressourcen gemäß dem tatsächlichen Verbrauch zu berechnen. Für die Rechnungsstellung wird entweder die beanspruchte Zeit oder die verbrauchten Ressourcen abgerechnet. Bei der Abrechnung über das Zeitmodell wird die Leistung in vollen Stunden berechnet. In Abhängigkeit von der verbrauchten Rechenleistung werden dann Preise zwischen 0,10 € und 2,00 € pro Stunde fällig. Durch das hohe Maß an Flexibilität und das Wegfallen von Hardwarekosten ist die Bandbreite an AWS Kunden enorm vielfältig. Besonders attraktiv sind die AWS Modelle für Start-Up Unternehmen oder für Firmen mit besonders großen Lastschwankungen. Für spezielle Kunden wie beispielsweise Bildungseinrichtungen hält AWS besondere Preisstaffelungen bereit (Repschläger et. al., 2014).

3.2 Platform as a Service

Platform as a Service (PaaS) bildet die mittlere Abstraktionsschicht und richtet sich in erster Linie an Anwendungsentwickler und Systemarchitekten. PaaS bietet ihnen eine Plattform, auf der sie eigene Software entwickeln, testen und ausführen können. Bei PaaS wird dem Nutzer keine fertige Software geboten, sondern der Anbieter stellt Programmierumgebungen und Ausführungsumgebungen (Programming Environments „PE“ und Execution Environments „EE“)

zur Verfügung. Damit kann Software in verschiedenen Programmiersprachen entwickelt werden. Der Nutzer kann mit PaaS den kompletten Entwicklungszyklus von Software (Design, Testen, Implementieren, Verteilen) in der Cloud realisieren. Oftmals kommen hierbei spezifische Elemente zum Einsatz, die einen Wechsel des Anbieters erschweren. Somit besteht bei PaaS zumeist eine hohe Abhängigkeit von dem jeweiligen Cloud Anbieter. Bekannte Dienste für PaaS sind beispielsweise AWS Elastic Beanstalk, Google App Engine oder Azure App Service von Microsoft. (Hentschel et. al., 2018).

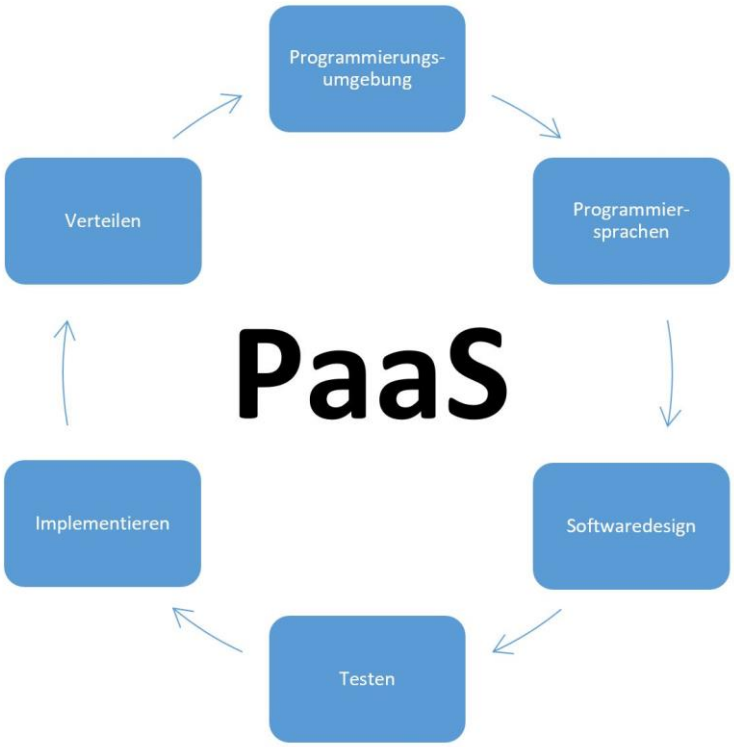

Abbildung 7: Platform as a Service

Das PaaS Modell umfasst im Gegensatz zu IaaS höherwertige Leistungen. Anstelle von Infrastruktur Lösungen werden hier technische Frameworks und Anwendungssoftware angeboten. PaaS bietet als Entwicklungsplattform die Basis für später daran anknüpfende SaaS Angebote. Die Kundengruppe von PaaS Angeboten umfasst Softwareanbieter, Anwendungsentwickler und „Value Added Resellers“ (VAR). Diese entwickeln neue Anwendungen, erweitern

bestehende Dienste und betreiben fertige Lösungen auf der Plattform und müssen dafür keinerlei eigene Kapazitäten vorhalten.

Als Beispiel sollen hier zwei verschiedene cloudbasierte Lösungen von Google vorgestellt werden. Die Google App Engine ist eine zentrale Plattform für die Entwicklung und das Hosting von Webanwendungen auf Google Servern. Dem Nutzer stehen dabei alle Hard- und Softwareressourcen online zur Verfügung. Die Programmiersprachen Python, Scala und JRuby werden hier unterstützt. Die Google Apps bilden die zweite Cloud Lösung von Google. Es handelt sich um Cloud Applikationen für Messaging, Büroanwendungen und Kollaborationen. Es kann kostenlos mit Werbeschaltung oder kostenpflichtig genutzt werden. Das kostenpflichtige Lizenzmodell bietet die Vorteile einer erhöhten Verbindungssicherheit und eines größeren Speicherplatzes für den Kunden. Die Entwicklungsplattform von Google ist für jeden frei zugänglich. Es gibt lediglich Mengeneinschränkungen für den Datenverkehr, die Speicherkapazität, die Rechenkapazität und den Email Versand. Die Mengen beziehungsweise Leistungen können durch Zukauf vergrößert werden. Drittanbieter, die nicht nur eine Anwendung auf der Entwicklungsplattform entwickeln möchten, sondern diese auch weitervertreiben wollen, bietet Google noch den „Google Apps Marketplace“ an. Im Rahmen des Partnerprogramms „Google Apps Authorized Reseller“ werden Anbieter angesprochen, die Beratungen auf Grundlage von Google Apps anbieten. Google verdient einerseits über den Marketplace, denn dort werden von Drittanbietern Kosten für das Einstellen ihrer Applikation verlangt. Außerdem erhält Google Anteile aus den Erlösen der jeweiligen Anwendung. Außerdem werden Leistungen wie CPU, Rechenzeit oder Datenspeicher, die im Rahmen des Applikationsbetriebs auf der Plattform anfallen, von den Kunden zugekauft (IaaS). Darüber hinaus erwirtschaftet Google noch Einnahmen aus der Google Apps Premium Lizenz. Die Google App Engine Plattform ist besonders attraktiv für externe Dienstleister. Sie können ihre Anwendung über die Plattform direkt nach der Fertigstellung einer breiten Masse zur Verfügung stellen, ohne dafür erforderliche Vertriebsinfrastrukturen aufzubauen. Die Google Apps Angebote werden von Privatpersonen und Geschäftskunden oder auch Forschungseinrichtungen gleichermaßen genutzt (Repschläger et. al., 2014).

3.3 Software as a Service

Software as a Service (SaaS) bildet die höchste der drei Abstraktionsschichten. Hier erfolgt die Bereitstellung von standardisierten Anwendungen für Endnutzer. Die Software wird dabei von dem jeweiligen Anbieter über das Internet bereitgestellt, sodass eine lokale Installation nicht nötig ist. Für die meisten SaaS Dienste benötigen die Nutzer lediglich einen Internetzugang sowie ein Endgerät mit Webbrowser. Der SaaS Anbieter ist zu jeder Zeit für den Betrieb und die Wartung der Software verantwortlich. Die Möglichkeiten zur Anpassung und Integration von SaaS Software sind meistens sehr begrenzt, da sie über eine Multi-Tenant-Architektur einer breiten Masse zur Verfügung gestellt werden. Die SaaS Leistungen werden meistens nach dem Pay-per-use Modell abgerechnet, sodass die Nutzer auch nur für das zahlen, was sie tatsächlich genutzt haben. Der Einsatz von SaaS Diensten ist in fast allen Bereichen möglich. Im betrieblichen Umfeld ist ein viel genutzter SaaS Dienst das Customer-Relationship-Management (CRM-Software). Der bekannteste Dienstleister für SaaS Implementierungen ist Salesforce, ein Anbieter für CRM-Software (Hentschel et. al., 2018).

Abbildung 8: Software as a Service

Bei dem SaaS Modell handelt es sich also um eine Form des Cloud Computing, bei der webfähige Anwendungen dem Kunden skalierbar angeboten werden. Diese können innerhalb des Unternehmens betrieben werden und werden vom Anbieter mit individuellen Einstellungen dem jeweiligen Unternehmen angepasst. Wesentliche Bestandteile des SaaS Angebots sind die Serviceorientierung und die flexible Skalierbarkeit.

Es folgt beispielhaft das SaaS Angebot von Salesforce.com. Das Angebot umfasst drei SaaS Produkte, eine Entwicklungsplattform und einen Applikationsmarktplatz. Die webfähige CRM-Lösung „Sales Cloud“ bietet dem Kunden eine ortsunabhängige Anwendung, die automatisiert Kundenanfragen erfasst, Workflows realisiert und Informationen personalisiert anzeigt. Die „Service Cloud“ bietet eine weitere Option, um Kundenservice zu ermöglichen. Eine unternehmensweite Kommunikation findet über die Cloud Lösung „Chatter“ statt. Die cloudbasierte Entwicklungsplattform „Force.com“ bietet Anwendungsentwicklern die Möglichkeit, eigene Applikationen zu entwickeln oder aus einem vorhandenen Pool aus dem internen Marketplace „AppExchange“ auszuwählen. Über die eigene Entwicklungsplattform können Programmierer und unabhängige Softwareanbieter neue cloudfähige Anwendungen erstellen, erweitern und dann auf der Plattform betreiben. Aktuell verfügt das Angebot von Salesforce.com über verschiedenste Geschäftslösungen wie beispielsweise Applikationen für das Rechnungswesen, die von Kunden oder Drittanbietern erstellt wurden. So können standardisierte firmeninterne CRM-Lösungen mit spezifischen Diensten individualisiert werden. Außerdem unterstützt die Plattform Fremdsysteme wie SAP oder Google Apps über definierte Schnittstellen. Eine Kooperationsvereinbarung zwischen Google Apps und Salesforce.com regelt zudem den Datenaustausch zwischen den beiden Anbietern und ermöglicht die Entwicklung und den anschließenden Betrieb einer Anwendung durch Software Drittanbieter. Die Einnahmen von Salesforce.com basieren zum einen auf den drei SaaS Produkten „Sales Cloud“, „Service Cloud“ und „Chatter“. Hier werden Kosten für den Kunden auf monatlicher Nutzerbasis abgerechnet. Zum anderen müssen unabhängige Softwareanbieter eine monatliche Nutzungsgebühr je nach dem persönlichen Leistungsumfang bezahlen. Die Rechnungsgestaltung richtet sich hier ausschließlich nach festgelegten Konditionen und wird nicht von den tatsächlich genutzten Ressourcen beeinflusst. Außerdem wird über den eigenen Marktplatz „AppExchange“ Gewinn gemacht. Pro angebotener Anwendung fällt hierbei eine jährliche Gebühr für den Ersteller an. Die Salesforce.com Angebote sprechen vor allem Unternehmenskunden an. Dies sind zum

einen unabhängige Softwareanbieter, die auf der Plattform ihre Anwendung entwickeln und im Anschluss skalierbar vertreiben möchten. Auf der anderen Seite sind die Kunden typische Nutzer von CRM-Systemen. Dies sind hauptsächlich kleine, mittelständische und große Unternehmen (Repschläger et. al., 2014).

3.4 Serverless Computing

Als Serverless Computing, auch Function as a Service, wird ein Ausführungsmodell innerhalb der Cloud bezeichnet, bei welchem der Cloud Anbieter eine dynamische Zuweisung der Rechenressourcen des Servers vornimmt. Es wurde ursprünglich als Erweiterung von Platform as a Service entwickelt, um dieses Modell leichter zugänglich und erschwinglicher zu machen. Es dient dazu, das Ressourcenmanagement einfacher, günstiger und effizienter zu gestalten. Dem Kunden wird bei diesem Modell lediglich die tatsächlich verbrauchte Menge an Ressourcen in Rechnung gestellt und nicht eine vorher vereinbarte Einheit an Rechenkapazitäten. Das Serverless Computing Modell wurde entwickelt, um ein Optimum an Kosten, ein Minimum an Konfigurationsaufwand undeine Steigerung in der Fähigkeit der Applikation zum Skalieren in der Cloud zu erreichen. Serverless Computing wird definiert als eine Software Architektur, bei der die jeweilige Anwendung aufgegliedert wird in Ereignisse und Funktionen. Diese Anwendung wird auf einer Plattform betrieben, die eine nahtlose Hosting- und Ausführungsumgebung bieten kann. Die Anwendung konsumiert dabei die Ressourcen bis zum Zeitpunkt der Ausführung und erst später werden die Ressourcen dann freigesetzt. Bei diesem Modell liegt die Verantwortung zum Management der Datenzentren, Server und Laufzeitumgebung komplett bei dem Serviceanbieter. Die drei größten Serverless Computing Cloudanbieter sind AWS Lambda, Google Cloud Function und Microsoft Azure Function (Rajan, 2018). AWS Lambda war das erste Serverless Computing Angebot überhaupt. Serverless Computing ist ein Angebot in der Cloud, bei dem die Applikationslogik in Funktionen aufgeteilt ist und ausgeführt wird in Bezug zu bestimmten Ereignissen. Diese Ereignisse können durch Quellen außerhalb der Cloud Plattform ausgelöst werden aber auch innerhalb der Service Angebote einer Plattform auftreten. Dies erlaubt es Entwicklern, Anwendungen zusammenzustellen, die sich über verschiedenste Services innerhalb der Cloud verteilen. Serverless Computing kann auch als Teilrealisierung eines ereignisbasierten Ideals verstanden werden, in welchem Anwendungen

durch Handlungen und Ereignisse definiert werden, die sie auslösen beziehungsweise anstoßen (McGrath et. al., 2017).

Es wird davon ausgegangen, dass die IT-Ausgaben für Serverless Computing bis zum Jahr 2021 8 Milliarden Dollar übersteigen werden.

> *„Serverless computing is a form of cloud computing that allows users to run event-driven and granularly billed applications, without having to address the operational logic.“* (van Eyk et. al., 2018, p. 9).

Die Definition beschreibt Serverless Computing als eine Rechenabstraktion, die teilweise Überschneidungen zu Platform as a Service aufweist. Mithilfe dieses Modells können Entwickler sich auf Abstraktionen höchster Ebene fokussieren und so Applikationen bauen, die Infrastrukturbetreiber konkrete Ressourcen und unterstützende Services zuordnen. Auf diese Weise ist die Aufgabentrennung klar definiert: die Entwickler konzentrieren sich auf die Geschäftslogik und suchen nach Wegen, um diese Logik mit komplexen Arbeitsabläufen zu verbinden während die Service Anbieter sicherstellen, dass die Serverless Anwendungen korrekt arrangiert sind (containerisiert, ausgeliefert, vorgehalten und verfügbar auf Abruf) und sie so den Kunden lediglich die genutzten Ressourcen in Rechnung stellen.

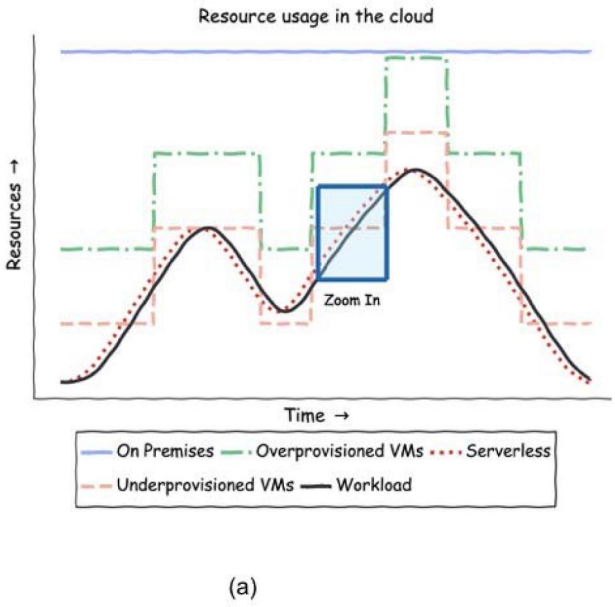

Abbildung 9: Ressourcennutzung in der Cloud

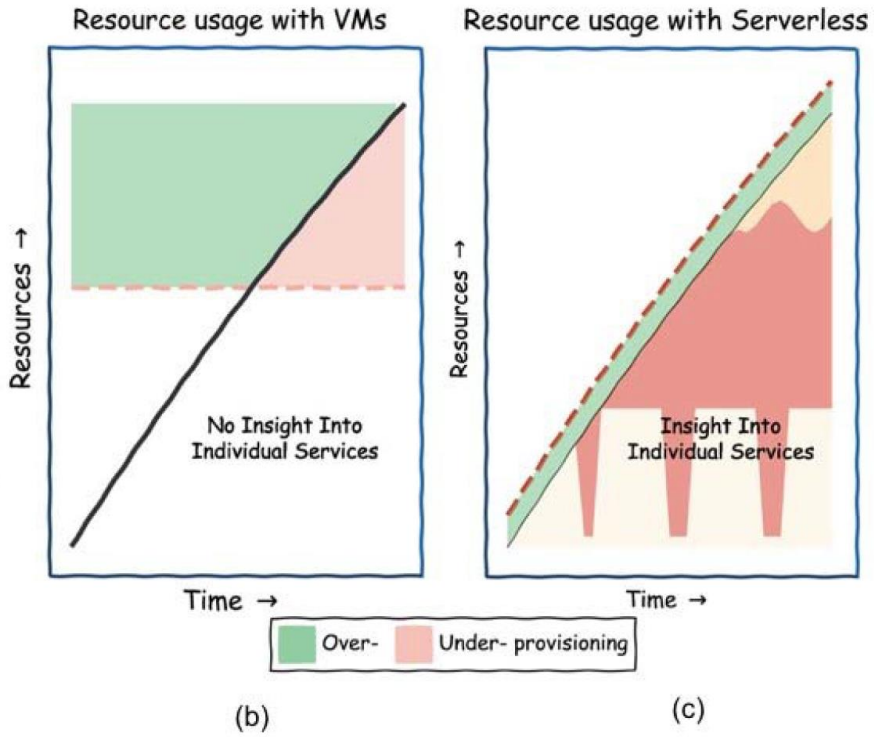

Abbildung 10: Ressourcennutzung VMs & Serverless

Die Abbildungen 9 und 10 zeigen einen typischen Anwendungsfall für Serverless Computing: höhere Ressourcenauslastung, feinere Granularität und eine detailliertere Kontrolle als bei containerbasiertem oder selbst gehostetem Computing. Abbildung 9 zeigt die Ressourcennutzung in der Cloud. Abbildung 10 zeigt die Ressourcennutzung mit virtuellen Maschinen (VMs) auf der einen Seite (b) und die Ressourcennutzung mit Serverless Computing auf der anderen Seite (c).

Die Serverless Technologie bietet viele Vorteile, wie zum Beispiel eine Verbesserung der Performance bei gleichzeitiger Reduzierung der betriebsbedingten Kosten der Anwendungen. Im traditionellen Cloud Computing ist der Nutzer verantwortlich dafür, konkrete Ressourcen auszuwählen und anzuwenden. Um den Nutzer damit nicht zu überfordern, wird meist nur eine kleine Auswahl an Ressourcen zur Verfügung gestellt (z.B. Container). Diese Einschränkung in der Ressourcenauswahl wird jedoch vielen Anwendungen nicht gerecht. Im Gegensatz dazu sind Anwendungen im Serverless Computing stets sehr feinkörnig, sodass die Cloud Anbieter den abstrakten Ressourcenbedarf besser und leichter an die tatsächlichen Systemressourcen

anpassen können. Darüber hinaus ist der Nutzer bei herkömmlichen Cloud Modellen dafür verantwortlich, all die Aufgaben im Lebenszyklus der Anwendungen zu überwachen. Vielen Nutzern fehlt es hierbei jedoch an der nötigen Expertise. Beim Serverless Computing liegt mehr Verantwortung beim Betreiber, wodurch er mehr Einsicht und Kontrolle erlangt. Die Betreiber können ihr Wissen über das Verhalten der Anwendung mit dem Nutzer teilen und so können bessere Entscheidungen in Bezug auf die Serverless Anwendung getroffen werden. Ein weiterer Vorteil von Serverless Computing ist, dass die Services unabhängig voneinander sind. Sie erlauben es Entwicklerteams, die richtigen Werkzeuge für einen speziellen Anwendungsfall auszuwählen, ohne dabei andere Teile des Systems oder der Organisation zu beeinflussen. Darüber hinaus ermöglicht das hohe Abstraktionslevel Softwareentwicklern sehr schnell eine wiederholte Ausführung an diesen verteilten Systemen vorzunehmen (van Eyk et. al., 2018).

4 Liefermodelle der Cloud

Die Cloud existiert in drei verschiedenen Organisationsformen beziehungsweise Liefermodellen: Public Cloud, Private Cloud und Hybrid Cloud. Neben den verschiedenen Organisationsformen der Cloud unterscheidet man noch zwischen zwei Sourcing Optionen: So wird eine Public Cloud vollständig durch einen externen Dienstleister betrieben (outsourced). Das Mitspracherecht des Unternehmens ist an dieser Stelle sehr gering, es gibt beispielsweise keine eigenen Service-Level-Agreements (SLAs). Eine SLA bezeichnet eine Vereinbarung zwischen Anbieter und Kunde und dient der Qualitätssicherung. Bei einer Private Cloud Lösung kann der Kunde selbst entscheiden. welche Mindestanforderungen erfüllt sein sollen. Das Unternehmen kann selbst bestimmen, ob die Cloud im eigenen Unternehmen betrieben werden soll (insourced), in diesem Fall ist das Unternehmen gleichzeitig auch der Inhaber der benötigten IT-Ressourcen, oder durch einen externen Dienstleister betrieben werden soll (managed). Basis für den Betrieb in einer managed Private Cloud sind individuell mit dem jeweiligen Kunden vereinbarte SLAs. Der Zugang zu einer Private Cloud ist meistens beschränkt auf Mitarbeiter, teilweise erhalten auch Kunden einen Zugang. Bei einer outsourced oder hosted Private Cloud befindet sich die gesamte Infrastruktur der Cloud beim Dienstleister. Dieser ist gleichzeitig auch der Besitzer der Infrastruktur und betreibt die Private Cloud für seinen Kunden eigenverantwortlich. Aus den beiden genannten Betriebsarten einer Cloud (Public und Private) kann die dritte mögliche Form kombiniert abgeleitet werden: Die Hybrid Cloud bezeichnet eine Verknüpfung mehrerer Clouds untereinander oder auch eine Kombination aus einer Cloud und einer traditionellen IT-Landschaft innerhalb eines Unternehmens. Bei dem Einsatz einer Hybrid Cloud hat das Unternehmen die Wahl über alle Sourcing Optionen. Lediglich der Teil der Public Cloud muss stets outsourced betrieben werden (Hentschel et. al., 2018 & Barton, 2014).

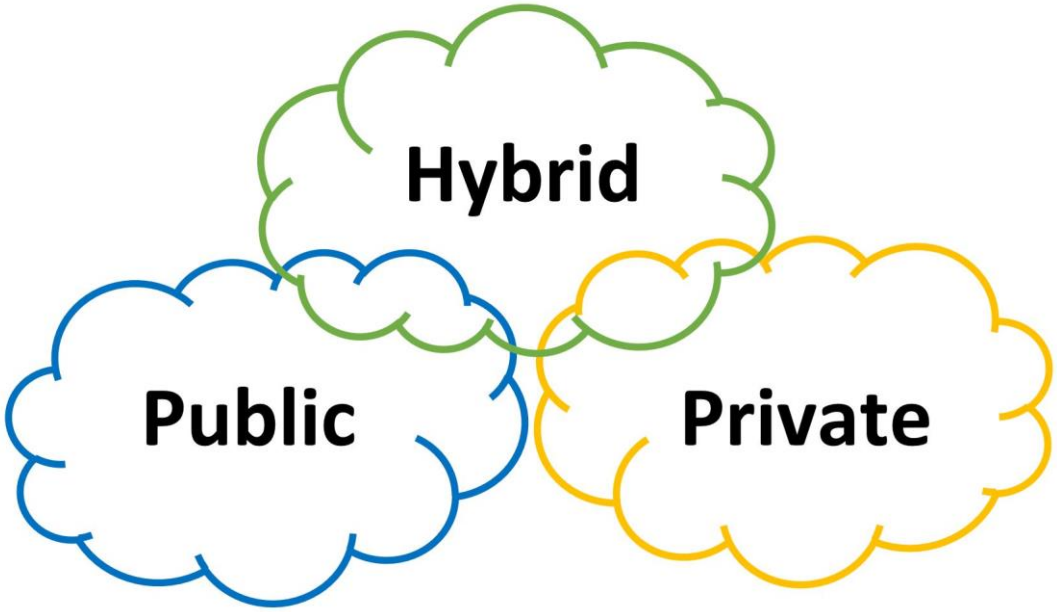

Abbildung 11: Liefermodelle der Cloud

Zusammengefasst bietet die Cloud in offenen Umgebungen (Public Cloud) viele Möglichkeiten für Wachstum und Verwertung. In geschlossenen Umgebungen (Private Clouds) findet man sehr starke Kontrollmechanismen mit spezifischen Regulierungen des vorherrschenden Ökosystems, wodurch aber auch ein höheres Sicherheitsniveau erreicht werden kann. In gemischten Umgebungen (Hybrid Clouds), können die Vorteile der Freiheit aus offenen Umgebungen mit der Genauigkeit und Stringenz aus den geschlossenen Umgebungen miteinander vereint werden.

4.1 Public Cloud

Bei der Public Cloud handelt es sich um einen öffentlich zugänglichen Pool an IT-Ressourcen. Daten und Dienste befinden sich in diesem Modell beim Cloud Anbieter (Repschläger et. al., 2014). In einer Public Cloud teilen sich mehrere Anwender dieselbe Infrastruktur. Der Serviceanbieter stellt eine klar definierte Leistung gegen Rechnung zur Verfügung. Die Abrechnung erfolgt in der Regel nach den tatsächlich verbrauchten Ressourcen (Hentschel et. al., 2018).

4.2 Private Cloud

Die Private Cloud verfügt über einen beschränkten Zugang (wie beispielsweise bei dem Intranet eines Unternehmens). Die Ressourcen und Anwendungen befinden sich hierbei in einem unternehmenseigenen Rechenzentrum (Repschläger et. al., 2014). In einer Private Cloud hat nur ein vorher definierter Nutzer Kontrolle über den Zugriff und die IT-Infrastruktur. Der Zugang erfolgt in der Regel über ein Intranet oder ein Virtual Private Network (VPN). Oft werden Private Clouds von den Unternehmen selbst betrieben, aber auch hier ist eine Auslagerung an externe Dienstleister möglich. Wenn die Cloud intern betrieben wird, hat dies den Vorteil, dass man sich nicht von Drittanbietern und Herstellern abhängig macht. Auch die Private Cloud ist nicht für alle Anwendungsfälle optimal, beispielsweise kann es zu Problemen kommen, wenn große Lastspitzen abgefangen werden sollen. An dieser Stelle kann der Einsatz einer Hybrid Cloud dann die sinnvollste Lösung sein (Hentschel et. al., 2018).

4.3 Hybrid Cloud

Die Hybrid Cloud kann als Mischform aus Private und Public Cloud angesehen werden. Hierbei werden keine besonders schützenswerten Anwendungen oder Daten an den Cloud Anbieter ausgelagert, geschäftskritische Ressourcen können parallel intern gelagert werden (Repschläger et. al., 2014). Bei diesem Modell werden einzelne Services und Funktionalitäten in eine Public Cloud ausgelagert, um den regelhaften Betrieb in der Private Cloud nicht zu beeinträchtigen. Genauer gesagt werden hierbei standardmäßig die eigenen IT-Ressourcen genutzt und nur im Bedarfsfall Rechenleistung an einen Cloud Anbieter ausgelagert. Der jeweilige Umfang der Kombination aus Private Cloud und Public Cloud hängt von dem Bedarf des jeweiligen Unternehmens ab. Die größte Herausforderung dieser Mischform liegt in der Security- und Serviceintegration (Hentschel et. al., 2018).

5 Chancen & Risiken von Cloud Computing

Der weltweite Public Cloud Markt wächst weiter und weiter (Aktuelle Zahlen siehe Abschnitt 2.4). Aufgrund dessen zeigen Industrie und Forschung großes Interesse daran, zu prüfen, welche Hindernisse die erfolgreiche Einführung von Cloud Services in einem Unternehmen haben kann. An dieser Stelle soll eine Studie von Morgan et. al. vorgestellt werden, die untersucht hat, welche Faktoren die Einführung von Cloud Services beeinflussen können. Die Autoren unterscheiden die untersuchten Faktoren hierbei in drei Gruppen: Technologisch (Welche Technologien sind in dem Unternehmen verfügbar?; Welche Technologiefaktoren beeinflussen den Einführungsprozess?), die Organisationsstruktur betreffend (Die Strukturen und Prozesse/Abläufe in einem Unternehmen können die Einführung von manchen Innovationen erzwingen oder ermöglichen) und Ökologisch (Regeln der Regierung geben Beschränkungen beziehungsweise Möglichkeiten für technologische Innovationen vor).

Aus der Studie geht hervor, dass die teilnehmenden Unternehmen als größte Vorteile von Cloud die folgenden Faktoren angaben: Kosteneinsparung, erhöhte Skalierbarkeit sowie Zeitersparnis. Einige gaben an, beim Wechsel in die Cloud innerhalb von 24 Stunden arbeitsfähig gewesen zu sein. Bei traditionellen IT-Systemen würde dies bis zu 6 Monate dauern. Als Nachteil nannten manche Unternehmen die schwere Integrierbarkeit in bestehende Systeme (wenn man nicht komplett umsteigen will). Außerdem befürchten manche Unternehmen, dass die Internetgeschwindigkeit beziehungsweise Bandbreite und Konnektivität nicht ausreichen würde für die Performance von Cloud Services. Manche Angestellte fürchten sich außerdem vor der Komplexität der Cloud. Die Anbieter müssten daher an der Intuitivität arbeiten. Alle Studienteilnehmer gaben an, dass sich durch die Einführung von Cloud die Kooperation entlang der Supply Chain, das Team Gefüge und die Kommunikation innerhalb der Organisation verbessert hat. Der Bedarf an gesteigerter Nachvollziehbarkeit und Prüffähigkeit ist ein weiterer Grund, um Cloud Services einzuführen. Alle Informationsdienste innerhalb eines

Unternehmens können via Cloud nachverfolgt werden. Gerade IT-Manager müssen sich umstellen, da die Normen und die Kultur des Unternehmens einen Wandel durchleben. Auch Sicherheits- und rechtliche Themen können die Einführung von Cloud beeinflussen. Anwender fühlen sich der Studie zufolge sicherer im Umgang mit der Cloud, wenn ihnen bekannt ist, wo sich das Rechenzentrum in der Realität befindet. Tatsächlich empfinden viele Anbieter das Wort „Cloud" an sich als problematisch, da es zu abstrakt ist. Die Studie ergab darüber hinaus, dass viele Probleme bezüglich der Einführung von Cloud eher Nutzerbezogen und weniger technisch sind (Morgan et. al., 2013).

Die Darstellung dieser Studie dient als Einstieg in die Gegenüberstellung der Chancen und Hindernisse von Cloud Computing und zeigt die Sichtweise von Unternehmen auf die Cloud Technologie. In den folgenden Abschnitten soll nun zunächst genauer auf die Vorteile eingegangen werden, ehe etwaige Sicherheitsbedenken und die schwierige Rechtslage beleuchtet werden.

5.1 Vorteile

Das Cloud Computing bietet viele Potenziale. So entsteht durch Cloud Computing beispielsweise ein Netzwerk der Wertschöpfung, bestehend aus einzelnen Parteien, die notwendige Vorleistungen für den Einsatz der Cloud (z.B. Speicherplatz) erbringen, Standardlösungen erstellen (CRM-Dienste), bereits vorhandene Lösungen an Kundenwünsche anpassen (z.B. HR-Lösungen) oder Softwarebestandteile verschiedener Hersteller integrieren.

Vorteile für Nutzer und Anbieter

Die vielen Vorteile des Cloud Computing können Repschläger zufolge aus zweierlei Blickwinkeln betrachtet werden: Der des Leistungsanbieters und der des Leistungsabnehmers. Für den Leistungsanbieter gilt auf der Infrastrukturebene, dass durch effiziente Ressourcenauslastung Kostenvorteile entstehen. Aufgrund von großen Kapazitätsmengen entstehen darüber hinaus Skalierungseffekte. IaaS Anbieter betreiben eigene Rechenzentren, die die Qualität der angebotenen Dienste global auf Basis verteilter Standorte sicherstellen. Auf der Plattformebene können PaaS Anbieter als Erweiterung des IaaS Angebots betrachtet werden. Sie stellen Basisdienste und die benötigte Applikationsinfrastruktur zur Verfügung. Auf der Plattform steht ein

standardisiertes Angebot zur Verfügung, das bei Bedarf von unabhängigen Herstellern erweitert werden kann. Diese Erweiterungen können dann auf einem Marktplatz angeboten werden. Durch diese Offenheit steigt die Anzahl der angebotenen Dienste und die Plattform wird attraktiver. Durch die Standards wiederum wird sichergestellt, dass die Abnehmer an diese Plattform gebunden sind. Auf Softwareebene gilt, dass SaaS Anbieter ihre Dienste auf Grundlage eines beschleunigten, flexiblen, skalierbaren und wartungsfreundlichen Anwendungsbetrieb anbieten. Eine Aktualisierung von einzelnen Anwendungen ist im Cloud Computing im Gegensatz zum klassischen IT-Betrieb ohne Störung des laufenden Betriebs möglich.

Die zwei größten Vorteile für Kunden, also den Leistungsabnehmer, bilden laut Repschläger die Kosteneinsparungen sowie die Flexibilität. Kunden von Cloud Services profitieren von einer geringen Kapitalbindung. Zudem bleiben hohe Anschaffungskosten von beispielsweise Hardware aus und die Komplexität der IT-Systeme wird heruntergefahren. Dadurch entsteht eine hohe Prozess- und Kostentransparenz. Für Unternehmen wird es dadurch einfacher, auf wechselnde Kapazitätsbedarfe flexibel zu reagieren. Dies liegt unter anderem an den kurzen Vertragslaufzeiten, den Pay-per-use Preismodellen und der skalierbaren Ressourcendeckung (Repschläger et. al., 2014).

Hentschel geht in seinem Werk noch auf weitere Potenziale des Cloud Computing insbesondere für die Nutzer ein und teilt diese ein in finanzielle, operative und strategische Vorteile. Die Vorteile von Cloud Computing aus finanzieller Sicht lassen sich in einzelne Aspekte aufteilen. Neben der wegfallenden Anschaffungskosten von Hard- und Software nennt Hentschel noch das Abrechnungsmodell als großen Vorteil für die Nutzer von Cloud Services. Nach dem verbrauchsabhängigen Kostenmodell wird nämlich nur für jene Leistungen gezahlt, die tatsächlich auch in Anspruch genommen wurden. Vor allem für kleine Start-Up Unternehmen, die noch über keine eigene IT-Infrastruktur verfügen, ist dies ein enormer Vorteil. Die Cloud ermöglicht ihnen nicht nur einen kostengünstigen Start, sondern bietet auch die Möglichkeit, bei erfolgsversprechenden Aussichten unkompliziert wachsen zu können. Die zunehmende Bündelung und Bereitstellung von Ressourcen für eine immer weiter wachsende Nutzerzahl der Cloud sorgt außerdem dafür, dass die Gesamtauslastung der jeweiligen Infrastruktur steigt. Dadurch sinken die Kosten pro Leistungseinheit, da zum Beispiel Kosten für Wartung und Betrieb auf die vielen Nutzer aufgeteilt werden können. Die größten operativen Vorteile für

Unternehmen sind die hohe Elastizität und Skalierbarkeit von Cloud Diensten. IT-Ressourcen wie beispielsweise Speicherkapazitäten lassen sich flexibel skalieren, erhöhen oder auch reduzieren. Je nachdem, was das Unternehmen gerade braucht. Auch wenn Unternehmen hauptsächlich eine eigene IT-Infrastruktur nutzen, können sie die Cloud Services zusätzlich für etwaige Lastspitzen als Reserve für einen bestimmten Zeitraum dazubuchen, ohne lange Vertragslaufzeiten eingehen zu müssen. Darüber hinaus wird die Komplexität der internen IT-Landschaften reduziert, sodass der Aufwand für Administration und Wartung für die Unternehmen sehr gering ist. Aus strategischer Sicht bringt der Einsatz von Cloud Computing vor allem den Vorteil, dass die Unternehmen keine unnötigen Energien mehr verschwenden müssen, indem sie sich Gedanken über die IT-Infrastruktur machen. Stattdessen können sie sich auf ihre Kernaufgaben konzentrieren und beispielsweise Geschäftsprozesse optimieren, die Wettbewerbsvorteile stärken und die Unternehmensziele weiter vorantreiben. Die Verantwortung für die Auswahl neuer IT-Services wird an Fachabteilungen delegiert, die auch tatsächlich mit den Services arbeiten und so über die nötigen fachlichen Kompetenzen verfügen, um neue Prozesse aktiv mitzugestalten. Ein weiterer Vorteil besteht in der gesteigerten Datensicherheit durch die Verteilung auf verschiedene Speichersysteme. Die Sicherstellung von Verfügbarkeit und Performance dieser Systeme trägt ebenfalls dazu bei. Die Einfachheit in der Ressourcenverfügbarkeit trägt dazu bei, dass Kunden unabhängiger von Anbieterunternehmen sind und nur kurzzeitige Verträge eingehen können (Hentschel et. al., 2018). Die folgende Abbildung zeigt die Hauptvorteile noch einmal im Überblick:

	Potenziale der Nutzung von Cloud Services
Finanziell	• Geringere Investitionskosten in eigene IT-Infrastruktur • Verringerung der Kapitalbindung • Niedrigere Betriebs- und Wartungskosten
Operativ	• Flexiblere, agilere und bedarfsorientiertere Skalierung der IT-Infrastruktur • Schnellere Realisierung von IT-Projekten, auch bei fehlendem Know-how • Reduzierter Administrations- und Wartungsaufwand • Ortsunabhängiger Zugriff
Strategisch	• Stärkung der Wettbewerbsvorteile sowie der Entwicklung neuer Geschäftsbereiche • Geringere Markteintrittsbarrieren (schnellere „Time-To-Market“) • Zugang zu Technologien, die bisher nur Großunternehmen zur Verfügung standen • Stärkung der Fachabteilungen durch höhere Verantwortung • Gesteigerte Datensicherheit und bessere Verfügbarkeit von IT-Systemen

Abbildung 12: Potenziale der Nutzung von Cloud Services

Big Data Applikationen

Liu geht in seinem Paper explizit auf die Vorteile von Cloud Computing für Big Data Applikationen ein. Der Hauptgrund, warum Unternehmen Cloud Services beanspruchen, sind ihm zufolge nicht etwa die Kosteneinsparungen, sondern die Steigerung der Unternehmensflexibilität. Die vorrangigen „Cloud Kandidaten“ seien Anwendungen, die nur wenig Integration beziehungsweise Umschreibung benötigen und, die keine sensiblen Daten beherbergen. Der Autor geht davon aus, dass Big Data Anwendungen die Zukunft der Cloud Technologien bestimmen werden. Derartige Anwendungen würden am meisten von den Cloud Vorteilen profitieren. Ein Geschäftsfall im Rahmen von Geschäftsflexibilität aufzubauen sei viel einfacher, als sich bloß auf den Faktor der Kostenersparnis zu fokussieren. Ein Schlüsselvorteil für Big Data Anwendungen in der Cloud ist zum Beispiel die schnelle Versorgung. Cloud Services sind stets sehr schnell verfügbar. Kein Mensch ist in den Bereitstellungsprozess involviert, sodass Kunden ihre Ressourcenanforderungen fast unmittelbar erfüllen können. Viele Unternehmen, die nicht mit Cloud arbeiten, benötigen für den Bereitstellungsprozess mehrere Monate. Bei Big Data Anwendungen verlängert sich dieser Prozess meist noch mehr, da sie mehr Investitionen benötigen, nämlich sowohl für die Infrastruktur der Hardware als auch für den Software

„stack“. Es ist einfach möglich, Dinge dynamisch in der Cloud bereitzustellen, ohne vorher dafür bezahlen zu müssen. Darüber hinaus können im Hintergrund dann auch Ressourcenanforderungen gesteigert werden, während die Anwendung läuft. Dies ist besonders für Echtzeit Big Data Anwendungen essentiell. Wenn der Zufluss an Daten rapide ansteigt und verarbeitet werden muss, werden einfach mehr Server bereitgestellt, um den neuen Workload bewältigen zu können. Ohne diese dynamische Skalierungskapazität würde die Servicequalität für den Kunden deutlich abnehmen. Anstelle von Investitionskosten, die man im Voraus tätigen muss, hat man in der Cloud die Möglichkeit, alles unter laufenden Kosten abzuwickeln und lediglich bedarfsgerechte Kosten zu verursachen. In der Cloud Umgebung zahlen Kunden also nur für die Menge der Ressourcen, die wirklich konsumiert werden. Big Data Anwendungen brauchen zwar viele Ressourcen für die Datenanalyse, aber sobald der Bericht generiert wurde, ist bis zur nächsten Berichtsperiode kein weiterer Ressourcenverbrauch nötig. Darüber hinaus bilden auch die reduzierten Betriebskosten einen enormen Vorteil. Um eine Anwendung zu bauen werden viele Komponenten benötigt, die nicht in Bezug stehen zu der Business Logik aber trotzdem notwendig sind, um die Anwendung zu starten und am Laufen zu halten (z.B. die Infrastruktur der Hardware aufsetzen, die Sicherheitsstrategie aufsetzen, die Database bereitstellen). All diese Aufgaben sind Voraussetzungen und müssen eingehalten werden, obwohl sie keinen direkten Mehrwert liefern. Die Cloud Anbieter bieten diese Aufgaben ebenfalls als Service an und ermöglichen so eine höhere Produktivität für die Entwickler der jeweiligen Unternehmen. Durch die Nutzung von managed Services in der Cloud können Unternehmen sich ganz auf ihre Differenzierungsmerkmale und das Kerngeschäft konzentrieren. Dadurch kann ein Unternehmen dann direkt mit einer Anwendung starten, ohne sich Gedanken darüber zu machen, beispielsweise einen separaten Database Administrator zu beschäftigen. Die Cloud kapselt die Komplexität für ihre Nutzer und hilft so auch dabei, die Automatisierung zu steigern. Durch ein hohes Maß an Automatisierung können sowohl Kosten gespart werden als auch der Replikationsprozess vereinfacht werden. So kann der Data Scientist schnell und unkompliziert ein separates Cluster bereitstellen, um beispielsweise eine neue Hypothese zu testen. Außerdem ist die Vielfalt an Services als einer der Vorteile von Cloud Computing zu nennen. Die Vielfalt an Big Data Problemen hat viele Innovationen der vergangenen Jahre inspiriert. Viele Database Systeme sind zwar open source, dennoch ist es viel leichter mit ihnen in einer Cloudumgebung zu experimentieren, als sie intern zu hosten. Darüber hinaus sind mehrere Systeme

nur als Cloud Services verfügbar. Durch die Vielfalt an Services wird auch die schnelle Zusammensetzung einer komplexen Anwendung viel einfacher (Liu, 2013).

5.2 Herausforderungen

Neben den vielen Vorteilen, die das Cloud Computing mit sich bringt, bestehen nach wie vor auch eine Reihe an Risiken bei der Cloud Nutzung durch Unternehmen. Sie verlieren beispielsweise bei der Migration von Anwendungen in die Cloud direkten Einfluss. Darüber hinaus bietet die zentrale Datenspeicherung eine große Angriffsfläche für Missbrauch. Die bis heute noch teilweise fehlenden Standards zu Integration und Migration erhöhen den Arbeitsaufwand. Hinzukommen fehlendes Vertrauen in Datenschutz- und Datensicherheitskonzepte seitens der Kunden. Teilweise besteht keine ausreichende Interoperabilität zwischen verschiedenen Cloud Diensten beziehungsweise fehlende Transparenz diesbezüglich. Wenn Unternehmen Cloud Computing einsetzen, stehen sie Herausforderungen in den Bereichen Technik, Recht und Organisation gegenüber. Das Stichwort Cloud Compliance spielt hierbei eine wesentliche Rolle. Mit der Abgabe der Verantwortung an Drittanbieter müssen die Regeln zur Nutzung und Bereitstellung der Cloud Services festgehalten, eingehalten und in der Unternehmensstrategie verankert werden. Darüber hinaus müssen die Unternehmen einen Aufwand zur Auswahl der einzelnen Cloud Services betreiben. Interessante Services müssen kategorisiert und bewertet werden, um sich kompetent und mit Hinblick auf eventuelle Risiken für oder gegen bestimmte Angebote entscheiden zu können. Um all diese Risiken möglichst gering zu halten ist es erforderlich, dass innerhalb des Unternehmens eine einheitliche Cloud Strategie entwickelt wird. Darauf aufbauend können dann entsprechende Cloud Dienstleister ausgewählt werden, die den Anforderungen des Unternehmens genügen (Hentschel et. al., 2018).

Um die vollen Potenziale des Cloud Computing ausschöpfen zu können, muss ein bestimmtes Grundgerüst mit speziellen Rahmenbedingungen seitens der Anbieter geschaffen werden. Damit Dienste und Softwareangebote flexibel und erweiterbar gehalten werden können, ist eine stringent implementierte, standardisierte und serviceorientierte Architektur (SOA) die Grundvoraussetzung. Die SOA ermöglicht es den Anbietern, verteilte und lose gekoppelte Dienste zu verwenden und die Anwendungsstruktur so zu gestalten, dass eine hohe Skalierbarkeit erreicht wird. Ohne standardisierte Schnittstellen der Marktplätze für Infrastruktur- und

Softwaredienste könnten die vielen Vorteile von Cloud Computing durch die erhöhte Komplexität und den Aufwand der Integration vernichtet werden. Die Cloud Migration stellt auch für die Anbieter von Cloud Services eine Herausforderung dar. Hierbei bilden Aspekte des Datenschutzes und der Datensicherheit einige Hürden, die es gilt zu überwinden. Um die Migration in eine Cloud Umgebung für Kunden attraktiv zu machen, betreiben die Anbieter einen Spagat zwischen effizienzfördernder Standardisierung zur Realisierung der Kostenersparnisse und den individuellen Kundenwünschen. Nicht jede cloudbasierte IT-Lösung ist automatisch kostensparend, sondern muss immer individuell den Kundenwünschen entsprechend analysiert werden. Bei der Migration in die Cloud muss die Vorgehensweise also mit Bedacht gewählt werden. Sie kann entweder komplementär umgesetzt werden oder den bisherigen IT-Betrieb gänzlich ersetzen (Repschläger et. al., 2014).

Neben den Risiken für Unternehmen und Anbieter geht Khan in seinem Paper noch auf mögliche Kostenfallen durch die Nutzung von Cloud Services ein. Demnach könnten mit dem Einsatz von Cloud auch mehr Kosten anfallen, da automatisierte Systeme fehleranfällig seien. Eine Downtime des Datenzentrums würde ein Unternehmen 5,600$ pro Minute kosten, so Khan. Bei einem veralteten Datenzentrum gehe man von 134 Minuten Downtime aus, das entspricht einem durchschnittlichen Verlust von 680,000$ (Khan, 2014). Natürlich muss bei der Berechnung der anfallenden Kosten die Größe der Daten sowie deren Sensibilität berücksichtigt werden. Dennoch soll der Ansatz von Khan hier genannt werden, da er einen weiteren Aspekt der Herausforderungen im Cloud Computing beleuchtet.

5.2.1 Sicherheitsaspekte

Datenmissbrauch

Heutzutage erfolgt sowohl die Datenspeicherung als auch die Datenverarbeitung größtenteils über die Nutzung von Cloud Diensten. Der maßgebliche Grund hierfür ist die enorme Kostenersparnis und Effizienzsteigerung durch die gemeinsame Nutzung von Ressourcen. Dazu kommt die Einfachheit des Zugriffs auf eben diese Daten per Internet über verschiedenste Geräte, die die Nutzung von Cloud Diensten für Endverbraucher und Unternehmen zunehmend attraktiver macht. Die Abrufbarkeit der Daten in der Cloud über das Internet birgt auch die Gefahr von Datenmissbrauch über internetbasierte Angriffe. In diesem Zusammenhang spielt

auch der Missbrauch von Identitäten eine immer größere Rolle. Ein solcher Missbrauch geschieht zum Beispiel, wenn Authentisierungsmedien (z.B. Passwort) eines Nutzers entfremdet werden. Laut Daten des US-amerikanischen Justizministeriums haben im Jahr 2014 rund 17,6 Mio. Bürger einen Identitätsmissbrauch in verschiedenen Bereichen des elektronischen Geschäftsverkehrs erfahren. Insbesondere der Onlinehandel und das Onlinebanking sind hierbei stark von Angriffen betroffen. Es ist also eine zentrale Aufgabe des Sicherheitsmanagements im Rahmen von Cloud Diensten, Daten vor dem Angriff unbefugter Dritter über das Internet zu schützen. Um dies zu gewährleisten bedarf es eines ausgereiften Identitätsmanagements. Das Identitätsmanagement unterliegt zahlreichen rechtlichen Anforderungen und ist somit eine Compliance Aufgabe, die sowohl Nutzer als auch Anwender von Cloud Diensten betrifft. Von Compliance wird als Erfüllung rechtlicher Anforderungen in einer Organisation gesprochen (Borges, 2018).

Angriffe auf das Cloud Computing

Golland et. al. gehen in ihrem Text detailliert auf die Arten von Missbrauchsfällen in Bezug auf das Cloud Computing ein. Demnach unterscheide man bei Angriffen auf das Cloud Computing von Außenstehenden zwischen zwei verschiedene Arten: Angriffe auf Systeme, bei denen die Authentisierung über Benutzername und Passwort erfolgt oder Angriffe auf Systeme, die mithilfe einer Zwei-Faktor-Authentifizierung geschützt sind. Die unterschiedlichen Schadensfälle würden dabei von dem jeweiligen Einsatzgebiet abhängen. Bei dem Einsatz in Unternehmen ist der größte Schaden wohl der zeitweilige Ausfall des laufenden Betriebs durch einen Angriff von außen. Die dauerhafte Verfügbarkeit der Cloud Dienste hat direkten Einfluss auf den Erfolg sowohl von Cloud Anbietern als auch Cloud Nutzern. Weiterhin besteht beim Einsatz in Unternehmen die Gefahr des Datenverlustes oder auch Datenmissbrauchs. Zudem könne dann die Vertraulichkeit der Daten nicht mehr garantiert werden. Hiervon ist zumeist nur der Cloud Nutzer und seine Kunden betroffen. Natürlich steht aber auch in diesem Szenario der Cloud Anbieter in einem schlechten Licht, da das Vertrauen der Nutzer und Kunden in seine Produkte Schaden nimmt. Bei Privatpersonen sind mögliche Schäden der Missbrauch von personenbezogenen Daten oder auch die unberechtigte Abbuchung von Geldbeträgen im Finanzwesen, zum Beispiel im Onlinebanking (Golland et. al., 2018).

Zugriffs- und Identitätsmanagement

Schilling geht in seinem Werk auf die Rollen des Zugriffs- und Identitätsmanagements ein. Um das Cloud Computing sicherer zu gestalten, können verschiedenste Sicherheitsaspekte berücksichtigt werden. Einer davon ist die Authentifizierung und die Einhaltung der damit einhergehenden Grundprinzipien. Im Cloud Computing muss bei allen Zugriffen auf Ressourcen die Identität der jeweiligen Person geprüft und der Zugriff authentifiziert werden. Hierfür gilt es, ein System zum Identitätsmanagement vorzulegen. Zunächst gibt die nutzende Person ihre Identität an. Diese bestätigt die Person dann mithilfe eines Berechtigungsnachweises (Authentisierung). Anschließend wird die Identität durch einen Kommunikationspartner im Authentifizierungsprozess bestätigt. Nur wenn die Identität der nutzenden Person eindeutig zugewiesen werden kann, erhält diese Zugriff auf die angeforderten Ressourcen (Autorisierung). Um diesen Ablauf zu erleichtern, wird jeder Person eine digitale Identität zugeordnet, welche mit spezifischen Zugangsberechtigungen hinterlegt ist. Das Zugriffsmanagement stellt im Cloud Computing ein Schlüsselelement für die Identifizierung dar. Von der Art des Zugriffs sind auch die Bedrohungs- und Schadensszenarien, die aus möglichen Angriffen resultieren, abhängig. Die meistgenutzte Zugriffsart ist aktuell die Einwahl ins System per Benutzername und Kennwort. Mittlerweile bieten jedoch bereits einige Cloud Anbieter zusätzlich noch die Möglichkeit der Zwei-Faktor-Authentifizierung an. Wenn eine besonders hohe Sicherheitsstufe erforderlich ist, wird auf die Zwei-Faktor-Authentifizierung zurückgegriffen. Dies geschieht beispielsweise durch Smartcards, elektronische Identitätsnachweise (eID) oder Single Sign-On (SSO) und kann die Sicherheit maßgeblich erhöhen. Die Identifizierung und Authentifizierung kann mit Hilfe von drei verschiedenen Faktoren erfolgen. Die drei möglichen Faktoren zur Identifizierung einer Person sind eine Wissensabfrage, biologische Eigenschaften der Person und die Authentifizierung über einen bestimmten Gegenstand. Die wissensbasierten Attribute können unterschiedlich stark sein, müssen aber mindestens ein Element beinhalten, das nur die zu identifizierende Person kennt. Die Sicherheit dieser Methode hängt grundlegend von der Geheimhaltungsfähigkeit des Nutzers ab. In der Praxis wird diese Methode sehr häufig verwendet, darunter fällt auch die Login Möglichkeit mittels eines Passworts. Untersuchungen haben jedoch gezeigt, dass die Passwortkomplexität meist nicht ausreichend ist und diese leicht durch Angriffe umgangen werden kann. Erfolgt eine Authentifizierung über biologische Eigenschaften einer Person werden biometrische Attribute, wie beispielsweise ein Fingerabdruck oder

eine Iriserkennung herangezogen. Auch hier gibt es allerdings Methoden, wie zum Beispiel ein Fingerabdruck repliziert werden kann, um so an gesicherte Daten und Ressourcen zu gelangen. Basiert die Authentifizierung ausschließlich auf dem Besitz eines speziellen Gegenstandes, ist eine eindeutige Identifizierung der nutzenden Person nicht möglich. Ein potentieller Angreifer könnte den Gegenstand entwenden und so die Identität der Person imitieren. Als Authentifizierungsmethode für Informationssysteme ist diese Methode daher meist nicht ausreichend. Die meisten Cloud Anwendungen verwenden zur Identifizierung von Personen die Wissensabfrage und ein Login über Benutzerkennung und Passwort erfolgt. Wenn aber aufgrund von höheren Sicherheitsanforderungen eine weiterführende Absicherung benötigt wird, so können mehrere Faktoren miteinander kombiniert werden. So kann das Risiko eines Angriffs minimiert werden. Bei den Amazon Web Services (AWS) ist beispielsweise eine Zwei-Faktor-Authentifizierung wählbar, jedoch nicht obligatorisch. Einige Anwendungen verwenden zum Beispiel digitale Zertifikate oder API Schlüssel (Schilling, 2018).

5.2.2 Rechtslage

Die Rechtslage im Zusammenhang mit der Nutzung von Cloud Computing ist leider bis heute nicht besonders spezifiziert. Stattdessen müssen Nutzer und Anbieter sich anhand anderer Rechte orientieren und jene Paragraphen herauskristallisieren, die auch auf das Cloud Computing anwendbar sind.

Datenschutzgesetz

Die größte Bedeutung für das Cloud Computing haben die Anforderungen des Datenschutzgesetzes, da oftmals personenbezogene Daten verarbeitet werden. Um beispielsweise die Abwehr von Identitätsmissbrauch und unbefugten Datenzugriffs sicherzustellen, ist es erforderlich, dass die Compliance eines Unternehmens über die rechtlichen Anforderungen an Schutzmaßnahmen Bescheid weiß. In der Rechtsprechung gibt es allgemeine rechtliche Anforderungen an das Cloud Computing, aus denen sich einige Informationen bezüglich des Identitätsmanagements herleiten lassen. Konkret festgeschrieben sind diese jedoch nicht. Aus den entsprechenden Absätzen des BDSG (Bundesdatenschutzgesetz) ergibt sich lediglich die Pflicht zur regelmäßigen Durchführung bestimmter Schutzmaßnahmen. Der Durchführungsbedarf dieser Schutzmaßnahmen ergebe sich aus einer Abwägung von Schutzbedarf und wirtschaftlicher

Zumutbarkeit eben dieser Maßnahme. Die hierin beschriebene Abwägung stellt hohe Anforderungen an die Adressaten dieser gesetzlichen Verpflichtung. Im Falle des Cloud Computing handelt es sich hierbei um Nutzer und Anbieter von Cloud Diensten. Da die Anforderungen nicht konkretisiert sind, besteht eine große Unsicherheit und viele Aspekte gelten als umstritten. Es gibt derzeit immer mehr Versuche, die Konkretisierung dieser Anforderungen voranzutreiben. So wurde beispielsweise gemeinsam mit dem Bundesministerium für Wirtschaft und Energie das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ gestartet. Hier soll ein Prüfstandard mit dem Ziel entwickelt werden, die datenschutzrechtlichen Anforderungen des BDSG für Cloud Dienste zu konkretisieren. Ergänzend kommen noch Regelungen zur IT-Sicherheit hinzu, die im Cloud Computing beachtet werden müssen. Die Festlegung des Schutzbedarfs von bestimmten Daten erfolgt auf Grundlage einer Risikoanalyse. Hierfür wird der Umfang eines möglichen Schadens durch Missbrauch berechnet. Für die IT-Sicherheitsstrategie eines Unternehmens spielt immer die Wahl geeigneter Maßnahmen der IT-Sicherheit eine wesentliche Rolle. Um die Wirtschaftlichkeit dabei nicht aus den Augen zu verlieren, muss hierfür eine Kosten-Nutzen-Analyse durchgeführt werden. Dabei liegt der Kern darin, welchen Sicherheitsgewinn eine bestimmte Maßnahme verspricht und welche Kosten sie auf der anderen Seite mit sich bringt. Eine zentrale Aufgabe der Compliance im Cloud Computing ist es, die bestehenden allgemeinen rechtlichen Anforderungen zur Datensicherheit speziell für das Identitätsmanagement zu konkretisieren. Entsprechend des gesetzlichen Rahmens müssen für das Konkretisieren von Anforderungen für das Identitätsmanagement branchenübergreifende und branchenspezifische Anforderungen voneinander unterschieden werden (Borges, 2018).

Vertragsrecht

Weiterhin sind auch Aspekte des Vertragsrechts für das Cloud Computing von Relevanz. Cloud Anbieter und Nutzer stehen in einem vertraglichen Verhältnis zueinander. In dem ausgehandelten Vertrag werden auch Pflichten im Rahmen des Identitätsmanagements festgehalten. Eine Haftung bei Pflichtverletzungen kann sich ebenfalls aus diesem Vertrag ergeben. Innerhalb der EU besteht die Regelung, dass Cloud Computing Dienstleistungen nach dem Recht des Landes verhandelt werden, in dem sich die Hauptniederlassung des Cloud Anbieters befindet. Eine Ausnahme stellt es dar, sollte der Cloud Nutzer gleichzeitig auch Verbraucher sein. Ist der entsprechende Cloud Dienst speziell auf Verbraucher mit Sitz im Ausland ausgelegt,

oder aber übt der Cloud Anbieter in diesem Land seine Tätigkeit aus, so gilt das Recht des jeweiligen Landes, in dem der Verbraucher ansässig ist. Generell ergibt sich in Bezug auf das Identitätsmanagement laut BGB eine Rücksichtnahmepflicht bezüglich der Rechte, Rechtsgüter und Interessen der jeweils anderen Vertragspartei. Insbesondere steht der Cloud Anbieter in der Verpflichtung, ein ausreichendes IT-Sicherheitsniveau zu gewährleisten. Er muss geeignete Maßnahmen ergreifen, um die Kundendaten vor Verlust oder Missbrauch zu schützen. Um die konkreten Maßnahmen im Einzelfall zu bestimmen, muss eine Risikoanalyse vorgenommen werden. Hierbei muss die Wahrscheinlichkeit möglicher Angriffe sowie die Sensibilität und die Menge der betroffenen Daten berücksichtigt werden. Auf der anderen Seite steht der Cloud Nutzer in der Verpflichtung, die zur Verfügung stehenden Authentisierungsmittel sicher aufzubewahren und deren Geheimhaltung sicherzustellen. Verwendet der Cloud Nutzer die angebotenen Dienste, um Daten seiner Kunden zu verarbeiten, so steht er wiederum seinen Kunden gegenüber in der Pflicht, einen Cloud Dienst zu wählen, der über ein ausreichendes Sicherheitsniveau verfügt. Auch aus dem Deliktsrecht lassen sich einzelne Aspekte für die Nutzung von Cloud Computing ableiten. Auch wenn Cloud Anbieter und Cloud Nutzer in keinem vertraglichen Verhältnis zueinanderstehen, besteht die Möglichkeit der Schadenregulierung. Im Rahmen des Deliktrechts werden Haftungen für unerlaubte Handlungen geregelt. Somit kann auch ein Geschädigter, der keinen Vertrag mit Cloud Anbieter oder Cloud Nutzer hatte, eine Entschädigung erhalten. Rechtlich gesehen wird hier jeweils das Recht des Ortes angewandt, an dem der Schaden entstanden ist. Dies ist bezogen auf das Cloud Computing jedoch fast unmöglich festzusetzen, da die Daten meist auf verschiedenen Servern an unterschiedlichen Standorten gespeichert sind. Somit kann kaum lokalisiert werden, wo genau ein Schaden entstanden ist. Eine alternative Lösung hierbei ist es, das jeweilige Recht des gewöhnlichen Aufenthaltsorts des Geschädigten heranzuziehen. Der Cloud Anbieter ist dazu verpflichtet, beispielsweise das Eigentum, die Immaterialgüterrechte oder auch die Persönlichkeitsrechte zu schützen, da er durch die Ansammlung an Datenbeständen eine potenzielle Gefahrenquelle eröffnet und ein mögliches Angriffsziel für Kriminelle erschafft (Verkehrssicherungspflichten). Diese Verkehrssicherungspflichten erfordern, dass ein ausreichendes IT-Sicherheitsniveau gewährleistet wird. Des Weiteren stehen Cloud Anbieter in der Verpflichtung, durch technische und organisatorische Maßnahmen sicherzustellen, dass kein unbefugter Zugriff auf die von ihnen genutzten technischen Einrichtungen erfolgen kann (Kriegesmann et. al., 2018).

Branchenspezifische und strafrechtliche Aspekte

Weitere Rechtsvorschriften, die im Cloud Computing Anwendung finden, sind spezielle branchenspezifische und auch strafrechtliche Aspekte. Beispielsweise in der Kreditwirtschaft oder auch im Versicherungssektor stehen Kreditinstitute in der Pflicht, bei der Auslagerung von Prozessen an Dritte angemessene Maßnahmen zu ergreifen, um die Entstehung von Risiken zu senken. Die Auslagerung von Prozessen ins Cloud Computing darf die Geschäftsorganisation des Kreditinstituts demzufolge nicht beeinflussen. Dies erfordert die Gewährleistung eines angemessenen Risikomanagements. Zudem müssen in einem vertraglichen Regelwerk umfassende Weisungs- und Kontrollrechte festgehalten werden. Eine besondere Herausforderung stellt das Cloud Computing bei Sozialversicherungsträgern dar. Hier muss laut Sozialgesetzbuch der mehrheitliche Teil des gespeicherten Datenbestandes beim öffentlich-rechtlichen Auftraggeber verbleiben. Dies schränkt die Cloud Lösung maßgeblich in ihrem Nutzen und ihrer Praktikabilität ein. Für manche Berufsgruppen, zum Beispiel Ärzte, müssen noch einzelne Gesetze, etwa zur Geheimhaltungspflicht, berücksichtigt werden. Bislang war die Gesetzeslage hierbei so, dass die Speicherung und Verarbeitung von entsprechenden Daten im Rahmen von Cloud Lösungen als unerlaubte Weitergabe dieser Daten an den Cloud Anbieter gewertet wurde und somit strafbar war. Hier wurden bereits mehrere Lösungsansätze erarbeitet, jedoch konnte bislang keiner zu einer Lösung des Problems verhelfen. Einen Lichtblick gibt es diesbezüglich seit der Neuregelung des entsprechenden Paragraphen im Strafgesetzbuch, welcher die Nutzung von Cloud Computing immer dann als legal einstuft, wenn sie erforderlich ist. Somit trägt weiterhin der jeweilige Berufsgeheimnisträger ein Restrisiko der Straffälligkeit, welches dann individuell bewertet werden muss (Kriegesmann et. al., 2018).

Anforderungen an das Cloud Computing

Aus den genannten Rechtsvorschriften, die für das Cloud Computing von Relevanz sind, lassen sich nun konkretere Anforderungen ableiten. Aus dem Recht ergeben sich zahlreiche Anforderungen und Verpflichtungen an die IT-Sicherheit für den Cloud Anbieter. So muss er beispielsweise eine Firewall einrichten, eine Verschlüsselungstechnik, ein Monitoring-System und eine Notfallstrategie implementieren. Die Benennung weiterer konkreter Maßnahmen ist abhängig von dem jeweiligen Nutzungsszenario und muss individuell beurteilt werden. Vertraglich gesehen, ist der Cloud Anbieter darüber hinaus dazu verpflichtet, sichere Authentifizierungs-

systeme zu implementieren. Allgemeingültige Aussagen zu dem erforderlichen Schutzniveau sind hier allerdings schwer zu tätigen. Stattdessen muss eine Abwägung nach unterschiedlichen Schutzbedürfnissen stattfinden. Kriterien, anhand derer Cloud Anbieter den Schutzbedarf ermitteln können, sind beispielsweise die Sensibilität der verarbeiteten Daten oder die Gefahr des Missbrauchs. Nun müssen die jeweils empfohlenen wirtschaftlichen Anforderungen einer rechtlichen Prüfung unterzogen werden. Je nach Budget des Unternehmens und Schutzbedürfnis der entsprechenden Daten kann hier eine Diskrepanz zwischen ökonomischem Ideal und rechtlicher Gebote aufkommen. Vor allem dann, wenn ein hoher Schutzbedarf mit einem niedrigen Unternehmensbudget zusammentrifft. Beispielsweise das Datenschutzgesetz setzt diesbezüglich sehr hohe Maßstäbe und gibt vor, dass ein festgelegtes Sicherheitsniveau bei der Verarbeitung personenbezogener Daten nicht unterschritten werden darf. Des Weiteren muss bei sensiblen personenbezogenen Daten die Authentifizierung mittels Zwei-Faktor vollzogen werden (Kriegesmann et. al., 2018).

6 Landing Zone in der Cloud

Eine Landing Zone, auch Cloud Landing Zone (CLZ), sollte stets zu Beginn einer Cloud Reise eingerichtet werden. Um den Begriff der Landing Zone anschaulicher zu machen, kann der folgende Vergleich einer Cloud Plattform mit einer Stadt sehr hilfreich sein. In diesem Beispiel steht die Cloud Landing Zone stellvertretend für einen Bauplan, der die wesentliche Infrastruktur der Stadt beschreibt. Sie stellt sicher, dass die Stadt wachsen kann und sich in einer gut organisierten Weise entwickelt. Mit diesem Bauplan wird sichergestellt, dass beim Hinzufügen neuer Abschnitte und Dienste in der Stadt, die Einwohner jederzeit wissen, wohin sie führen und wie sie in Bezug auf alles, was bereits vorhanden ist, eingerichtet werden können. Die Festlegung dieses Gerüsts als Grundlage erleichtert später die Lösung komplexerer Probleme. Die Einrichtung einer Multi Account Landing Zone vereinfacht wiederum unter anderem Cloud Governance, Compliance und Security. In dem folgenden Abschnitt soll eine Übersicht über die Landing Zone in der Cloud erstellt werden, ehe genauer auf die Multi Account Umgebung eingegangen wird. Anschließend sollen verschiedenste Aspekte von Cloud Governance beleuchtet werden. Als ein Bestandteil einer Landing Zone spielt auch die Cloud Governance eine wichtige Rolle, um die Cloud Computing Adoption und Implementierung zu regeln. Analog zu dem Stadtbeispiel kann Cloud Governance stellvertretend als Politik der Stadt betrachtet werden.

6.1 Übersicht Cloud Landing Zone

Unter einer Landing Zone in der Cloud versteht man eine vorkonfigurierte, sichere Multi Account Umgebung. Sie bildet das Fundament für den Start in der Cloud, für neue Entwicklungen, Experimente oder Migrationen. Eine Landing Zone muss folgende Eigenschaften besitzen:

- Sicherheit und Konformität
- Skalierbarkeit und Resilienz
- Adaptierbarkeit und Flexibilität

Die üblichen Ergebnisse, die dadurch erzielt werden, sind die Folgenden:

- Reduzierte Kosten durch die Migration in die Cloud
- Agilität durch die reduzierte Zeit von der Planung bis zur Umsetzung
- Verbesserte Sicherheit durch eine sichere und konforme Umgebung
- Globale Präsenz durch die Nutzung bestehender globaler Infrastruktur
- In der Entwicklung kann sich auf das Kerngeschäft fokussiert werden

Die Konfigurierung einer Landing Zone ist komplex. So müssen viele Entwurfsentscheidungen getroffen werden, die Konfiguration von vielen Accounts und Diensten muss erfolgen, es muss eine Sicherheitsgrundlage erstellt werden sowie Benutzerzugriffe und Berechtigungen eingerichtet werden. Bei dem Entwurf einer Landing Zone werden zumeist die folgenden Überlegungen angestellt:

- Sicherheits- und Ressourcengrenzen
- API Limits und Throttling
- Abrechnungstrennung
- Multiple Teams
- Isolation
- Sicherheitskontrollen
- Businessprozesse

All diese Aspekte müssen bei dem Entwurf einer Landing Zone Beachtung finden (Internetquelle AWS Landing Zone & Azure Landing Zone).

6.2 Multi Account Umgebung

Die folgende Abbildung zeigt das Design einer typischen AWS Landing Zone. AWS ermöglicht es seinen Kunden, schneller zu experimentieren und zu skalieren und bietet gleichzeitig eine flexible und sichere Cloud Umgebung. Wenn Kunden Workloads erstellen und

bereitstellen, verwenden sie häufig mehrere Accounts, um ihre Ressourcen zu isolieren, da sie Grenzen für Sicherheit, Zugriff und Abrechnung bieten. Benutzer haben außerhalb Ihres Accounts standardmäßig keinen Zugriff auf Ihre Ressourcen. Ebenso werden die Kosten der von ihnen verbrauchten AWS Ressourcen nur Ihrem Account zugewiesen. Auch wenn ein AWS Account mit nur einem einzigen Account erstellt werden kann, wird empfohlen, mehrere Accounts einzurichten, wenn die Workloads an Größe und Komplexität zunehmen.

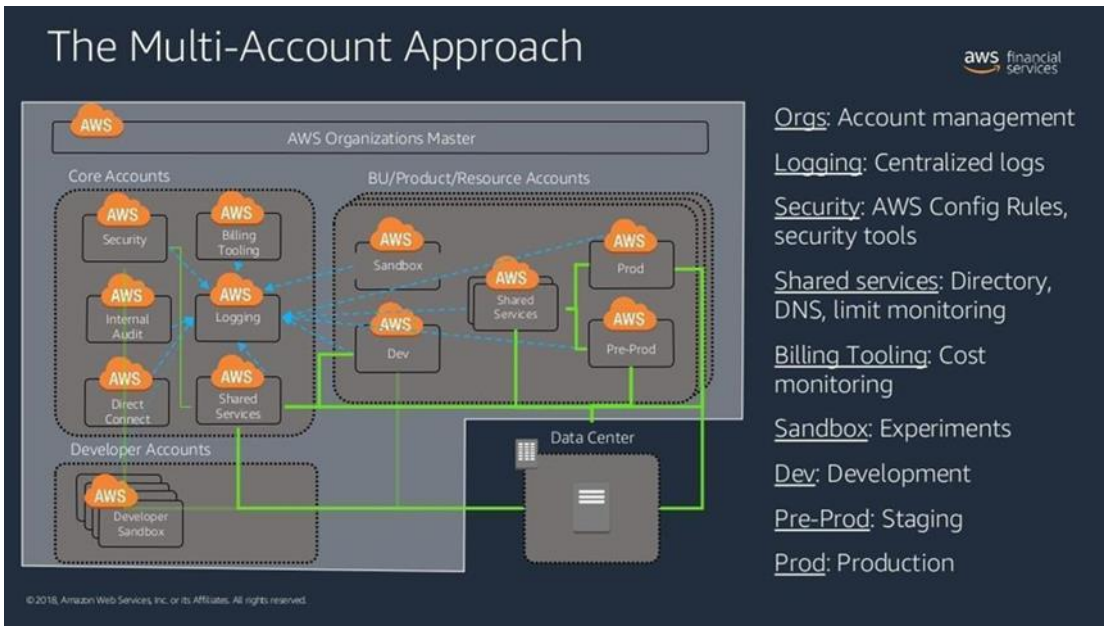

Abbildung 13: Typischer Aufbau einer Landing Zone

Als erste Annäherung an das Thema Landing Zone dient in dieser Arbeit die Ausarbeitung einer zentralen Account Management Lösung (siehe Abschnitt 7). Die Verwendung einer Umgebung mit mehreren Accounts ist eine bewährte Methode, die schnelle Innovation mit unterschiedlichen Anforderungen ermöglicht. So können Accounts beispielsweise Teams, Workloads oder Produkten zugeordnet werden. Separate Accounts können benutzerdefinierte Umgebungen bereitstellen und den unterschiedlichen Sicherheitsanforderungen der einzelnen Teams gerecht werden. Auch die Abrechnung kann mit dieser Vorgehensweise erleichtert werden. Die Verwendung mehrerer Accounts vereinfacht die Zuweisung von AWS Kosten, da genau ermittelt werden kann, welche Projekte oder Services für AWS Gebühren verantwortlich sind. Auch Sicherheitskontrollen werden durch die Verwendung einer Umgebung mit mehreren Accounts flexibler. Es können Gruppierungsmechanismen erstellt werden, um

sicherzustellen, dass bestimmte Accounts die geltenden Compliance Anforderungen erfüllen. Darüber hinaus wird die Anpassung an Geschäftsprozesse vereinfacht. Die Verwendung mehrerer Accounts ermöglicht es, die IT-Infrastruktur eines Unternehmens so einzurichten, dass die Bedürfnisse der Geschäftsprozesse und Anforderungen erfüllt werden. Letztendlich ermöglicht es die AWS Umgebung mit mehreren Accounts, die Cloud zu nutzen, um schneller voranzukommen und differenzierte Produkte und Dienstleistungen zu entwickeln, während gleichzeitig Mechanismen bereitgestellt werden, um dies auf sichere, skalierbare und widerstandsfähige Weise zu tun (Internetquelle AWS Organizations Best Practices).

6.3 Cloud Governance

Neben den genannten Aspekten spielt auch die Cloud Governance eine immer wichtigere Rolle, da die Cloud Computing Lösungen in der aktuellen Zeit immer komplexer werden und struktureller Unterstützung bedürfen. Es stellt sich die Frage, wie die Cloud geführt werden soll oder welche Richtlinien in der Cloud Anwendung finden. Governance Strategien beinhalten die Gründung von Verantwortlichkeiten und die Inkraftsetzung der jeweils verantwortlichen Partei. Eine Landing Zone kann ein sinnvoller Bestandteil von Cloud Governance sein, weshalb es an dieser Stelle näher erläutert werden soll.

Cloud Computing Governance ist definiert als eine Reihe von Prozessen, Verantwortlichkeiten und Verfahren, die genutzt werden, um die Cloud Computing Adoption und Implementierung zu regeln und zu kontrollieren. Dabei müssen bestimme Regelungen und Prüfungsprozeduren berücksichtigt werden. Eine Cloud Governance Strategie ist also für Unternehmen unumgänglich, um die Geschäftsziele und -vorgaben zu erreichen, eine preisgünstige Auslieferung zu gewährleisten, die Sicherheit zu verbessern und eine angemessene Entscheidungsfindung zu ermöglichen. Die folgenden Kernelemente werden von den Autoren Bounagui et. al. für die Einführung beziehungsweise Erarbeitung eines Cloud Computing Governance Ansatzes empfohlen: das effektive Management von Cloud Computing Sicherheitsrisiken muss sichergestellt werden; kritische Geschäftsprozesse müssen kontinuierlich fortgeführt werden; klare Geschäftsziele müssen bereits zu Beginn kommuniziert werden; die neue Cloud Computing Governance muss in bereits existierende Geschäfts-IT Governance-Systeme integriert werden; die Umformung von IT-Regeln und Entscheidungen hin zu Richtlinien muss sichergestellt

werden; Flexibilität, Skalierbarkeit und die Services der Cloud müssen angepasst werden, um dem Unternehmen zu erlauben, neue Möglichkeiten zu kreieren und Kosten zu reduzieren; eine Vielzahl von Regulierungen müssen gehandhabt werden (Bounagui et. al., 2015).

Strategie zur Steuerung der Cloud

Bezogen auf Cloud Governance stellt sich die zentrale Frage, wer für die Steuerung der Cloud verantwortlich ist. Der Cloud Anbieter alleinig oder ist es eine geteilte Aufgabe zwischen dem Anbieter und dem Nutzer? Für Thuraisingham steht fest, dass jeder Cloud Anbieter zumindest eine Strategie zur Steuerung der Cloud vorhalten muss. Diese müsse Aspekte umfassen, wie beispielsweise, ob die Cloud kompatibel mit den jeweils vorherrschenden Regularien und Gesetzen ist. Außerdem müssen Informationen über die Sicherheits- und Privatsphärebestimmungen enthalten sein. Darüber hinaus sollte der Anbieter ein Statement bezüglich der Betriebsbereitschaft der Cloud darin abgeben. Neben dem Anbieter steht aber auch die jeweilige Firma, die die Cloud nutzen möchte, in der Verantwortung. Diese muss beispielsweise sicherstellen, dass nicht nachlässig mit der Cloud umgegangen und diese etwa durch Schadprogramme beschädigt wird. Außerdem muss das Unternehmen alle Bestimmungen, die durch die Cloud in Kraft treten befolgen, sowie die Mitarbeiter im Hinblick auf den Umgang mit der Cloud weiterbilden. Abschließend muss das Unternehmen einen festen Ansprechpartner für die Kommunikation mit dem Anbieter festlegen. Diese Person sollte eine feste Rolle im Unternehmen einnehmen. Die maßgeblichen Aspekte von Cloud Governance sind der Schutz der Cloud gegen Cyberangriffe, die Integration künstlicher Intelligenz, die Cyber-Risiko-Versicherung und die Wahl der Cloud Strategie. Der Schutz der Cloud gegen Cyber Angriffe und Privatsphäreverletzungen sollte die höchste Priorität in der Steuerung der Cloud einnehmen, sowohl für den Anbieter als auch für den Nutzer. Es müssen Überlegungen dazu angestellt werden, wie die Privatsphäre geschützt werden kann, wenn erstmal alle Daten in der Cloud gespeichert sind. Des Weiteren muss bedacht werden, wie die Daten vor Diebstahl oder Missbrauch geschützt werden können. Die Anbieter müssen in Zuge dessen eine Versicherung für diese Sicherheitsaspekte bieten können. Die Integration von künstlicher Intelligenz, Cyber-Sicherheit und die Cloud gehen stets Hand in Hand. Dies beruht darauf, dass immer mehr Unternehmen KI-Techniken anwenden, um ihre Produkte zu entwickeln. Manche Unternehmen benutzen die Cloud ebenfalls, um die KI-Algorithmen auszuführen, da hier eine bessere Performance gewährleistet

wird. Natürlich können sowohl die Cloud als auch die KI-Techniken angegriffen werden. Daher ist es erforderlich, dass die Sicherheit des Betriebs ständig gewahrt wird. Abschließend muss die Cloud Strategie sowohl mit der KI-Strategie als auch mit der Cybersicherheits-Strategie des Unternehmens integriert werden. Ein weiterer Bestandteil von Cybersicherheit ist die Cyber-Risiko-Versicherung. Die Idee hierhinter ist eine Risikoanalyse für verschiedenste Rechensysteme mit Bezug zu Cyberangriffen durchzuführen. Im Anschluss sollen dann verschiedene Risikomodelle angeschaut werden, um die Höhe der Versicherung berechnen zu können. Aus Anbietersicht besteht das Risiko hierbei nicht bloß in potenziellen Angriffen auf das System, sondern auch in Bezug auf Ausfallzeiten und Konformität. Der Anbieter muss beispielsweise bei der Risikoabwägung berechnen, wie viele Stunden in der Woche die Cloud in Betrieb sein wird. Dies muss ebenfalls in den Vereinbarungen mit dem Nutzer festgehalten werden. Im Falle des Nichteinhaltens dieses Versprechens muss der Anbieter also eine entsprechende Versicherung erwerben. Das Unternehmen, welches die Cloud nutzt, muss wiederum eine Versicherung abschließen, um die Qualität seines Produktes für die eigenen Kunden zu garantieren (Thuraisingham, 2020).

Problemfelder

Auch Linthicum hat sich in seinem Paper mit dem Thema Cloud Governance auseinandergesetzt. Er beschreibt zunächst aktuelle Probleme in Bezug auf Cloud Governance. Diese würden vor allem die Bereiche Service Location, Abhängigkeiten, Überwachung und Sicherheit betreffen. Viele Services, die von Unternehmen genutzt werden, werden nicht von den jeweiligen Unternehmen selbst betrieben, sondern sind cloudbasiert. Daher müssen ständige Kontrollen erfolgen, um mögliche Risiken zu minimieren. Die Notwendigkeit von Kontrollen steigt in Anbetracht des regulatorischen Drucks der verschiedenen Ebenen. Serviceorientierte Architekturen platzieren eine Ebene mit verschiedenen Prozessen und Technologien um den Service herum, sodass jegliche Störfaktoren, wie beispielsweise ausfallende Services, schnell erkannt werden können. Dieses Wissen bemächtigt das Unternehmen wiederum dazu, Handlungen zur Behebung des Problems zu ergreifen oder etwa eine selbstkorrigierende Technologie einzusetzen. Eine derartige Architektur ist eine Kombination aus serviceorientierten Architekturen und Cloud Computing. Es erfordert die Erstellung einer Reihe von Services, die ausgebildet werden, um Geschäftslösungen zu erstellen. Diese Services können entweder aus dem hauseigenen

Rechenzentrum oder aus der Cloud sein. Die Nutzung kann entweder über eine Applikation oder Prozesse stattfinden. Wichtig ist nur, dass diese Aspekte stets für den Nutzer transparent sind. Eine solche Lösung hat enormen Wert bezogen auf Beweglichkeit und die Fähigkeit eine Geschäfts-IT mit extrem reduzierten Kosten zu betreiben. Viele der verwendeten Services rufen wiederum andere Services ab oder es gibt einen Serviceverbund. Services, die Ausfälle haben oder sich unautorisiert verändern, lösen einen Dominoeffekt auf andere Services und die darauf basierenden Applikationen aus. Daher muss immer die Kettenreaktion bedacht werden, die durch die Anpassung eines einzelnen Service ausgelöst werden kann. Der Einsatz von Service Governance Ansätzen und der dazugehörigen Technologie kann derartige Risiken mildern. Durch das Platzieren verschiedener Kontrollmechanismen um die verschiedenen Services herum, können alle Services, egal ob On-Premise oder in der Cloud, während ihrer Laufzeit überwacht werden. Die Grundvoraussetzung hierfür ist, dass das Unternehmen versteht, an welcher Stelle und in welchem Umfang derartige Kontrollmechanismen Sinn machen und wo nicht. Manche Services benötigen lediglich eine Statusmeldung „aktiv/inaktiv“, während andere hingegen eine Überwachung der jeweiligen Performance (inklusive Datenbanken- und CPU-Nutzung) nötig haben. Darüber hinaus müssen diese Daten wiederum als ein Service bereitgestellt werden, damit sie in eine örtliche Governance Lösung integriert werden können. Manche Governance Anbieter bieten zusätzlich grundlegende Sicherheits Services an. Diese beinhalten meistens die Nutzung von Identitätsmanagement, rollenbasierte Sicherheit und Unterstützung beim Datensammeln und der Rechnungsprüfung. Wenn Unternehmen sich ein Sicherheitspaket im Rahmen der Cloud Governance aussuchen, müssen einige Aspekte berücksichtigt werden. Die gewählte Sicherheitslösung muss immer für die zu beschützende Applikation und Information angemessen sein. Hier gilt es eine Balance zwischen Sicherheit und betrieblicher Effektivität zu schaffen. Darüber hinaus sollte der Sicherheitsansatz für den Anwendungsfall kreiert werden. Dabei muss bedacht werden, in welchem Ausmaß Sicherheit auf den verschiedenen Ebenen des Systems benötigt wird (Linthicum, 2015).

Macropolicies

Weiterhin geht Linthicum noch auf verschiedene Arten von Richtlinien (Policies) ein, die innerhalb einer Cloud Governance Strategie beachtet werden müssen. Man könne diese unterscheiden zwischen Macropolicies (Generelle Regelungen) und Micropolicies (Bestimmungen,

die spezifisch für einen bestimmten Service sind). Macropolicies werden typischerweise von kreiert, um größere Problembereiche, die mehrere Services, Daten, Prozesse und Anwendungen betreffen, zu beheben. Beispiele dafür könnten sein: On-Premise Services müssen innerhalb von 0.05 Sekunden antworten, Cloud Computing basierte Services müssen innerhalb von 0.10 Sekunden antworten; Eine Führungsperson muss Änderung an Prozessen zustimmen; Alle Services müssen auf Grundlage von Java gebaut werden. Neben einfachen Grundregeln können Macropolicies auch kleinschrittigere Vorgaben enthalten, beispielsweise eine 20-schrittige Anleitung dazu, wie eine Datenbank verändert werden muss oder der Prozess einer Neuregistrierung von einem Nutzer auf einer Cloud Computing Plattform. Diese Vorgaben variieren natürlich je nach Unternehmen und Führungsriege. Es geht dabei um grundsätzliche Regeln, die festlegen, wie das System entwickelt, verändert und überwacht wird. So können Risiken minimiert werden während Kosten gespart werden. Dies hat innerhalb eines Unternehmens einen enormen Wert. Wichtig bei der Arbeit mit Macropolicies ist es, das Gleichgewicht nicht zu verlieren. Es sollten genügend Vorgaben gestellt werden, um die Sicherheit zu garantieren aber auch nicht so viele, dass die Produktivität darunter leidet. Ein guter Anhaltspunkt dafür sei, dass sich das IT-Department eines Unternehmens ungefähr 5% der Arbeitszeit mit Themen rund um Macropolicies beschäftigen sollte.

Micropolicies

Micropolicies oder servicebasierte Policies beschäftigen sich typischerweise mit einem speziellen Regelfall, der einen bestimmten Service, Prozess oder Datenelement betrifft. Micropolicies legen fest, wie eine Vorgabe auf der niedrigsten Ebene ausgeführt werden soll. Beispiele dafür könnten sein: Nicht mehr als eine Anwendung, ein Service oder ein Prozess kann zur selben Zeit auf den Service XY zugreifen; Das XY-Datenelement kann ausschließlich von Mitarbeiter XY bearbeitet werden und nicht von allen Entwicklern; Die Antwortzeit des XY-Service muss unter 0.0001 Sekunden liegen. Servicebasierte Policies sind typischerweise innerhalb der Service Governance Technologie implementiert. Um den Wert von Governance für ein Unternehmen zu beschreiben, ist es notwendig einige Kernaspekte zu beleuchten. Zunächst müssen die Gesetze und Regelungen, die von außen auf das Unternehmen und speziell die Abteilung einwirken, in Betracht gezogen werden. Automatisierte Vorgaben im Rahmen des Governance Modells sollen dafür sorgen, dass externe Gesetze und Regeln eingehalten werden.

Der Einsatz einer Governance Struktur sollte immer direkt mit dem vorhandenen Sicherheitssystem verknüpft sein und sowohl diesem als auch dem Unternehmen im Ganzen einen Vorteil bringen. Governance- und Sicherheitssysteme arbeiten Hand in Hand, um sicherzustellen, dass die unternehmensinternen Informationen beschützt werden und nur von befugten Personen eingesehen werden können. Beweglichkeit beziehungsweise die Möglichkeit Dinge zu verändern, erlaubt es dem Nutzer schnell zu reagieren und Konfigurationen am System vorzunehmen, um den Anforderungen des Unternehmens zu entsprechen. Das bedeutet, dass es möglich sein muss, neue Cloud Computing Services ohne großen Aufwand hinzuzufügen oder nicht mehr relevante Services zu entfernen. Der Einsatz von Governance erleichtert diesen Prozess. Betriebliche Kontrolle heißt in diesem Kontext, dass die Produktion von lokalen und cloudbasierten Services während des Betriebs kontrolliert werden können. Dies befähigt die IT-Abteilung dazu, die Services während der Produktion zu managen und zu überwachen. Dabei soll sichergestellt werden, dass die Services korrekt funktionieren und sich dabei an die Vorgaben der IT halten (Linthicum, 2015).

7 Umsetzung Projekt

Im Folgenden soll die Entwicklung der in der Einleitung beschriebenen Anwendung zum zentralen Account Management vorgestellt werden. Es handelt sich dabei um eine automatisierte Accounterstellungslösung, die auf einer Serverless Architektur basiert und über APIs konsumiert werden kann. Zunächst sollen die für die Anwendungsentwicklung genutzten Cloud Technologien vorgestellt werden. In den darauffolgenden Abschnitten sollen die einzelnen Aspekte der Projektentwicklung dargestellt werden. Dabei soll auf die einzelnen Entwicklungsschritte während der Anwendungsentwicklung eingegangen werden. Zur Veranschaulichung der verschiedenen Entwicklungsschritte der Applikation werden Screenshots der Anwendungsumgebung hinzugezogen.

7.1 Herangehensweise

Die Gründe für die Umsetzung dieses Projektes sind, dass jedes Unternehmen, das die AWS Cloud nutzen möchte, dazu in der Lage sein sollte, AWS Accounts einfach einzurichten. Darüber hinaus kann durch die Nutzung einer zentralen Account Management Lösung eine Reihe von Accounts für verschiedenste Zwecke eingerichtet werden, die wiederum zentral gesteuert werden können. Die Anwendung sollte möglichst ein Self-Service sein, der es ermöglicht, schnell auf Kundenanforderungen zu reagieren. Erfolg hat dieses Projekt erst dann, wenn ein nutzbarer Service kreiert wurde, der AWS Accounts mit Rückbuchungsfunktionalität und einer konsolidierten Abrechnung produziert.

Es folgt eine tabellarische Übersicht der Roadmap, die für das Zeitmanagement des Projektes erstellt wurde:

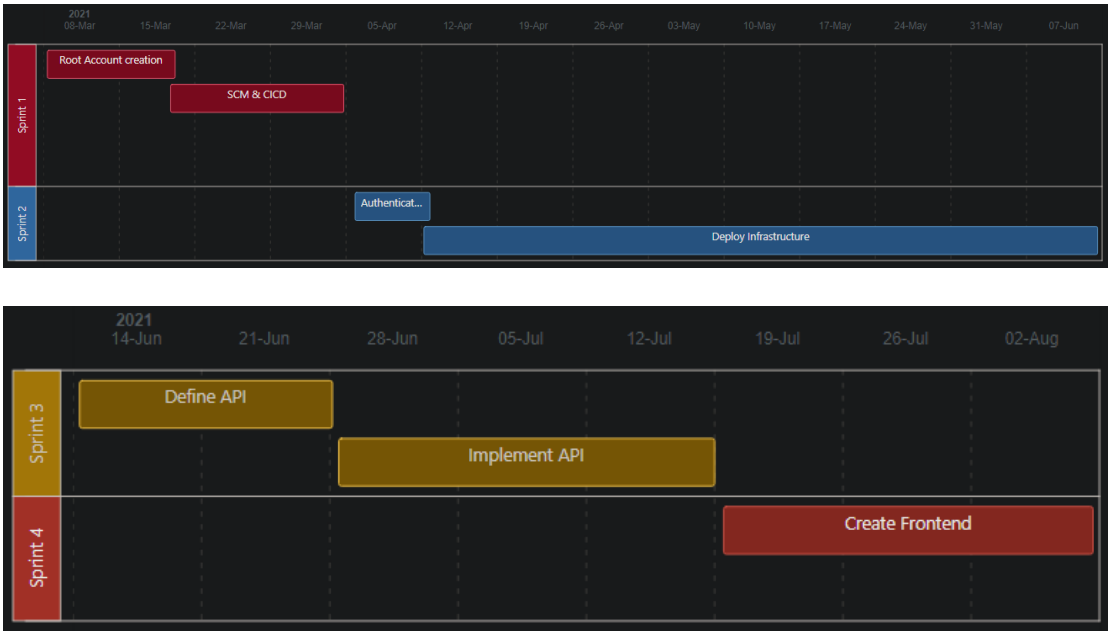

Abbildung 14: Roadmap des Projekts

Außerdem wurde eine Übersicht über den Umfang mit einer detaillierten Roadmap erstellt, um einen Überblick über die zu erledigenden Teilschritte zu gewähren:

Feature	Initiative	Priority	Effort	Notes
SCM	Operational Excellence	HIGH	LOW	Define the SCM structure, define and identify the number of repositories, align the structure and automation approach
CICD	Operational Excellence	HIGH	LOW	Determine the schedule of key operations, align on a common approach for CICD
Authentication and Authorization	Security	HIGH	MEDIUM	Cognito, IAM Solution
Account Factory	Performance Efficiency	HIGH	HIGH	Creates AWS accounts and places them in organizational units
Service API	Performance Efficiency	HIGH	HIGH	Swagger definition of the API, API infrastructure
Bootstrap IAM user	Security	HIGH	MEDIUM	Bootstrap an IAM user into the vended account

Tabelle 1: Überblick über die Teilschritte des Projekts

Anschließend folgt eine Übersicht zu Aufgaben, die außerhalb des Projektumfangs liegen:

Feature	Initiative	Priority	Effort	Notes
Reporting	Cost Optimisation	HIGH	HIGH	Monthly reports, Account breakdown
SCP Security Policies	Security	HIGH	MEDIUM	Automate account wide policies
Notification Mechanism	Operational Excellence	HIGH	MEDIUM	Account wide notification
Monitoring	Reliability	HIGH	HIGH	Cloudwatch metrics and alarms for the estate
DevSecOps Config Rules	Security	MEDIUM	HIGH	Automated inspection based on rules
Config Rules	Operational Excellence	MEDIUM	MEDIUM	Leverage AWS config rules across the estate
Guard Duty Enablement	Security	MEDIUM	MEDIUM	Enablement of guard duty
Centralised Logging	Operational Excellence	LOW	HIGH	Centralised the consumption of logs from across the estate
Trusted Advisor	Cost Optimisation	MEDIUM	MEDIUM	Leverage trusted advisor for cost

Tabelle 2: Aufgaben außerhalb des Projektumfangs

Zur Veranschaulichung der geplanten Architektur, dient die folgende Abbildung:

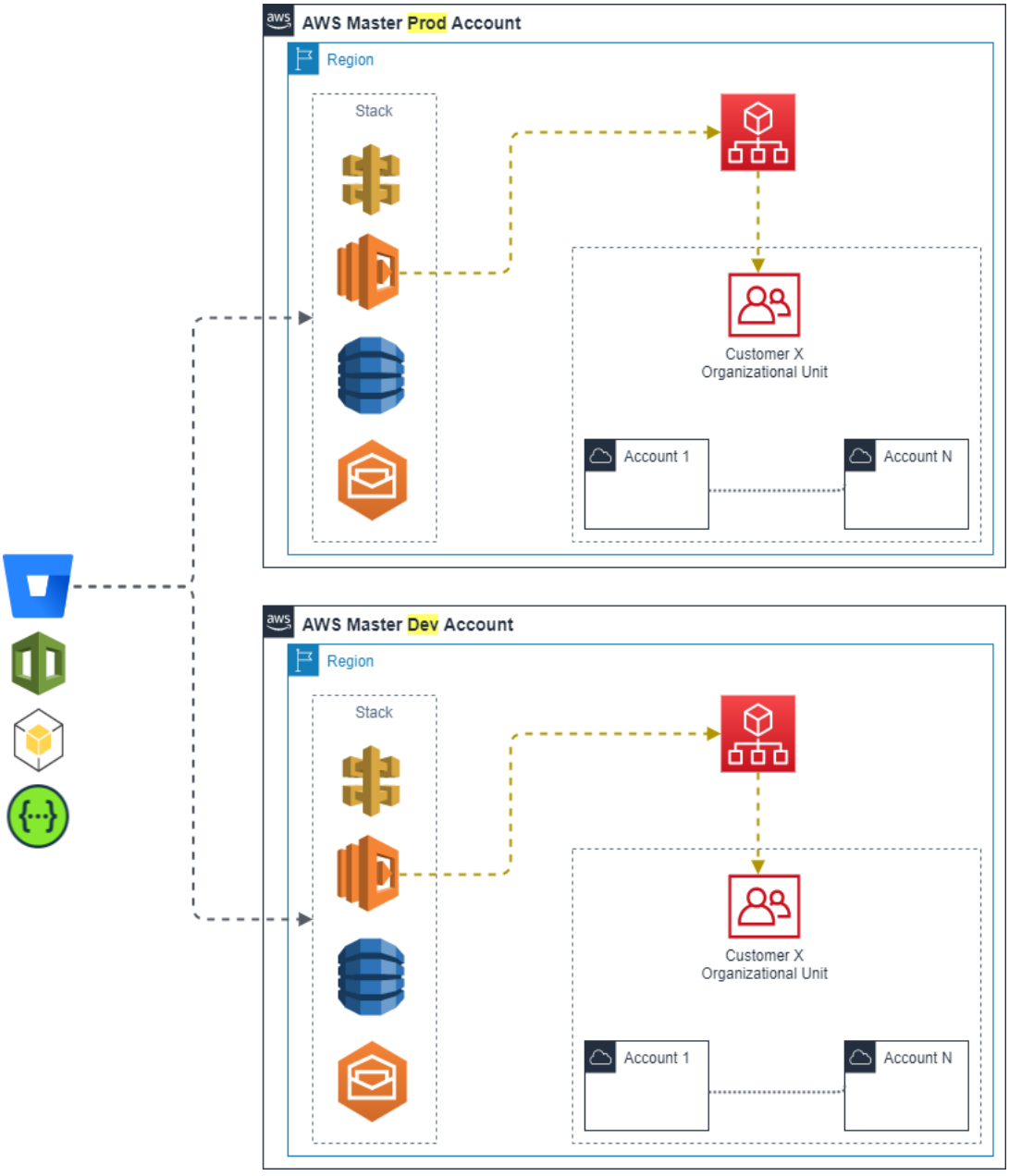

Abbildung 15: Geplante Projektarchitektur

In der folgenden Tabelle werden noch die unterschiedlichen Komponenten der Architektur und deren jeweilige Aufgabe beschrieben:

Element	Component	Purpose	Description
Cloud Formation	Automation	Infrastructure as Code	Will be leveraged to use Infrastructure as Code and deploy all needed infrastructure via Code (template)
Boto3 (AWS SDK for Python)	Automation	Infrastructure as Code (for more complicated logic)	Will be used to create event based / dependent infrastructure and / or for retrieving information from the stack
API Gatway	Infrastructure	API Gateway layer	This infrastructure will be the REST API based on the swagger definition. It will control the access to the AVM. It will perform any request transformation if required
Lambda	Infrastructure	Application	This application coordinates the following: Account Creation, Account Organisation, Datastore Updating, Notification
DynamoDB	Infrastructure	Account Meta inforamtion Datastore	Store information regarding the AVM consumers (cost center, requester etc)

Swagger API	API	REST API	Define RESTFUL API, Provide documentation about API Consumption, Provide API SDK
Python function	Application	Create AWS account Organise AWS account in Organisational Unit Store received information from APIGW in Datastore Notify success/failure	Python function developed using TDD, interacts with different AWS services (Organisations, DynamoDB, SNS, APIGW)
WorkMail	Email	Will hold the Root Email for vended accounts	Each account needs an Email attached which is the root for the member account. To hold control and access to the vended accounts the root will stay and created in the Master Account

Tabelle 3: Komponenten der Projektarchitektur

7.1.1 Wahl des Cloud Anbieters

Für die Umsetzung des Projekts wurde AWS als Cloud Anbieter gewählt. Dies hat mehrere Gründe. An erster Stelle steht das persönliche Interesse, welches basiert auf Vorkenntnissen und dem größten Erfahrungsschatz in AWS bezogen auf die verschiedenen Cloud Anbieter. Darüber hinaus spielte auch die Loyalität zu AWS als Arbeitgeber eine Rolle bei der Wahl des Cloud Anbieters zur Umsetzung des Projekts. Rein technisch wäre eine Umsetzung auch mit anderen Anbietern realisierbar gewesen. Zum Aufsetzen einer Cloud Umgebung wird immer eine Landing Zone benötigt. Neben AWS bietet auch beispielsweise Microsoft Azure einen solchen Service an. Eine Landing Zone sollte daher nicht bloß als eine Cloud Lösung verstanden werden, sondern vielmehr als ein Konzept, das bei der Verwendung von Cloud in

Unternehmen nicht ignoriert werden darf. Da die Wahl aus den genannten Gründen auf AWS gefallen ist, soll der Anbieter im Folgenden kurz vorgestellt werden.

Amazon Web Services (AWS) bietet Kunden On-Demand Cloud Services und APIs über ein Pay-as-you-go-Modell an. AWS startete 2002 als Subunternehmen von Amazon mit der Bereitstellung allgemeiner Dienste und stellte 2006 seine ersten Cloud Produkte zur Verfügung. Heute werden bereits mehr als 175 verschiedene Cloud Dienste für eine Vielzahl von Technologien und Branchen veröffentlicht. AWS ist im Jahr 2020 weltweit einer der beliebtesten öffentlichen Cloud Infrastruktur- und Plattformdienste, die Anwendungen ausführen, gefolgt von Microsoft Azure und den Google Cloud Diensten. Da Unternehmen ihre Anwendungen und Daten kontinuierlich in die AWS Cloud migrieren, anstatt sie auf lokalen Computern zu speichern, wird es möglich, von verschiedenen Standorten aus auf Ressourcen zuzugreifen. Zu den wichtigsten AWS Diensten für Cloud Anwendungen gehören Speicher-, Datenbank-, Sicherheits- und Verwaltungstools. Einige der größten weltweit operierenden Unternehmen verwenden AWS für ihre Cloud Dienste, darunter Netflix, BBC und Baidu. Dementsprechend ist AWS einer der führenden Cloud Anbieter im globalen Cloud Markt (siehe auch Abschnitt 2.4). Aufgrund des kontinuierlich erweiterten Leistungsportfolios ist das Unternehmen weiterhin ein besonders attraktiver Geschäftspartner (Internetquelle Statista AWS).

7.1.2 AWS Cloud Adoption Framework

Wie bereits in Abschnitt 6 beschrieben, sollten Unternehmen, die die AWS Cloud nutzen möchten, dazu in der Lage sein, AWS Accounts einfach einzurichten. Eine Landing Zone sollte daher stets zu Beginn einer Cloud Reise eingerichtet werden. Sie bildet unter anderem das Fundament für die Migration in die Cloud. Neben dem Errichten einer Landing Zone bietet AWS noch eine weitere Methode an, um eine erfolgreiche Strategie für den Einsatz der Cloud zu entwickeln und die Einführung in einem Unternehmen schnell und sicher umzusetzen. Diese soll im Folgenden vorgestellt werden.

Das AWS Cloud Adoption Framework soll Unternehmen bei der Entwicklung und Umsetzung effizienter Pläne für ihre Cloud Adoption unterstützen. Die im Cloud Adoption Framework enthaltenen Methoden helfen den Unternehmen dabei, eine erfolgreiche Strategie für den Einsatz der Cloud in ihrer Organisation zu entwickeln. Darüber hinaus stellt das Cloud Adoption

Framework sicher, dass die Cloud Einführung im Unternehmen schnell und mit wenig Risiko umgesetzt werden kann. Der Prozess des AWS Cloud Adoption Frameworks kann in vier Phasen aufgeteilt werden. Diese sind Envision, Align, Start und Wert realisieren:

Envision:

Workshop zur Planung und Schaffung von Grundlagen der gewünschten Cloud Strategie. Es soll darauf geachtet werden, dass die gewählte Strategie dem Unternehmen einen messbaren Nutzen bringt, die Geschäftsziele mit den passenden unterstützenden Technologien verbunden werden und Schlüsselziele festgelegt werden. Darüber hinaus dient diese Phase der Priorisierung der Cloud Initiativen.

Align:

Workshop zur Erstellung eines durchführbaren Aktionsplans. In dieser Phase geht es darum, die Beweggründe des Unternehmens für den Einsatz der Cloud herauszufiltern. Es soll festgestellt werden, was die Einführung der Cloud für das Unternehmen bedeutet, wie die wichtigsten Interessengruppen von der Cloud profitieren können und den besten Ansatz zu bestimmen. Außerdem soll in dieser zweiten Phase Klarheit über die anstehenden Änderungsprozesse des Unternehmens auf dem Weg in die Cloud geschaffen werden.

Start:

Die zuvor erstellten Aktionspläne sollen in dieser Phase genutzt werden, um Workstreams für die Bereitstellung der Cloud für die Produktion zu entwickeln. Außerdem dienen sie als Leitfaden für die Durchführung der Cloud Projekte. Zudem sollen sie genutzt werden, um eine proaktive Berücksichtigung der Bedürfnisse und Wünsche der verschiedenen Interessengruppen zu gewährleisten und so den vollen Nutzen aus der Cloud zur Steigerung des Geschäftswerts zu ziehen.

Wert realisieren:

Die letzte Phase dient dazu, die Steigerung des Unternehmenswertes voranzutreiben. Dazu soll die Cloud Strategie kontinuierlich bewertet werden, um sich an geplante Vorgehensweisen zu halten. Darüber hinaus sollen zusätzliche Cloud Projekte erkannt werden, um den Nutzen kontinuierlich zu steigern.

Im Rahmen des AWS Cloud Adoption Framework werden sechs verschiedene Perspektiven beleuchtet: Business, Mitarbeiter, Governance, Plattform, Sicherheit und Betriebsablauf. Die Geschäftsperspektive (Business) hilft den Unternehmen dabei, zu einem Modell überzugehen, welches die IT-Strategie integriert und sie nicht getrennt vom Businessmodell zu betrachten. Derartige agile IT-Strategien sind dafür gedacht, Geschäftsergebnisse zu unterstützen sowie schnell auf sich ändernde Anforderungen oder technische Fähigkeiten zu reagieren. Die Personalperspektive (Mitarbeiter) unterstützt die Personalabteilung sowie das Personalmanagement dabei, die jeweiligen Teams auf die Einführung der Cloud vorzubereiten. Dabei werden sowohl die Fähigkeiten und Fertigkeiten der Mitarbeiter als auch die organisatorischen Prozesse um Cloud basierte Kompetenzen und Konzepte erweitert. Die Governance-Perspektive integriert IT-Governance und Organizational Governance. Hierin enthalten sind Anleitungen zum Feststellen und Implementieren von geeigneten Methoden für die IT-Governance. Zudem sollen Geschäftsprozesse mit verschiedenen Technologien unterstützt werden. Die Plattformperspektive soll Unternehmen dabei helfen, eine auf den Unternehmenszielen basierte Architektur der AWS Technologie zu entwerfen, zu implementieren und zu optimieren. Dabei sollen die Unternehmen bei der Erstellung von strategischen Leitlinien für das Design, Prinzipien, Tools und Richtlinien unterstützt werden, die zur Definition der AWS Infrastruktur verwendet werden sollen. Darüber hinaus werden unter dieser Perspektive auch Prinzipien und Muster für die Kommunikation der Ziel-Zustandsumgebung, für die Implementierung neuer Lösungen in der Cloud sowie die Migration bestehender Workloads in die Cloud vorgehalten. Die Sicherheitsperspektive dient dazu, die Auswahl und Implementierung von Kontrollen zu organisieren. Durch die Beachtung der jeweiligen Hinweise können Bereiche der Nichteinhaltung ermittelt werden und laufende Sicherheitsinitiativen geplant werden. Die Betriebsperspektive hilft den Unternehmen dabei, IT-Workloads so auszuführen, zu nutzen, zu betreiben und wiederherzustellen, dass sie den Geschäftsinteressen dienen. Die dadurch erlangten Erkenntnisse bestimmen die aktuellen Betriebsabläufe, Prozessänderungen und Schulungen, die für eine gelingende Einführung der Cloud erforderlich sind. Erfolgreiche IT-Betriebsabläufe können Unternehmen bei dem alltäglichen Betrieb, bei der Planung und Aufrechterhaltung sowie beim Wechsel- und Vorfallmanagement unterstützen (Internetquelle AWS Cloud Adoption Framework).

7.2 Verwendete Cloud Technologien

In den kommenden Abschnitten sollen einige Cloud Services vorgestellt werden, die für die Entwicklung und Umsetzung des Projekts genutzt wurden. Dabei soll auf die Themenfelder AWS Organizations, Bitbucket, Bitbucket Pipelines, AWS IAM, AWS Cloud Formation, Swagger, Open API, AWS API Gateway, AWS Lambda, AWS Amplify, Amazon Cognito und Angular eingegangen werden.

7.2.1 AWS Organizations (Accountmanagement)

Bei AWS Organizations handelt es sich um einen Kontoverwaltungsservice (Accountmanagement), mit dem mehrere AWS Accounts in einer zentral erstellten und verwalteten Organisation konsolidiert werden können. AWS Organizations umfasst verschiedene Services, die es ermöglichen, die Budget-, Sicherheits- und Compliance Anforderungen eines Unternehmens besser zu erfüllen. Für Administratoren einer Organisation besteht die Möglichkeit, verschiedene Accounts anzulegen und bereits bestehende Accounts dazu einzuladen, der Organisation beizutreten. AWS Organizations bietet den Kunden folgende Funktionen:

Zentrale Verwaltung der gesamten AWS Accounts:

Bestehende Accounts können in einer Organisation zusammengefasst und zentral verwaltet werden. Außerdem können Richtlinien angehängt werden, die sich auf einige oder alle Accounts auswirken.

Konsolidierte Abrechnung für alle Mitgliedsaccounts:

Das Verwaltungskonto der Organisation kann zur Konsolidierung und Zahlung für alle Mitgliedskonten genutzt werden. Bei der konsolidierten Fakturierung kann das Verwaltungskonto auch auf die Fakturierungsdaten, Kontoinformationen und Kontoaktivitäten von Mitgliedskonten innerhalb der Organisation zugreifen.

Hierarchische Gruppierung der Accounts:

Die Accounts können mit Hilfe von Organisationseinheiten (OUs) gruppiert werden und es können an jede OU andere Zugriffsrichtlinien angehängt werden, um Budget-, Sicherheits- und Compliance Anforderungen umzusetzen. Wenn zum Beispiel Accounts genutzt werden, die nur auf die AWS Services mit bestimmten gesetzlichen Anforderungen zugreifen sollen, dann können diese Accounts in einer Organisationseinheit zusammengefasst werden.

Richtlinien zur Zentralisierung der Kontrolle:

Der Administrator des Verwaltungskontos einer Organisation kann Service Control Policies (SCPs) verwenden, um verschiedene Berechtigungen für Mitgliedskonten in der Organisation anzugeben. In den SCPs kann eingeschränkt werden, auf welche AWS Services, -Ressourcen und einzelne API Aktionen die Benutzer in jedem Mitgliedskonto zugreifen dürfen.

Richtlinien zur Standardisierung von Tags:

Mithilfe von Tag-Richtlinien für alle Ressourcen in den Accounts einer Organisation kann eine konsistente Tag-Verwaltung sichergestellt werden.

Richtlinien zur Steuerung:

Es können Deaktivierungsrichtlinien für KI-Services verwendet werden, um die Datenerfassung und -speicherung für alle AWS KI-Services abzulehnen, die nicht verwendet werden sollen.

Konfigurieren der automatischen Backups:

Backup Richtlinien können verwendet werden, um AWS Backup Pläne zu konfigurieren und automatisch auf Ressourcen in allen Accounts einer Organisation anzuwenden.

Integration und Unterstützung für AWS Identity and Access Management (IAM):

IAM ermöglicht eine genaue Kontrolle über die Benutzer in den einzelnen Accounts. AWS Organizations erweitert diese Kontrolle auf die Kontoebene, wodurch der Administrator die Kontrolle darüber erhält, was Benutzer in einem Account oder einer Accountgruppe durchführen können.

Integration in andere AWS Services:

Die in AWS Organizations verfügbaren Services für die Multikontenverwaltung können für bestimmte AWS Services genutzt werden, um Aufgaben für alle Accounts auszuführen, die Mitglied der jeweiligen Organisation sind.

Globaler Zugriff:

AWS Organizations ist ein globaler Service mit einem einzelnen Endpunkt, der von allen AWS Regionen aus arbeiten kann. Dabei muss keine Region explizit ausgewählt werden, in der gearbeitet werden soll.

Eventually-Consistent-Datenreplikation:

AWS Organizations ist zu jeder Zeit verfügbar, da die Daten über mehrere AWS Rechenzentren in einer Region repliziert werden. Wenn eine Anforderung zur Änderung von Daten erfolgreich ist, wird die Änderung übernommen und sicher gespeichert.

Kosten:

AWS Organizations ist eine Funktion, die ohne zusätzliche Kosten angeboten wird. Es werden nur dann Kosten in Rechnung gestellt, wenn über die Accounts in einer Organisation auf andere AWS Services zugegriffen wird (Internetquelle AWS Organizations).

7.2.2 Bitbucket (Git Hosting)

Bitbucket Cloud ist ein Git Hosting Angebot für Teams, welches die Zusammenarbeit erleichtern soll. Dank der Integrationen von Jira in Bitbucket kann das gesamte Softwareteam an einem Projekt zusammenarbeiten. Bitbucket bietet einen zentralen Ort, an dem ein Team vom Konzept bis zur Cloud gemeinsam an einem Code arbeiten, einen hochwertigen Code durch automatische Tests erstellen und den Code dann zuverlässig bereitstellen kann (Internetquelle Bitbucket).

Source Control Management

Das Source Control Management (SCM) beinhaltet Systeme zur Quellcodeverwaltung. Das SCM stellt kontinuierlich den Verlauf der Codeentwicklung dar und trägt zur Lösung von

Konflikten beim Zusammenführen von Beiträgen aus mehreren Quellen bei. Unter Quellcodeverwaltung versteht man die Praxis der Nachverfolgung und Verwaltung von Änderungen am Code. Die Quellcodeverwaltung ist eine wichtige Komponente des Entwicklungsprozesses. Mit Quellcodeverwaltungs-Systemen können Codeänderungen nachverfolgt werden. Darüber hinaus kann mithilfe der Quellcodeverwaltung der Revisionsverlauf des Codes angezeigt werden und bei Bedarf ältere Versionen eines Projekts wiederhergestellt werden. Quellcodeverwaltungs-Systeme ermöglichen es einem Team gemeinsam am Code zu arbeiten. Sie optimieren so den Entwicklungsprozess und stellen eine zentrale Quelle für den gesamten Code dar (Internetquelle Source Control).

7.2.3 Bitbucket Pipelines (CI/CD)

Bei Bitbucket Pipelines handelt es sich um das integrierte CI/CD Tool von Bitbucket Cloud. Dank der integrierten CI/CD-Lösung Bitbucket Pipelines ist eine Verwaltung von Servern, die Synchronisierung von Repositories und die Konfiguration der Benutzerverwaltung nicht mehr nötig. Mit Hilfe von Bitbucket Pipelines können Builds erstellt, getestet und bereitgestellt werden (Internetquelle Bitbucket Pipelines).

Continuous Integration

Die Abkürzung CI steht für Continuous Integration. Entwickler, die damit arbeiten, führen ihre Änderungen so oft wie möglich in den Haupt-Branch zurück. Zur Prüfung der vorgenommenen Änderungen wird dann ein Build erstellt, der automatische Tests durchführt. So wird sichergestellt, dass Integrationsprobleme vermieden werden, die möglicherweise auftreten, wenn die Entwickler mit dem Zusammenführen der Änderungen bis zum Auslieferungsdatum warten. Bei dem Verfahren wird großer Wert auf die Testautomatisierung gelegt, um die Anwendung auf Fehlerfreiheit zu überprüfen. Wird Continuous Integration in einem Unternehmen eingesetzt, kommen einige Anforderungen auf die Mitarbeiter zu. So müssen beispielsweise für jede neue Funktion, Verbesserung oder Fehlerbehebung automatisierte Tests geschrieben werden. Außerdem wird ein Continuous Integration Server zum Überwachen des Haupt-Repositories und zum Ausführen der automatisierten Tests benötigt. Darüber hinaus müssen die Entwickler die durchgeführten Änderungen häufiger zusammenführen. Der Einsatz von CI in einem Unternehmen bietet aber auch viele Vorteile. So werden weniger Fehler in die Produktion

übergeben, da diese durch die automatisierten Tests früh entdeckt werden. Dies sorgt ebenfalls dafür, dass das Erstellen des Release-Builds sehr einfach ist. Zudem besteht ein geringerer Kontextwechsel, da die Entwickler umgehend darüber informiert werden, wenn ihnen beim Build ein Fehler unterläuft. Außerdem werden die Testkosten maßgeblich reduziert und der CI-Server kann eine Vielzahl von Tests in hoher Geschwindigkeit durchführen. Durch die Automatisierung und die dadurch gewonnene Zeit kann die Qualität der Software weiter verbessert werden.

Continuous Delivery/Deployment

CD steht für Continuous Delivery oder auch Continuous Deployment. Continuous Delivery ist eine Erweiterung der Continuous Integration, da alle durchgeführten Änderungen nach der Build-Phase automatisch in einer Test- beziehungsweise Produktionsumgebung implementiert werden. Zusätzlich zu den bereits erwähnten automatisierten Tests verfügt das Unternehmen dadurch also auch über einen automatisierten Release Prozess. Die entworfene Anwendung kann dadurch jederzeit mit wenig Aufwand auf einer Schaltfläche bereitgestellt werden. Mithilfe von Continuous Delivery können Entwickler frei entscheiden, ob sie ihre Anwendung täglich, wöchentlich, vierzehntägig oder in einem anderen beliebigen Rhythmus veröffentlichen wollen. Auch beim Einsatz von Continuous Delivery in einem Unternehmen müssen die Mitarbeiter mit einigen Anforderungen rechnen. So muss an erster Stelle natürlich die Basis durch die CI gegeben sein. Außerdem müssen Deployments automatisiert werden. Der Trigger ist dabei zwar immer noch manuell, aber sobald ein Deployment gestartet ist, sollte kein menschliches Eingreifen mehr erforderlich sein. Darüber hinaus kann der Einsatz von Feature Flags eine Notwendigkeit darstellen. So werden die Kunden in der Produktion durch unvollständige Funktionen nicht beeinträchtigt. Neben diesen Umstellungen bietet Continuous Delivery aber auch einige Vorteile. Die Software Deployments sind weniger komplex, sodass die Entwickler sich nicht mehr tagelang auf einen Release vorbereiten müssen. Zudem können diese öfter stattfinden, was die Rückkopplung mit den Kunden beschleunigt. Außerdem lastet weniger Druck auf Entscheidungen für kleine Änderungen, was die Mitarbeiter noch weiter motivieren kann.

Continuous Deployment ist wiederum als eine Steigerung von Continuous Delivery anzusehen. Bei diesem Verfahren wird jede Änderung, die die Produktionsabschnitte durchlaufen hat, für

die Kunden freigegeben. Dieser Prozess erfolgt automatisch und wird nur dann unterbrochen, wenn ein Test fehlschlägt. Dann wird die entsprechende Änderung nicht in der Produktion bereitgestellt. Durch den Einsatz von Continuous Deployment können die Mitarbeiter sich auf die Entwicklung von Software konzentrieren und beobachten, wie ihre Anwendung Minuten nach der Fertigstellung veröffentlicht wird. Wird Continuous Deployment in einem Unternehmen eingesetzt, kommen auch hier einige Anforderungen auf die Mitarbeiter zu. Zum einen muss die Testkultur optimal sein. Das heißt, die Qualität der Testsuite entscheidet über die Qualität der Releases. Darüber hinaus muss der Dokumentationsprozess mit dem schnelleren Deployment mithalten können. Außerdem müssen Feature Flags zu einem festen Bestandteil des Release Prozesses werden, damit die Abstimmung mit anderen Abteilungen zu jeder Zeit sichergestellt ist. Auch dieses Verfahren bietet den Unternehmen neben den Anforderungen einige Vorteile. Die Mitarbeiter können beispielsweise schneller entwickeln, da die Entwicklung für Releases nicht unterbrochen wird. Deployment-Pipelines werden bei jeder Änderung automatisch ausgelöst. Die Releases sind darüber hinaus weniger riskant und eventuell auftretende Probleme sind dadurch leichter zu beheben. Für die Kunden bringt diese Methode den großen Vorteil, dass die stetigen Verbesserungen tägliche statt monatliche Qualitätssteigerungen nach sich ziehen.

Den größten Kostenfaktor im Zusammenhang mit CI/CD birgt die Installation und Wartung eines CI-Servers. Dieser Kostenpunkt kann wiederum deutlich reduziert werden, wenn das Unternehmen einen Cloud Service wie Bitbucket Pipelines verwendet, der jedem Bitbucket-Repository Automatisierung hinzufügt (Internetquelle Unterscheidung CI/CD).

7.2.4 AWS Identity & Access Management (IAM)

AWS Identity and Access Management (IAM) bietet eine differenzierte Zugriffskontrolle für die gesamte AWS Plattform. Mit IAM kann festgelegt werden, wer auf welche Services und Ressourcen unter welchen Voraussetzungen zugreifen darf. Mit IAM-Richtlinien können zusätzlich noch die Berechtigungen für Mitarbeiter und Systeme verwaltet werden. IAM ist ein AWS Service, der ohne zusätzliche Kosten angeboten wird, sofern bereits ein AWS Account vorhanden ist. Mit IAM können AWS Berechtigungen für Benutzer und Workloads verwaltet werden. Für Mitarbeiter wird empfohlen, AWS Single Sign-On (AWS SSO) zu verwenden,

um den Zugriff auf AWS Accounts und damit einhergehende Berechtigungen zu verwalten (Internetquelle AWS IAM).

7.2.5 AWS CloudFormation (Infrastructure as Code)

AWS CloudFormation ist die native Lösung für Infrastructure as Code von Amazon Web Services. Es handelt sich dabei um einen Service, der die Entwicklung und Einrichtung von AWS Ressourcen erleichtert, sodass Kunden weniger Zeit für die Verwaltung der Ressourcen aufbringen müssen. Dafür müssen die Nutzer ein Template erstellen, in dem alle gewünschten AWS Ressourcen beschrieben werden, und CloudFormation übernimmt dann die Bereitstellung und Konfigurierung dieser Ressourcen. Ein Template beschreibt dabei stets alle Ressourcen und die dazugehörigen Eigenschaften. Nachdem der Stack erfolgreich erstellt worden ist, sind die AWS Ressourcen eingerichtet und können in Betrieb genommen werden. Außerdem kann mit CloudFormation eine Sammlung von Ressourcen als Einheit verwaltet werden. Wenn eine Anwendung zusätzliche Verfügbarkeit erfordert, sollte sie stets in mehreren Regionen repliziert werden, damit die Kunden die Anwendung bei einem möglichen Ausfall auch in anderen Regionen weiter nutzen können. Hierfür kann ebenfalls das CloudFormation Template verwendet werden. Der Service dient also dazu, die Infrastrukturverwaltung für den Kunden zu vereinfachen und ein schnelleres Replizieren der Infrastruktur zu ermöglichen. Zudem wird das Kontrollieren und Nachverfolgen von Änderungen an der Infrastruktur vereinfacht (Internetquelle AWS Cloud Formation).

7.2.6 Swagger / Open API

Die OpenAPI Spezifikation ist ein Standard, der als API Beschreibungsformat für REST-APIs verwendet wird. Mit einer OpenAPI Datei können Nutzer ihre gesamte API beschreiben. Dazu gehören:

- Verfügbare Endpunkte und Operationen auf jedem Endpunkt
- Operationsparameter Eingabe und Ausgabe für jede Operation
- Authentifizierungsmethoden
- Kontaktinformationen, Lizenz und Nutzungsbedingungen
- API Spezifikationen können in YAML oder JSON geschrieben werden.

Swagger beschreibt eine Reihe von Open-Source-Tools, die auf der OpenAPI Spezifikation basieren und Nutzern beim Entwerfen, Erstellen, Dokumentieren und Verwenden von REST-APIs helfen können. Zu den wichtigsten Swagger Tools gehören:

- Swagger Editor: browserbasierter Editor, in dem OpenAPI Spezifikationen geschrieben werden können
- Swagger UI: rendert OpenAPI Spezifikationen als interaktive API Dokumentation
- Swagger Codegen: generiert Server-Stubs und Client-Bibliotheken aus einer OpenAPI Spezifikation

Die Fähigkeit von APIs, ihre eigene Struktur zu beschreiben, ist der Kern in OpenAPI. Einmal geschrieben, können eine OpenAPI Spezifikation und Swagger Tools die API Entwicklung auf verschiedene Weise vorantreiben. So können beispielsweise API-bezogene Tools mit der API des Nutzers verbunden werden, wenn die Spezifikation verwendet wird. Auf diese Weise können automatisierte Tests für die API erstellt werden (Internetquelle Swagger).

7.2.7 Amazon API Gateway & AWS Lambda

Amazon API Gateway

Amazon API Gateway ist ein vollständig verwalteter Service, der das Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von APIs für Entwickler vereinfacht. APIs übernehmen die Rolle der „Vordertür“ für Anwendungen, die jeweils über Backend Services auf Daten, Geschäftslogik oder Funktionalitäten zugreifen. Mit API Gateway können RESTful-APIs und WebSocket-APIs erstellt werden, die eine Kommunikation in Echtzeit ermöglichen. API Gateway unterstützt sowohl containerisierte und serverlose Workloads als auch Webanwendungen. API Gateway erfüllt alle Aufgaben für das Akzeptieren und Verarbeiten von bis zu Hunderttausenden gleichzeitigen API Aufrufen. Dazu gehören die Verwaltung des Datenverkehrs, der CORS-Support, Autorisierung und Zugriffskontrolle, Einschränkung, Überwachung und Verwaltung der jeweiligen API Version. Bei API Gateway wird lediglich für eingehende API Aufrufe und ausgehende Datenübertragungen bezahlt. AWS bietet hierfür ein gestaffeltes Preissystem an, mit welchem die Kosten durch die Skalierung der API Nutzung gesenkt werden (Internetquelle Amazon API Gateway).

AWS Lambda

AWS Lambda ist ein serverloser Datenverarbeitungsservice, mit dem Nutzer Code für praktisch jede Art von Anwendung oder Backend Service ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda kann in über 200 AWS Services und Software as a Service Anwendungen eingesetzt werden und erweitert diese mit benutzerdefinierter Logik oder erstellt Backend Services. AWS Lambda führt den Code des jeweiligen Nutzers beim Eintreten bestimmter Ereignisse aus und verwaltet automatisch die dazugehörigen Datenverarbeitungsressourcen. Zu derartigen Ereignissen zählen beispielsweise Zustandsänderungen oder Aktualisierungen, etwa wenn ein Kunde einen Artikel in den Einkaufswagen auf einer E-Commerce Website legt. Lambda führt den Code dabei auf einer hochverfügbaren Computing Infrastruktur aus und erledigt alle rechenintensiven und verwaltungstechnischen Aufgaben. Dies umfasst die Wartung von Servern und Betriebssystemen, die Bereitstellung von Kapazitäten, die automatische Skalierung und die Bereitstellung von Code und Sicherheitspatches. Darüber hinaus dient Lambda auch der Codeüberwachung und -protokollierung. Nutzer müssen lediglich den Code zur Verfügung stellen (Internetquelle AWS Lambda).

Python-Code kann in AWS Lambda ausgeführt werden. Lambda stellt dann Laufzeiten für Python bereit, die den Code ausführen, um Ereignisse zu verarbeiten. Der Code wird dann in einer Umgebung ausgeführt, die das Software Development Kit (SDK) für Python (Boto3) enthält. Die Anmeldeinformationen werden hierbei von einer AWS Identity and Access Management (IAM) Rolle übernommen (Internetquelle Lambda Python). Der Einstieg in AWS kann mit Boto3, dem AWS SDK für Python, beschleunigt werden. Boto3 erleichtert die Integration einer Python Anwendung in AWS Services. Boto3 besitzt zwei getrennte Ebenen von APIs. Die Client APIs (API auf niedriger Ebene) bieten eine direkte Zuordnung der dazugehörigen HTTP API Vorgänge. Ressourcen APIs verbergen explizite Netzwerkaufrufe und stellen Ressourcenobjekte bereit, um auf Attribute zugreifen und Aktionen durchführen zu können. Die Client- und Ressourcen-Schnittstellen von Boto3 haben dynamisch generierte Klassen, die AWS APIs beschreiben. Dadurch können schnelle Aktualisierungen mit starker Konsistenz für alle unterstützten Services bereitgestellt werden (Internetquelle Python).

7.2.8 AWS Amplify, Amazon Cognito & Angular

AWS Amplify

AWS Amplify ist eine Sammlung speziell entwickelter Werkzeuge und Funktionen, mit denen Entwickler von Frontend-Web-Mobilanwendungen vollständige Anwendungen auf AWS erstellen können. Dabei haben die Nutzer die Möglichkeit, die Bandbreite aller AWS Services zu nutzen, wenn sich die Anwendungsfälle weiterentwickeln. Mit Amplify können App Backends konfiguriert werden und Anwendungen in minutenschnelle verbunden werden. Darüber hinaus können statische Web Apps mit wenigen Klicks bereitgestellt und App Inhalte problemlos auch außerhalb der AWS Konsole verwaltet werden (Internetquelle AWS Amplify).

Amazon Cognito

Amazon Cognito dient als Tool zur Registrierung und Anmeldung von Benutzern. Kunden können mit Amazon Cognito die Zugriffskontrolle schnell und einfach ihren Web- und mobilen Anwendungen hinzufügen. Amazon Cognito Benutzerpools bieten einen sicheren Identitätsspeicher und können für Millionen von Benutzern skaliert werden. Es ermöglicht den Anmeldeprozess sowohl über soziale Identitätsanbieter wie Apple, Facebook, Google und Amazon als auch für Unternehmens-Identitätsanbieter über SAML 2.0 und OpenID Connect. Cognito Benutzerpools können unkompliziert eingerichtet werden, ohne dass eine Infrastruktur bereitgestellt werden muss. Alle Mitglieder des Benutzerpools haben Zugriff auf ein Verzeichnisprofil, das sie über ein Software Development Kit (SDK) verwalten können. Amazon Cognito bietet Steuerungsoptionen des Zugriffs auf AWS Ressourcen aus der betreffenden Anwendung. So können zum Beispiel Rollen definiert werden und Benutzer verschiedenen Rollen zugeordnet werden. Auf diese Weise kann die Anwendung nur auf die Ressourcen zugreifen, die für jeden Benutzer autorisiert wurden. Zusätzlich können auch Attribute von Identitätsanbietern in den Berechtigungsrichtlinien von AWS Identity and Access Management verwendet werden, um den Zugriff auf Ressourcen für Benutzer zu steuern. Amazon Cognito unterstützt sowohl die Multifaktor-Authentifizierung als auch eine Datenverschlüsselung im Speicher und auf dem Übertragungsweg (Internetquelle Amazon Cognito).

Angular

Angular ist sowohl ein Anwendungsdesign-Framework als auch eine Entwicklungsplattform zum Erstellen effizienter und anspruchsvoller Single-Page-Anwendungen. Angular basiert auf TypeScript. Als Plattform beinhaltet Angular ein komponentenbasiertes Framework zum Erstellen skalierbarer Webanwendungen. Zudem bietet es eine Sammlung gut integrierter Bibliotheken, die eine Vielzahl von Funktionen abdecken (darunter Routing, Formularverwaltung, Client-Server-Kommunikation). Außerdem beinhaltet Angular eine Reihe von Entwicklertools, die Nutzer beim Entwickeln, Erstellen, Testen und Aktualisieren ihres Codes unterstützen. Mit Angular nutzen Entwickler die Vorteile einer Plattform, die von Einzelprojekten bis hin zu Anwendungen auf Unternehmensebene skaliert werden kann (Internetquelle Angular).

7.3 Dokumentation

Es folgen die einzelnen Entwicklungsschritte, die für die Programmierung der Anwendung vollzogen wurden. Dabei wird auf die Punkte Root Account Creation, Source Control Management, CI/CD, Authenticitation & Authorization, Deploy Infrastructure, Define API, Implement API und Create Frontend eingegangen.

7.3.1 Root Account Creation

Die folgende Abbildung schafft ein besseres Verständnis einer Multi Account Architektur in AWS:

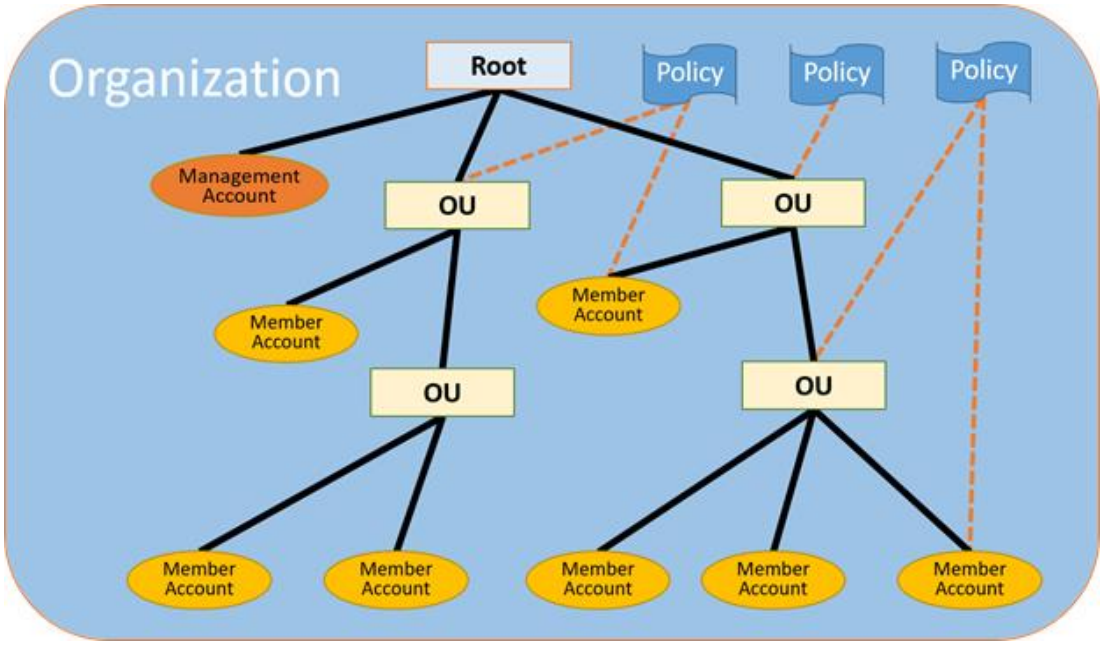

Abbildung 16: Multi Account Architektur in AWS

Der Root Account ist verantwortlich für das Management aller Member Accounts und zahlt die auftretenden Kosten aller Accounts in einer zusammengefassten Rechnung. Der erste Schritt, um eine neue AWS Organisation für Cloud Adoption einzuführen, ist die Kreierung eines Root Accounts. Im Grunde ist ein Root Account ein normaler AWS Account wie jeder andere auch, mit dem einzigen Unterschied, dass im Root Account AWS Organisationen eingeschaltet sind. Unterhalb des Root Accounts können weitere neue Accounts erstellt werden

(Member Accounts). Außerdem können auch bereits bestehende Accounts zu der jeweiligen Organisation eingeladen werden (Internetquelle AWS Organizations).

Einige Methoden, die sich im Umgang mit Root Accounts sehr bewährt haben, sind die Folgenden (Internetquelle AWS Security Best Practices):

- MFA sollte aktiviert sein
- Die Credentials sollten sicher verwahrt sein
- Die Root Credentials sollten nicht für beliebige Aufgaben genutzt werden
- Stattdessen sollte ein Admin Benutzer mit Privilegien für die tägliche Arbeit erstellt werden
- Es kann hilfreich sein, ein Budget zu setzen, um eine Benachrichtigung zu erhalten, wenn eine bestimmte Grenze erreicht wurde

7.3.2 Source Control Management (SCM) Repositories

Das Projekt wurde auf verschiedene Layer und Funktionen aufgeteilt und dies spiegelt sich auch in den sechs Repositories wider (siehe Abbildung 17). In dem „api“ Respository befindet sich unter anderem die Swagger API Definition. Das „application“ Repository beinhaltet unter anderem den Lambda Code mit der Geschäftslogik. In dem „bootstrap_account“ Repository befindet sich unter anderem ebenfalls ein Lambda Code, der einen neuen Account initialisiert. Das „frontend“ Repository enthält alles rundum das User Interface. Das „infrastructure“ Repository beinhaltet unter anderem das CloudFormation Template, um die gesamte Infrastuktur automatisiert aufzusetzen. Im „user_validation“ Repository befindet sich unter anderem eine Lambda Funktion, die im Registrierungsprozess aufgerufen wird und die Daten auf individuelle Kriterien überprüft. Die Repositories befinden sich auf der CD, die dieser Arbeit beiliegt.

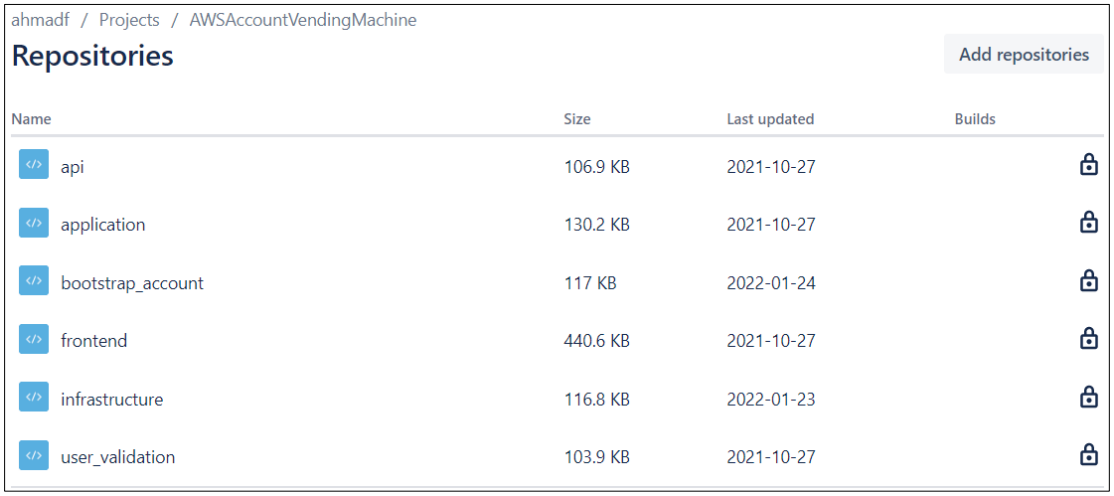

Abbildung 17: Repositories

7.3.3 Continuous Integration / Continuous Deployment (CI/CD)

Als Versionierungstool für den Source Code wurde git verwendet und als Hosting-Lösung Bitbucket. Außerdem werden Bitbucket Pipelines für die automatisierte Integration und Verwendung (CI/CD) der Applikation genutzt. Jedes Depot wird Bitbucket Pipelines enthalten, welche die Konfiguration und das Setup der Pipeline beinhalten. Im Rahmen des Projekts wurden mehrere Repositories erstellt. Der dazugehörige Code wurde auf der CD im Anhang dieser Arbeit bereitgestellt.

7.3.4 Authenticitation & Authorization

Um eine Verbindung von den Bitbucket Repositories zu der AWS Umgebung herzustellen, musste ein zugehöriger Service User mit entsprechenden Berechtigungen erstellt werden. In der folgenden Abbildung ist ein Ausschnitt von dem AWS Identity und Access Management (IAM) Service zu sehen. Es wurde ein Service User erstellt.

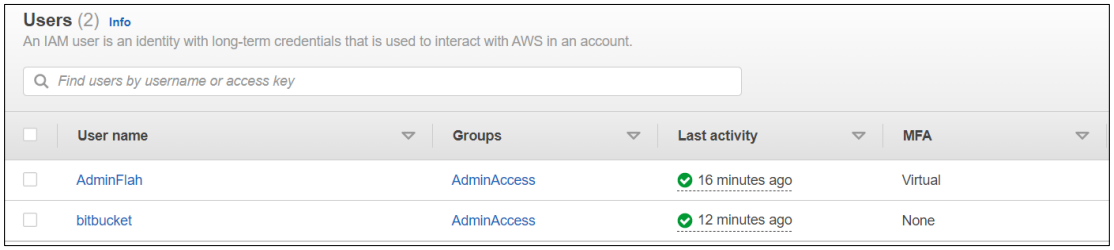

Abbildung 18: Service User

Darüber hinaus musste sichergestellt werden, dass die Credentials sicher verwahrt werden. Die Credentials können im Bitbucket Workspace verwahrt werden. Auf die im Workspace angelegten Variablen kann von allen zugehörenden Repositories zugegriffen werden. Damit können die Credentials an einer zentralen Stelle abgelegt werden und von allen Repositories, speziell von Bitbucket Pipelines, für den CI/CD-Prozess, verwendet werden (Internetquelle Bitbucket Workspace). Auf Abbildung 19 sieht man die abgelegten AWS Credentials, wie sie im Bitbucket Workspace sicher und verschlüsselt gespeichert sind.

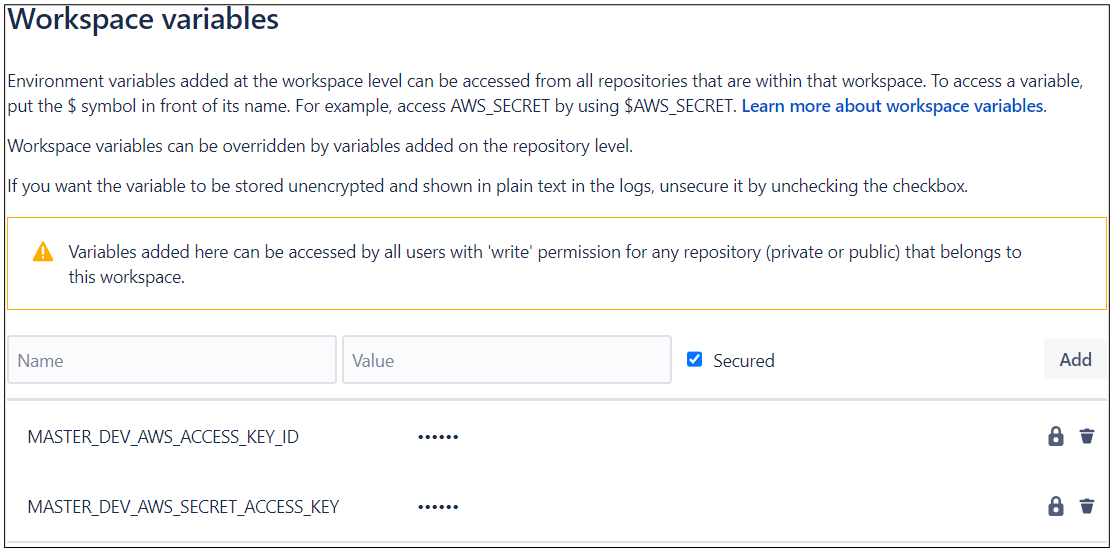

Abbildung 19: Bitbucket Workspace

7.3.5 Deploy Infrastructure

Das Tool, welches für Infrastructure as Code verwendet wurde, ist AWS CloudFormation. Das Template ist in einem Bitbucket Repository gespeichert und wird mittels Bitbucket Pipelines deployed. Der Ablauf, sowie die bereitgestellten Ressourcen sind auf der folgenden Abbildung dargestellt:

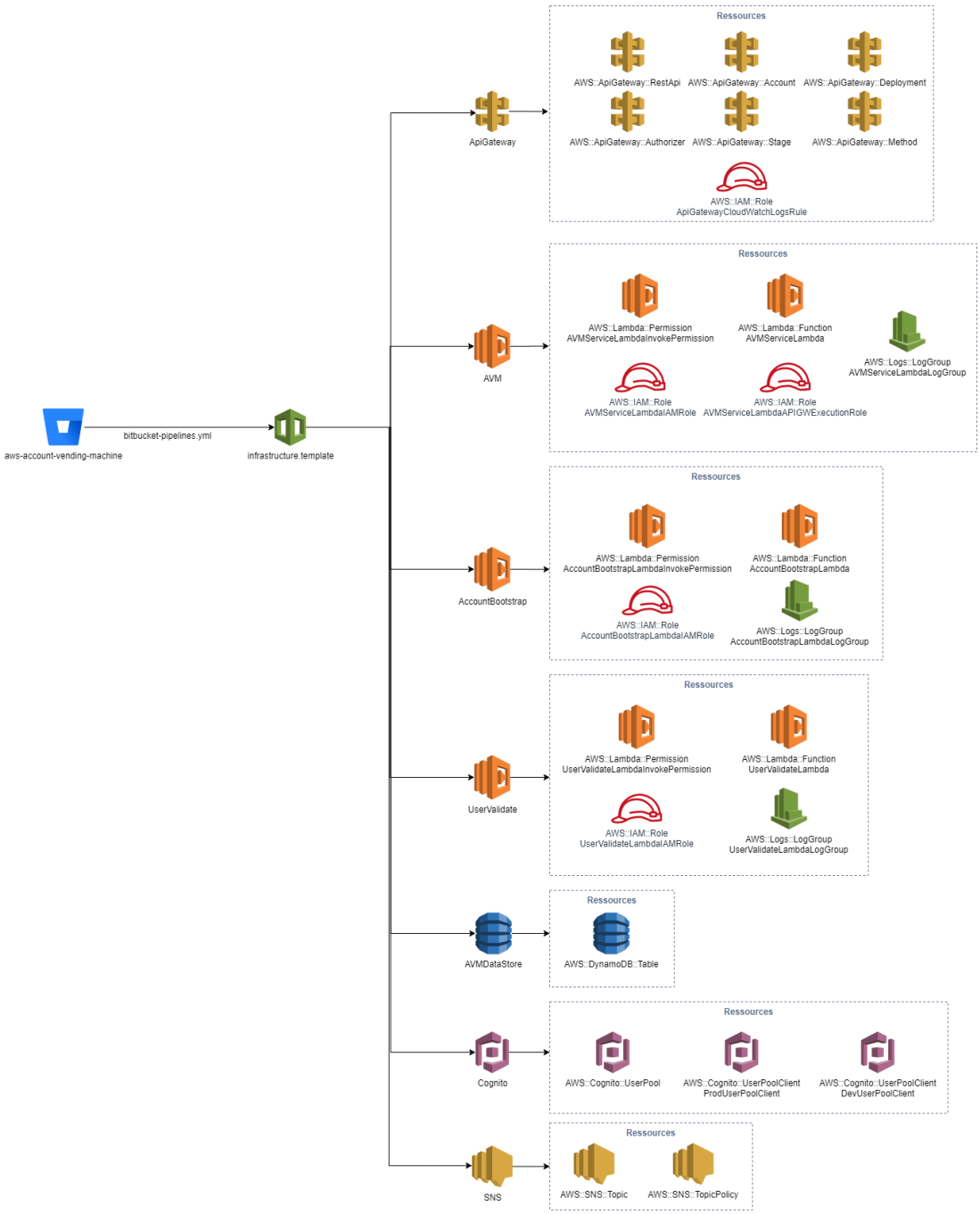

Abbildung 20: Komponenten der Infrastruktur

7.3.6 Define API

Es wurde die OpenAPI Spezifikation verwendet im Zusammenspiel mit Swagger als Tool für die Definition und Visualisierung. Im Folgenden dient ein Auszug der API in Swagger zur Veranschaulichung. Der dazugehörige Code befindet sich auf der CD, die der Arbeit beiliegt.

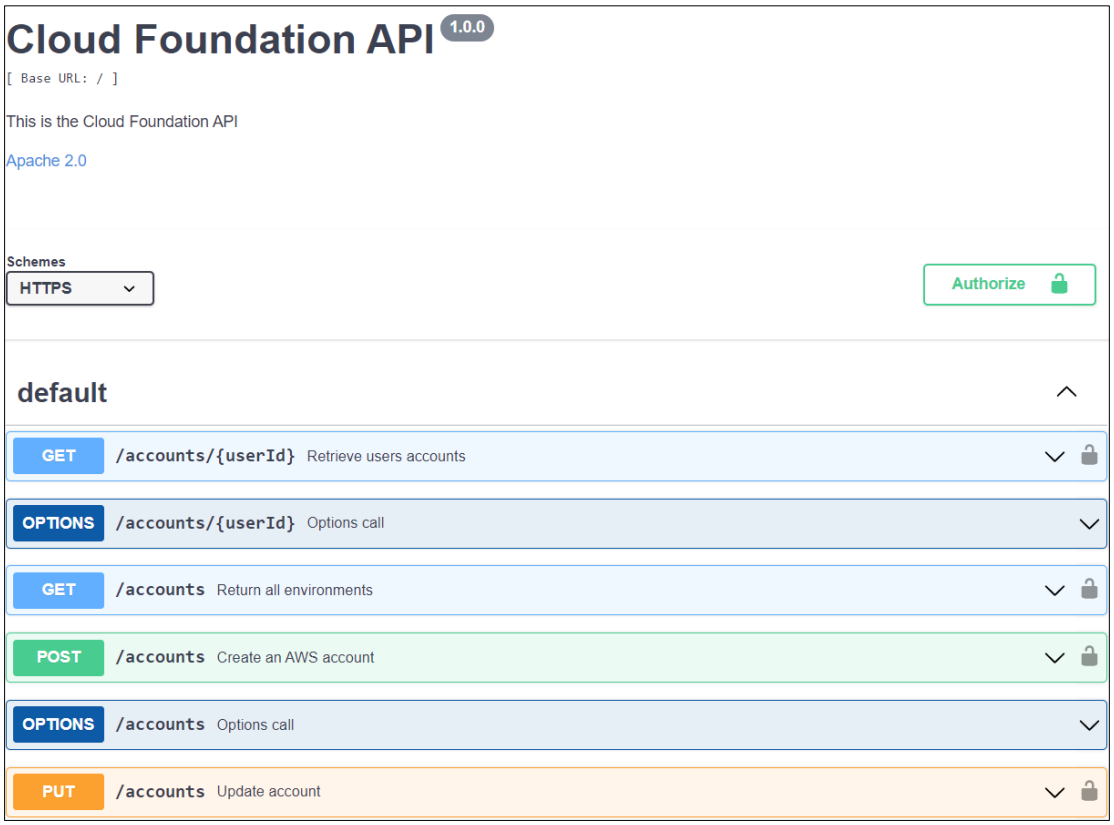

Abbildung 21: API in Swagger

7.3.7 Implement API

Für die Implementation der API wurde Amazon API Gateway verwendet. Dieser Service ermöglicht das Erstellen, Veröffentlichen, Warten, Überwachen und Sichern von REST, HTTP und WebSocket APIs in jeglicher Größenordnung. API Gateway unterstützt die OpenAPI Spezifikation in Version 2 und 3. Für die Logik und Rechenleistung wurde AWS Lambda verwendet, welches sich in API Gateway integrieren lässt. Jeder API Aufruf triggert eine eigenständige

Funktion. Als Programmiersprache wurde Python gewählt. Amazon bietet für Python ein Software Development Kit (Boto3) an, um die AWS Services nutzen zu können.

7.3.8 Create Frontend

Das Frontend wurde mit Hilfe von AWS Amplify und Angular erstellt. Dieser Service vereinfacht die Integration und unterstützt den Nutzer mit einer Vielzahl an Features. Außerdem wurde das Ngx-Template von Akveo als Starttemplate für die UI verwendet (Internetquelle Ngx-Template).

7.4 Produktvorstellung

Die Login-Seite des Frontends ist der Startpunkt der Applikation. Die Maske dafür ist eine Komponente des AWS Amplify Services, welche importiert wurde. Die Authentifizierung und Autorisierung im Backend wurde mittels des Amazon Cognito Services umgesetzt.

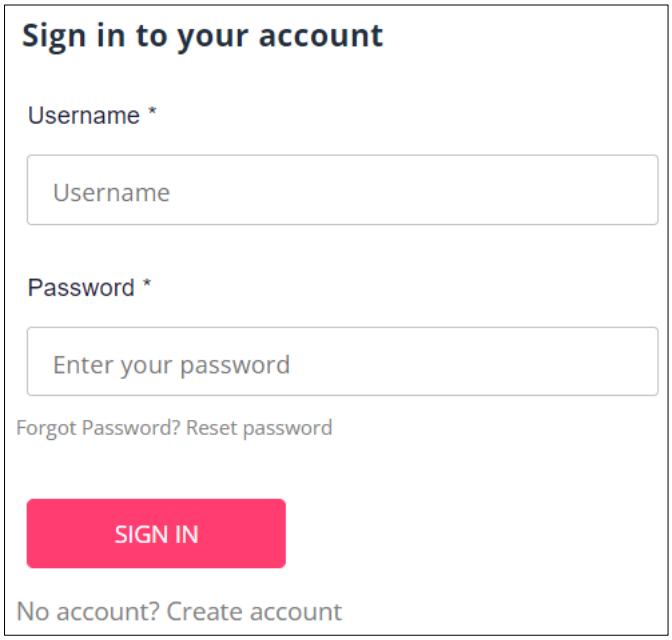

Abbildung 22: Frontend Login-Seite

Ganz in Self-Service Manier kann man sich selbst für die Anwendung registrieren und es können spezifische Kriterien dafür festgelegt werden, wie beispielsweise die Unternehmens-

domäne als Sicherheitsmerkmal beziehungsweise Beschränkung. In dem umgesetzten Beispiel können für die Registrierung ausschließlich @haw-hamburg.de Email-Adressen verwendet werden. Erfüllt man die Kriterien, dann wird eine Bestätigungsmail an die angegebene Adresse versendet, um die Identität und Richtigkeit zu überprüfen. Sobald man den Bestätigungslink in der Email angeklickt hat, kann man sich in der Anwendung anmelden.

Nach dem erfolgreichen Login landet man auf dem folgendem Dashboard:

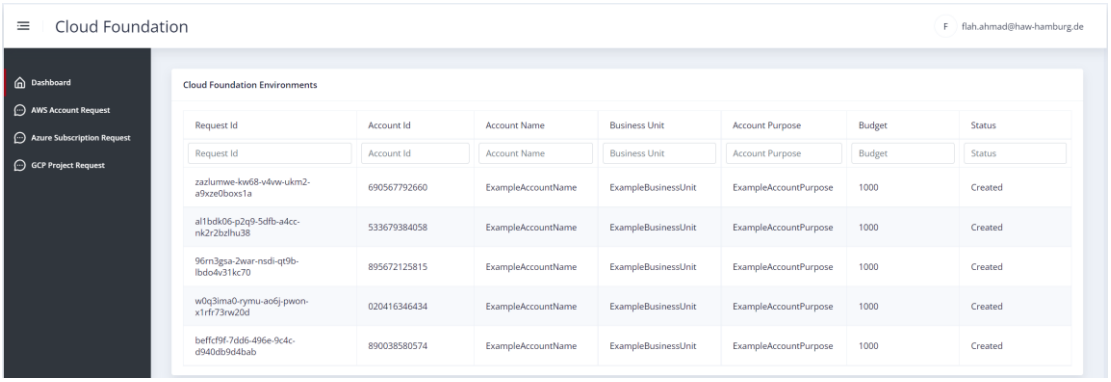

Abbildung 23: Cloud Foundation Dashboard

In der Mitte befindet sich eine Übersicht aller erstellten Accounts des eingeloggten Users. Es folgt eine vergrößerte Ansicht auf die Tabelleninhalte in der Mitte:

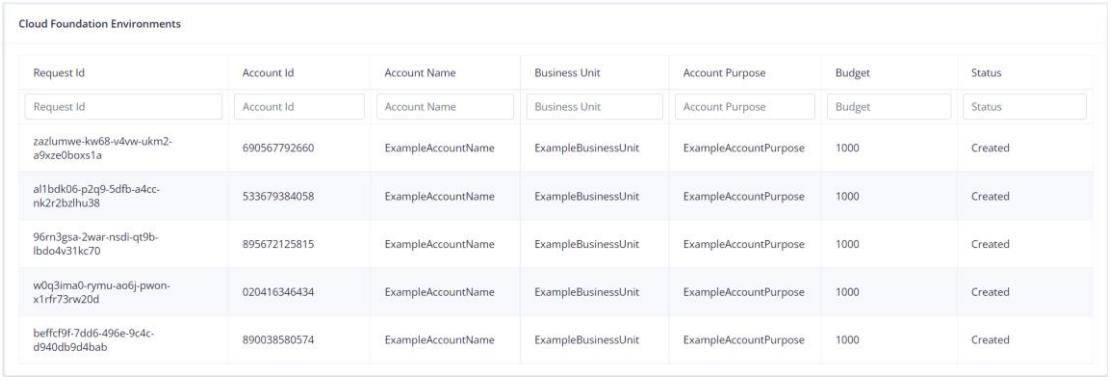

Abbildung 24: Dashboard Accountübersicht

Die Spalte „Request Id“ wird für jede Anfrage generiert und kann diese eindeutig identifizieren. Seitens AWS wird die Spalte „Account Id“ generiert und kann wiederum jeden AWS Account eindeutig identifizieren. Die Spalten „Account Name“, „Business Unit“, „Account

Purpose“ und „Budget” werden vom Nutzer in dem User Interface der Anwendung (siehe Abbildung 24) angegeben. Der aktuelle Stand der Anfrage wird in der Spalte „Status“ angezeigt.

Es folgt eine vergrößerte Ansicht auf die Liste auf der linken Seite:

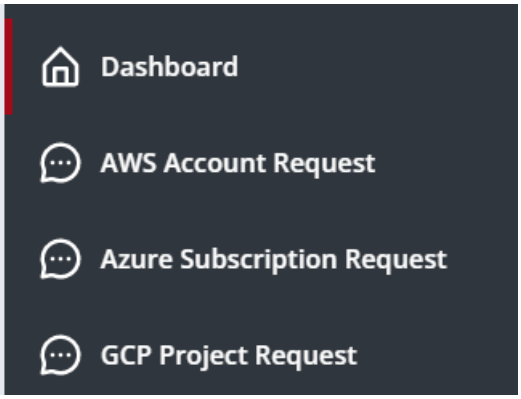

Abbildung 25: Dashboard Liste

Im Rahmen dieser Arbeit wurde der Punkt AWS Account Request umgesetzt und die weiteren Punkte dienen als Platzhalter um die Idee eines zentralen Account Management Systems in einer Multicloud Umgebung zu verdeutlichen.

Klickt man nun auf „AWS Account Request“ wird folgende Seite dargestellt:

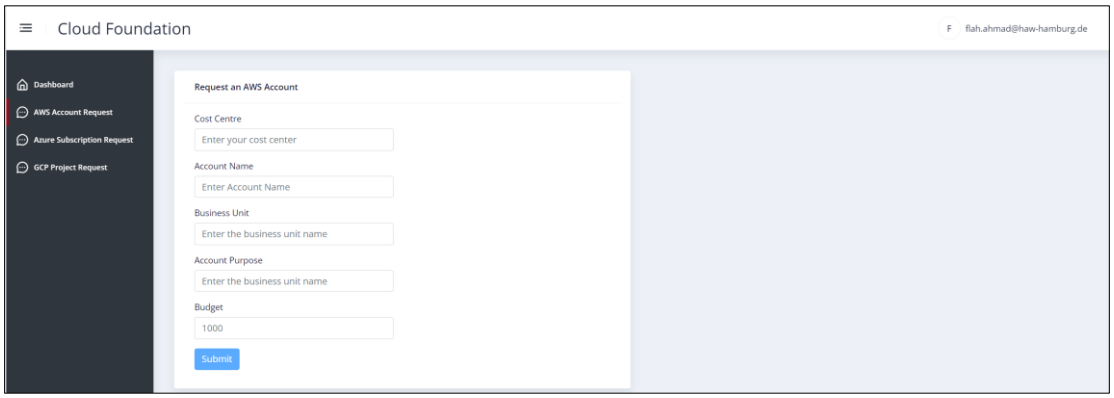

Abbildung 26: AWS Account Request

Es folgt eine vergrößerte Ansicht auf den mittleren Teil:

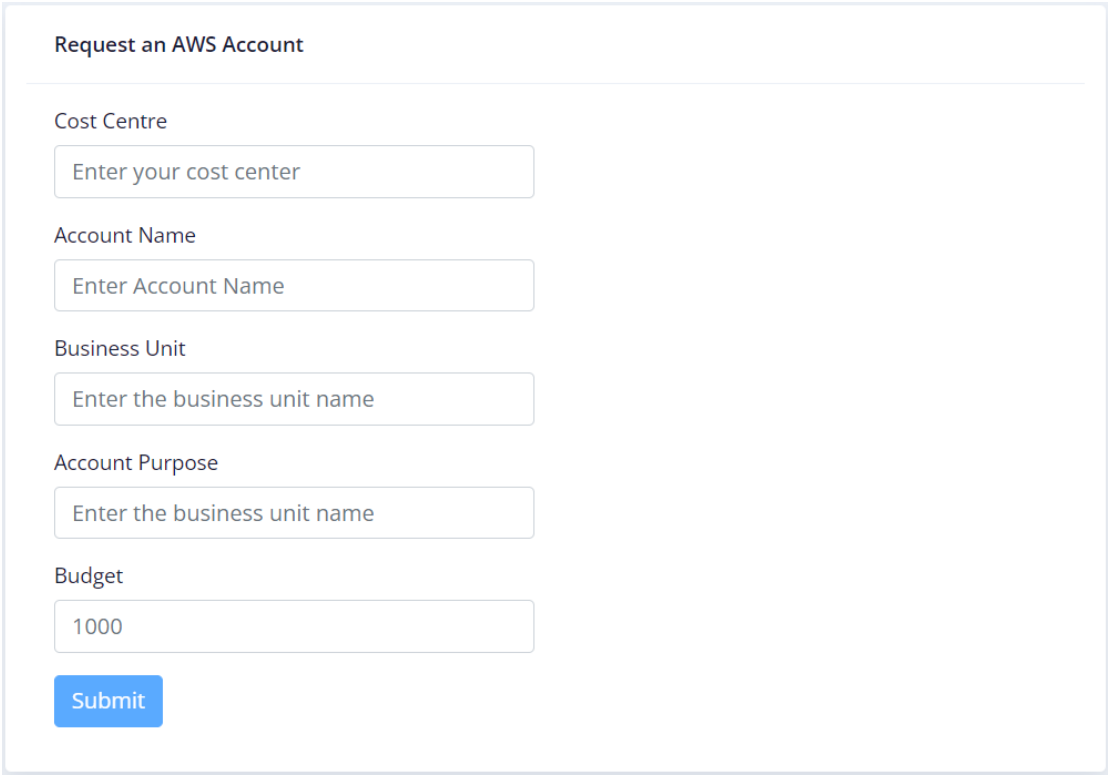

Abbildung 27: AWS Account Request Maske

In das Feld „Cost Centre" muss ein Unternehmensschlüssel eingetragen werden, der eine Abteilung oder ein Team eindeutig für die Zuordnung der entstandenen Kosten identifizieren kann. Das Feld „Account Name" sollte einen sinnvollen Namen für den Account beinhalten. In das Feld „Business Unit" sollte der Abteilungsname oder Teamname eingetragen werden. Das Feld „Account Purpose" dient als Platz, um zusätzliche Informationen über den Account einzutragen. In das Feld „Budget" muss das zur Verfügung stehende Budget für den Account eingetragen werden. Hier wird standardmäßig eine Email beim Erreichen von 80% und 100% zur Information versendet. Dies kann natürlich im Account selbst angepasst werden.

Nach dem Klick auf den „Submit" Button, wird man automatisch zurück zur Übersicht gebracht und der Status der Accounterstellung wird mit „Pending" dargestellt. Innerhalb von wenigen Sekunden aktualisiert sich der Inhalt und man sieht den Status „Erstellt".

Im gleichen Moment erhält der eingeloggte User eine Email mit den Accountdetails, sowie den Zugangsdaten zur Verwendung des Accounts:

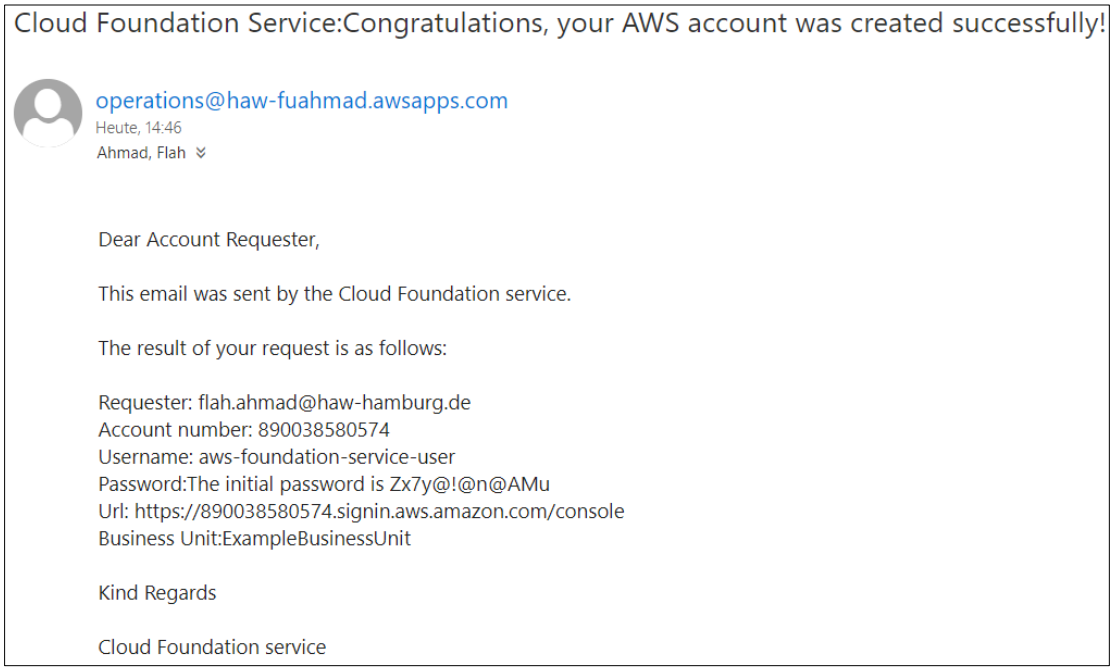

Abbildung 28: Emailbestätigung

Die URL in der Email führt zum direkten Login für den erstellten Account. Nach dem ersten Login mit dem Benutzernamen und Einmal-Passwort, wird man aufgefordert das Passwort zu ändern, um den Account nutzen zu können:

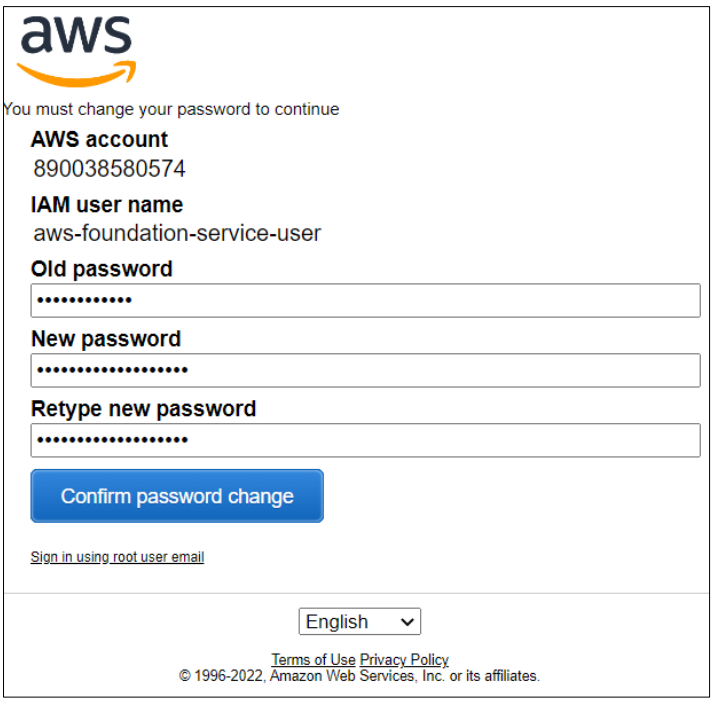

Abbildung 29: AWS Login Maske

Anschließend landet man auf der Landing Page von AWS als eingeloggter Benutzer und die gesamte Palette an Services und Produkten wird zur Verfügung gestellt:

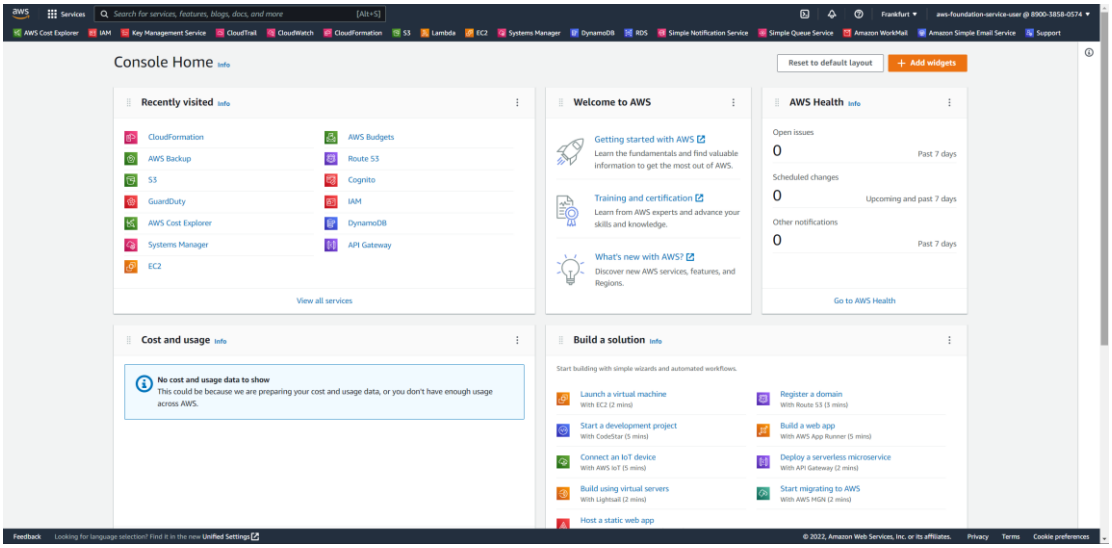

Abbildung 30: AWS Landing Page

8 Auswertung

In den folgenden Abschnitten folgt die abschließende Auswertung dieser Arbeit. Dabei soll zunächst eine Evaluation des Projekts erfolgen, ehe eine Alternativlösung vorgestellt wird. Anschließend sollen die noch offen gebliebenen Fragstellungen beantwortet werden und schlussendlich erfolgt ein Ausblick.

8.1 Evaluation des Projekts

In diesem Abschnitt soll ein Rückblick auf die Projektentwicklung geworfen werden. Hierbei sollen sowohl positive als auch negative Aspekte beleuchtet werden.

Alle vorgenommenen und in Abschnitt 7.1 beschriebenen Projektziele wurden erreicht und umgesetzt. Auch die Projektplanung inklusive der Aufwandsabschätzung zum zeitlichen Rahmen war größtenteils gut durchdacht. Lediglich der Entwicklungsschritt „Deploy Infrastructure“ hat aufgrund von einer starken Corona Erkrankung und einer Fehleinschätzung bezüglich der Komplexität mehr Zeit in Anspruch genommen als ursprünglich geplant. Obwohl wie in Abschnitt 7.2 beschrieben überwiegend managed Services zur Umsetzung des Projekts verwendet wurden, bedarf es doch eines großen Wissensstandes, um diese alle miteinander integrieren zu können. Hier musste noch viel Zeit investiert werden, um einzelne Wissenslücken zu füllen und das Projekt dann so wie geplant umsetzen zu können. Zusätzlich erschwerend kam die „Infrastructure as Code“ Komponente hinzu, die auf längere Sicht neben der Wiederverwendbarkeit und vielen anderen Vorteilen natürlich essentiell für ein solches Projekt und die Nutzung im Unternehmen ist und daher nicht vernachlässigt werden kann. Während der Entwicklung bringt sie jedoch im Gegenzug dazu einen nicht unerheblichen Mehraufwand mit sich. In der grafischen Oberfläche von AWS (AWS Web Console) kann man die Services einfacher und mit weniger Vorwissen verwenden (da vieles abgenommen und erklärt wird). Dabei gehen allerdings die Reproduzierbarkeit und das Nachvollziehen der Schritte verloren, weshalb

im Rahmen dieses Projekts darauf verzichtet wurde. Das reine YAML Skript, was für den AWS CloudFormation Abschnitt (Infrastrucutre as Code) entwickelt wurde und nur die Infrastrukturbereitstellung abdeckt, enthält fast 1000 Zeilen Code. Dies verdeutlicht den großen Umfang des Projekts. In einem Unternehmen würde üblicherweise ein ganzes Team an einem solchen Projekt arbeiten. Auf diese Art und Weise hätten einige Entwicklungsschritte parallel vollzogen werden können und das gesamte Projekt hätte schneller umgesetzt werden können. Die entwickelte Lösung ist enorm flexibel und hat keine Einschränkungen in Bezug auf die Weiterentwicklung und den Ausbau einzelner Funktionalitäten. Je nach Anforderungen und Richtlinien können Wächterfunktionen an die Accounts oder Accountgruppen angehängt werden und somit kann zu jeder Zeit kontrolliert werden, welche Workloads und Services in den Accounts laufen. Die Lösung ist ein sehr guter Anfang und bringt wichtige und essentielle Funktionalitäten für einen erfolgreichen Start mit AWS mit sich. Im nächsten Schritt müssten noch unternehmensspezifische Anforderungen und Richtlinien eingespielt werden, um das Produkt in einem Unternehmen einzusetzen (mehr dazu in Abschnitt 8.4).

8.2 Alternativlösung

Alternativ zu dem eigenständig entwickelten Produkt bietet AWS auch eine managed Lösung an, die automatisiert eine Landing Zone bereitstellt (AWS Control Tower). Wie in vielen Bereichen muss auch hier abgewägt werden, ob auf ein fertiges Produkt zurückgegriffen wird oder eigens etwas entwickelt werden soll. Die managed Lösung von AWS wirkt natürlich arbeitserleichternd und kann mit Standards viel abdecken. Eine Eigenentwicklung hingegen bietet die größtmögliche Flexibilität und Anpassbarkeit. Der Vollständigkeit halber soll der AWS Control Tower im Folgenden kurz vorgestellt werden.

Der AWS Control Tower ist ein AWS-nativer Service, um eine Multi Account Umgebung einzurichten und zu steuern. AWS Control Tower arrangiert dabei die Fähigkeiten verschiedener anderer AWS Services, einschließlich AWS Organizations, AWS Service Catalog und AWS Single Sign-On, um eine Landing Zone in kürzester Zeit aufzubauen. AWS Control Tower kann als Erweiterung der Funktionen von AWS Organizations betrachtet werden. Wenn eine größere Menge an Accounts gehostet werden sollen, ist es von Vorteil, einen Orchestrierungslayer zu haben, der die Kontobereitstellung und Kontoführung erleichtert. AWS Control Tower

kann dabei als Möglichkeit zur Bereitstellung von Accounts und Infrastruktur verwendet werden. AWS Control Tower ermöglicht es Kunden in den jeweiligen Teams, mithilfe konfigurierbarer Kontovorlagen in der Account Factory schnell neue AWS Accounts bereitzustellen. Dabei können die Administratoren jederzeit überwachen, ob die Accounts den Compliance Richtlinien des Unternehmens entsprechen. Zusammenfassend kann gesagt werden, dass AWS Control Tower eine sehr unkomplizierte Möglichkeit zum Einrichten und Verwalten einer sicheren AWS Umgebung für mehrere Accounts bietet. AWS Control Tower bietet im Detail folgende Funktionen:

Leitlinien:

Hierbei handelt es sich um Regeln auf hoher Ebene, die eine fortlaufende Governance für die gesamte AWS Umgebung bieten. Es wird hierbei zwischen zwei Arten von Leitlinien unterschieden: präventive und entdeckende. Diese können wiederum in drei Subkategorien unterteilt werden: obligatorisch, dringend empfohlen oder wahlweise.

Account Factory:

Die Account Factory ist eine konfigurierbare Kontovorlage, die dabei hilft, neue Accounts mit standardisierten Kontokonfigurationen zu versehen. AWS Control Tower bietet eine integrierte Account Factory, mit der die Kontobereitstellung automatisiert erfolgen kann.

Dashboard:

Das Dashboard dient den Administratoren zur kontinuierlichen Überwachung der Landing Zone. Auf dem Dashboard werden für das Unternehmen bereitgestellte Accounts, für die Richtliniendurchsetzung aktivierte Leitlinien, für die kontinuierliche Erkennung von Richtlinienverstößen aktivierte Leitlinien und nicht konforme Ressourcen angezeigt.

Automatisierte Kontokonfiguration:

AWS Control Tower automatisiert die Kontobereitstellung und -registrierung wie bereits beschrieben mithilfe einer Account Factory (oder eines „Verkaufsautomaten“). Die Account Factory kann AWS Accounts erstellen und registrieren und automatisiert das Anwenden von Compliance Richtlinien auf diese Accounts.

Zentralisierte Governance:

Durch die integrierte Nutzung der Funktionen von AWS Organizations richtet AWS Control Tower ein Framework ein, das eine einheitliche Compliance und Governance mit mehreren Accounts gewährleistet.

Erweiterbarkeit:

Kunden können eine eigene AWS Control Tower Umgebung erstellen oder eine bereits vorhandene erweitern, indem sie direkt in AWS Organizations und in der AWS Control Tower Konsole arbeiten. Dort kann die Landing Zone des AWS Control Tower aktualisiert werden, um etwaige Änderungen widerzuspiegeln (Internetquelle AWS Control Tower).

8.3 Beantwortung der Fragestellungen

Die Einrichtung einer Multi Account Landing Zone bietet für Unternehmen viele Vorteile. So kann durch den Einsatz einer Landing Zone beispielsweise Governance, Compliance und Sicherheit vereinfacht werden. Durch klar definierte Grenzen und fest zugeschriebene Verantwortlichkeiten für Identitäten und Dienste können sich Unternehmen komplett auf ihr Kerngeschäft konzentrieren und müssen sich nicht mit organisatorischen Fragen auseinandersetzen.

Cloud Computing birgt sowohl für Unternehmen als auch für Privatpersonen enormes Potenzial. Die Vorteile des Cloud Computing speziell für Unternehmen lassen sich in finanzielle, operative und strategische Vorteile unterordnen. Aus finanzieller Sicht punktet Cloud Computing mit enormen Kosteneinsparungen gegenüber traditioneller IT-Infrastruktur durch geringe Anschaffungskosten, eine niedrigere Kapitalbindung und Betriebs- und Wartungskosten, die gegen Null gehen. Dadurch entsteht eine hohe Kostentransparenz, welche für Unternehmen gleichzeitig eine erhöhte Flexibilität mit sich bringt, da es für sie leichter wird, auf wechselnde Kapazitätsbedarfe zu reagieren. Es wird möglich, genaue Kostenangaben für Teams, Bereiche oder Anwendungen einzusehen. Operativ betrachtet sorgt die Cloud für eine flexiblere, agilere und bedarfsgerechte Skalierung der IT-Infrastruktur von Unternehmen. Neue Projekte können schneller umgesetzt werden, da ein geringerer Administrationsaufwand besteht und der Zugriff zudem ortsunabhängig möglich ist. Gerade in Zeiten wie diesen, wo das Homeoffice für viele Arbeitnehmer immer attraktiver wird, spielt dies eine wesentliche Rolle. Aus strategischer

Perspektive befähigt die Cloud Unternehmen dazu, mit der Konkurrenz mithalten zu können. Durch die Fokussierung auf das Kerngeschäft werden Wettbewerbsvorteile gestärkt und neue Geschäftsbereiche können leichter erschlossen werden. Darüber hinaus kann der Eintritt in einen neuen Markt vereinfacht und beschleunigt vollzogen werden, da auch einzelne Abteilungen eines Unternehmens mit mehr Verantwortung ausgestattet sind und Entscheidungen eigenständig treffen können. Außerdem besteht ein nahezu grenzenloser Zugang zu neuen Technologien, die Verfügbarkeit zu IT-Systemen ist gesteigert und es besteht eine höhere Datensicherheit.

Wenn Unternehmen Cloud Computing einsetzen, stehen sie allerdings auch Hindernissen in den Bereichen Technik, Recht und Organisation gegenüber. Das Stichwort Cloud Compliance spielt hierbei eine wesentliche Rolle. Wenn die Compliance Strategie fehlt oder nicht ausreichend ausgearbeitet ist, können viele Probleme entstehen, die eine Migration in die Cloud für Unternehmen eher unattraktiv machen. An dieser Stelle knüpft das Errichten einer Landing Zone an. Durch den Aufbau einer Landing Zone können Compliance Anforderungen zentral eingebettet werden. Weiterhin stellen Sicherheitsaspekte ein Hindernis für die Nutzung der Cloud dar. So haben Nutzer die Befürchtung, dass die Abrufbarkeit der Daten in der Cloud über das Internet die Gefahr von Datenmissbrauch über internetbasierte Angriffe mit sich bringt. In diesem Zusammenhang steht auch der Missbrauch von Identitäten. Hier ist es wiederum die Aufgabe des Cloud Anbieters, ein Zugriffs- und Identitätsmanagement vorzuhalten, um das Cloud Computing sicherer zu gestalten. Auch hierbei kann die Landing Zone einen Mehrwert bieten, indem Zugriffs- und Identitätsmanagement zentralisiert wird und damit die Angriffsfläche für Missbrauch minimiert wird.

Insgesamt betrachtet wird das Cloud Computing oftmals mit der traditionellen IT-Infrastruktur, also einem unternehmenseigenen Rechenzentrum, verglichen. Auf den ersten Blick kann es so erscheinen, als ob der in-house Betrieb günstiger und damit attraktiver wäre. Meist hängt diese Beurteilung an einer fehlenden ganzheitlichen Betrachtung und der fehlenden Einsicht aller Kostenfaktoren. Zu den Kosten eines unternehmenseigenen Rechenzentrums zählt nämlich nicht nur die reine Soft- und Hardwareanschaffung, sondern auch die Mietkosten für die Lokalität, Energiekosten, Wartungs- und Instandhaltungskosten, Personalausgaben, Erneuerung der Hardware sowie das Vorhandensein mindestens eines zweiten Rechenzentrums zur

Ausfallsicherheit (plus alle genannten Grundkosten hierfür). Im Vergleich dazu, müssen derartige Grundkosten im Cloud Computing nicht von einem Unternehmen oder einer Privatperson einzeln getragen werden, sondern der Anbieter ist für die effiziente Nutzung und Verteilung verantwortlich. Dies ist in der folgenden Abbildung dargestellt. Der direkte Vergleich macht deutlich, dass die vermeintlichen Kosten beim Cloud Computing eventuell etwas höher erscheinen, als bei traditionellen IT-Infrastrukturen. Dies ist allerdings auf die Transparenz der Abonnementpreise durch die Cloud Anbieter zurückzuführen. Bei näherer Betrachtung wird schnell klar, dass beim Cloud Computing unter der Oberfläche nur noch sehr wenige Posten hinzukommen. Im Gegensatz dazu lockt die traditionelle IT-Infrastruktur mit scheinbar geringen Anschaffungskosten für beispielsweise Softwarelizenzen. Welche Kosten dann unter der Oberfläche noch folgen, ist vielen Anwendern zunächst nicht bewusst. Um eine fundierte Wahl treffen zu können, müssen also stets alle Kosten bis hin zur Stromversorgung berücksichtigt werden.

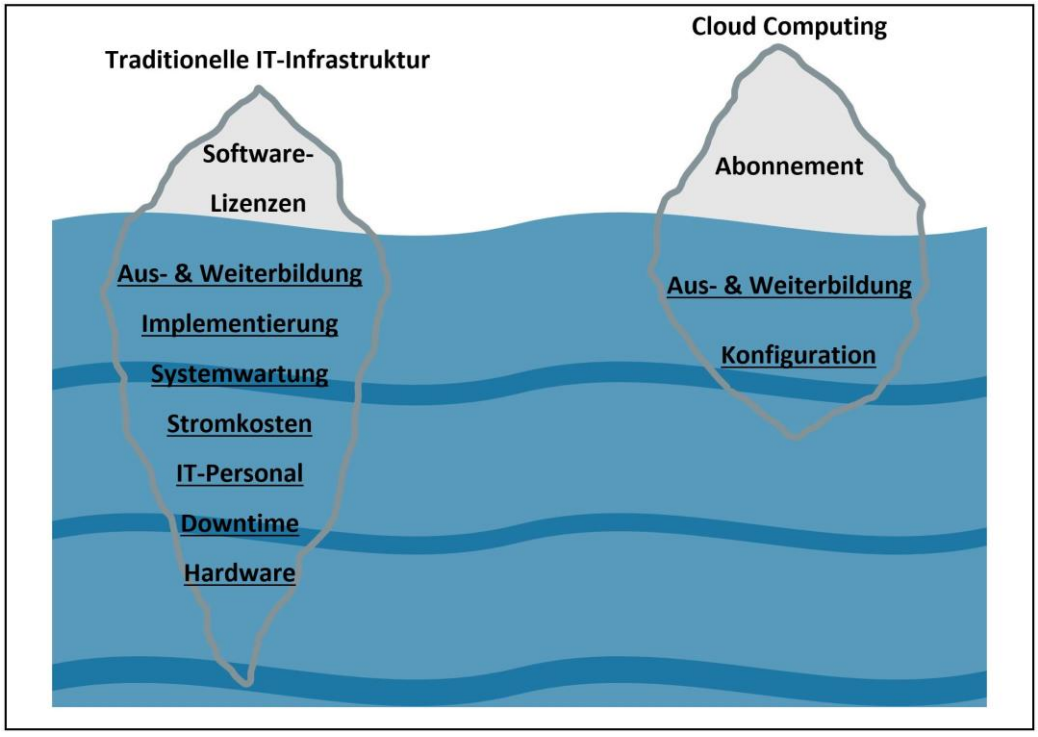

Abbildung 31: Traditionelle IT-Infrastruktur vs. Cloud Computing

Ein zentrales Account Management ermöglicht es, die Budget-, Sicherheits- und Compliance-Anforderungen eines Unternehmens besser umzusetzen. Für Administratoren einer Organisation besteht dadurch die Möglichkeit, bestehende Accounts in einer Organisation zusammenzufassen und zentral zu verwalten. Darüber hinaus besteht durch das zentrale Management die Möglichkeit der konsolidierten Fakturierung, wobei das Verwaltungskonto auf die Fakturierungsdaten, Kontoinformationen und Kontoaktivitäten von Mitgliedskonten innerhalb der Organisation zugreifen kann. Des Weiteren kann der Administrator Accounts oder Accountgruppen individuelle Zugriffsrichtlinien zuweisen und so steuern, welche Nutzer auf welchen Inhalt Zugriff erhalten. Außerdem kann der Administrator des Verwaltungskontos Service Control Policies verwenden, um Mitgliedskonten in ihrem Zugriff auf verschiedene Cloud Services, Ressourcen und einzelne API Aktionen einzuschränken. Auch ein Gesamtbackup aller Accounts einer Organisation lässt sich durch das zentrale Account Management realisieren.

Die Verwendung einer Umgebung mit mehreren Accounts hat viele Vorteile. So können Accounts beispielsweise leichter zugeordnet werden und auch die Abrechnung kann mit dieser Vorgehensweise erleichtert werden. Darüber hinaus werden beispielsweise auch Sicherheitskontrollen durch die Verwendung einer Umgebung mit mehreren Accounts flexibler. Durch das Arbeiten mit einer Landing Zone wird es ermöglicht, spezielle Mechanismen zu etablieren, um sicherzugehen, dass einzelne Accounts die geltenden Compliance Anforderungen erfüllen. Die Verwendung mehrerer Accounts ermöglicht es, die IT-Infrastruktur eines Unternehmens so einzurichten, dass die Geschäftsprozesse und Anforderungen erfüllt werden. Für die optimale Sicherheit in der Cloud ist eine Multi Account Umgebung beziehungsweise Landing Zone unabdingbar. Durch die dedizierten Accounts pro Workload oder Team können starke Grenzen gezogen werden, sodass sich jene nicht gegenseitig stören oder bei Problemen nicht andere Bereiche beeinflusst werden. Die Berechtigungen werden rollenbasiert vergeben, sodass jede Identität nur mit dem Mindestmaß an Rechten ausgestattet wird. So kann sichergestellt werden, dass kein unzulässiger Zugriff erfolgt. Durch die Trennung in den Accounts kann außerdem zusätzliche Sicherheit im Falle eines Datenmissbrauchs oder einer Kompromittierung gewonnen werden, da nicht die gesamte Organisation, sondern lediglich einzelne Accounts oder gar Ressourcen in den Accounts betroffen sind.

8.4 Ausblick

Eine Möglichkeit zur Weiterarbeit an dem Projekt besteht in der Individualisierung für ein beliebiges Unternehmen. Wie bereits in Abschnitt 8.1 beschrieben, wäre der nächste logische Entwicklungsschritt die Einspielung von unternehmensspezifischen Anforderungen und Richtlinien, um das Produkt dann tatsächlich in einem Unternehmen einzusetzen. Weiterhin könnte das User Interface noch um eine Adminübersicht erweitert werden. Aktuell können die Daten lediglich gelesen werden und Änderungen werden nicht unterstützt. Außerdem wird die Kostenstelle nicht gelistet. Auch dies könnte noch hinzugefügt werden.

Im Rahmen dieser Arbeit wurde, wie in Abschnitt 7.4 beschrieben, der Punkt AWS Account Request umgesetzt und die weiteren Punkte des User Interface (siehe Abbildung 25) dienten bisher nur als Produktvision. In einem nächsten Projekt könnte also die automatisierte Erstellung einer Landing Zone für Microsoft Azure oder die Google Cloud Platform umgesetzt und in die Anwendung integriert werden. Damit könnte ein einheitliches Portal über verschiedene Cloudanbieter hinweg erstellt werden und für das Unternehmen einfach nutzbar gemacht werden.

Literaturverzeichnis

Barton, T., 2014. *E-Business mit Cloud Computing. Grundlagen – Praktische Anwendungen –verständliche Lösungsansätze*. Wiesbaden: Springer.

Borges, G., 2018. *Einführung: Herausforderungen an das Identitätsmanagement im Cloud Computing.*
In: Borges, G. & Werners, B. (Hrsg.): Identitätsmanagement im Cloud Computing – Evaluation ökonomischer und rechtlicher Rahmenbedingungen (p. 1 – 10). Berlin: Springer.

Bounagui, Y.; Hafiddi, H. & Mezrioui, A., 2015. *Requirements Definition for a Holistic Approach of Cloud Computing Governance.*
Published at: 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA).

van Eyk, E. et. al., 2018. *Serverless is More: From PaaS to Present Cloud Computing*.
Published in: IEEE Internet Computing, vol. 22, no. 5, p. 8-17.

Golland, A. & Scheidereit, P., 2018. *Rechtliche Rahmenbedingungen des Identitätsmanagements im Cloud Computing.*
In: Borges, G. & Werners, B. (Hrsg.): Identitätsmanagement im Cloud Computing – Evaluation ökonomischer und rechtlicher Rahmenbedingungen (p. 53 – 104). Berlin: Springer.

Golland, A. & Schilling, A., 2018. *Cloud Computing: Einsatz- Bedrohungs- und Schadensszenarien.*
In: Borges, G. & Werners, B. (Hrsg.): Identitätsmanagement im Cloud Computing – Evaluation ökonomischer und rechtlicher Rahmenbedingungen (p. 11 – 32). Berlin: Springer.

Hahn, C., 2018. *Digitalisierung der IT-Industrie mit Cloud Plattformen – Implikationen für Entwickler und Anwender.*
In: Reinheimer, S. (Hrsg.): Cloud Computing – Die Infrastruktur der Digitalisierung (p. 155 - 168). Wiesbaden: Springer.

Hentschel, R. & Leyh, C., 2018. *Cloud Computing: Status quo, aktuelle Entwicklungen und Herausforderungen.*
In: Reinheimer, S. (Hrsg.): Cloud Computing – Die Infrastruktur der Digitalisierung (p. 3 - 20). Wiesbaden: Springer.

Khan, S. U., 2014. *Elements of Cloud Adoption.*
Published in: IEEE Cloud Computing (Volume: 1, Issue: 1, May 2014).

Kriegesmann, T. & Scheidereit, P., 2018. *Konkretisierung rechtlicher Anforderungen an das Identitätsmanagement im Cloud Computing.*
In: Borges, G. & Werners, B. (Hrsg.): Identitätsmanagement im Cloud Computing – Evaluation ökonomischer und rechtlicher Rahmenbedingungen (p. 137 – 184). Berlin: Springer.

Linthicum, David S., 2015. *The Evolution of Cloud Service Governance.*
Published in: IEEE Cloud Computing (Volume: 2, Issue: 6, Nov.-Dec. 2015).

Liu, H.,2013. *Big Data Drives Cloud Adoption in Enterprise.*
Published in: IEEE Internet Computing (Volume: 17, Issue: 4, July-Aug. 2013).

McGrath, G. & Brenner, P. R., 2017. *Serverless Computing: Design, Implementation, and Performance*.
Published at: 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), p. 405-410.

Mell, P. & Grance, T., 2011. *The NIST Definition of Cloud Computing. Recommendations oft he National Institute of Standards and Technlogy.*
Published in: NIST Special Publication 800-145. Gaithersburg: U.S. Department of Commerce.

Morgan, L. & Conboy, K., 2013. *Key Factors Impacting Cloud Computing Adoption.*
Published in: Computer (Volume: 46, Issue: 10, October 2013).

Munteanu, V.; Fortis, T. & Negru, V., 2012. *Service lifecycle in the cloud environment.*
Published in: 2012 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing.

Rajan, R. A. P., 2018. *Serverless Architecture – A Revolution in Cloud Computing.*
Published at: 2018 Tenth International Conference on Advanced Computing (ICoAC), 2018, p. 88-93.

Repschläger, J.; Pannicke, D. & Zarnekow, R., 2014. *Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale*.
Published in: HMD Praxis der Wirtschaftsinformatik 47 (p. 6 – 15).

Schilling, A., 2018. *Schutzmaßnahmen zur sicheren Identifizierung und Authentifizierung für Cloud-basierte Systeme*.
In: Borges, G. & Werners, B. (Hrsg.): Identitätsmanagement im Cloud Computing – Evaluation ökonomischer und rechtlicher Rahmenbedingungen (p. 33 – 52). Berlin: Springer.

Thuraisingham, B., 2020. *Cloud Governance.*
Published at: 2020 IEEE 13th International Conference on Cloud Computing (CLOUD).

Internetquellen:

Amazon API Gateway: https://aws.amazon.com/de/api-gateway/ (zuletzt abgerufen am 15.07.22)

Amazon Cognito: https://aws.amazon.com/de/cognito/ (zuletzt abgerufen am 15.07.22)Angular: https://angular.io/ (zuletzt abgerufen am 15.07.22)

AWS Amplify: https://aws.amazon.com/de/amplify/ (zuletzt abgerufen am 15.07.22)

AWS Cloud Adoption Framework: https://aws.amazon.com/de/professional-services/CAF/ (zuletzt abgerufen am 02.03.22)

AWS Cloud Formation: https://docs.aws.amazon.com/de_de/AWSCloudFormation/latest/UserGuide/Welcome.html (zuletzt abgerufen am 03.03.22)

AWS Control Tower: https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html (zuletzt abgerufen am 03.03.22)

AWS IAM: https://aws.amazon.com/de/iam/ (zuletzt abgerufen am 15.07.22)

AWS Lambda: https://aws.amazon.com/de/lambda/ (zuletzt abgerufen am 15.07.22)

AWS Landing Zone: https://aws.amazon.com/solutions/implementations/aws-landing-zone/?nc1=h_ls (zuletzt abgerufen am 02.03.22)

AWS Open API: https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-import-api.html (zuletzt abgerufen am 02.03.22) NEU!

AWS Organizations: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html (zuletzt abgerufen am 03.03.22)

AWS Organizations Best Practices: https://aws.amazon.com/de/blogs/mt/best-practices-for-organizational-units-with-aws-organizations/ (zuletzt abgerufen am 04.03.22)

AWS Security Best Practices: https://aws.amazon.com/de/blogs/security/getting-started-follow-security-best-practices-as-you-configure-your-aws-resources/ (zuletzt abgerufen am 02.03.22)

Azure Landing Zone: https://docs.microsoft.com/de-de/azure/cloud-adoption-framework/ready/landing-zone/ (zuletzt abgerufen am 02.03.22)

Bitbucket: https://bitbucket.org/product/de/guides/getting-started/overview (zuletzt abgerufen am 15.07.22)

Bitbucket Pipelines: https://bitbucket.org/product/de/features/pipelines (zuletzt abgerufen am 15.07.22)

Bitbucket Workspace: https://support.atlassian.com/bitbucket-cloud/docs/variables-and-secrets/ (zuletzt abgerufen am 03.03.22)

Lambda Python: https://docs.aws.amazon.com/lambda/latest/dg/lambda-python.html (zuletzt abgerufen am 15.07.22)

Ngx-Template: https://akveo.github.io/ngx-admin/ (zuletzt abgerufen am 02.03.22)

Python: https://aws.amazon.com/de/sdk-for-python/ (zuletzt abgerufen am 15.07.22)

Source Control: https://aws.amazon.com/de/devops/source-control/ (zuletzt abgerufen am 15.07.22)

Statista AWS: https://www.statista.com/statistics/422273/yoy-quarterly-growth-aws-revenues/ (zuletzt abgerufen am 27.06.22)

Statista Cloud Marktanteile: https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/ (zuletzt abgerufen am 27.06.22)

Statista Corona & Homeoffice: https://de.statista.com/statistik/daten/studie/1204173/umfrage/befragung-zur-homeoffice-nutzung-in-der-corona-pandemie/ 27.06.22)

Statista Covid & Cloud: https://www.statista.com/statistics/1225221/covid-impact-cloud-usage-global/ (zuletzt abgerufen am 27.06.22)

Statista Umsatz Cloud Computing: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/ (zuletzt abgerufen am 27.06.22)

Swagger: https://swagger.io/docs/specification/about/ (zuletzt abgerufen am 15.07.22)

Unterscheidung CI/CD: https://www.atlassian.com/de/continuous-delivery/principles/continuous-integration-vs-delivery-vs-deployment (zuletzt abgerufen am 03.03.22

Abbildungen:

Begleit-CD

Inhaltsverzeichnis:

1. Code-Repositories (Root-Verzeichnis)
    a. api (Verzeichnis)
    b. application (Verzeichnis)
    c. bootstrap_account (Verzeichnis)
    d. frontend (Verzeichnis)
    e. infrastructure (Verzeichnis)
    f. user_validation (Verzeichnis)
    g. README.md
2. Masterarbeit (PDF-Datei)

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

_____	_____	_____
Ort	Datum	Unterschrift im Original