Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Agin Punneliparambil

Integration von MS Azure Sicherheitsfunktionen am Beispiel der HAW Hamburg

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Agin Punneliparambil

Integration von MS Azure Sicherheitsfunktionen am Beispiel der HAW Hamburg

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Angewandte Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Herr Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Herr Prof. Dr. Martin Hübner

Abgegeben am 13.07.2020

Agin Punneliparambil

Thema der Arbeit
Integration von MS Azure Sicherheitsfunktionen am Beispiel der HAW Hamburg

Stichworte
IT-Sicherheit, Cloud Computing, Microsoft Azure, Sicherheitsfunktionen

Kurzzusammenfassung
Das Ziel dieser Arbeit ist die Identifikation von MS-Azure-Sicherheitsfunktionen und deren Integration in einer Hochschule. Repräsentativ für eine Hochschule wird die HAW Hamburg ausgewählt. Anhand eines IT-Sicherheitsmodelles werden Sicherheitsanforderungen an den Einsatz von Cloud-Anwendungen durch die HAW definiert. Mithilfe des Anforderungskataloges werden Azure-Sicherheitsfunktionen identifiziert und überprüft, wie diese in der HAW eingeführt werden können. Die Ergebnisse zeigen, in welchen Bereichen Cloud-Anwendungen und ihre Sicherheitsmechanismen integriert werden können.

Agin Punneliparambil

Title of the paper
Integration of MS Azure security features using the example of HAW Hamburg

Keywords
IT-Security, Cloud Computing, Microsoft Azure, Security features

Abstract
The aim of this work is to identify MS-Azure safety functions and their integration in a university. The HAW Hamburg is selected as representative for a university. Using an IT security model, security requirements for the use of cloud applications by the HAW are defined. With the help of the catalogue of requirements, Azure security functions will be identified and will be checked how they can be introduced at HAW. The results show in which areas cloud applications and their security mechanisms can be integrated.

Inhaltsverzeichnis

Abbildungsverzeichnis 7

Tabellenverzeichnis 8

1 Einleitung 9

1.1 Die Unsicherheit des Cloud Computings 9

1.2 Zielsetzung und Vorgehen 10

1.3 Abgrenzung 11

1.4 Aufbau der Arbeit 11

2 Grundlagen 12

2.1 Definition des Cloud Computing 12

2.2 Cloud-Service-Modelle 13

2.2.1 Software as a Service 14

2.2.2 Platform as a Service 15

2.2.3 Infrastructure as a Service 16

2.3 Cloud-Bereitstellungsmodelle 16

2.3.1 Public Cloud 16

2.3.2 Private Cloud 17

2.3.3 Hybrid Cloud 17

3 Microsoft Azure 19

3.1 Office 365 20

3.1.1 E-Mail-Verschlüsselung 20

3.2 SharePoint Online 21

3.2.1 Sicheres Teilen 22
3.2.2 Zugriffskontrolle durch Geräte und Netzwerkadressen 23
3.2.3 Authentifizierung 24
3.3 Azure Active Directory 25
3.3.1 Role Based Access Control (RBAC) 26
3.3.2 Multi-Faktor Authentifizierung (MFA) 26
3.3.3 Single Sign On 27
3.4 Azure Storage 28
3.4.1 Speicheroptionen 28
3.4.2 Verschlüsselung 29
3.4.3 Datenredundanz 30
4 Sicherheitsanforderungen an eine Cloud 32
4.1 Auswahl der Sicherheitsmodelle 32
4.2 CIA-Modell 35
4.3 Parkerian Hexad 36
4.3.1 Besitz/Kontrolle 36
4.3.2 Authentizität 37
4.3.3 Nützlichkeit 37
4.4 Aufstellung der Sicherheitsanforderungen 38
4.4.1 Sicherheitsanforderungen: Vertraulichkeit 38
4.4.2 Sicherheitsanforderungen: Integrität 40
4.4.3 Sicherheitsanforderungen: Verfügbarkeit 40
4.4.4 Sicherheitsanforderungen: Besitz/Kontrolle 41
4.4.5 Sicherheitsanforderungen: Authentizität 43
4.4.6 Sicherheitsanforderungen: Nützlichkeit 44
5 Sicherheitsanalyse von MS Azure 45
5.1 Sicherheitsanforderungen: Vertraulichkeit 47
5.2 Sicherheitsanforderungen: Besitz/Kontrolle 51
5.3 Sicherheitsanforderungen: Daten-Integrität 54
5.4 Sicherheitsanforderungen: Authentizität 55
5.5 Sicherheitsanforderungen: Verfügbarkeit 57

5.6 Sicherheitsanforderungen: Nützlichkeit 59
5.7 Azure Sicherheitsereignisse 59
5.8 Bewertung der Azure-Schwachstellen 61
5.8.1 STRIDE-Bedrohungen 62
5.8.2 Azure Sicherheitslücken 63
5.9 Abschließende Bewertung 65
6 Integration von MS AZURE 66
6.1 Sicherheitsfunktionen in Azure 66
6.2 Integration der technischen Sicherheitsfunktionen 67
7 Zusammenfassung und weiterführende Aspekte 70
7.1 Zusammenfassung 70
7.2 Weiterführende Aspekte 73
Literaturverzeichnis 74

Abbildungsverzeichnis

Abbildung 1: Cloud-Service-Modelle 14
Abbildung 3: SharePoint Online Authentifizierungsschritte 25
Abbildung 4: RBAC Rollen- und Rechtezuweisung.....26
Abbildung 5: Verteilung der Verantwortung in Cloud-Modellen 46

Tabellenverzeichnis

Tabelle 1: MFA Identifizierungsverfahren 27
Tabelle 2: Informationssicherheitsziele aus der Literatur und von IT-Normen 34
Tabelle 3: Ergebnisse der Sicherheitsanforderung Vertraulichkeit 51
Tabelle 4: Ergebnisse der Sicherheitsanforderung Besitz/Kontrolle 54
Tabelle 5: Ergebnisse der Sicherheitsanforderung Integrität 55
Tabelle 6: Ergebnisse der Sicherheitsanforderung Authentizität 57
Tabelle 7: Ergebnisse der Sicherheitsanforderung Verfügbarkeit 58
Tabelle 8: Ergebnisse der Sicherheitsanforderung Nützlichkeit 59
Tabelle 9: STRIDE-Bedrohungen 62
Tabelle 10: Azure Schwachstellen 64
Tabelle 11: Gegenüberstellung von HAW-Cloud und OneDrive 68

1 Einleitung

1.1 Die Unsicherheit des Cloud Computings

Das Cloud Computing[1] erfreut sich Jahr für Jahr gesteigerter Beliebtheit, sowohl bei Unternehmen als auch bei privaten Anwendern. Zu den meistgenutzten Funktionen gehört die Datenspeicherung. Daten werden bei einem Drittanbieter gespeichert und abgerufen. Dabei werden seine Infrastruktur und Anwendung genutzt. Zu den prominentesten Beispielen gehören iCloud von Apple, Google Drive und OneDrive von Microsoft. Ein weiterer Hauptanwendungsfall ist die Verlagerung von IT-Workloads auf die Cloud-Infrastruktur. Immer mehr kleine und mittelständische Unternehmen nutzen die Ressourcen von Cloud-Anbietern und verzichten auf lokale Lösungen [1]. Die Vorteile sind unter anderen entfallende Anschaffungskosten von Hard- und Software sowie deren Instandhaltung. Hinzu kommt die Flexibilität bei Cloud-Lösungen. Nutzer können die Cloud nach ihrem eigenen Bedarf skalieren und müssen nur für tatsächlich genutzte Ressourcen zahlen (Pay-per-Use-Prinzip).
Die oben genannten Gründe würden für zahlreiche Unternehmen den Wechsel von einer lokalen Lösung zu einer Cloud rechtfertigen. Dennoch meiden viele den kompletten Umstieg. Begründet wird dies zum Teil mit dem mit der Cloud-Nutzung verbundenen Kontrollverlust und mit Sicherheitsrisiken.

Anders als bei einem lokal betriebenen Server verliert eine Organisation die Kontrolle über den Schutz ihrer Daten und Systeme. Die Verantwortung liegt dann zum Teil bei den Cloud-Anbietern. Diese müssen Sicherheitsmechanismen auf Hard- und Software-Ebene implementieren, um Kunden eine sichere Nutzung zu gewährleisten. Ansonsten droht ihnen der Verlust aktueller oder potenzieller Kunden. Umfragen [2, 3] ergaben, dass Kunden der

[1] Das Kapitel bezieht sich auf eine öffentliche Cloud. Kurze Definition: Eine für alle Personen über das Internet erreichbare Cloud. Geteilte Nutzung von Hard- und Software. Ausführliche Erläuterung in Kapitel 2.2.1

öffentlichen Cloud primär um deren Sicherheit besorgt sind. Die Umfrage aus dem Jahr 2019 [3] hat Unternehmen nach Sicherheitsvorfällen in der öffentlichen Cloud befragt. Als Zeitspanne für die aufgetretenen Vorfälle wurden die vorangegangenen 12 Monate definiert. Der Umfrage nach haben 28 % der Unternehmen angegeben, dass sie mit Sicherheitsereignissen konfrontiert wurden. Datenleck-Vorfälle führen dabei mit einem Anteil von 27 % die Liste an, gefolgt von Malware-Infektionen (20 %), kompromittierten Konten (19 %) und Schwachstellenausnutzung (17 %). Cloud-Anbieter betonen häufig, dass die Sicherheit ihrer Dienste für sie die höchste Priorität habe. Denn Sicherheitsvorfälle geben dem Kunden Raum für Zweifel. Die fehlende Kontrolle über IT-Systeme führt zu Unsicherheit bei der Nutzung von Cloud-Lösungen.
Hinzu kommt, dass die Cloud-Umgebung für viele IT-Mitarbeiter Neuland ist. Durch Fehlkonfigurationen können ernste Bedrohungen entstehen. Letzten Endes bleibt die Frage bestehen, ob die von Cloud-Anbietern getroffenen Sicherheitsvorkehrungen ausreichen, um die Nutzung zu begründen.

1.2 Zielsetzung und Vorgehen

Das Ziel dieser Bachelorarbeit ist es herauszufinden, wie Microsoft Azure mit seinen Sicherheitsfunktionen im Kontext einer Hochschule integriert werden könnte. Hierfür wird repräsentativ die HAW Hamburg ausgewählt. Um das Ziel zu erreichen, müssen zuerst die angebotenen Funktionen untersucht werden. Die Sicherheitsanalyse von Microsoft Azure und die Frage, inwieweit die Sicherheitsanforderungen der HAW bezüglich des Cloud Computings erfüllt werden, ist Kernbestandteil dieser Arbeit. Zunächst werden relevante Azure-Dienste vorgestellt und ihre Sicherheitsmechanismen erläutert. Eine vollständige Untersuchung der angebotenen Dienste ist im Rahmen dieser Arbeit nicht realisierbar. Im Anschluss erfolgt die Erarbeitung der Sicherheitsanforderungen an das Cloud Computing im Kontext einer Hochschule. Die Notwendigkeit, sie zu definieren, begründet sich durch das Fehlen eines allgemeingültigen Sicherheitsanforderungskatalogs für die Cloud. Zunächst werden Schutzziele aufgestellt, aus denen Sicherheitsanforderungen abgeleitet werden. Die Anforderungserarbeitung ermöglicht die anschließende Untersuchung der Sicherheitsfunktionen von Azure. Für eine fundierte Analyse werden zudem bekannte Sicherheitsvorfälle und -lücken von Azure hinzugezogen. Darauf aufbauend werden Anwendungsfälle der HAW Hamburg aus den Bereichen Forschung und Lehre betrachtet und es wird überprüft, inwieweit diese durch die Azure-Sicherheitsmechanismen abgedeckt werden können.

1.3 Abgrenzung

In dieser Arbeit werden primär die sicherheitsspezifischen Aspekte der Microsoft-Cloud behandelt. Neben der Sicherheit einer Cloud haben noch verschiedene andere Faktoren Einfluss auf die Wahl des Cloud-Anbieters. Dazu zählen die Kostenrechnung und der Vergleich mit anderen Cloud-Anbietern. Diese sind nicht Bestandteil dieser Arbeit. Ausgeschlossen werden zudem die technischen Implementationen von Sicherheitsfunktionen.
Bei der Betrachtung der HAW Hamburg stehen die Stakeholder Forschung und Lehre (Dozenten und Studierende) im Vordergrund. Ein weitere Nutzergruppe sind die Personen aus der Hochschulverwaltung. Diese unterliegt den Regularien der Hansestadt Hamburg und kann somit nicht uneingeschränkt zur Zielgruppe von hochschulinternen Vorgaben bezüglich der genutzten Dienste werden. Hier sind die geltenden Landesdatenschutzgesetze zu beachten und die Frage, ob diese die Nutzung einer öffentlichen Cloud zulassen.

1.4 Aufbau der Arbeit

Diese Arbeit ist in insgesamt sieben Kapitel gegliedert. Das erste Kapitel ist die Einleitung und beinhaltet die Motivation sowie die Zielsetzung und Vorgehensweise der Arbeit. In Kapitel 2 werden die Grundlagen des Cloud Computing vorgestellt. Dazu gehören die verschieden Cloud-Service- und die Cloud-Bereitstellungs-Modelle. In Kapitel 3 wird die Microsoft-Cloud Azure und einige ihrer relevanten Dienste und Sicherheitsfunktionen vorgestellt. In Kapitel 4 werden zwei Sicherheitsmodelle miteinander verglichen, von denen eines für die nachfolgende Erarbeitung der Sicherheitsanforderungen an eine Cloud ausgewählt wird. Ziel des Kapitels ist die Erstellung eines Anforderungskatalogs. Dieser wird in Kapitel 5 für die Anforderungsanalyse verwendet. Das Kapitel beinhaltet zudem die Analyse von Sicherheitsvorfällen und -lücken. Kapitel 6 befasst sich mit der Integration der Sicherheitsfunktionen von Azure am Beispiel der HAW Hamburg. Das Fazit erfolgt in Kapitel 7. In diesem werden abschließend weiterführende Aspekte thematisiert.

2 Grundlagen

In diesem Kapitel wird die Definition des Cloud Computing betrachtet und welche Eigenschaften eine Cloud charakterisieren. Nachfolgend werden drei Cloud-Service-Modellen (CSM) und drei Cloud-Bereitstellungsmodellen (CB) vorgestellt und miteinander verglichen.

2.1 Definition des Cloud Computing

Eine allgemeingültige Definition des Cloud Computing ist in der Literatur nicht vorhanden. Die US-amerikanische Standardisierungsinstitution National Institute of Standards and Technology (NIST) beschreibt den Begriff wie folgt:

„Cloud Computing ist ein Modell der Datenverarbeitung, mit dem bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zugegriffen werden kann. Diese können schnell und mit minimalem Verwaltungsaufwand bzw. geringer Serviceprovider-Interaktion zur Verfügung gestellt werden.“ [2]

Diese Definition wird ebenfalls von der ENISA (European Union Agency for Cybersecurity) verwendet.

[2] [4]. Zitiert nach [5] (Deutsche Übersetzung)

Das NIST beschreibt zudem fünf essenzielle Eigenschaften des Cloud Computing[4]:

1. **On-demand self-service**. Ein Konsument kann eigenständig die Ressourcen, wie z.B. Rechenleistung und Speicher, provisionieren ohne die menschliche Interaktion mit dem Service Provider.
2. **Broad network access**. Der Zugriff auf die Services erfolgt über das Netzwerk und unabhängig von Klient-Plattformen, wie Handy, Tablet oder Laptop.
3. **Resource pooling**. Die Ressourcen des Anbieters werden für eine breite Masse an Nutzern zur Verfügung gestellt und isoliert. Die Zuteilung von physischen und virtuellen Ressourcen erfolgt dynamisch nach den Bedürfnissen der Klienten. Sie wissen zudem nicht den genauen Standort der Dienste, können aber den Speicherort ihrer Daten bestimmen oder einsehen.
4. **Rapid elasticity**. Ressourcen können schnell bedarfsabhängig hinzugebucht oder abgegeben werden. Der Prozess erfolgt manuell oder automatisch. Für die Klienten entsteht somit eine Illusion von unendlichen Kapazitäten.
5. **Measured service**. Der Ressourcenverbrauch kann berechnet, überwacht und kontrolliert werden. Die Daten stehen Cloud-Kunden und dem Provider zur Verfügung.

2.2 Cloud-Service-Modelle

Jeder Cloud-Dienst ist ein Service des Anbieters für seine Kunden. Die Angebote werden geleast, nach dem Pay-Per-Use Prinzip genutzt oder stehen kostenlos zur Verfügung. Eine CRM-Software kann beispielsweise für einen oder mehrere Monate für ein entsprechende Gebühr genutzt werden. Virtuelle Maschinen hingegen werden in den meisten Fällen nach der Ressourcenverbrauch abgerechnet.
Die Cloud-Services lassen sich in drei Hauptkategorien unterteilen, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). In Abbildung 1 wird ein Cloud-Computing-Stack dargestellt. Als Cloud-Computing-Stack werden Hardware- und Softwarelösungen der Cloud, die aufeinander aufbauen, bezeichnet.

Die Abbildung zeigt den Grad der Eigenverantwortung abhängig vom CSM und der traditionellen IT. Mit traditioneller IT ist das Betreiben eines eigenen Servers[3] im eigenen Datenzentrum eines Unternehmens gemeint. Die Verantwortung für die Hardware bis hin zu der genutzten Software liegt in diesem Fall bei der Organisation selbst. Im Vergleich zum Cloud Computing, bietet dieses Modell die meiste Kontrolle über die verwendeten Systeme. Die Kontrolle über die Sicherheit ist ein weiterer Vorteil. Sicherheitsfunktionen können frei

[3] Lokale Softwarelösungen werden im Englischen als On-Premises bezeichnet.

gewählt werden und die Daten werden in den meisten Fällen lokal gespeichert. Folglich verliert eine Organisation die Kontrolle über ihre Daten nicht.

In der Abbildung ist zu sehen, wie die Aufgabenbereiche, abhängig von dem Modell, an den Cloud-Anbieter delegiert wird. Zu erkennen ist zudem, wie die drei Services aufeinander aufbauen. Im Folgenden werden die Services im Einzelnen betrachtet.

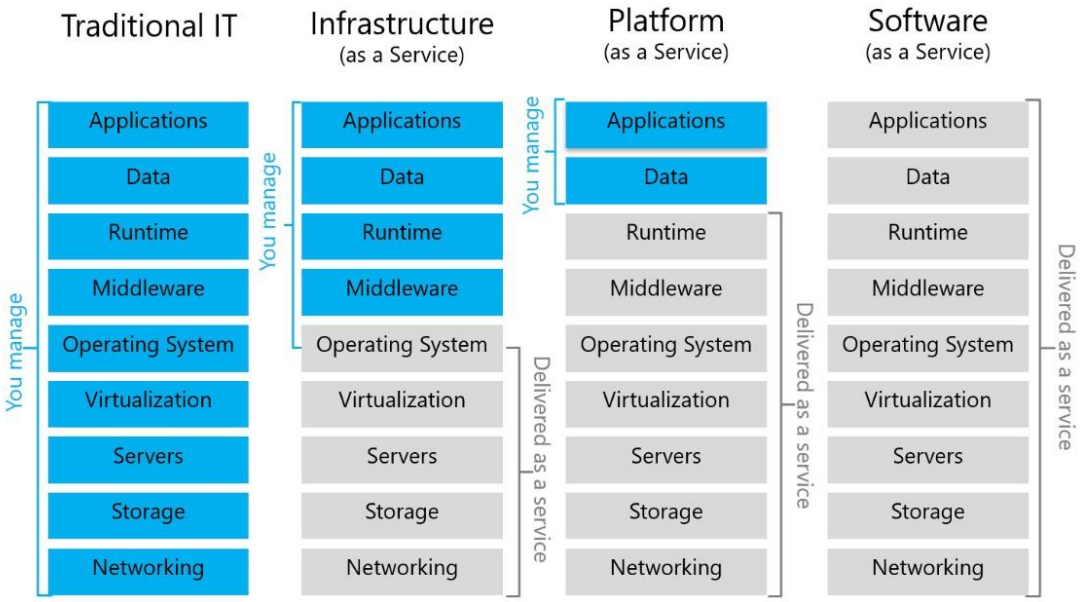

Abbildung 1: Cloud-Service-Modelle [6]

2.2.1 Software as a Service

Bei dem klassischen Ansatz wird Software dem Kunden als lokales Installationsobjekt zur Verfügung gestellt. Für die Installation, das Updaten und die geforderte Hardware ist der Benutzer verantwortlich. Mit der stetig steigenden Bandbreite des Internets ergibt sich die Möglichkeit, Software direkt beim Anbieter zu deployen und den Zugriff per Internet anzubieten. Weitere Faktoren sind die Fortschritte, die in der Virtualisierung erreicht werden konnten, die Weiterentwicklung von Netzwerkkommunikationsprotokollen und die der physikalischen Schicht [6].
Mit dem SaaS-Konzept sollen Programme nicht auf privater Hardware betrieben werden, sondern der Service-Anbieter stellt die Rechenleistung und die weiteren Komponenten (siehe Abb. 1) zur Verfügung. Die Interaktion mit den Programmen erfolgt üblicherweise über

einen Webbrowser oder eine App. Die Daten werden bei dem Cloud-Anbieter gespeichert. Zudem ist dieser für die Sicherung der Daten verantwortlich.

Die Nutzung einer SaaS-Lösung verringert die Investitionsausgaben durch das Mieten der Software im Vergleich zu einer Neuanschaffung. Mitarbeiter eines Unternehmens können ihre eigenen Endgeräte nutzen und unabhängig von ihrem Standort auf ihre Daten und die Programme zugreifen. Dafür erforderlich sind eine stabile Internetverbindung und eine Benutzerauthentifizierung. Weitere Vorteile sind das Entfallen der Instandhaltungskosten und die sofortige Verfügbarkeit der Anwendung. Für die Instandhaltung und Weiterentwicklung der Software ist der Anbieter verantwortlich. Die Kunden sparen nicht nur Geld, sondern auch Zeit. Die bei der lokalen Nutzung einer Software notwendigen Installationsschritte erübrigen sich. Für die Nutzung sind lediglich ein Zugriffspunkt, z.B. ein Webbrowser, und Authentisierungsschritte notwendig.

Neben den oben genannten Vorteilen existieren Nachteile, die gegen eine SaaS-Lösung sprechen könnten. Die Kontrolle der Daten und ihre Sicherheit wird an den Service-Anbieter delegiert. Der Kunde muss Vertrauen in die Sicherheitsmaßnahmen des Anbieters haben. Zudem kann er die Programme nicht frei an seine Bedürfnisse anpassen. Die Programm-Upgrades könnten nicht seinem Wunsch entsprechen und würden eine Beendigung der SaaS-Nutzung begründen. Dies kann sich als schwierig erweisen, wenn eine gewisse Abhängigkeit zu dem Dienst entstanden ist oder die Portierung der Daten zu dem Dienst eines anderen Herstellers vom Anbieter erschwert wird.
Die Anforderung an ein schnelles Internet kann als Nachteil ausgelegt werden, da nicht jedes Land bzw. jede Region diese erfüllen kann. Verbindungsabbrüche könnten die Produktivität eines Unternehmens beinträchtigen.

2.2.2 Platform as a Service

Platform as a Service bietet dem Kunden eine Plattform aus Hardware und Software für die Entwicklung von Anwendungen. Die konkrete Zielgruppe für diesen Service sind die Entwickler. In PaaS können Anwendungen direkt über das Internet entwickelt, getestet und in der Cloud für die Benutzer bereitgestellt werden. [7] Der Cloud-Anbieter ist für die Sicherung des Betriebssystems und der physischen Infrastruktur verantwortlich. Kunden hingegen müssen ihre Anwendung und die Daten eigenständig sichern.
PaaS erleichtern die Kollaboration mit anderen Entwicklern. Diese benötigen lediglich eine Internetverbindung und einen Computer. Weitere allgemeine Cloud-Vorteile wie die Skalierbarkeit und die Ersparnis der Anschaffungskosten sind weiterhin vorhanden.
Nachteile ergeben sich durch die eingeschränkte Portabilität der entwickelten Anwendung. Die meisten Plattformen bieten nur eine auserwählte Kollektion an Programmiersprachen. Der Kunde muss dies bei der Auswahl der Plattform berücksichtigen. In einigen Fällen kann daraus ein Vendor-Lock-In resultieren. Das bedeutet, dass eine Abhängigkeit zu der genutzten Plattform entsteht und ein Transfer der Anwendung zu einem anderen Anbieter

problematisch wird. Zudem können Entwickler die Software anpassen, aber nicht die verwendete Hardware. Somit ist die komplette Optimierung einer Software nicht möglich. [7]

2.2.3 Infrastructure as a Service

Im Gegensatz zum SaaS bezieht sich IaaS hauptsächlich auf die Nutzung der Hardwareinfrastruktur eines Cloud-Anbieters. Dazu gehören beispielsweise die Server und deren Rechen- und Speicherleistung. Der Zugriff auf die Ressourcen wird über virtuelle Maschinen bereitgestellt. IaaS bietet den Kunden die größtmögliche Freiheit (siehe Abb. 1). Der Kunde profitiert zudem durch das Pay-Per-Use-Prinzip. Das Leistungskontingent kann flexibel bestimmt werden, d.h. dass nur für die tatsächlich gebuchte Leistung bezahlt werden muss. [7] Für kleine bis mittelständische Unternehmen ist es meist nicht profitabel, eine eigene Hardwarelandschaft zu konstruieren und zu pflegen. Dazu zählen auch Neuinvestitionen bei überholter Hardware. Das technische Know-how ist bei einem externen Anbieter meist besser, da die Bereitstellung von IaaS zu seinen Kerngeschäften zählen.
Ein mögliches Anwendungsszenario ist folgendes: Die Rechenressourcen einer Hochschule sind für einige Forschungssimulationen unzureichend. Die Forscher können ihre Workloads auf die Cloud übertragen und von dem erhöhten Kontingent des Cloud-Anbieters profitieren. Nach dem Simulationsende können die Ressourcen wieder freigegeben werden. Die kostspielige Anschaffung neuer Hardware wird dadurch vermieden.

2.3 Cloud-Bereitstellungsmodelle

2.3.1 Public Cloud

Die Public Cloud (öffentliche Cloud) ist eine für die Allgemeinheit über das Internet erreichbare Cloud. Sie kann im Besitz von Unternehmen, Bildungseinrichtungen oder staatlichen Einrichtungen sein und von ihnen verwaltet werden. [4]
Zu den bekanntesten Anbietern gehören Microsoft Azure, Amazon Web Services, IBM Cloud und Google Cloud. Vorrangig bei der Nutzung von Public Clouds ist die Kostenersparnis durch fehlende Anschaffungs- und Instandhaltungskosten. Diese werden von dem Anbieter getragen. Darüber hinaus versuchen sie die Illusion eines unbegrenzten Ressourcenpools zu erhalten, um dem Kunden die Angst vor Verfügbarkeitsproblemen zu nehmen. Neben der Sicherheit ist die Verfügbarkeit der Dienste entscheidend für das Image eines Cloud-Dienstleisters.
Die verwalteten Daten liegen beim Anbieter und er ist, abhängig vom Servicemodell, für den Schutz der Daten zuständig. Dieser Aspekt kann als Vorteil oder Nachteil ausgelegt werden. Zum einen muss ein Unternehmen bei einem eigenständig betriebenen Rechenzentrum die nötigen Sicherheitsvorkehrungen implementieren und die Sicherheit der Systeme stetig überwachen. Dafür werden dedizierte Sicherheitsteams mit dem nötigen Know How

benötigt. Falls ein Unternehmen die Bedingungen nur unzureichend erfüllt, kann dies als Sicherheitsrisiko interpretiert werden. Ein etablierter Cloud-Anbieter, der den Fokus verstärkt auf die Sicherheit seiner Systeme legt, kann für manche Unternehmen eine bessere Wahl sein. Nachteilig ist die eingeschränkte Transparenz der Wahl der Sicherheitsmechanismen. Zudem wird die öffentliche Cloud mit anderen unbekannten Kunden geteilt und ist für alle gleichermaßen zugänglich. Diese Eigenschaften einer öffentlichen Cloud führen zu neuen Bedrohungen.

2.3.2 Private Cloud

Wie der Name schon andeutet ist die private Cloud anders als eine öffentliche Cloud für die Öffentlichkeit nicht zugänglich und wird laut der Definition von NIST nur für ein einziges Unternehmen betrieben. Die Nutzung dieser Cloud beschränkt sich somit auf eine selektierte Gruppe von Anwendern. Die private Cloud befindet sich häufig in den eigenen oder gemieteten Rechenzentren eines Drittanbieters. [4] Sie gewährt das höchste Maß an Kontrolle. Die Ressourcen werden nicht mit unbekannten Entitäten geteilt und die Daten bleiben unter der Kontrolle des Cloud-Eigentümers. Der Besitzer hat zudem eine freie Auswahl bei der Implementierung der Sicherheitsfunktionen und ist nicht an die Vorgaben einer öffentlichen Cloud gebunden. Ein weiterer Vorteil ist die Anpassungsfähigkeit der genutzten Soft- und Hardware. Bei der Entwicklung von Software kann diese an die zugrundeliegende Hardware angepasst werden und umgekehrt.

Eine private Cloud ist für Organisationen, die mit sensiblen Daten agieren und daher an spezielle Regeln und Gesetze gebunden sind, attraktiv. Eine mögliche Einschränkung, die einige Organisationen zu beachten haben, ist die externe Datenspeicherung oder -verarbeitung. Dieser Aspekt spielt besonders bei staatlichen Einrichtungen oder auch in anderen Bereichen, wie dem Gesundheitswesen eine Rolle.

2.3.3 Hybrid Cloud

Die hybride Cloud ist meist eine Kombination aus öffentlicher und privater Cloud und wird eingesetzt, um von den Vorteilen beider Modelle zu profitieren. Ein Unternehmen, welches seine Daten nicht extern speichern darf, kann die Daten in den eigenen Datenzentren speichern und weiterhin Funktionalitäten eines öffentlichen Cloud-Anbieters nutzen. Denkbar ist auch die umgekehrte Variante, wobei die Daten in einer öffentlichen Cloud gespeichert werden und die interne Rechenleistung genutzt wird. Vorteil hierbei ist die hohe Erreichbarkeit der Daten. Dieser Variante ist aus Sicherheitsgründen für Organisationen eher ungeeignet.
Des Weiteren können IT-Workloads bei Bedarf an die öffentliche Cloud delegiert werden und sie ist eine weitere Möglichkeit der Redundanz. Nicht kalkulierbare Ereignisse können die Funktionalität der lokalen Cloud einschränken. In diesem Fall können wichtige Prozesse auf

die Public Cloud verlagert werden, um den potenziellen Schaden zu minimieren. Zuletzt ist die Anschaffung von neuer Hardware für bestimmte Prozesse nicht rentabel. Ein Beispiel ist die Big-Data-Analyse, die auf der Enterprise-Hardware etablierter Public Cloud-Anbieter, durchgeführt werden kann.

3 Microsoft Azure

Microsoft Azure ist die Cloud-Plattform von Microsoft (MS) , welche offiziell im Jahr 2010 [8] gestartet wurde. Sie ist primär eine öffentliche Cloud, bietet jedoch auch hybride Lösungen für Kunden an. Das Kontingent umfasst mehr als 100 Dienste, die den Klienten bei der Umsetzung seiner Ziele unterstützen sollen. Die Office-Suite von Microsoft, mit Programmen wie Word, Excel und PowerPoint, ist im Produktivitätsbereich seit Jahren unumgänglich. Diese Dienste haben den Weg in die Cloud gefunden und sind lokal sowie auch online nutzbar. MS ist sich bewusst, dass die Sicherheit ihrer Plattform für die meisten Kunden höchste Priorität hat. So investieren sie jährlich ca. 1 Mrd. US-Dollar in Sicherheit und beschäftigen hierfür zudem ca. 3.500 Experten [9]. Ihre Rechenzentren sind weltweit in mehr als 60 Regionen vorhanden und nach eigenen Angaben mehr als die Konkurrenz. [10]

Azure bietet Produkte im Bereich IaaS, PaaS und SaaS. Mit Azure bezeichnet Microsoft in ihren Dokumentationen in erster Linie ihre Cloud-Plattform aus IaaS- und PaaS-Diensten. Strenggenommen ist jede Software, die online zur Verfügung steht, SaaS zuzuordnen. Die meisten ihrer SaaS-Dienste, die nicht in direkter Verbindung zu der Azure-Entwicklungsplattform stehen, werden in dem Portfolio mit der Bezeichnung Office 365 angesprochen. In dieser Arbeit werden die drei Cloud-Servicemodelle von Microsoft unter dem Begriff Azure zusammengefasst.

Im Folgenden werden einige Azure-Dienste und die Sicherheitsfunktionen, die sie zur Verfügung stellen vorgestellt. Dazu gehören SharePoint Online, die Nachrichtenverschlüsselung in Office 365, der Verzeichnisdienst und die Speicheroptionen in Azure.

3.1 Office 365

Office 365 ist die Bezeichnung eines Portfolios mit SaaS-Diensten und Desktopapplikationen von Microsoft. Dazu gehören weltweit bekannte Anwendungen wie Word, Excel und Skype. Die Office-Suite bietet die Möglichkeit einige dieser Dienste lokal zu installieren und zu nutzen. Sie können auch direkt aus der MS Cloud mit einem Browser genutzt werden. Office 365 bietet Programme, die in diversen Bereichen eingesetzt werden können. Dazu gehören [11]:

- Maschinelles Lernen
- Sprachtelefonie
- Internes soziales Netzwerk
- Chat
- Online-Konferenzen
- Content-Erstellung und Zusammenarbeit
- Geschäftsanalysen
- E-Mail
- Mobilität

3.1.1 E-Mail-Verschlüsselung

Das Senden von E-Mails gehört zu den meist getätigten Aktionen in einer Organisation. E-Mails können vertrauliche Information beinhalten und somit ein mögliches Angriffsziel darstellen. Dementsprechend muss die Nachricht auf dem Übertragungsweg und während ihrer Speicherung geschützt werden. Um sie vor unautorisierten Entitäten zu schützen bietet sich die Verschlüsselung der Nachricht an. Office 365 stellt drei verschiedene Verfahren für die Verschlüsselung von Nachrichten zur Verfügung.

Office-Nachrichtenverschlüsselung (OME)
Der Sender erstellt in Outlook eine E-Mail und wählt die Option, die Nachricht zu verschlüsseln, aus. Empfänger in derselben Organisation können die Nachricht direkt in Outlook entschlüsselt ansehen. Empfänger außerhalb der Organisation erhalten eine E-Mail, die sie zum Outlook-Web-Interface weiterleitet. Outlook unterstützt die direkte Authentifizierung mit Gmail, Yahoo! Mail oder Microsoft-Konten. Für andere erfolgt die Authentifizierung mit einem zugesendeten einmaligen Passwort (OTP). Die E-Mail verlässt nicht das Postfach von Office Exchange, dem E-Mail-Server von Office.
MS macht keine Angaben bezüglich des angewendeten Verschlüsselungsverfahrens. Die E-Mail kann nicht mit Restriktionen gekoppelt werden. Z.B. kann die Weiterleitung einer verschlüsselten Nachricht nicht unterbunden werden [12]. Die Schlüsselverwaltung erfolgt durch MS und die Verbindung zu Outlook Web wird durch HTTPS gesichert.

Information Rights Management (IRM)
Mit IRM können Zugangskontrollregeln definiert und auf Nachrichten angewendet werden. Die IRM-Restriktionen werden der E-Mail angehängt und diese wird verschlüsselt. Die Nachricht kann allein von einem Outlook Client lokal oder im Web, nach der Authentifizierung des Empfängers, geöffnet werden. Bei der erstmaligen Öffnung der Datei wird eine Verbindung zu einem Lizenzserver hergestellt. Der Server gewährt die Rechte auf die E-Mail. [4] Mit IRM können Beschränkungen durchgesetzt werden, wie das Weiterleiten der Nachricht verhindern. Allerdings kann der Empfänger den Inhalt der Nachricht kopieren und an eine unberechtigte Person schicken.

Secure/Multipurpose Internet Mail Extensions (S/MIME)
S/MIME ist ein Verfahren für die sichere Peer-2-Peer-Nachrichtenübertragung. Es nutzt dabei ein Signier- und Verschlüsselungseigenschaft von asymmetrischen Schlüsseln in Kombination mit symmetrischer Verschlüsselung.
E-Mails können verschlüsselt und mit einer digitalen Signatur versehen werden. Die Sicherheitsaspekte die S/MIME abdeckt sind Authentifizierung, Unanfechtbarkeit, Datenintegrität und Vertraulichkeit. Durch die Signatur wird die Identität des Absenders bestätigt. Er kann seine Urheberschaft nicht leugnen und die Herkunft der Nachricht ist unanfechtbar. Die Verschlüsselung des Inhaltes mit dem öffentlichen Schlüssel des Empfängers, ermöglicht es ausschließlich ihm, die Nachricht mit Hilfe seines privaten Schlüssels zu lesen. Eine Veränderung der Daten durch Angreifer wird somit ausgeschlossen. Auf die Überprüfung des Inhaltes auf Schadsoftware und Spam muss verzichtet werden, da die jeweiligen Programme den Inhalt nicht einsehen können.
S/MIME kann in den Microsoft-Produkten Outlook, Outlook im Web und Exchange ActiveSync eingerichtet werden [13].

3.2 SharePoint Online

SharePoint Online ist eine websitebasierte Kollaborationsplattform, welche dem SaaS-Portfolio von Office 365 angehört. SharePoint soll in einer Organisation die Teamarbeit stärken, Zugang zu Informationen erleichtern und die Zusammenarbeit fördern und vereinfachen [14]. SharePoint bietet den Benutzern im Kern eine Plattform, um gemeinsam an Dokumenten zu arbeiten und die ineffiziente Zusammenarbeit per E-Mail-Austausch zu ersetzen. Mit SharePoint kann eine Sammlung von Webseiten erstellt werden. Anwender nutzen eine Seite, um Informationen zu speichern, organisieren, teilen oder darauf zuzugreifen. Die Seiten können von jedem Gerät mit einem Webbrowser aufgerufen werden; alternativ erfolgt der Zugriff mit der SharePoint Mobil-App für Android, iOS und Windows Phone. Mithilfe der integrierten Suchfunktion sind Objekte, wie Dokumente oder Personen auffindbar. SharePoint bietet vordefinierte Gruppen mit einer Zuweisung von

[4] Die offizielle Dokumentation von Office 365 ermöglicht wenig Einblick in die IRM-Verschlüsselung von E-Mails.

unterschiedlichen Berechtigungsstufen. Administratoren können eigene Gruppen erstellen und so den spezifischen Aufbau ihrer Organisation abbilden.

3.2.1 Sicheres Teilen

Zu den Hauptfunktionen von SharePoint gehört das Teilen von Ressourcen. Es ist wichtig, dass der Teilvorgang mit einer umfangreichen Optionsauswahl, die die Sicherheit betrifft, gekoppelt ist. Der Vorgang muss für die Benutzer und IT-Mitarbeiter eindeutig sein. Das bedeutet, dass zu keinem Zeitpunkt, Zweifel bezüglich der geteilten Informationen und des Empfängerkreises bestehen dürfen. Das Teilen von kritischen Daten beispielsweise kann Unsicherheit hervorrufen und ein Fehler bei dem Teilvorgang würde die Vertraulichkeit der Daten gefährden. SharePoint Nutzer erhalten auf der Benutzeroberfläche eine Liste mit Personen, die Zugriff auf die zu teilende Datei haben werden. Das Teilen mit Entitäten außerhalb der Organisation stellt ein höheres Risiko dar und eine Warnung wird ausgegeben, um das Risiko des Vorgangs zu verdeutlichen. Administratoren haben die Entscheidungsgewalt darüber, wie die Organisationsressourcen geteilt werden dürfen. Einige Konfigurationsentscheidungen sind:

- das Teilen mit externen Benutzern einzuschränken
- das externe Teilen von vertraulichen Informationen zu begrenzen
- das Anhängen von vertraulichen Dateien an E-Mails zu unterbinden
- den Zeitraum des externen Zugriffs zu bestimmen
- die Zulassungs- oder Verweigerungsliste für Domänen mit denen Informationen geteilt werden dürfen, zu erstellen.

Dateien und Ordner können per Linkfreigabe mit anderen Personen geteilt werden. Die Links werden in drei Kategorien mit unterschiedlichen Sicherheitsstandards gegliedert.

Jeder-Link: Ein Jeder-Link ist ein widerruflicher sowie, übertragbarer geheimer Schlüssel. Ausreichende Sicherheitsmechanismen sind nicht vorhanden und jede Person, die im Besitz des Links ist, kann auf die Dateien zugreifen. Durch das Löschen des Links wird der Schlüssel widerrufen. Schlüssel sind weder ableitbar noch können sie erraten werden: sie sind somit geheim. Um die Vertraulichkeit der Daten zu wahren, ist es wichtig, die Vertraulichkeit des Links zu schützen. Geteilte SharePoint-Webseiten sind nur für authentifizierte Benutzer verfügbar. Nicht authentifizierte Benutzer können nur auf geteilte Dateien und Ordner zugreifen. Vertrauliche Informationen sollten niemals durch Jeder-Links geteilt werden. Die Identität der Nutzer des Links kann nicht überprüft werden. Dafür werden in Überwachungsprotokollen die IP-Adressen der Nutzer erfasst. In SharePoint kann die Erstellung von Jeder-Links unterbunden werden, was die Gefahr der versehentlichen Freigabe ohne Schutzmechanismen minimiert. Für die optimale Funktionalität der Domänenfilterliste sollten Jeder-Links deaktiviert werden, da sie die Filterregeln umgehen. [15]

Personen-in-Ihrer-Organisation-Link: Hierbei handelt es sich um einen organisationsinternen Link, auf den nur authentifizierte Mitglieder im Verzeichnis der Organisation zugreifen können. Gästen in demselben Verzeichnis bleibt der Zugang verwehrt. Weiterhin handelt es sich, genau wie Jeder-Links, um widerrufliche sowie übertragbare geheime Schlüssel. Im Vergleich zu diesen bieten sie jedoch eine erhöhte Sicherheit. [15]

Bestimmte-Personen-Link: Diese Art von Link stellt einen nicht übertragbaren sowie widerruflichen geheimen Schlüssel dar. Nur die vom Ersteller angegebenen Personen können auf den Link und seine Inhalte zugreifen. Diese Empfänger müssen sich autorisieren. Diese Art des Teilens ist besonders empfehlenswert bei der Freigabe von vertraulichen Informationen. Externe Empfänger erhalten per E-Mail einen einmaligen Zugangscode (One Time Password) [16]. Liegt ein Arbeits- oder Schulkonto einer anderen Organisation in Azure AD vor, so wird dieses zum Verzeichnis der Organisation hinzugefügt und die Code-Abfrage erfolgt nur einmal. Ohne eine Zugehörigkeit der oben genannten Konten, findet die Code-Authentifizierung bei jedem Zugriff auf die Datei erneut statt. [15]

Für die drei Link-Optionen gilt, dass bei der Erstellung ein Ablaufdatum bestimmt werden sollte. Besonders wichtig ist das Vornehmen dieser Einstellung bei den unsichersten der oben genannten Links, den Jeder-Links.

3.2.2 Zugriffskontrolle durch Geräte und Netzwerkadressen

SharePoint- und OneDrive-Inhalte können auf nicht autorisierten Geräten eingeschränkt oder blockiert werden. Der SharePoint- oder der Microsoft-365-Administrator kann den Zugang für Benutzer bzw. Benutzergruppen und für Webseiten in der Organisation blockieren oder einschränken. Die folgenden drei Optionen stehen zur Auswahl: [17]

1. einen uneingeschränkten Zugriff von Desktop-Apps, Mobil-Apps und Web gewähren.
2. einen eingeschränkten Zugriff nur durch das Web zu erlauben. Benutzer können Dateien weder herunterladen noch drucken oder synchronisieren.
3. den Zugang zu blockieren. Es erfolgt kein Zugang zu der Webseite und somit auch nicht zu den Dateien.

Diesen Einstellungen können weitere Bedingungen hinzugefügt werden. So kann bei der Auswahl des eingeschränkten Zugriffes eine Modifizierung der Dateien im Web verweigert oder zugelassen werden. Die Einschränkungen auf nicht verwalteten Geräten senken die Benutzerfreundlichkeit und die Produktivität. Sie minimieren allerdings die Gefahr eines versehentlichen Datenverlustes. Genehmigte Geräte erhalten weiterhin einen Vollzugriff mit Ausnahme einiger Browser- und Betriebssystemkombinationen. [17]

Eine weitere Möglichkeit der Zugriffskontrolle von SharePoint- und OneDrive-Inhalten ist die Einführung von festen Netzwerkgrenzen. Dabei definiert der Administrator autorisierte IP-

Adressbereiche und nur Geräte, die sich innerhalb des angegeben IP-Raums befinden, erhalten Zugriff. Diese Selektionsmethode ist mit mehreren Konflikten verknüpft. Die externe Freigabe außerhalb des IP-Bereichs ist nicht möglich und Empfänger erhalten keinen Ressourcenzugriff. Apps, die den standortbasierten Zugriff nicht unterstützen, werden ebenfalls blockiert, und zwar unabhängig davon, ob sie in einer vertrauenswürdigen Netzwerkgrenze ausgeführt werden. Zuletzt entsteht ein Konflikt mit Applikationen, die mit dynamischen IP-Adressen arbeiten. Die Voraussetzung des festen IP-Adressbereichs kann nicht erfüllt werden. [18]

3.2.3 Authentifizierung

SharePoint arbeitet bei der Authentifizierung grundsätzlich mit zwei Arten von Cookies, dem Federation Authentication Cookie (FedAuth) und dem root Federation Authentication Cookie (rtFA). Der rtFA-Cookie authentisiert Benutzer, die eine neue Seite auf der obersten Ebene oder eine Webseite einer anderen Organisation öffnen. Somit bleibt ihnen ein weiterer Authentifizierungsschritt erspart und sie erhalten ein verbessertes Benutzererlebnis. Die Sitzungs-Cookies werden in der Standardeinstellung nicht im Cookie-Cache des Browsers gespeichert und werden nach der Schließung des Browsers gelöscht. Benutzer, die keine erneute Anmeldung favorisieren, können in Azure AD persistente Cookies aktivieren, die nach einer Terminierung des Browsers oder nach einem Neustart des Computers im Speicher verbleiben. In der Abbildung 3 wird der Authentifizierungsprozess für SharePoint Online dargestellt. Die Identitätsprüfung kann mit einem eigenen lokalen Identitätsprovider (IdP) konfiguriert werden oder erfolgt cloudbasiert mit Azure AD. [19]

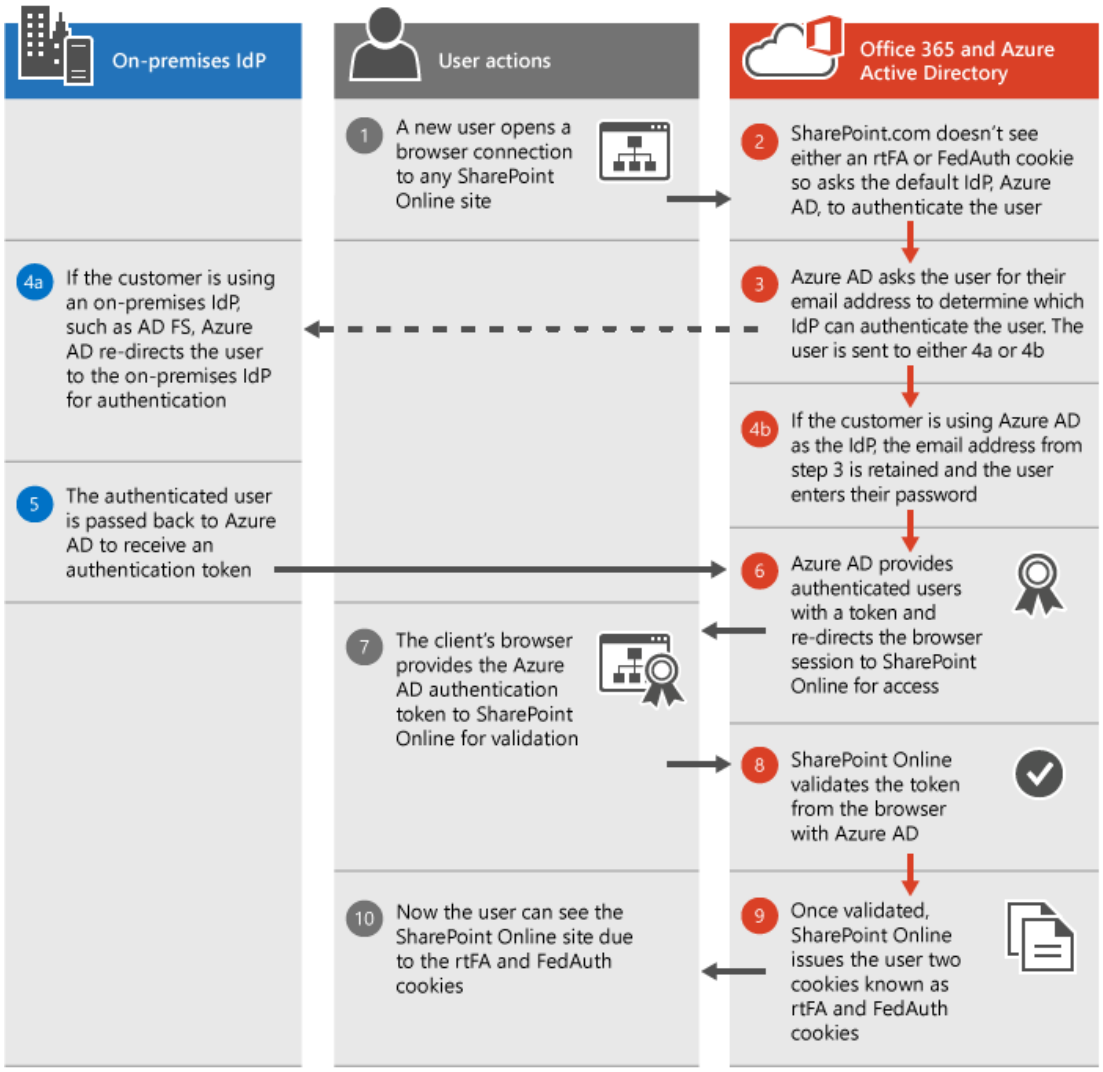

Abbildung 2: SharePoint Online Authentifizierungsschritte [19]

3.3 Azure Active Directory

Das Azure Active Directory (AAD) ist ein Identitäts- und Zugriffsverwaltungsdienst in der Azure Cloud. Er wird daher als Identity as a Service bezeichnet. Die Kernaufgabe ist die Authentifizierung von Benutzern. AAD ist ein Multi Tenant Cloud Service, d.h. mehrere Benutzer, die logisch voneinander isoliert sind, teilen sich den Service. Bei der Nutzung eines Azure-Abonnements oder Office 365 findet automatisch eine Verknüpfung zu einem neuen AAD-Verzeichnis statt.

Microsoft geht von der Annahme aus, dass Angreifer in das Intranet eingedrungen sind [20]. Die Identität wird zum neuen Sicherheitsperimeter. Laut Microsoft findet eine Verlagerung des primären Sicherheitsbereichs von Netzwerk auf Identität statt. In der lokalen Bereitstellung ist der primäre Sicherheitsbereich, auf den der Fokus liegt, das Netzwerk. Das Netzwerk wird als Black-Box betrachtet und die Minimierung der Zugangspunkte ist ein primäres Ziel bei der Sicherheitskonzeption. Dieses Konzept stößt durch die steigende Anzahl an Endgeräten und vermehrte Nutzung von Cloud-Anwendungen an seine Grenzen. [21] Bei cloud-basierten Anwendungen und Ressourcenspeicherung ist dieses Konzept gegensätzlich. Verschiedene Entitäten ohne eine Beziehung zueinander nutzen das gleiche Netzwerk. Benutzer sollen unabhängig von ihrem Standort einen sicheren Zugriff auf ihre Ressourcen haben und somit rückt die Identität in den Vordergrund.

3.3.1 Role Based Access Control (RBAC)

RBAC ist eine Möglichkeit der Rechtezuweisung und kann im Azure Portal (Konfigurationshub für Azure) konfiguriert werden. Einem Benutzer werden die Rechte für Dateien und der Zugriff auf Systeme nicht einzeln zugewiesen. Stattdessen werden abhängig von der Struktur der Organisation, Rollen gebildet. Die Rechte werden den Rollen zugeordnet und diese wiederum den Benutzern. Eine Person kann einer Gruppe mit anderen Benutzern angehören. Auch einer Gruppe können Rollen zugewiesen werden. Diese Rollen werden direkt an die Gruppenmitgliedern vererbt.

Abbildung 3: RBAC Rollen- und Rechtezuweisung

Rollen sollten nach dem Prinzip der geringst-möglichen Privilegien erstellt werden. Einzelberechtigungen können einzeln hinzugefügt werden. Ohne RBAC entsteht die Gefahr, dass neuen Personen die Berechtigungsliste eines anderen Mitarbeiters zugewiesen wird und die Einzelberechtigungen mit übertragen werden.

3.3.2 Multi-Faktor Authentifizierung (MFA)

Die Ein-Faktor-Authentifizierung durch ein Passwort stellt für einen potenziellen Angreifer nur eine Barriere dar, die es zu überwinden gilt. Die Komplexität eines Angriffes wird durch eine schwache Passwortwahl und die Nutzung von denselben Passwörtern für mehrere Dienste durch den Benutzer verringert. Mindestens ein weiterer Authentisierungsschritt wird benötigt, um den Angriffsschutz zu erhöhen. AAD bietet hierfür die Möglichkeit der MFA.

Die Multi-Faktor-Authentifizierung in Azure verlangt mindestens zwei der unten gelisteten Authentisierungsschritte, bevor der Zugang zu einer Ressource gewährt wird:

Tabelle 1: MFA Identifizierungsverfahren [22]

Identifizierungsverfahren	Beschreibung
Wissen	Informationen, die nur dem Benutzer bekannt sein sollten, meist ein Passwort.
Besitz	Objekt mit beschränktem Zugang wie z.B. ein verifiziertes Telefon oder Hardware-Schlüssel. Der Benutzer erhält beispielsweise eine Pin per SMS oder vertrauenswürdiger App.
Biometrie	Biometrische Authentisierung durch Fingerabdruck oder Gesichtsscan.

Administratoren können eine MFA für ausgewählte Anwendungen erzwingen oder Benutzer können diese selbst in ihrem Profil ergänzen [22]. Mit der Nutzung von MFA können folgende Angriffe verhindert bzw. erschwert werden:

- Phishing
- Keylogger
- Credential Stuffing
- Brute Force
- Man-in-the-Middle-Angriffe

3.3.3 Single Sign On

Das Single Sign On (SSO) erleichtert den Zugang zu unterschiedlichen Anwendungen, indem die Identitätsprüfung lediglich einmal stattfindet. Benutzer können nach einmaliger Anmeldung Zugang zu SaaS-Diensten, Webanwendungen, Unternehmensressourcen und Domänengeräte erhalten [23]. Das SSO verringert den Verwaltungsoverhead für Benutzer und Administratoren. Benutzer müssen nur ein starkes Passwort wählen und merken, statt für jeden Dienst ein anderes einzuprägen. Der Mensch als Schwachstelle, durch das Wiederverwenden von gleichen oder ähnlichen Passwörtern, kann somit geschützt werden. IT-Mitarbeiter werden durch die Minimierung des Zugangsdatenmanagements entlastet. Für neue Dienste müssen keine benutzerspezifischen Konfigurationen vorgenommen werden.

Der Hauptvorteil vom SSO ist auch die größte Schwachstelle. Die einmalige Anmeldung und somit der Zugang zu allen Benutzerdiensten wird zum Single Point of Failure. Sollte ein Angreifer in Besitz der Zugangsdaten kommen, so kann er jede verfügbare Anwendung kompromittieren. Die Wahl eines starken Passwortes und die Nutzung von MFA sollten in diesem Kontext, besonders für Benutzer mit Zugang zu kritischen Anwendungen und Ressourcen, obligatorisch sein.

3.4 Azure Storage

Azure Storage ist ein von Microsoft verwalteter Cloud-Speicher-Service und verspricht eine hohe Verfügbarkeit, Redundanz, Skalierbarkeit und Sicherheit [24]. Im Folgenden wird der Aufbau von Azure Storage und die zugehören Speicherdienste erklärt. Es wird untersucht, wie MS notwendige Aspekte wie Datensicherheit und Redundanz gewährleistet.

Im Mittelpunkt von Azure Storage steht das Azure-Speicherkonto. Dieses ist der zentrale Hub für die Erstellung und Verwaltung von Storage-Datenobjekten, wie Dateien, Blobs, Warteschlangen und Tabellen. Ohne ein Speicherkonto können die Azure-Speicherlösungen nicht genutzt werden.

3.4.1 Speicheroptionen

Blob
Blob ist die Abkürzung von Binary large object. Blobs sind Objektspeicher für das Sichern von großen unstrukturierten Datenmengen. Unstrukturierte Daten liegen in einer nicht normalisierten Form vor und lassen sich nicht in einer zeilen- und spaltenorientierten Datenbank ablegen. Dazu zählen Text- und Binärdaten. Big-Data-Anwendungen arbeiten mit unstrukturierten Daten und versuchen, Informationen durch die Analyse dieser Daten zu gewinnen. Laut MS sind Blobs für die folgenden Anwendungsfälle konzipiert [24]:

- Bildern oder Dokumenten für Browser zur Verfügung stellen
- Verteilter Zugriff auf Daten
- Streamen von Video- und Audiodaten
- Schreiben in Protokolldateien
- Wiederherstellung, Notfallwiederherstellung und Archivierung der Daten
- Analyse der Daten durch Azure oder lokalen Anwendungen

Die Daten in Blobs können weltweit mittels HTTP oder HTTPS aufgerufen werden. Die Strukturierung mehrerer Blobs erfolgt durch Container. Z.B. werden mehrere Bilder in einem Container mit dem Namen „Bilder“ gebündelt. Container werden wiederum einem Blob-Speicherkonto mit einer eindeutigen Bezeichnung zugeordnet. Speicherkonten können eine beliebige Anzahl von Containern enthalten und in diesen wiederum können beliebig viele Blobs gespeichert werden [25].

Blob-Speicher werden in zwei Kategorien eingeteilt, die sich durch Leistung und Preis differenzieren. Der Hot Access Tier garantiert eine geringe Latenz. Er sollte für die Speicherung von häufig zugegriffen Objekten verwendet werden. Aufgrund der hohen Leistung ist er teurer als die zweite Variante. Diese ist der Cold Access Tier. Er ist langsamer und sollte für Objekte, auf die selten zugegriffen wird genutzt, werden.

Queue
Warteschlangen werden in der Regel für die asynchrone Abarbeitung von Nachrichten genutzt. Eine Nachricht kann eine maximale Größe von 64KB [24] haben. Eine Warteschlange kann Millionen von Nachrichten speichern, und zwar bis die Speicherkontokapazität voll wird. Ein authentifizierter Zugriff auf die Liste erfolgt über HTTP/HTTPS.
Ein Anwendungsbeispiel wäre folgendes: Es findet ein Zugriff auf eine Webseite statt, und zwar mit der Funktionalität Dateien zu verarbeiten. Die auszuführenden Aktionen werden als Tasks in einer Warteschlange gespeichert. Backend-Server, die für die Abarbeitung der Aufgaben zuständig sind, entnehmen nach dem Wartschlangenprinzip eine Nachricht und führen die verlangte Aufgabe durch. Durch den zentralen Ansatz wird die Synchronisation der Warteschlange auf die Backend-Server vermieden. [26]

Table
Der Azure-Tabellenspeicher wurde für die Speicherung von großen Mengen an strukturierten NoSQL-Daten konzipiert. Die Daten werden in einer Tabelle im Key-Value-Format abgespeichert.

File
Azure File Storage kommt primär für den lokalen Datenzugriff zum Einsatz. Computer und virtuelle Maschinen in der Cloud können damit direkt verbunden werden. Der Datenaustausch erfolgt in erster Linie mit den Protokollen SMB 2.1 und SMB 3.0. Azure Blob und Azure File werden für die Speicherung von großen Datenmengen genutzt. Sie unterscheiden sich aber in ihren Einsatzgebieten und in ihrem Aufbau. Blob Storage hat eine flache Hierarchie mit Unterteilungen in Container. File Storage ermöglicht die Verwendung einer Ordnerstruktur. Der Zugriff per SMB ist im Blob-Speicher nicht möglich. Beide erlauben die Interaktion mit einer REST-Schnittstelle.

3.4.2 Verschlüsselung

Ruhende Daten im Speicherkonto werden automatisch mit AES-256-Verschlüsselung vor einem unbefugten Zugriff geschützt. Die Verschlüsselung ist in der Standardkonfiguration aktiviert und kann vom Kunden nicht deaktiviert werden [27]. Neben den Blobs, Datenträgern, Dateien, Warteschlangen und Tabellen werden auch die Objektmetadaten verschlüsselt. Die Schlüssel werden von MS in Azure Key Vault verwaltet. Dieser Service ist unabhängig von den verfügbaren Service-Optionen Standard oder Premium. Durch die automatische Verschlüsselung bleibt dem Kunden der Konfigurationsaufwand erspart. Falls dieser mehr Kontrolle über die Verschlüsselungsschlüssel haben möchte, kann er seine eigenen Schlüssel verwenden und verwalten. Diese Möglichkeit ist nur im Azure Blob verfügbar. Die Verwaltung der von Azure erzeugten Schlüssel ist in den Diensten Blob und File möglich. Queues und Table werden von MS kontrolliert.
Daten im Transit können durch die Protokolle HTTPS, SMB 3.0 oder ein VPN sicher übertragen werden. Azure-Speicherkonten unterstützen zudem HTTP. Durch fehlende

Sicherheitsmechanismen ist der Gebrauch von HTTP nur in einer vertrauenswürdigen Umgebung empfehlenswert.

3.4.3 Datenredundanz

Azure verspricht in der Dienstleistungsvereinbarung von Azure Storage eine Verfügbarkeit von mehr als 99% [28]. Zu den Bedrohungen, die die Verfügbarkeit beeinflussen können, gehören z.B. Hardware-Fehler, Stromausfälle und Naturkatastrophen. Zum Schutz werden die Daten immer redundant gespeichert. Azure nennt vier Replikationsoptionen, die dem Kunden zur Auswahl stehen.

Lokal redundanter Speicher (LRS)
Das bedeutet eine dreifache Replikation der Daten innerhalb desselben physischen Standortes in der primären Region. Schutz vor Serverrack- und Laufwerkfehlern. Ein Katerstrophenfall im Rechenzentrum kann zum absoluten Datenverlust führen. Schreibvorgänge gelten erst nach der dreifachen Replikation als erfolgreich. Das Schreiben erfolgt synchron. Die Dauerhaftigkeit für ein Jahr wird mit 99,999999999% (11 Neunen) angegeben. [29]

Zonenredundanter Speicher (ZRS)
Dies Form der Speicherung garantiert eine synchrone Replikation der Daten in drei Azure-Verfügbarkeitszonen in der primären Region. Laut MS ist die Verfügbarkeitszone ein *„getrennter physischer Standort mit unabhängigen Stromversorgungs-, Kühlungs- und Netzwerkgeräten*“[29]**.** Hier wird ein Erhöhter Schutz als mit LRS gewährt. Die Daten sind bei einem Katerstrophenfall im primären Rechenzentrum weiterhin verfügbar. Es besteht allerding kein Schutz vor Ereignissen, die die Verfügbarkeit einer gesamten Region betreffen. Die Dauerhaftigkeit für ein Jahr wird mit 99,9999999999% (12 Neunen) angegeben.[29]

Georedundanter Speicher (GRS) / georedundanter Speicher mit Lesezugriff (RA-GRS)
Hiermit ist eine dreifache synchrone Replikation der Daten innerhalb des gleichen physischen Standortes in der primären Region gemeint. Anschließend findet der Vorgang in der sekundären Region statt. Insgesamt werden die Daten 6 Mal gesichert und vor einem regionalen Ausfall geschützt. RA-GRS agiert nach demselben Verfahren wie GRS. Die zusätzliche Funktionalität beinhaltet einen Lesezugriff auf die Daten im sekundären Speicherort. Die Dauerhaftigkeit für ein Jahr wird mit 99,99999999999999% (16 Neunen) angegeben.[29]

Geozonenredundanter Speicher (GZRS) / geozonenredundanter Speicher mit Lesezugriff (RA-GZRS)
Hierbei findet eine synchrone Replikation der Daten in drei Verfügbarkeitszonen in der primären Region statt. Anschließend erfolgt eine asynchrone Replikation in der sekundären geografischen Region. Mit RA-GZRS ist ein schreibgeschützter Zugriff auf die Daten in der

sekundären Region möglich. Die Dauerhaftigkeit für ein Jahr wird mit 99,99999999999999% (16 Neunen) angegeben. [29]

4 Sicherheitsanforderungen an eine Cloud

Ziel dieses Kapitels ist die Erarbeitung von Sicherheitsanforderungen an den Einsatz von Cloud-Anwendungen durch die HAW. Für die Anforderungsableitung ist das Verständnis der Schutzziele in einer Cloudumgebung relevant. Dafür werden die Modelle CIA-Triade und Parkerian Hexad (PH), die die Schutzziele der Informationssicherheit betrachten, miteinander verglichen. Anschließend wird ein Modell ausgewählt, um die Sicherheitsanforderungen zu definieren.

4.1 Auswahl der Sicherheitsmodelle

Die Hauptziele der IT-Sicherheit sind der Schutz der Systeme und Informationen vor dem Zugriff unautorisierte Entitäten und vor systeminternen Fehlern. Für die Umsetzung geeigneter Maßnahmen ist das Verständnis der zu schützenden Bereiche relevant. Diese werden als Schutzziele bezeichnet. Für Angreifer sind sie ihre Angriffsziele. Somit ist die Identifikation dieser Ziele für die weiterführende Entwicklung von Sicherheitsfunktionen unumgänglich.

Das Militär gehörte zu den ersten Nutzern von Computersystemen. Besonders im militärischen und staatlichen Bereich ist der Schutz der Daten besonders kritisch. Es ist somit nicht überraschend, dass viele der anfänglichen Untersuchungen zum Schutz der Informationen von dem US-Militär in Auftrag gegeben wurden[5]. So entstand eines der ersten adaptierten Modelle, das Bell-LaPadula-Modell [30]. In seinem Fokus lag die Vertraulichkeit der Informationen und ihr Schutz durch Zugangskontrollen. Der Ansatz folgte den Prinzipien

[5] Zwei Untersuchungen sind Security Controls Systems (The Rand Corporation, 1970) und Computer Security Technology Planning Study (James P. Anderson, 1972). Ergebnis: Identifizierung von Gefahren

des Militärs nach dem Need-to-Know-Prinzip. Der Schutz vor Veränderung der Information durch Unberechtigte wurde nicht konkretisiert. Dies erfolgte in einem nachfolgenden Modell, dem Biba-Modell [31]. Ziel dieses Modells ist es, die Daten vor unautorisierter Veränderung durch nicht berechtigte und berechtigte Entitäten zu schützen. Ein weiteres Modell ist das Intrution-Detection-Modell von Dorothy E. Denning (1987) [32] mit dem Fokus auf der Verfügbarkeit von Informationen und Systemen. Denning betrachtet insbesondere die Abwehrmechanismen, die diese sicherstellen.[6]

Die oben aufgeführten Modelle betrachten die Kernziele der Informationssicherheit. Das Defizit der Modelle ist ihre eingeschränkte Perspektive und der Fokus auf ein einziges Sicherheitsziel. Die Vereinigung der genannten Schutzziele stellt ein vollkommeneres Modell dar. Dieses Modell wird als CIA-Triade (engl. **C**onfidentiality, **I**ntegrity, **A**vailability) bezeichnet und ist zum Grundbestandteil weiterer Modelle und Normen geworden.

Die Tabelle 1 beinhaltet Sicherheitsziele und die zugehörigen Modelle beziehungsweise die Normen, in denen sie genannt werden. Einige Schutzziele können als Schutzmechanismen interpretiert werden, wie Authentifizierung (engl. Authentication) oder Administration. Aus der Tabelle ist ersichtlich, dass das CIA-Modell in den meisten Fällen als Basismodell betrachtet wird. Darauf aufbauend werden neue Sicherheitsziele ergänzt. Die Ergebnisvielfalt der Schutzziele kann aufgrund unterschiedlicher Perspektiven der Akteure entstanden sein [7]. Abhängig von der Interpretation können einige Aspekte dem CIA-Modell zugeordnet werden. Als Beispiel wird das Ziel der „Identifikation“ betrachtet. Es kann als Mechanismus für die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit interpretiert werden. Des Weiteren ist es möglich die Autorisierung als Bestandteil zum Schutz der Vertraulichkeit und Integrität zu umschrieben.

[6] Absatz folgt der Darstellung von [33].
[7] Für die genaue Begründung ist eine ausführliche Analyse der Modelle notwendig.

Tabelle 2: Informationssicherheitsziele aus der Literatur und von IT-Normen [8]

Reference	Confidentiality	Integrity	Availability	Accountability	Assurance	Authentication	Non-Repudation	Authenticity	Reliability	Effectiviness	Efficiency	Compliance	Utility	Possesion/Control	Authorisation	Awareness	Access	Identification	Accuracy	Administration	Information Classification	Anonymity	Audit	Safety	Maintainability	Other (not specified)
(NCSC, 1991)	X	X	X																							
(McCumber, 1991)	X	X	X																							
(Parker, 1998)	X	X	X					X					X	X												
(Pipkin, 2000)	X		X	X		X									X	X	X	X	X	X						
(Schneier, 2000)		X				X															X	X	X			
(NIST, 2002)	X	X	X	X	X																					
(Gordon and Loeb, 2002)	X	X	X				X	X																		
(Avizienis et at., 2004)	X	X	X						X															X	X	
(ISO 13335, 2004)	X	X	X	X			X	X	X																	
(ITGI, 2007)	X	X	X						X	X	X	X														
(JF, 2007)	X	X	X	X		X									X						X					
(ISACA, 2008)	X	X	X																							
(ISO 15408, 2009)	X	X	X																							
(ISO 27000, 2009)	X	X	X	X			X	X	X																	
(CC, 2009)	X	X	X																							X
(CNSS, 2010)	X	X	X			X	X																			
(Tiller, 2010)	X	X	X																							
(Dubois et al., 2010)	X	X	X	X			X																			
(HMG, 2011)	X	X	X																							
(Whitman and Mattord, 2012)	X	X	X					X				X	X					X								
(BSI IT-Grundschutz, 2020)	X	X	X					X																		

Angesichts des fehlenden allgemeingültigen Standards, insbesondere in Bezug auf das Cloud Computing, gibt es keine Einschränkung bei der Wahl des Sicherheitsmodells in dieser Arbeit für die weiterführende Anforderungsdefinition. Aufgrund der allgemeinen Akzeptanz, wie in Tabelle 1 zu erkennen ist, wird das CIA-Modell als Ausgangsmodell für die weitere Untersuchung gesetzt.

Bei näherer Betrachtung sind deutliche Schwächen des Modells erkennbar. Das Modell hat den Grundgedanken, dass Information nur lokal verfügbar ist. Die stetige Weiterentwicklung von Technologien und das veränderte Nutzungsprofil von Informationen sind dafür verantwortlich, dass das CIA-Modell in die Jahre gekommen ist und heutige Kernpunkte der IT-Sicherheit nur teilweise abbilden kann. Durch die Einführung des Internets sind neue Akteure und neue Kommunikationsbeziehungen entstanden. Dadurch rückt die Identität der Kommunikationspartner und die Korrektheit der erhaltenen Information in den Vordergrund.

[8] Diese Abbildung folgt dem Konzept und der Vorarbeit von [34].

Hinzu kommt, dass Informationen über das Internet verteilt und nicht nur lokal gespeichert werden. Folglich verlieren Dateneigentümer die Kontrolle über ihre Daten. Gesucht wird somit ein Modell, welches die neuen Gegebenheiten berücksichtig und weiterhin die drei anerkannten Kernziele enthält.

Eine direkte Kritik an der Triade wird von dem Informationssicherheitsforscher Donn Parker geübt. Er schlägt ein alternatives Modell vor, das die Schwächen der Triade ausgleichen soll, indem drei weitere Aspekte hinzugefügt werden. Im Folgenden werden die einzelnen Attribute des CIA-Modell vorgestellt und nachfolgend die Ergänzungen, die Parker als notwendig erachtet.

4.2 CIA-Modell

Das CIA- Modell ist ein erprobtes und bekanntes Informationssicherheitsmodell. Die drei angestrebten Ziele sind Vertraulichkeit, Integrität und Verfügbarkeit. In Kapitel 4.2 wurden die Schwächen des Modells aufgedeckt sowie die Begründung dafür gegeben, dass die Bewertung der Sicherheit eines Systems nicht allein mit den drei Attributen möglich ist. Im Folgenden werden die einzelnen Attribute näher vorgestellt.

Vertraulichkeit
Vertraulichkeit besagt, dass nur autorisierte Individuen, Entitäten und Prozesse auf Informationen zugreifen und sie einsehen können [35]. Unautorisierten muss der Zugang stets verwehrt bleiben. Dabei ist zu beachten, dass auch bei der Datenübertragung die Vertraulichkeit gewährleistet sein muss. Zu den essenziellen Schutzmaßnahmen gehört die Trennung der Daten nach Nutzergruppen und die Verschlüsselung der Daten. Bei letzterem Verfahren muss wiederum der Schlüssel geschützt werden. Ein Beispiel ist der Schutz von personenbezogenen Daten, wie Name, Adresse und Zahlungsinformationen, die der Kunde dem Verkäufer bzw. Dienstleister anvertraut. Einer der bekanntesten Datenverluste im Kontext der Cloud betraf die Cloud-Plattform iCloud von Apple. Private Bilder von Prominenten wurden im Internet veröffentlicht und dies führte zu einem Image-Verlust für Apple und auch zum Teil für Cloud-Plattformen.

Integrität
Integrität ist die Eigenschaft, richtig und vollständig zu sein [35]. Informationen müssen vor nicht autorisierter Veränderung und Entfernung geschützt werden. Es ist auch wichtig sicherzustellen, dass die Daten auf dem Übertragungsweg nicht modifiziert werden, dazu gehört auch die Veränderung durch einen Übertragungsfehler [36]. Der Übertragungsschutz kann beispielsweise durch geeignete kryptographische Verfahren erhöht werden. Zudem soll sichergestellt werden, dass eine unautorisierte Modifikation, sei es eine irrtümliche Veränderung durch eine autorisierte Person oder eine beabsichtigte, durch einen Angreifer, reversibel ist.

Verfügbarkeit
Verfügbarkeit beschreibt die Eigenschaft für eine autorisierte Entität verfügbar und nutzbar zu sein [35]. Hardware, die beispielsweise bei einem Stromausfall auf einen Generator zugreifen kann, oder eine Redundanz bei der Datenspeicherung stellen dies sicher. Die Software muss einen hohen Belastungsgrad aufweisen und muss bei Versagen, schnell wieder verfügbar sein. Das Ausmaß der Nichtverfügbarkeit kann sich unterscheiden. Im besten Fall sind die Daten nur temporär nicht verfügbar. Der kritischste Fall ist der irreparable Datenverlust.

4.3 Parkerian Hexad

Der Informationssicherheitsexperte Donn B. Parker stellte in seinem Buch *Fighting Computer Crime* eine Alternative zum CIA-Dreieck vor, das Parkerian Hexad. Es soll das CIA-Modell nicht rundum ersetzen, sondern ist als eine Art Update für die heutigen Herausforderungen zu verstehen. Die drei Kernpunkte sind weiterhin enthalten und werden durch drei zusätzliche Anforderungen ergänzt. Die Ergänzungen sind:

- Besitz oder Kontrolle
- Authentizität
- Nutzbarkeit

Alle Attribute sind atomar und somit nicht weiter unterteilbar. Zudem überschneiden sich die sechs Kernziele nicht. Durch einen Angriff können jedoch mehrere Attribute betroffen sein. [36]
Nachfolgend werden die neuen Punkte vorgestellt und ihr Zusammenhang zu den CIA-Zielen näher erläutert.

4.3.1 Besitz/Kontrolle

Das Kriterium „Besitz oder Kontrolle“ bezieht sich auf die physische Disposition von Datenträgern, die Informationen enthalten[9]. Es soll Fälle umfassen, bei denen Informationen im Besitz oder unter der Kontrolle einer unautorisierten Entität stehen, ohne dass die Vertraulichkeit verletzt wird. Folgendes Beispiel [39] verdeutlicht das Schutzziel und die Beziehung zum Attribut der Vertraulichkeit: Der Inhalt eines Speichermediums wird ohne die Erlaubnis des Besitzers kopiert. Der Täter schaut sich nicht den Inhalt der Festplatte an. Laut dem klassischen Modell würde hier kein Verstoß vorliegen, da der Täter keinen Einblick in den Inhalt hatte (Vertraulichkeit), den Inhalt nicht verändert hat (Integrität) und das Speichermedium dem Besitzer zur Verfügung (Verfügbarkeit) steht.
Ein Verstoß gegen die Vertraulichkeit betrifft auch das Attribut Besitz/Kontrolle. Ein Verstoß gegen dieses muss keinen Einfluss auf die Vertraulichkeit haben, wie das oben aufgeführte Beispiel zeigt.

[9] [37] Zitiert nach [38].

4.3.2 Authentizität

Das Attribut der Authentizität soll die korrekte Zuweisung von Daten zu ihren Urhebern sicherstellen[10]. Die Daten müssen somit authentisch, d.h. die Angaben zu den Daten müssen korrekt sein. Daraus lässt sich ableiten, dass die Verknüpfung der Informationen mit ihrem Bezeichner authentisch sein muss [36]. Folgendes Beispiel[11] dient zur Verdeutlichung des Schutzziels: Ein Betrüger verändert den Header einer E-Mail und gibt sich als eine unschuldige Person aus. Die Integrität der Daten wird nicht verletzt, da die falsche Information von dem Absender beabsichtigt war. Auch mit den weiteren fünf Attributen lässt sich das Beispiel nicht einordnen. In diesem Fall wird die Authentizität verletzt, da die Verknüpfung der Bezeichner nicht korrekt ist. Somit wird ein Beweis der Identität benötigt. Im Internet wird dies häufig durch digitale Zertifikate erreicht. Zertifikate werden von einer Zertifizierungsstelle, die von Web-Browsern als souverän und vertrauenswürdig eingestuft worden ist, vergeben. Für den Klienten bedeutet dies, dass bei einer gesicherten Verbindung (HTTPS) zu einem Server mit einem digitalen Zertifikat, welches von einer anerkannten Stelle ausgegeben wurde, die Identitätsprüfung des Servers stattgefunden hat.
Attacken, die die Authentizität betreffen, werden als Spoofing (engl. Manipulation, Verschleierung) bezeichnet. Angreifer können beispielsweise Opfer per E-Mail auf eine manipulierte Webseite lenken, die sich wie eine originale Seite verhält, um vertrauliche Nutzerinformationen abzugreifen. Die meisten Webbrowser geben eine Warnung bei nicht vertrauenswürdigen Seiten aus oder indizieren, dass es keine gesicherte Verbindung ist.

4.3.3 Nützlichkeit

Dieses Attribut bestimmt die Nützlichkeit der Daten[9]. Folgendes Beispiel[3] soll das Ziel verdeutlichen: Ein Professor schickt seinen Studenten sein Vorlesungsskript. Die Datei ist passwortgeschützt und zum Entschlüsseln wird das Passwort benötigt. Der Professor hat vergessen, das Passwort mitzuteilen. Für die Studenten liegt die Datei zwar vor (Verfügbarkeit gewährleistet), jedoch nicht in einer nützlichen Form. Das Szenario verdeutlicht, dass zusätzlich zu den anderen fünf Kriterien das Attribut Nützlichkeit erforderlich ist. Die Daten eines Cloud-Kunden werden dem Cloud-Anbieter anvertraut. Der Kunde fordert neben dem Schutz der Daten, dass sie für ihn weiterhin nützlich sind.

[10] [37] Zitiert nach [38].
[11] Beispiel folgt der Darstellung von [40].

4.4 Aufstellung der Sicherheitsanforderungen

In diesem Kapitel werden Sicherheitsanforderungen an eine Cloud mithilfe des Parkerian Hexad abgeleitet[12]. Das PH bietet im Gegensatz zum CIA-Modell ein größeres Betrachtungsspektrum und behebt die Defizite des etablierten Modells. Die Notwendigkeit der Ergänzungen wurde in Kapitel 4.2 aufgezeigt.

Die Erarbeitung der Sicherheitsanforderungen ist für die Identifizierung und Bewertung der Azure-Sicherheitsfunktionen relevant. Anhand der Anforderung kann untersucht werden, ob Azure die für ihre Erfüllung benötigten Sicherheitsmaßnahmen bereitstellt und inwieweit diese ausreichen. Dementsprechend werden die Sicherheitsanforderungen für die Sicherheitsanalyse von MS Azure in Kapitel 5 herangezogen.

Die folgenden Anforderungen sind in den Kontext einer Hochschule einzuordnen. Der Cloud-Kunde wird mit einer Hochschule gleichgesetzt. Die Cloud-Benutzer werden dem Cloud-Kunden untergeordnet. Zu den Nutzern zählen diejenigen, die über den Cloud-Kunden Nutzer einer Cloud sind. Im Fall einer Hochschule sind es Personen aus der Forschung und der Lehre. Studenten werden der Gruppe Lehre zugeordnet. Weitere wichtige Akteure sind die Internet-Service-Provider (ISP), die die Kommunikationskanäle zwischen Kunde und Cloud kontrollieren.
Aus den drei in Kapitel 2.1 vorgestellten Servicemodellen des Cloud-Computings werden für die Anforderungsdefinition die Modelle SaaS und IaaS betrachtet. PaaS sind für eine Hochschule von geringer Bedeutung, da die Anwendungsentwicklung nicht zu ihren Kerntätigkeiten zähl. Eine Hochschule möchte durchgängig die Kontrolle über ihre kritischen Daten behalten. Aus diesem Anlass fällt die Wahl des Cloud-Bereitstellungsmodells auf die hybride Variante. Die Aufstellung der Sicherheitsanforderungen erfolgt unter Berücksichtigung der oben genannten Aspekte.

4.4.1 Sicherheitsanforderungen: Vertraulichkeit

Vertraulichkeit der Daten
Bei der Nutzung einer Cloud werden Daten in der Cloud gespeichert, übertragen und verarbeitet. Die Anforderung an die Cloud ist, die Vertraulichkeit der Daten während ihrer gesamten Lebenszeit zu sichern oder die Möglichkeit, dies zu gewährleisten, bereitzustellen. In IaaS ist der Kunde für die Sicherung seiner Daten selbst verantwortlich. Die Untersuchung sollte sich in diesem Fall auf die zur Verfügung stehenden Sicherheitsfunktionen fokussieren. In SaaS werden die Daten des Kunden dem Anbieter anvertraut. Angreifer sollen zu keinem Zeitpunkt Einblick in den Inhalt der Daten erhalten.

[12] Die abgeleiteten Sicherheitsanforderungen folgen der Darstellung von [36] Kapitel 3.4 – 3.9. Eine ausführliche Beschreibung ist der genannten Arbeit vorzufinden.

Die Sicherheitsanforderungen sind:

- Vertraulichkeit ruhender Daten
- Vertraulichkeit der Daten in Transfer
- Vertraulichkeit der Daten in Nutzung

Vertraulichkeit bei der Datentrennung
In öffentlichen Clouds werden die Ressourcen des Cloud-Anbieters mit anderen Benutzern geteilt. Die Isolation der Daten und Systeme ist dabei kritisch und Benutzer sollten niemals Zugriff auf die Daten eines anderen Cloud-Kunden erhalten. Sollte es zu Überschneidungen kommen und die Daten in einer kryptographisch ungesicherten Form vorliegen, so würde der Vorfall die Vertraulichkeit der Daten verletzen. Für die Datentrennung im privaten Teil der hybriden Cloud trägt die Hochschule die Verantwortung.

Vertraulichkeit der Metadaten
Metadaten sind Daten, die Information über andere Daten enthalten. Eine Metadatei akkumuliert Kerneigenschaften ihrer zugehörigen Datei. Metadaten können sich auch auf die Kommunikation beziehen [36]. Sie können manuell oder automatisch erstellt werden und enthalten häufig strukturierte Information über Dateiformat, Größe und Erstellungszeit. Da die Information in einer strukturierten Form vorliegt, ist sie wesentlich einfacher zu analysieren als der tatsächliche Inhalt der Datei und macht sie zu einem Ziel für Angreifer, Datensammler und Behörden. Letztere können eine Metadatenanalyse der Kommunikation einer suspekten Person durchführen [41]. Die Analyseergebnisse können zu einer Genehmigung der Überwachung des Kommunikationsinhalts führen.

Cloud-Benutzer erzeugen während der Nutzung Metadaten und Cloud-Anbieter können durch ihre Services Metadaten sammeln. Die Vertraulichkeit der Metadaten stellt somit eine Sicherheitsanforderung dar. Neben den beiden Akteuren kann auch der ISP Metadaten über die Kommunikation erstellen. Dies muss gesondert betrachtet werden, da es außerhalb des Kontrollbereichs des Cloud-Anbieters liegt.

Vertraulichkeit des Kommunikationsinhalts
Diese Anforderung verlangt, dass der Cloud-Anbieter den Kommunikationskanal und somit seinen Inhalt zu schützen hat. Dazu zählt auch die Vertraulichkeit der Kommunikationspartner. Der Fokus liegt hier auf der Kommunikationsbeziehung zwischen Cloud-Anbieter und seinen Kunden. Die Sicherheitsanforderungen sind:

- Vertraulichkeit des Kommunikationsinhalts
- Vertraulichkeit der Kommunikationspartner

Identifikation als Cloud-Kunde
Diese Anforderung bezieht sich auf den möglichen Wunsch des Cloud-Kunden seine Cloud-Nutzung geheim zu halten. Der Kunde möchte wenig Informationen über sich und die von ihm benutzten Teilsystems preisgeben. Je mehr Informationen ein Angreifer über sein Ziel

sammeln kann, desto mehr Angriffsmöglichkeiten können sich für ihn ergeben. Ein Angreifer kann sich als Mitarbeiter des verwendeten Dienstleisters ausgeben, um das Vertrauen des Cloud-Kunden zu erlangen und daraufhin weiteren Schaden anzurichten [36]. Diese Form des Angriffs wird der Angriffsform des Social Engineering zugeordnet.

4.4.2 Sicherheitsanforderungen: Integrität

Integrität der Daten
Daten dürfen während ihrer gesamten Lebensdauer und in all ihren Zuständen (ruhend, in Transfer, in Verarbeitung) nicht durch unautorisierte Entitäten verändert werden. Dazu zählen auch Veränderungen durch Systemfehler. Wichtig ist insbesondere die Erkennung von veränderten Daten und die Möglichkeit, sie in ihren ursprünglichen Zustand zurückzuführen. Der Cloud-Anbieter muss zudem die Integrität der Kommunikation zwischen ihm und dem Cloud-Kunden sicherstellen. Die Möglichkeit der Datenwiederherstellung ist in diesem Fall schwierig. Die andere Partei kann jedoch über die Verletzung der Integrität in Kenntnis gesetzt werden, um eine erneute Übermittlung der Information zu veranlassen.

Die sich ergebenden Sicherheitsanforderungen sind:
- Integrität der Daten
- Integrität der Kommunikation

4.4.3 Sicherheitsanforderungen: Verfügbarkeit

Verfügbarkeit der Infrastruktur (ISP)
Bei der Nutzung einer öffentlichen Cloud spielt der ISP eine entscheidende Rolle. Er stellt die Brücke zwischen einem Cloud-Anbieter und seinem Kunden dar. Der ISP besitzt bzw. kontrolliert diesen Kommunikationsweg. Die Verfügbarkeit des ISP ist für die Cloud-Nutzung essenziell. Die Verfügbarkeitsstörungen des ISP haben direkten Einfluss auf die Verfügbarkeit der Cloud. Eine Trennung des Internets zwischen Cloud und Kunde würde jegliche Cloud-Funktionalität einstellen. Somit besteht eine starke Abhängigkeit zu den ISPs. Diese Anforderung liegt nicht im direkten Anforderungsbereich des Cloud-Anbieters, da er nicht die Kontrolle über die beteiligten ISPs hat. Er kann jedoch bei der Auswahl des ISP Einfluss nehmen und die Wahl eines besonders robusten Netzwerk treffen. ISPs lassen sich in Bezug auf die Verbindungsgeschwindigkeit in drei Kategorien unterteilen: Tier-1, Tier-2 und Tier-3. Tier-1-Provider besitzen ihr eigenes Netzwerk. Tier-2 und Tier-3-Provider leasen die Ressourcen eines Tier-1-Providers. Somit hat ein Tier-1-Provider mehr Kontrolle über die Infrastruktur und ist zudem zuverlässiger. Cloud-Anbieter sollten dies bei der Auswahl berücksichtigen.

Verfügbarkeit der Daten
Für Cloud-Kunden und die Benutzer ist es wichtig, dass sie jederzeit Zugriff auf ihre Daten haben. Der Cloud-Anbieter muss sicherstellen, dass Daten aufgrund von Systemfehlern oder durch nicht autorisierte Entitäten gelöscht werden. Eine Absicherung in Form von Datenredundanz ist hier unumgänglich. Wenn ein Benutzer seine Daten unbeabsichtigt löschen sollte, ist es wünschenswert, diese Aktion rückgängig machen zu können. Die Anforderungen müssen darüber hinaus auch für Metadaten erfüllt werden.

Verfügbarkeit der Ressourcen
Die Kernidee des Cloud Computing ist die Ressourcenteilung. Der Cloud-Anbieter muss die Verfügbarkeit dieser Dienstleistung sicherstellen. Ressourcen bedeuten in diesem Fall die Hardware in einem Rechenzentrum, aber auch die Eigenschaften der Hardware. Dazu zählen z.B. Bandbreite und Rechenleistung. Ressourcenengpässe können beispielsweise durch eine zu hohe Benutzeranzahl entstehen und würden die Verfügbarkeit der Dienste einschränken. Folgendes Beispiel soll die Relevanz dieser Anforderung verdeutlichen: Studenten wollen sich kurz vor Ablauf der Anmeldefrist für die Prüfungen anmelden und rufen die Anmeldeseite auf. Durch eine erhöhte Benutzerzahl kann das System nicht alle Anfragen gleichzeitig beantworten. Die Anmeldung steht somit für einige Studenten nicht zur Verfügung. Betroffen von den Konsequenzen wären in diesem Fall die Studenten und die Hochschulverwaltung.

Verfügbarkeit der Teilsysteme
Neben den physischen Systemen werden auch andere Teilsystem für die Gewährleistung der Cloud-Funktionen benötigt. Diese Anforderung betrachtet im Kern die Verfügbarkeit der verwendeten Software. Dazu zählen die Firewall, Programme zur Steuerung und Kontrolle und Programme für die automatische Skalierung. Die Ausfallsicherheit dieser Systeme ist hinsichtlich der Cloud-Sicherheit und Cloud-Funktionalitäten besonders wichtig. Zudem muss der Cloud-Anbieter Programme, die zur Überwachung und Analyse der Cloud-Nutzung dienen bereitstellen. Diese sollen gewährleisten, dass der Cloud-Kunde jederzeit den Überblick über seine Cloud behält.

4.4.4 Sicherheitsanforderungen: Besitz/Kontrolle

Das Parkerian Hexad bezieht sich auf die physische Kontrolle von Datenträgern. Im Cloud-Computing-Szenario muss diese Definition ausgeweitet werden. Der Cloud-Anbieter ist Eigentümer von Teilsystemen seiner Cloud und kontrolliert sie. Neben dem physischen Schutz der Systeme muss auch der digitale Schutz betrachtet werden. Angreifer können durch digitale Angriffe die Kontrolle über die Ressourcen der Cloud übernehmen. Die Betrachtung der rein physischen Sicherheit ist hier unzureichend.

Besitz/Kontrolle der Daten
Daten in der Cloud sind im Besitz und unter der Kontrolle des Cloud-Anbieters. Eine Hochschule erteilt dem Cloud-Anbieter die Rechte dazu unter der Bedingung, dass sie weiterhin Eigentümer bleibt und der Datenmissbrauch durch den Anbieter verhindert wird. Ziel der Sicherheitsanforderung in Bezug auf Besitz/Kontrolle der Daten (inkl. Metadaten) ist somit, diese vor unberechtigten Dritten zu schützen.
Die physische Sicherheit der Datenträger muss zu jedem Zeitpunkt gewährleistet sein. Dazu zählt der Schutz vor Diebstahl mithilfe geeignete Sicherheitsmechanismen.
Aussortierte Datenträger können weiterhin Daten enthalten. Diese müssen vor der Beseitigung des Datenträgers entfernt werden. Der Diebstahl von verschlüsselten Daten würde ebenfalls gegen die Sicherheitsanforderung Besitz/Kontrolle verstoßen. In der verschlüsselten Form haben die Daten für den Dieb keinen Nutzen. Er ist aber im Besitz der Daten unabhängig von ihrer Form. Ihm bleibt weiterhin die Option, die Daten zu entschlüsseln.

Besitz/Kontrolle der Kommunikation
Diese Anforderung verlangt, dass die Kommunikation zwischen Cloud und Kunde, kontrolliert wird. Im Idealfall ist der Cloud-Anbieter derjenige, der im Besitz der zugrundeliegenden Kommunikationsinfrastruktur ist. In der Realität spielen ISP, die den größten Teil der Infrastruktur besitzen und kontrollieren, eine wesentliche Rolle. In dieser Betrachtung werden ISP als vertrauenswürdig eingestuft und der Fokus liegt auf der Kommunikationsschnittstelle der Cloud. Zudem soll die Kommunikation der Teilsysteme in der Cloud unter der Kontrolle des Cloud-Anbieter stehen.

Besitz/Kontrolle der Ressourcen
Die Ressourcen, in diesem Fall die Hardware, der Cloud sollen unter der Kontrolle und im Besitz des Cloud-Anbieters sein. Ziel ist die Sicherung dieser Hardware vor Unbefugten. Das Rechenzentrum sollte im Hinblick auf die Sicherheit der Infrastruktur konzipiert werden. Der Cloud-Anbieter muss geeignete Sicherheitsmechanismen implementieren, die die Sicherheit der Ressourcen gewährleisten. Dazu gehört z.B. die Überprüfung von Personen, die das Rechenzentrum betreten, oder auch die stetige Überwachung der Räume.

Besitz/Kontrolle der Teilsysteme
Teilsysteme sind in diesem Fall diejenigen Systeme, die die Hardware-Ressourcen kontrollieren und steuern. Sie müssen unter der Kontrolle des Cloud-Anbieters bleiben. Ein kompromittiertes System kann schwerwiegende Folgen haben und gegen andere Sicherheitsanforderungen verstoßen. In diesem Fall stellt sich die Frage, inwieweit ausgehend von einem kompromittierten Teilsystem ein anderes Teilsystem angegriffen werden kann, um die Kontrolle auszuweiten, und welchen Schutz der Cloud-Anbieter vorgesehen hat.

Besitz/Kontrolle des Rechtsraumes
Abhängig vom Ort der Cloud-Rechenzentren können Behörden Einfluss auf die in der Cloud gespeicherten Daten und andere Informationen hinsichtlich der Cloud-Nutzung ausüben. Sie können die Kommunikation überwachen oder den Cloud-Anbieter dazu auffordern die Speichermedien auszuhändigen. Der Cloud-Anbieter muss in diesem Fall den Gesetzen des jeweiligen Standortes folgen und verliert die Kontrolle bzw. den Besitz.
Die Transparenz ist in diesem Fall entscheidend und sie stellt eine Sicherheitsanforderung an eine Cloud dar. Kunden sollten Informationen zu dem Rechtsraum, in dem ihre Daten gespeichert werden, erhalten und im besten Fall ihn selbst bestimmten dürfen. Institutionen der Bundesrepublik Deutschland, wie z.B. die HAW Hamburg, möchten den Rechtsraum, dem die Daten unterstehen, kontrollieren. In diesem Fall müssen Datenzentren des Cloud-Anbieters in Deutschland vorhanden sein.

Besitz/Kontrolle des Identitätsdienstes
Die HAW Hamburg möchte den Besitz und die Kontrolle ihres Identitätsdienstes beibehalten und ihre Verzeichnisstrukturen geheim halten[13]. Der Cloud-Anbieter muss dem Kunden die Freiheit bei der Wahl seines Identitätsdienstes lassen und somit eine lokale Authentisierung erlauben.

4.4.5 Sicherheitsanforderungen: Authentizität

Authentizität der Kommunikationspartner
Die Identität der Kommunikationspartner soll geprüft werden bzw. die Möglichkeit für eine Identitätsprüfung soll vorhanden sein. Im Cloud-Szenario ist der Cloud-Anbieter für die Authentizität der Kommunikationspartner in den SaaS-Diensten verantwortlich. Der Cloud-Anbieter trägt zusätzlich die Verantwortung dafür, die Authentizität der Kommunikationspartner seiner Teilsysteme sicherzustellen. Dazu gehört die Management-Plattform, die zu der Erstellung von virtuellen Instanzen in IaaS benötigt wird.

Authentizität der Nachricht
Zusätzlich zu der Überprüfung der Authentizität des Kommunikationspartners muss die Authentizität des Kommunikationsinhaltes sichergestellt werden. Diese Anforderung dient der Vermeidung von der Übermittlung falscher Informationen.

Authentizität der Daten
Die Authentizität der Daten ist gesichert, wenn die Verknüpfung der Daten zu den Bezeichnern richtig ist. In der IaaS-Umgebung liegt die Aufgabe im Verantwortungsbereich der Cloud-Kunden. Bei SaaS-Diensten muss der Cloud-Kunde die Korrektheit seiner

[13] Quelle: Informationssicherheitsbeauftragter der HAW Hamburg, Herr Prof. Klaus-Peter Kossakowski

eingegebenen Daten und ihrer Verknüpfung prüfen. Der Cloud-Anbieter muss sicherstellen, dass die Verknüpfung exakt nach dem Wunsch des Kunden umgesetzt wird.

Authentizität der Daten zur Steuerung
In einer Cloud werden Daten für die Steuerung, Konfiguration und Abrechnung der Cloud-Dienste eingesetzt [36]. Die Korrektheit dieser Daten ist sicherzustellen. Ein inkorrekter Datenbestand über den Leistungsverbrauchs eines Kunden in der Cloud könnte für ihn negative Konsequenzen haben.

Authentizität der Teilsysteme
Im Fokus dieser Anforderung stehen die diversen Teilsysteme einer Cloud und ihre Beziehungen zueinander. Diese müssen stets korrekt sein. Durch eine komplexe Vernetzung der Teilsysteme könnte die inkorrekte Verbindung zweier Teilsysteme weitreichende negative Konsequenzen für das Gesamtsystem haben.

4.4.6 Sicherheitsanforderungen: Nützlichkeit

Nützlichkeit der Daten
Die Daten des Cloud-Kunden in der Cloud müssen für ihn in einer nützlichen Form abrufbar sein. Die Daten werden als nützlich bezeichnet, wenn sie für die Erfüllung der Aufgaben einer autorisierten Entität verwendet werden können. Folgendes Beispiel soll diese Dateieigenschaft verdeutlichen: Die Daten eines Cloud-Benutzers werden in einer Cloud verschlüsselt hinterlegt. Der Cloud-Anbieter ist für die Schlüsselverwaltung zuständig. Der Schlüssel kommt abhanden. Der Cloud-Anbieter kann die Daten nicht mehr in eine nützliche Form überführen und verletzt somit das Attribut der Nützlichkeit.
In IaaS und lokale gespeicherten Daten ist der Kunde für die Nützlichkeit seiner Daten verantwortlich. Der Cloud-Anbieter ist des Weiteren für die Nützlichkeit der Daten zur Steuerung und Kontrolle seiner Teilsysteme verantwortlich.

Die Sicherheitsanforderungen sind:
- Nützlichkeit der Daten
- Nützlichkeit der Daten zur Steuerung und Kontrolle.

5 Sicherheitsanalyse von MS Azure

Im Kapitel 4 wurde das Parkerian Hexad eingeführt und wichtige Sicherheitsanforderungen an eine Cloud abgeleitet. In diesem Kapitel wird untersucht, ob und wenn ja mit welchen Sicherheitsmaßnahmen Azure die Anforderungen erfüllen kann. Im ungünstigsten Fall kann eine Anforderung nicht abgedeckt werden.

Vor der Untersuchung der Sicherheitsanforderungen muss der Verantwortungsbereich bei der Nutzung von Azure eingegrenzt werden. Microsoft spricht von einer „geteilten Verantwortung“[42]. Das Service-Modell bestimmt die Zuteilung des Verantwortungsbereichs. Folgende Abbildung verdeutlicht die Anteile von Azure und die des Kunden:

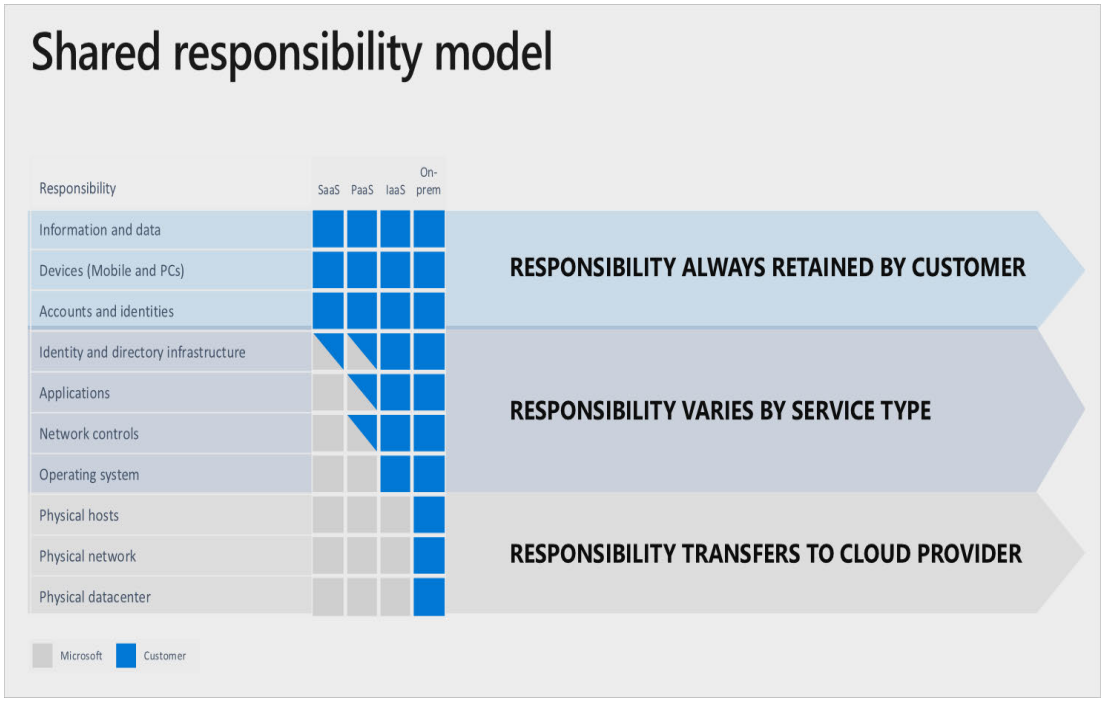

Abbildung 4: Verteilung der Verantwortung in Cloud-Modellen [43].

Die Zeilen zeigen die unterschiedlichen Verantwortungsbereiche und die Spalten das jeweilige Servicemodell einschließlich des On-Premises-Modells. Die blaue Füllfarbe steht für die Verantwortung der Cloud-Kunden und die graue für die von MS Azure.

Im lokalen Datenzentrum (On-Premises) ist der Betreiber alleiniger Verantwortungsträger für die Sicherheit aller Systeme. Bei der Nutzung der Azure-Dienste variiert der Grad der Verantwortung je nach Modell. In jedem der drei Cloud-Service-Modelle übernimmt Azure die komplette Verantwortung für die physikalische Schicht. Laut [42] ist dieser Aspekt für Kunden der entscheidende Grund, aus dem sie sich für einen Wechsel zur Cloud entscheiden.

Für andere Bereiche, wie z.B. die Identitäts- und Zugriffskontrolle, sind beide Partner verantwortlich. Der Kunde muss bei der Nutzung des Azure Active Directory Konfigurationsentscheidungen treffen. Dazu zählen unter anderem die Auswahl der Authentisierungsverfahren und die Nutzung der MFA. Azure muss im Gegenzug sicherstellen, dass die angebotenen Funktionalitäten fehlerfrei arbeiten. Die Abbildung zeigt zudem, dass die Verantwortung in den drei Cloud-Service-Modellen immer geteilt wird. Zu keinem Zeitpunkt übernimmt der CSP die volle Verantwortung.

In diesem Kapitel werden aus den zuvor genannten Gründen primär diejenigen Sicherheitsmaßnahmen behandelt, die den Verantwortungsbereich von Azure schützen. Außerdem werden Mittel genannt, die Azure seinen Kunden zum Schutz ihres Bereiches bietet.

Die folgende Analyse prüft Azure auf die in Kapitel 4.3 vorgestellten Sicherheitsanforderungen. Der Betrachtungsraum wird auf SaaS und IaaS eingegrenzt. Zusätzlich wird die Option der lokalen Datenspeicherung in Form des Hybrid-Cloud-Bereitstellungsmodells berücksichtigt. Fehlen Schutzmaßnahmen, die die jeweilige Sicherheitsanforderung betreffen, wird dies negativ bewertet. Für einen potenziellen Kunden sollten die sicherheitsrelevanten Informationen bei der Recherche auffindbar sein.

5.1 Sicherheitsanforderungen: Vertraulichkeit

Vertraulichkeit ruhender Daten
Die Dienste aller Cloud-Servicemodelle verfügen über eine Verschlüsselungsoption für den Schutz ruhender Daten. Viele Dienste verschlüsseln die Daten bereits in der Default-Konfiguration, am häufigsten in den SaaS-Diensten [44], da hier der Verantwortungsbereich von Azure am größten ist. Der Kunde muss in einigen Fällen entscheiden, ob seine Daten und wenn ja, wie sie verschlüsselt werden sollen. Laut Microsoft benutzen alle Azure-Speicherplattformen zur Verschlüsselung das 256-Bit-AES-Verfahren [45]. Es ist ein weltweit anerkanntes Standardverfahren und bietet eine sehr hohe Sicherheit.

Die Entwürfe für die Verschlüsselung seitens Azure bestehen aus symmetrischen Verfahren. Diese sind besonders schnell und bieten eine hohe Performanz, besonders bei dem Ver- und Entschlüsseln großer Datenmengen. Es wird verlangt, dass der Verschlüsselungsschlüssel an einem Ort mit identitätsbasierter Zugriffssteuerung gespeichert wird [44]. Azure empfiehlt die eigene Schlüsselspeicherlösung Azure Key Vault.
Bei Bedarf kann der Datenverschlüsselungsschlüssel (DEK) durch einen weiteren Schlüssel verschlüsselt werden, dem Schlüsselverschlüsselungsschlüssel (KEK). Der KEK erhöht den Schutz des DEK, solange die Speicherorte der beiden getrennt liegen. Der Zugriff auf den KEK sollte beschränkt sein. Entitäten, die den DEK benötigen, erfordern die Zustimmung des KEK-Verwalters. Mit dem Azure Active Directory (AAD), die im Mittelpunkt des Sicherheitskonzepts von Azure steht, sollte die Zugriffskontrolle der vorhandenen Schlüssel verwaltet werden. [44]

Kunden haben die Auswahl zwischen zwei grundlegenden Verschlüsselungsmodellen: das Client-Verschlüsselungsmodell und das serverseitige Verschlüsselungsmodell. Bei der serverseitigen Verschlüsselung wird der Prozess vom Azure-Ressourcenanbieter übernommen. Kunden können entweder die Schlüsselverwaltung Azure anvertrauen, selbst per Key Vault übernehmen und auch ihre eigenen Keys mitbringen (Bring Your Own Keys, BYOK) oder die Schlüssel auf der eigenen Hardware verwalten (Host Your Own Keys, HYOK).

Durch die client-seitige Verschlüsselung erhält der Kunde eine größere Kontrolle und ein positiver Nebeneffekt ist die Vertraulichkeit der Daten beim Transfer. Die Nachteile bestehen in dem erhöhten Overhead und in der eingeschränkten Funktionalität der Cloud-Dienste, da diese die Daten nicht eigenständig entschlüsseln können. [44]

Bei einer Kündigung des Abonnements sind die gespeicherten Daten 90 Tage mit Lesezugriff verfügbar und werden danach irreversibel gelöscht. Dazu gehören auch zwischengespeicherte Daten und Sicherungskopien. Liegt ein Hardware-Defekt des Speichermediums vor, so werden die Daten gelöscht oder das Laufwerk laut Microsoft unbrauchbar gemacht, bevor es für die Reparatur oder zum Austausch dem Hersteller übergeben wird. [46]Die Löschung erfolgt in diesem Fall gemäß der NIST-800-88-Richtlinien [47].

Vertraulichkeit der Daten in Bewegung
Der Datentransfer unter allen MS-Servern und Client-Computern wird durch das Transferprotokoll TLS geschützt. Aktuell werden die Versionen 1.0, 1.1 und 1.2 unterstützt, wobei für die ersten beiden der offizielle Support eingestellt wurde. Microsoft will in naher Zukunft die Unterstützung für die älteren und weniger sicheren Versionen TLS 1.0 und TLS 1.1 beenden. [45] TLS 1.2 wird zudem mit Perfect Forward Secrecy geschützt, indem die asymmetrischen Schlüssel des Servers nur für die Authentisierung genutzt werden und nicht für die Verschlüsselung des Session Keys. TLS 1.3, welches eine verbesserte Performanz und Sicherheit bietet, wird aktuell nicht unterstützt und ein Zeitraum für seine Einführung wird nicht genannt. [48]

Für die Sicherheit auf der Vermittlungsschicht (OSI Layer 3) ist die Internet Protocol Security (IPsec) in IaaS konfigurierbar. Sie ist eine Erweiterung des Internet Protokolls (IP), und zwar mit der Zielsetzung, IP-Pakete kryptographisch gesichert zu transportieren [49]. MS setzt für die interne Kommunikation ihrer Server TLS oder IPsec ein [50]. Kundendaten, die sich intern unter den Diensten von Azure bewegen, werden ebenfalls durch TLS geschützt. Für die interne Kommunikation werden von MS selbstsignierte Zertifikate und für die externe Kommunikation, die von Microsoft Certificate Authority verwendet. [51]

Der Kunde ist für die Beschaffung und das Deployen der Zertifikate in seiner Azure-Infrastruktur selbst verantwortlich. Die virtuellen Maschinen des Kunden im Azure-Netzwerk, auf denen Windows Server 2012 oder eine neuere Version läuft, können die Kommunikation zu VMs desselben Netzwerks mit dem SMB-3.0-Protokoll verschlüsseln. Der direkte Zugriff auf die Maschinen erfolgt per SSH.

Vertraulichkeit der Daten in Nutzung
Die Skepsis gegenüber der Cloud begründet sich zum Teil dadurch, dass Ressourcen wie Rechenleistung und Speicher in einer öffentlichen Cloud mit vielen anderen Nutzern geteilt wird und eine physische Trennung nur selten vorliegt. Es wird folglich angenommen, dass die Umgebung, in der der Code ausgeführt wird, nicht vertrauenswürdig ist.

Für die Sicherheit der Daten in Nutzung, bietet Azure das Azure Confidential Computing (ACC) an. Laut Microsoft ist ACC der erste Service in einer öffentlichen Cloud, der den Schutz der Daten in Nutzung durch Verschlüsselung erreicht. Die Daten können nur für autorisierten Code in entschlüsselter Form vorliegen. Der Schutz wird durch das Konzept der Trusted Execution Environments (TEE) erreicht. Diese sicheren Enklaven werden durch Hardwaretrennung und Software realisiert. [52]
ACC wurde mit Hinblick auf einen Multi-Plattform-Support entwickelt, insbesondere Windows und Linux. Es steht aktuell für IaaS-Anwender zur Verfügung. Des Weiteren möchten Microsoft ACC für ihre PaaS- und SaaS-Dienste implementieren. [53] Es ist nicht ersichtlich, ob die Einführung stattgefunden hat und wenn ja, für welche SaaS-Dienste.

Neben ACC wird eine weitere Funktion für die Vertraulichkeit der Daten in Nutzung zur Verfügung gestellt. Mit Microsoft Seal, einer Open-Source-Bibliothek, können Daten mithilfe homomorpher Verschlüsselungen direkt in der Cloud verarbeitet werden ohne dass diese im Klartext vorliegen müssen. Die Ergebnisse sind ebenfalls verschlüsselt. Nur der Schlüsseleigentümer kann die Daten entschlüsseln und muss seinen Schlüssel für die Verarbeitung nicht mit Azure teilen. [54] Die Bibliothek ist in erster Linie für Entwickler, also Nutzer von PaaS relevant.

Vertraulichkeit bei der Datentrennung
Die Benutzer der öffentlichen Cloud teilen die Hardware mit anderen, ihnen unbekannten, Personen. Eine physische Isolation der Hardware ist aus Kostengründen selten vorzufinden. Azure setzt in meisten Fällen auf eine logische Isolierung der Mandanten. Die Trennung der Daten ist an die AAD-Architektur verknüpft. Jedem Kunden wird nach Abschluss eines Azure-Abonnements eine AAD-Instanz zugeteilt. Kundendaten und Identitätsinformationen werden laut MS durch die AAD-Architektur isoliert. [46] Microsoft gibt an:

> *„Azure AD wird auf „Bare-Metal"-Servern ausgeführt, die in einem abgetrennten Netzwerksegment isoliert sind, für das per Paketfilterung auf Hostebene und über die Windows-Firewall unerwünschte Verbindungen und Datenübertragungen blockiert werden."*[46].

Vertraulichkeit der Metadaten
In Azure Storage werden alle Objektmetadaten verschlüsselt. Aus dem Prüfbericht [51] wird seitens MS bestätigt, dass sie keinen Zugriff auf die Metadaten der gespeicherten Daten des Kunden haben:

„Moreover, Microsoft does not know what kind of data customers choose to store in Azure“
[51]

Microsoft weist in seiner Datenschutzerklärung für Deutschland darauf hin, dass Metadaten über den Kunden gesammelt werden. Der Kunde erteilt beim Abschluss seines Vertrages, Microsoft seine Zustimmung, dass sie seine Daten sammeln und benutzen dürfen. Die Daten werden beispielsweise für die Verbesserung des Nutzererlebnisses oder Spam- und Malwarebekämpfung genutzt. Microsoft versichert, dass die Daten sicher geschützt werden, unbefugten keinen Einblick gewährt wird und die Daten nicht für Werbezwecke missbraucht werden. [55]
In dem Kriterienkatalog C5:2020 des Bundesamts für Sicherheit in der Informationstechnik (BSI) wird gefordert, dass nur anonymisierte Metadaten für die Verbesserung des Cloud-Dienstes genutzt werden dürfen. [56] Alle Metadaten müssen nach der Erfüllung ihres Zweckes gelöscht werden. In dem C5-Prüfbericht [51](RB-11) von Azure wird die Einhaltung der oben genannten Aspekte bestätigt. Problematisch an der Anforderung des C5-Katalogs ist, dass der Cloud Provider die Dauer der Speicherung bestimmen darf.

Vertraulichkeit des Inhaltes der Kommunikation
Jede Kommunikation mit dem Azure-Portal ist durch HTTPS geschützt. Die Storage REST API kann mit HTTPS aufgerufen werden. Mithilfe der Azure Information Protection können E-Mails, Dokumente und andere sensible Daten mit einem klassifizierenden Label versehen werden. Die Labels bestimmen den Sicherheitsgrad und verhindern beispielsweise das Weiterleiten einer E-Mail, die als geheim eingestuft wurde. Außerdem kann die E-Mail-Kommunikation mit S/MIME und anderen Verfahren gesichert werden[14].

In einer IaaS-Umgebung mit mehreren virtuellen Netzwerken wird empfohlen, die Kommunikationsverbindungen der Netzwerke mit VPN zu sichern. Hier gelten weiterhin die Sicherheitsmaßnahmen wie in „Vertraulichkeit der Daten in Bewegung“.

Vertraulichkeit der Kommunikationsteilnehmer
Azure als Kommunikationspartner soll nicht geheim gehalten werden, da sie eine öffentliche Cloud sind und der IP-Adressbereich allgemein bekannt ist. Kunden, die eine Verbindung zu SaaS-Diensten aufbauen, können die Nutzung eines vertrauenswürdigen Proxy-Servers in Betracht ziehen, um ihre Identität hinter der Identität des Proxys zu verschleiern.

Virtuelle Computer in IaaS müssen in Verbindung mit einem virtuellen Azure-Netzwerk sein. Laut Azure ist ein virtuelles Netzwerk von den anderen virtuellen Netzwerken isoliert. Andere Kunden haben somit keinen Einblick in die Kommunikationsbeziehungen der virtuellen Maschinen des gleichen Netzwerks. Die Verbindung von außerhalb zu den Maschinen kann durch die Nutzung eines VPN geschützt werden. [46]

[14] Siehe Kapitel 3.1.1 E-Mail-Verschlüsselung

Identifikation als Cloud-Kunde
Zu dieser Anforderung sind keine direkten Angaben zu finden. MS listet auf ihrer Webseite einige Kunden auf, die den Cloud-Dienst nutzen und damit zufrieden sind. Hier kann nur spekuliert werden, dass dies mit dem Einverständnis des Kunden erfolgt ist.

Aus der technischen Sicht kann ein Kunde durch die Kommunikationsbeziehung zu Azure identifiziert werden. Azure ist eine öffentliche Cloud und der IP-Adressbereich wird nicht als Geheimnis behandelt. Durch eine Kommunikationsüberwachung (Packet Sniffing) können Benutzer als Cloud-Kunden identifiziert werden. Dieser Aspekt wird nicht negativ bewertet, da es Grundbestandteil einer öffentlichen Cloud ist.

Ergebnis: Vertraulichkeit

Tabelle 3: Ergebnisse der Sicherheitsanforderung Vertraulichkeit

Sicherheitsanforderung	Ergebnis
Vertraulichkeit (data-at-rest)	Azure trifft/bietet Maßnahmen
Vertraulichkeit (data-in-motion)	Azure trifft/bietet Maßnahmen
Vertraulichkeit (date-in-use)	Azure trifft/bietet Maßnahmen
Vertraulichkeit (data-segregation)	Azure trifft/bietet Maßnahmen
Vertraulichkeit Metadaten	Azure trifft/bietet Maßnahmen
Vertraulichkeit Kommunikationsinhalt	Azure trifft/bietet Maßnahmen
Vertraulichkeit Kommunikationspartner	Azure trifft/bietet Maßnahmen
Identifikation als Cloud-Kunde	Externer Verantwortungsbereich

5.2 Sicherheitsanforderungen: Besitz/Kontrolle

Besitz/Kontrolle: Daten
Microsoft versichert, dass der Kunde alleiniger Besitzer seiner Kundendaten ist und dass die Daten nicht für Werbezwecke missbraucht werden.

„*Microsoft beansprucht nicht den Datenbesitz über die in Azure eingegebenen Kundeninformationen*.“[57]

Sollten Microsoft-Betriebs- und -Supportpersonal Zugriff auf Kundendaten benötigen, muss die Zustimmung aus der Führungsebene erfolgen. Jeder Zugriff lasse sich anhand der Protokollierung zurückverfolgen.

Die Daten in der Cloud sind nur unter Aufsicht der Managementebene für interne Techniker verfügbar. Der Zugriff wird laut MS für die betriebsbezogenen Prozesse und Kontrollen erteilt. Es wird keine Angabe gemacht, welche genauen Zwecke der Datenzugriff erfüllen soll.

Diesbezüglich verweist MS auf seine Nutzungsbedingungen für Online Services. Zudem wird bestätigt, dass Subunternehmen ebenfalls beschränkte Zugriffsrechte erteilt werden können. MS versichert, dass regelmäßig Prüfungen der Subunternehmen stattfänden. [46] Die exakten Gründe für die Verlagerung der Arbeit werden nicht genannt. Das technische Knowhow und monetäre Ressourcen sollten bei einem internationalen Unternehmen wie Microsoft „im Haus“ verfügbar sein.

Defekte Geräte, die Daten beinhalten werden physisch vernichtet. Zu den Verfahren gehören laut MS Zersetzen, Schreddern, Pulverisieren oder Verbrennen. Der Zugang zu einem Rechenzentrum erfolgt streng nach einem Protokoll. Zu den Sicherheitsmechanismen gehören die räumliche und zeitliche Begrenzung des Aufenthaltes. Gäste und Mitarbeiter müssen eine zweistufige biometrische Authentifizierung durchlaufen. Die Besucher werden durch einen Metalldetektor beim Ein- und Auslass auf metallische Gegenstände untersucht. Nur berechtigte Hardware darf in ein Rechenzentrum mitgenommen werden. Die Adressen der Rechenzentren werden zum Schutz dieser nicht offengelegt. [47]
Ein Angriff auf die physische Infrastruktur in Rechenzentren ist höchst unwahrscheinlich, da der Aufwand und das Risiko für potenzielle Angreifer zu hoch sind.

Besitz/Kontrolle: Kommunikation
Der Kommunikationskanal zwischen Azure und seinen Kunden ist im Besitz und unter der Kontrolle der beteiligten ISPs. Somit entfällt dieser Abschnitt aus dem Verantwortungsbereich von Azure. Azure kontrolliert hingegen seine Kommunikationsschnittstelle. Diese wird in diesem Fall als die Firewall zwischen dem Azure-Netzwerk und dem Internet gesehen [36]. MS macht keine Angaben über die Personen, die Einfluss auf die Firewall ausüben können. Die Information ist als Firmengeheimnis einzustufen. Für die Kontrolle der Kommunikation durch den Kunden in IaaS stellt Microsoft die Azure Firewall zur Verfügung. Für die Konfiguration ist der Kunde verantwortlich.

Laut Microsoft besitzen sie eines der größten Wide-Area-Netzwerke (WAN) der Welt mit einer Streckenlänge von mehr als 160.000 Meilen. Dieses verbindet die Microsoft Rechenzentren weltweit miteinander und der interne Verkehr wird niemals durch das öffentliche Internet geleitet. Somit besitzen und kontrollieren sie die Kommunikation zwischen ihren Rechenzentren. [58].

Besitz/Kontrolle: Ressourcen (genutzte & nicht direkt genutzte) & Infrastruktur
Die Kontrolle/ der Besitz der Ressourcen und der Infrastruktur wird durch die in Kapitel 5.2.1 genannten Maßnahmen sichergestellt. Die Maßnahmen beziehen sich nur auf die physische Sicherheit. Die digitalen Schutzmaßnahmen werden in Kapitel 5.2.4 Besitz/Kontrolle: Teilsysteme behandelt.

Besitz/Kontrolle: Teilsysteme
Die Kommunikation der Teilsysteme untereinander erfolgt in privaten WAN von Microsoft. Für die Überwachung der Teilsysteme ist das Sicherheitsteam von Microsoft verantwortlich. Diese findet rund um die Uhr statt, um schnell auf Ereignisse reagieren zu können. Die Konfigurationseinstellung der Software, Hardware und Netzwerkgeräte werden jährlich überprüft und vor jeder Aktualisierung werden die neuen Einstellungen in einer isolierten Umgebung getestet bevor sie im Betrieb zum Einsatz kommen. [59]
In IaaS ist der Kunde für die Überwachung der durch ihn kontrollierten Systeme verantwortlich. Azure stellt dem Kunden entsprechende Dienste zur Verfügung, die beispielsweise den Verkehr überwachen oder Bedrohung erkennen und melden.

Besitz/Kontrolle: Rechtsraum
Azure gibt dem Kunden die Auswahl seiner Region und damit den Ort der Datenspeicherung. Zur Auswahl stehen mehr als 60 Regionen. Microsoft bestätigt, dass Daten auf Anfrage der Strafverfolgung oder Behörden herausgegeben werden. Voraussetzung für die Offenlegung ist eine rechtliche Forderung z.B. durch einen Gerichtsbeschluss. Abhängig von dem rechtlichen Rahmen kann eine Forderung die Weitergabe der Content- und Non-Content-Daten bedeuten. Non-Content-Daten sind personenbezogene Daten, die bei der Nutzung der Services gesammelt werden. Content sind Daten, die der Kunde erzeugt oder speichert. Der Inhalt einer E-Mail ist z.B. eine Content-Datei. Microsoft informiert den betroffenen Kunden über die rechtliche Forderung, falls dies in der Forderung nicht explizit untersagt wurde. Microsoft macht keine Angaben, wie sie in diesem Kontext mit verschlüsselten Daten agieren. [60] Die von Azure verwalteten Schlüssel unterliegen der Kontrolle durch Microsoft und es ist nicht auszuschließen, dass sie diese gegen den Wunsch eines Kunden für die Erfüllung einer rechtlichen Forderung nutzen. Auf Basis dessen sollten ruhende Daten (siehe Kapitel 5.1.1) durch Schlüssel des Kunden verschlüsselt werden. Dieser sollte somit auch die Verwaltung der Schlüssel übernehmen.

Besitz/Kontrolle des Identitätsdienstes
In AAD kann die Authentisierung in der Cloud oder lokal erfolgen. Diese Option wird als Hybrididentität bezeichnet. Bei einer lokalen Authentisierung wird beim Anmeldevorgang der Benutzer des AAD zum lokalen Identitätsprovider weitergeleitet, wo die die weiteren Anmeldeschritte erfolgen. Bei einer erfolgreichen Identitätsprüfung wird der Authentisierungstoken an AAD weitergeleiten und dieses erteilt die Berechtigung für den jeweiligen Cloud-Dienst. Der lokale Dienst stellt in diesem hybriden Ansatz einen Single Point of Failure dar. Falls dieser ausfällt, können die Cloud-Dienste nicht genutzt werden. [61]

Ergebnis: Besitz/Kontrolle

Tabelle 4: Ergebnisse der Sicherheitsanforderung Besitz/Kontrolle

Sicherheitsanforderung	Ergebnis
Besitz/Kontrolle: Daten	Azure trifft/bietet Maßnahmen
Besitz/Kontrolle: Kommunikation	Externer Verantwortungsbereich / Azure trifft/bietet Maßnahmen
Besitz/Kontrolle: Ressourcen & Infrastruktur	Azure trifft/bietet Maßnahmen
Besitz/Kontrolle: Teilsysteme	Azure trifft/bietet Maßnahmen
Besitz/Kontrolle: Rechtsraum	Azure trifft/bietet Maßnahmen
Besitz/Kontrolle des Identitätsdienstes	Azure trifft/bietet Maßnahmen

5.3 Sicherheitsanforderungen: Daten-Integrität

Daten-Integrität: Daten
MS bietet nur vereinzelt Information, wie genau die Integrität der Daten gesichert wird. Sie verknüpfen den Begriff der Integrität häufig mit der Verschlüsselung. So wird in [62] geschrieben:

> „*Data encryption. You can encrypt data in storage and in transit to align with best practices for protecting the confidentiality and integrity of your data*."

Verschlüsselung schützt Daten vor unautorisierte Einsicht aber nicht die Integrität der Daten. Die Datei in verschlüsselter Form kann weiterhin verändert werden und stellt eine Integritätsverletzung dar. Dabei ist es irrelevant, ob Informationen sinngemäß verändert wurden.

Mit dem Dienst Azure Security Center (ASC) kann die Sicherheit der Infrastruktur verwaltet und überwacht werden. Eine Funktion von ASC ist die Überwachung der Datenintegrität von Windows- und Linux-Dateien sowie für Windows-Registry-Einträge. Die folgenden Aktivitäten können laut Azure überwacht werden:

- „*Erstellen und Löschen von Dateien und Registrierungen*" [63]
- „*Änderungen an Dateien (an der Dateigröße, der Zugriffssteuerungsliste und dem Hash des Inhalts)*" [63]
- „*Änderungen an Registrierungen (an der Größe, der Zugriffssteuerungsliste, am Typ und am Inhalt)*" [63]

Die zu überprüfenden Objekte müssen in diesem Fall im ASC angegeben werden. Aus der obigen Auflistung kann entnommen werden, dass Veränderungen beispielsweise anhand der gespeicherten Hashes und der Dateigröße erkannt werden. Es sind keine Angaben zu den verwendeten Hashverfahren auffindbar.

Azure Storage kann durch Cyclic Redundancy Checks Integritätsverletzungen erkennen und mit Hilfe redundanter Daten den vorherigen Zustand der Daten wiederherstellen [64].

PaaS-Dienste scheinen ohne jede weitere Konfiguration unter der Aufsicht des Security Centers zu stehen:

„Da Security Center ein nativer Teil von Azure ist, werden PaaS-Dienste in Azure – z.B. Service Fabric, SQL-Datenbanken und Speicherkonten – mit Security Center überwacht und geschützt, ohne dass eine Bereitstellung erforderlich ist.“ [65]

Es wird angenommen, dass bei SaaS-Diensten ebenfalls dieselben Sicherheitsmechanismen agieren, die die Integrität der Daten schützen.

Daten-Integrität: Kommunikation

Die Basisintegritätsprüfung bietet TCP durch die Prüfsumme im Header. Darüber hinaus wird die Kommunikation durch Transportverschlüsselung (durch TLS) und eine weitere Prüfsumme geschützt. Der Sender verschickt neben den Daten einen Message Authentication Code (MAC). Dieser wird mit Hilfe des vereinbarten geheimen Schlüssels und der gesendeten Daten berechnet. Der Empfänger kann die gleiche Berechnung mit den empfangen Daten und dem geheimen Schlüsseln durchführen. Unterschiedliche Ergebnisse sind mit einer Verletzung der Integrität gleichzusetzen.

In der IaaS Umgebung und somit in den virtuellen Maschinen muss der Kunde auf die Verwendung der geeigneten Sicherheitsprotokolle achten. In SaaS wird die Kommunikation verschlüsselt und wie oben beschrieben die Integrität der Kommunikationsdaten geschützt.

Ergebnis: Integrität

Tabelle 5: Ergebnisse der Sicherheitsanforderung Integrität

Sicherheitsanforderung	Ergebnis
Daten-Integrität: Daten	Azure trifft/bietet Maßnahmen
Daten-Integrität: Kommunikation	Azure trifft/bietet Maßnahmen

5.4 Sicherheitsanforderungen: Authentizität

Authentizität der Kommunikationspartner

Die Authentizität des Kunden gegenüber dem Azure-Portal für die Verwaltung der IaaS- und PaaS-Dienste ist teilweise vorhanden. Eine Identitätsprüfung soll durch die Überprüfung der Telefonnummer und einer Kreditkarte stattfinden. Beide Verfahren bieten keine ideale Identitätsprüfung. Durch die Verifizierung der Telefonnummer können keine personenbezogenen Daten ermittelt werden. Die Angaben der Kreditkarte beweisen nur, dass eine Person Informationen zu einer Kreditkarte besitzt. Eine juristische

Authentifizierungsmöglichkeit, wie z.B. das Post-Ident-Verfahren der Deutschen Post ist nicht vorhanden.

Das Erstellen eines sogenannten „Fake-Accounts“ für Microsoft ist problemlos möglich und wurde getestet. SaaS-Dienste wie Office 365 konnten nach der Erstellung eines Accounts genutzt werden. Das unterschiedliche Sicherheitsniveau von SaaS- zum IaaS-Zugang begründet sich vermutlich dadurch, dass Azure die SaaS-Dienste kontrolliert und dem Nutzer nur wenig Freiraum geboten wird. Bei IaaS hat der Kunde direkte Kontrolle über einen Teil der Azure Infrastruktur.

Die Authentisierung der Webdienste gegenüber dem Nutzer erfolgt mittels HTTPS bzw. TLS und dem dazugehörigen Zertifikat, welches durch Microsoft Certificate Authority ausgestellt wird.

Die Authentizität der Kommunikationspartner (beim E-Mailverkehr) kann durch die Signatureigenschaft von asymmetrischer Verschlüsselung bestätigt werden. Voraussetzung ist, dass der Empfänger den öffentlichen Schlüssel des Senders besitzt und dieser seine Nachricht mit seinem privaten Schlüssel signiert. In Outlook wird hierfür das S/MIME Verfahren verwendet.

Authentizität der Nachrichten
Die Authentizität der Nachricht kann durch den Beweis des Ursprungs sichergestellt werden. Im Falle der Kommunikation per E-Mail bietet Azure die Nachrichtensignatur durch S/MIME. Bei dem Nachrichtenaustausch vom Cloud-Benutzer zu SaaS-Diensten oder Azure-Platform wird HTTPS bzw. TLS eingesetzt. Mit Hilfe eines vertrauenswürdigen Zertifikates identifiziert sich der Azure-Dienst gegenüber dem Benutzer. Eine Integritätsverletzung würde auch die Authentizität der Nachricht verletzen. Maßnahmen, die dies sicherstellen, werden in Daten-Integrität: Kommunikation (siehe Kapitel 5.3) genannt.

Authentizität der Daten
IaaS liegt außerhalb des Betrachtungsfeldes, da die Verantwortlichkeit der korrekten Verknüpfung der Bezeichner zu den Daten, bei dem Kunden liegt. In SaaS-Diensten ist der Benutzer verantwortlich für die korrekte Angabe der Daten zu ihren Bezeichnern. Azure kann dies nicht überprüfen.

Authentizität der Daten zur Steuerung und der Teilsysteme
Azure nennt keine konkreten Maßnahmen wie diese Anforderungen erreicht werden. Betrachtet man hingegen die Dienstleistungsvereinbarung, die Microsoft mit dem Kunden schließt, so wird diese Anforderung von Azure gedeckt. Ist die Authentizität der Daten zu Steuerung und die Authentizität der Teilsysteme verletzt, so führt dies in den meisten Fällen zu der Einschränkung der beteiligten Dienste. Microsoft gibt in seiner

Dienstleistungsvereinbarung eine Verfügbarkeit von mehr als 99% an (siehe Kapitel. 5.5.2 Verfügbarkeit der Daten und der Teilsysteme).

Ergebnis: Authentizität

Tabelle 6: Ergebnisse der Sicherheitsanforderung Authentizität

Sicherheitsanforderung	Ergebnis
Authentizität der Kommunikationspartner	Azure trifft/bietet Maßnahmen
Authentizität der Nachricht	Azure trifft/bietet Maßnahmen
Authentizität der Daten	Externer Verantwortungsbereich
Authentizität der Daten zur Steuerung und der Teilsysteme	Azure trifft/bietet Maßnahmen

5.5 Sicherheitsanforderungen: Verfügbarkeit

Verfügbarkeit der Infrastruktur (ISP)
Der Cloud-Client ist verantwortlich für die Auswahl seines Internet-Service-Providers. Für eine Verbindung mit hoher Verfügbar und Ausfallsicherheit sollte ein ISP mit entsprechender robuster Infrastruktur genutzt werden. Azure bietet keine Information über ihren Auswahlprozess eines ISP. Diese Anforderung ist nicht im direkten Verantwortungsbereich von Azure.

Verfügbarkeit der Daten und der Teilsysteme
MS führt, keine kaum Maßnahmen vor, die die Verfügbarkeit der Teilsysteme sicherstellen. Für die Verfügbarkeit der Dienste werden Garantien bis zu einem bestimmten Grad ausgesprochen. Bei Vertragsabschluss mit Azure gehen die Kunden eine Dienstleistungsvereinbarung (DLV) ein. Für kostenlos verfügbare Dienste werden keine Garantien versichert. Dienste, die durch die Tätigungen einer Zahlung genutzt werden, erhalten eine finanziell gestützte DLV. Die Verfügbarkeit der IaaS und PaaS Dienste wird immer mit mehr als 99 % angegeben. Interessant ist, dass die Verfügbarkeit des Dienstes Azure DNS in der DLV als einziges mit 100% garantiert wird: „*Wir garantieren, dass gültige DNS-Anforderungen stets zu 100 % eine Antwort von mindestens einem Azure DNS-Namensserver erhalten.*“[66] Es wird angenommen, dass mehrere Instanzen eines Dienstes parallel laufen und so Schutz vor Ausfällen bietet.

MS bezeichnet Ereignisse, die die Verfügbarkeit der Dienste stören als Dienstincidents. Diese werden in zwei Kategorien unterteilt. Die erste sind geplante Wartungsereignisse, die die Dienstverfügbarkeit einschränken können. Kunden werden mindestens fünfe Tage vor dem

geplanten Ereignis benachrichtigt und haben somit Zeit sich darauf einzustellen. Zu der zweiten Kategorie gehören ungeplante Ausfallzeiten wie beispielsweise Naturkatastrophen oder Störungen in einem Rechenzentrum. Ungeplante Dienstincidents werden erst durch Störungen bei mehreren Mandanten als solche eingestuft. Die konkrete technische Maßnahme ist die Verfügbarkeit von mehreren Rechenzentren in einer Region. Bei Ausfall des primären Standorts werden die Dienste im sekundären Standort betreiben. Allerdings kann laut MS eine gewisse Zweit vergehen, bis alle Funktionen unterbrechungsfrei laufen. Es gilt weiterhin die Bedingungen in der DLV und die damit verbunden Entschädigungsansprüche.[67]

In Azure Storage stehen mehrere Replikationsoptionen zur Verfügung, wie in Kapitel 3.5.4 beschrieben. Alle Daten werden repliziert und sind vor den meisten kritischen Ereignissen geschützt. Eine Ausnahme bilden extreme Naturkatastrophen, die mehrere Rechenzentren gleichzeitig betreffen. Nach einer Kündigung der MS-Dienstleistungen, wie bereits in Vertraulichkeit ruhender Daten (Kapitel 5.1) aufgeführt, sind die Daten des Kunden bis 90 Tage nach der Kündigung des Vertrages mit Leseberechtigung verfügbar.

Verfügbarkeit der Ressourcen

Die Azure Dienste unterliegen einem Ressourcenlimit und dieser wird abhängig von dem Dienst bestimmt. Das Limit kann auf Anfrage, wenn möglich, erhöht werden. Dazu folgendes Beispiel: Jedes Azure Abonnement ist mit der Rechenleistung von 20 Prozessorkernen verknüpft. Dieses Kontingent kann auf Nachfrage bis zu einer Kernanzahl von 10.000[15] skaliert werden. [68]

Die Verfügbarkeit von mehreren Rechenzentren in einer Region kann zudem als Sicherheitsmechanismus gewertet werden. Bei Verfügbarkeitsstörungen in einer Lokalität können die Ressourcen der anderen Rechenzentren dies kompensieren.

Ergebnis: Verfügbarkeit

Tabelle 7: Ergebnisse der Sicherheitsanforderung Verfügbarkeit

Sicherheitsanforderung	Ergebnis
Verfügbarkeit der Infrastruktur (ISP)	Externe Verantwortung
Verfügbarkeit der Daten und der Teilsysteme	Azure trifft/bietet Maßnahmen
Verfügbarkeit der Ressourcen	Azure trifft/bietet Maßnahmen

[15] Abhängig von der Verfügbarkeit in der jeweiligen Region.

5.6 Sicherheitsanforderungen: Nützlichkeit

Nützlichkeit der Daten
Der Kunde ist für die Nützlichkeit der Daten in IaaS verantwortlich. In SaaS ist Azure unter der Voraussetzung, dass die vom Kunden übermittelten Daten authentisch sind, der Verantwortungsträger.
Bei der Betrachtung verschlüsselter Daten und der Schlüsselverwaltung durch Azure muss diese die Verfügbarkeit und Nützlichkeit der Schlüssel sicherstellen. Kommt der Schlüssel abhanden, so verlieren die Daten ihren Nutzen. Die Daten in Azure Key Vault werden innerhalb derselben Region und in einer weiteregen Region, die mindestens 150 Meilen entfernt ist, repliziert. Die zweite Region befindet sich in der gleichen geographischen Zone wie die primäre Region. Störung, die Azure Key Vault betreffen, werden durch redundante Systeme in der gleichen Region behoben. Im Falle eines regionalen Ausfalls werden die Prozesse auf die sekundäre Region ausgelagert. [69]

Nützlichkeit der Daten zur Steuerung und Kontrolle
Azure ist für den Nutzen der Daten zur Steuerung und Kontrolle verantwortlich. Azure nennt keine technischen Maßnahmen, wie dies sichergestellt wird. Auch hier wird die Anforderung durch die Dienstleistungsvereinbarung erfüllt. Korrupte Daten würden die Verfügbarkeit der jeweiligen Dienstfunktionen beinträchtigen. MS nennt keine technischen Mechanismen, die diese Anforderung erfüllen. Auch hier führt der Weg über die DLV, die eine Verfügbarkeit der Dienste mit mehr als 99% angibt.

Ergebnis: Nützlichkeit

Tabelle 8: Ergebnisse der Sicherheitsanforderung Nützlichkeit

Sicherheitsanforderung	Ergebnis
Nützlichkeit der Daten	Azure trifft/bietet Maßnahmen
Nützlichkeit der Daten zur Steuerung und Kontrolle	Azure trifft/bietet Maßnahmen

5.7 Azure Sicherheitsereignisse

In Kapitel 4.2 wurden Maßnahmen erläutert, die MS trifft, um den in Kapitel 4.1 aufgelisteten Sicherheitsanforderungen gerecht. Zudem kann MS ihre Azure Sicherheitsmaßnahmen z.B. durch die Konformität zum C5-Anforderungskatalog des BSI nachweisen. Die folgenden Ereignisse bezüglich des Datenschutzes bei MS zeigen, dass Zertifikate in vielen Fällen nur die Grundschutzmaßnahmen bestätigen. Sie bieten jedoch keine Garantie für die Sicherheit der Systeme.

250 Millionen Einträge der Kundensupportdaten online verfügbar

Im Januar des Jahres 2020 wurde ein großer Daten-Leak seitens MS veröffentlicht. Sicherheitsforscher des Comparitech-security-research-Teams entdeckten fünf Elasticsearch-Server mit 250 Millionen Dateneinträgen zu Kundendaten und zu Servicekommunikation mit den Kunden. Das Datenleck entstand durch eine fehlerhafte Konfiguration der Datenbank, welche in Azure gehostet wurde. Laut Bob Diachenko, dem Teamleiter des Sicherheitsteams, waren die Datensätze auf allen fünf Servern identisch. Informationen, die mit einer Person in Verbindung gebracht werden konnten, seien geschwärzt gewesen. Dazu zählten die Vertragsnummer und Zahlungsinformationen. Zu den Daten, die im Klartext vorzufinden waren, gehörten laut Diachenko:

- E-Mail-Adresse des Kunden
- IP-Adressen
- Standorte
- Informationen zu Supportfällen
- MS-Support-Agent-E-Mails
- Interne Notizen, die als geheim markiert wurden [16]

Dadurch wurde gegen diverse Sicherheitsanforderungen verstoßen, insbesondere gegen die Vertraulichkeit. Die zugänglichen Informationen stufen eine Person nicht direkt als Kunden ein. Angreifer erhalten jedoch die Information darüber, dass eine bestimmte E-Mail zu einem MS-Kunden gehört. Somit ist der Kunde über seine E-Mail identifizierbar. IP-Adresse und Standortinformationen ergänzen das Profil des Kunden.

Angreifer, die die Daten kopieren, würden somit in den Besitz der Daten kommen. Damit wäre der Kunde nicht der alleinige Eigentümer seiner Daten. Die Information über die Kommunikationsteilnehmer und der Kommunikationsinhalt wurden offengelegt und dies verstößt gegen die Anforderung der Vertraulichkeit.

Zwei kritische Aspekte wurden bei der Konfiguration der Datenbank missachtet: Der Zugriff auf die Datenbank sollte Außenstehenden verwehrt sein und die Daten hätten verschlüsselt hinterlegt werden müssen. Weitere Kritik kann an der unzureichenden Überprüfung der Systeme geübt werden.

Die verfügbaren Informationen bieten die Möglichkeit eines Social-Engineering-Angriffs. Diese Art von Angriff gewinnt mehr und mehr an Popularität, da der Mensch als Schwachstelle einfacher zu überwinden ist als Hardware- oder Software-Schwachstellen. Ein bekanntes Beispiel ist der Anruf eines vermeintlichen Supportmitarbeiters von MS: Der Angreifer versucht, das Opfer zu einer Aktion zu verleiten, die seine eigene Kontrolle erhöht. Mit Informationen aus dem Datenbankleck kann ein Angreifer seine Vertrauenswürdigkeit zusätzlich steigern.

Laut Diachenko waren die Daten zwei Tage verfügbar, bevor MS die Schwachstelle geschlossen hat. Es sei nicht bekannt, ob unautorisierte Personen Einsicht in die Daten hätten. Die Daten umfassten einen Zeitraum von 14 Jahren (bis Dezember 2019). [71]

[16] Dieser Absatz folgt der Darstellung von [70].

SharePoint Phishing Scam
Das Forscherteam von AVANAN, einem E-Mail-Sicherheitsunternehmen, identifizierte eine Phishing-Attacke im Kontext von SharePoint. Die betroffenen Personen erhielten eine E-Mail, die sie zu einer Kollaboration über SharePoint einlud. Nach Aufruf des angegebenen Links wurden die Opfer auf eine SharePoint-Datei weitergeleitet. Diese enthielt einen weiteren Jeder-Link, der die Opfer auf ein OneDrive-Dokument delegierte. Die OneDrive-Einladung wurde einer authentischen Einladung durch OneDrive nachgeahmt. Nach Aufruf des zweiten Links wurden die Opfer auf eine imitierte Microsoft-Log-In-Seite weitergeleitet und aufgefordert, sich mit ihren Credentials anzumelden. Den Personen, die dies taten und keine MFA nutzten, wurden somit ihre Anmeldeinformationen gestohlen. [72] In diesem Fall wurden die Anforderungen Vertraulichkeit, Besitz/Kontrolle und Authentizität verletzt. Angreifer erhielten Einblick in die vertraulichen Anmeldeinformationen und besaßen die Daten ebenso wie das Opfer. Des Weiteren können sie damit die Kontrolle über die Daten und Systeme, die mit dem betroffenen Account verknüpft sind, ausüben.

Office 365 überprüft die Links in einer E-Mail auf blockierte oder suspekte Domains. In dem oben genannten Fall konnten die Angreifer diesen Sicherheitsmechanismus umgehen, indem sie den authentischen Einladungslink von SharePoint verwendeten. Die Forscher kritisieren hierbei die unzureichende Überprüfung von Links auf der untersten Ebene und die fehlende Überprüfung in anderen Diensten (wie in diesem Fall SharePoint) [72].

5.8 Bewertung der Azure-Schwachstellen

Im Folgenden werden veröffentlichte Schwachstellen von MS Azure gesammelt und in tabellarischer Form dargestellt. Betrachtet werden nur Schwachstellen, die von MS offiziell bestätigt wurden. Die National Vulnerability Database (NVD) ist eine online zugängliche Datenbank für die standardisierte Sammlung von Schwachstellen. Sie ist Eigentum der US-Behörden und bietet die Möglichkeit, sicherheitsrelevante Schwachstellen in Bezug auf ein Produkt einzusehen. Die Datenbank bietet unter anderem Angaben zu einer standardisierten Schwachstellen-ID, zu der Zeit der Veröffentlichung und zur Beurteilung durch einen Wert, der die Schwere der Schwachstelle indiziert.
Die Bewertung findet anhand des Common Vulnerability Scoring Systems Version 3.x (CVSS 3.x) statt. Dieses berechnet anhand verschiedener Metriken einen numerischen Wert, der die Auswirkung einer Schwachstelle einstufen kann. Eine qualitative Abstufung wird durch die Indikatoren *low, high, medium* und *critical* repräsentiert. [73]

Im Folgenden wird die Vorgehensweise bei der Datenfilterung in Bezug auf Azure-Schwachstellen aufgelistet:

1. Suche in der NVD nach dem Begriff „Azure“.

2. Filterung der Resultate nach einer offiziellen Stellungnahme von MS. Teilsysteme, wie Plug-Ins sind nicht Teil der Analyse, da externe Unternehmen für deren Sicherheit verantwortlich sind.
3. Pro Schwachstelle werden die Informationen Schwachstellen-ID, Datum der Veröffentlichung und CVSS-Wert gesammelt.
4. Die Schwachstellen werden nach den Angaben von MS den STRIDE-Kriterien zugeordnet.

5.8.1 STRIDE-Bedrohungen

Die STRIDE-Bedrohung wurden bei MS für die Bedrohungsmodellierung entwickelt und unterscheiden sechs Bedrohungsfälle. In der folgenden Tabelle werden die Bedrohungen aufgelistet und kurz beschrieben. Die Mehrheit der Bedrohungen kann mit den Attributen des Parkerian Hexads in Verbindungen gebracht werden. Eine vollständige Abdeckung ist nicht möglich.

Tabelle 9: STRIDE-Bedrohungen

STRIDE-Bedrohung	**Beschreibung der Bedrohung**	**Überlappung mit dem Parkerian Hexad**
Spoofing	Verschleierung der eigenen Identität, um autorisierten Zugang zu erlangen	Authentizität
Tampering	Unautorisierte Modifikation von Daten	Integrität
Repudiation	Das abstreiten einer getätigten Aktion durch einen Benutzer	Authentizität
Information disclosure	Unautorisierter Zugang zu Informationen	Vertraulichkeit
Denial of Service	Beeinträchtigung eines Systems in dem die Verfügbarkeit und Nutzbarkeit eingeschränkt wird	Verfügbarkeit
Elevation of Privilege	Nicht berechtigte Rechteerweiterung eines Benutzers	Es kann alle Attribute des Parkerian Hexads betreffen.

5.8.2 Azure Sicherheitslücken

Die Tabelle 3 enthält die gefilterten Schwachstellen von MS Azure. Die letzte Spalte beinhaltet die Zuordnung der einzelnen Bedrohungen zu den STRIDE-Kriterien und weiteren Bedrohungsarten. Dazu zählen Security Feature Bypass (SFB) und Remote Code Execution (RCE). Ein SFB bedeutet die Umgehung von Sicherheitsfunktionen. Diese schränken die Rechte von autorisierten und nicht autorisierten Benutzern ein. Aus der Perspektive eines externen Angreifers kann dieser durch die Umgehung von Sicherheitsfunktionen Rechte im System erhalten. Daher kann der SFB der STRIDE-Bedrohung Elevation of Privilege (EoP) zugeordnet werden kann.

Durch eine RCE-Schwachstelle können Angreifer Schadcode auf den betroffenen Systemen ausführen. Die sich daraus ergebende Bedrohung kann allen sechs STRIDE-Bedrohungen zugeordnet werden. Bei genauerer Betrachtung ist das erste Bedrohungsszenario die Erweiterung der Rechte. In der Ausgangssituation haben externe Angreifer nicht die Rechte, ihren Code im Kontext des betroffenen Systems auszuführen. Durch eine RCE-Schwachstelle erhalten sie die dafür nötigen Privilegien. Folglich wird RCE genau wie SFB der STRIDE-Bedrohung EoP zugeordnet. EoP-Bedrohungen werden durch den CVSS-Score in den meisten Fällen als hoch oder kritisch bewertet (siehe Tabelle 3). Auf Grundlage der neuen Zuordnung sind die drei kritischen Schwachstellen auf EoP zurückzuführen.

In Tabelle 2 wurde der Versuch unternommen, die STRIDE-Bedrohungen den jeweiligen Schutzzielen des Parkerian Hexads zuzuordnen, was jedoch nicht vollständig möglich war. Ein EoP kann beispielsweise Auswirkungen auf alle Attribute des PH haben. Die häufigsten Arten der Bedrohung sind das Spoofing und das EoP. Ersteres betrifft das Schutzziel Authentizität. Die Schwere dieser Schwachstelle wird in den meisten Fällen durch den CVSS als unkritisch bewertet. EoP-Schwachstellen hingegen werden oft als kritisch eingestuft. Direkte Verfügbarkeitsverletzungen sind am seltensten vorhanden. Microsoft gibt an, dass die unten aufgelisteten Schwachstellen durch Softwareupdates geschlossen wurden und dass bis dahin kein durch sie bedingter Angriff erfolgt war.

Tabelle 10: Azure Schwachstellen

Schwachstellen ID	Veröffentlicht	CVSS Severity V3.x	Art der Bedrohung
CVE-2016-7191	09.08.2016	8.1 HIGH	Elevation of Privilege
CVE-2017-8613	29.06.2017	8.1 HIGH	Elevation of Privilege
CVE-2018-8119	09.05.2018	5.6 MEDIUM	Spoofing
CVE-2018-8479	12.09.2018	5.6 MEDIUM	Spoofing
CVE-2018-8531	10.10.2018	8.8 HIGH	Remote Code Execution
CVE-2018-8600	13.11.2018	6.1 MEDIUM	Spoofing
CVE-2018-8652	11.12.2018	5.4 MEDIUM	Spoofing
CVE-2019-0729	05.03.2019	9.8 CRITICAL	Elevation of Privilege
CVE-2019-0741	05.03.2019	7.5 HIGH	Information Disclosure
CVE-2019-5917	12.03.2019	7.5 HIGH	Denial-of-service
CVE-2019-0804	08.04.2019	6.5 MEDIUM	Information Disclosure
CVE-2019-0816	08.04.2019	5.1 MEDIUM	Security Feature Bypass
CVE-2019-0857	09.04.2019	6.5 MEDIUM	Spoofing
CVE-2019-0866	09.04.2019	6.1 MEDIUM	Spoofing
CVE-2019-0867	09.04.2019	6.1 MEDIUM	Spoofing
CVE-2019-0868	09.04.2019	6.1 MEDIUM	Spoofing
CVE-2019-0869	09.04.2019	6.1 MEDIUM	Spoofing
CVE-2019-0870	09.04.2019	6.1 MEDIUM	Spoofing
CVE-2019-0871	09.04.2019	6.1 MEDIUM	Spoofing
CVE-2019-0874	09.04.2019	6.1 MEDIUM	Spoofing
CVE-2019-0875	09.04.2019	7.5 HIGH	Elevation of Privilege
CVE-2019-0872	16.05.2019	5.4 MEDIUM	Spoofing
CVE-2019-0971	16.05.2019	6.5 MEDIUM	Information Disclosure
CVE-2019-0979	16.05.2019	5.4 MEDIUM	Spoofing
CVE-2019-1000	16.05.2019	5.3 MEDIUM	Elevation of Privilege
CVE-2019-0996	12.06.2019	6.5 MEDIUM	Spoofing
CVE-2019-0962	15.07.2019	4.9 MEDIUM	Elevation of Privilege
CVE-2019-1072	15.07.2019	9.8 CRITICAL	Remote Code Execution
CVE-2019-1172	14.08.2019	4.3 MEDIUM	Information Disclosure
CVE-2019-1258	14.08.2019	8.8 HIGH	Elevation of Privilege
CVE-2019-1306	11.09.2019	9.8 CRITICAL	Remote Code Execution
CVE-2019-1372	10.10.2019	10.0 CRITICAL	Remote Code Execution
CVE-2019-1234	12.11.2019	7.5 HIGH	Spoofing
CVE-2020-0700	12.03.2020	5.4 MEDIUM	Spoofing
CVE-2020-0758	12.03.2020	7.5 HIGH	Elevation of privilege
CVE-2020-0815	12.03.2020	7.5 HIGH	Elevation of privilege

5.9 Abschließende Bewertung

In diesem Kapitel wurden mithilfe der in Kapitel 4 definierten Sicherheitsanforderungen die Sicherheitsfunktionen, die Azure bereitstellt, erarbeitet. Dabei wurde die Erkenntnis gewonnen, dass sie für einige Aspekte konkrete technische Maßnahmen zur Verfügung stellen. Die meisten Anforderungen jedoch werden durch organisatorische Maßnahmen erfüllt. Für einige von ihnen wie z.B. die an die „Nützlichkeit der Daten zur Steuerung und Kontrolle“ führt der Weg über die DLV, um sie als erfüllt einzustufen. Außerdem wird die Integrität der Daten von MS fälschlicherweise mit der Vertraulichkeit der Daten verbunden. Konkrete Funktionen, die die Integrität der Daten (data at rest) in den SaaS-Diensten sicherstellen werden nicht genannt.

Die aufgeführten Sicherheitsereignisse und Schwachstellen zeigen, dass die Dienste kritische Lücken enthalten können, die die Schutzziele des PH verletzen. Der Vorfall der öffentlich zugänglichen Kundendaten zeigt, dass die von MS getroffenen organisatorischen Maßnahmen bezüglich der Überprüfung von Konfigurationsentscheidungen durch Mitarbeiter unzureichend sind.

6 Integration von MS AZURE

In diesem Kapitel wird untersucht, wie die in Kapitel 4 und 5 identifizierten Sicherheitsfunktionen an HAW Hamburg integriert werden können und welchen Nutzen die Hochschule aus ihnen ziehen kann. Dazu werden zwei Anwendungsfälle betrachtet und diesen werden Azure-Dienste mit ihren jeweiligen Sicherheitsmechanismen zugeordnet.

6.1 Sicherheitsfunktionen in Azure

In Kapitel 5 wurden neben den in Kapitel 3 vorgestellten Sicherheitsfunktionen, die Azure zur Verfügung stellt, weitere anhand des Sicherheitsanforderungskatalogs aus Kapitel 4 identifiziert. Die erarbeiteten Funktionen sind:

- E-Mail-Verschlüsselung und -Signatur durch S/MIME
- TLS 1.2 für den Schutz der Schicht 5 im OSI-Modell
- Serverseitige Authentisierung durch Zertifikate
- IPsec für den Schutz der Schicht 3 im OSI-Modell
- Microsoft-Bitlocker-Verschlüsselung der Datenträger mit einer Schlüssellänge von 256 Bit
- Verschlüsselung ruhender Daten mit dem AES-256-Verfahren
- Information Rights Management in SharePoint Online
- Zugriffskontrolle für SharePoint-Online-Inhalte anhand der Geräteidentität oder durch die Angabe von Netzwerkadressen
- Authentisierung und Isolation der Benutzerdaten durch AAD
- MFA durch AAD
- Trusted Execution Environments und homomorphe Verschlüsselung für die Vertraulichkeit der Daten in Nutzung

- Redundante Speicherung von Schlüsseln und Daten, verteilt über unabhängige Rechenzentren
- Objektmetadatenverschlüsselung in Azure Storage
- Sicherung und Überwachung der Datenzentren

Die aufgeführten Punkte lassen sich in technische und nicht-technische Sicherheitsfunktionen unterteilen. Zu dem letzten Aspekt gehören z.B. organisatorische Maßnahme wie die Überwachung der Rechenzentren oder die redundante Speicherung der Verschlüsselungsschlüssel.

6.2 Integration der technischen Sicherheitsfunktionen

Anwendungsfall 1
Ein Dozent möchte das von ihm angefertigte Dokument für die kommende Klausur sicher speichern. Nur er oder von ihm autorisierte Personen dürfen Einblick in das Dokument erhalten oder es bearbeiten. Die erste Möglichkeit der Sicherung ist, die Datei lokal auf seinem Computer zu speichern. Das Endgerät stellt in diesem Fall ein Single Point of Failure dar. Das bedeutet, dass bei technischen Störungen am Rechner das Dokument nicht mehr verfügbar wäre. Um dem vorzubeugen, könnte er die Datei auf externen Datenträgern speichern. Diese müssen sicher aufbewahrt werden, was wiederum einen Nachteil darstellt. Zudem kann jeder, der Zugriff auf den Computer oder den externen Datenträger hat, die Datei einsehen, falls sie nicht kryptographisch gesichert wurde.

Eine alternative Lösung ist die Speicherung in der Cloud. Unter der Annahme, dass die HAW Hamburg sich für die Speicherlösung OneDrive von Microsoft entscheidet, ist der erste von dem Dozenten auszuführende Schritt die Authentisierung bei OneDrive. Da die Hochschule ihren eigenen Identitätsdienst behalten möchte, erfolgt der Authentisierungsschritt lokal in ihrem Rechenzentrum. Anschließend wird der Authentisierungs-Token mit TLS gesichert und an AAD übertragen, welches dem Dozenten den Zugang gewährt. Nach der erfolgreichen Anmeldung können Dateien in die Cloud übertragen werden. Die Vertraulichkeit und Integrität des Dokuments auf dem Übertragungsweg werden mit TLS 1.2 gesichert. Die Implementation von TLS 1.2 in Azure unterstützt zudem das Perfect Forward Secrecy. Somit können einzelne Sessions bei Kompromittierung des privaten Serverschlüssels entschlüsselt werden. Im zweiten Schritt erfolgt die Verschlüsselung der Datei mit einem AES-256-Bit-Schlüssel und ihre anschließende Speicherung in der Cloud. Der zugehörige Datenträger wird mit MS Bitlocker ebenfalls mit einer Schlüssellänge von 256 Bit verschlüsselt. Die Daten und die Schlüssel werden zudem über mehrere Rechenzentren repliziert, was somit einen Single Point of Failure vermeidet.

Die HAW Hamburg betreibt einen vergleichbaren Cloud-Dienst für die Datenspeicherung. Ihr eigener Cloud-Speicher, die HAW-Cloud, ist für ihre Studenten und Beschäftigten zugänglich

und basiert auf dem OpenSource-Cloud-Dienst ownCloud [74]. Die Daten werden im internen Datenzentrum der Hochschule gespeichert [75]. Es handelt sich demnach um eine private Cloud.

Tabelle 11: Gegenüberstellung von HAW-Cloud und OneDrive

Technische Sicherheitsmaßnahmen	HAW-Cloud	OneDrive
Verschlüsselung des Datenträgers und der Datei	Die Dateien werden mit dem AES-256-Verfahren verschlüsselt.[76]. Keine integrierte Datenträ-gerverschlüsselung	Die Dateien werden mit dem AES-256-Verfahren verschlüsselt. Festplattenverschlüsselung mit Bitlocker
Sicherung des Kommunikationskanals	Ja, mit TLS 1.2. Keine Unterstützung für TLS 1.3[17]	Ja, mit TLS 1.2. Keine Unterstützung für TLS 1.3[17]
Authentisierung	Ja	Ja
MFA	möglich	möglich
Integritätscheck bei der Datenübertragung	Überprüfung durch integrierte Mechanismen in TLS 1.2	Überprüfung durch integrierte Mechanismen in TLS 1.2
Replikation der Daten über mehrere Rechenzentren	Nein, die Daten werden im internen Datenzentrum der Hochschule gespeichert.	Ja
Replikation der Verschlüsselungsschlüssel	Nein	Ja

OneDrive unterscheidet sich von der HAW-Cloud in erster Linie durch die Replikationsfunktion für die Daten und die verwendeten Schlüssel. Des Weiteren sind neben den Daten auch die Datenträger verschlüsselt. Um ein ähnliches Maß an Sicherheit zu bieten, müsste die HAW ein zweites externes Rechenzentrum für die HAW-Cloud betreiben.

Anwendungsfall 2

Der zweite Anwendungsfall ist das Verschicken von Nachrichten in Form von E-Mails. Der Inhalt muss bei der Übertragung und Speicherung im Postfach für Unberechtigte geheim bleiben. Zudem wird eine Zusicherung, dass der Absender der E-Mail genau der ist, für den er sich ausgibt, verlangt.

Office 365 ermöglicht dies mit der Nachrichtenverschlüsselung und -Signatur durch S/MIME. Die Nachrichten werden Ende-zu-Ende verschlüsselt und gespeichert. Die Authentizität der Kommunikationspartner und der Nachricht sowie die Datenintegrität werden durch die

[17] Überprüfung durch einen SSL-Server-Test durch https://www.ssllabs.com/ssltest/

Eigenschaft asymmetrischer Schlüssel in Kombination mit symmetrischer Verschlüsselung erreicht.

Die HAW verwendet zurzeit Microsoft Exchange als E-Mail-Server. Der Zugriff kann über ein Webinterface oder lokale Clients erfolgen. Für die Verwendung von S/MIME in Outlook muss der Server-Administrator zunächst eine Windows-basierte Zertifizierungsstelle einrichten [13], um X.509-Zertifikate zu erstellen. Die Studenten und Beschäftigten können anschließend ihr Zertifikat bei der zentralen Vergebungsstelle beantragen und ihre Nachrichten damit schützen.

Eine Alternative zu S/MIME bietet das Verfahren OpenPGP. PGP kann neben der Sicherung von E-Mails auch andere Daten verschlüsseln. Die Funktionsweise beider Methoden ist ähnlich, sie unterscheiden sich jedoch bei der Vergabe der Schlüssel. Während bei S/MIME die Zertifikate von einer zentralen CA ausgestellt werden und die öffentlichen Schlüssel anderen Benutzern zentral zugänglich sind, muss der Benutzer bei OpenPGP die Zertifikate selbst erzeugen und seinen öffentlichen Schlüssel verteilen.

7 Zusammenfassung und weiterführende Aspekte

7.1 Zusammenfassung

Zunächst wurde in den Grundlagen eine anerkannte Definition des Cloud Computings eingeführt, die auch vom Europäischen Parlament genutzt wird. Anschließend erfolgte der Vergleich zwischen den drei Cloud-Service-Modellen und zwischen den drei Cloud-Bereitstellungsmodellen. Anhand einer Abbildung wurde gezeigt, dass sich die Verwaltungsbereiche des Kunden und des Cloud-Anbieters abhängig vom Service-Modell unterscheiden. Der Vergleich zwischen öffentlicher und privater Cloud zeigte, wie diese sich im Hinblick auf Sicherheit und Kontrolle unterscheiden: Die private Cloud bietet mehr Freiheiten bei der Wahl der Sicherheitsmechanismen, der Lagerung der Daten und der Anpassung an die genutzte Software. Die öffentliche Cloud hingegen weist mehr Funktionalitäten in Form von Verfügbarkeit, Anwendungsdiensten und schneller Skalierbarkeit auf.

Im Anschluss an die Grundlagen wurde die Cloud-Plattform Azure von Microsoft vorgestellt. Dargelegt wurden u.a. der SaaS-Dienst SharePoint Online mit seinen integrierten Sicherheitsfunktionen, die E-Mail-Verschlüsselung in Office 365, insbesondere durch das S/MIME-Verfahren, und der zentrale Authentisierungsdienst Azure Active Directory. Microsoft kommt zu dem Schluss, dass eine Verlagerung des Sicherheitsperimeters von dem Netzwerk auf die Identität stattfindet, da ersteres als kompromittiert angesehen werden

muss. Dies gilt insbesondere für die öffentliche Cloud, da sie bedingt durch ihr Konzept für alle zugänglich ist.

Ziel dieser Arbeit war es herauszufinden, wie die Sicherheitsfunktionen von Azure in einer Hochschule integriert werden könnten. Dafür mussten zuerst die darin angebotenen Sicherheitsfunktionen identifiziert werden. Die Herangehensweise bestand darin, zunächst Sicherheitsanforderungen an den Einsatz einer Cloud in der HAW Hamburg zu definieren. Anhand der Anforderungen konnte im Anschluss untersucht werden, ob Azure Maßnahmen vorsieht, die diese erfüllen. Für die systematische Aufstellung von Sicherheitsanforderungen wurde zunächst ein Sicherheitsmodell benötigt, das die zu schützenden Bereiche bei der Verwendung einer Cloud aufzeigt. Dabei offenbarte sich das Problem eines fehlenden allgemeingültigen und anerkannten Modells für das Cloud Computing. Daraufhin wurde zunächst die Forschung in diesem Bereich betrachtet, mit dem Ergebnis, dass die CIA-Triade die Basis für diverse andere Modelle darstellt. Bei näherer Untersuchung der Triade ergab sich jedoch folgende Schwierigkeit: ihre Schutzziele wurden vor der Verbreitung des modernen Internets entwickelt und weisen diesbezüglich Defizite auf. Eine direkte Kritik an der Triade wurde von dem Sicherheitsforscher Donn Parker geübt, der eine Ergänzung mit drei zusätzlichen Attributen vorschlug, um die eingeschränkte Sichtweise der Triade für die neuen Gegebenheiten zu erweitern. Zur Überprüfung seiner Kritik wurden die beiden Modelle miteinander verglichen, mit dem Ergebnis, dass Parkers Modell für die Anforderungsdefinition der Cloud besser geeignet ist. Anschließend wurde die Sicherheitsanforderung mithilfe der Vorarbeit von T. Tetzner formuliert.

Vor der Untersuchung der Maßnahmen anhand des im Kapitel 4 eingeführten Sicherheitsfunktionskatalogs wurde der Verantwortungsbereich des Kunden im Vergleich zu dem von Azure aufgezeigt. MS spricht von einer geteilten Verantwortung, d.h. zu keinem Zeitpunkt kann sie ihnen die komplett zugesprochen werden, denn der Kunde trägt auch einen Teil davon. Die Abarbeitung der Anforderung ergab, dass Azure für die meisten Aspekte Maßnahmen trifft oder dem Kunden die jeweiligen Funktionen bietet, die diese erfüllen. Dabei wurde die Erkenntnis gewonnen, dass Azure für einige Sicherheitsanforderungen konkrete technische Sicherheitsfunktionen implementiert oder zur Verfügung stellt. Andere hingegen werden durch organisatorische Maßnahmen abgedeckt. Dazu gehören beispielsweise die Überwachung und Überprüfung ihrer Rechenzentren oder auch die redundante Speicherung von Verschlüsselungsschlüsseln. Werden keine Maßnahmen genannt, führt der Weg über die Dienstleistungsvereinbarung. In dieser garantiert Microsoft, dass ihre Dienste und die zugehörigen Funktionalitäten zu einem gewissen Grad (über 99%) verfügbar sein werden.
Die meisten technischen Maßnahmen werden zum Service IaaS geboten und die wenigsten zu den fertigen Software-Lösungen von Office im Bereich SaaS. Des Weiteren verknüpft MS den Schutz der Datenintegrität häufig mit der Datenverschlüsselung. Dies ist jedoch als

inkorrekt zu beurteilen, da verschlüsselte Daten verändert werden können und eine Verschlüsselung nicht die notwendigen Sicherheitsmechanismen bietet, diese zu erkennen.
Nach der Identifikation der Sicherheitsfunktionen wurden zwei Azure betreffende Sicherheitsereignisse vorgestellt. In einem Fall waren Kundensupportdaten mit persönlichen Kundendaten durch eine falsche Konfiguration der Datenbank frei zugänglich. Der Vorfall zeigt, dass die organisatorischen Maßnahmen seitens MS unzureichend waren. Im Anschluss wurden bekannte Sicherheitsschwachstellen in Azure und ihre Zuordnung den STRIDE-Bedrohungen tabellarisch dargestellt. Zudem wurde der Versuch unternommen, die Bedrohungen den sie betreffenden Schutzzielen des Parkerian Hexads zuzuordnen. Eine konkrete Verknüpfung ist in einigen Fällen nicht möglich und so kann es sein, dass eine Bedrohung mehrere Schutzziele gefährdet. Die häufigsten Bedrohungen, die Azure betrafen, waren das Spoofing und die unautorisierte Rechteerweiterung, wobei letztere alle Attribute des PH gefährden könnte.

Im abschließenden Kapitel des Hauptteils wurden die in Kapitel 3 und 5 identifizierten Sicherheitsfunktionen aufgelistet. Es wurde überprüft, wie vor allem die technischen Funktionen an der HAW Hamburg integriert werden könnten. Dafür wurden zwei Anwendungsfälle angeführt. Im ersten Fall wurde das Betreiben eines Cloud-Speichers für Studierende und Beschäftigte betrachtet. Die HAW betreibt in ihrem internen Rechenzentrum bereits ihren eigenen Cloud-Speicher, und zwar basierend auf einem OpenSource-Programm. Im Anschluss wurden dessen Sicherheitsfunktionen mit denen des Cloud-Speichers OneDrive von Office 365 (Azure) verglichen. Die HAW-Cloud setzt in den meisten Fällen die gleichen Funktionen ein wie der Azure-Dienst. Sie differieren jedoch bezüglich der Redundanzoptionen. Azure bietet eine größere Infrastruktur und kann Daten und Verschlüsselungsschlüssel auf mehrere unabhängige Rechenzentren verteilen, was die Aspekte der Verfügbarkeit und Nützlichkeit der Daten stärkt.
Im zweiten Anwendungsfall wurde die sichere Übertragung und Speicherung von E-Mails in der HAW betrachtet. Diese benutzt aktuell MS-Systeme wie Exchange und Outlook Web App. Die Einrichtung einer zentralen Zertifizierungsstelle ist noch nicht erfolgt. Eine Alternative zu S/MIME stellt das OpenPGP-Verfahren dar. Ersteres hat den Vorteil, dass die Vergabe der Zertifikate zentral durch die HAW erfolgen kann. In diesem Anwendungsfall müssten weitere organisatorische Maßnahmen getroffen werden. Die Benutzer müssten über das Verfahren informiert und die Wichtigkeit verdeutlicht werden.

Die Untersuchungen in dieser Arbeit haben gezeigt, dass die Azure Cloud zum Teil als Black Box betrachtet wird. Abhängig von den Service-Modellen stellt MS teils ausreichende, teils jedoch zu wenig Informationen über ihre Sicherheitsmaßnahmen zur Verfügung. Bei IaaS, in dem der Benutzer auf die Implementierung der notwendigen Mechanismen achten muss, werden seitens MS mehr Informationen zur Verfügung gestellt. Bei von MS verwalteten SaaS-Diensten hingegen sind zu wenige konkrete Maßnahmen zu finden. Des Weiteren wird von Microsoft das Basissicherheitsmodell, die CIA-Triade, bei der Betrachtung der Azure-Systeme

genutzt. Hier ist es wünschenswert, dass alternative Modelle wie das PH und deren Sichtweise auf die IT-Schutzziele berücksichtigt werden.

7.2 Weiterführende Aspekte

Im Jahr 2019 erklärte der hessische Datenschutzbeauftragte die Nutzung von Office 365 an hessischen Schulen für rechtswidrig. Nach intensiven Gesprächen mit MS wurde die Nutzung an Schulen jedoch unter Einhaltung gewisser Bedingungen erlaubt. Es wurde angeordnet, dass MS den Schulen die notwendigen Handlungsanleitungen zur Verfügung stellen müsse, damit diese die Übermittlung der Diagnosedaten unterbinden könnten. [77]
Eine wichtige Frage, die bei der Nutzung von Cloud-Diensten aufkommt, ist demnach die des Datenschutzes. Die Speicherung von personenbezogenen Daten in einer öffentlichen Cloud ist an sich unzulässig. Es wäre daher sinnvoll, in Zukunft zu überprüfen, ob und wie bei der Nutzung einer Cloud dennoch personenbezogene Daten entstehen könnten.

Neben Azure sind weitere etablierte Cloud-Plattformen wie der Amazon Web Service oder die Google Cloud vorhanden. Hier bietet sich der Vergleich dieser Plattformen und ihrer Sicherheitsfunktionen an.

Literaturverzeichnis

[1] L. Columbus, *Roundup Of Small & Medium Business Cloud Computing Forecasts And Market Estimates, 2015.* [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2015/05/04/roundup-of-small-medium-business-cloud-computing-forecasts-and-market-estimates-2015/ (accessed: Jul. 10 2020).

[2] IDG Communications, "2018 Cloud Computing Executive Summary," 2018.

[3] Cybersecurity Insiders, "2019 Cloud Security Report (ISC)2," 2019.

[4] P. M. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[5] Civic Consulting, "Cloud Computing (Deutsche Übersetzung)," 2012.

[6] Cinar Kilcioglu, Justin M. Rao, Aadharsh Kannan, and R. Preston McAfee, *Usage Patterns and the Economics of the Public Cloud*. Perth, Australia: International World Wide Web Conferences Steering Committee. [Online]. Available: https://doi.org/10.1145/3038912.3052707

[7] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, "Benefits and challenges of three cloud computing service models," in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, 2012, pp. 198–205.

[8] A. C. Michael, "The cloud as an innovation platform for software development," *Commun. ACM*, vol. 62, no. 10, pp. 20–22, 2019, doi: 10.1145/3357222.

[9] Microsoft, *Vertrauen Sie Ihrer Cloud | Microsoft Azure.* [Online]. Available: https://azure.microsoft.com/de-de/overview/trusted-cloud/ (accessed: Jul. 3 2020).

[10] Microsoft, *Globale Infrastruktur | Microsoft Azure.* [Online]. Available: https://azure.microsoft.com/de-de/global-infrastructure/ (accessed: Jul. 3 2020).

[11] *Warum Office 365? - Die Fakten.* [Online]. Available: https://www.communardo.de/warum-office-365-die-fakten/ (accessed: Jun. 2 2020).

[12] Leslie H Cole, *E-Mail-Verschlüsselung - Microsoft 365 Compliance.* [Online]. Available: https://docs.microsoft.com/de-de/microsoft-365/compliance/email-encryption?view=o365-worldwide (accessed: Jun. 1 2020).

Literaturverzeichnis

[13] C. D. Matt Penna, *S/MIME für die Nachrichtensignierung und -verschlüsselung.* [Online]. Available: https://docs.microsoft.com/de-de/Exchange/policy-and-compliance/smime/smime?view=exchserver-2019 (accessed: Jun. 1 2020).

[14] Kaarin Shumate et al., *Einführung in SharePoint Online - SharePoint Online.* [Online]. Available: https://docs.microsoft.com/de-de/sharepoint/introduction (accessed: May 12 2020).

[15] Mike Plumley et. al., *Planen & Bereitstelleneiner Datei Zusammenarbeitsumgebung – SharePoint - SharePoint Online.* [Online]. Available: https://docs.microsoft.com/de-de/sharepoint/deploy-file-collaboration (accessed: May 31 2020).

[16] Mike Plumley et. al., *Externe Freigabe – Übersicht - SharePoint Online.* [Online]. Available: https://docs.microsoft.com/de-de/sharepoint/external-sharing-overview (accessed: May 31 2020).

[17] Kaarin Shumate et. al., *Steuern des Zugriffs von nicht verwalteten Geräten - SharePoint Online.* [Online]. Available: https://docs.microsoft.com/de-de/sharepoint/control-access-from-unmanaged-devices (accessed: May 31 2020).

[18] Kaarin Shumate, *Netzwerkstandort basierter Zugriff auf SharePoint und OneDrive - SharePoint Online.* [Online]. Available: https://docs.microsoft.com/de-de/sharepoint/control-access-based-on-network-location (accessed: May 12 2020).

[19] Mike Plumley et. al., *SharePoint-Authentifizierung - SharePoint Online.* [Online]. Available: https://docs.microsoft.com/de-de/sharepoint/authentication (accessed: Jun. 15 2020).

[20] TerryLanfear, *Bewährte Methoden für sichere PaaS-Bereitstellungen – Microsoft Azure | Microsoft Docs.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/paas-deployments (accessed: Mar. 11 2020).

[21] Barclayn, *Bewährte Methoden für die Azure-Identitäts- und Zugriffssicherheit | Microsoft Docs.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/identity-management-best-practices (accessed: Mar. 11 2020).

[22] Microsoft, *Azure Multi-Factor Authentication – Übersicht.* [Online]. Available: https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-howitworks (accessed: May 26 2020).

[23] Microsoft, *Einmaliges Anmelden bei Anwendungen – Azure Active Directory.* [Online]. Available: https://docs.microsoft.com/de-de/azure/active-directory/manage-apps/what-is-single-sign-on (accessed: May 27 2020).

[24] Microsoft, *Einführung in Azure Storage – Cloudspeicher in Azure.* [Online]. Available: https://docs.microsoft.com/de-de/azure/storage/common/storage-introduction (accessed: Jun. 3 2020).

[25] Microsoft, *Einführung in den Blob(objekt)speicher - Azure Storage.* [Online]. Available: https://docs.microsoft.com/de-de/azure/storage/blobs/storage-blobs-introduction (accessed: Jun. 3 2020).

[26] Hemant Sharma, *Azure Storage Tutorial – Tables, Blobs, Queues & File Storage in Microsoft Azure.* [Online]. Available: https://www.edureka.co/blog/azure-storage-tutorial/ (accessed: Jun. 3 2020).

Literaturverzeichnis

[27] Microsoft, *Azure Storage-Verschlüsselung für ruhende Daten.* [Online]. Available: https://docs.microsoft.com/de-de/azure/storage/common/storage-service-encryption (accessed: Jun. 3 2020).

[28] Microsoft, *SLA für Speicherkonten | Microsoft Azure.* [Online]. Available: https://azure.microsoft.com/de-de/support/legal/sla/storage/v1_5/ (accessed: Jun. 3 2020).

[29] Microsoft, *Datenredundanz - Azure Storage.* [Online]. Available: https://docs.microsoft.com/de-de/azure/storage/common/storage-redundancy (accessed: Jun. 3 2020).

[30] David E. Bell, Leonard J. LaPadula, "Secure Computer System: Unified Exposition and Multics Interpretation," 1976.

[31] K.J. Biba, "Integrity Considerations for Secure Computer System," 1975. [Online]. Available: https://www.cs.colostate.edu/~cs656/reading/ieee-se-13-2.pdf

[32] Denning, "An Intrusion-Detection Model," 1987.

[33] S. Samonas and D. Coss, "THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY," *Journal of Information System Security*, vol. 10, no. 3, 2014. [Online]. Available: http://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf

[34] Y. CHERDANTSEVA and J. Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," 2013.

[35] ISO, *ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary.* [Online]. Available: https://www.iso.org/obp/ui/ (accessed: Jun. 28 2020).

[36] Thaddäus Tetzner, "Sicherheitsanforderungen_an_das_Cloud_Computing," 2009.

[37] D. B. Parker, *Fighting computer crime: A new framework for protecting information*. New York: Wiley, 1998.

[38] J. Andress and S. Winterfeld, Eds., *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice,* 2nd ed. Amsterdam: Elsevier/Syngress, 2014.

[39] *Parkerian Hexad - an overview | ScienceDirect Topics.* [Online]. Available: https://www.sciencedirect.com/topics/computer-science/parkerian-hexad (accessed: Jun. 13 2020).

[40] GPender-Bey, "The parkerian hexad," 2012.

[41] *Here's How Metadata on Billions of Phone Calls Predicts terrorist Attacks.* [Online]. Available: http://trumancenter.org/doctrine-blog/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/ (accessed: Jun. 14 2020).

[42] E. T. Frank Simorjay, "Shared Responsibility for Cloud Computing," 2019.

[43] Microsoft, *Gemeinsame Verantwortung in der Cloud – Microsoft Azure.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility (accessed: Jun. 15 2020).

[44] Microsoft, *Azure-Datenverschlüsselung ruhender Daten | Microsoft Docs.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-atrest (accessed: Mar. 10 2020).

Literaturverzeichnis

[45] Markus Feichtner, Debra Shinder, Dr. Christoph Siegert, “Sicherheit und Compliance bei der Datenverarbeitung mit Azure,” [Online]. Available: https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/de-de/Achieving_Compliant_Data_Residency_and_Security_with_Azure_de-DE.pdf

[46] Microsoft, *Isolation in der öffentlichen Azure-Cloud.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/isolation-choices (accessed: May 1 2020).

[47] Microsoft, *Physische Sicherheit der Azure-Rechenzentren.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/physical-security (accessed: May 10 2020).

[48] Microsoft, *Übersicht über die Azure-Verschlüsselung.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview (accessed: Jul. 12 2020).

[49] *IPsec - Security Architecture for IP (VPN).* [Online]. Available: https://www.elektronik-kompendium.de/sites/net/0906191.htm (accessed: May 4 2020).

[50] KC Cross, *Encryption for data in transit - Microsoft 365 Compliance.* [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-for-data-in-transit?view=o365-worldwide (accessed: Jul. 5 2020).

[51] T. Jain, “Azure + Dynamics 365 (Germany) SOC 2 Type II + C5 + CSA Star Report (2019-04-01 to 2020-03-31),”

[52] Mark Russinovich, *Introducing Azure confidential computing | Azure-Blog und - Updates| Microsoft Azure.* [Online]. Available: https://azure.microsoft.com/de-de/blog/introducing-azure-confidential-computing/ (accessed: May 6 2020).

[53] Mark Russinovich, *The Rise of Confidential Computing.* Accessed: May 6 2020. [Online]. Available: https://www.youtube.com/watch?v=rJpFHADlvQA

[54] Microsoft, *Microsoft SEAL: Fast and Easy-to-Use Homomorphic Encryption Library.* [Online]. Available: https://www.microsoft.com/en-us/research/project/microsoft-seal/ (accessed: Jul. 12 2020).

[55] Microsoft, *Datenschutzerklärung für Microsoft Cloud Germany.* [Online]. Available: https://azure.microsoft.com/de-de/support/legal/privacy-statement/germany/ (accessed: May 6 2020).

[56] Bundesamt für Sicherheit in der Informationstechnik, “Anforderungskatalog Cloud Computing,” 2020.

[57] Microsoft, *Schutz der Azure-Kundendaten.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/protection-customer-data (accessed: May 8 2020).

[58] Microsoft, *Globales Microsoft-Netzwerk.* [Online]. Available: https://docs.microsoft.com/de-de/azure/networking/microsoft-global-network (accessed: Jun. 28 2020).

[59] Microsoft, *Azure-Infrastrukturüberwachung.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure-monitoring (accessed: Jun. 28 2020).
[60] Microsoft, *Law Enforcement Requests Report – Microsoft CSR.* [Online]. Available: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (accessed: Jul. 12 2020).
[61] Microsoft, *Authentifizierung für Azure AD-Hybrididentitätslösungen - Active Directory.* [Online]. Available: https://docs.microsoft.com/de-de/azure/active-directory/hybrid/choose-ad-authn (accessed: Jul. 12 2020).
[62] Debra Shinder, "Trusted Cloud: Microsoft Azure Security, Privacy, Compliance, Reliability/Resiliency, and Intellectual Property," 2019.
[63] Microsoft, *Überwachung der Dateiintegrität in Azure Security Center.* [Online]. Available: https://docs.microsoft.com/de-de/azure/security-center/security-center-file-integrity-monitoring (accessed: May 12 2020).
[64] Microsoft, *Datenredundanz - Azure Storage.* [Online]. Available: https://docs.microsoft.com/de-de/azure/storage/common/storage-redundancy (accessed: May 12 2020).
[65] C. C. Sunny Deng, *Was ist Azure Security Center?* [Online]. Available: https://docs.microsoft.com/de-de/azure/security-center/security-center-intro (accessed: May 12 2020).
[66] Microsoft, *Übersicht der Dienstleistungsvereinbarungen | Microsoft Azure.* [Online]. Available: https://azure.microsoft.com/de-de/support/legal/sla/summary/ (accessed: Jun. 2 2020).
[67] Microsoft, *Service health and continuity.* [Online]. Available: https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity (accessed: Jul. 7 2020).
[68] Jason Roth, *Understanding Azure Limits and Increases | Azure-Blog und -Updates| Microsoft Azure.* [Online]. Available: https://azure.microsoft.com/de-de/blog/azure-limits-quotas-increase-requests/ (accessed: Jun. 21 2020).
[69] ShaneBala-keyvault, *Vorgehensweise bei einer Azure-Dienstunterbrechung mit Auswirkungen auf Azure Key Vault – Azure Key Vault.* [Online]. Available: https://docs.microsoft.com/de-de/azure/key-vault/general/disaster-recovery-guidance (accessed: Jul. 12 2020).
[70] Paul Bischoff, *250 million Microsoft customer service & support records exposed.* [Online]. Available: https://www.comparitech.com/blog/information-security/microsoft-customer-service-data-leak/ (accessed: May 29 2020).
[71] *Azure Misconfiguration Exposes 250 Million Microsoft Customer Accounts -- Redmond Channel Partner.* [Online]. Available: https://rcpmag.com/articles/2020/01/22/azure-misconfiguration-exposes-250-million.aspx (accessed: May 13 2020).
[72] R. Guida, *PhishPoint: New SharePoint Phishing Scam Affects an Estimated 10% of Office 365 Users.* [Online]. Available: https://www.avanan.com/blog/sharepoint-phishing-scam (accessed: Jun. 29 2020).

Literaturverzeichnis

[73] *Common Vulnerability Scoring System SIG.* [Online]. Available: https://www.first.org/cvss/ (accessed: Jul. 2 2020).
[74] Oli Neumann, *HAW-Cloud - HAW Cloud - Confluence.* [Online]. Available: https://dokumentation.itsc.haw-hamburg.de/display/HCS/HAW-Cloud (accessed: Jul. 9 2020).
[75] HAW Hamburg, *HAW-Cloud.* [Online]. Available: https://www.haw-hamburg.de/online-services/cloud-der-haw/ (accessed: Jul. 9 2020).
[76] ownCloud, "ownCloud's Data Encryption Model,"
[77] *Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen.* [Online]. Available: https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen (accessed: Jul. 12 2020).

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den _____ _[redacted]