universität wien

BACHELORARBEIT / BACHELOR'S THESIS

Titel der Bachelorarbeit / Title of the Bachelor's Thesis

„Strategien und Werkzeuge zur Sicherung von Cloud-Diensten: Entwicklung eines umfassenden Sicherheits-Wikis“

verfasst von / submitted by

Florian Chocholka

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Bachelor of Science (BSc)

Wien, 2024 / Vienna, 2024

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 033526
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Bachelorstudium Wirtschaftsinformatik
Betreut von / Supervisor:	Univ.-Prof. Dipl.-Ing. Dr. Dr. Gerald Quirchmayr

Contents

1 Abstract

Die vorliegende Bachelorarbeit untersucht Strategien und Werkzeuge zur Sicherung von Cloud-Diensten, insbesondere durch die Entwicklung eines umfassenden Cloud Security Wikis und eines interaktiven Tools. Ziel ist es, die Sicherheitsrisiken verschiedener Cloud-Dienste zu identifizieren und effektive Maßnahmen zu deren Bewältigung zu entwickeln. Um die Forschungsziele zu erreichen, wurden zunächst die verschiedenen Cloud-Dienstmodelle (IaaS, PaaS, SaaS) und deren spezifische Sicherheitsrisiken analysiert. Zudem wurden unterschiedliche Deployment-Modelle (Public Cloud, Private Cloud, Hybrid Cloud, Multi-Cloud) untersucht. Ein Schwerpunkt lag auf der Analyse von Service Level Agreements (SLAs) und der Auswahl von Cloud-Anbietern nach den Richtlinien des National Cyber Security Centre (NCSC). Basierend auf diesen Untersuchungen wurde ein Cloud Security Wiki entwickelt, ergänzt durch ein interaktives Tool, das die 14 Sicherheitsprinzipien des NCSC vermittelt. Die Arbeit resultierte in der Entwicklung eines Cloud Security Wikis und eines interaktiven Tools. Das Wiki dient als umfassende Ressource für Entscheidungsträger und bietet detaillierte Informationen zu Cloud-Sicherheitsstrategien. Das interaktive Tool erleichtert das Erlernen und Anwenden der NCSC-Sicherheitsprinzipien durch eine benutzerfreundliche, interaktive Oberfläche. Die Ergebnisse zeigen, dass das entwickelte Wiki und das interaktive Tool eine effektive Unterstützung bei der Implementierung und dem Verständnis von Cloud-Sicherheitsstrategien bieten. Diese Werkzeuge tragen dazu bei, Sicherheitslücken zu schließen und die Sicherheit in der Cloud zu verbessern. Durch regelmäßige Aktualisierungen und Benutzerfreundlichkeit bieten sie eine zuverlässige Grundlage für die sichere Nutzung von Cloud-Diensten. Die Qualität und Nützlichkeit des Cloud Security Wikis und des interaktiven Tools wurden durch eine Evaluierung mittels eines Onlinefragebogens sichergestellt. Die Befragung ergab, dass die Nutzer das Wiki und das Tool als benutzerfreundlich, informativ und gut strukturiert bewerteten. Die positiven Rückmeldungen bestätigten, dass die Zielsetzung der Arbeit erreicht wurde und die entwickelten Werkzeuge eine wertvolle Ressource zur Verbesserung der Cloud-Sicherheit darstellen.

2 Introduction

In der heutigen digitalen Welt, die von rasantem technologischen Fortschritt und zunehmender Vernetzung geprägt ist, spielt die Cloud-Technologie eine zentrale Rolle. Die Cloud ermöglicht es Unternehmen und Einzelpersonen Daten und Anwendungen über das Internet bereitzustellen und zu nutzen. Hierdurch wird Flexibilität, Skalierbarkeit und Effizient erreicht. Der Umfang reicht vom speichern von Daten bis hin zu Nutzung von bereits entwickelten Anwendungen. Der Große Vorteil hierbei ist, das keine lokalen Hardware-Ressourcen mehr benötigt werden. [MS19]
Diese Vorteile haben dazu geführt, dass Cloud-Technologie heutzutage in fast allen Branchen vertreten ist. Unternehmen wie Amazon mit ihrer Plattform Amazon Web Services (AWS), Microsoft mit Microsoft Azure und Google mit der Google Cloud Platform dominieren den Markt und treiben Innovationen voran, die die Nutzungsmöglichkeiten der Cloud stetig erweitern. Alleine im vierten Quartal des Jahres 2023 belief sich der Marktanteil von AWS auf 31 Prozent, von Microsoft Azure auf 26 Prozent und von Google Cloud auf 10 Prozent. Diese Prozentsätze beziehen sich auf die Bereitstellung von IaaS- und PaaS-Diensten. [Sta23]
Trotz der zahlreichen Vorteile bringt die Abhängigkeit von Cloud-Diensten auch bedeutende Herausforderungen und Sicherheitsrisiken mit sich. Datenschutzverletzungen, unautorisierte Datenzugriffe, Dienstausfälle und Compliance-Verstöße stellen nur einen Bruchteil der Schwierigkeiten dar, mit denen Organisationen und Einzelpersonen konfrontiert sind. Die Sicherheit in der Cloud ist sehr komplex und umfasst nicht nur den Schutz gespeicherter Daten, sondern auch die Sicherheit der Übertragungswege, der Zugriffskontrollen und der Anwendungen, die in der Cloud ausgeführt werden. Aufgrund der ständigen Weiterentwicklung in der Bedrohungslandschaft ist es von Bedeutung, dass ein tiefes Verständnis für die spezifischen Sicherheitsrisiken entwickeln wird, die mit der Nutzung und Entwicklung von Cloud-Diensten verbunden sind. Aus diesem Grund müssen aktuelle und wirksame Strategien zur Minimierung von Sicherheitsrisiken implementiert werden. [Cen24b, MYD21]
Um eine sichere Cloud-Umgebung zu gewährleisten, müssen Unternehmen eine mehrschichtige Sicherheitsstrategie verfolgen, die sowohl technische als auch organisatorische Maßnahmen umfasst. Zu den technischen Maßnahmen gehören die Verschlüsselung von Daten, sowohl in Ruhe als auch während der Übertragung, die Implementierung von starken Authentifizierungs- und Autorisierungsverfahren sowie die Nutzung von Sicherheitsdiensten, die von Cloud-Anbietern angeboten werden. [Cen24b]
Darüber hinaus ist die Einhaltung von branchenspezifischen und regionalen Datenschutz- und Sicherheitsvorschriften wie der Europäischen Datenschutz-Grundverordnung (DSGVO) oder dem California Consumer Privacy Act (CCPA) unerlässlich für Unternehmen, die Cloud-Dienste nutzen. Die Vorschriften fordern von Organistationen angemessene Maßnah-

men zum Schutz der Privatsphäre und Sicherheit der Daten zu ergreifen um sicherzustellen das die Rechte der betroffenen Personen aufrechterhalten bleiben. [Kom24, oC24]
Daraus folgt das die Sicherheit in der Cloud ein fortlaufender Prozess ist, der eine kontinuierliche Anpassung an neue Sicherheitsbedrohungen erfordert. Nur durch eine umfassende Strategie, die technische, organisatorische und rechtliche Aspekte integriert, können Unternehmen die Vorteile der Cloud-Technologie voll ausschöpfen, ohne dabei Kompromisse bei der Sicherheit und dem Datenschutz einzugehen.
Um die Zielsetzung dieser Arbeit zu erreichen, wird zunächst das Thema Cloud-Sicherheit eingegrenzt. Es werden die verschiedenen Arten von Cloud-Diensten (IaaS, PaaS, SaaS) und die damit verbundenen Sicherheitsrisiken beleuchtet. Anschließend werden die aktuellen Strategien und Technologien zur Bewältigung dieser Sicherheitsrisiken diskutiert. In diesem Kontext zielt die vorliegende Arbeit darauf ab, ein umfassendes Cloud Security Wiki zu entwickeln. Dieses wird eine Sammlung von Richtlinien, Werkzeugen und Empfehlungen beinhalten, die speziell darauf abzielen, Entscheidungsträger in Organisationen zu unterstützen. Es soll verständlich aufzeigen, auf welche Sicherheitsaspekte sowohl intern in der eigenen Organisation als auch bei der Auswahl und Nutzung von Cloud-Anbietern geachtet werden soll. Zusätzlich wird ein interaktives Tool entwickelt, das es Entscheidungsträgern erleichtert, die Sicherheitsanforderungen in der Cloud zu verstehen und anzuwenden.
Besonders wird dabei auf die Einbeziehung diverser Sicherheitsstandards und -prinzipien vom National Cyber Security Centre (NCSC) [Cen24b] geachtet. Somit wird gewährleistet, dass das Cloud Security Wiki auf anerkannten und aktuellen Sicherheitspraktien basiert und verstärkt dadurch die Nützlichkeit und Relevanz in der Praxis.
Die Struktur dieser Arbeit ist wie folgt gegliedert: Zunächst werden die verschiedenen Arten von Cloud-Diensten (IaaS, PaaS, SaaS) vertieft und die spezifischen Sicherheitsrisiken diskutiert, die mit jedem Dienst verbunden sind. Weiterhin wird auf die Deployment-Modelle in der Cloud eingegangen und deren jeweilige Vor- und Nachteile beleuchtet. Es werden die verschiedenen Aspekte der Service Level Agreements im Cloud Computing detailliert betrachtet und die Auswahl sowie Überprüfung von Cloud-Anbietern nach den Richtlinien des NCSC [Cen24b] erläutert. Abschließend wird ein Leitfaden zur sicheren Nutzung von SaaS-Anwendungen vorgestellt. Danach wird das entwickelte Cloud Security Wiki vorgestellt und zusätzlich ein interaktives Tool präsentiert, das auf den 14 Sicherheitsprinzipien des NCSC [Cen24b] basiert und Entscheidungsträgern sowie Einzelpersonen interaktiv das Erlernen und Anwenden der Sicherheitsprinzipien erleichtert. Es folgt die Evaluierung der beiden Praxisteile, wobei Methodik und Ergebnisse im Fokus stehen. Abschließend werden die Erkenntnisse zusammengefasst und ein Ausblick auf zukünftige Entwicklungen im Bereich der Cloud-Sicherheit gegeben.

3 Motivation

Die vorliegende Arbeit adressiert festgestellte Informationslücken in bestehenden Cloud Security Wikis, die sich hauptsächlich auf die technische Konfiguration von Cloud-Diensten konzentrieren. Spezifische Ressourcen wie die Cloud Security Wikis von NotSoSecure [Not21] und WithSecure [Wit23] bieten zwar wertvolle Anleitungen, vernachlässigen jedoch die Behandlung spezifischer Sicherheitsbedrohungen und die Integration von Prinzipien und Richtlinien führender Sicherheitsorganisationen wie dem National Cyber Security Centre (NCSC).[Cen24b]
Ziel dieser Arbeit ist die Entwicklung eines Cloud Security Wiki, die diese Informationslücken schließt. Durch die Integration spezifischer Informationen über Bedrohungen, sowie die Prinzipien und Richtlinien von NCSC [Cen24b], zielt das Projekt darauf ab, ein breiteres Spektrum an Cloud Sicherheitsaspekten abzudecken. Es soll eine ganzheitliche Ressource bieten, die sowohl technische Implementierungsleitfäden umfasst, als auch tiefgreifendes Wissen über die Sicherheitslandschaft der Cloud-Technologie vermittelt.
Zusätzlich zum Cloud Security Wiki wird ein interaktives Tool entwickelt, das Einzelpersonen und Unternehmen das Erlernen und Anwenden der 14 Cloud Security Prinzipien der NCSC [Cen24b] erleichtern soll.
Eine weitere Notwendigkeit für eine solche umfassende Ressource ergibt sich aus der wachsenden Abhängigkeit von Cloud-Diensten in verschiedenen Organisationen. Besonders in Europa zeigt sich diese Abhängigkeit deutlich: In Schweden nutzten im Jahr 2021 etwa 75,4 Prozent der Unternehmen mit mehr als zehn Mitarbeitern kostenpflichtige Cloud-Computing-Dienste, was auf eine hohe Akzeptanz und Integration dieser Technologie hinweist. [Sta21].
Ein verbessertes Verständnis der Cloud-Sicherheitsrisiken und -strategien ist entscheidend, um effektive Schutzmaßnahmen implementieren zu können. Das entwickelte Cloud Security Wiki wird sowohl aktuelle als auch zukunftsorientierte Sicherheitsstrategien beleuchten und spezifische Empfehlungen detailliert behandeln. Es soll durch leichte Wartbarkeit und einfache Benutzbarkeit schnell und effizient auf Änderungen in der Bedrohungslandschaft aktualisiert werden können. Ein Beispiel für die Dringlichkeit der Aktualisierung solcher Ressourcen ist das Wiki von NotSoSecure [Not21], das zuletzt im Jahr 2021 aktualisiert wurde. Diese Verzögerung bei der Aktualisierung kann schnell zu Informationslücken führen, besonders in einem schnelllebigen Bereich wie der Cloud-Sicherheit.
Zusammenfassend soll das Cloud Security Wiki und Tool Organisationen aller Größen und Branchen helfen, ihre Cloud-Nutzung sicher und verantwortungsvoll zu gestalten. Sie zielen darauf ab, ein praktisches Verständnis für Sicherheitsrisiken und Schutzmaßnahmen zu fördern und dient als Brücke zwischen Theorie und Praxis, um Kompetenzen zu stärken und Entscheidungen zu erleichtern.

4 Hauptteil

4.1 Einführung in die Cloud-Dienstmodelle

In diesem Abschnitt werden die drei Hauptmodelle des Cloud-Computings vorgestellt: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Jedes dieser Modelle bietet spezifische Vorteile und Herausforderungen, die im Detail betrachtet werden, um ein umfassendes Verständnis für ihre Anwendung zu vermitteln. Abbildung 4.1 verdeutlicht, in welchem Umfang sich die drei Modelle in der Verwaltung unterscheiden.

4.1.1 IaaS (Infrastructure as a Service)

Infrastructure as a Service (IaaS) beschreibt ein Modell, das Netzwerkkomponenten, Speicherkapazitäten und Rechenleistung über das Internet an Kunden bereitstellt. Der große Vorteil bei der Verwendung von IaaS ist, dass Unternehmen ohne hohe Vorabinvestitionen auf Geschäftsanforderungen reagieren können. Ebenfalls entfällt die Wartung, die bei einer eigenen physischen Infrastruktur anfallen würde. IaaS liefert somit die physischen und virtuellen Ressourcen, die als Basis für weitere Cloud-Services dienen. Die zugrunde liegende Architektur besteht aus großen Rechenzentren, die rund um den Globus verteilt sind. Diese Zentren beinhalten die benötigte Hardware, auf die Nutzer über virtuelle Maschinen zugreifen können. Der große Unterschied von IaaS zu den anderen beiden Modellen PaaS (Platform as a Service) und SaaS (Software as a Service) liegt in der Abstraktion der Kontrolle. Während PaaS und SaaS höhere Ebenen der Abstraktion und des Managements von Anwendungsstacks bieten, legt IaaS den Schwerpunkt auf die Bereitstellung der Grundinfrastruktur. Zusätzlich bieten die meisten IaaS-Angebote die Möglichkeit, eine virtuelle Private Cloud (VPC) zu nutzen. Diese ermöglicht die Erstellung eines privaten Netzwerks innerhalb einer öffentlichen Cloud-Umgebung. Dies bietet Sicherheit und Isolation von anderen Diensten und Benutzern und fördert somit die Compliance-Anforderungen, die für die Verwaltung hochsensibler Daten meistens erforderlich sind. Die Preisbestimmung von IaaS erfolgt normalerweise nutzungsbasiert. Das bedeutet, dass der Kunde nur jene Ressourcen bezahlt, die er auch tatsächlich nutzt. Viele Anbieter bieten auch Rabatte für längerfristige Reservierungen oder größere Ressourcenverpflichtungen an. IaaS bietet eine Vielzahl an Vorteilen. Zum einen fallen keine Kapitalinvestitionen für teure physische Infrastruktur an. Dies ist besonders attraktiv für Start-up-Unternehmen, die nicht über großes Kapital verfügen. Ebenfalls steigert die Auslagerung der Infrastruktur die Flexibilität und Skalierbarkeit, was das Anpassen an neue Geschäftsanforderungen enorm vereinfacht. IaaS bietet zudem

verbesserte Disaster-Recovery-Fähigkeiten und ermöglicht es Unternehmen, schnell auf veränderte Anforderungen zu reagieren. [IBM24b]

4.1.2 PaaS (Platform as a Service)

Platform-as-a-Service (PaaS) ist ein Cloud-Computing-Modell, das Hardware, Software und die Infrastruktur bereitstellt. Kunden können hiermit die Entwicklung, Ausführung und Verwaltung der Anwendungen auslagern und über das Internet darauf zugreifen, ohne hohe Komplexität oder Kosten zu verursachen. Die Architektur von PaaS zeichnet sich wie bei IaaS durch Rechenzentren aus, in denen alle benötigten Mittel zum Entwickeln, Testen und Warten bereitgestellt werden, darunter Betriebssysteme, Datenbanken und Entwickler-Tools. Diese werden mithilfe einer Benutzeroberfläche (GUI) integriert. Platform-as-a-Service (PaaS) bietet eine Reihe von Vorteilen. Darunter eine verkürzte Entwicklungszeit, da keine Zeit mehr für Installationen oder Wartung von Hardware und Software investiert werden muss. Dies resultiert in einer beschleunigten Projektumsetzung und effizienteren Nutzung von Ressourcen jeglicher Art. Zudem bieten PaaS-Anwendungen eine breite Palette an Anwendungsstacks, die von den Kunden während der Entwicklung genutzt werden können. Dies ist kostengünstiger, da Unternehmen diese nicht mehr selbst bereitstellen oder warten müssen. Diese Kosteneffizienz zieht besonders Start-ups und kleine Unternehmen an, die möglicherweise nicht das Kapital besitzen, um dies selbst umzusetzen. Da die Anwendungsstacks so vielfältig sind, fördert es das Experimentieren mit neuen Technologien, die möglicherweise zu effizienteren und besseren Lösungen führen. Die Flexibilität, die PaaS bietet, indem es Entwicklungsteams ermöglicht, von überall aus auf die benötigten Tools zuzugreifen, unterstützt die Nutzung global verteilter Teams und fördert eine kollaborative Arbeitsumgebung. IaaS und PaaS sind miteinander verbunden, da PaaS IaaS einbindet. PaaS erweitert das IaaS-Modell, um den Kunden das selbstständige Entwickeln zu ermöglichen. IaaS bietet hierzu die notwendige Infrastruktur. Im Vergleich zu SaaS-Anwendungen ermöglicht PaaS den Nutzern, ihre eigenen Anwendungen zu entwickeln und somit nicht an SaaS gebunden zu sein. PaaS unterstützt eine Vielzahl von IT-Projekten wie API-Entwicklung, Internet der Dinge (IoT), agile Entwicklung und DevOps, Cloud-Migration und cloudnative Entwicklung sowie Hybrid-Cloud-Strategien. PaaS bietet eine integrierte, sofort einsatzbereite Plattform, die Unternehmen von der Infrastrukturverwaltung entlastet. [IBM24c]

4.1.3 SaaS (Software as a Service)

Software-as-a-Service (SaaS) ist ein dominierendes Modell in der modernen Cloud-basierten Softwarebereitstellung. Es ermöglicht Unternehmen und Einzelpersonen, Anwendungssoftware über das Internet zu nutzen, wobei der Dienstanbieter für den Betrieb, die Wartung und das Management der Software sowie der Infrastruktur verantwortlich ist. Kunden benötigen lediglich eine Internetverbindung und können über Webbrowser, mobile Apps oder Thin Clients auf die Services zugreifen. SaaS nutzt die Vorteile der Cloud-Computing-Infrastruktur, um eine skalierbare und effiziente Softwarenutzung zu ermöglichen. Da das Management und die Wartung vom Cloud-Anbieter übernommen werden, fällt somit min-

imaler Aufwand für den Kunden an. Hierbei schließt der Kunde meistens ein Abonnement ab, die sich im Nutzungsumfang voneinander unterscheiden. Dies reicht von kostenlosen Tarifen bis hin zu Premium-Tarifen, die eine reiche Anzahl an Funktionen versprechen. SaaS ist nur eine Ebene des Cloud-Service-Modells, das auch Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) umfasst. Im Vergleich zu PaaS und IaaS bietet SaaS vollständige Anwendungen und besitzt eine schnelle Einsatzbereitschaft. Der Kunde kann nach erfolgreichem Abschluss des gewünschten Abonnements die Software umgehend nutzen. Somit fallen weder Entwicklungskosten noch Wartungskosten, wie bei traditioneller lokaler Software, an. Wie auch bei IaaS und PaaS fallen hier ebenfalls keine hohen Anfangsinvestitionen an. Zudem entledigt sich der Nutzer der Verantwortung für Wartungsarbeiten, da der SaaS-Anbieter alle Updates und technischen Probleme übernimmt. Trotz seiner Vorteile kann SaaS auch Herausforderungen mit sich bringen, wie etwa die potenzielle Schwierigkeit beim Wechsel zwischen verschiedenen SaaS-Anbietern oder die Risiken im Zusammenhang mit der Datensicherheit. Unternehmen müssen die Service-Level-Agreements (SLAs) sorgfältig prüfen und sicherstellen, dass ihre Daten geschützt und die Dienste zuverlässig sind. Insgesamt stellt SaaS eine kosteneffiziente Lösung dar, um schnell und einfach auf Unternehmensoftware zuzugreifen. Dies ist für Unternehmen besonders interessant, die Wert auf schnelle Implementierung und geringe Vorlaufkosten legen. [IBM24a]

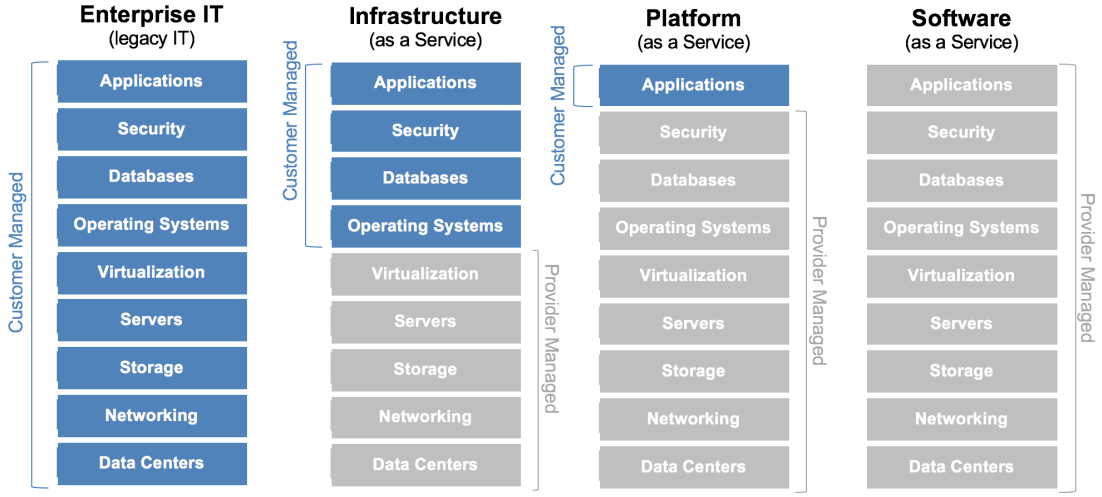


Figure 4.1: Darstellung der Unterschiede in der Verwaltung von IT-Komponenten bei verschiedenen Cloud Modellen.

[Cho18]

4.2 Deployment-Modelle in der Cloud

In der Cloud-Technologie gibt es verschiedene Deployment-Modelle, die jeweils spezifische Merkmale, Vorteile und Herausforderungen aufweisen. Diese Modelle sind entscheidend für die Art und Weise, wie Daten gespeichert, verarbeitet und verwaltet werden. In diesem Unterkapitel werden die vier Haupttypen von Cloud-Deployment-Modellen diskutiert: Public Cloud, Private Cloud, Hybrid Cloud und Multi-Cloud. Jedes dieser Modelle bietet unterschiedliche Sicherheits-, Compliance- und Betriebsmerkmale, die für Unternehmen von kritischer Bedeutung sind. [Cen24a]

4.2.1 Public Cloud

Die Public Cloud ist das bekannteste Modell des Cloud-Computings und über das Internet öffentlich zugänglich. Jeder, der bereit ist, die Servicegebühren zu bezahlen, kann diesen Dienst nutzen und von überall im Internet darauf zugreifen. Sie bietet eine flexible und kosteneffiziente Lösung für Unternehmen, die schnell skalieren möchten, ohne in eigene Hardware investieren zu müssen. Public Clouds sind in der Regel multinational vertreten, mit Datenzentren auf der ganzen Welt. Dabei kann der Kunde die gewünschte Region auswählen, in der seine Daten gespeichert und verwaltet werden sollen. Diese Flexibilität kann jedoch Herausforderungen in Bezug auf Verfügbarkeit und Redundanz mit sich bringen. Die Sicherheitsmaßnahmen in Public Clouds sind hochentwickelt und orientieren sich am OFFICIAL-Bedrohungsmodell [GOV24], das grundlegende Schutzmechanismen gegen gängige Bedrohungen bietet. Für eine höhere Sicherheitsstufe von Daten sind zusätzliche Maßnahmen erforderlich. Eine interessante Erweiterung der Public Cloud ist Edge Computing. Hierbei wird ein Dienst in lokale Rechenzentren ausgelagert, um die Bandbreitenanforderungen und Latenzzeiten deutlich zu verringern. Besonders nützlich ist diese Technologie für IoT-Geräte (Internet of Things) wie Smartwatches oder auch mobile Geräte, die eine sofortige Datenverarbeitung erfordern. [Cen24a]

4.2.2 Private Cloud

Eine Private Cloud wird exklusiv für eine einzige Organisation auf einem privaten Netzwerk eingesetzt. Dieses Modell bietet ein hohes Maß an Kontrolle und Sicherheit und ist somit ideal für Unternehmen, die strengen Datenschutzregelungen unterliegen oder sehr vertrauliche Daten verarbeiten und speichern. Da die Infrastruktur der Private Cloud nur auf ein Unternehmen ausgerichtet ist, können eigene Sicherheits- und Compliance-Anforderungen leichter implementiert und verwaltet werden. Dies umfasst auch die Fähigkeit, den physischen Standort der Daten zu kontrollieren, was in einer Public Cloud nicht immer möglich ist. Eine Erweiterung der Private Cloud ist die Community Cloud. Diese ermöglicht das Zusammenfassen von Organisationen innerhalb einer Cloud, die gleiche oder ähnliche Geschäftsanforderungen besitzen. Beispielsweise ermöglicht es Partnerorganisationen, Ressourcen effizient und kostengünstig zu teilen, während gleichzeitig ein hoher Stellenwert auf den Datenschutz gelegt wird. [Cen24a]

4.2.3 Hybrid Cloud

Eine Hybrid Cloud ermöglicht es, lokale Dienste von Unternehmen leicht mit Cloud-Diensten zu kombinieren und dabei eine nahtlose Interaktion zu erreichen. Spezifischer gesagt, erweitern sie bereits intern bestehende Infrastrukturen mit Cloud-Funktionen. Unternehmen müssen jedoch sicherstellen, dass während der Kommunikation von Daten zwischen dem lokalen Dienst und dem Cloud-Dienst der Datenschutz gewährleistet bleibt. Dabei spielt auch die Internetverbindung eine entscheidende Rolle, da die Nutzung einer Hybrid Cloud die Bandbreitennutzung enorm erhöht. Da lokale Dienste bei diesem Modell stark mit Cloud-Diensten gekoppelt sind, muss zudem ein rollenbasiertes Zugriffssteuerungsmodell (RBAC) implementiert werden, um sicherzustellen, dass ein Sicherheitsvorfall in einem Dienst keinen anderen Dienst beeinträchtigen oder gar übergreifen kann. [Cen24a]

4.2.4 Multi-Cloud

Bei einer Multi-Cloud-Strategie werden Dienste von mehreren Cloud-Anbietern genutzt, um die spezifischen Bedürfnisse verschiedener Projekte zu erfüllen. Dieses Modell bietet eine hohe Flexibilität und ermöglicht es Unternehmen, das Beste aus verschiedenen Cloud-Angeboten zu nutzen, ohne sich auf einen einzelnen Anbieter verlassen zu müssen. Jedoch zieht dies den Nachteil mit sich, dass das Risiko und die Komplexität erhöht werden, wenn mehrere Cloud-Anbieter innerhalb von Projekten verwendet werden. Zudem erhöht sich die Angriffsfläche. Wenn eine Multi-Cloud verwendet wird, müssen einige Punkte beachtet werden, um die Sicherheit und Betriebskontinuität aufrechtzuerhalten. Wie auch bei Hybrid-Clouds müssen die Datenflüsse zwischen den Diensten genau überwacht und analysiert werden. Die Schnittstellen zwischen den verwendeten Cloud-Services sollten als externe Schnittstellen behandelt und entsprechend abgesichert werden. Zudem müssen die Auswirkungen vorübergehender Ausfälle der Verbindungen oder Dienste berücksichtigt werden und wie diese möglicherweise andere Dienste beeinflussen könnten. [Cen24a]

4.3 Service Level Agreements im Cloud Computing

Service Level Agreements (SLAs) sind formelle Verträge, die zwischen Cloud-Service-Anbietern und ihren Kunden geschlossen werden. Diese Verträge enthalten und definieren die erwartete Servicequalität und legen Maßnahmen fest, die im Falle einer Abweichung von Metriken vom Anbieter zu ergreifen sind. Für Entscheidungsträger sind SLAs von großer Wichtigkeit, da sie Klarheit und Sicherheit bieten und dabei helfen, die Anforderungen des Unternehmens an den Serviceanbieter durchzusetzen. SLAs können je nach Anwendungsbereich in kundenbasierte, servicebasierte und mehrstufige SLAs unterteilt werden. Kundenbasierte SLAs betreffen einzelne Kunden und die vom Kunden genutzten Services des Anbieters. Servicebasierte SLAs werden auf standardisierte Services angewendet, die für mehrere Kunden gleich angeboten werden, sodass hier dieselben Metriken für alle Kunden vorhanden sind. Mehrstufige SLAs kombinieren verschiedene Service-Levels in einem einzigen Vertrag, was für Anbieter, die mehrere Dienste in unterschiedlichen Konfigurationen anbieten, nützlich ist. Im Allgemeinen umfasst ein SLA eine Übersicht

aller zwischen dem Kunden und Anbieter geschlossenen Vereinbarungen. Dazu gehören beispielsweise das Start- und Enddatum, die beteiligten Parteien und die genutzten Services, die vom Anbieter für den Kunden bereitgestellt werden. Die Beschreibung des Services muss genau festlegen, welche Leistung erbracht wird. Dazu gehören die Service-Level-Ziele (SLOs), die Leistungskriterien wie Reaktionszeiten und Verfügbarkeit des Dienstes umfassen. Um die Durchsetzung der SLAs zu erreichen, müssen Entscheidungsträger regelmäßige Leistungsberichte erstellen und analysieren. Diese sollten vor allem Metriken wie Verfügbarkeit und Reaktionszeiten enthalten. Es empfiehlt sich, Systeme zur regelmäßigen Überprüfung dieser Metriken zu implementieren, um sicherzustellen, dass der ausgewählte Anbieter die im SLA festgelegten Standards einhält. Für Nichteinhaltung oder Abweichung der Standards sollten im SLA klare Richtlinien bezüglich Vertragsstrafen oder Kompensationsmöglichkeiten vorhanden sein. Diese können finanzielle Strafen, Gutschriften oder andere Formen der Wiedergutmachung umfassen, die sicherstellen, dass der Anbieter für die Nichteinhaltung der Vereinbarung verantwortlich gemacht wird. Ausschlüsse, Sicherheitsstandards und Notfallwiederherstellungspläne sind ebenfalls kritische Bestandteile eines SLAs. Diese Abschnitte definieren mögliche Umstände, unter denen die SLAs nicht gelten, legen die vereinbarten Sicherheitsstandards fest und enthalten einen Notfallplan für den Fall eines kompletten Dienstausfalls. Schlussendlich minimieren Service Level Agreements (SLAs) Risiken im Cloud Computing beträchtlich und bieten rechtliche Sicherheit für die beteiligten Parteien. Ebenso setzen SLAs präzise Erwartungen an die Servicequalität fest. Die genaue Kenntnis von SLAs ist für Entscheidungsträger von grundlegender Wichtigkeit. Sie bildet die Basis für eine fundierte Auswahl und Bewertung von Cloud-Dienstleistern. Durch das Verständnis von SLAs wird sichergestellt, dass ausgewählte Cloud-Services die geschäftlichen Anforderungen erfüllen und gleichzeitig die Einhaltung von Sicherheits- und Compliance-Standards gewährleisten. [AWS24]

4.4 Auswahl und Überprüfung von Cloud-Anbietern nach NCSC-Richtlinien

Die Auswahl eines Cloud-Anbieters ist eine kritische Entscheidung, die die Sicherheit und die operative Effizienz von Datenverarbeitungssystemen in Organisationen maßgeblich beeinflusst. Dieses Kapitel erörtert die Methodiken des National Cyber Security Centre (NCSC), die Organisationen bei der Bewertung potenzieller Cloud-Dienste unterstützen. Die Kernaspekte dieser Bewertung umfassen das Aufbauen von Vertrauen in die Fähigkeit des Anbieters, verantwortungsvoll mit sensiblen Daten umzugehen, und die Notwendigkeit, dieses Vertrauen durch unabhängige Überprüfungen zu validieren. Besondere Aufmerksamkeit wird dem prinzipienbasierten Ansatz gewidmet, der für Organisationen entwickelt wurde, die mit sensiblen oder umfangreichen Datenmengen arbeiten. Dieser Ansatz hilft dabei, die Eignung eines Cloud-Dienstes hinsichtlich der Sicherheitsanforderungen zu bewerten und ist besonders relevant für Entscheidungsträger, die die Integrität und Sicherheit ihrer Daten gewährleisten müssen. Der prinzipienbasierte Ansatz des NCSC umfasst 14 Sicherheitsprinzipien, die eine umfassende Beurteilung der Konzeption, Implementierung und des Betriebs eines Cloud-Dienstes ermöglichen. Diese Prinzipien

sind insbesondere für größere Organisationen relevant, können jedoch von jedem, der mit sensiblen Datentypen arbeitet, angewandt werden. [Cen24b]

- Prinzip 1: Schutz von Daten während der Übertragung
- Prinzip 2: Schutz und Widerstandsfähigkeit von Vermögenswerten
- Prinzip 3: Trennung zwischen Kunden
- Prinzip 4: Governance-Rahmenwerk
- Prinzip 5: Betriebssicherheit
- Prinzip 6: Personalsicherheit
- Prinzip 7: Sichere Entwicklung
- Prinzip 8: Sicherheit der Lieferkette
- Prinzip 9: Sichere Benutzerverwaltung
- Prinzip 10: Identität und Authentifizierung
- Prinzip 11: Schutz externer Schnittstellen
- Prinzip 12: Sichere Dienstverwaltung
- Prinzip 13: Auditinformationen und Alarmierung für Kunden
- Prinzip 14: Sichere Nutzung des Dienstes

Im folgenden Abschnitt werden die oben angeführten Prinzipien der NCSC Cloud-Sicherheitsrichtlinien detailliert untersucht. Für jedes Prinzip werden Implementierungsansätze, Ziele und Erwartungen dargelegt. Diese tiefergehende Betrachtung soll ein umfassendes Verständnis der spezifischen Anforderungen und Maßnahmen ermöglichen, die für eine effektive Umsetzung dieser Prinzipien erforderlich sind. [Cen24b]

4.4.1 Prinzip 1: Schutz von Daten während der Übertragung

Das erste Prinzip beschreibt die Notwendigkeit, Benutzerdaten, die über Netzwerke versendet werden, gegen Abhörung und Manipulation zu schützen. Dies ist von grundlegender Bedeutung, da Daten während der Übertragung eine große Angriffsfläche bieten, besonders wenn sie über unsichere oder öffentliche Netzwerke gesendet werden. Es sollten Maßnahmen ergriffen werden, wie Verschlüsselung, die verhindert, dass potenzielle Angreifer die Daten lesen oder verändern können, Netzwerkschutz, um Angreifern das Abfangen von Daten zu verhindern, und Authentifizierung, um sicherzustellen, dass der Angreifer einen Dienst oder eine Person nicht imitieren kann. Für die Verschlüsselung müssen moderne und bewährte Algorithmen und Protokolle verwendet werden, wie TLS (Transport Layer Security) und IPSec. Ziel ist es, sowohl einen Schutz zwischen Endgeräten und dem

ausgewählten Dienst zu gewährleisten als auch die interne Kommunikation zwischen Komponenten zu schützen. Netzwerkschutz schützt Daten durch Maßnahmen, die verhindern, dass Angreifer Daten auf dem Übertragungsweg abfangen können. Dazu gehören die Nutzung von sicheren Netzwerkverbindungen, erreicht durch die Verwendung einer VPN, und die Überwachung des Netzwerkverkehrs auf Anomalien. Bei der Authentifizierung von Identitäten sind Technologien wie TLS-Zertifikate und VPNs zu bevorzugen. Cloud-Anbieter müssen ihre Sicherheitsmaßnahmen durch unabhängige Zertifizierungen wie die CSA STAR [All24], SOC2 [CIM24] und ISO 27017:2015 [ISO24] nachweisen können, da diese eine zusätzliche Versicherung bieten, dass die implementierten Sicherheitsmaßnahmen eines Cloud-Anbieters angemessen und fortlaufend geprüft werden, um somit die Sicherheit und Integrität von Kundendaten zu gewährleisten. Somit beschreibt dieses Prinzip drei wichtige Ziele die bei der Auswahl eines Cloud-Anbieters umgesetzt sein müssen: die Gewährleistung, dass Daten zwischen dem Endgerät des Benutzers und dem Dienst sicher übertragen werden, die Sicherstellung, dass Datenübertragungen zwischen den internen Komponenten des Dienstes geschützt sind, und dass die Kommunikation mit externen APIs ebenfalls überwacht und sicher ist. Beim Übertragen großer Datenmengen, insbesondere persönlicher Daten, sollten Organisationen auch Leitlinien zum Schutz großer Datenmengen beachten. Wenn Datenträger zur Datenübertragung verwendet werden, sollten diese gemäß dem Prinzip 2 zum Schutz von Daten in Ruhe gesichert sein. [Cen24b]

4.4.2 Prinzip 2: Schutz und Resilienz von Vermögenswerten

Das zweite Prinzip beschreibt die Wichtigkeit, sowohl physische als auch digitale Assets, die im Zusammenhang mit der Speicherung und Verarbeitung von Daten genutzt werden, ausreichend zu schützen. Dies schließt vor allem Anmeldeinformationen, Konfigurationsdateien, Metadaten und Protokolle mit ein, da diese in den meisten Fällen gerne übersehen werden. Die wichtigsten Aspekte, die dieses Prinzip behandelt, sind der physische Standort und die rechtliche Zuständigkeit, Sicherheitsmaßnahmen in den Rechenzentren und die Datenverschlüsselung. Beim physischen Standort sollten Entscheidungsträger darauf achten, wo die Daten der Organisation gespeichert werden und wer direkten Zugriff darauf hat. Maßnahmen, die hier angestrebt werden, umfassen die Aufforderung an den Cloud-Anbieter, eine Liste der Länder vorzulegen, die genau dokumentiert, wo die Daten gespeichert und verarbeitet werden. Es muss sichergestellt werden, welche rechtlichen Bestimmungen in den jeweiligen Ländern gelten, damit die Rahmenbedingungen des Landes, in dem sich die Daten befinden, auch mit den Sicherheits- und Datenschutzanforderungen der Organisation vereinbar sind. Ebenfalls muss überprüft werden, welche Rechte der Dienstanbieter bezüglich der Daten hat und unter welchen Umständen die Daten ohne Zustimmung zugänglich gemacht werden können. Bei den Sicherheitsmaßnahmen im Rechenzentrum muss gewährleistet sein, dass der Zugang von unautorisierten Personen strengstens untersagt ist, um mögliche Manipulation, Diebstahl oder auch eine Neukonfiguration von Systemen zu verhindern. Diese Informationen müssen vom Dienstanbieter offengelegt werden und bestenfalls durch Zertifizierungen, z.B. CSA CCM v3.0.1, ISAE 3402, abgesichert sein. Entscheidungsträger sollten Dienstanbieter bevorzugen, die diese genannten Punkte umgesetzt haben. Bei der Datenverschlüsselung

handelt es sich bei diesem Prinzip um den Schutz der Daten im Ruhezustand. Dies ist vor allem in Fällen wichtig, in denen sich Angreifer physischen Zugriff zur Infrastruktur verschaffen. Der Cloud-Anbieter sollte standardmäßig alle Benutzerdaten im Ruhezustand verschlüsseln. Als Technologie sollten hier Algorithmen wie AES-GCM und AES-XTS verwendet werden. [Cen24b]

4.4.3 Prinzip 3: Trennung zwischen den Benutzern

Das dritte Prinzip konzentriert sich auf Trennungstechniken, die implementiert werden müssen, um den Zugriff und Missbrauch von Daten durch verschiedene Nutzer innerhalb eines Cloud-Dienstes zu verhindern. Ein ausgewählter Cloud-Anbieter muss nachweisen, wie die Trennungen in den Bereichen Rechenressourcen (wie Containerisierung und IaaS), Speicher, Datenflüsse und Netzwerke umgesetzt sind. Diese Sicherheitsgrenzen sorgen dafür, dass der Zugriff auf die Daten kontrolliert erfolgt und der Dienst gegen internen bösartigen Code abgesichert ist. Es ist wichtig zu betonen, dass wenn ein Anbieter SaaS- oder PaaS-Dienste verwendet die auf anderen PaaS- oder IaaS-Diensten basieren, der Anbieter erläutern sollte, welche Trennungstechniken von den zugrundeliegenden Komponenten und der Infrastruktur geerbt werden. Die Granularität der Trennungstechniken hängt vom Cloud-Modell ab. Bei PaaS, wo Kunden benutzerdefinierten Code entwickeln und ausführen können, muss eine stärkere Separation vorhanden sein als bei einem SaaS-Modell. Entscheidungsträger sollten unbedingt nach externen Nachweisen wie Penetrationstests und Sicherheitsüberprüfungen Ausschau halten, um zu verstehen, ob die implementierten Sicherheitsgrenzen ausreichend für die Anforderungen sind. Bei der Rechenressourcen-Trennung sollte genau überlegt werden, welche Technologien zur Trennung verwendet werden. Hierbei sollte ein Anbieter gewählt werden, der eine hardwaregestützte Trennung anstrebt, bevorzugt durch Virtualisierung mit Hypervisor. Bei der Speichertrennung muss zuerst verstanden werden, wie genau auf die Daten zugegriffen wird und welche Technologien im Hintergrund eingesetzt werden, um den Zugriff zu verweigern. Standardmäßig muss der Zugriff auf Daten verweigert sein. Es soll nur mittels rollenbasierter Zugriffskontrollen jenen Zugriff gewährt werden, die dafür autorisiert sind. Zuletzt muss die Netzwerktrennung betrachtet werden. Hierbei sollten Anbieter gewählt werden, die SDN (softwaredefinierte Netzwerke) implementiert haben. Bei SDN ist darauf zu achten, dass an beiden Enden des Datenverkehrs Zugriffskontrollen existieren. [Cen24b]

4.4.4 Prinzip 4: Governance und Betriebsmanagement

Das Prinzip 4 beschreibt die Einbindung eines Governance-Rahmenwerks, um ein koordiniertes und übersichtliches Management des Cloud-Dienstes zu erreichen. Dieses muss prozedurale, personelle, physische und technische Kontrollen über den gesamten Lebenszyklus des Dienstes umfassen. Cloud-Anbieter müssen sicherstellen, dass die Kontrollen im Laufe des Betriebs ordnungsgemäß funktionieren. Das Rahmenwerk muss auf Änderungen im Dienst, technologische Änderungen und auf das Auftreten neuer Bedrohungen angepasst und evaluiert werden. Entscheidungsträger müssen sicherstellen, dass der ausgewählte Service ein Governance-Rahmenwerk besitzt und ob dieses für die beabsichtigte

Nutzung geeignet ist. Dabei sollten etablierte Governance-Praktiken beachtet werden, wie die Benennung einer verantwortlichen Führungskraft, z.B. dem „Chief Security Officer“, „Chief Information Officer“ oder „Chief Technical Officer“, der direkt für die Sicherheit des Cloud-Services zuständig ist. Zudem sollte der Cloud-Anbieter ein formal dokumentiertes Sicherheits-Governance- und Risikomanagementsystem vorlegen können, das wesentliche Bereiche der Informationssicherheit abdeckt, die für die Nutzung des Dienstes relevant sind. Wichtig zu beachten sind Verfahren zur Identifikation und Einhaltung gesetzlicher Anforderungen. Es wird empfohlen, auf Standards wie CSA CCM v3.0.1, SOC2 und ISO/IEC 27001 zurückzugreifen. Diese beinhalten Bewertungskriterien, um zu prüfen, wie gut das umgesetzte Governance-Rahmenwerk bestimmte Risiken abdeckt. Zu beachten ist hierbei, dass diese Standards in der Detaillierung und im Umfang variieren. Hier muss darauf geachtet werden, dass diese Standards die oben genannten Ziele eines Governance-Rahmenwerks abdecken. [Cen24b]

4.4.5 Prinzip 5: Betriebssicherheit

Das fünfte Prinzip betont die Notwendigkeit, dass der Betrieb und die Verwaltung von Cloud Services so zu erfolgen haben, dass potenzielle Angriffe behindert, erkannt oder gar verhindert werden. Eine effektive Betriebssicherheit sollte niemals komplex, bürokratisch oder kostenintensiv sein. Die wichtigsten Aspekte, auf die Entscheidungsträger bei der Betriebssicherheit achten müssen, sind:

- Schwachstellenmanagement
- Schutzüberwachung
- Vorfallmanagement
- Konfigurations- und Änderungsmanagement

[Cen24b]
Schwachstellenmanagement: Der Anbieter sollte Prozesse implementiert haben, die es erleichtern, Schwachstellen in allen zuständigen Komponenten des Dienstes zu identifizieren, zu priorisieren und zu mindern. Umgesetzt kann dies durch kontinuierliche Überwachung von Bedrohungen, aber auch durch die Bewertung neuer potenzieller Bedrohungen. Zertifizierungen wie ISO/IEC 30111:2019 und CSA CCM v3.0.1 können die Effektivität dieser Prozesse bestätigen. [Cen24b]
Schutzüberwachung: Es sollten Mechanismen vorhanden sein, um Angriffe, Missbrauch und Fehlfunktionen zu überwachen. Dabei sollen sowohl erfolglose als auch erfolgreiche Angriffe erkannt werden. Erreicht wird dies durch eine Kombination aus Datenerfassung und einer darauffolgenden Analyse, unterstützt durch Threat Intelligence. Somit können Kompromittierungen und eine unzulässige Nutzung innerhalb eines Cloud-Dienstes identifiziert werden. [Cen24b]
Vorfallmanagement: Dies beinhaltet vorgeplante Prozesse, die eine schnelle und effektive Reaktion auf Sicherheitsvorfälle ermöglichen. Cloud-Anbieter müssen Prozesse

vorlegen können, die sicherstellen, dass ein Kunde so schnell wie möglich über einen Sicherheitsvorfall informiert wird. Bei Vorfallmanagementprozessen sind Standards wie ISO/IEC 27035-1:2016 sehr wichtig, und der Anbieter sollte sicherstellen können, dass diese eingehalten werden. [Cen24b]
Konfigurations- und Änderungsmanagement: Cloud-Service Anbieter müssen die einzelnen Komponenten und deren Konfigurationen genauestens kennen, um auf Änderungen, die eine mögliche Sicherheitslücke öffnen, schnellstens reagieren zu können. Allgemein sollten alle Änderungen, die den Cloud-Dienst betreffen, auf potenzielle Sicherheitsrisiken bewertet und nachverfolgt werden. [Cen24b]

4.4.6 Prinzip 6: Personalsicherheit

Personalsicherheit beschreibt die Überwachung und Überprüfung von Personal des Cloud-Anbieters. Dabei muss der Anbieter Prozesse besitzen, um das Personal, das Zugriff auf Systemdaten und Nutzerdaten hat, einzuschränken. Es müssen technische Kontrollen erfolgen, um Handlungen des Personals zu erfassen. Dadurch soll das Risiko einer unbeabsichtigten oder böswilligen Kompromittierung durch das Servicepersonal verhindert werden. Dabei sind die nachfolgenden Aspekte besonders wichtig. [Cen24b]
Minimierung des Zugriffs: Entscheidungsträger sollten darauf achten, dass der Zugriff des Personals beim Cloud-Anbieter auf das notwendige Minimum beschränkt ist. Dies verhindert das Auftreten von Datenlecks oder anderen Sicherheitsvorfällen. [Cen24b]
Positive Sicherheitskultur: Der Cloud-Anbieter sollte eine positive Sicherheitskultur verfolgen. Es muss geprüft werden, wie dies der Anbieter erreicht. Gute Praktiken sind wiederkehrende Sicherheitsschulungen und angemessene Hintergrundprüfungen der Mitarbeiter. Besonders wichtig sind diese Praktiken für Personen, die hochprivilegierte Rollen im System besitzen. [Cen24b]
Technische Kontrollen: Eine Kontrolle zur Überwachung und Einschränkung von Aktionen der Mitarbeiter ist von äußerster Dringlichkeit. Es müssen Protokollierungen erfolgen über Mitarbeiter, die Zugriffe auf Kunden- und Systemdaten durchgeführt haben. Für die Umsetzung dieser technischen Maßnahmen wird eine rollenbasierte Zugriffskontrolle (RBAC) bevorzugt. Hiermit wird sichergestellt, dass Mitarbeiter nur auf das Nötigste Zugriff haben, das ihrer Rolle im System entspricht. Ebenfalls muss der Anbieter ein Meldesystem besitzen, das Kunden umgehend informiert, falls das Personal Aktionen durchführt, die die Daten des Benutzers betreffen. Bei Administratoren, die administrative Fähigkeiten besitzen, müssen diese zeitlich begrenzt werden und streng an Aufgaben oder Datenabfragen gebunden sein. [Cen24b]

4.4.7 Prinzip 7: Sichere Softwareentwicklung

Das siebte Prinzip der NCSC-Richtlinien unterstreicht die Bedeutung einer sicheren Gestaltung, Entwicklung und Implementierung von Cloud-Services, um Bedrohungen zu minimieren. Eine unsichere Softwareentwicklung erhöht die Gefahr von bösartigen Aktivitäten, Datenverlust oder einem kompletten Dienstausfall. Um dies zu verhindern, sollten Entscheidungsträger darauf achten, dass der Anbieter eine sichere Softwareentwicklung

verfolgt. Dazu zählen Entwicklungsschulungen, Code-Reviews und die Verwendung von zuverlässigen und sicheren Bibliotheken. Bei der Entwicklung selbst sollte eine Entwicklungspipeline integriert werden, um eine detaillierte Überwachung und Konsistenz der Software zu gewährleisten. Eine klare Trennung in Produktions-, Test- und Entwicklungsumgebungen sollte vorhanden sein, um möglichen Datenverlust auszuschließen, da die Sicherheitsvorkehrungen pro Umgebung unterschiedlich sind. Für die Verwendung externer Bibliotheken muss ein Risikomanagement durch den Anbieter erfolgen, um die Sicherheit und Zuverlässigkeit dieser zu garantieren. In späteren Entwicklungsphasen sollte ein Plan für die Wartung der Software vorliegen, um auf potenzielle Bedrohungen zu reagieren. Die Implementierung sollte Sicherheitsüberlegungen während des gesamten Designs und der Entwicklung des Services beinhalten. Beispielsweise müssen neue Funktionen auf potenzielle Schwachstellen sofort analysiert und, wenn vorhanden, effektive Maßnahmen ergriffen werden. Sicherheitsstandards wie ISO/IEC 27034, ISO/IEC 30111:2019 und CSA CCM v3.0.1, die über Zertifizierungsmöglichkeiten verfügen, können genutzt werden, um Vertrauen in den Softwareentwicklungsprozess des Anbieters zu gewinnen. Wenn der Anbieter auf Drittanbieter-Software zurückgreift, muss eine kontinuierliche Überwachung hinsichtlich Risiken erfolgen und regelmäßige Sicherheitspatches durchgeführt werden. [Cen24b].

4.4.8 Prinzip 8: Sicherheit der Lieferkette

Dieses Prinzip betont die Wichtigkeit, dass alle Sicherheitsanforderungen des Cloud-Anbieters auch bei dessen Drittanbieter-Lieferketten vorhanden sein müssen. Die große Gefahr hierbei ist, dass, wenn dies nicht der Fall ist, die Sicherheit des gesamten Services durch den Drittanbieter ausgehebelt werden könnte. Entscheidungsträger müssen verstehen, wie ihre Daten mit der Lieferkette von Drittanbietern geteilt werden und auch den Prozess dahinter, warum diese die Daten überhaupt benötigen. Bei den übermittelten Daten muss auf die Art geachtet werden, wie Kundendaten oder aber auch abgeleitete Metadaten. Der Cloud-Anbieter muss daher Sicherheitsanforderungen an seine Lieferkette stellen, damit diese auch von den Drittanbietern implementiert werden. Es muss klar hervorgehen, welche Partei für welche Sicherheitsrisiken verantwortlich ist, um im Falle eines Sicherheitsbruchs schnell reagieren zu können. [Cen24b]

4.4.9 Prinzip 9: Sicheres Benutzermanagement

Sicheres Benutzermanagement umfasst die Bereitstellung von Werkzeugen, die Nutzern es einfach erlauben, den Service sicher zu verwalten. Darunter fällt das Verhindern von unzulässigen Zugriffen und Änderungen an System- und Kundendaten. Es muss ein klares Benutzermodell definiert sein, und Entscheidungsträger müssen jegliche Mechanismen, die für die Autorisierung und den darauffolgenden Zugriff auf Daten vom Cloud-Anbieter verwendet werden, verstehen. Die bereitgestellten Werkzeuge müssen es ermöglichen, dass Kunden Zugriffskontrollen so konfigurieren können, damit sie auf dem Prinzip der geringsten Privilegien basieren. Diese Privilegien umfassen sowohl Administratoren- als auch Standardkonten. Diese Konfigurationen dürfen von anderen Kunden des Services

nicht beeinflusst werden, wie bereits im Prinzip 3 "Trennung von Benutzern" beschrieben. Die Zugriffskontrolle sollte auf individuellen Berechtigungen basieren, die einer Identität, sei es menschlich oder maschinell, zugeordnet sind. Ebenfalls ist ein einheitliches Zugriffskontrollsystem zu bevorzugen, da hiermit die Verwaltung und das Übersehen von Sicherheitslücken in der Autorisierung deutlich vereinfacht werden. Bei hoch privilegierten Nutzerrollen muss eine zeitlich begrenzte Berechtigung vorliegen. Somit kann das irrtümliche Vergessen der Rollenentfernung vermieden werden. Entscheidungsträger sollten somit Cloud-Anbieter bevorzugen, die das Verwalten und Überwachen der Zugriffe auf Ressourcen übersichtlicher und einfacher gestalten. Dies betrifft auch das leichte Entfernen von Berechtigungen von Nutzern. [Cen24b]

4.4.10 Prinzip 10: Identität und Authentifizierung

Das zehnte Prinzip der NCSC-Richtlinien betont die Notwendigkeit, den Zugang zu Serviceschnittstellen auf authentifizierte und autorisierte Personen zu beschränken. Hierbei sind sowohl Benutzer als auch Dienstidentitäten zu beachten. Entscheidungsträger müssen die Authentifizierung der Schnittstellen des Services kennen, um sicherzugehen, dass der Zugang nur auf zugelassene Identitäten beschränkt ist. Der Cloud-Anbieter muss hierzu eine moderne Passwortpolitik verfolgen und die gängige Multi-Faktor-Authentifizierung (MFA) einsetzen. Die Authentifizierungsmechanismen müssen auf Prozesse für die Verwaltung neuer, wechselnder und ausscheidender Mitarbeiter angewendet werden. Ebenso müssen Prozesse implementiert sein, um den Lebenszyklus von Anmeldeinformationen zu verwalten. Eine effektive Authentifizierung zeichnet sich durch die Verifizierung einer eindeutigen Identität aus. Jeder Zugriff muss genau zu einer Identität führen. Für Dienstidentitäten sollten kryptografische Methoden wie Signaturen genutzt werden. Diese Identitäten sollten als kompromittiert gelten und abgelehnt werden, wenn sie von außerhalb der Cloud-Umgebung verwendet werden. Bei den Benutzeranmeldedaten muss ein Zyklus befolgt werden, der unter anderem das Löschen von ausscheidenden Mitarbeitern sowie das schnelle und einfache Entfernen von kompromittierten Anmeldedaten umfasst. Ebenso dürfen Anmeldedaten keine dauerhafte Gültigkeit besitzen. Bei potenziellen Angriffen muss der Cloud-Anbieter sofortige Sicherheitswarnungen für den Kunden bereitstellen. Es sollte eine benutzerfreundliche Authentifizierung in Kombination mit einer starken Methodik verwendet werden. Die Implementierung von Single Sign-On (SSO) wird empfohlen, um Identitäten zu einem Unternehmensverzeichnis zu verknüpfen und ein robustes Authentifizierungsmanagement zu ermöglichen. Entscheidungsträger müssen ebenfalls sicherstellen, dass sich der Cloud-Anbieter selbst authentifiziert, um den Zugriff auf den Service gegen gängige Man-in-the-Middle-Angriffe und Imitierungsdienste zu schützen. Dies wird, wie bereits in Prinzip 1 beschrieben, durch Protokolle wie TLS erreicht [Cen24b]

4.4.11 Prinzip 11: Schutz externer Schnittstellen

Das elfte Prinzip befasst sich mit der Sicherheit aller internen und externen Schnittstellen des Cloud-Services. Darunter versteht man, Webkonsolen, CLI, Verwaltungsschnittstellen

des Cloud-Anbieters und jene Schnittstellen, die zum Kundenservice gehören. Wichtig für Entscheidungsträger ist es hierbei zu verstehen, welche physischen und logischen Schnittstellen vorhanden sind und wie der Zugang gemäß Prinzip 10 mithilfe von Authentifizierung geschützt ist. Ein Cloud-Anbieter sollte eine Liste vorlegen, die detailliert dokumentiert, welche Schnittstellen oder Dienste dem Internet direkt ausgesetzt sind. Insbesondere muss klar gekennzeichnet sein, welche ohne Authentifizierung erfolgen. Dies kann der Fall sein, wenn für Performancezwecke die Authentifizierung deaktiviert wird. Ebenfalls muss genau dargelegt werden, welche Schutzmaßnahmen für die einzelnen Schnittstellen implementiert wurden und wie diese die gängigsten Angriffe abwehren. Bei internetzugänglichen Schnittstellen ist die Gefahr eines Angriffs sehr hoch, da diese von überall angegriffen werden können. Der Cloud-Anbieter sollte jede Schnittstelle seines Dienstes so gestalten, dass sie robust gegen Angriffe ist und kontinuierlich getestet wird, um die Sicherheit zu gewährleisten. Insbesondere sollte erkennbar sein, welche Dienste dem Internet ausgesetzt sind und welche davon keinen Schutz gegen gängige Angriffe wie DoS-Angriffe, Passwort-Spraying und Anwendungsebene-Angriffe haben. [Cen24b]

4.4.12 Prinzip 12: Sichere Dienstverwaltung

Prinzip 12 stellt die Anforderung an Cloud-Anbieter, ihre Verwaltungsschnittstellen nach Unternehmenspraktiken zu entwerfen, zu implementieren und zu verwalten. Die Notwendigkeit besteht darin, dass Verwaltungssysteme meist hoch privilegierten Zugriff auf den Cloud-Service besitzen und somit attraktiv für Angreifer sind. Eine Kompromittierung dieser Systeme kann massive Auswirkungen nach sich ziehen, wie Diebstahl oder Manipulation großer Datenmengen. Entscheidungsträger sollten darauf vertrauen können, dass der Cloud-Anbieter robuste Maßnahmen zur Sicherung der Verwaltungssysteme implementiert. Dies umfasst das Vertrauen in die Geräte, die benutzt werden, um den Cloud-Service zu verwalten. Hierbei sollte der Cloud-Anbieter in kurzen Intervallen Sicherheitskontrollen der verwendeten Geräte durchführen. Der Anbieter sollte seine Verwaltungsschnittstellen schützen und ein gestaffeltes Risikomanagement implementieren. Es sollten Strategien des Privileged Access Managements wie „Just-in-Time“ und „Just-Enough“ Administration verwendet werden. Unter anderem ist es wichtig, dass Verwaltungsschnittstellen detaillierte Auditinformationen liefern. Diese dienen zur Erkennung von anomalem Verhalten und liefern wichtige Anhaltspunkte, die für die Sicherheit essentiell sind. Um zu verhindern, dass Verwaltungsschnittstellen kompromittiert werden und sich Angreifer lateral bewegen können, müssen diverse Implementierungen vorliegen. Privilegierte Zugriffe dürfen nur über interne APIs erfolgen, die Auditinformationen produzieren. Bei hoch privilegierten Zugriffen, die meist sensible Kundendaten betreffen, sollte die Authentifizierung über mehrere Instanzen erfolgen und gegebenenfalls zusätzlich durch MFA gesichert werden. Bei der höchsten Privilegierungsstufe darf nur von sogenannten "Privileged Access Workstations" (PAWs) auf die Verwaltungsschnittstellen zugegriffen werden.Verwaltungsschnittstellen zugegriffen werden. Diese Stationen sollten sich in den Unternehmensgebäuden befinden und der Zugriff sollte eingeschränkt werden, wie in Prinzip 2 beschrieben. Diese Implementierungsansätze erschweren sowohl den unbeabsichtigten Missbrauch als auch gezielte Angriffe. [Cen24b]

4.4.13 Prinzip 13: Auditinformationen und Sicherheitswarnungen

Das dreizehnte Prinzip der NCSC-Richtlinien betont die Wichtigkeit und Nützlichkeit, den Benutzern notwendige Protokolle zur Verfügung zu stellen, um den Zugriff auf den Dienst und Kundendaten zu überwachen und nachvollziehen zu können. Diese sind relevant, um Sicherheitsvorfälle schnell zu identifizieren und angemessen darauf zu reagieren. Ziel ist es, den Nutzern die benötigten Informationen bereitzustellen, um den Zusammenhang von Vorfällen mit der Nutzung und den gespeicherten Daten nachzuvollziehen. Dabei spielt die Qualität der Informationen eine große Rolle, um genau zu analysieren, welche bösartigen Aktivitäten genau passiert sind. Wichtig ist ebenso, dass der Cloud-Anbieter jegliche Informationen über die Aufbewahrungsfrist beilegt. Entscheidungsträger müssen selbst entscheiden, ob die bereitgestellten Informationen für ihre intern gesetzten Anforderungen genügen, um Missbrauch oder Vorfälle untersuchen zu können. Zusätzlich sollte der Cloud-Anbieter Auditinformationen betreffend seines Personals bereitstellen, die für den Kundendienst zuständig sind. Ebenfalls wichtig ist, dass Auditinformationen während eines definierten Aufbewahrungszeitraums weder von Kunden noch vom Cloud-Anbieter gelöscht werden dürfen. Auditinformationen sollten standardmäßig aktiviert und verfügbar sein. Wenn dies nicht der Fall ist, muss der ausgewählte Cloud-Anbieter Optionen bieten, die das Aktivieren leicht ermöglichen. Entscheidungsträger müssen dem Cloud-Anbieter das gewünschte Format der Auditinformationen mitteilen. Dabei können meistens zwei Formate bereitgestellt werden: maschineller Form oder textuelle Form. Der Detaillierungsgrad der Informationen muss dementsprechend hoch sein, um eine effektive forensische Untersuchung von Vorfällen zu gewährleisten. Der zweite wichtige Punkt dieses Prinzips betrifft Sicherheitswarnungen. Diese sollten vom Anbieter standardmäßig aktiviert sein, um im Falle eines Zugriffs auf den Kundenservice und Kundendaten eine Warnung an den betroffenen Kunden zu übermitteln. Der Warnungsprozess sollte schnell und automatisch vonstattengehen und in einem für den Kunden passenden Format übermittelt werden. Bei der Auswahl eines Anbieters sollte darauf geachtet werden, wie dieser Prozess umgesetzt wurde und in welchem Umfang der Kunde miteinbezogen wird. Anbieter sollten den Kunden von Anfang an schnellstmöglich darüber informieren, wenn eine Misskonfiguration, die die Sicherheit betrifft, erkannt wurde. Ebenfalls muss der Anbieter Benutzer warnen, wenn dieser Anomalien entdeckt. Zu diesen Anomalien gehören unerwartete Verfügbarkeit des Dienstes oder eine große Datenübertragung. [Cen24b]

4.4.14 Prinzip 14: Sichere Nutzung des Dienstes

Das vierzehnte Prinzip der NCSC-Richtlinien hebt die Bedeutung hervor, dass Cloud-Anbieter ihre Kunden unterstützen sollten, ihre Daten sicher zu verwalten. Ein entscheidender Punkt dabei ist, dass die Dienste von Anfang an sicher gestaltet und standardmäßig gegen häufige Bedrohungen geschützt sind. Dies bedeutet, dass die Standardeinstellungen der Dienste bereits viele Sicherheitsanforderungen erfüllen. Kunden sollten wissen, welche Sicherheitsziele durch die Standardkonfiguration erreicht werden und welche zusätzlichen Anpassungen notwendig sind, um alle Sicherheitsanforderungen zu erfüllen. Der Anbieter sollte kontinuierlich daran arbeiten, die Standardeinstellungen zu verbessern, um neuen

Bedrohungen zu begegnen. Sicherheitsfunktionen sollten standardmäßig aktiviert sein. Zudem sollte der Anbieter Mechanismen zum Schutz vor häufigen netzwerkbasierten Angriffen wie DDoS bieten. Zusätzlich zur Bereitstellung sicherer Dienste sollten Cloud-Anbieter ihre Kunden unterstützen, ihre Sicherheitsverantwortungen wahrzunehmen. Dies umfasst die Bereitstellung von Tools und Schnittstellen, die es Kunden ermöglichen, ihre Dienste sicher und einfach zu konfigurieren. Kunden sollten die Möglichkeit haben, alle bereitgestellten Ressourcen und deren Konfiguration zentral zu überwachen und zu verwalten. Der Anbieter sollte Warnungen ausgeben, wenn die Konfiguration eines Kunden potenziell unsicher ist, und Werkzeuge zur Verfügung stellen, die bei der Behebung von Sicherheitslücken helfen. Cloud-Anbieter sollten auch Mechanismen bereitstellen, um veraltete Abhängigkeiten und fehlende Sicherheitsupdates in den Workloads der Kunden zu überwachen und entsprechende Sicherheitswarnungen auszugeben. Dashboards und vordefinierte Warnungen können helfen, gute und schlechte Sicherheitspraktiken zu identifizieren und Prioritäten für Sicherheitsverbesserungen zu setzen. Letztlich sind Kunden immer für bestimmte Aspekte der Sicherheit ihrer Daten verantwortlich. Die genaue Verantwortlichkeit hängt von dem genutzten Dienst und dessen Konfiguration ab. Es ist wichtig, diese Verantwortlichkeiten zu identifizieren und regelmäßig zu überprüfen, ob die aktuellen Sicherheitsmaßnahmen den Anforderungen entsprechen. Dies sollte während des gesamten Bereitstellungszyklus des Services erfolgen. [Cen24b].

4.5 Leitfaden zur sicheren Nutzung von SaaS-Anwendungen

Im folgenden Kapitel wird untersucht, wie Software as a Service (SaaS)-Anwendungen unter Einbeziehung der NCSC-Sicherheitsprinzipien sicher konfiguriert und genutzt werden können. Dieses Kapitel dient als direkte Verbindung zwischen den oben genannten theoretischen Sicherheitsprinzipien und den praktischen Anforderungen an die Nutzung eines Cloud-Dienstes und hilft somit, die Zielsetzung dieser Arbeit zu erreichen. Angesichts der zentralen Rolle von SaaS-Lösungen in der digitalen Infrastruktur moderner Unternehmen konzentriert sich die Analyse auf Sicherheitsmaßnahmen, die darauf abzielen, die Betriebskontinuität zu gewährleisten und potenzielle Risiken zu minimieren. Es werden Authentifizierungsstrategien, Datenverschlüsselung und Zugriffskontrollmechanismen betrachtet, um einen umfassenden Sicherheitsansatz für SaaS-Umgebungen zu gewährleisten. [Cen24c]

Verständnis der Anwendung und ihres Zwecks

Bevor überhaupt mit der Konfiguration der ausgewählten SaaS-Anwendungen begonnen wird, ist es notwendig, zuerst den Zweck und die Anwendung zu verstehen, um fundierte Entscheidungen treffen zu können. Dieser Schritt dient als Grundlage für weitere Entscheidungen, die sowohl die Benutzer- als auch die Sicherheitsanforderungen betreffen. Um zu identifizieren, welche Art von Daten im Service verarbeitet werden und welche regulatorischen Anforderungen bestehen, sollten Entscheidungsträger die Hilfsmittel und Dokumentationen des SaaS-Anbieters heranziehen. Diese Dokumentationen

beinhalten Best Practices, die von großem Nutzen für die Konfiguration und Nutzung der Anwendung sind. Für das Testen der gewählten Konfigurationen bieten viele Anbieter eigene Testumgebungen an. Dies bietet den Vorteil, dass hiermit ein tiefes Verständnis für eine Vielzahl von Konfigurationen geschaffen wird, insbesondere für die zuständigen Administratoren. Ein weiterer Vorteil bei der Nutzung von Testumgebungen ist, dass hier viel experimentiert werden kann, ohne die tatsächliche Produktionsumgebung zu beeinträchtigen. [Cen24c]

Gestaltung des Benutzer-Lebenszyklusmanagements

Der nächste Schritt umfasst das Benutzer-Lebenszyklusmanagement. Entscheidungsträger müssen hierbei besonders auf das Benutzer-Onboarding und -Offboarding für SaaS-Anwendungen achten. Zugriffsrechte müssen rechtzeitig für neue Mitarbeiter vergeben und so schnell wie möglich für ausscheidende Mitarbeiter entzogen werden. Des Weiteren sollte der Zugang für Benutzer auf das Minimum beschränkt sein. Benutzer können sowohl interne Mitarbeiterteams als auch externe Kollaborationspartner sein. Es ist wichtig zu identifizieren, welche Identitäten Zugriff auf das System benötigen, um den Betrieb aufrechtzuerhalten und eine passende Zugriffskontrolle zu implementieren. Ein zentrales Identitätssystem wird bevorzugt, um Konsistenz und einen guten Überblick zu gewährleisten. Ein weiterer wichtiger Aspekt, der betrachtet werden sollte, ist, wie leicht bestehende Benutzer im System neue Benutzer registrieren können. Die Benutzerfreundlichkeit spielt hierbei eine große Rolle, denn wenn diese nicht gegeben ist, könnten Benutzer dazu verleitet werden, Sicherheitsvorkehrungen zu umgehen oder eigene Lösungen zum Hinzufügen und Entfernen von Nutzern zu verwenden. [Cen24c].

Robuste Nutzerauthentifizierung

Als Nächstes müssen sich Entscheidungsträger Gedanken über Authentifizierungsmethoden machen. Empfohlen wird hierbei die Nutzung moderner Methoden wie Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA). Dabei ist es wichtig, dass die zu überprüfenden Benutzeridentitäten eindeutige Attribute aufweisen, die dabei helfen, eine robuste Zugriffskontrolle durchzusetzen. Dadurch können auch Spoofing- und Manipulationsangriffe verhindert werden. SSO sollte aus diesem Grund verwendet werden, da es die Verwaltung von Benutzeridentitäten vereinfacht und die Benutzer sich nur ein Anmeldeset merken müssen. Falls SSO nicht umgesetzt werden kann, sollte auf eine direkte Authentifizierung zurückgegriffen und diese mit MFA und einer aktuellen Passwortpolitik abgesichert werden. [Cen24c]

Absicherung administrativer Zugänge

Der nächste Aspekt, der bei der sicheren Nutzung einer SaaS-Anwendung beachtet werden muss, ist die Verwaltung administrativer Benutzer. Diese Benutzer besitzen Privilegien, um Konfigurationen des Services zu verändern und auf die Ressourcen von Benutzern zuzugreifen. Um einen möglichen Missbrauch von System- oder Benutzerdaten zu vermeiden,

muss eine strikte Verwaltung dieser Privilegien erfolgen. Es ist wichtig, die Anzahl der administrativen Benutzer zu minimieren und das Prinzip der minimalen Rechtevergabe anzuwenden, um den Schaden im Falle eines kompromittierten Administrationskontos zu reduzieren. Dies sollte durch eine rollenbasierte Zugriffskontrolle (RBAC) umgesetzt werden. Jeder administrative Zugriff muss protokolliert und überwacht werden, um schnell auf Sicherheitsvorfälle reagieren zu können. Für besonders sensible Daten sollte Privileged Access Management (PAM) verwendet werden, um ständige Administratorrechte zu entfernen. Administrative Tätigkeiten sollten nur auf vertrauenswürdigen Geräten, wie einer Privileged Access Workstation (PAW), durchgeführt werden. [Cen24c]

Berechtigungsmanagement für Standardnutzer

Bei der Vergabe von Privilegien für externe Partner und interne Mitarbeiter ist es entscheidend, nur so viel Handlungsspielraum im System zu gewähren, wie der Nutzer tatsächlich benötigt, um seine Aufgaben zu erfüllen. Dies minimiert potenzielle Sicherheitsrisiken und schützt sensible Daten. Die Zugriffskontrolle sollte rollenbasiert erfolgen, um eine klare und strukturierte Verwaltung der Berechtigungen zu gewährleisten. Ein Zero-Trust-Modell ist besonders empfehlenswert, da hierbei nicht nur die Identität des Nutzers, sondern auch der Kontext des Zugriffs berücksichtigt wird. Dies bedeutet, dass der Zugriff auf hochsensible Ressourcen nur von vertrauenswürdigen Geräten und Netzwerken aus erfolgen darf. Durch die Implementierung dieser Ansätze wird sichergestellt, dass der Zugang zu Systemen und Daten auf das notwendige Minimum beschränkt bleibt und Sicherheitsverletzungen effektiv verhindert werden können. [Cen24c]

Nutzung vertrauenswürdiger Geräte

Beim Zugriff auf den Service müssen die verwendeten Geräte genauestens untersucht werden. Es sollte sichergestellt sein, dass der Zugriff nur von vertrauenswürdigen Geräten erfolgt, wie zum Beispiel Firmenlaptops. Es sollte nicht möglich sein, mit privaten Computern internen Zugriff zu bekommen. Beim Zugriff auf hochsensible Daten sollten nur gesicherte Geräte verwendet werden, die sich am Firmengelände befinden, um eine Kompromittierung zu verhindern. Hierbei sollte das Zero-Trust-Modell miteinbezogen werden, da es hilfreich ist, die Gerätesicherheit zu erreichen. [Cen24c]

Datenschutz und Datensicherheit gewährleisten

Die Daten sollten gemäß den Best Practices verschlüsselt, sowohl in Transit als auch in Ruhe, und nur in rechtskonformen Rechtsräumen gespeichert und verarbeitet werden die mit den gesetzliche Anforderungen der Kunden vereinbar sind. Wie im Prinzip 1 und 2 bereits beschrieben. Es sollte nicht willkürlich möglich sein auf die Daten durch das Personal des Anbieters zuzugreifen. Hierbei muss im Falle eine Einwilligung von Kunden eingeholt werden. [Cen24c]

Prüfung auf Schadsoftware und gefährliche Inhalte

SaaS-Anwendungen können von Angreifern verwendet werden, um bösartige Inhalte an Kunden zu verbreiten. Der Cloud-Anbieter sollte Sicherheitsmechanismen implementiert haben, die sowohl empfangene Daten als auch bereits gespeicherte Daten auf bösartige Komponenten untersuchen. Die dabei angewendeten Kontrollen sollten auf die gängigsten Bedrohungen abgestimmt sein, wie zum Beispiel das Prüfen von hochgeladenen Dateien auf Malware und URLs in Nachrichten auf Phishing-Versuche. Die Erkennung und Behebung von Bedrohungen sollte in die vom Kunden vorgenommenen Sicherheitsüberwachungs- und Vorfallsreaktionsprozesse integriert sein. [Cen24c]

Sichere Freigabe und Nutzung von Ressourcen

Entscheidungsträger müssen sicherstellen, dass der Zugang zu Ressourcen sicher geteilt wird, um unbeabsichtigte und beabsichtigte Datenfreigaben zu vermeiden. Es sollte standardmäßig nicht möglich sein, auf Daten ohne eingeholte Einwilligung zuzugreifen. Die anfallenden Ressourcen sollten eindeutige Kennzeichnungen besitzen, die sofort ersichtlich zeigen, wie sensibel diese Daten eingestuft sind. Es sollten Schulungen und Leitfäden entwickelt werden, die die richtige Verwaltung und Nutzung von Ressourcen fördern. Ebenfalls sollten Tools verwendet werden, die es vereinfachen, den Überblick über geteilte Ressourcen zu behalten und verhindern, dass Ressourcen nach eigenem Ermessen geteilt werden. [Cen24c]

Management von Dienstidentitäten

Dienstidentitäten sollten effektiv und sicher verwaltet werden, um das Risiko von Missbrauch zu vermeiden. Es sollte eine kontinuierliche Überwachung hinsichtlich der Nutzungshistorie und der vorhandenen Berechtigungen der Dienstidentität erfolgen. Hochrisiko-Zugänge sollten eine administrative Genehmigung erfordern. Dabei ist es wichtig, regelmäßig den Umfang des Zugriffs zu prüfen, um sicherzustellen, dass dieser für die auszuführenden Arbeiten notwendig ist. Zudem sollten die Aktivitäten dieser Dienste in die Sicherheitsüberwachungs- und Auditierungsprozesse integriert werden, um böswillige Nutzung zu erkennen. [Cen24c]

Reaktionsstrategien für Sicherheitsvorfälle und Notfälle

Reaktionsstrategien sind wichtig für ein schnelles Agieren bei Sicherheitsvorfällen und eine schnelle Erholung von dabei erlittenen Schäden. Entscheidungsträger müssen sicherstellen, dass hierfür gut definierte und getestete Prozesse vorliegen, die sowohl die eigene Nutzung als auch den gesamten Dienst betreffen. Es ist wichtig zu wissen, wie Sicherheitsbenachrichtigungen geliefert werden und wie man den Anbieter im Falle eines Vorfalls benachrichtigt. Die verwendeten Kontaktinformationen müssen aktuell und gültig sein. Die Reaktionsprozesse sollten alle Vorfälle abdecken und kritische Daten sichern. Robuste Verfahren zur Zugriffswiederherstellung sollten eingerichtet werden, um im Katastrophenfall den Zugang schnell wiederherzustellen. [Cen24c]

Überwachung von Sicherheitsereignissen

Die kontinuierliche Überwachung und die Analyse von Audit-Daten sind notwendig, um Sicherheitsvorfälle frühzeitig zu erkennen. Aktivitätenprotokolle sollten manipulationssicher gespeichert und lange genug aufbewahrt werden, um forensische Analysen zu ermöglichen. [Cen24c]

Aufrechterhaltung der Sicherheitsstandards

Die kontinuierliche Anpassung an technologische Entwicklungen und Sicherheitsupdates ist erforderlich, um die Schutzmaßnahmen aktuell zu halten. Die regelmäßige Überprüfung der Sicherheitsstrategien und -konfigurationen gewährleistet, dass Anwendungen den Sicherheitsanforderungen weiterhin entsprechen. [Cen24c].

5 Implementierung

Der Praxisteil dieser Arbeit besteht aus zwei zusammenhängenden Komponenten. Zum einen ein Cloud Security Wiki, das als umfassende Ressource rund um das Thema Cloud Security dient, und zum anderen ein dynamischer Teil, der das Verinnerlichen und Anwenden der 14 NCSC Security Prinzipien [Cen24b] interaktiv vereinfacht.

5.1 Cloud Security Wiki

Einleitung

Im Rahmen der Bachelorarbeit wurde ein Cloud Security Wiki in Moodle entwickelt, das als umfassendes Nachschlagewerk für Entscheidungsträger in Organisationen sowie für Einzelpersonen dient, die auf die Cloud wechseln oder ihre bestehende Infrastruktur in die Cloud integrieren wollen. Abbildung 5.1 zeigt die Darstellung des ersten von vierzehn NCSC-Sicherheitsprinzipien [Cen24b] im Cloud Security Wiki.

Ziele

Die Hauptziele des Cloud Security Wikis sind die Bereitstellung von Informationen über grundlegende Cloud-Modelle und die verschiedenen Deployment-Modelle sowie ein umfangreiches Abdecken aller häufigen Bedrohungen und Maßnahmen, die beim Umstieg und während der Nutzung eines Cloud-Services beachtet werden sollten. Dabei wurde sich auf die 14 Cloud-Sicherheitsprinzipien der NCSC gestützt. [Cen24b]

Anforderungen

Als Plattform für das Deployment wurde das Lernmanagementsystem Moodle verwendet. [Moo24] Der Hauptgrund, warum Moodle gewählt wurde, basiert auf der dauerhaften Aufrechterhaltung der Aktualität der Inhalte des Wikis. Moodle bietet hierzu bereits vordefinierte Funktionen, die das Verwalten der einzelnen Seiten erleichtern. Ebenso wichtig war die bereits vorhandene Funktion der Rollenzuweisung der einzelnen Nutzer. Somit konnte effizient ein RBAC (Role-Based Access Control) implementiert werden.

Implementierungsschritte

1. **Installation und Konfiguration**: Moodle wurde zunächst für Testzwecke und die Migration der Informationen lokal mittels Docker aufgesetzt. Dabei wurde das Docker-Image aus dem Bitnami-Repository [bit24] verwendet. Für die Inhalte

wurde HTML-Code mit Styling eingesetzt, um die Struktur, den Aufbau und das Design zu entwickeln.

2. **Migration von Informationen**: Mithilfe von HTML-Styling wurden die Informationen klar und übersichtlich strukturiert und aufbereitet. Dabei wurden die Informationen aus den Themengebieten der Bachelorarbeit entnommen und an ein Wiki-Leseformat angepasst.
3. **Benutzerverwaltung**: Anhand eines Admin-Users wurden alle Einstellungen vorgenommen. Danach wurde das Wiki auf die offizielle Moodle-Seite des Kurses Informationssicherheit der Universität Wien migriert.
4. **Benutzerverwaltung lokal**: Es wurde eine Admin-Rolle erstellt, die Zugriff auf alle Informationen des Wikis hatte. Diesem User ist es möglich, die Moodle-Seiten aktuell zu halten, falls sich Bedrohungs- oder Sicherheitslandschaften verändern.

Strukturierung

Das Wiki wurde in fünf Kategorien gegliedert:

- Einführung in die Cloud-Modelle
- Deployment-Modelle in der Cloud
- Service Level Agreements
- Auswahl und Überprüfung von Cloud-Anbietern nach NCSC-Richtlinien [Cen24b]
- Sichere Nutzung von SaaS-Anwendungen

Jede dieser Hauptkategorien besitzt mehrere Unterkategorien mit spezifischen Informationen. Die Inhalte wurden mit einheitlichen Überschriften und Aufzählungen in klare Abschnitte unterteilt.

Inhalte

Die Inhalte des Wikis wurden sorgfältig recherchiert und erstellt, basierend auf aktuellen Sicherheitsstandards und Best Practices. Eine der wichtigsten Quellen umfasst die Cloud-Sicherheitsprinzipien des NCSC. [Cen24b]

Testing und Bereitstellung

Vor der endgültigen Fertigstellung wurde das Wiki ausführlich in einer lokalen Umgebung intensiv getestet. Der Fokus beim Testing lag einerseits auf der Suchfunktion und der Menüführung sowie auf der rollenbasierten Gruppierung der Benutzer. Ebenfalls wurde die Aktualisierung der Inhalte in Bezug auf sich ändernde Bedrohungslandschaften getestet und ob diese Änderungen sofort in der Datenbank persistiert wurden. Die endgültige Bereitstellung erfolgte über das Moodle der Lehrveranstaltung "051061 VU Informationssicherheit".

5.2 Interaktives Fallbeispiel-Tool der 14 NCSC Sicherheitsprinzipien

Einleitung

Der zweite Praxisteil der Bachelorarbeit umfasst ein interaktives Tool, das Entscheidungsträgern sowie Privatpersonen das Verinnerlichen und Anwenden der 14 NCSC Sicherheitsprinzipien [Cen24b] interaktiv erleichtern soll. Dabei kann der Nutzer jedes der 14 Prinzipien mithilfe von Fallbeispielen als Quiz kennenlernen und absolvieren. Abbildung 5.2 zeigt die Startseite des dynamischen Tools und die ersten vier Szenarien.

Ziele

Die Hauptziele des interaktiven Teils sind die Förderung der Anwendung und des Verständnisses der 14 Cloud-Sicherheitsprinzipien des NCSC. [Cen24b] Wobei darauf geachtet wurde eine benutzerfreundliche Plattform und ein dynamisches Lernumfeld zu erschaffen.

Anforderungen

Um die Dynamik des Praxisteils zu gewährleisten, wurde React für die Entwicklung verwendet. Dabei lag der Fokus auf einer intuitiven Navigation und Benutzerfreundlichkeit. Zudem wurden für Tabellen und Menüpunkte bewährte MUI-Komponenten [MUI24] integriert, um eine optimale Nutzung sowohl auf Desktop- als auch auf Mobilgeräten zu gewährleisten.

Implementierungsschritte

1. **Einrichtung der React App**: Zunächst wurde ein neues React-Projekt mit Create React App in Visual Studio Code aufgesetzt. Alle notwendigen Abhängigkeiten und Bibliotheken wurden installiert, um die Entwicklung zu unterstützen. Das Projekt wurde in verschiedene Komponenten unterteilt, um eine modulare und übersichtliche Struktur zu gewährleisten. Die Hauptkomponenten umfassen die App-Komponente und die Szenarien-Komponenten. Als Bibliotheken wurden unter anderem Material-UI (MUI) verwendet. Für ein leichtes Deployment wurde ein GitHub-Repository erstellt.

2. **Entwicklung der Szenarien**: Für jedes der 14 Cloud-Sicherheitsprinzipien wurde eine eigene Szenario-Komponente erstellt. Diese Komponenten enthalten interaktive Elemente, die den Benutzern erleichtern, die Prinzipien zu verstehen und anzuwenden. Jedes dieser interaktiven Elemente, wie Fragen, Multiple-Choice-Optionen und Feedback-Mechanismen, wurde mit React States und Props verwaltet.

3. **Entwicklung der App-Komponente**: Die App-Komponente enthält alle Mechanismen für die Navigation zwischen den verschiedenen Szenarien. Es wurde auf eine herkömmliche Menüleiste verzichtet und stattdessen MUI-Cards-Komponenten mit

Hintergrundbildern verwendet, um die jeweiligen Szenarien leicht zu identifizieren und zu navigieren. Die verwendeten Hintergrundbilder (Cliparts) für die vierzehn Prinzipien wurden mithilfe von OpenAI ChatGPT [Ope24] generiert.

4. **State Management**: Für das State-Management wurde React State verwendet, um den aktuellen Zustand der App zu verwalten und Benutzereingaben zu verarbeiten.

Strukturierung

Das React-Projekt wurde in mehrere Seiten (Pages) unterteilt, um eine intuitive und klare Übersicht für die Benutzer zu erreichen.

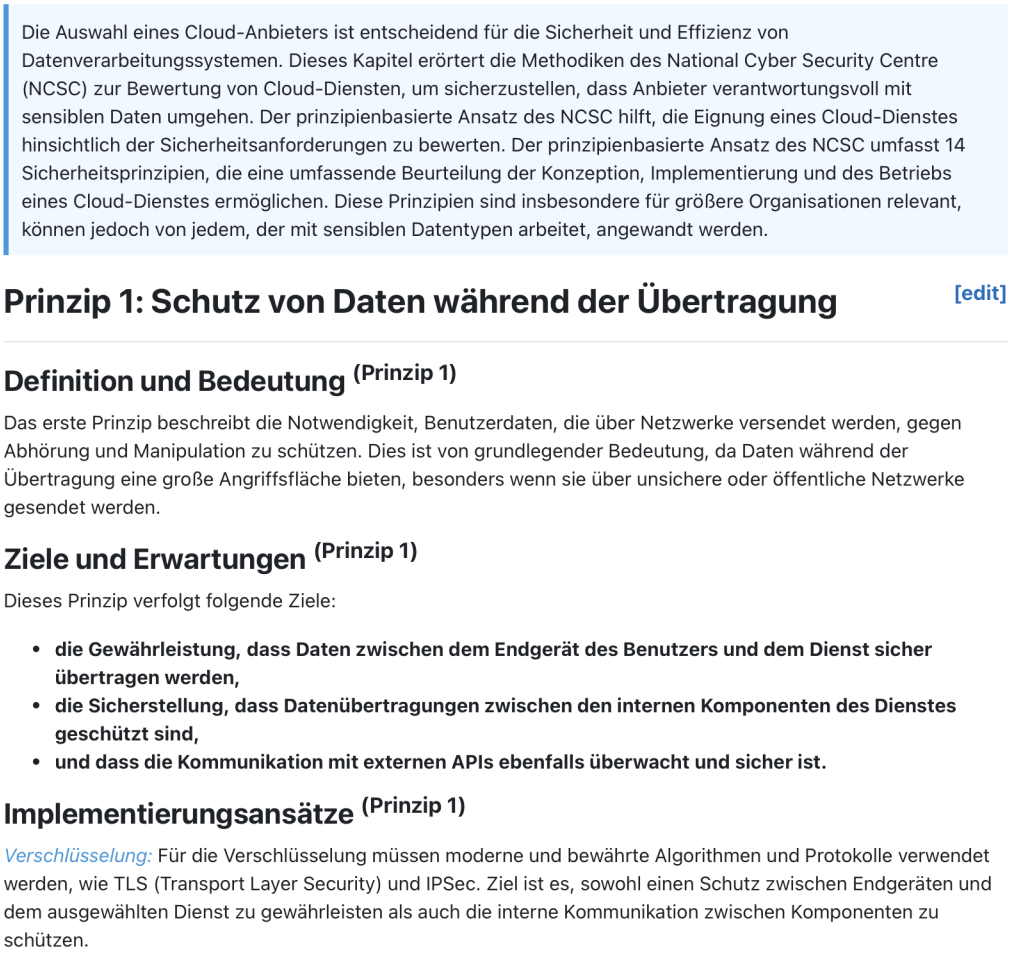
- **Home Page**: Die Startseite, die eine Einführung in die Anwendung und Links (MUI-Card Components) zu den verschiedenen Szenarien bietet.

- **Scenario Pages**: Jede der 14 NCSC Sicherheitsprinzipien [Cen24b] hat eine eigene Seite, die ein spezifisches Szenario präsentiert. Diese Seiten sind:
  - Scenario 1: Schutz von Daten während der Übertragung
  - Scenario 2: Schutz von Daten im Ruhezustand
  - Scenario 3: Trennung zwischen den Benutzern
  - Scenario 4: Governance-Framework
  - Scenario 5: Betriebssicherheit
  - Scenario 6: Personalsicherheit
  - Scenario 7: Sichere Entwicklung
  - Scenario 8: Lieferketten-Sicherheit
  - Scenario 9: Sicheres Benutzermanagement
  - Scenario 10: Identität und Authentifizierung
  - Scenario 11: Schutz von Schnittstellen
  - Scenario 12: Sicheres Management der Dienste
  - Scenario 13: Audit-Informationen und Sicherheitswarnungen
  - Scenario 14: Sicheres Benutzerverhalten

- **Result Page**: Eine Seite, die die Ergebnisse der Benutzereingaben zusammenfasst und Feedback über die getroffenen Entscheidungen gibt. Dieses Feedback umfasst die ausgewählte Antwort, die richtige Antwort und eine zusätzliche Erklärung zu den Antwortmöglichkeiten jeder Frage.

Testen und Bereitstellung

Die Bereitstellung der App erfolgte über den Anbieter "Vercel". [Ver24] Hierbei wurde durch die Verknüpfung mit einem GitHub-Repository bei jedem Push-Command eine Pipeline durchlaufen und die App wurde immer wieder neu gebaut. Vor der endgültigen Bereitstellung wurde intensives Testing betrieben. Dabei wurden Anzeigefehler sowie Logikfehler gefunden und behoben.



> Die Auswahl eines Cloud-Anbieters ist entscheidend für die Sicherheit und Effizienz von Datenverarbeitungssystemen. Dieses Kapitel erörtert die Methodiken des National Cyber Security Centre (NCSC) zur Bewertung von Cloud-Diensten, um sicherzustellen, dass Anbieter verantwortungsvoll mit sensiblen Daten umgehen. Der prinzipienbasierte Ansatz des NCSC hilft, die Eignung eines Cloud-Dienstes hinsichtlich der Sicherheitsanforderungen zu bewerten. Der prinzipienbasierte Ansatz des NCSC umfasst 14 Sicherheitsprinzipien, die eine umfassende Beurteilung der Konzeption, Implementierung und des Betriebs eines Cloud-Dienstes ermöglichen. Diese Prinzipien sind insbesondere für größere Organisationen relevant, können jedoch von jedem, der mit sensiblen Datentypen arbeitet, angewandt werden.

Prinzip 1: Schutz von Daten während der Übertragung [edit]

Definition und Bedeutung (Prinzip 1)

Das erste Prinzip beschreibt die Notwendigkeit, Benutzerdaten, die über Netzwerke versendet werden, gegen Abhörung und Manipulation zu schützen. Dies ist von grundlegender Bedeutung, da Daten während der Übertragung eine große Angriffsfläche bieten, besonders wenn sie über unsichere oder öffentliche Netzwerke gesendet werden.

Ziele und Erwartungen (Prinzip 1)

Dieses Prinzip verfolgt folgende Ziele:

- **die Gewährleistung, dass Daten zwischen dem Endgerät des Benutzers und dem Dienst sicher übertragen werden,**
- **die Sicherstellung, dass Datenübertragungen zwischen den internen Komponenten des Dienstes geschützt sind,**
- **und dass die Kommunikation mit externen APIs ebenfalls überwacht und sicher ist.**

Implementierungsansätze (Prinzip 1)

Verschlüsselung: Für die Verschlüsselung müssen moderne und bewährte Algorithmen und Protokolle verwendet werden, wie TLS (Transport Layer Security) und IPSec. Ziel ist es, sowohl einen Schutz zwischen Endgeräten und dem ausgewählten Dienst zu gewährleisten als auch die interne Kommunikation zwischen Komponenten zu schützen.

Figure 5.1: Darstellung des ersten NCSC-Sicherheitsprinzips: Schutz von Daten während der Übertragung, einschließlich Definition und Implementierungsansätze im Cloud Security Wiki.

Figure 5.2: Startseite des interaktiven Cloud Security Fallstudien-Tools.

6 Evaluierung

In diesem Kapitel werden die Methodik und Ergebnisse der Evaluierung der beiden Praxisteile, dem Cloud Security Wiki und dem interaktiven Fallbeispiel-Tool der 14 NCSC Sicherheitsprinzipien [Cen24b], präsentiert.

6.1 Methodik

Die Evaluierung der beiden Praxisteile, dem Cloud Security Wiki und dem interaktiven Fallbeispiel-Tool der 14 NCSC Sicherheitsprinzipien [Cen24b], wurde mithilfe eines Onlinefragebogens durchgeführt. Der Fragebogen wurde mit dem Online-Tool "Survio" [Sur24] erstellt und enthielt sowohl offene als auch Single-Choice-Fragen. Die Befragung zielte darauf ab, die Effektivität, Benutzerfreundlichkeit und die Qualität der Informationen der beiden Werkzeuge zu bewerten.
Der in der Evaluierung benutzte Fragebogen wurde so konzipiert, dass Aspekte wie Usability, Struktur und Organisation sowie Qualität der Inhalte erfasst werden. Zusätzlich wurden für jeden Praxisteil offene Feedbackfragen eingebaut, um detaillierte Rückmeldungen der Nutzer zu erhalten. Insgesamt umfasste der Fragebogen 39 Fragen, die in folgende Gruppen unterteilt waren:

- **Usability**: Fragen zur Benutzerfreundlichkeit und intuitiven Handhabung der Werkzeuge.
- **Struktur und Organisation**: Fragen zur logischen Anordnung und Übersichtlichkeit der Inhalte.
- **Qualität der Inhalte**: Fragen zur Relevanz, Genauigkeit und Aktualität der bereitgestellten Informationen.
- **Feedbackfragen**: Offene Fragen zur Sammlung von Verbesserungsvorschlägen und allgemeinen Eindrücken.

Die Evaluierung fand am 13. Juni 2024 in der Informatik- und Publizistik-Fakultät der Universität Wien im Rahmen der Lehrveranstaltung "051061 VU Informationssicherheit" statt und umfasste eine Zeitdauer von fünf Stunden. An der Befragung nahmen drei unterschiedliche Gruppen mit circa 50 Studenten teil. Diese Gruppen boten eine repräsentative Stichprobe der potenziellen Nutzer des Cloud Security Wikis und des interaktiven Fallbeispiel-Tools. Die Durchführung der Studie in einem akademischen Umfeld gewährleistete konstruktives Feedback von möglichen angehenden Fachkräften im

Bereich Informationssicherheit.
Die Auswertung der Daten erfolgte qualitativ und quantitativ, um sowohl statistische Trends als auch individuelle Rückmeldungen zu erfassen und zu analysieren.

6.2 Ergebnisse

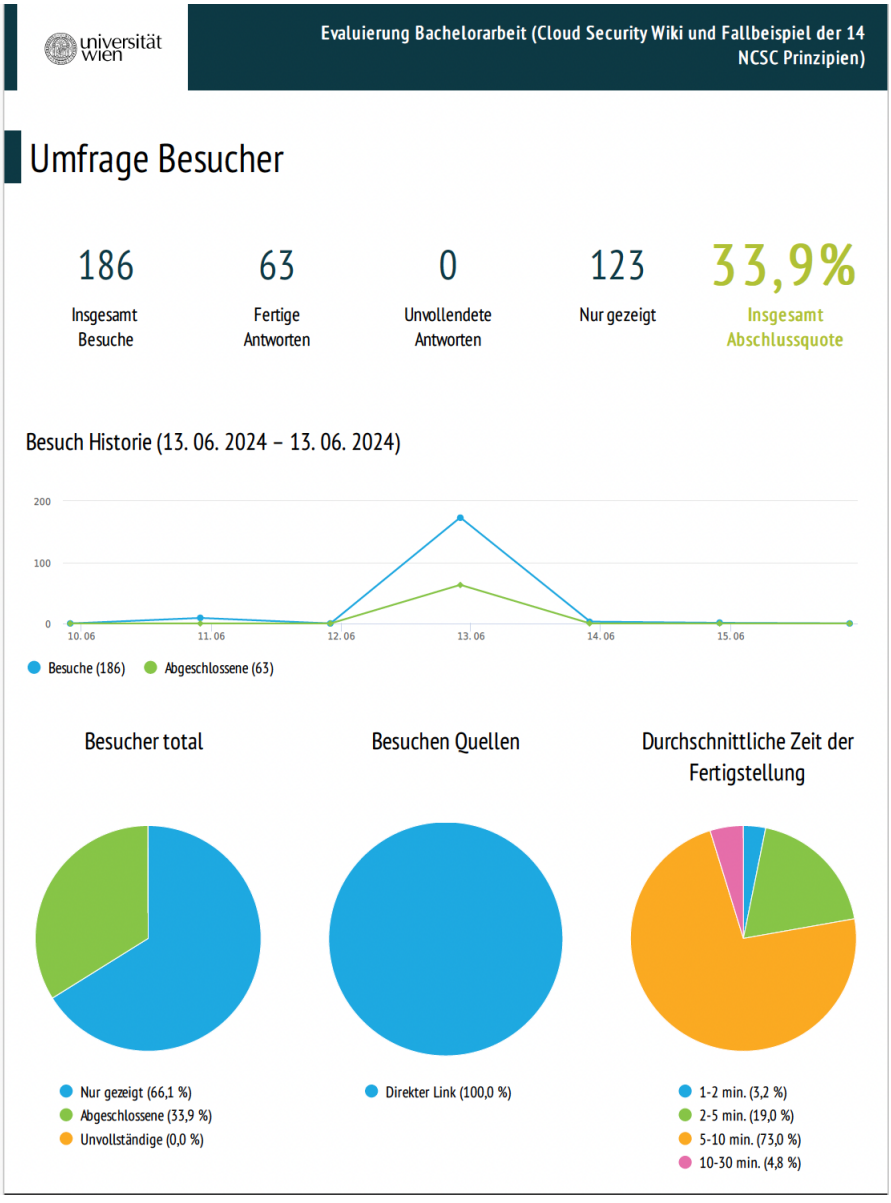


Figure 6.1: Umfragestatistik

Abbildung 6.1 zeigt, dass der Fragebogen von 186 Besuchern geöffnet wurde, von denen 63 Personen teilgenommen und ihn vollständig abgeschlossen haben. Die Ergebnisse wurden in Kategorien unterteilt und detailliert dargestellt.

6.2.1 Cloud Security Wiki

- **Erfahrungen und Wissen**:
  - Die meisten Teilnehmer hatten wenig bis keine Erfahrung im Bereich Cloud Security. 85.7% der Teilnehmer gaben an, weniger als ein Jahr oder keine Erfahrung zu haben.
- **Informationsinhalt und Richtigkeit**:
  - 96.8% der Nutzer fanden die gesuchten Informationen.
  - 87.3% fanden die Informationen schnell oder sehr schnell.
  - 88.1% waren mit der Vollständigkeit der gefundenen Informationen zufrieden.
  - 95.3% fanden die bereitgestellten Informationen hilfreich oder sehr hilfreich.
  - 88.9% bewerteten die Informationen als klar oder sehr klar und verständlich.
- **Usability und Navigation**:
  - 80.9% bewerteten die Navigation innerhalb des Artikels als gut oder sehr gut.
  - 49.2% fanden die Suchfunktion des Wikis hilfreich oder sehr hilfreich.
  - 77.8% fanden die Navigation im Wiki intuitiv oder sehr intuitiv.
  - 77.8% bewerteten das Layout und Design des Wikis als gut oder sehr gut.
  - 81.0% fanden die Informationen im Wiki leicht oder sehr leicht zu finden.
  - 73.0% bewerteten die Anweisungen zur Navigation im Wiki (z.B. Menüführung, Suchfunktion) als klar oder sehr klar und verständlich.
- **Struktur und Organisation**:
  - 85.8% bewerteten die Struktur des Cloud Security Wikis (z.B. Kategorien, Unterkategorien) als gut oder sehr gut.
  - 82.6% bewerteten die Hierarchie der Themen im Wiki als logisch oder sehr logisch.
  - 77.8% bewerteten die Anordnung der Inhalte im Wiki als übersichtlich oder sehr übersichtlich.
- **Gesamtzufriedenheit**:
  - 84.1% der Teilnehmer waren insgesamt zufrieden oder sehr zufrieden mit dem Cloud Security Wiki.

- **Verbesserungsvorschläge**:
  Hierbei handelt es sich um gezielt ausgewählte Verbesserungsvorschläge, die für das Ziel dieser Arbeit von großer Wichtigkeit sind.
  - Verbesserung der Suchfunktion, insbesondere keine Unterscheidung zwischen Groß- und Kleinschreibung.
  - Implementierung detaillierterer Erklärungen für bestimmte Themen, wie z.B. das softwaredefinierte Netzwerk (SDN).
  - Hinzufügen einer Seite mit weiterführenden externen Links als Ergänzung zum Wiki.
  - Verbesserung der Struktur und des Layouts, um die Übersichtlichkeit zu erhöhen.

6.2.2 Interaktives Fallbeispiel-Tool der 14 NCSC Sicherheitsprinzipien

- **Verständnis und Lernzielerreichung**:
  - 73% der Nutzer fanden das Quiz hilfreich oder sehr hilfreich zur Verinnerlichung der 14 NCSC Cloud Principles [Cen24b].
  - 74.6% der Teilnehmer gaben an, dass das Quiz ihr Verständnis der Prinzipien verbessert hat.
  - 38.1% fühlten sich durch das Quiz motiviert, sich weiter mit den Prinzipien zu beschäftigen.
  - 74.6% bewerteten die Fragen des Quizzes als relevant oder sehr relevant für das Verständnis der Prinzipien.
  - 92% bewerteten die Fragen als klar und verständlich.
  - 76.2% empfanden den Schwierigkeitsgrad des Quizzes als einfach oder sehr einfach.
- **Usability und Organisation**:
  - 87.3% fanden die Benutzeroberfläche des Quizzes intuitiv oder sehr intuitiv.
- **Technische Probleme und Schwierigkeiten**:
  - 98.4% der Teilnehmer hatten keine technischen Probleme beim Durchführen des Quizzes.
- **Gesamtzufriedenheit**:
  - 81% der Nutzer waren insgesamt zufrieden oder sehr zufrieden mit dem Quiz.
- **Verbesserungsvorschläge**:
  Hierbei handelt es sich um gezielt ausgewählte Verbesserungsvorschläge, die für das Ziel dieser Arbeit von großer Wichtigkeit sind.
  - Erhöhung des Schwierigkeitsgrades der Fragen, um das Raten zu erschweren.

- Einheitliche Formatierung der Antworten, um die richtige Antwort nicht zu offensichtlich zu machen.
- Verbesserung der Benutzeroberfläche, insbesondere deutlicherer Hinweise auf die Art der Fragen (Multiple Choice oder Single Choice).
- Sofortige Anzeige der richtigen Antwort mit Erklärung nach jeder Frage.

7 Diskussion und Ausblick

In den zwei folgenden Sektionen, Diskussion und Ausblick, werden die in der Evaluierung präsentierten Ergebnisse interpretiert und Schlussfolgerungen daraus gezogen. Zudem wird ein Ausblick auf zukünftige Entwicklungen der beiden Praxisteile gegeben.

7.1 Diskussion

Die Evaluierungsergebnisse zeigen, dass sowohl das Cloud Security Wiki als auch das interaktive Fallbeispiel-Tool der 14 NCSC-Sicherheitsprinzipien [Cen24b] von den Nutzern positiv bewertet wurden. Die Mehrheit der Teilnehmer fand die bereitgestellten Informationen relevant und hilfreich, wobei besonders die Benutzerfreundlichkeit und Navigation des Wikis hervorgehoben wurden. Dies deutet auf eine erfolgreiche Strukturierung und Organisation der Inhalte hin.
Ein zentraler Aspekt der Verbesserungsvorschläge betraf die Optimierung der Suchfunktion des Wikis. Eine erweiterte Suchfunktion, die Groß- und Kleinschreibung ignoriert, könnte die Benutzererfahrung erheblich verbessern. Zudem wurde vorgeschlagen, detailliertere Erklärungen zu spezifischen Themen und weiterführende externe Links zu integrieren, um den Nutzern tiefere Einblicke zu ermöglichen.
Die Mehrheit der Teilnehmer hatte wenig bis keine Erfahrung im Bereich Cloud Security. 85,7% der Teilnehmer gaben an, weniger als ein Jahr oder keine Erfahrung zu haben. Dies deutet darauf hin, dass das Wiki besonders für Anfänger nützlich ist, die grundlegendes Wissen erwerben möchten.
Das interaktive Fallbeispiel-Tool wurde ebenfalls positiv aufgenommen, insbesondere in Bezug auf die Unterstützung beim Verständnis und der Anwendung der NCSC-Sicherheitsprinzipien [Cen24b]. Die intuitive Benutzeroberfläche und die Relevanz der Fragen wurden geschätzt. Dennoch wurde der Schwierigkeitsgrad der Fragen als zu einfach empfunden, was auf die Notwendigkeit einer Anpassung hinweist, um das Tool herausfordernder und lehrreicher zu gestalten.
Ein weiteres wichtiges Feedback betraf die sofortige Anzeige der richtigen Antworten nach jeder Frage im Quiz, um den Lernprozess zu unterstützen. Dies könnte nicht nur das Verständnis vertiefen, sondern auch eine noch direktere Lernkontrolle ermöglichen.
Die in der Motivation dieser Arbeit gesetzten Ziele wurden größtenteils erreicht. Die entwickelten Werkzeuge basieren auf umfassenden Recherchen und den aktuellsten Sicherheitsrichtlinien der NCSC [Cen24b], was eine technisch und inhaltlich hochwertige Ressource geschaffen hat. Diese fundierte Basis ermöglichte es, Informationslücken in bestehenden Cloud Security Wikis erfolgreich zu schließen. Die Einbindung eines interaktiven Tools hat dazu beigetragen, dass Entscheidungsträger die Sicherheitsanforderungen

besser verstehen und praktisch anwenden können. Dies zeigt, dass die Kombination aus theoretischer Wissensvermittlung und praktischer Anwendung ein effektives Mittel zur Förderung des Verständnisses und der Umsetzung von Sicherheitsprinzipien ist. Ein weiterer Vorteil der entwickelten Werkzeuge ist die Implementierung des Wikis im Lernmanagement-System Moodle. Dadurch kann die Aktualität der Inhalte schnell und einfach gewährleistet werden. Dies ist besonders wichtig, da die State-of-the-Art-Analyse gezeigt hat, dass einige bestehende Wikis veraltet sind. Durch die einfache Aktualisierungsmöglichkeit in Moodle bleibt das Cloud Security Wiki stets auf dem neuesten Stand und bietet den Nutzern relevante und aktuelle Informationen.

7.2 Ausblick

Aufbauend auf den Evaluierungsergebnissen gibt es mehrere Maßnahmen, die zur Verbesserung der beiden Werkzeuge ergriffen werden können. Für das Cloud Security Wiki sollte die Suchfunktion optimiert werden, um eine benutzerfreundlichere und effizientere Suche zu ermöglichen. Darüber hinaus sollten detailliertere Erklärungen zu komplexen Themen und eine Sammlung weiterführender Links integriert werden, um den Nutzern umfassendere Informationen zu bieten.
Für das interaktive Fallbeispiel-Tool ist eine Erhöhung des Schwierigkeitsgrades der Fragen notwendig, um die Nutzer stärker zu fordern und ein tieferes Verständnis der Sicherheitsprinzipien zu fördern. Die Implementierung eines Features zur sofortigen Anzeige der richtigen Antworten nach jeder Frage könnte den Lerneffekt weiter verstärken.
Langfristig ist es notwendig, beide Werkzeuge regelmäßig zu aktualisieren, um mit den neuesten Entwicklungen und Bedrohungen im Bereich Cloud-Sicherheit mithalten zu können. Dies würde die Relevanz und Nützlichkeit für die Nutzer sicherstellen. Zudem könnte eine breitere Nutzerbasis durch gezielte Einbindung in weitere Lehrveranstaltungen erreicht werden, was zusätzliches Feedback und kontinuierliche Verbesserungen ermöglichen könnte.
Insgesamt haben die Evaluierung und die erhaltenen Rückmeldungen wertvolle Einblicke in die Stärken und Schwächen der entwickelten Werkzeuge geliefert. Durch zukünftige Verbesserungen können sowohl das Cloud Security Wiki als auch das interaktive Fallbeispiel-Tool weiter optimiert und an die Bedürfnisse der Nutzer angepasst werden, um eine effektive Unterstützung im Bereich der Cloud-Sicherheit zu gewährleiste

Bibliography

[All24] Cloud Security Alliance. STAR. https://cloudsecurityalliance.org/star, 2024. [Online; accessed 5. Jun. 2024].

[AWS24] Inc Amazon Web Services. Was ist SLA? – Service Level Agreement erklärt. https://aws.amazon.com/de/what-is/service-level-agreement, 2024. [Online; accessed 6. Jun. 2024].

[bit24] bitnami. Bitnami LMS powered by Moodle LMS. https://github.com/bitnami/containers/tree/main/bitnami/moodle#how-to-use-this-image, 2024. [Online; accessed 4. Jul. 2024].

[Cen24a] National Cyber Security Center. Service and Deployment Models: NCSC Cloud Security Guidance. https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/service-and-deployment-models, 2024. [Online; accessed 7. Jun. 2024].

[Cen24b] National Cyber Security Center. The Cloud Security Principles: NCSC Cloud Security Guidance. https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles, 2024. [Online; accessed 7. Jun. 2024].

[Cen24c] National Cyber Security Center. Using Cloud Services Securely: NCSC Cloud Security Guidance. https://www.ncsc.gov.uk/collection/cloud/using-cloud-services-securely/using-saas-securely, 2024. [Online; accessed 7. Jun. 2024].

[Cho18] David Chou. Cloud Service Models (IaaS, PaaS, SaaS) Diagram. https://dachou.github.io/2018/09/28/cloud-service-models.html, 2018. [Online; accessed 26. Jun. 2024].

[CIM24] AICPA & CIMA. SOC 2 - SOC for Service Organizations: Trust Services Criteria. https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2, 2024. [Online; accessed 5. Jun. 2024].

[GOV24] GOV. Guidance 1.5 - Considerations for Security Advisors. https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html#threat-model-at-official, 2024. [Online; accessed 4. Jun. 2024].

[IBM24a] IBM. SaaS – Software-as-a-Service. https://www.ibm.com/de-de/topics/saas, 2024. [Online; accessed 3. Jun. 2024].

[IBM24b] IBM. Was ist IaaS (Infrastructure as a Service)? https://www.ibm.com/de-de/topics/iaas, 2024. [Online; accessed 3. Jun. 2024].

[IBM24c] IBM. Was ist Platform-as-a-Service (PaaS)? https://www.ibm.com/de-de/topics/paas, 2024. [Online; accessed 3. Jun. 2024].

[ISO24] ISO. ISO/IEC 27017:2015(en), Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. https://www.iso.org/obp/ui/#iso:std:iso-iec:27017:ed-1:v1:en, 2024. [Online; accessed 5. Jun. 2024].

[Kom24] Europäische Kommission. Datenschutz in der EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_de, 2024. [Online; accessed 5. Jun. 2024].

[Moo24] Moodle.org. Startseite. https://moodle.org, 2024. [Online; accessed 10. Jun. 2024].

[MS19] Narendra Mishra and R K Singh. Taxonomy analysis of cloud computing vulnerabilities through attack vector, cvss and complexity parameter. 2019.

[MUI24] MUI. Material UI components - Material UI. https://mui.com/material-ui/all-components, 2024. [Online; accessed 10. Jun. 2024].

[MYD21] Oumayma Mejri, Dana Yang, and Inshil Doh. Cloud security issues and log-based proactive strategy. 2021.

[Not21] NotSoSecure. Cloud security wiki. https://cloudsecwiki.com, 2021. [Online; accessed 1. Jun. 2024].

[oC24] State of California. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa, 2024. [Online; accessed 5. Jun. 2024].

[Ope24] OpenAI. ChatGPT. https://openai.com/chatgpt/, 2024. [Online; accessed 25. May 2024].

[Sta21] Statista. Cloud Computing - Nutzeranteil der Unternehmen in Europa 2021. https://de.statista.com/statistik/daten/studie/183491/umfrage/nutzung-von-cloud-computing-diensten-in-unternehmen-in-europa, 2021. [Online; accessed 2. Jun. 2024].

[Sta23] Statista. Cloud Computing - Marktanteile Unternehmen 2023. https://de.statista.com/statistik/daten/studie/150979/umfrage/marktanteile-der-fuehrenden-unternehmen-im-bereich-cloud-computing, 2023. [Online; accessed 5. Jun. 2024].

[Sur24] Survio. Umfrage Erstellen. https://www.survio.com/de, 2024. [Online; accessed 10. Jun. 2024].

[Ver24] Vercel. Build and deploy the best web experiences with the Frontend Cloud. `https://vercel.com`, 2024. [Online; accessed 10. Jun. 2024].

[Wit23] WithSecure. Cloud security wiki. `https://www.secwiki.cloud`, 2023. [Online; accessed 1. Jun. 2024].