Hochschule für Technik Stuttgart

Studiengang „Informatik“

Analyse und Vergleich von Compliance-Werkzeugen in Multi-Cloud-Umgebungen

Bachelorarbeit

zur Erlangung des akademischen Grades eines

Bachelor of Science

vorgelegt von

Levi Lübbe

(Mat. Nr. 1000144)

Bearbeitungszeit: von: 17.04.2023 bis 16.07.2023

Betreuer 1: Prof. Dr. Seedorf

Betreuer 2: Dr. Luna Garcia

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952633

Stuttgart, den 16.07.2023

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Abschlussarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder sinngemäß aus den Quellen entnommen wurden, sind als solche kenntlich gemacht. Weiterhin erkläre ich, dass die Arbeit nicht anderweitig veröffentlicht oder an anderer Stelle als Prüfungsleistung vorgelegt wurde.

Stuttgart, den 16.07.2023

Unterschrift

Levi Lübbe
Prof. Dr. Seedorf (HFT), Dr. Luna Garcia (Robert Bosch GmbH)
17.04.2023 – 16.07.2023
Semester IF7, SoSe 2023

Abstract

Analyse und Vergleich von Compliance-Werkzeugen in Multi-Cloud-Umgebungen

Die Cloud ist heutzutage allgegenwärtig. Immer mehr Unternehmen nutzen Multi-Cloud-Umgebungen, um von verschiedenen anbieterspezifischen Funktionen profitieren zu können. Multi-Cloud-Umgebungen stellen Unternehmen vor neue Herausforderungen in Bezug auf Cybersecurity einschließlich Compliance. Cloud Security Posture Management (CSPM)-Werkzeuge werden benötigt, um diese Herausforderungen zu bewältigen. Sie haben die Aufgabe, Konfigurationsfehler, die zu Compliance-Verstößen führen können, zu überwachen und entsprechende Empfehlungen zur Behebung zu bieten. Angesichts der Komplexität und des Umfangs von Multi-Cloud-Umgebungen erweist sich die Auswahl geeigneter CSPM-Werkzeuge als auch die Gewährleistung der Interoperabilität zwischen CSPM-Werkzeugen als schwierig.

Im Rahmen dieser Bachelorarbeit wird ein Framework entwickelt, das Unternehmen bei der Analyse und dem Vergleich von CSPM-Werkzeugen in Multi-Cloud-Umgebungen unterstützen soll. Dazu werden verschiedene Funktionen und Fähigkeiten zum Vergleich von CSPM-Werkzeugen bereitgestellt. Des Weiteren wird eine Fallstudie durchgeführt, welche einen Lösungsansatz für das Problem der Interoperabilität zwischen CSPM-Werkzeugen in der Multi-Cloud-Umgebung aufzeigen soll. Dazu wird ein Kommunikationsstandard definiert, der die Interoperabilität zwischen CSPM-Werkzeugen verbessern soll und Unternehmen dabei unterstützen soll, die Anforderungen der Cybersecurity Compliance besser zu erfüllen.

Die Ergebnisse aus der Analyse des Frameworks zeigen, dass pauschale Empfehlungen für CSPM-Werkzeuge nicht möglich sind, da die Auswahl stark von den individuellen Anforderungen des Unternehmens abhängt. Das Framework bietet jedoch eine gute Entscheidungshilfe für die Auswahl von CSPM-Werkzeugen in Multi-Cloud-Umgebungen und kann durch Weiterentwicklung verbessert und verfeinert werden.

Die Fallstudie hat als Ergebnis einen Kommunikationsstandard hervorgebracht, der als Lösungsansatz für das Interoperabilitätsproblem zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebungen angesehen werden kann. Für eine mögliche Weiterentwicklung dieses Kommunikationsstandards werden die Ergebnisse der Fallstudie dem National Institute of Standards and Technology (NIST) zur weiteren Untersuchung zur Verfügung gestellt.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AICPA ..... American Institute of Certified Public Accountants
APIs ..... Programmierschnittstellen
AWS ..... Amazon Web Services
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
BSI C5 ..... BSI Cloud Computing Compliance Criteria Catalogue
CASB ..... Cloud Access Security Broker
CSPM ..... Cloud Security Posture Management
CWPP ..... Cloud Workload Protection Platform
EISA ..... Enterprise IT Security Architecture
GEC ..... Generic Evidence Collector
IaaS ..... Infrastructure as a Service
IEC ..... International Electrotechnical Commission
ISO ..... International Organization for Standardization
ITL ..... Information Technology Laboratory
NIST ..... National Institute of Standards and Technology
OCI ..... Oracle Cloud Infrastructure
OSCAL ..... Open Security Controls Assessment Language
PaaS ..... Platform as a Service
SaaS ..... Software as a Service
SOC 2 ..... Service Organization Control 2

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Einführung in das Thema

Cloud Computing hat einen Paradigmenwechsel in der IT-Branche eingeleitet, bei dem IT- und Rechenzentren vor Ort durch IT-Ressourcen ersetzt werden, die von großen Cloud-Anbietern bereitgestellt werden. Cloud Computing bietet Unternehmen die Möglichkeit, IT zu mieten, anstatt sie zu kaufen und damit erhebliche Summen in Datenbanken, Software und Hardware zu investieren. Können Unternehmen nun über das Internet oder die Cloud auf die benötigten Cloud Services (Server, Speicher, Datenbanken usw.) zugreifen und bezahlen nur für das, was sie auch nutzen. „Cloud-Computing bietet die Geschwindigkeit, Skalierbarkeit und Flexibilität, die Unternehmen das Entwickeln, Erneuern und Unterstützen von geschäftlichen IT-Lösungen ermöglichen.“ [1]. Diese Aussage unterstreicht die Vorteile von Cloud Computing in Bezug auf die schnelle und flexible Anpassung und Skalierung von IT-Lösungen, wodurch es für Unternehmen einfacher wird, sich an veränderte Geschäftsanforderungen anzupassen. Während früher jedoch ein einziger Cloud-Anbieter alle Geschäftsanforderungen eines Unternehmens erfüllen konnte, benötigen Unternehmen heute mehrere Cloud-Anbieter gleichzeitig (Multi-Cloud), um von verschiedenen Funktionen profitieren zu können. Dadurch entstehen jedoch neue Herausforderungen bei der Gewährleistung der Sicherheit und der Einhaltung von Cybersecurity Standards (Cybersicherheitsstandards) in der Multi-Cloud-Umgebung. Konfigurationsfehler sind die häufigste Form menschlichen Versagens in Cloud-Umgebungen. Multi-Cloud-Umgebungen sind aufgrund ihrer hohen Komplexität besonders anfällig für solche Konfigurationsfehler. Sie entstehen beispielsweise häufig durch mangelnde Transparenz und Sichtbarkeit, insbesondere in Multi-Cloud-Umgebungen kann schnell der Überblick verloren gehen. Konfigurationsfehler stellen ein Risiko für die Cloud-Sicherheit und Cybersecurity Compliance dar. Vor diesem Hintergrund sind Cloud Security Posture Management (CSPM) Werkzeuge, die entwickelt wurden, um den Sicherheitsstatus von Cloud-Umgebungen auf bekannte Sicherheitsrisiken hin zu überwachen, zu bewerten und zu verbessern, eine notwendige Voraussetzung für die Automatisierung von Cybersecurity-Governance-Prozessen (z.B. zur Identifikation von Konfigurationsfehlern und Compliance-Risiken). [1] [2] [3] [4]

CSPM-Werkzeuge stehen jedoch vor einem Problem, wenn sie in Multi-Cloud-Umgebungen eingesetzt werden sollen: die unterschiedlichen Programmierschnittstellen (APIs) und Datenformate, die von den Cloud-Anbietern zur Verfügung gestellt werden. Führen zu einem Mangel an standardisierten Schnittstellen und Datenformaten. Was der Grund für Interoperabilitätsproblemen sein kann, wenn die Informationen der verschiedenen CSPM-Werkzeuge in einem zentralen System vereinheitlicht

werden sollen. Mit dem Ziel, die optimale Sichtbarkeit der von den CSPM-Werkzeugen gefundenen Informationen in der Multi-Cloud-Umgebung zu gewährleisten. [5] [6]

1.2 Zielstellung der Arbeit

Ein Ziel dieser Arbeit ist es, ein Framework bzw. eine Methodik zur Analyse und zum Vergleich von Cloud-Security-Posture-Management (CSPM)-Werkzeugen zu entwickeln, insbesondere im Hinblick auf ihre Fähigkeiten zur automatisierten Überprüfung von Konfigurationsfehlern, Compliance-Verletzungen in Multi-Cloud-Umgebungen. Es soll gezeigt werden, welche enorme Bedeutung die automatisierte Überprüfung von Konfigurationsfehlern und Compliance-Verletzungen für die Cloud Security in Multi-Cloud-Umgebungen hat und wie CSPM-Werkzeuge hier eine Lösung bieten können. Um diesen Vergleich zu gewährleisten, wird im Rahmen dieser Bachelorarbeit ein Framework entwickelt, welches Unternehmen bei der Entscheidung für das passende CSPM-Werkzeug unterstützen soll. Ein weiteres Ziel ist die Entwicklung einer Fallstudie, die eine mögliche Lösung zur Sicherstellung der Interoperabilität zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebungen darlegen soll. Wie bereits in Kapitel 1.1 abgehandelt, kann die fehlende Interoperabilität zwischen CSPM-Werkzeugen ein großes Problem darstellen. Aus diesem Grund ist es wichtig, in dieser Arbeit eine Fallstudie zu erstellen, die einen praktischen Ansatz oder eine Methode zur Verbesserung der Interoperabilität zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebungen aufzeigt. Ziel der Fallstudie ist es, eine allgemeine Methode und einen Lösungsansatz vorzustellen, der die Ergebnisse von CSPM-Werkzeugen verschiedener Anbieter in standardisierter Weise erfasst und verarbeitet. Durch die Fallstudie können konkrete Einblicke in die Umsetzung und Effektivität des gewählten Ansatzes gewonnen werden. Der Ansatz kann dazu beitragen, Sicherheitsüberprüfungen durch CSPM-Werkzeuge in Multi-Cloud-Umgebungen zu verbessern, da durch die verbesserte Interoperabilität die Übersicht über die Multi-Cloud-Umgebung wieder gewonnen werden kann.

1.3 Struktureller Aufbau

Die vorliegende Bachelorarbeit unterteilt sich in sieben Kapitel. Das erste Kapitel gibt dabei eine Einführung in das Thema, die Ziele sowie den strukturellen Aufbau der Bachelorarbeit. Das zweite Kapitel führt den Begriff Cloud Computing ein. Dazu werden die verschiedenen Cloud Deployment Modelle und verschiedene Arten von Cloud Services näher erläutert. Im darauffolgenden Kapitel wird die Cloud Security näher betrachtet, um Einblick in die Bedrohungslage zu gewährleisten und diese dabei mit der Bedeutung der Konfigurationsfehler zu verknüpfen. Im vierten Kapitel werden die Cloud

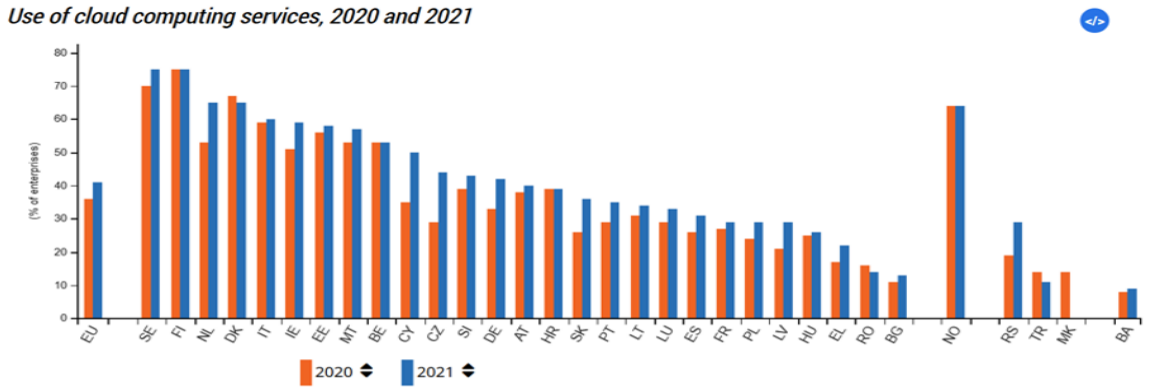
Security Posture Management (CSPM) Werkzeuge und deren Funktion und Fähigkeiten näher betrachtet und anschließend anhand eines Beispiels verdeutlicht. Im fünften Kapitel wird das Framework entwickelt, welches bei der Analyse und dem Vergleich von Cloud Security Posture Management (CSPM)-Werkzeugen unterstützen soll, um eine Hilfestellung bei der Wahl eines geeigneten Werkzeuges zu geben. Im vorletzten Kapitel wird ein Ansatz vorgestellt, der eine standardisierte Kommunikation zwischen APIs und einem zentralen System zur Verarbeitung der Informationen, welche mit CSPM-Werkzeugen gewonnen worden sind, zu ermöglichen. Somit soll die Interoperabilität in der Multi-Cloud-Umgebung sichergestellt werden. Abschließend werden die wichtigsten Punkte der Bachelorarbeit zusammengefasst und die daraus resultierenden Ergebnisse festgehalten. Zudem werden auf Basis der Ergebnisse konkrete Handlungsempfehlungen für Unternehmen ausgesprochen und um auch die Zukunft des Themas nicht auszulassen, wird noch ein Ausblick gegeben.

2 Cloud Computing

Das Kapitel beschäftigt sich mit dem Thema Cloud Computing und gibt dabei eine Einführung in das Thema. Wobei die Bedeutung des Cloud Computing in der heutigen Zeit für Unternehmen erläutert wird und die verschiedenen Cloud Deployment Modelle sowie Cloud Services genauer untersucht werden.

2.1 Einführung in Cloud Computing

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” [7]. Der Cloud-Nutzer muss sich nicht um den Betrieb und die Wartung der Server kümmern. Diese Aufgabe übernimmt der Cloud-Anbieter, der sich auch um die Datensicherung und die Ausfallsicherheit kümmert. Jedoch ist Cloud nicht gleich Cloud. „Moderne Cloud-Lösungen helfen Unternehmen dabei, die Herausforderungen des digitalen Zeitalters zu meistern. Anstatt Zeit und Kosten für die Verwaltung ihrer IT-Infrastruktur aufbringen zu müssen, können Unternehmen mit der Cloud schnell auf einen komplexeren Markt reagieren.“ [1]. Die Abbildung 1 zeigt den Anstieg bei der Nutzung von Cloud Services innerhalb eines Jahres, und zwar im Zeitraum 2020 bis 2021.



(1) Data for 2021: not available yet.
Note: Montenegro: 2020 and 2021 data unreliable. Iceland: 2020 and 2021 data not available
Source: Eurostat (online data code: isoc_cicce_use)

Abbildung 1: Nutzung von Cloud Computing Services, im Jahr 2020 und 2021 (Eigene Darstellung) [8]

2.2 Arten von Cloud Deployment Models

Es gibt verschiedene Ansätze für das Deployment von Cloud-Umgebungen. Im Rahmen des folgenden Kapitels werden die verschiedenen Cloud Deployment Modelle (Public Cloud, Private Cloud, Hybrid-Cloud und Multi-Cloud) vorgestellt. Zudem wird die Frage geklärt, ob die Hybrid-Cloud dasselbe ist wie die Multi-Cloud.

2.2.1 Public Cloud

Große Public Cloud-Anbieter wie Amazon Web Services (AWS), Google Cloud und Microsoft Azure stellen eine Public Cloud bereit, die in der Regel aus IT-Infrastrukturen besteht, die nicht dem Endnutzer gehören. In der Vergangenheit wurden Public Clouds ausschließlich „Off-Premise" betrieben. Dies ist heute jedoch nicht mehr Stand der Technik: Cloud-Anbieter erbringen solche Services vor Ort, d. h. „On-Premise" in den Rechenzentren ihrer Kunden. Aus diesem Grund spielen der Standort und die Eigentumsverhältnisse der Cloud heute keine Rolle mehr, während sie in der Vergangenheit wichtige Argumente waren. Beispiele für kostenlose Services aus der Public Cloud sind Webmail-Services oder das bekannte Google Docs sowie kostenpflichtige Services wie Microsoft 365 oder SAP Business by Design diese Services sind somit für jeden über das Internet zu erreichen. [9] [10]

Die Abbildung 2 soll hierbei das Prinzip der Public Cloud anhand eines Beispiels verdeutlichen.

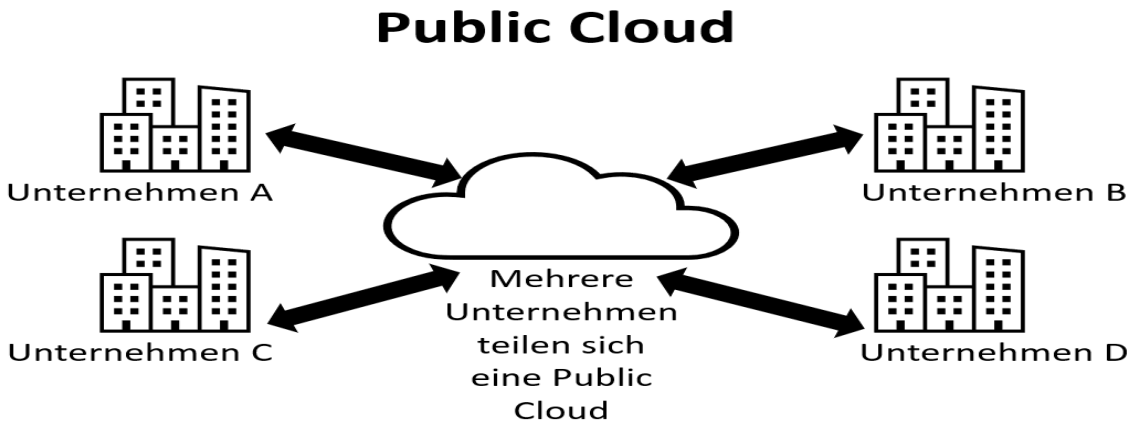


Abbildung 2: Public Cloud (Eigene Darstellung) [11]

2.2.2 Private Cloud

Die Private Cloud hingegen bietet die Möglichkeit, die Infrastruktur komplett für sich zu beanspruchen, wie in der Abbildung 3 zu sehen. Der Endbenutzer oder eine Nutzergruppe muss sich diese also nicht mit anderen teilen. In der Regel werden diese hinter der Firewall dieses Nutzers oder dieser Nutzergruppe ausgeführt. Private Clouds müssen nicht länger auf lokalen IT-Infrastrukturen basieren. Heute können Unternehmen Public Clouds in gemieteten Off-Premise-Rechenzentren eines Cloud-Anbieters aufbauen, sodass Argumente wie Standort und Eigentum auch bei Private Clouds an Bedeutung verlieren. [9]

Die Abbildung 3 zeigt hierbei das Prinzip einer Private Cloud an einem Beispiel auf.

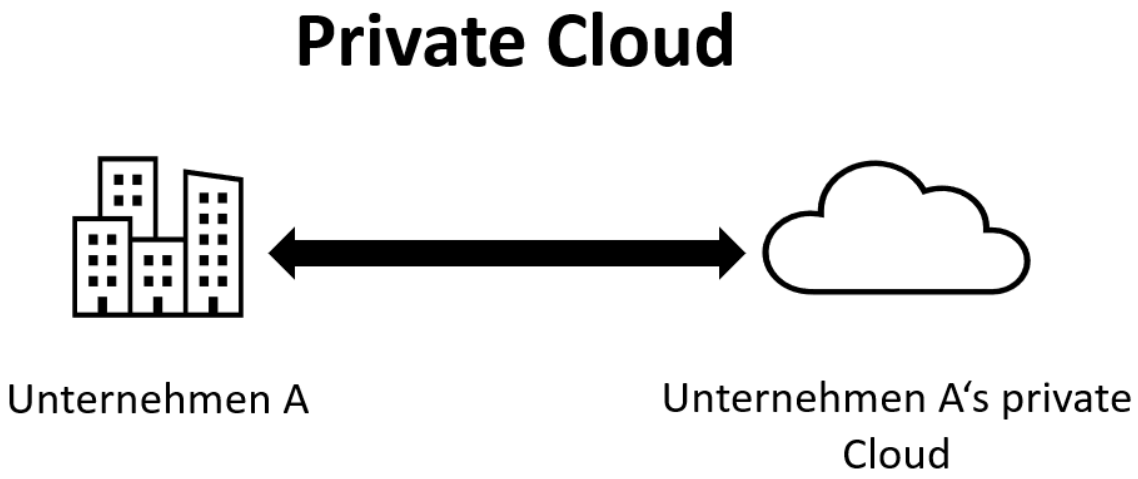


Abbildung 3: Private Cloud (Eigene Darstellung) [11]

2.2.3 Hybrid-Cloud

„Hybrid-Cloud-Lösungen umfassen Anwendungen oder ihre Komponenten wie Computing, Netzwerke und Speicher, wenn sie in öffentlichen und privaten Clouds bereitgestellt werden. Lokale Server werden oft auch als private Clouds bezeichnet.“ [12]. Da heutzutage kaum ein Unternehmen nur eine einzige Cloud nutzt, sind Hybrid-Cloud-Umgebungen weit verbreitet. Die Hybrid-Cloud-Lösungen funktionieren dabei wie folgt. In Hybrid-Cloud-Umgebungen lassen sich die Arbeitslasten zwischen den verschiedenen Cloud-Umgebungen verschieben und verwalten. Ein IT-System ist eine Hybrid-Cloud, wenn Anwendungen grenzenlos über mehrere getrennte, aber miteinander verbundene Umgebungen verschoben werden können. Die Hauptgründe für Unternehmen, sich für eine Hybrid-Cloud zu entscheiden, sind die Reduzierung von Kosten und Risiken sowie die Möglichkeit, bestehende Funktionen zu erweitern, größere Flexibilität, schnellere Entwicklung von Innovationen, verbesserte Leistung und geringere Latenzzeiten. Dies ermöglicht Unternehmen eine einfache Auf- und Abwärtsskalierung je nach Bedarf, so dass beispielsweise neue Technologien einfacher integriert werden können, ohne dass die Infrastruktur entsprechend erweitert oder gar ersetzt werden muss. [9] [12] [13]

Abbildung 4 zeigt ein Beispiel für eine Hybrid-Cloud.

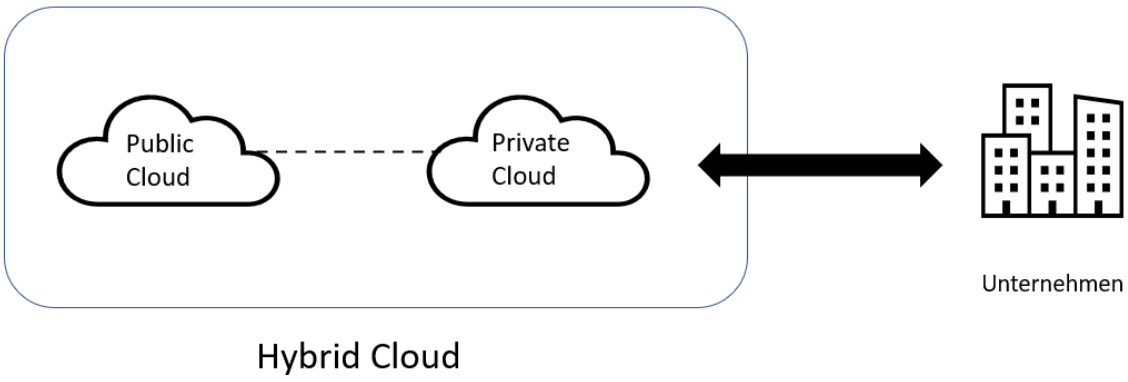


Abbildung 4: Hybrid-Cloud (Eigene Darstellung) [14]

2.2.4 Multi-Cloud

„„Multi-Cloud“ bezieht sich auf die Kombination und Integration mehrerer öffentlicher Clouds.“ [15]. Aus der Sicht des Nutzers handelt es sich dabei um eine einzige Cloud, die Multi-Cloud vereint jedoch Cloud Services und Clouds verschiedener Cloud-Anbieter. „Das Konzept lässt sich am besten anhand einer Analogie aus dem Supermarkt erklären. Wenn Kunden zum Beispiel ihre Lieblingsbioprodukte in einem Naturkostladen kaufen, nehmen sie in Kauf, dass die Preise etwas höher sind. Für die meisten Grundnahrungsmittel gehen sie jedoch lieber in ein normales Geschäft, da die Preise dort viel niedriger sind. Kurz gesagt, sie optimieren ihren Lebensmitteleinkauf auf der Grundlage des individuellen Angebots und der Preise der einzelnen Geschäfte, was einer Multi-Cloud-Strategie ähnelt.“ [6]. Dies hat zur Folge, dass Services, Anwendungen und Infrastrukturen auf verschiedene Cloud-Anbieter verteilt werden können, sodass parallel und unabhängig von einzelnen Cloud-Anbietern gearbeitet werden kann und die besten Services und Preise der verschiedenen Cloud-Anbieter für die jeweilige Anwendung ausgewählt werden können. Darüber hinaus wird durch die Verteilung der Service auf verschiedene Cloud-Anbieter eine gewisse Ausfallsicherheit erreicht. Beim Ausfall eines Cloud-Anbieter ist man also nicht völlig aufgeschmissen, da die anderen Cloud-Anbieter in der Regel nicht ebenfalls ausfallen. Viele Unternehmen bewegen sich bereits in Richtung Multi-Cloud-Umgebungen. Mit dieser Entwicklung nehmen auch die damit verbundenen Sicherheitsprobleme zu. [6] [16]

Ein vereinfachtes Architekturmodell der Multi-Cloud ist in der Abbildung 5 zu sehen. Wobei verschiedene Public Cloud Anbieter vom Unternehmen genutzt werden.

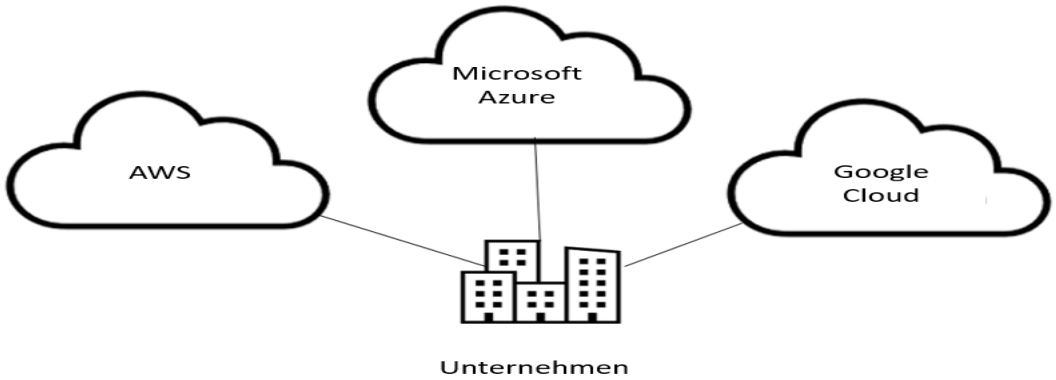


Abbildung 5: Multi-Cloud Beispiel (Eigene Darstellung)

2.2.5 Ist die Hybrid-Cloud dasselbe wie die Multi-Cloud?

Obwohl die Begriffe Hybrid-Cloud und Multi-Cloud häufig in einem Zusammenhang verwendet werden, sind sie nicht identisch. Eine Hybrid-Cloud umfasst mehrere miteinander verbundene Public- und Private Clouds, die sowohl Daten als auch Prozesse gemeinsam nutzen, um die gleiche Aufgabe zu erledigen. Im Gegensatz dazu nutzt eine Multi-Cloud Dienste aus mehreren Public Clouds, um verschiedene Aufgaben unabhängig von ihrem Hosting-Standort auszuführen. Dabei ist jedoch zu beachten, dass auch eine Hybrid-Cloud als Multi-Cloud betrachtet werden kann, wenn sie Ressourcen aus einer Private Cloud und Ressourcen von mindestens zwei Public Cloud Anbietern enthält. Zusammenfassend kann also gesagt werden, dass Multi-Cloud-Lösungen zwar Hybrid-Cloud-Lösungen beinhalten, eine Hybrid-Cloud aber nicht automatisch als Multi-Cloud betrachtet werden kann. [12]

Es gibt nicht nur verschiedene Cloud Deployment Models, sondern auch verschiedene Cloud Services. Welche Arten von Cloud Services es gibt, wird im folgenden Kapitel näher erläutert.

2.3 Cloud Services

Dieses Kapitel befasst sich mit den unterschiedlichen Cloud Services.

2.3.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) ist ein Pay-as-you-go-Service. Cloud-Anbieter ermöglichen ihren Kunden den Zugriff auf Speicher- und Netzwerkkomponenten, Server und andere IT-Ressourcen über die Cloud oder das Internet. Dies ist ein sehr interessantes Modell für Cloud-Nutzer, die eine Infrastruktur benötigen, sich aber nicht selbst um deren Wartung und Aktualisierung kümmern möchten. Die benötigten Komponenten können flexibel beschafft und je nach Bedarf hoch oder runter skaliert werden. Die Betriebskosten sind gering, da die sonst anfallenden Anschaffungs- und Wartungskosten entfallen. Beispiele für IaaS umfassen verschiedene Public Cloud-Anbieter. [17]

2.3.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) ist eine Möglichkeit für Nutzer, über das Internet auf eine Plattform in Form einer integrierten Lösung eines Lösungspakets oder eines Services zuzugreifen, wobei der Cloud-Anbieter das Hosting der Hard- und Software in der eigenen Infrastruktur übernimmt und diese den Nutzern in Form einer Plattform zur Verfügung stellt. Diese Lösung dient in erster Linie der Entwicklung und Programmierung von Anwendungen und ermöglicht dem Nutzer auch deren Verwaltung und Ausführung. Allerdings ohne den Aufbau und die Verwaltung der für diese Prozesse notwendigen Infrastruktur. „Mit PaaS können Entwicklungsteams ein Framework erstellen, auf dem sie ihre webbasierten Anwendungen erstellen und anpassen können. Entwicklerinnen und Entwickler können für ihre Anwendungen auf integrierte Softwarekomponenten zurückgreifen. Dadurch wird die Menge an Code reduziert, den sie selbst schreiben müssen.“ [17]. AWS Elastic Beanstalk, Heroku und Red Hat OpenShift sind Beispiele für PaaS-Produkte. [17]

2.3.3 Software as a Service (SaaS)

„SaaS (Software-as-a-Service), auch als Cloud Application Services bezeichnet, ist die umfassendste Form von Cloud-Computing-Services und stellt eine komplette Anwendung, die vom Anbieter verwaltet wird, über einen Webbrowser bereit.“ [17]. Die großen Vorteile von SaaS-Anwendungen

bestehen darin, dass die gesamte Wartung der Software und die Behebung potenzieller Fehler von den Anbietern übernommen werden. Die Benutzer der Anwendung stellen die Verbindung über ein Dashboard oder eine Programmierschnittstelle (API) her. Auf diese Weise muss die Anwendung nicht auf den einzelnen Geräten installiert werden, was den Gruppenzugriff auf die Anwendung erleichtert. Beispiele für SaaS-Anwendungen, mit denen jeder schon mal zu tun hatte, sind webbasierte Services für E-Mail-Konten wie Google Mail oder Outlook. [17]

Die Abbildung 6 zeigt, wie die Verwaltung zwischen den Cloud-Anbietern (Rot) und den Nutzern (Blau) aufgeteilt ist.

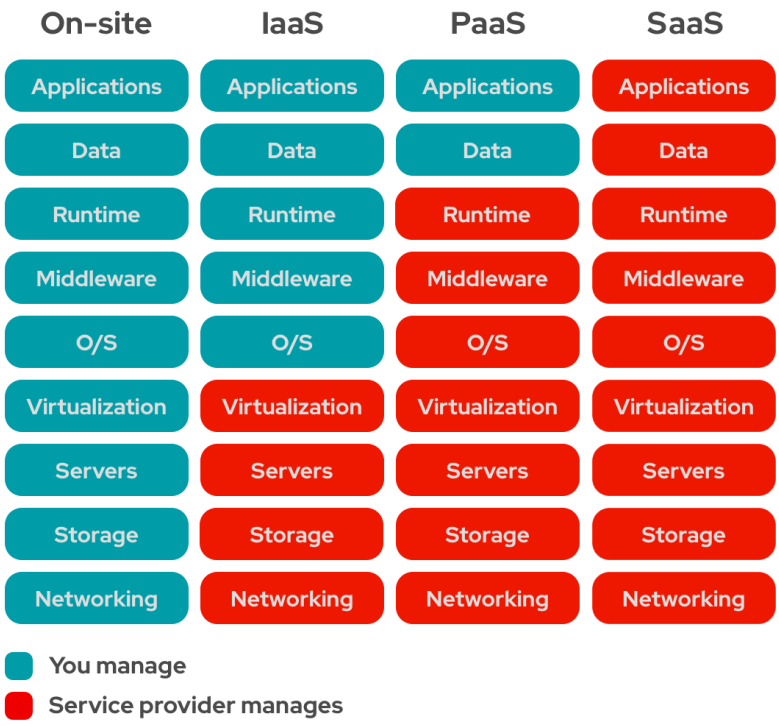


Abbildung 6: IaaS, PaaS und SaaS Diagramm [17]

3 Cybersecurity Compliance in Multi-Cloud-Umgebungen

„Mit der Weiterentwicklung der digitalen Landschaft haben sich auch die Sicherheitsrisiken verschärft. Die Bedrohungen sind explizit auf Cloud-Computing-Anbieter ausgerichtet, da die Unternehmen insgesamt keinen Überblick über Datenzugriff und Datenbewegungen haben.“ [18]. Für Unternehmen ist es daher von großer Bedeutung, im Rahmen der Cybersecurity Compliance zu prüfen, ob die Cloud-Anbieter Cybersecurity Standards für die Cloud Security implementiert haben.

3.1 Cloud Security

Unter Cloud Security versteht man eine Reihe von Prozessen und Technologien, die mit dem Ziel entwickelt wurden, externe und interne Bedrohungen abzuwehren. Die Cloud Security ist für Unternehmen von entscheidender Bedeutung, wenn sie die Cloud und ihre Werkzeuge und Services nutzen möchten. Um die Bedeutung der Cloud Security zu verstehen, ist es wichtig, die unterschiedlichen Bedrohungen zu verstehen, denen Unternehmen in der Cloud ausgesetzt sind. [18]

Bedrohungen in der Cloud:

Unzureichendes Identitäts-, Berechtigungs-, Zugangs- und Schlüsselmanagement:

Das Identitäts-, Berechtigungs-, Zugriffs- und Schlüsselmanagement umfasst Werkzeuge, mit denen Unternehmen den Zugriff auf geschäftskritische Ressourcen verwalten, überwachen und absichern können. Beispiele für diese geschäftskritischen Ressourcen können Dateien, Computersysteme, aber auch physische Ressourcen wie Serverräume oder Gebäude sein. [19]

Unsichere Schnittstellen und APIs:

Die Absicherung von Schnittstellen hat enorm an Bedeutung gewonnen, da die Verwendung von APIs in den letzten Jahren immer populärer geworden ist. Dies hat zur Folge, dass auch die Schnittstellen intensiv auf mögliche Fehlkonfigurationen, schlechte Codierung, absente Authentifizierung und inadäquate Autorisierungen überprüft werde müssen. Wenn das Unternehmen bei der Sicherung der Schnittstellen nicht aktiv wird, kann dies dazu führen, dass die Schnittstellen anfällig für Angriffe von Cyberkriminellen werden. Einige Beispiele für häufige Schwachstellen an Schnittstellen sind nicht authentifizierte Endpunkte, unzureichende Authentifizierung und zu hohe Berechtigungen. [19]

Fehlkonfigurationen und Unzureichende Änderungskontrollen:

Unter Fehlkonfigurationen versteht man die falsche oder unsachgemäße Konfiguration von Computersystemen. Fehlkonfigurationen können verschiedene Ursachen haben, z. B. mangelnde Systemkenntnisse, fehlendes Verständnis für notwendige Sicherheitseinstellungen, aber auch böswillige Absichten können zu Fehlkonfigurationen führen. Diese Fehlkonfigurationen können Systeme sowohl für unbeabsichtigte Schäden als auch für externe oder interne Angreifer verwundbar machen. Fehlkonfigurationen treten in verschiedenen Situationen auf, in denen entweder unsichere Datenspeicher, Container, veraltete oder Standardanmeldeinformationen verwendet werden. Aber auch die Nichtanpassung der werkseitigen Standardkonfiguration kann zu Fehlkonfigurationen führen. Um nur einige wenige Beispiele für fehlerhafte Konfigurationen zu nennen. [19]

Mangelnde Cloud Security Architektur und Strategie:

Der Entwurf einer umfassenden Cloud Security Strategie und -architektur erfordert eine sorgfältige Abwägung und Auswahl der verschiedenen Komponenten, einschließlich der in Kapitel 2.2, Kapitel 2.3, Cloud-Anbieter, Service Verfügbarkeitszonen sowie der allgemeinen Prinzipien und vordefinierten Richtlinien beschriebenen Komponenten. Durch eine vorausschauende Gestaltung von Identitäts- und Zugriffsmanagement, Netzwerk- und Sicherheitskontrollen über verschiedene Cloud-Knoten, Anbieter, Services und Umgebungen hinweg können völlig neue Gestaltungsmöglichkeiten erschlossen werden. Aus diesem Grund sollten strategische Überlegungen dem Planungsprozess vorausgehen und ihn leiten, auch wenn in der Praxis die einzigartigen Herausforderungen der Cloud eine schrittweise und anpassungsfähige Planungsstrategie erfordern. [19]

Dies sind nur einige repräsentative Bedrohungen, denen Unternehmen in der Cloud ausgesetzt sind, wobei die Bedrohung durch Fehlkonfigurationen besonders ins Auge sticht. Die Anfälligkeit der Cloud für Konfigurationsfehler wurde bereits in Kapitel 1.1 als besondere Bedrohung für die Cloud Security und Cybersecurity Compliance herausgestellt. Unternehmen sollten sich bei der Migration in die Cloud immer bewusst sein, dass mit den Vorteilen der Cloud auch immer Bedrohungen einhergehen. Daher ist es unerlässlich, entsprechende Gegenmaßnahmen zu ergreifen, Cybersecurity Standards zur Einhaltung der Cybersecurity Compliance zu implementieren und somit über eine durchdachte Cloud Security Strategie verfügen. Im Folgenden werden einige Maßnahmen näher beleuchtet. [18]

Ein weiterer wichtiger Aspekt, den kein Unternehmen im Zusammenhang mit den Bedrohungen der Cloud Security vernachlässigen sollte, ist ein Incident Response Plan bzw. ein Incident Response Team, das diesen Plan umsetzt. Der Plan hilft Unternehmen, die Dauer und den Schaden von Sicherheitsvorfällen zu minimieren. Darüber hinaus ermöglicht der Incident Response Plan betroffene Stakeholder zu identifizieren, die digitale Forensik zu unterstützen, die Wiederherstellung zu beschleunigen und unter Umständen negative Publicity und die Abwanderung von Kunden zu vermeiden. „Unternehmen mit einem Reaktionsteam, das seinen Reaktionsplan überprüft, verzeichneten durchschnittlich um 2,66 Mio. USD niedrigere Kosten pro Datenschutzverletzung als Unternehmen ohne Reaktionsteam und ohne solche Überprüfungen. Die Differenz von 3,26 Mio. USD gegenüber 5,92 Mio. USD entspricht Einsparungen in Höhe von 58 %“. [20]. Es ist zwar nicht möglich, alle Bedrohungen zu eliminieren, aber mit einem Incident Response Plan ist es möglich, die größten Risiken für die allgemeine Cybersecurity zu minimieren. [21]

3.2 Cybersecurity Compliance

„Die Einhaltung von Cybersicherheitsstandards ist eine Reihe von Normen, die Unternehmen und Organisationen befolgen müssen, um als "konform" zu gelten. Diese Standards können je nach Art des Unternehmens oder der Organisation variieren, umfassen aber im Allgemeinen Richtlinien, Verfahren und Kontrollen, die sicherstellen, dass ein Unternehmen sich vor Cyberangriffen schützt.“ [22] Um eine gute Cybersecurity Compliance zu gewährleisten, greifen Unternehmen auf eine Vielzahl von Werkzeugen und Prozessen zurück, wobei es insbesondere für die Cybersecurity Compliance in Multi-Cloud-Umgebungen erforderlich ist automatisierte Überprüfungen durchzuführen. Die Vorteile der Automatisierung liegen auf der Hand: Höhere Genauigkeit durch weniger menschliche Fehler, schnellere Reaktion auf Bedrohungen durch weniger manuelle Überprüfungen und darüber hinaus eine bessere Sammlung und Analyse von Compliance-relevanten Daten sind nur einige der Vorteile, die mit der Automatisierung verbunden sind. So können Compliance-Verstöße frühzeitig erkannt, aufgeklärt oder verhindert werden, bevor das Unternehmen mit schwerwiegenden Konsequenzen wie Strafverfolgung, Bußgeldern oder einem gravierenden Reputationsschaden konfrontiert wird. [23] [24]

Nachfolgend sind einige gängige Cybersecurity Standards sowie ein interner Standard der Robert Bosch GmbH aufgeführt, diese Standards wurden aufgrund ihrer Relevanz für die Cybersecurity ausgewählt.

ISO/IEC 27001:

Diese Norm ist ein international anerkannter Standard für das Informationssicherheitsmanagement. Der Standard umfasst eine Vielzahl von Anforderungen, welche für die Implementierung, Überwachung, Bewertung und Verbesserung von Informationssicherheits-Managementsystemen wichtig sind. Die Zertifizierung nach International Organization for Standardization (ISO [25])/**I**nternational **E**lectrotechnical **C**ommission (IEC [26]) 27001 gilt als Nachweis, dass Unternehmen ein System implementiert haben, welches dazu dient, die Risiken im Hinblick auf die Sicherheit der Daten, die sich im Besitz des Unternehmens befinden oder von ihm verarbeitet werden, zu managen. Dabei ist sicherzustellen, dass das System alle in ISO/IEC 27001 festgelegten Verfahren und Grundsätze einhält. [27]

BSI C5:

Der Kriterienkatalog vom Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue (BSI C5) enthält die für Cloud-Services nötigen Mindestanforderungen der Informationssicherheit, welche es nicht zu unterschreiten gilt. Das Ziel, welches mit dem BSI C5 Standard verfolgt wird, ist es, auf Grundlage einer standardisierten Überprüfung eine transparente Darstellung der Informationssicherheit eines Cloud Services zu ermöglichen. Durch die Umsetzung der im BSI C5 festgelegten Mindestanforderungen können Cloud-Anbieter die Sicherheit ihrer Cloud Services verbessern und sich zudem die Einhaltung der Mindestanforderungen durch einen Auditor bestätigen lassen. [28]

NIST 800-53:

NIST 800-53 ist ein Sicherheitsstandard, der durch das National Institute of Standards and Technology (NIST) unter Berücksichtigung der vom Information Technology Laboratory (ITL) geforderten Mindestkontrollstandards entwickelt wurde. Dabei umfasst der Standard einen Katalog von Sicherheitskontrollen und Datenschutzkontrollen für Informationssysteme oder Organisationen. Die Organisationen können sich dazu Entscheiden, die im Standard beschriebenen Maßnahmen und Empfehlungen anzunehmen und umzusetzen, um dem Federal Information Security Modernization Act (FISMA) zu entsprechen. Dadurch können die Organisationen ihre eigene Cybersecurity optimieren. [29] [30]

SOC 2:

Service Organization Control 2 (SOC 2) ist ein Sicherheitsstandard, der vom amerikanischen Berufsverband der Wirtschaftsprüfer, dem American Institute of Certified Public Accountants (AICPA), entwickelt wurde. Mithilfe dieses Standards können Service-Organisationen Compliance, Berichte über den Status der grundlegenden Prinzipien (Datenschutz, Sicherheit, Verfügbarkeit, Vertraulichkeit und Prozessintegrität) erstellen. Unternehmen können sich durch das Einhalten dieser Grundprinzipien von externen Auditoren des AICPA bestätigen lassen und bei Erfolgreichem bestehen, erhalten sie die SOC 2-Zertifizierung. [31] [32]

Bosch EISA:

Bei der Bosch Enterprise IT Security Architecture (EISA) handelt es sich um einen Bosch internen Standard, welcher ein einheitliches Verständnis und eine konsistente Implementierung der IT-Sicherheit zum Ziel hat. Dabei soll der EISA-Standard den Grad der Einhaltung von internen und externen Vorschriften wie beispielsweise ISO/IEC 27001 und NIST 800-53 verbessern. [33]

Im Rahmen der Cybersecurity Compliance ist es enorm wichtig zu verstehen, dass es sich bei der Einhaltung von Cybersecurity Standards um einen fortlaufenden Prozess handelt, der eine kontinuierliche Überwachung erfordert. Dabei müssen die Kontrollen und Sicherheitsmaßnahmen, welche für die Überprüfung der Einhaltung von Cybersecurity Standards verwendet werden, ständig auf ihre Angemessenheit überprüft werden. [34]

3.3 Technische Anforderungen für die Cybersecurity Compliance in Multi-Cloud-Umgebungen

Auch wenn die Nutzung von Multi-Cloud-Umgebungen aus geschäftlicher Sicht sinnvoll ist, kann sie die Anstrengungen zur Gewährleistung von Sicherheit und Cybersecurity Compliance erheblich erschweren. Aus diesem Grund ist es für Unternehmen besonders wichtig, sicherzustellen, dass sie die geltenden Cybersecurity Standards einhalten, um die Integrität und Vertraulichkeit von Daten in Multi-Cloud-Umgebungen zu gewährleisten. Sowohl die technischen Anforderungen als auch die organisatorischen Anforderungen zur Einhaltung der Cybersecurity Standards sind daher von entscheidender Bedeutung. Diese Arbeit beschäftigt sich jedoch ausschließlich mit den technischen Anforderungen. [6] [35]

Zu Beginn ist es enorm wichtig für Unternehmen, dass sie das Prinzip des Shared Responsibility Model verstanden haben. Das Shared Responsibility Model beschreibt die geteilte Sicherheitsverantwortung zwischen Cloud-Anbietern und den Kunden, die diese Cloud-Anbieter nutzen. Das Modell legt also fest, wer für welche Sicherheitsaspekte verantwortlich ist. Abbildung 7 zeigt die Aufteilung der Verantwortlichkeiten zwischen dem Kunden (Customer) und dem Cloud-Anbieter, in diesem Fall AWS. AWS ist für die Sicherheit in der Cloud verantwortlich, d. h. für den Schutz der Infrastruktur, auf der die AWS Cloud Services ausgeführt werden, wie Hardware, Software, Netzwerke und Einrichtungen. Die Verantwortung des Kunden für die Sicherheit in der Cloud hängt stark davon ab, welche AWS Cloud Services der Kunde wählt. Kunden müssen sich um die Sicherheitskonfiguration kümmern. Beispielsweise müssen sich Kunden bei IaaS-Services um das Sicherheitsmanagement des Betriebssystems, der Anwendungssoftware, der Firewall-Konfiguration und weitere Aspekte kümmern. Bei anderen Services muss sich der Kunde um zusätzliche Aspekte der Sicherheit kümmern. [36]

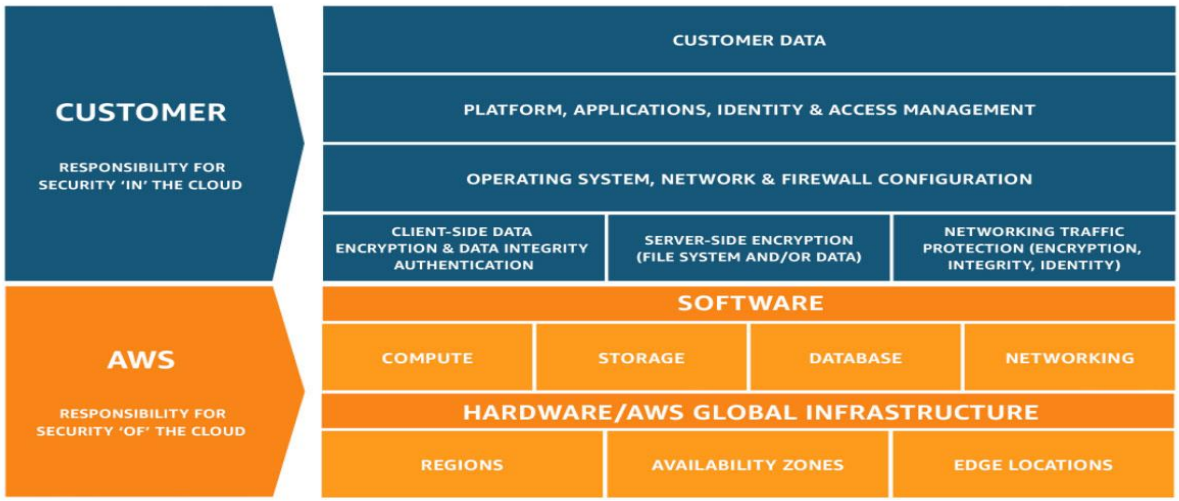


Abbildung 7: Shared Responsibility Model [36]

Um sicherzustellen, dass die technischen Anforderungen zur Einhaltung von Cybersecurity Standards erfüllt werden, müssen Unternehmen eine Reihe von Aspekten berücksichtigen. Zunächst sollten Unternehmen sicherstellen, dass die Cloud-Anbieter, für die sie sich entscheiden, die geltenden Cybersecurity Standards einhalten. Einige Beispiele für die verschiedenen Cybersecurity Standards wurden bereits im Kapitel 3.2 behandelt. Unternehmen sollten Cloud-Anbieter auf diese Cybersecurity Standards hin überprüfen und feststellen, ob entsprechende Zertifizierungen vorliegen. Auch die Frage, ob Cloud-Anbieter das Hinzufügen oder Anpassen eigener Standards ermöglichen, sollte im Rahmen dieser Überprüfung geklärt werden. Eine solche Absicherung ist nicht nur für die eigene Sicherheit relevant, sondern insbesondere auch für die Außenwirkung gegenüber Kunden und

Geschäftspartnern sowie für die Festigung des Vertrauensverhältnisses zwischen Cloud-Anbietern und Cloud-Nutzern wichtig. So können sie sicher sein, dass ihre Daten vertraulich behandelt werden. [37] [38]

Eine solide Sicherheitskonfiguration ist unerlässlich, um potenzielle Sicherheitslücken zu schließen oder gar nicht erst entstehen zu lassen und so eine starke Abwehr gegen Bedrohungen zu gewährleisten. Dies ist besonders wichtig im Zusammenhang mit der Einhaltung von Cybersecurity Standards. Ein solides Konfigurationsmanagement legt einen wichtigen Grundstein für eine sichere Multi-Cloud-Umgebung und trägt zur Einhaltung von Cybersecurity Standards bei. Abbildung 8 verdeutlicht den Zusammenhang zwischen einer soliden Sicherheitskonfiguration und der Einhaltung von Cybersecurity Standards. Durch die Konfiguration von Zugriffskontrollen, Verschlüsselung, Netzwerkeinstellungen, Firewalls und anderen sicherheitsrelevanten Aspekten können Unternehmen sicherstellen, dass sie bereits bei der Konfiguration den Grundstein für eine sichere Cloud-Umgebung legen. Die Komplexität von Multi-Cloud-Umgebungen macht die Aufgabe, solide Sicherheitskonfigurationen zu implementieren, nicht einfacher, sondern stellt Unternehmen vor noch größere Herausforderungen, da die verschiedenen anbieterspezifischen Sicherheitskonfigurationen korrekt konfiguriert werden müssen. Daher ist es wichtig, geeignete Compliance-Werkzeuge und -Methoden einzusetzen, um die Sicherheitskonfigurationen effektiv zu überwachen und sicherzustellen, dass sie den relevanten Cybersecurity Standards entsprechen. [39]

Darüber hinaus sollten Unternehmen sicherstellen, dass sie geeignete Sicherheitskontrollen in ihrer Multi-Cloud-Umgebung implementieren, dazu gehören zum einen Maßnahmen zur Erhöhung der Perimetersicherheit in der Multi-Cloud-Umgebung durch Netzwerksegmentierung und Datenklassifizierung, Datenverschlüsselung und Identitäts- und Zugriffsmanagement. Eine der wichtigsten Sicherheitskontrollen ist die automatisierte Überwachung von Sicherheitskonfigurationen mit einem CSPM-Werkzeug, dabei handelt es sich um ein Werkzeug zur automatisierten Überwachung, welches näher in Kapitel 4.1 erläutert wird. Dabei vergleichen CSPM-Lösungen die Cloud-Anwendungskonfigurationen mit Cybersecurity Standards und eliminieren so einerseits Sicherheitsrisiken und sorgen andererseits für eine schnellere Bereitstellung. Verstöße werden in Echtzeit erkannt und können direkt behoben werden, für die Korrektur von Konfigurationsfehlern stehen geführte Korrekturmöglichkeiten und Leitlinien zur Fehlervermeidung zur Verfügung. Die CSPM-Lösungen werden im Detail im Kapitel 4.1 behandelt. Sicherheitskontrollen sind in Multi-Cloud-Umgebungen besonders wichtig, da sie von Natur aus sehr komplex sind, was auch die Überwachung erheblich erschwert. Aus diesem Grund müssen die Sicherheitskontrollen an die genauen Anforderungen der Multi-Cloud-Umgebung und die geltenden Cybersecurity Standards angepasst

werden. Mit Hilfe der implementierten Sicherheitskontrollen kann der Schutz der Multi-Cloud-Umgebung am besten gewährleistet werden. [40] [41]

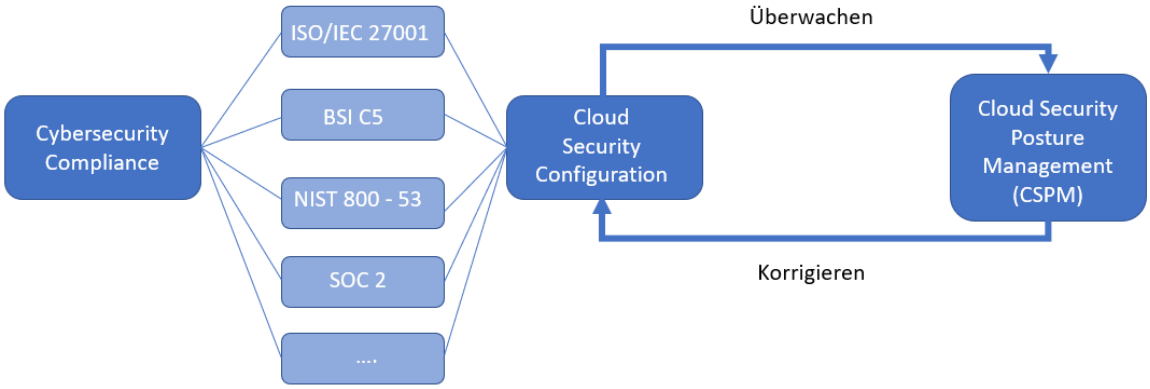


Abbildung 8: Zusammenhang der Relevanten Komponenten (Eigene Darstellung)

Durch die Implementierung dieser Anforderungen können Unternehmen die Cybersecurity Compliance mit den geltenden Cybersecurity Standards sicherstellen und ihre Multi-Cloud-Umgebung sicher und geschützt halten.

3.4 Herausforderungen bei der Cybersecurity Compliance und Interoperabilität in Multi-Cloud-Umgebungen

Die Einhaltung der Cybersecurity Compliance und die Interoperabilität stellen in Multi-Cloud-Umgebungen eine besondere Herausforderung dar. Unternehmen können Schwierigkeiten damit haben, eine kohärente Compliance-Strategie in der Multi-Cloud-Umgebung umzusetzen, wenn sie nicht darauf achten, von Anfang an standardisierte Sicherheitskontrollen und Cybersecurity Standards in allen Bereichen der Multi-Cloud-Umgebung zu nutzen. Wenn es nicht möglich ist, die Sicherheitskontrollen und Überprüfungen von Cybersecurity Standards in einem zentralen System darzustellen, führt dies zu den folgenden Herausforderungen. Durch die Nutzung verschiedener CSPM-Werkzeuge kann es dazu führen, dass Unternehmen den zentralen Überblick über den Sicherheitsstatus der Multi-Cloud-Umgebung verlieren. Hohe Kosten, die auf das Unternehmen wegen der Nutzung der verschiedenen CSPM-Werkzeuge zukommen können. Die Verwaltung und Konfiguration der verschiedenen CSPM-Werkzeuge können sich als komplexe Aufgaben herausstellen. Es muss sichergestellt werden, dass jedes Werkzeug die entsprechenden Sicherheitskontrollen und

Compliance-Prüfungen durchführt. Um diesen Überblick wieder zu gewinnen, ist es deshalb umso wichtiger, dass die Interoperabilität in Multi-Cloud-Umgebungen hergestellt wird. Interoperabilität in Multi-Cloud-Umgebungen ist von großer Bedeutung, damit Systeme effizient und effektiv über verschiedene Cloud-Plattformen hinweg zusammenarbeiten können. Im Wesentlichen erfordert Interoperabilität in Multi-Cloud-Umgebungen gemeinsame Prozesse, APIs, Container und Datenmodelle. Damit die Kommunikation zwischen den verschiedenen Anwendungskomponenten auf unterschiedlichen Cloud-Plattformen gewährleistet werden kann. Dabei verfolgen Unternehmen mit der Interoperabilität in Multi-Cloud-Umgebungen drei Hauptziele: Zuverlässigkeit, Leistung und Sicherheit. Während die Zuverlässigkeit und Leistung notwendig dafür sind die maximale Systemleistung aufrechtzuhalten, spielt die Sicherheit eine wichtige Rolle beim Versuch der Aufrechterhaltung der Ausfallsicherheit von verschiedenen Cloud-Plattformen zu gewährleisten. [5] [6]

Unter den vorgestellten Herausforderungen liegt der Schwerpunkt im weiteren Verlauf auf der Interoperabilität jedoch vorab das folgende Kapitel zu den CSPM-Werkzeugen, welche eine wichtige Rolle bei der Lösung des Interoperabilitätsproblems spielen werden.

4 Compliance-Werkzeuge in Multi-Cloud-Umgebungen

Dieses Kapitel befasst sich mit der Rolle von Compliance-Werkzeugen, insbesondere von CSPM-Werkzeugen, bei der Einhaltung von Sicherheits- und Cybersecurity Compliance in Multi-Cloud-Umgebungen. Es werden die verschiedenen Funktionen und Fähigkeiten (Capabilities) von CSPM-Werkzeugen näher erläutert, da sie wichtig für Kapitel 5 sind. Außerdem wird ein konkretes Beispiel behandelt, um die praktische Anwendung in der Realität zu veranschaulichen.

4.1 Cloud Security Posture Management (CSPM)-Werkzeuge

Cloud Security Posture Management (CSPM)-Werkzeuge sind für die kontinuierliche und automatisierte Überwachung der Cloud-Umgebung auf Konfigurationsfehler verantwortlich, um auf Lücken in der Umsetzung von Cybersecurity Standards zu stoßen. Damit bilden sie die perfekte Grundlage, um die Cloud Security zu automatisieren, die Cybersecurity Compliance in der Cloud-Umgebung zu gewährleisten und somit das potenzielle Risiko von Datenschutzverletzungen deutlich zu reduzieren. [3]

Aber was genau sind überhaupt die Funktionen von CSPM-Werkzeugen?

1. **Kontinuierliche automatisierte Überwachung**
   Die kontinuierliche automatisierte Überwachung der Cloud-Umgebung dient dazu, die lückenlose Umsetzung der geltenden Cybersecurity Standards zu gewährleisten, dazu werden die Konfigurationen überwacht. [3]
2. **Identifikation von Sicherheitsproblemen**
   Automatisches Erkennen von potenziellen Sicherheitsproblemen, Schwachstellen und Fehlkonfigurationen und im besten Fall auch direkt das automatisierte Beheben der Sicherheitsprobleme. [41]
3. **Priorisierung und Risikobewertung**
   Gefundene Schwachstellen, die auf Fehlkonfigurationen zurückzuführen sind, werden je nach Umgebung priorisiert, um die Anzahl der Warnmeldungen zu reduzieren, da sich CSPM-Werkzeuge auf die Bereiche konzentrieren, die Angreifer am ehesten Ausnutzen. Darüber hinaus sucht das CSPM-Werkzeug mithilfe von Echtzeit-Bedrohungserkennung kontinuierlich nach böswilligen oder nicht autorisierten Aktivitäten in der Umgebung sowie nach nicht autorisierten Zugriffen auf Cloud-Ressourcen. [41]

4. **Erkennung von Compliance-Risiken**

   Automatisierte Überwachung von Compliance-Richtlinien zur Früherkennung, Warnung und Einleitung von Gegenmaßnahmen bei Compliance-Risiken [3]

5. **Empfehlungen und Behebungen**

   „Für die Korrektur von Konfigurationsfehlern, offenen IP-Ports, nicht genehmigten Änderungen und anderen Problemen, die die Sicherheit von Cloud-Ressourcen beeinträchtigen, werden **geführte Behebungsmaßnahmen und Leitlinien angeboten, um Fehler zu vermeiden".** [41]

Damit bieten CSPM-Werkzeuge eine gute Möglichkeit, die Sicherheit zu automatisieren und die Cybersecurity Compliance in der Multi-Cloud-Umgebung zu gewährleisten. [3]

Es sollte jedoch nicht vergessen werden, dass es auch andere Werkzeuge gibt, die die Cloud Security verbessern. Ansätze wären zum einen der Cloud Access Security Broker (CASB) und die Cloud Workload Protection Platform (CWPP), diese Werkzeuge bieten eine zusätzliche Sicherheitsschicht für die Multi-Cloud-Umgebung. „Der Cloud Access Security Broker (CASB) ist ein Service oder eine Anwendung, die Cloud-Applikationen absichert. Der CASB befindet sich zwischen dem Anwender und der Cloud und ist in der Lage, die Kommunikation zu überwachen, zu protokollieren und zu steuern." [42]. Durch die Überwachung der Kommunikation ist der CASB ideal dafür geeignet, verdächtigen Datenverkehr zu erkennen und entsprechend zu alarmieren. Aber auch für die Einhaltung geltender Compliance-Richtlinien ist der CASB notwendig. „Dank der Verwendung eines Cloud Access Security Brokers lassen sich die intern einzuhaltenden Sicherheitsrichtlinien auf externe Services ausweiten und durchsetzen." [42]. „Eine Cloud Workload Protection Platform (CWPP) ist ein Sicherheitstool, das Bedrohungen innerhalb von Cloud-Software erkennt und entfernt." [43].

Damit Unternehmen eine umfassende Cloud Security Strategie umsetzen können, müssen die verschiedenen Ansätze miteinander kombiniert werden, um den Anforderungen und Risiken gerecht zu werden. Ein Beispiel hierfür bietet die Abbildung 9, in dieser Abbildung wird ein Beispiel aufgezeigt, wie die verschiedenen Werkzeuge miteinander auf ein IaaS angewendet werden können. Dabei übernimmt das CSPM die Aufgabe der Überwachung der Konfigurationen der Ressourcen, um mögliche Konfigurationsfehler zu entdecken und um entsprechende Handlungsempfehlungen zu geben, um Compliance-Verstöße zu beseitigen. Dazu wird in dem in der Abbildung 9 gekennzeichneten Schritt 1 eine Verbindung zwischen dem CSPM und der API der Cloud hergestellt, wodurch das CSPM in der Lage ist, die IaaS-Services wie z. B. Webserver, Datenbanken und Speicher zu überwachen. Das CASB wird in Abbildung 9 dazu verwendet, verdächtigen Datenverkehr im Netzwerk zwischen den Nutzern und der Cloud zu erkennen, in Schritt 2. Aber auch zur Überwachung

der IaaS-Services und unterstützt dabei das CSPM die Compliance-Richtlinien einzuhalten Schritt 3. Das CWPP installiert sogenannte Agents (Software, die Bedrohungen erkennen und entfernen) auf den Cloud Workloads (Webserver, Datenbanken, usw.). Dieser Ablauf wird in der Abbildung 9 durch den Schritt 4 gekennzeichnet.[1]

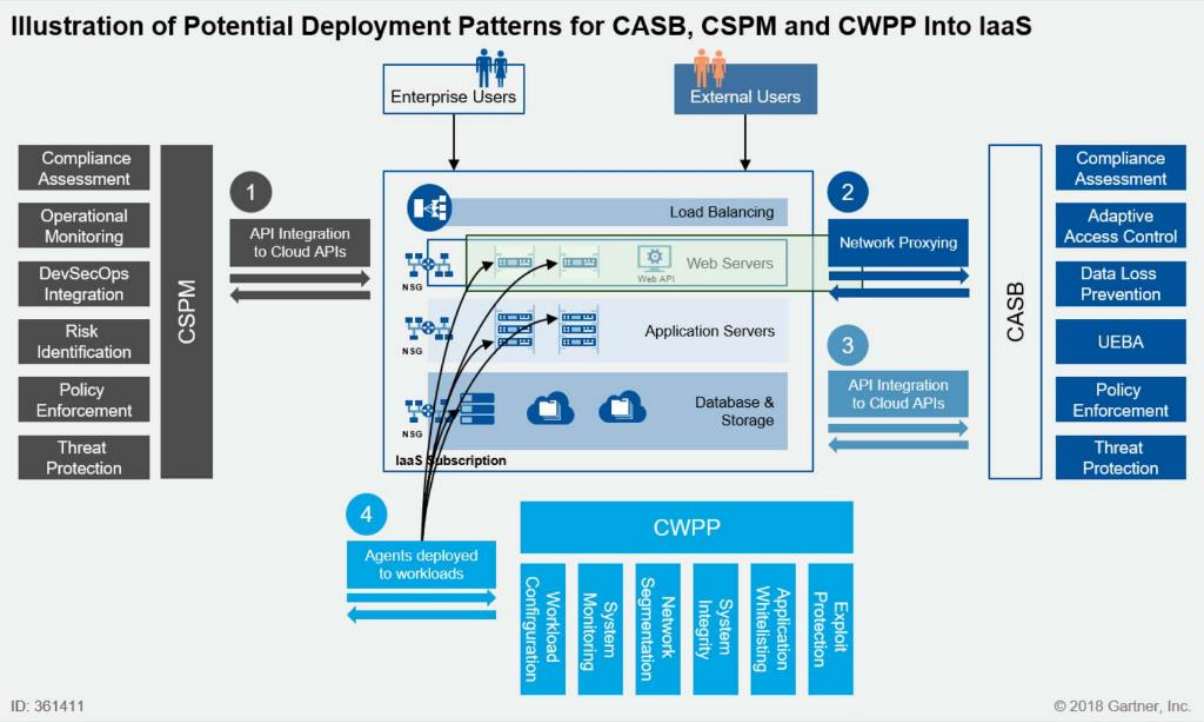


Abbildung 9: CASB, CSPM und CWPP in IaaS [44]

[1] Die Fähigkeiten (Capabilities) der CASB und CWPP die in der Abbildung 9 zu sehen sind werden im Rahmen dieser Bachelorarbeit nicht näher erläutert.

4.2 Fähigkeiten von CSPM-Werkzeugen

Die CSPM-Anbieter drücken die verschiedenen Fähigkeiten (Capabilities) der CSPM-Werkzeuge auf unterschiedliche Weise aus. Um den besten Anbieter von CSPM-Werkzeugen zu finden, muss das Unternehmen die Capabilities entsprechend den Anforderungen und Zielen des Unternehmens bewerten.

Capabilities von CSPM-Werkzeugen (Abbildung 10**):**

Abbildung 10: CSPM Capabilities (Screenshot) [48]

Compliance Assessment:

CSPM-Werkzeuge unterstützen die Einhaltung von Cybersecurity Standards, indem sie die Cloud-Umgebung automatisch überwachen und bewerten. [3]

Operational Monitoring:

CSPM-Werkzeuge überwachen Cloud-Umgebungen in Echtzeit, um potenzielle Sicherheitsvorfälle oder Unregelmäßigkeiten zu erkennen. Die kontinuierliche Überwachung bietet somit einen umfassenden Überblick über den Sicherheitsstatus der Cloud-Umgebung. [3]

DevSecOps Integration:

CSPM-Werkzeuge ermöglichen die Integration von Sicherheit in den DevOps-Prozess von Beginn des Entwicklungs- und Bereitstellungszyklus an. Dadurch erhalten Sicherheitsexperten und DevOps-Teams eine zentrale Quelle für Informationen über den Sicherheitsstatus von Ressourcen, sodass Sicherheitsexperten verhindern können, dass kompromittierte Ressourcen weiterhin verwendet werden. [41]

Risk Identification:

Durch die kontinuierliche automatisierte Überwachung der Cloud-Konfiguration und der Cloud Services können Konfigurationsfehler frühzeitig erkannt und ggf. sofort automatisch behoben werden. [3]

Policy Enforcement:

CSPM-Werkzeuge unterstützen die Einhaltung von Cybersecurity Standards. Bei Verstößen gegen die Standards werden Warnungen generiert und Maßnahmen zur Behebung der Verstöße empfohlen. [3] [45]

Threat Protection:

Durch die proaktive Erkennung von Sicherheitslücken mit CSPM-Werkzeugen können potenzielle Bedrohungen frühzeitig erkannt und durch geeignete Maßnahmen abgewendet bzw. der potenzielle Schaden minimiert werden. [41]

Die meisten CSPM-Werkzeuge sind in der Lage, Bewertungen anhand der Cybersecurity Standards durchzuführen, die in Kapitel 3.2 erläutert wurden. Unternehmen sollten jedoch insbesondere bei spezifischen Cybersecurity Standards prüfen, ob diese von dem gewünschten CSPM-Werkzeug unterstützt werden und ob die Cybersecurity Standards dann auch einfach bei internen und externen Audits berücksichtigt werden können. CSPM-Werkzeuge können die Vorbereitungen für ein Audit nämlich erheblich vereinfachen, indem Informationen über die Bewertung des Compliance-Status mithilfe von CSPM-Werkzeugen generiert werden. Welche Auskunft darüber geben können, ob gewisse Sicherheitskontrollen wie in Kapitel 3.3 bereits eingehend erläutert, auch wirklich implementiert worden sind und Funktionieren. Das bedeutet, mithilfe des CSPM-Werkzeuges lassen sich die überprüften Sicherheitskontrollen direkt den von den Auditoren verwendeten Cybersecurity Standards zuordnen. Dieser Ansatz erleichtert die Arbeit der Auditoren, verringert die Belastung der IT-Teams bei der Erstellung von Berichten, welche die Informationen zur Bewertung des Compliance-Status enthalten. Wodurch sich die Auditerfahrung für alle beteiligten sowohl das zuständige IT-Team als auch die Auditoren verbessert. [45]

4.3 Microsoft Defender for Cloud als Beispiel

Das vorliegende Kapitel widmet sich den CSPM-Funktionen von Azure Defender for Cloud und konzentriert sich dabei auf eine bestimmte Funktion: **Bewerten der Einhaltung gesetzlicher Bestimmungen**. Dieses Beispiel wurde aufgrund der Wichtigkeit dieser Funktion ausgewählt, um einen Überblick über den Compliance-Status zu geben, wobei Azure Defender for Cloud über die beste Dokumentation verfügt, um diese Funktion verständlich zu erklären.

Microsoft Defender for Cloud

Microsoft Defender for Cloud ist eine einheitliche Cloud-native Plattform für das CSPM zum Schutz von Anwendungen, die den Sicherheitsstatus verbessert, Schutz vor modernen Bedrohungen bietet und Risiken während des gesamten Lebenszyklus von Cloud-Anwendungen in Multi-Cloud- und hybriden Umgebungen reduziert. [46]

Bewerten der Einhaltung gesetzlicher Bestimmungen

Das Compliance Dashboard, wie in Abbildung 11 zu sehen, zeigt ausgewählte Cybersecurity Standards mit allen zugehörigen Anforderungen. Den Anforderungen sind Sicherheitsbewertungen zugeordnet. Der angezeigte Status zeigt an, ob der entsprechende Cybersecurity Standard eingehalten wird oder nicht. Das Dashboard kann verwendet werden, um einen Überblick über auftretende Compliance-Lücken in Bezug auf ausgewählte Cybersecurity Standards zu erhalten. Durch diese kontinuierliche Überwachung ist es möglich, einen fokussierten Überblick über den Compliance Status in der dynamischen Cloud-Umgebungen zu erhalten, entsprechend den in Kapitel 4.1 und Kapitel 4.2 beschriebenen Funktionen und Capabilities. [47]

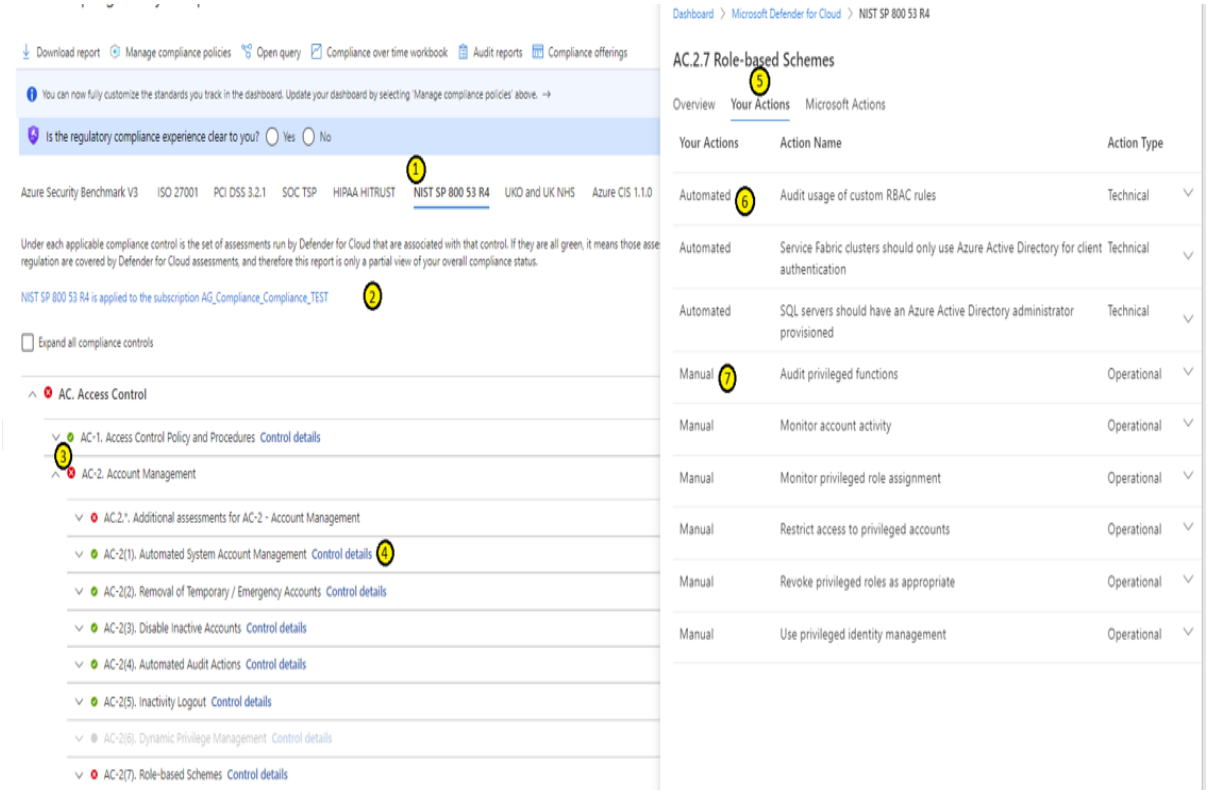


Abbildung 11: Compliance-Dashboard (Screenshot) [47]

Die Abbildung 11 erfordert eine detaillierte Erklärung der einzelnen Komponenten, die durch eine Nummerierung gekennzeichnet sind:

1. Bietet eine Auswahl verschiedener Cybersecurity Standards nach Auswahl eines bestimmten Standards, wird eine Liste aller Überprüfungen angezeigt, die für diesen Standard durchgeführt werden. [47]
2. Zeigt an, auf welches Abonnement (Subscription) der entsprechende Cybersecurity Standard angewendet wird. [47]
3. Durch Erweitern der Kontrolle (Control) werden die Bewertungen der ausgewählten Kontrolle angezeigt. Es ist nun möglich, durch Auswahl einer Bewertung eine Liste der zugehörigen Ressourcen und der entsprechenden Aktionen zur Behebung der fehlenden Konformität mit dem ausgewählten Cybersecurity Standard anzusehen. [47]
4. Kontrolldetails (Control details) zeigt die entsprechende Übersicht der Registerkarte im rechten Teil der Abbildung 11 an. [47]
5. Der Reiter Ihre Aktionen (Your Actions) in der Registerkarte zeigt die automatisierte (Automated (6)) und die manuelle (Manual (7)) Bewertung der ausgewählten Kontrolle an. [47]

6. Die automatisierten Bewertungen zeigen die Anzahl der fehlgeschlagenen Ressourcen und Ressourcentypen an, die mit der für die Empfehlung entsprechenden Korrekturfunktion verknüpft sind. [47]
7. Manuelle Bewertungen können manuell bestätigt werden und anschließend verknüpft werden und dienen somit als Beweis der Konformität. [47]

Korrigieren einer automatisierten Bewertung

Für dieses Beispiel wird der Azure Cybersecurity Standard CIS 1.1.0 mit der entsprechenden Empfehlung Datenträgerverschlüsselung sollte auf virtuelle Maschinen angewendet werden (Disk encryption should be applied on virtual machines). In Abbildung 12 wird dann eine entsprechende virtuelle Maschine unter Affected resources ausgewählt, beispielsweise VM6, um weitere Informationen und Empfehlungen zur Behebung zu erhalten. Außerdem bekommt man mit Severity High eine Auskunft darüber, wie dringend dieses Problem behoben werden sollte. [47]

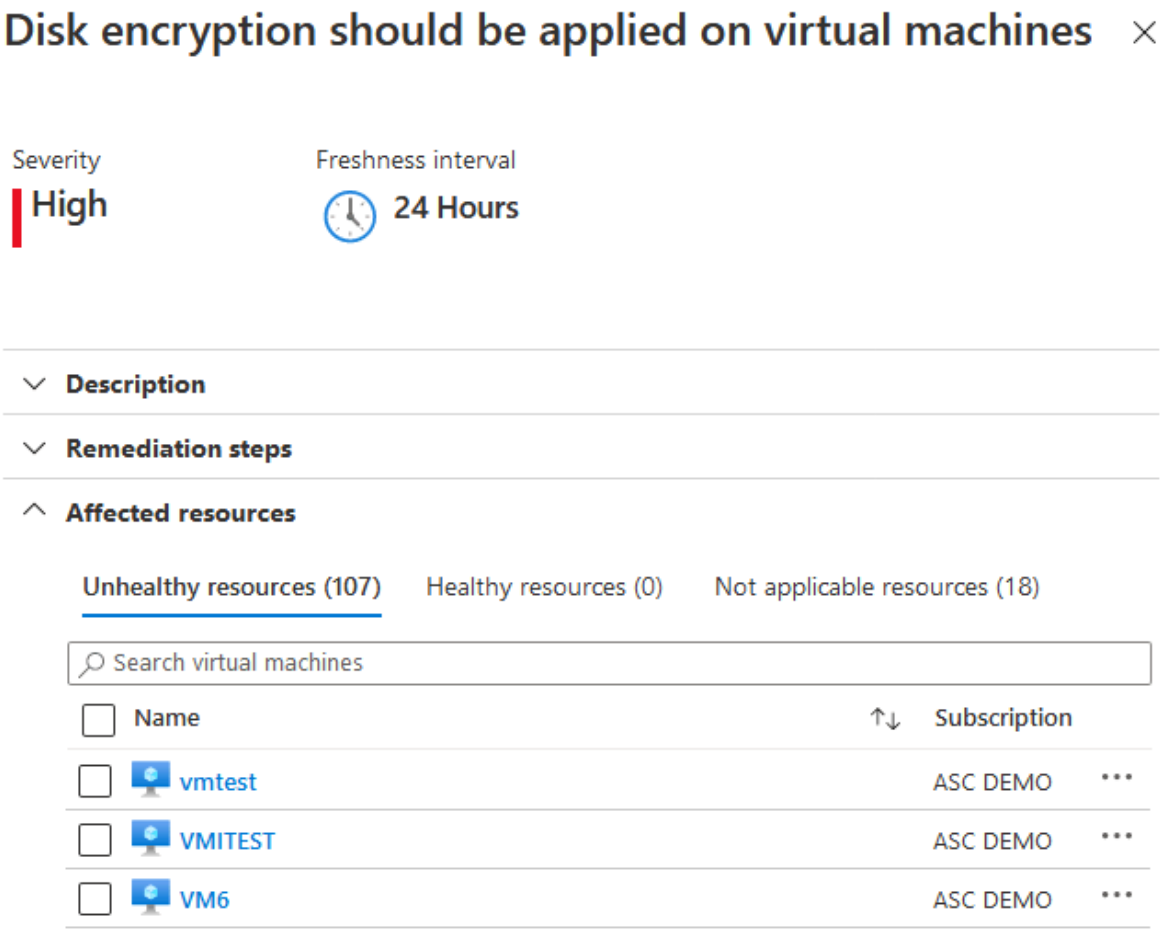


Abbildung 12: Beispiel Empfehlung [47]

Abbildung 13 zeigt nun die Aktivierung der Verschlüsselung für die zuvor ausgewählte Ressource an. Welche aktiviert werden muss, um den entsprechenden Compliance-Verstoß zu beheben. Nach der Aktivierung der Verschlüsselung wird das Ergebnis auf dem Compliance Dashboard angezeigt (ca. nach 12 Stunden, da die Bewertungen in diesem Intervall durchgeführt werden). [47]

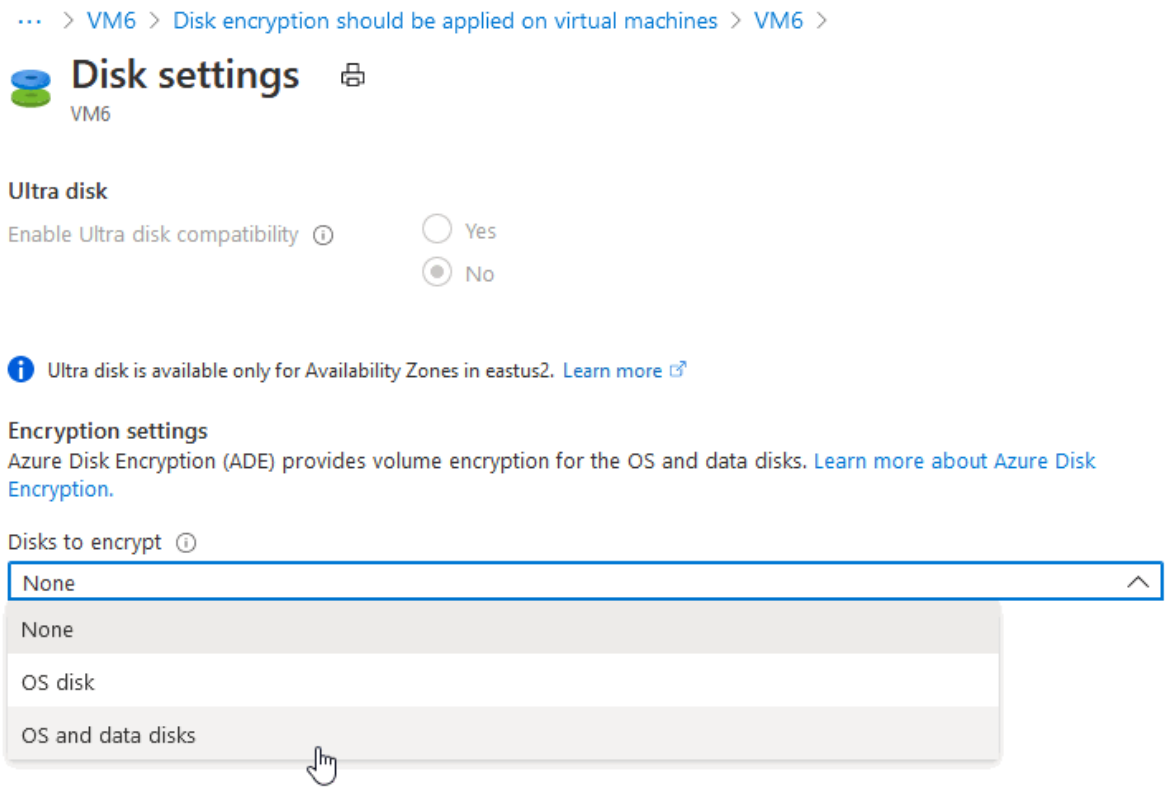


Abbildung 13: Verschlüsselung umsetzen [47]

Das eben aufgezeigte Beispiel ist eine praktische Verdeutlichung der in Kapitel 4.2 aufgezeigten Möglichkeit von CSPM-Werkzeugen zur Verbesserung der Auditerfahrung. Aber auch ein gutes Beispiel dafür, wie man sich selbst einen Überblick über den Compliance-Status seines Abonnements verschaffen und Compliance-Lücken beheben kann.

Im folgenden Kapitel wird das Framework für die Analyse und Vergleich von CSPM-Werkzeugen in Multi-Cloud-Umgebungen vorgestellt, das auf den zuvor im Rahmen dieses Kapitels vorgestellten Konzepten der Funktionen und Fähigkeiten von CSPM-Werkzeugen basiert.

5 Framework für die Analyse und den Vergleich von CSPM-Werkzeugen in Multi-Cloud-Umgebungen

Das Kapitel widmet sich dem im Rahmen der Bachelorarbeit entwickelten Framework für die Analyse und den Vergleich von CSPM-Werkzeugen in Multi-Cloud-Umgebungen. Dabei werden der Entwurf, die Anwendung und die gefundenen Ergebnisse des Frameworks vorgestellt. Das Framework dient als Unterstützung für Unternehmen, um fundierte Entscheidungen bei der Auswahl und Implementierung von CSPM-Werkzeugen in Multi-Cloud-Umgebungen treffen zu können. In einer Multi-Cloud-Umgebung mit verschiedenen Cloud-Anbietern kann es schwierig werden, ein CSPM-Werkzeug auszuwählen, besonders da es bei der Nutzung verschiedener Cloud-Anbieter häufig zu Schwierigkeiten mit der Interoperabilität der APIs kommt. Daher ist es umso wichtiger, dass beim Vergleich verschiedener CSPM-Werkzeuge besonderes Augenmerk auf die Funktionen und Capabilities gelegt wird, welche für eine optimale Überwachung einer Multi-Cloud-Umgebung entscheidend sind. [48] [49]

5.1 Entwurf des Frameworks

Das Vergleichs- und Analyse Framework für Cloud Security Posture Management (CSPM)-Werkzeuge dient grundsätzlich der Evaluierung und Unterstützung bei der Auswahl von Cloud Security Posture Management (CSPM)-Werkzeugen. Ohne ein Framework kann sich die Auswahl von Cloud Security Posture Management (CSPM)-Werkzeugen als eine echte Herausforderung darstellen. Durch den Einsatz des Frameworks können Ressourcen eingespart, Kosten gesenkt und redundante Prozesse eliminiert werden, um nur einige der Vorteile zu nennen, die Unternehmen durch die Nutzung des Frameworks haben [50]. Bevor es zur Anwendung des Frameworks kommen kann, ist es zunächst notwendig, die einzelnen Funktionen zu definieren, die für einen objektiven Vergleich und die Analyse entscheidend sind. Dabei werden Fähigkeiten und Funktionen von CSPM-Werkzeugen, die teilweise bereits im Kapitel 4 behandelt wurden, aufgegriffen, um für Multi-Cloud-Umgebungen relevante Funktionen ergänzt und entsprechend den Anforderungen der Multi-Cloud-Umgebung neu definiert.

Funktionen:

Kontinuierliches/ automatisches Monitoring:

Überwachung der Multi-Cloud-Umgebung und ihrer Ressourcen in Echtzeit, um auffällige Sicherheitslücken oder Compliance-Verstöße zu identifizieren. Dazu werden die Sicherheitskonfigurationen automatisch und kontinuierlich überprüft. [3]

Sicherheitswarnungen und Empfehlungen:

Die gefundenen Sicherheitslücken und die daraus resultierenden Bedrohungspotenziale müssen auf verschiedenen Wegen an die verantwortlichen Personen kommuniziert werden. Dazu gehören auch die ggf. automatische Behebung von Sicherheitslücken oder die Generierung von Empfehlungen zur Behebung der gefundenen Sicherheitslücken bzw. Fehlkonfigurationen oder zur generellen Verbesserung der Konfiguration. [41]

Compliance-Berichterstellung:

Erstellung eines Berichts über die Einhaltung ausgewählter Cybersecurity Standards, wie sie in Kapitel 3.2 beschrieben sind.

Unterstützte Standards:

Unterstützen die CSPM-Werkzeuge die ausgewählten Cybersecurity Standards, die im Kapitel 3.2 näher erläutert wurden überhaupt?

Einfügen eigener Standards

Bieten die CSPM-Werkzeuge auch die Möglichkeit, an die Anforderungen angepasste oder selbst entwickelte Standards zu unterstützen?

„Out of the Box“ Multi-Cloud-Kompatibilität:

Ist es möglich, verschiedene Cloud-Plattformen in der Multi-Cloud-Umgebung mit ausgewählten CSPM-Werkzeugen zu überwachen und zu sichern, ohne dass aufwendige manuelle Anpassungen erforderlich sind?

Native Integration mit Cloud Services und APIs:

Ist es möglich, Cloud-Plattform übergreifende native Services und APIs in die CSPM-Werkzeuge zu integrieren, um somit eine effektive Überwachung und Absicherung der Multi-Cloud-Umgebung zu gewährleisten.

Abschließend dürfen die Kosten der verschiedenen CSPM-Werkzeuge nicht vernachlässigt werden, um einen transparenten Überblick über die anfallenden Kosten bei der Nutzung der CSPM-Werkzeuge zu geben.

5.2 Anwendung des Frameworks

Nachdem die Funktionen des Frameworks definiert wurden, widmet sich dieses Kapitel der Anwendung, also dem Vergleich der ausgewählten CSPM-Werkzeuge anhand der zuvor definierten Funktionen.

Tabelle 1 zeigt einige der untersuchten Funktionen, die aus folgenden Gründen als wichtig für CSPM-Werkzeuge in Multi-Cloud-Umgebungen erachtet werden. Wie bereits bei der Erläuterung der Funktionen von CSPM-Werkzeugen im Kapitel 5.1 näher erläutert, stehen diese Funktionen für CSPM-Werkzeuge in Multi-Cloud-Umgebungen im Vordergrund. Da die Funktionen eine optimale Grundlage für einen Vergleich der ausgewählten CSPM-Werkzeuge bieten. Die in Tabelle 1 verglichenen CSPM-Werkzeuge wurden ausgewählt, weil AWS Security Hub, Microsoft Defender for Cloud und Google Cloud Security Command Center die nativen CSPM-Werkzeuge der drei weltweit führenden Cloud-Anbieter sind. Somit ist ein Vergleich dieser CSPM-Werkzeuge naheliegend, wenn man bereits Kunde bei einem der Cloud-Anbieter ist, wäre es ideal auch ein natives CSPM-Werkzeug für die Überwachung der Multi-Cloud-Umgebung nutzen zu können. Um jedoch nicht nur native Werkzeuge zu vergleichen, wird das laut einer Gartner Umfrage beste CSPM-Werkzeug von Palo Alto Networks zur Verfügung gestellte Prisma Cloud in den Vergleich mit aufgenommen [51] [52]

Tabelle 1: Vergleich der CSPM-Werkzeuge

Funktion	**AWS Security Hub** [53]	**Microsoft Defender for Cloud** [54]	**Google Cloud Security Command Center** [55]	**Palo Alto Networks Prisma Cloud** [56]
Kontinuierliches/ automatisches Monitoring	Ja	Ja	Ja	Ja
Sicherheitswarnungen und Empfehlungen	Ja	Ja	Ja	Ja
Compliance-Berichterstellung	Ja	Ja	Ja	Ja
Unterstützte Standards	[57]	[58]	[59]	[60]
ISO/IEC 27001	Nein	Ja	Ja	Ja
BSI C5	Nein	Nein	Nein	Nein
NIST 800-53	Ja	Ja	Ja	Ja
SOC 2	Nein	Ja	Nein	Ja
Einfügen eigener Standards	[61]	[62]	[63]	[64]
Bosch EISA	Ja	Ja	Ja	Ja
„Out of the Box“ Multi-Cloud-Kompatibilität	Nein	Ja	Nein	Ja
Native Integration mit Cloud Services und APIs	AWS	Azure, AWS und Google Cloud	Google Cloud	AWS, Azure, Google Cloud, Alibaba Cloud und Oracle Cloud Infrastructure (OCI) [65]
Kosten pro Monat [2]	1683 USD [66]	n. a.	613 USD [67]	n. a.

[2] Die Kosten pro Monat sind schwer zu vergleichen, da die Anbieter entweder keine oder sehr unverständliche Abrechnungsmethoden haben. Die Kosten hängen stark von den Anforderungen des Unternehmens ab und können daher variieren.

5.3 Analyse des Frameworks

Nachdem in Kapitel 5.2 ein Vergleich der ausgewählten CSPM-Werkzeuge durchgeführt wurde, soll in diesem Kapitel eine umfassende Analyse der Ergebnisse vorgenommen werden.

Der Vergleich der verschiedenen CSPM-Werkzeuge hat gezeigt, dass alle CSPM-Werkzeuge die vordefinierten Grundfunktionen wie kontinuierliches und automatisiertes Konfiguration Monitoring, Sicherheitswarnungen und -empfehlungen sowie Compliance-Berichterstellung bieten. Diese Funktionen sind für die Gewährleistung von Sicherheit und Compliance in der Multi-Cloud-Umgebung von entscheidender Bedeutung und daher unerlässlich, um potenzielle Sicherheitsbedrohungen oder Verstöße gegen Cybersecurity Standards proaktiv zu erkennen und angemessen darauf zu reagieren. Die Unterstützung der wichtigsten Cybersecurity Standards ist ein wichtiger Faktor bei der Auswahl von CSPM-Werkzeugen. Hier haben Microsoft Defender for Cloud, Google Cloud Security Command Center und Palo Alto Networks Prisma Cloud auf den ersten Blick einen Vorteil gegenüber AWS Security Hub, da sie standardmäßig eine breite Palette an Cybersecurity Standards wie ISO/IEC 27001, NIST 800-53 und teilweise auch SOC 2 unterstützen. Bei allen Anbietern besteht die Möglichkeit, eigene Cybersecurity Standards hinzuzufügen und individuelle Anpassungen vorzunehmen, um unternehmensspezifische Standards wie beispielsweise die Bosch EISA zu erfüllen. Die „Out of the Box“ Multi-Cloud-Kompatibilität ist dabei ein weiterer entscheidender Punkt für Unternehmen, die CSPM-Werkzeuge zur Überwachung einer Multi-Cloud-Umgebung einsetzen möchten. Insbesondere Microsoft Defender for Cloud und Palo Alto Networks Prisma Cloud spielen hier ihre Stärken aus, da sie die einfache Integration verschiedener Cloud-Plattformen ermöglichen und somit die Überwachung und Sicherheitskontrolle verschiedener unterstützter Cloud-Plattformen erleichtern. Ein besonders wichtiger Punkt ist die native Integration von CSPM-Werkzeugen mit den Cloud Services und APIs verschiedener Cloud-Anbieter. Die APIs liefern dabei den Zugriff zu Konfigurationsdaten, Logs und anderen relevanten Daten, welche entscheidend für die Sicherheitsüberwachung der Multi-Cloud-Umgebung sind. Es ist sehr schwierig einen Kostenvergleich durchzuführen, da die verschiedenen CSPM-Anbieter teilweise unklare Darstellungen und unterschiedliche Berechnungsmodelle verwenden.

Aus diesem Vergleich sollte hervorgehen, dass es nicht möglich ist, allgemeine Empfehlungen für das „richtige“ CSPM-Werkzeug zu geben. Dies ist immer eine individuelle Entscheidung unter Berücksichtigung der Anforderungen, die an ein CSPM-Werkzeug zur Überwachung einer Multi-Cloud-Umgebung gestellt werden. Das erstellte Framework kann jedoch als Grundlage für einen individuellen Vergleich dienen und dabei helfen, das passende CSPM-Werkzeug zu finden. Es sollte jedoch nicht vergessen werden, dass die Wahl eines nativen CSPM-Werkzeugs wie Security Command

Center, Azure Defender for Cloud oder Security Command Center oder eines Drittanbieter-Werkzeugs wie Prisma Cloud immer mit der entsprechenden Darstellung und der Art und Weise verbunden ist, wie die CSPM-Werkzeuge die Überwachung durchführen. Es kann jedoch auch der Fall eintreten, dass mehr als ein CSPM-Werkzeug benötigt wird, da diese über gewisse Funktionen verfügen, welche besser zur Überwachung der eigenen Infrastruktur geeignet sind als andere CSPM-Werkzeuge. In diesem Fall kann die zentrale Darstellung der gesammelten Informationen aufgrund der proprietären Modelle der APIs mit einem enormen Entwicklungsaufwand verbunden sein. Um dieses Problem zu lösen, sollte es einen einheitlichen Kommunikationsstandard geben, der die Grundlage für eine Einfache und mit deutlich geringerem Entwicklungsaufwand zu realisierende Interoperabilität zwischen verschiedenen CSPM-Werkzeugen in der Multi-Cloud-Umgebung bietet.

6 Fallstudie zur Erreichung der Interoperabilität in Multi-Cloud-Umgebungen

Dieses Kapitel widmet sich der Fallstudie, welche als möglicher Lösungsansatz für Unternehmen dienen soll, die mit Interoperabilitätsproblemen zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebung konfrontiert sind. Dabei zeigt die Fallstudie einen möglichen Weg auf, wie die Integration und Nutzung verschiedener CSPM-Werkzeuge in Multi-Cloud-Umgebungen durch das Einführen eines einheitlichen Kommunikationsstandards verbessert werden kann. Wodurch die Interoperabilität zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebungen gewährleistet ist.

6.1 Beschreibung der Fallstudie

In dieser Fallstudie wird die Policy States API von Azure verwendet, um Sicherheitskonfigurationen in der Cloud zu überprüfen. Die Ergebnisse werden auf einem dem Assessment Result Model der Open Security Controls Assessment Language (OSCAL) ähnlichen Model abgebildet, um eine standardisierte Darstellung von Compliance- und Sicherheitsinformationen zu ermöglichen. Anschließend werden die Ergebnisse an das MEDINA Security Framework gesendet, um eine umfassende Sicherheitsbewertung in Multi-Cloud-Umgebungen durchzuführen. Das Security Framework des Medina-Projekts ist eine Sicherheitsstruktur, die eine kontinuierliche auditbasierte Zertifizierung ermöglicht und gleichzeitig einen Überblick über die überwachten Cloud-Ressourcen und deren Compliance-Status bietet. Die Kombination dieser Design-Entscheidungen der Fallstudie stellt sicher, dass die Interoperabilität von CSPM-Werkzeugen in Multi-Cloud-Umgebungen gewährleistet ist. Der Ablauf der Fallstudie wird dabei in Abbildung 14 dargestellt. [68] [69]

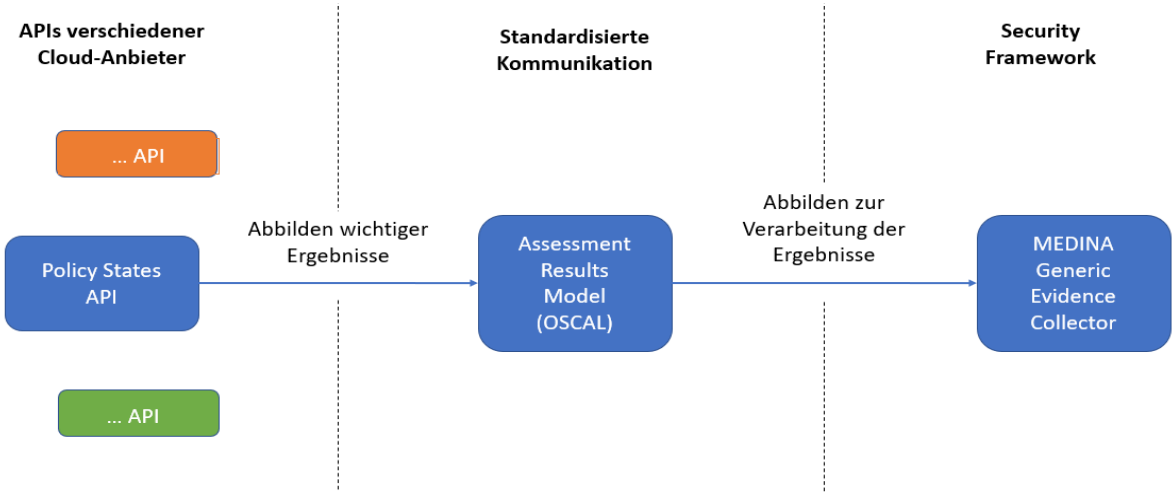


Abbildung 14: Ablauf der Fallstudie (Eigene Darstellung)

6.1.1 Policy States

Die Policy States API ist eine Programmierschnittstelle von Azure, die es ermöglicht, den aktuellen Compliance-Status zu liefern, ob Ressourcen, auf die bestimmte Richtlinien (Policies) angewendet werden, auch diesen Richtlinien entsprechen und somit Compliance gewährleistet ist oder nicht (Compliant oder NonCompliant). Der Nutzer der Policy States API erhält somit einen Überblick über den Compliance-Status der überwachten Cloud-Umgebung in Azure und kann diese überwachen und Richtlinienverstöße frühzeitig erkennen. Abbildung *15* zeigt einen Teil der Ergebnisse im JSON-Format, die die Policy State API liefert, in diesem Beispiel eine Ressource, die nicht den Richtlinien des Cybersecurity Standards entspricht und daher als NonCompliant deklariert wird, zu sehen an der gelb markierten Stelle. [70]


```
{
    "@odata.id": null,
    "@odata.context": "https://management.azure.com/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/providers/Microsoft.PolicyInsights/policyStates/$metadata#latest/$entity",
    "timestamp": "2019-10-09T17:48:05Z",
    "resourceId": "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/resourcegroups/myGroup/providers/microsoft.compute/virtualmachines/test-vm",
    "policyAssignmentId": "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/providers/Microsoft.Authorization/policyAssignments/Enable Monitoring in Azure Security Center",
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/1f7c564c-0a90-4d44-b7e1-9d456cffaee8",
    "effectiveParameters": null,
    "isCompliant": false,
    "subscriptionId": "fffedd8f-ffff-fffd-fffd-fffed2f84852",
    "resourceType": "/microsoft.compute/virtualmachines",
    "resourceLocation": "eastus",
    "resourceGroup": "myGroup",
    "resourceTags": "tbd",
    "policyAssignmentName": "Enable Monitoring in Azure Security Center",
    "policyAssignmentOwner": "tbd",
    "policyAssignmentParameters": "{}",
    "policyAssignmentScope": "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852",
    "policyDefinitionName": "1f7c564c-0a90-4d44-b7e1-9d456cffaee8",
    "policyDefinitionAction": "AuditIfNotExists",
    "policyDefinitionCategory": "tbd",
    "policySetDefinitionId": "/providers/Microsoft.Authorization/policySetDefinitions/1f3afdf9-d0c9-4c3d-847f-89da613e70a8",
    "policySetDefinitionName": "1f3afdf9-d0c9-4c3d-847f-89da613e70a8",
    "policySetDefinitionOwner": null,
    "policySetDefinitionCategory": null,
    "policySetDefinitionParameters": null,
    "managementGroupIds": "mymg,fff988bf-fff1-ffff-fffb-fffcd011db47",
    "policyDefinitionReferenceId": null,
    "complianceState": "NonCompliant",
    "policyDefinitionGroupNames": [
        "myGroup"
    ],
    "policyDefinitionVersion": "1.0.0-preview",
    "policySetDefinitionVersion": "2.0.1",
    "policyAssignmentVersion": "1.0.0"
},
```


Abbildung 15*: Ressource NonCompliant (Eigene Darstellung) [70]*

6.1.2 Open Security Controls Assessment Language (OSCAL)

Die Open Security Controls Assessment Language (OSCAL) wird vom National Institute of Standards and Technology (NIST) als einheitliches, datenzentriertes Framework zur Erfassung und Bewertung von Sicherheitskontrollen in Informationssystemen entwickelt. Sicherheitskontrollen werden dabei heute jedoch in proprietären Formaten dargestellt, d. h. diese Formate sind Eigentum des Herstellers. Im Umkehrschluss bedeutet das, dass eine enorm aufwändige Konvertierung der Daten erforderlich ist, um die gewünschte Implementierung zu erreichen. Weshalb es sich OSCAL zum Ziel gemacht hat, weg vom textbasierten manuellen Ansatz hin zu einer Reihe von standardisierten, maschinenlesbaren

Formaten zu kommen. Durch diese Änderung können Sicherheitsexperten die Prozesse, welche im Zusammenhang mit der kontinuierlichen Überwachung von Sicherheitsbewertungen und den Audits stehen, automatisieren. OSCAL wurde hierbei als Kommunikationsstandard gewählt, da er großes Potenzial hat, ein standardisiertes Format zu entwickeln, welches von Maschinen gelesen werden kann und dabei von den Experten des NIST entwickelt wird, die über umfangreiche Erfahrungen mit der Standardisierung verfügen. Zudem werden vom NIST auch Bemühungen ergriffen, den Standard in Europa zu fördern, dafür wurde eigens die EUROSCAL Gemeinschaft ins Leben gerufen, welche motivierte und Interessierte Menschen an der Nutzung von OSCAL zusammenbringen soll. [68] [71] [72]

Assessment Results Model

Das Assessment Results Model definiert die Informationen, welche bei der Sicherheitsbewertung und -überprüfung gesammelt und dokumentiert werden. Womit das Modell eine gute Möglichkeit bietet, die kontinuierliche Bewertung zu überwachen, und die Ergebnisse der Bewertung bieten somit die Grundlage zur Bewertung des Compliance-Status des überwachten Systems. [73]

Abbildung 16 zeigt das Assessment Results Model jedoch wird es im Rahmen dieser Bachelorarbeit nicht vollumfänglich erläutert, sondern nur die relevanten Komponenten, welche zur Abbildung der Ergebnisse der Policy States API benötigt werdem.

Metadata:

Enthält Informationen wie den Titel der Datei, die Veröffentlichungsversion, das Veröffentlichungsdatum und die OSCAL-Version. Metadaten werden auch verwendet, um Rollen, Parteien (Personen, Teams und Organisationen) und Standorte zu definieren. [73]

Import AP:

Stellt fest, um welchen Bewertungsplan von OSCAL es sich handelt und importiert dabei wichtige Informationen über das zu bewertende System. [73]

Assessment Subject:

Identifiziert die Elemente des Systems, die für die Bewertung relevant sind. Zum Beispiel Standorte, Komponenten, Inventarpositionen und Nutzer. Die Identifizierung des Assessment Subjects hilft beim Setzen der Grenzen einer Bewertung. [73]

Finding:

Es handelt sich um Beobachtungen oder Risiken, die während des Bewertungsprozesses identifiziert wurden. [73]

Abbildung 16: Assessment Results (AR) [73]

6.1.3 MEDINA

Bei dem MEDINA-Projekt handelt es sich um ein von der EU gefördertes Forschungsprojekt, das sich auf die Bereiche der Cloud-Sicherheitsleistung und dem Audit-Evidenzmanagement konzentriert. Wie in Abbildung 17: MEDINA PartnerAbbildung 17 zu sehen ist, verteilen sich die Partner des MEDINA-Projekts auf 6 verschiedene europäische Länder zu diesem Partner zählen die folgenden TECNALIA, Centro Nazionale della Ricerca, Hewlett Packard, Fabasoft, XLAB, BOSCH, Fraunhofer und NIXU. Der Hauptfokus des MEDINA-Projekts liegt auf der Etablierung eines Sicherheitsframeworks für eine kontinuierliche auditbasierte Zertifizierung im Einklang mit dem Cloud-Sicherheitszertifizierungssystem der EU. Das MEDINA-Projekt hat eigens dafür Cybersecurity- und Sicherheitslösungen, welche sowohl von Unternehmen als auch von Forschungseinrichtungen implementiert werden können. Wodurch sie ihre Widerstandskraft gegen gängige Cyber-Bedrohungen verbessern und damit Sicherheitsrisiken minimieren können. Infolgedessen kann die Einhaltung von Cybersecurity Standards mithilfe des MEDINA-Projekts sichergestellt werden. [74] [69]

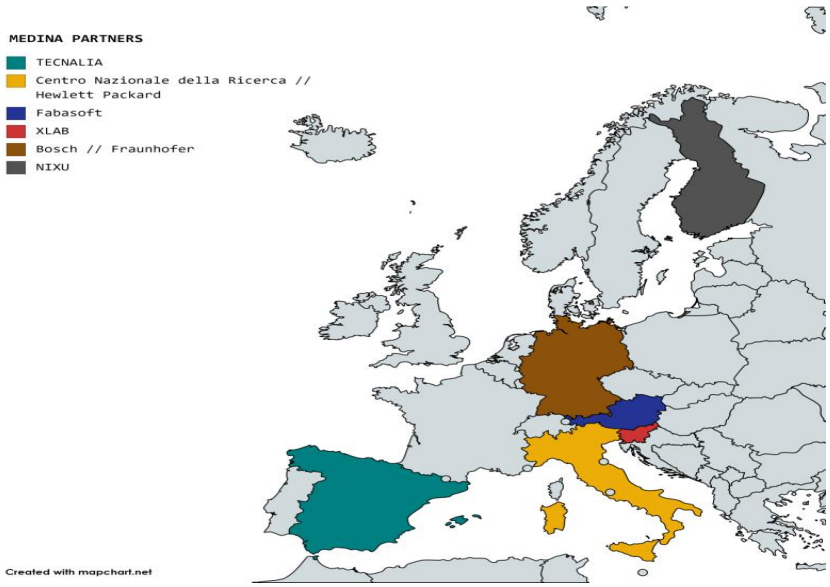


Abbildung 17: MEDINA Partner [74]

Das MEDINA-Projekt definiert den sogenannten Generic Evidence Collector (GEC), dieser bietet eine Vorlage für einen Evidence Collector welcher anpassbar an die Bedingungen des Nutzers ist. Dadurch ist es beispielsweise möglich, einen minimalen Satz an Informationen zu definieren, der für die Durchführung von Compliance-Bewertung der Ressourcen verschiedener Cloud-Anbieter benötigt wird. Der Collector kann leicht an spezifische Cloud-Anbieter angepasst werden, es handelt sich also nicht um eine vollständige Implementierung, sondern um eine Vorlage, die den Anforderungen angepasst werden kann. [75]

6.2 Methodik und Datenbeschaffung

Die für die Durchführung der Fallstudie notwendige Datenbeschaffung wurde wie folgt durchgeführt. Um die Ergebnisse der Policy States API abzufragen, wurde in diesem Fall auf ein von Microsoft zur Verfügung gestelltes Python Skript [76] zurückgegriffen. Das Skript, welches in Abbildung 18 zu sehen ist, wurde an die entsprechenden Anforderungen angepasst und speichert die Ergebnisse der Policy State API in einer JSON-Datei.

```python
from azure.identity import InteractiveBrowserCredential
from azure.mgmt.policyinsights import PolicyInsightsClient
import json

def main():
    client = PolicyInsightsClient(
        credential=InteractiveBrowserCredential(),
        subscription_id='[redacted]',
    )

    response = client.policy_states.list_query_results_for_subscription(
        policy_states_resource="latest",
        subscription_id="[redacted]"
    )

    data = [item.as_dict() for item in response]

    output_json = {
        "@odata.nextLink": "",
        "@odata.context": "https://management.azure.com/subscriptions/[redacted]/providers/Microsoft.PolicyInsights/policyStates/$metadata#latest",
        "@odata.count": len(data),
        "value": data
    }
    output_file="policy_states_results.json"
    with open(output_file, "w") as file:
        json.dump(output_json, file,indent=4)
    print("Resultdaten wurden erflogreich in", output_file, "gespeichert.")

if __name__ == "__main__":
    main()
```

Abbildung 18: Python Skript zur Abfrage der Policy States API (Eigene Darstellung)

Abbilden auf ein dem OSCAL Assessment Results Model ähnliches Modell

Um die relevanten Informationen auf das Assessment Results Model von OSCAL abbilden zu können, muss vor der eigentlichen Implementierung genau überlegt werden, welche Informationen aus dem Ergebnis der Policy States API im Rahmen dieser Arbeit überhaupt relevant sind. Dazu gehören die in der ersten Spalte von Tabelle 2 aufgeführten Informationen, die aus der Policy States API gewonnen werden. Sie geben Auskunft darüber, welche Ressource in der Cloud-Umgebung bewertet wurde, wann dies geschah, um die Bewertung auch in einen zeitlichen Kontext einordnen zu können, welche Richtlinie für die Bewertung verwendet wurde und welches Ergebnis die Bewertung hatte. Diese Informationen können als das Minimum an Informationen angesehen werden, das für eine automatisierte Compliance-Bewertung erforderlich ist.

Abbilden auf eine Metrik des MEDINA Generic Evidence Collector

In der dritten Spalte der Tabelle 2 wird die verwendete Richtlinie auf die der Richtlinie entsprechende Metrik abgebildet. Eine Metrik ist ein Maß, um einen Überblick über die Leistung und den Fortschritt zu erhalten. Durch die Messung der Leistung können Trends frühzeitig erkannt werden und durch die Messung des Fortschritts ist ein Vergleich mit den zu erreichenden Zielen möglich. Metriken liefern somit die Grundlage für fundierte Entscheidungen und kontinuierliche Verbesserungen. Die ausgewählte Metrik enthält dabei genauere Informationen, die von Auditoren und Compliance Managern verstanden und entsprechend gedeutet werden können. [77] [78]

Tabelle 2: Abbildung relevanter Informationen[3]

<table>
<tr><th>Policy State API Ergebnisse</th><th>Assessment Results Model
(ähnliches Schema)</th><th>MEDINA Metrik</th></tr>
<tr><td>timestamp = "2023-07-03T01:50:39.726521Z "</td><td>Metadata:
timestamp = "2023-07-03T01:50:39.726521Z "</td><td rowspan="2">timestamp = "2023-07-03T01:50:39.726521Z"
metricId = "MalwareProtectionOutput"
description = “" This metric states whether automatic notifications are enabled (e.g. e-mail) about malware threats. This relates to EUCS’ definition of “continuous monitoring”” [78]
policyDefintionId = "/providers/microsoft.authorization/policydefinitions/1f7c564c-0a90-4d44-b7e1-9d456cffaee8"</td></tr>
<tr><td>policyDefinitionId = "/providers/Microsoft.Authorization/policyDefinitions/1f7c564c-0a90-4d44-b7e1-9d456cffaee8"</td><td>Import AP:
assessmentPolicy="/providers/Microsoft.Authorization/policyDefinitions/1f7c564c-0a90-4d44-b7e1-9d456cffaee8"</td></tr>
<tr><td>resourceId = "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/resourcegroups/myGroup/providers/microsoft.compute/virtualmachines/test-vm"</td><td>Assessment Subject:
resource = "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/resourcegroups/myGroup/providers/microsoft.compute/virtualmachines/test-vm"</td><td>targetResourceType = "Virtual Machine"
targetResource = "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/resourcegroups/myGroup/providers/microsoft.compute/virtualmachines/test-vm"</td></tr>
<tr><td>isCompliant = false
complianceState = "NonCompliant"</td><td>Finding:
isCompliant = false
complianceState =“NonCompliant”</td><td>targetValue = false
targetValueDescription = "NonCompliant"</td></tr>
</table>

[3] Einige der dargestellt Informationen in „“ welche für die Tabelle 2 verwendet wurden, entspringen teilweise einer Sample Response der Policy States API [70] dem Katalog der Metriken von MEDINA [78] oder sind Selbst erstellt, um die Daten der Robert Bosch GmbH zu schützen.

Technische Umsetzung

Der in Tabelle 2 dargestellte Abbildungsansatz wird im Folgenden technisch umgesetzt. Die Beschaffung der abzubildenden Ergebnisse wurde bereits in Abbildung 18 erläutert. Abbildung 19 zeigt einen Ausschnitt aus dem Python-Skript, mit dem die relevanten Ergebnisse der Policy States API auf ein dem OSCAL Assessment Results Model ähnliches Schema abgebildet werden. Das Skript extrahiert zunächst die relevanten Informationen aus der JSON-Datei, die die Ergebnisse der Policy States API enthält. Anschließend werden die relevanten Ergebnisse auf ein speziell für diese Fallstudie entwickeltes JSON-Schema abgebildet zu sehen in Abbildung 20.

```python
assessment_results = []

for i in range(counter):

    metadata = {
        "timestamp": timestamps[i]
    }

    assessment_subject = {
        "resource": resource_ids[i],
    }

    assessment_plan = {
        "assessmentPolicy": policy_definition_ids[i],
    }

    finding = {
        "isCompliant": is_compliant_list[i],
        "complianceState":compliance_states[i]
    }

    assessment_result = {
        "metadata": metadata,
        "importAssessmentPlan": assessment_plan,
        "assessmentSubject": assessment_subject,
        "findings": finding
    }

    assessment_results.append(assessment_result)

json_data = {
    "assessmentResults": assessment_results
}

output_file_path = [redacted]
with open(output_file_path, "w") as output_file:
    json.dump(json_data, output_file, indent=4)

print("Die Assessment-Ergebnisse wurden erflogreich in JSON-Format gespeichert")
```

Abbildung 19: Python Skript zur Abbildung auf OSCAL ähnliches Schema (Eigene Darstellung)

```json
"assessmentResults": [
  {
    "metadata": {
      "timestamp": "2023-07-03T01:50:39.726521Z"
    },
    "importAssessmentPlan": {
      "assessmentPolicy": "/providers/Microsoft.Authorization/policyDefinitions/1f7c564c-0a90-4d44-b7e1-9d456cffaee8"
    },
    "assessmentSubject": {
      "resource": "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/resourcegroups/myGroup/providers/microsoft.compute/virtualmachines/test-vm"
    },
    "findings": {
      "isCompliant": false,
      "complianceState": "NonCompliant"
    }
  },
```

Abbildung 20: OSCAL ähnliches Schema (Eigene Darstellung)

Abbildung 21 zeigt einen Ausschnitt des Python-Skripts, das für die Abbildung auf eine spezifische MEDINA Metrik verwendet wurde. Da es sich um die Abbildung eines gefundenen Ergebnisses aus dem zuvor erstellten Schema handelt, ist zu beachten, dass für eine vollständige Abbildung aller gefundenen Ergebnisse eine Lookup-Tabelle erforderlich wäre, die die gefundenen Richtlinien und die entsprechende MEDINA Metrik enthält. Ein Beispiel für ein statische Abbildung auf die MEDINA-Metrik findet sich in Abbildung 22

```python
requirements = []

for i in range(counter):
    requirement = {
        "requirementId": "OPS-05.3H",
        "control": "PROTECTION AGAINST MALWARE – IMPLEMENTATION",
        "metricId": "MalwareProtectionOutput",
        "policyDefinitionId": policy_definition_id,
        "description": "This metric states whether automatic notifications are enabled (e.g. e-mail) about malware threats. This relates to EUCS' definition of "continuous monitoring".",
        "timestamp": timestamp,
        "targetValue": is_compliant,
        "targetValueDescription": compliance_state,
        "targetValueDatatype": "Boolean",
        "intervalH": "1",
        "targetResourceType": "VirtualMachine",
        "targetResource": resource_id,
        "securityFeature": "malwareProtection.applicationLogging.loggingService"
    }

    requirements.append(requirement)

    json_data = {
        "Metrics": requirements
    }

output_file_path = "medinaMetric.json"
with open(output_file_path, "w", encoding='utf-8') as output_file:
    json.dump(json_data, output_file, ensure_ascii=False, indent=4)
```

Abbildung 21: Python-Skript zur Abbildung auf Medina-Metrik (Eigene Darstellung)


```json
{
    "Metrics": [
        {
            "requirementId": "OPS-05.3H",
            "control": "PROTECTION AGAINST MALWARE – IMPLEMENTATION",
            "metricId": "MalwareProtectionOutput",
            "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/1f7c564c-0a90-4d44-b7e1-9d456cffaee8",
            "description": "This metric states whether automatic notifications are enabled (e.g. e-mail) about malware threats. This relates to EUCS' definition of "continuous monitoring".",
            "timestamp": "2023-07-03T01:50:39.726521Z",
            "targetValue": false,
            "targetValueDescription": "NonCompliant",
            "targetValueDatatype": "Boolean",
            "intervalH": "1",
            "targetResourceType": "VirtualMachine",
            "targetResource": "/subscriptions/fffedd8f-ffff-fffd-fffd-fffed2f84852/resourcegroups/myGroup/providers/microsoft.compute/virtualmachines/test-vm",
            "securityFeature": "malwareProtection.applicationLogging.loggingService"
        }
    ]
}
```


Abbildung 22: MEDINA Metrik (Eigene Darstellung)

Alle Skripte sind leicht modifiziert unter https://github.com/lluebbe/bachelor/ zu finden.

6.3 Ergebnis der Fallstudie

Die Fallstudie liefert wertvolle Einblicke und Erkenntnisse zur Verbesserung der Interoperabilität von CSPM-Werkzeugen in Multi-Cloud-Umgebungen. Demnach ist es für Unternehmen entscheidend, sich auf die wichtigsten Informationen, die zur automatischen Compliance Bewertung benötigt werden, zu konzentrieren. Dadurch ist es möglich einen Kommunikationsstandard zu entwickeln welcher eine Grundlage dafür liefert automatische Überprüfungen verschiedener Cloud-Anbieter durchzuführen und die gewonnenen Ergebnisse in einem Zentralen System darzustellen unabhängig davon, ob die CSPM-Werkzeuge vollumfängliche Information über den Zustand der überwachten Multi-Cloud-Umgebung liefern oder nicht. Es ist nicht notwendig, die gewonnenen Informationen vollständig auf das OSCAL Assessment Results Model abzubilden. Es genügt, die gewonnenen Informationen auf ein wesentlich kompakteres Schema abzubilden, das dem OSCAL Assessment Results Model nachempfunden ist. Der damit entwickelte Kommunikationsstandard ist die Voraussetzung für die Interoperabilität zwischen CSPM-Werkzeugen in der Multi-Cloud-Umgebung. Dazu wurde in dieser Fallstudie eine Methode aufgezeigt, wie die Ergebnisse der APIs verschiedener CSPM-Werkzeuge auf ein Schema ähnlich dem OSCAL Assessment Results Model abgebildet werden können, dass die wichtigsten Informationen für die Bewertung des Compliance-Status einer Cloud-Ressource enthalten. OSCAL ist dabei eine optimale Basis für den Kommunikationsstandard für die Vereinheitlichung der minimal erforderlichen Information der API-Ergebnisse von CSPM-Werkzeugen, die für die Bewertung benötigt werden. Ein aus den Ergebnissen ausgewähltes Bewertungsergebnis wurde auf der MEDINA Metrik der für die Bewertung verwendeten Richtlinie abgebildet und gibt so einen detaillierten Überblick über die auf die entsprechende Ressource angewandte Richtlinie. Die Ergebnisse der Fallstudie bestätigen die Relevanz und den Nutzen einer standardisierten Kommunikation zur Sicherstellung der Interoperabilität von CSPM-Werkzeugen in Multi-Cloud-Umgebungen. Sie bieten eine solide Grundlage für die weitere Entwicklung von Methoden und Techniken zur Verbesserung Interoperabilität.

7 Schlussfolgerung

Die Tatsache, dass viele Unternehmen heute eine Multi-Cloud-Umgebung nutzen, bringt, wie eingangs in Kapitel 1.1 erläutert, einige neue Herausforderungen in Bezug auf Sicherheit und Cybersecurity Compliance mit sich. Insbesondere Konfigurationsfehler stellen gerade in komplexen Multi-Cloud-Umgebungen ein hohes Risiko dar. Zur Überwachung werden Cloud Security Posture Management (CSPM) Werkzeuge eingesetzt, die jedoch aufgrund unterschiedlicher APIs und Datenformate der Cloud-Anbieter mit Interoperabilitätsproblemen zu kämpfen haben. Die fehlende Standardisierung erschwert die zentrale Darstellung von Compliance-Bewertungen. Um diese grundlegende Problematik zu adressieren, wurden im Rahmen dieser Bachelorarbeit verschiedene Themen wie Cloud Computing, Cybersecurity Compliance in Multi-Cloud-Umgebungen und CSPM-Werkzeuge näher beleuchtet. Dazu wurde im Rahmen dieser Arbeit ein Framework entwickelt, welches die bei der Auswahl eines CSPM-Werkzeuges unterstützen soll. Da die mangelnde Interoperabilität zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebungen ein großes Problem darstellt, wurde anhand einer Fallstudie ein praktischer Ansatz aufgezeigt, um die Interoperabilität zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebungen zu verbessern. Damit können generell Sicherheitsaudits in Multi-Cloud-Umgebungen effizienter durchgeführt werden und eine übersichtliche Darstellung von Sicherheitsbewertungen gewährleistet werden.

7.1 Zusammenfassung der Ergebnisse

Das im Rahmen der Bachelorarbeit entwickelte Framework bietet die Möglichkeit, bei der Auswahl eines geeigneten CSPM-Werkzeuges zu unterstützen, sodass Unternehmen das für ihre Anforderungen passende Werkzeug auswählen können. Somit bietet das Framework die Möglichkeit, Ressourcen für die Analyse und den Vergleich zu sparen, Kosten zu senken und möglicherweise redundante Prozesse eliminieren zu können. Es ist dabei zwar möglich, durch das in Kapitel 5.1 vorgestellte Framework einen generellen Vergleich darüber zu machen, ob die grundlegenden Funktionen, welche in einer Multi-Cloud-Umgebung relevant sind, von den verschiedenen CSPM-Werkzeugen bereitgestellt werden. Die Auswahl von CSPM-Werkzeugen bleibt jedoch letztlich ein sehr individueller Prozess, bei dem sowohl die technischen Anforderungen an das CSPM-Werkzeug als auch die mit dem Einsatz eines CSPM-Werkzeugs verbundenen Kosten genau auf die Anforderungen und finanziellen Möglichkeiten des Unternehmens abgestimmt werden müssen. Man kann also nicht pauschal ein CSPM-Werkzeug zur Überwachung einer Multi-Cloud-Umgebung als die optimale Lösung empfehlen.

Bei der Auswahl oder der Suche nach einem geeigneten CSPM-Werkzeug kann es vorkommen, dass mehr als ein CSPM-Werkzeug benötigt wird, da bestimmte Funktionen, die benötigt werden, nicht optimal von einem anderen CSPM-Werkzeug bereitgestellt werden. In diesem Fall kann die zentrale Darstellung der gesammelten Bewertungsergebnisse eine große Herausforderung darstellen. Der im Rahmen der Fallstudie vorgeschlagene Lösungsansatz sieht daher vor, dass es einen einheitlichen Kommunikationsstandard geben sollte, welcher als Grundlage zur Realisierung der Interoperabilität zwischen CSPM-Werkzeugen in Multi-Cloud-Umgebungen dient.

Die Durchführung der Fallstudie hat dazu beigetragen, das eingangs in Kapitel 1.2 definierte Ziel zu erreichen. Durch die gewonnenen Einblicke und Erkenntnisse konnte die Interoperabilität von CSPM-Werkzeugen, die zur Überwachung von Multi-Cloud-Umgebungen eingesetzt werden, verbessert werden in dem ein Lösungsansatz vorgestellt wurde, der einen Weg aufzeigt, wie die Ergebnisse von CSPM-Werkzeugen in einem Kommunikationsstandard vereinheitlicht und für die Darstellung und Verarbeitung in einem zentralen System optimal aufbereitet werden können. Zu diesem Zweck wurde eine Methode entwickelt, die die Bewertungsergebnisse verschiedener Werkzeug-APIs auf ein Schema abbildet, das dem in Kapitel 6.1.2 näher beschriebenen OSCAL Assessment Results Model ähnelt. Dabei konzentriert sich das Schema auf die wichtigsten Informationen, die zur Bewertung des Compliance-Status einer Cloud-Ressource benötigt werden. Das Schema definiert somit die Mindestinformationen, die zur Bewertung des Compliance-Status erforderlich sind. OSCAL erwies sich als eine optimale Basis für den Kommunikationsstandard zur Vereinheitlichung der minimal erforderlichen Informationen, natürlich vor dem Hintergrund, dass OSCAL vom National Institute of Standards and Technology (NIST) entwickelt wird. Das Ergebnis dieses standardisierten Schemas wurde dann auf die MEDINA-Metrik abgebildet, die für die zur Bewertung des Compliance-Status verwendete Richtlinie geeignet ist. Somit liefert die Durchführung der Fallstudie eine solide Basis für die Weiterentwicklung des vorgestellten Lösungsansatzes und trägt somit zur Verbesserung der Interoperabilität in Multi-Cloud-Umgebungen bei, was eine bessere Sichtbarkeit gewährleistet und somit die Cloud Security insgesamt verbessert.

7.2 Handlungsempfehlungen für Unternehmen

Unternehmen sollten vor der Auswahl von CSPM-Werkzeugen eine umfassende Bestandsaufnahme ihrer Multi-Cloud-Umgebungen durchführen. Dabei sollten sie feststellen, welche Cloud-Anbieter Teil ihrer Multi-Cloud-Umgebung sind, welche Funktionen für die Überwachung des Compliance-Status relevant sind und wie hoch das Budget ist, welches ihnen zur Verfügung steht. Anschließend können sie das im Rahmen der Arbeit entwickelte Framework für einen Vergleich nutzen und ggf. um

spezifische Funktionalitäten erweitern, die benötigt werden. Um die Interoperabilität zwischen den CSPM-Werkzeugen in ihrer Multi-Cloud-Umgebung sicherzustellen, sollten Unternehmen die Weiterentwicklung des in der Fallstudie vorgestellten Lösungsansatzes in Betracht ziehen. Dazu könnten sie eine automatisierte Pipeline entwickeln, die automatisch wichtige Informationen für die Bewertung des Compliance-Status von einer API eines beliebigen CSPM-Werkzeuges abfragt und diese in das vorgestellte Schema ähnlich dem OSCAL Assessment Results Model abbildet, um sie dann durch einen Abgleich mit einer Lookup-Tabelle auf eine MEDINA Metrik abzubilden.

7.3 Ausblick

Das entwickelte Framework zum Vergleich und zur Analyse von CSPM-Werkzeugen in Multi-Cloud-Umgebungen hat ein vielversprechendes Potenzial zur Weiterentwicklung, um Unternehmen bei der Auswahl und Implementierung von CSPM-Werkzeugen zu unterstützen. Für die Weiterentwicklung des vorgestellten Frameworks gibt es verschiedene Möglichkeiten: Eine Option wäre, die für den Vergleich der CSPM-Werkzeuge genutzten Funktionen zu erweitern, beispielsweise um Aspekte wie Skalierbarkeit und Integration mit anderen Sicherheitswerkzeugen. Darüber hinaus sollte das Framework regelmäßig mit den neuesten CSPM-Werkzeugen aktualisiert werden, um bei der Auswahl auf die neuesten Technologien zurückgreifen zu können. In Zeiten der ständigen Reizüberflutung ist es besonders wichtig, sich auf das Wesentliche zu konzentrieren, so auch bei der Überwachung des Compliance-Status der Multi-Cloud-Umgebungen durch CSPM-Werkzeuge. Durch die Beschreibung eines einheitlichen Kommunikationsstandards auf Basis des Assessment Results Model von OSCAL, ist es für Unternehmen möglich, sich auf die wichtigsten Informationen zu Konzentrieren die notwendig sind, um eine Bewertung des Compliance-Status der Multi-Cloud-Umgebung durchzuführen. Die Notwendigkeit einer stetigen Weiterentwicklung dieses Standards wurde bereits in Angriff genommen und die im Rahmen dieser Bachelorarbeit gewonnenen Erkenntnisse werden an das National Institute of Standards and Technology (NIST) zur weiteren Untersuchung und eventuellen Weiterentwicklung weitergeleitet. So könnte es in Zukunft einen frei verfügbaren einheitlichen Kommunikationsstandard geben, der das Problem der Interoperabilität zwischen CSPM-Werkzeugen beseitigt und gleichzeitig die wichtigsten Informationen enthält, die für die Bewertung Compliance-Status benötigt werden. So könnte unabhängig davon, welche Informationen die verschiedenen APIs der CSPM-Werkzeuge liefern, durch den einheitlichen Kommunikationsstandard sichergestellt werden, dass die wichtigsten Informationen zur Bewertung des Compliance-Status zur Verfügung stehen. Sodass auch bei der Verwendung mehrerer CSPM-Werkzeuge eine einfache Bewertung des Compliance-Status der Cloud-Ressourcen durchgeführt werden kann. Darauf aufbauend wäre es sinnvoll, eine vollständige Lookup-

Tabelle mit allen benötigten Richtlinien der verschiedenen CSPM-Anbieter mit den entsprechenden MEDINA Metriken zu entwickeln. Diese kann als Grundlage für eine übersichtliche Darstellung im MEDINA Security Framework dienen und somit einen Überblick über den Compliance-Status der Multi-Cloud-Umgebung in einem zentralen System gewährleisten.

Literaturverzeichnis

[1] Orcale, „Was versteht man unter Cloud-Computing?," Orcale, [Online]. Available: https://www.oracle.com/de/cloud/what-is-cloud-computing/. [Zugriff am 22 05 2023].

[2] Cloudflare, „Was ist Multi-Cloud? | Multi-Cloud Definition," Cloudflare, o.D. [Online]. Available: https://www.cloudflare.com/de-de/learning/cloud/what-is-multicloud/. [Zugriff am 10 07 2023].

[3] A. S. Gillis, „Cloud Security Posture Management (CSPM)," 01 2021. [Online]. Available: https://www.computerweekly.com/de/definition/Cloud-Security-Posture-Management-CSPM. [Zugriff am 02 03 2023].

[4] L. Goasduff, „Why Organizations Choose a Multicloud Strategy," Gartner, 07 05 2019. [Online]. Available: https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy. [Zugriff am 10 07 2023].

[5] Accenture, „Navigating the interoperability challenge in multi-cloud environments," 03 07 2019. [Online]. Available: https://www.accenture.com/us-en/blogs/cloud-computing/kishore-durg-cloud-interoperability-challenges. [Zugriff am 06 06 2023].

[6] H. Wieler, „Herausforderungen bei Multi-Cloud-Sicherheit und Compliance," Infopoint, 03 02 2022. [Online]. Available: https://www.infopoint-security.de/herausforderungen-bei-multi-cloud-sicherheit-und-compliance/a30252/. [Zugriff am 04 05 2023].

[7] P. Mell und T. Grance , „The NIST Definition of Cloud Computing," 09 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final. [Zugriff am 07 07 2023].

[8] „Cloud computing - statistics on the use by enterprises," 22 06 2022. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises. [Zugriff am 02 07 2023].

[9] Red Hat, „Die wichtigsten Cloud-Modelle und Cloud-Services," Red Hat, 18 03 2018. [Online]. Available: https://www.redhat.com/de/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud. [Zugriff am 19 04 2023].

[10] Fraunhofer, „Public, Private und Hybrid Cloud?," Fraunhofer, o.D. [Online]. Available: https://www.cloud.fraunhofer.de/de/faq/publicprivatehybrid.html. [Zugriff am 21 04 2023].

[11] Cloudflare, „Was ist eine Public Cloud?," Cloudflare, o.D. [Online]. Available: https://www.cloudflare.com/de-de/learning/cloud/what-is-a-public-cloud/. [Zugriff am 02 07 2023].

[12] Google Cloud, „Was ist eine Hybrid-Cloud?," Google Cloud, o.D. [Online]. Available: https://cloud.google.com/learn/what-is-hybrid-cloud?hl=de. [Zugriff am 06 06 2023].

[13] Red Hat, „Was ist eine Hybrid Cloud?," Red Hat, 20 10 2022. [Online]. Available: https://www.redhat.com/de/topics/cloud-computing/what-is-hybrid-cloud. [Zugriff am 10 07 2023].

[14] Cloudflare, „Was bedeutet „Hybrid Cloud“?,“ Cloudflare, o.D. [Online]. Available: https://www.cloudflare.com/de-de/learning/cloud/what-is-hybrid-cloud/. [Zugriff am 13 07 2023].

[15] Cloudflare, „Multi-Cloud oder Hybrid Cloud: Was ist der Unterschied?,“ Cloudflare, o.D. [Online]. Available: https://www.cloudflare.com/de-de/learning/cloud/multicloud-vs-hybrid-cloud/. [Zugriff am 20 04 2023].

[16] S. Luber, „Was ist eine Multi Cloud?,“ Cloudcomputing Insider, 25 10 2017. [Online]. Available: https://www.cloudcomputing-insider.de/was-ist-eine-multi-cloud-a-654964/. [Zugriff am 10 03 2023].

[17] Red Hat, „Vergleich von IaaS, PaaS und SaaS,“ Red Hat, 16 08 2022. [Online]. Available: https://www.redhat.com/de/topics/cloud-computing/iaas-vs-paas-vs-saas. [Zugriff am 09 06 2023].

[18] IBM, „Was ist Cloud-Sicherheit?,“ IBM, o.D. [Online]. Available: https://www.ibm.com/de-de/topics/cloud-security. [Zugriff am 24 05 2023].

[19] J.-M. C. Brook, V. Chin, H. Foskett, A. Getzin, V. Hargrave, S. Levy, A. McCormick, S. Pieraldi, M. Roza, M. Ryan, A. Schindel und S. Shamban, „Top Threats to Cloud Computing,“ 06 06 2022. [Online]. Available: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/. [Zugriff am 30 06 2023].

[20] IBM Security, „Bericht über die Kosten einer Datenschutzverletzung 2022,“ IBM Security, 07 2022. [Online]. Available: https://www.ibm.com/downloads/cas/DG4NV420. [Zugriff am 12 07 2023].

[21] A. T. Tunggal, „What is an Incident Response Plan?,“ upguard, 20 04 2023. [Online]. Available: https://www.upguard.com/blog/incident-response-plan. [Zugriff am 05 05 2023].

[22] A. Rudra, „Cybersecurity Compliance 101,“ 28 06 2022. [Online]. Available: https://powerdmarc.com/de/cybersecurity-compliance/. [Zugriff am 29 06 2023].

[23] K. Leisering, „Compliance: Definition, Bedeutung & Tipps für den Einstieg,“ 08 12 2022. [Online]. Available: https://www.eqs.com/de/compliance-wissen/blog/was-ist-compliance/. [Zugriff am 21 04 2023].

[24] J. DeCesare, „www.ispartnersllc.com,“ 26 08 2022. [Online]. Available: https://www.ispartnersllc.com/blog/automation-cybersecurity-compliance/. [Zugriff am 24 05 2023].

[25] ISO, ISO, o.D. [Online]. Available: https://www.iso.org/home.html. [Zugriff am 11 07 2023].

[26] IEC, IEC, o.D. [Online]. Available: https://iec.ch/homepage. [Zugriff am 14 07 2023].

[27] ISO, „ISO/IEC 27001,“ ISO, 10 2022. [Online]. Available: https://www.iso.org/standard/27001. [Zugriff am 08 05 2023].

[28] Bundesamt für Sicherheit in der Informationstechnik, „C5 Einführung,“ Bundesamt für Sicherheit in der Informationstechnik, o.D. [Online]. Available:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/C5_Einfuehrung_node.html. [Zugriff am 08 05 2023].

[29] Specops, „NIST 800-53 Richtlinien und Anforderungen," Specops, 09 11 2022. [Online]. Available: https://specopssoft.com/de/blog/nist-800-53-richtlinien-und-anforderungen/. [Zugriff am 08 05 2023].

[30] NIST, „Security and Privacy Controls for Information Systems and Organizations," NIST, o.D. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. [Zugriff am 08 05 2023].

[31] Redaktion ComputerWeekly.de, TechTarget, „SOC 2 (Service Organization Control 2)," ComputerWeekly, 04 2012. [Online]. Available: https://www.computerweekly.com/de/definition/SOC-2-Service-Organization-Control-2. [Zugriff am 08 05 2023].

[32] DataGuard, „SOC 2 oder ISO 27001 Zertifizierung: Vergleich der InfoSec Standards," DataGuard, 14 12 2022. [Online]. Available: https://www.dataguard.de/blog/soc-2-vs-iso-27001. [Zugriff am 09 05 2023].

[33] Robert Bosch GmbH, „BOSCH EISA," Robert Bosch GmbH, o.D. [Online]. Available: interne Information. [Zugriff am 04 07 2023].

[34] RiskOptics, „What is Compliance in Cybersecurity?," RiskOptics, 8 04 2022. [Online]. Available: https://reciprocity.com/resources/what-is-compliance-in-cybersecurity/. [Zugriff am 30 06 2023].

[35] it-daily, „Multi-Cloud-Sicherheit und Compliance," 07 02 2022. [Online]. Available: https://www.it-daily.net/it-sicherheit/cloud-security/multi-cloud-sicherheit-und-compliance. [Zugriff am 04 05 2023].

[36] AWS, „Modell der geteilten Verantwortung," AWS, o.D. [Online]. Available: https://aws.amazon.com/de/compliance/shared-responsibility-model/. [Zugriff am 02 07 2023].

[37] Computerfutures, „Ab in die Cloud – doch was ist bei der Compliance zu beachten?," Computerfutures, 24 12 2021. [Online]. Available: https://www.computerfutures.com/de-de/wissens-hub/cloud-technologien/ab-in-die-cloud-doch-was-ist-bei-der-compliance-zu-beachten/. [Zugriff am 04 05 2023].

[38] Bundesamt für Sicherheit in der Informationstechnik, „Cloud-Zertifizierung," Bundesamt für Sicherheit in der Informationstechnik, o.D. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Cloud-Zertifizierung/cloud-zertifizierung_node.html. [Zugriff am 04 05 2023].

[39] Checkpoint, „What is a Cloud Security Misconfiguration?," Checkpoint, o.D. [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/what-is-a-cloud-security-misconfiguration/. [Zugriff am 12 06 2023].

[40] Crowdstrike, „Best Practices der Cloud Security," Crowdstrike, 17 11 2022. [Online]. Available: https://www.crowdstrike.de/cybersecurity-101/cloud-security/cloud-security-best-practices/. [Zugriff am 04 05 2023].

[41] D. Puzas, „Was ist Sicherheitsverwaltung für Cloud-umgebungen (CSPM)?," Crowdstrike, 16 03 2022. [Online]. Available: https://www.crowdstrike.de/cybersecurity-101/cloud-security/cloud-security-posture-management-cspm/. [Zugriff am 16 05 2023].

[42] S. Luber, „Was ist ein Cloud Access Security Broker (CASB)?," Security-Insider, 26 07 2017. [Online]. Available: https://www.security-insider.de/was-ist-ein-cloud-access-security-broker-casb-a-627324/. [Zugriff am 16 05 2023].

[43] Cloudflare, „Was ist eine Cloud Workload Protection Platform (CWPP)?," Cloudflare, o.D. [Online]. Available: https://www.cloudflare.com/de-de/learning/cloud/what-is-cwpp/. [Zugriff am 16 05 2023].

[44] R. Bartley, „Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services," Gartner , 2018.

[45] P. Shelton, „Understand the Essential Capabilities of Cloud Security Posture Management Tools," o.D. [Online]. Available: https://www.cdw.com/content/cdw/en/articles/security/understand-the-essential-capabilities-of-cloud-security-posture-management-tools.html. [Zugriff am 29 06 2023].

[46] Microsoft Azure, „Microsoft Defender for Cloud," Microsoft Azure, o.D. [Online]. Available: https://azure.microsoft.com/de-de/products/defender-for-cloud. [Zugriff am 04 07 2023].

[47] GitHub Benutzernamen, ElazarK, helderpinto, prmerger-automator[bot], bmansheim, AlizaBernstein, rayne-wiselman, msmbaldwin, v-stsavell, yehKardos und memildin, „Tutorial: Verbessern der Einhaltung gesetzlicher Vorschriften," Microsoft Azure, 22 06 2023. [Online]. Available: https://learn.microsoft.com/de-de/azure/defender-for-cloud/regulatory-compliance-dashboard. [Zugriff am 29 06 2023].

[48] J. Grange, „The Challenges Managing Multi-Cloud Environments," 5 05 2021. [Online]. Available: https://opscompass.com/resources/blog/the-challenges-managing-multi-cloud-environments/. [Zugriff am 22 03 2023].

[49] D. Shackleford, „How cloud security posture management protects multi-cloud," Voodoo Security, o.D. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/How-cloud-security-posture-management-protects-multi-cloud. [Zugriff am 22 03 2023].

[50] P. Gillin, „The importance of IT frameworks," TechTarget, 03 2021. [Online]. Available: https://www.techtarget.com/whatis/reference/The-importance-of-IT-frameworks. [Zugriff am 27 06 2023].

[51] M. Zhang, „Top 10 Cloud Service Providers Globally in 2023," 01 01 2023. [Online]. Available: https://dgtlinfra.com/top-10-cloud-service-providers-2022/. [Zugriff am 06 07 2023].

[52] Gartner, „Cloud Security Posture Management Tools Reviews and Ratings," Gartner, o.D. [Online]. Available: https://www.gartner.com/reviews/market/cloud-security-posture-management-tools. [Zugriff am 06 07 2023].

[53] AWS, „AWS Security Hub features," AWS, o.D. [Online]. Available: https://aws.amazon.com/de/security-hub/features/?nc=sn&loc=2. [Zugriff am 29 06 2023].

[54] GitHub Benutzernamen, ElazarK, memildin, prmerger-automator[bot], AlizaBernstein, mrmonaco22, orserokjeppa, rayne-wiselman, huypub, Shereen-Bhar, helderpinto, bmansheim und shsagir, „Cloud Security Posture Management (CSPM)," Microsoft Azure, 25 06 2023. [Online]. Available: https://learn.microsoft.com/de-de/azure/defender-for-cloud/concept-cloud-security-posture-management. [Zugriff am 29 06 2023].

[55] Google Cloud, „Security Command Center," Google Cloud, o.D. [Online]. Available: https://cloud.google.com/security-command-center?hl=de#section-6. [Zugriff am 28 03 2023].

[56] Palo Alto Networks, „Cloud Security Posture Management," Palo Alto Networks, o.D. [Online]. Available: https://www.paloaltonetworks.com/prisma/cloud/cloud-security-posture-management. [Zugriff am 03 04 2023].

[57] AWS, „Referenz zu Security Hub Standards," AWS, o.D. [Online]. Available: https://docs.aws.amazon.com/de_de/securityhub/latest/userguide/standards-reference.html. [Zugriff am 29 06 2023].

[58] GitHub Benutzernamen, ElazarK, bmansheim, AlizaBernstein, yura-lee, v-dirichards, LianaT, computeronix und memildin, „What regulatory compliance standards are available in Defender for Cloud?," 18 06 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulatory-compliance-standards-are-available-in-defender-for-cloud. [Zugriff am 29 06 2023].

[59] Google Cloud, „Detektoren und Compliance," Google Cloud, o.D. [Online]. Available: https://cloud.google.com/security-command-center/docs/concepts-security-health-analytics?hl=de#sha_compliance. [Zugriff am 29 06 2023].

[60] Palo Alto Networks, „Visibility, Compliance and Governance," Palo Alto Networks, o.D. [Online]. Available: https://www.paloaltonetworks.com/prisma/cloud/visibility-compliance-governance. [Zugriff am 29 06 2023].

[61] AWS, „AWS ConfigRegeln hinzufügen, aktualisieren und löschen," AWS, o.D. [Online]. Available: https://docs.aws.amazon.com/de_de/config/latest/developerguide/evaluate-config_manage-rules.html. [Zugriff am 06 07 2023].

[62] GitHub Benutzernamen, AlizaBernstein, dcurwin, bomagusi, memildin und bmansheim, „Create custom recommendations and security standards," 28 03 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/defender-for-cloud/create-custom-recommendations. [Zugriff am 01 07 2023].

[63] Google Cloud, „Ergebnisse und Abhilfemaßnahmen scannen," Google Cloud, o.D. [Online]. Available: https://cloud.google.com/security-command-center/docs/concepts-rapid-

vulnerability-detection-overview?hl=de#scan_findings_and_remediations. [Zugriff am 06 07 2023].

[64] Palo Alto Networks, „Create a Custom Compliance Standard," Palo Alto Networks, 29 06 2023. [Online]. Available: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard. [Zugriff am 01 07 2023].

[65] Palo Alto Networks, „Connect Your Cloud Platform to Prisma Cloud," Palo Alto Networks, o.D. [Online]. Available: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/connect-your-cloud-platform-to-prisma-cloud. [Zugriff am 12 07 2023].

[66] AWS, „aws.amazon.com," AWS, o.D. [Online]. Available: https://aws.amazon.com/de/security-hub/pricing/. [Zugriff am 01 07 2023].

[67] Google Cloud, „cloud.google.com," Google Cloud, o.D. [Online]. Available: https://cloud.google.com/security-command-center/pricing?hl=de. [Zugriff am 03 04 2023].

[68] National Institute of Standards and Technology, „Learn more about OSCAL," National Institute of Standards and Technology, 16 06 2023. [Online]. Available: https://pages.nist.gov/OSCAL/about/. [Zugriff am 28 06 2023].

[69] Medina, „Mission and Vision," Medina, o.D. [Online]. Available: https://medina-project.eu/mission-and-vision/. [Zugriff am 28 06 2023].

[70] Microsoft Azure, „Policy States - List Query Results For Subscription," Microsoft Azure, o.D. [Online]. Available: https://learn.microsoft.com/en-us/rest/api/policy/policy-states/list-query-results-for-subscription?tabs=HTTP#query-latest-at-subscription-scope. [Zugriff am 29 06 2023].

[71] J. O. Orlik, „Proprietäre Software," in *Konzept einer mittelständischen Controlling-Lösung basierend auf einer Open Source Software*, Hamburg, Diplomica Verlag, 2010, p. 16.

[72] Euroscal, „The EU Friends of OSCAL," Euroscal, o.D. [Online]. Available: https://euroscal.eu/. [Zugriff am 11 07 2023].

[73] National Institute of Standards and Technology, „OSCAL Assessment Layer: Assessment Results Model," National Institute of Standards and Technology, o.D. [Online]. Available: https://pages.nist.gov/OSCAL/concepts/layer/assessment/assessment-results/. [Zugriff am 28 06 2023].

[74] Medina, „medina-project.eu," Medina, o.D. [Online]. Available: https://medina-project.eu/partners/. [Zugriff am 28 06 2023].

[75] H. Ratkajec, I. Kunz, F. J. Deimling und C. Regueiro, „3.6 The Generic Evidence Collector (GEC)," Medina, 30 04 2023. [Online]. Available: https://medina-project.eu/wp-content/uploads/2023/05/MEDINA_D3.3_Tools_and_techniques_for_the_management_of_trustworthy_evidence-v3_v1.0.pdf. [Zugriff am 09 07 2023].

[76] Microsoft, „Query latest at subscription scope Sample Request,“ Microsoft, o.D. [Online]. Available: https://learn.microsoft.com/en-us/rest/api/policy/policy-states/list-query-results-for-subscription?tabs=Python#query-latest-at-subscription-scope. [Zugriff am 12 07 2023].

[77] t2informatik, „Metrik – ein Maß für Leistung oder Fortschritt,“ t2informatik, o.D. [Online]. Available: https://t2informatik.de/wissen-kompakt/metrik/. [Zugriff am 07 07 2023].

[78] Medina, „Appendix 2: MEDINA Security metrics,“ Medina, o.D. [Online]. Available: https://medina-project.eu/wp-content/uploads/2023/05/MEDINA_D2.2_Continuously-certifiable-technical-and-organizational-measures-and-Catalogue-of-cloud-security-metrics-v2_v1.0.pdf. [Zugriff am 09 07 2023].