

Inhaltsverzeichnis

Inhaltsverzeichnis	I
Abkürzungsverzeichnis	III
Abbildungsverzeichnis	III
Tabellenverzeichnis	IV
1 Einleitung.....	1
1.1 Motivation.....	1
1.2 Unternehmensvorstellung	2
1.3 Grundlagen	3
1.3.1 Sicherheitsrelevante Begrifflichkeiten und Verfahren	3
1.3.1.1 Authentifizierung und Autorisierung	3
1.3.1.2 JSON-Web-Token	4
1.3.1.3 Authorization Code Flow with Proof-Key-of-Code-Exchange.....	5
1.3.2 Einführung in die Cloud Taxonomie	5
1.3.2.1 Infrastructure-as-a-Service	6
1.3.2.2 Platform-as-a-Service.....	6
1.3.2.3 Software-as-a-Service.....	7
2 Hauptteil.....	8
2.1 Beschreibung des operationalisierbaren Szenarios	8
2.2 Kriterien-Bereiche für die Analyse	10
2.2.1 Organisation der Informationssicherheit (OIS)	10
2.2.2 Sicherheitsrichtlinien und Arbeitsanweisungen (SP).....	11
2.2.3 Personal (HR)	11
2.2.4 Asset Management (AM)	11
2.2.5 Physische Sicherheit (PS)	12
2.2.6 Regelbetrieb (OPS)	12
2.2.7 Identitäts- und Berechtigungsmanagement (IDM)	13

2.2.8	Kryptographie und Schlüsselmanagement (CRY).....	14
2.2.9	Kommunikationssicherheit (COS)	14
2.2.10	Portabilität und Interoperabilität (PI)	15
2.2.11	Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) ...	15
2.2.12	Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)	16
2.2.13	Umgang mit Sicherheitsvorfällen (SIM)	16
2.2.14	Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)	17
2.2.15	Compliance (COM).....	17
2.2.16	Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ).....	18
2.2.17	Produktsicherheit (PSS)	18
2.3	Kriterienkatalog für die STP Cloud	19
2.4	Maßnahmen zu der Optimierung des Ergebnisses	21
2.5	Analyse der vorhandenen Sicherheitskonzepte.....	21
2.5.1	Ist-Zustand.....	21
2.5.2	Soll-Zustand.....	23
2.6	Erkennung und Prävention von Gefahren	23
2.6.1	Konzeption einer Testumgebung	23
2.6.2	Mögliche Architektur mit ML.NET Proxy Service.....	24
3	Schluss	25
4	Literaturverzeichnis	25

Abkürzungsverzeichnis

IaaS*Infrastructure-as-a-Service*

Abbildungsverzeichnis

Abbildung 1 JSON-Web-Token in kodierten und dekodierten Zustand.....	4
Abbildung 2 Verantwortung über die genutzten Cloud Services. Grafik: Security Guidance v4.0, CSA	6
Abbildung 3 Verantwortung von Cloud Kunde und Cloud Betreiber Quelle: https://www.magenium.com/magenium/Magenium_Cloud_Services_Diagram.jpg	7
Abbildung 4 Vereinfachte Darstellung der STP Cloud SaaS-Lösung.....	22
Abbildung 5 Testumgebung für die Simulation der realen Anwendungslandschaft.....	24
Abbildung 6 Beispiel-Architektur mit zusätzlichem Service für die Prüfung der eingehenden Requests mit Möglichkeit zum Throttling.....	24

Tabellenverzeichnis

Tabelle 1 Anwendbare Kriterien aus dem Bereich OIS	10
Tabelle 2 Anwendbare Kriterien aus dem Bereich SP	11
Tabelle 3 Anwendbare Kriterien aus dem Bereich HR.....	11
Tabelle 4 Anwendbare Kriterien aus dem Bereich AM	12
Tabelle 5 Anwendbare Kriterien aus dem Bereich PS	12
Tabelle 6 Anwendbare Kriterien aus dem Bereich OPS	13
Tabelle 7 Anwendbare Kriterien aus dem Bereich IDM	13
Tabelle 8 Anwendbare Kriterien aus dem Bereich CRY	14
Tabelle 9 Anwendbare Kriterien aus dem Bereich COS.....	14
Tabelle 10 Anwendbare Kriterien aus dem Bereich PI.....	15
Tabelle 11 Anwendbare Kriterien aus dem Bereich DEV	15
Tabelle 12 Anwendbare Kriterien aus dem Bereich SSO	16
Tabelle 13 Anwendbare Kriterien aus dem Bereich SIM	16
Tabelle 14 Anwendbare Kriterien aus dem Bereich BCM.....	17
Tabelle 15 Anwendbare Kriterien aus dem Bereich COM.....	17
Tabelle 16 Anwendbare Kriterien aus dem Bereich INQ	18
Tabelle 17 Anwendbare Kriterien aus dem Bereich PSS	18
Tabelle 18 Bewertungskriterien und Erfüllungsgrad für die Bewertung der STP Cloud	19
Tabelle 19 Grafische Darstellung mit prozentualer Verteilung des Erfüllungsgrades.....	21

1 Einleitung

1.1 Motivation

Gestützt durch Vorfälle aus jüngster Zeit ist die Sicherheit in der Informationstechnologie für Firmen auf der ganzen Welt zu einem immer mehr an Bedeutung gewinnenden Bestandteil geworden. Als Folge der aktuellen Angriffe wie zum Beispiel das unautorisierte Entwenden von mehr als 500 Millionen Nutzerdaten von Facebook [1] oder das Ausnutzen der Schwachstellen der Microsoft Exchange Server in zahlreichen Unternehmen [2] nehmen immer mehr Firmen die IT-Sicherheit ihrer Produkte genauer in den Fokus. Dies gilt nicht nur für Software wie native Applikationen auf Mobiltelefonen oder Desktopanwendungen, sondern auch für Anwendungen, die ihren Nutzern als Clouddienste zur Verfügung stehen und öffentlich über das Internet erreichbar sind. Jedoch sind Kriterien, die für die Absicherung dieser Dienste gedacht sind, wie zum Beispiel des National Institut for Standards and Technology (NIST), der Cloud Security Alliance (CSA) oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) nur wenig verbreitet und werden von den betreffenden Firmen mehr oder weniger umgesetzt. Des Weiteren ist festzustellen, dass sich die aufgezählten Kriterienkataloge immer wieder aufeinander beziehen, jedoch keine einheitliche Norm zur Regelung und Umsetzung der Sicherheitskriterien vorliegt. Als Richtlinie und Maßstab für zukünftige Entwicklungen an Cloudprodukten sollte jedes Unternehmen einen Katalog an bestehenden Sicherheitsmaßnahmen und Regularien entwerfen, der den Endnutzern ein gewisses Maß an Sicherheit garantiert.

1.2 Unternehmensvorstellung

Die STP Informationstechnologie GmbH (nachfolgend kurz: STP GmbH) ist ein in Karlsruhe gegründetes IT-Unternehmen. Der Schwerpunkt der angebotenen Softwarelösungen und Informationssysteme zielt auf die Anwendungen in den Berufsgruppen im Rechtssektor wie Anwälte, Justizverwaltungen und weiteren fachnahen Institutionen ab. Gegründet wurde das Unternehmen im Jahr 1993 von Gunter Thies und Ralph Suikat als „Suikat-Thies + Partner GmbH“. Im Jahre 2001 wurde die Unternehmensform in eine Aktiengesellschaft umgewandelt [3]. Die STP AG im Rahmen eines Zertifizierungsprogramms durch SGS-International Certification Services GmbH nach DIN ISO 9001 zertifiziert. Seit November 2011 gilt dieses Zertifikat für die komplette STP Gruppe: STP Informationstechnologie AG, STP Holding GmbH, STP Portal GmbH und STP Solution GmbH. Seit dem 05. März 2021 ist die STP von einer Aktiengesellschaft in eine GmbH umfirmiert [3].

Intern untergliedert sich die STP weiterhin in einzelne Abteilungen, Arbeitsbereiche und -gruppen, die mit verschiedenen Themen betraut sind. Der Schwerpunkt jeder einzelnen Abteilung liegt auf einem anderen Gebiet der Software- bzw. Produktentwicklung.

Der Fokus bei der Softwareentwicklung liegt jedoch primär auf der Umsetzung von Kundenlösungen mit dem .NET-Framework. Die Produktpalette umfasst neben On-Premise Lösungen, die lokal beim Kunden eingesetzt werden, auch Dienstleistungen wie Consulting- bzw. Beratungslösungen, die von internen Beratern bzw. Fachbearbeitern angeboten werden.

Der Wirkungsbereich der STP Informationstechnologie umfasst die gesamte DACH-Region. Dies bedeutet, es werden neben Kunden aus Deutschland auch Kunden aus der Schweiz, Standort der jüngsten Zweigstelle, und Österreich betreut. Die Niederlassung in Bulgarien fungiert in diesem Unternehmensverbund bisher als Zuarbeiter für spezielle Aufgaben der Entwicklung.

Das erarbeitete Projekt wurde hauptsächlich in der Abteilung Produktentwicklung (PDE) mit Betreuung durch Manuel Naujoks durchgeführt und erarbeitet. Der Fokus dieser Abteilung liegt auf der Evaluation und Verwendung von neuen Technologien im Ökosystem .NET, die bei der Entwicklung von neuen hauseigenen Produkten verwendet werden sollen.

1.3 Grundlagen

1.3.1 Sicherheitsrelevante Begrifflichkeiten und Verfahren

1.3.1.1 Authentifizierung und Autorisierung

Aufgrund der Relevanz der Begriffe **Authentifizierung** und **Autorisierung** im Bereich der Informationssicherheit werden diese zunächst zum allgemeinen Verständnis in den Kontext eingeordnet und erläutert.

Beginnend mit dem Begriff der **Authentifizierung**. Für das nachfolgende theoretische Beispiel wird von einer Kommunikation zwischen einem menschlichen Nutzer mit einer Anwendung (Maschine) ausgegangen.

Die Authentifizierung des Nutzers bei einer Anwendung ist in vielen Fällen der erste Schritt, wenn der Nutzer Zugriff auf geschützte Ressourcen, wie zum Beispiel die Daten seines Profils in einem sozialen Netzwerk haben möchte. Hierzu wird er vom System bzw. der Anwendung zuerst aufgefordert den Usernamen und sein Passwort (nachfolgend Zugangsdaten) einzugeben. Diesen Vorgang der Authentifizierung nutzt die Anwendung, um zu prüfen, ob es sich bei dem vorliegenden Nutzer wirklich um den Nutzer handelt, der er vorgibt zu sein. Stimmen die Zugangsdaten, die meistens via Abgleich von verschlüsselten Werten in der Datenbank überprüft werden, mit den angegebenen Werten überein, ist der Nutzer erfolgreich authentifiziert. Ist dies nicht der Fall, wird dem Nutzer der Zugriff verwehrt. Bei erfolgreicher Authentifizierung erhält der Nutzer in den meisten Fällen ein Token, der ihm als Beweis seiner Identität dient, um sich gegenüber dem System auszuweisen. Somit wird verhindert, dass bei erneuter Interaktion des Nutzers mit dem System, dieser sich erneut anmelden muss.

Bei der **Autorisierung** kommt der bereits genannte Token zum Einsatz. Möchte der Nutzer nun auf die Daten seines Profils zugreifen, sendet er neben dem Request noch seinen Token, im Header des Requests, mit. Dieser Token wird anschließend evaluiert und auf seine Gültigkeit geprüft. Stimmen die notwendigen Rollen mit denen im mitgelieferten Token überein, erhält der Nutzer den gewünschten Zugriff. Ansonsten wird ihm der Zugriff verwehrt.

Die Form und der Informationsgehalt dieser Tokens kann sich in den unterschiedlichen Authentifizierungs-Verfahren (nachfolgend auch Flows genannt) unterscheiden. In den meisten Fällen handelt es sich jedoch um einen sogenannten JSON-Web-Token (JWT), der im Bearer Schema vorliegt. Diese Art von Tokens wird zur Übermittlung von Informationen genutzt und sind in den meisten Fällen signiert und verschlüsselt.

1.3.1.2 JSON-Web-Token

Der grundlegende Aufbau des Tokens lässt sich in drei Bestandteile aufgliedern. Beginnend mit dem „Header“ oder auch Kopf, der den Typ des Tokens und den Algorithmus zur Signatur festlegt. Anschließend folgt durch einen Punkt getrennt der „Payload“, der userspezifische Informationen und die Berechtigungen des Users enthält. Als letzter Bestandteil folgt erneut durch einen Punkt getrennt die „Signature“ oder auch Signatur, mit der die Validität des Tokens überprüft werden kann.

Die gängigste Variante ist das Signieren der Tokens von Seiten des Identity Providers und eine Bereitstellung des Public Keys über einen öffentlichen Endpunkt. Mit Hilfe dieses Public Keys kann anschließend eine Client-Anwendung die Echtheit und die Validität des gesendeten Tokens überprüfen. Zugriff auf diese Informationen erhalten die Clients bzw. Anwendungen über spezielle Endpunkte, die die Identity Provider hierfür zur Verfügung stellen. Der derzeitige Standard zur Ausgabe dieser Informationen definiert eine URL in dem Format `<IdentityProviderDomain>/.well-known/openid-configuration`.

Das nachfolgende Beispiel zeigt einen JWT in seinem kodierten und dekodierten Zustand. Eine Kodierung mittels Base64 minimiert die Größe des Tokens und erleichtert somit die Übertragung auf HTTP-Ebene.

Encoded	Decoded
HASTE A TOKEN HERE	EDIT THE PAYLOAD AND SECRET
<pre> eyJhbGciOiJSUzI1NiIsImtpZCI6IjGRDA1RDQ zQkM4QzIyODIwNTJGNkFGNjJCMTNCQjk1IiwidH lwIjoIYXQrand0In0.eyJpc3MiOiJodHRwciovL 3JldmVyc2UucHJveHkubG9yYWxob3N0L2lkZW50 eXR0SiwiwibmJmIjoxNjIwNjQ4NzgZCjPpYXQiOjE 2MjA2NDg3ODMsImV4cCI6MTYtYMDY1MjM4MywiYX VkIjpIndlYXRoZXJkYXRhIiwibG9yYXRpb25kY XRhIiwiaHR0cHM6Ly9yZXZlcnNlLnByb3h5Lmxv Y2FsaG9zdC9pZGVudG0leS9yZXNvdXJzX2MiXSwi ic2NvcGU0i0iJvcGluaWQhcHJvZmlsZSB3ZF0aG VyZGF0YS5yZWFKIGxvY2F0aW9uZGF0YS5yZWFKI iwiYWlyIjpbInB3ZCJdLCJjbGllbnRfaWQ0i0iJh bmd1bGfYXd1YmFwcCI5InN1YiI6Ig4NDIXMTE zIiw1YXV0aF90aW11IjoxNjIwNjQ4NzgZCjPpZH Ai0iJsb2NhbmCI5InnPCZCI6IKIxOUi3MzI1RDEzO EVBNUEU5QzNDQM5REY5MTc2MkJFIiwianRpIjoI MkNmNDMjJDJjZGM0YwOUVGOTkwNzAtM0MwNjA2MDZ EMUEiEQ.Jo3bB0eW107Im6FR2UZqegE20r9wsXD HnMur9F- y8gn3QPAAW6qlxFqINmGu3EvK3vaJfIEJPkq0Q6Q 7qv1kUZlw2b3I6PCSgkBkbDtlv828mhJilD5Dhd OVZgJraYo5ZOloLELUZ- VB_Ns32PmK2N00FLP5B3dhdb108WRPbGrFRH9s 4c4Laf1AK_4yIKi1BxxwDvc_2n40ywzoHvstJdS mrWDzbQWLGPuKTBTlks_TF1_eb79EWRSPh_LHD EsKhN_pK21YAc67ftBpkfZW_PDGCC2EcXUXbr pUIDnhJR7R93spaHeXS- Ef4MdjW7sQpomAbxQLHB7nJXG9pFQ </pre>	<div> <div>HEADER: ALGORITHM & TOKEN TYPE</div> <pre>{ "alg": "RS256", "kid": "8FD05D43BC8228052F6AF62B13BB95", "typ": "at+jwt" }</pre> </div> <div> <div>PAYLOAD: DATA</div> <pre>{ "iss": "https://reverse.proxy.localhost/identity", "nbfi": 1628648783, "iat": 1628648783, "exp": 1628652383, "aud": ["weatherdata", "locationdata"], "https://reverse.proxy.localhost/identity/resources" }, { "scope": "openid profile weatherdata.read locationdata.read", "amr": ["pwd"], "client_id": "angular-webapp", "sub": "88421113", "auth_time": 1628648783, "idp": "local", "sid": "B1987325D13BEA4E9C3CC09F91762BE", "jti": "2CC22C6F3BF89F99805833CB06060601A" }</pre> </div> <div> <div>VERIFY SIGNATURE</div> <pre> RSASHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), -----BEGIN PUBLIC KEY----- </pre> </div>

Abbildung 1 JSON-Web-Token in kodierten und dekodierten Zustand

1.3.1.3 Authorization Code Flow with Proof-Key-of-Code-Exchange

Zuerst erfolgt eine Erläuterung des “**Authorization Code Flow + Proof Key of Code Exchange (PKCE)**”. Diese Authentifizierungsmethode ist derzeit der Standard zur Authentifizierung mittels Webapplikationen, wie einer SPA bei Identity Providern. Der Vorgang besteht darin, dass der Client (hier eine Webapplikation) eine **Code_Challenge** an den Authorization Server (hier den Identity Provider, kurz AS genannt) schickt. Bei dieser **Code_Challenge** handelt es sich um eine Zeichenkette aus Base64-kodierten Werten. Diese Werte können Zeichen im Format von **a-z, A-Z, 0-9, . , , ‘, ~** und **-** enthalten.

Anschließend wird diese Zeichenkette mittels SHA-256 verschlüsselt und an den AS geschickt. Nach Eingang der **Code_Challenge** speichert der AS den Wert ab und sendet eine **Code_Verification** zurück.

Möchte der Client nun einen Token zum Zugriff auf geschützte Bereiche des Ressource Server (kurz RS genannt), muss er neben der **Code_Challenge** zusätzlich die **Code_Verification** an den AS schicken, um sich zu authentifizieren [4]. Der Nachteil bei dieser Authentifizierungsvariante besteht darin, dass bei Entwendung des Tokens, dieser für die restliche Zeit seiner Gültigkeit weiterverwendet werden kann, ohne dass der Nutzer dies verhindern kann.

1.3.2 Einführung in die Cloud Taxonomie

Für die Einordnung und das Verständnis der Cloud Taxonomie werden in diesem Kapitel der Thesis alle notwendigen Begriffe und deren Definition eingeführt. Die Ressourcen eines Cloud Computing Dienstes reichen von Software-Diensten bis zu Datenspeichern, Betriebssystemen und ganzen Hardware-Infrastrukturen. Basierend auf der Granularität des Dienstes kann in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) unterschieden werden [5, S. 5]. Neben diesen bereits aufgeführten Service Modellen gibt es noch eine Bandbreite an weiteren Diensten, die über die Cloud angeboten werden können. Hierunter zählen zum Beispiel Communication-as-a-Service (CaaS), Compute-as-a-Service (CompaaS), Data-Storage-as-a-Service (DSaaS) bzw. Database-as-a-Service (DaaS) oder Network-as-a-Service (NaaS) [6, S. 17]. In diesem Grundlagenkapitel bzw. im Rahmen der Thesis werden jedoch nur die ersten drei Modelle genauer beschrieben. Sie sind im Rahmen der Cloud Sicherheit am besten für die Einordnung der Verantwortung des Kunden bezüglich der Wartung und Absicherung der in Anspruch genommenen Cloud Leistung geeignet.



Abbildung 2 Verantwortung über die genutzten Cloud Services. Grafik: Security Guidance v4.0, CSA

1.3.2.1 Infrastructure-as-a-Service

Durch die Verwendung von Infrastructure-as-a-Service hat der Cloud Kunde den kompletten Zugriff auf alle Komponenten (wie z.B. Betriebssysteme, Middleware, Laufzeit, Daten und Applikationen) des gemieteten Cloud Servers. Hierauf kann über vordefinierte grafische Benutzerschnittstellen oder VPN Verbindungen zugegriffen werden [6, S. 17]. Dies garantiert neben einer Vielzahl an Konfigurationsmöglichkeiten eine große Verantwortung hinsichtlich der Wartung des Servers und den darauf ausgerollten Applikationen. Zusätzlich muss darauf geachtet werden, dass die neusten kritischen Sicherheits- und Betriebssystem-Updates installiert sind. Dies rundet die Konfiguration der Firewall, die den Server vor unbefugtem Zugriff schützt, ab.

1.3.2.2 Platform-as-a-Service

Im Rahmen von Platform-as-a-Service werden dem Cloud Kunden unterschiedliche Plattformen für das Betreiben seiner Anwendungen zur Verfügung gestellt. In diesem Rahmen kann dieser seine Applikationen mit Hilfe von vorhandenen Entwickler-Tools und Laufzeitumgebungen ohne größeren Aufwand hinsichtlich der Konfiguration platzieren [6, S. 16-17].

1.3.2.3 Software-as-a-Service

Der Cloud-Dienst Software-as-a-Service impliziert eine in der Cloud betriebene Anwendung, auf die der Kunde über einen Web-Browser zugreifen kann. Der Nutzer dieser Software hat somit den Vorteil, dass die Anwendung nicht lokal auf seinem System betrieben werden muss und somit keinerlei lokale Ressourcen verbraucht. Hiermit entfallen der Installationsprozess auf der lokalen Umgebung und der Kauf von Desktop- und Server-Lizenzen. Abgerechnet wird je nach Nutzungsdauer und der Anzahl der Nutzeraccounts, die für den jeweiligen Tenant angelegt wurden. Typische Anwendungen in diesem Service Modell sind E-Mail- und Dokumentenmanagement-Programme [6, S. 16].

Wie in der nachfolgenden Grafik nochmals genauer veranschaulicht ist innerhalb der einzelnen Service Modelle ein Gefälle an Verantwortung zu erkennen, die der Cloud Kunde selbst übernehmen muss. Von der kompletten Verwaltung von eigenen On-Premises Systemen bis hin zur fremdverwalteten SaaS-Lösung.

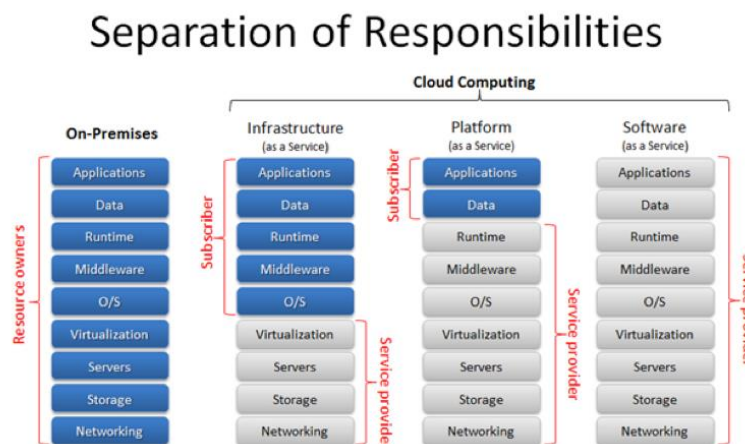


Abbildung 3 Verantwortung von Cloud Kunde und Cloud Betreiber
Quelle: https://www.magenium.com/magenium/Magenium_Cloud_Services_Diagram.jpg

2 Hauptteil

Inhalt dieses Kapitels ist die theoretische Ausarbeitung des Kriterienkataloges anhand eines vorher vorgegebenen operationalisierbaren Szenarios mit anschließender Konzeption eines Dienstes, der mit passenden Gegenmaßnahmen die negativen Effekte abmildern soll.

2.1 Beschreibung des operationalisierbaren Szenarios

Für die Erarbeitung des Kriterienkatalogs für die STP Cloud und dessen Anspruch an Vergleichbarkeit wird anhand eines der gängigsten Risiken für Anwendungen in der Cloud, eine Situation konstruiert, welches die Basis für die Auswahl der Kriterien für die Gefahrenanalyse bildet.

Die Auswahl des Angriffsvektors basiert auf der Liste der Cloud Security Alliance, die auch in unterschiedlichen Literaturbeiträgen wie [7] zur Veranschaulichung von Risiken für Cloudanwendungen gewählt wird:

- Datenpannen
Ausnutzen von schlecht konfigurierten Datenbanken, über die Angreifer Zugriff auf gespeicherte Kundendaten erhalten können.
- Datenverlust
Durch Angreifer, unachtsame Service Provider oder Naturkatastrophen ausgelöste Verluste von Daten.
- Übernahme von Account oder Dienst Netzwerkverkehr (Traffic Hijacking)
Diese Art von Risiko kann unterschiedliche Ursachen besitzen. Ein Angreifer könnte zum Beispiel durch Umleiten von Nutzern auf gefälschte Login-Seiten oder die Manipulation von Daten Zugriff auf Nutzerkonten des Dienstes erlangen und dies als Basis weiterer Angriffsvektoren verwenden.
- Unsichere APIs und Benutzeroberflächen
Zur Verwaltung der Cloud-Infrastrukturen und deren Überwachung (auch Monitoring genannt) werden von den IT-Administratoren in den meisten Fällen APIs oder grafische Benutzeroberflächen verwendet. Falls diese ohne eine Absicherung frei aus dem öffentlichen Netzwerk adressiert werden können, ist hier eine kritische Sicherheitslücke vorhanden.

- Denial of Service (DoS) Attacken

Im Rahmen von DoS Attacken können durch das ständige Anfragen der Dienste in der Cloud Probleme in der Verfügbarkeit auftreten. Dies kann wiederum erhebliche Kosten für den Anbieter der Cloud-Dienste bedeuten, da viele Bezahlmodelle nach dem Pay-As-You-Go Prinzip verwaltet werden. Bedeutet, dass durch die höhere Auslastung der virtuellen Maschinen, diese durch kostspielige Upgrades wie virtuellen Arbeitsspeicher erweitert werden, um die Lastspitzen abfangen zu können.

- Bösertige Insider

Beschreibt das Risiko eines Angestellten des Cloud-Anbieters oder einer dritten Partei, der durch böswilliges Verhalten dem Cloud Kunden sowie dem Cloud-Anbieter zufügen kann.

- Missbrauch von Cloudinfrastrukturen (Cloud Abuse)

Der Missbrauch von Cloudinfrastrukturen stellt das Ausnutzen der Rechenkapazität des verteilten Systems als Risiko dar. Anwendungsfälle wären zum Beispiel die Nutzung der Rechenleistung für das Knacken einer Verschlüsselung oder die Durchführung einer DoS-Attacke.

- Unbedachte Nutzung von Cloud Technologien durch Unternehmen

Hier wird die unüberlegte Migration von Unternehmenssoftware in die Cloud thematisiert. Durch fehlendes Verständnis der Risiken, die durch eine Cloudmigration entstehen, die für zum Beispiel eine vorherige On-Premises Software nicht relevant waren, muss bei dieser Entscheidung miteinbezogen werden. In vielen Fällen wird dies von Firmen nicht mit ins Kalkül gezogen.

- Sicherheitslücken auf technischer Ebene

Dieses Risiko macht auf die Gefahren von Sicherheitslücken auf der Ebene der Software, Plattform oder Infrastruktur aufmerksam, auf der die Anwendungen des Cloud Kunden laufen. Hierdurch kann auch eine sichere Anwendung durch Kompromittierung der darunterliegenden Infrastruktur lahmgelegt werden.

Bei der Entscheidung für die Wahl des Angriffsvektors wurden die aktuellen Gegebenheiten der Anwendung berücksichtigt. In Folge des Hostings der Lösung bei einem externen Anbieter und somit der Elimination von einigen der oben genannten Risiken fiel die Entscheidung auf die Denial of Service (DoS) Attacken. Dies lässt im späteren Teil der Implementierung von Gegenmaßnahmen die reine technische Behandlung des Problems, ohne das Einwirken von dritten, wie zum Beispiel eines menschlichen Nutzers, zu (Social Engineering Attacken müssen somit nicht berücksichtigt werden).

2.2 Kriterien-Bereiche für die Analyse

Zur Bewertung der SaaS-Lösung wird anhand der Bewertungskriterien des Cloud Computing Compliance Criteria Catalogue des Bundesamtes für Sicherheit in der Informationstechnik C5:2020, der am 21.01.2020 neu aufgelegt wurde, ein Rahmen für das zugrundeliegende Szenario entworfen. Hierfür wird der Kriterienkatalog zuerst auf die wichtigsten Bewertungskriterien heruntergebrochen. Der komplette Katalog besteht aus 17 unterschiedlichen Bereichen, die wiederum aus 121 Basiskriterien bestehen. Neben der Sicherheit von Softwareanwendungen, die Umsetzung von Sicherheitsstandards in den zu prüfenden Unternehmen werden auch allgemeine Vorkehrungen zur Absicherung bestimmter Bereiche innerhalb von Rechenzentren bewertet. Zu der Bearbeitung der hier vorliegenden Fragestellung ist dieses Sammelwerk zu umfangreich. Für die Bewertung der vorhandenen Sicherheitsmechanismen des Systems bedarf es dem Streichen einzelner Punkte. Zur besseren Übersicht der abgedeckten Bereiche innerhalb des C5 werden diese nachfolgend aufgeführt und mit einer groben Definition ihrer Bewertungsgrundlage beschrieben. Die komplett gestrichenen bzw. gekürzten Bestandteile des Katalogs werden zusätzlich jeweils mit einer Begründung versehen, die den Grund für das Nichtverwenden innerhalb des eigenen Kriterienkatalogs aufzeigt.

2.2.1 Organisation der Informationssicherheit (OIS)

Der Bereich Organisation der Informationssicherheit (OIS) beschäftigt sich mit dem Ziel der "Planung, Umsetzung, Aufrechterhaltung und (der) kontinuierliche(n) Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der (zu bewertenden) Organisation" [8, S. 16].

Bezüglich des anzuwendenden Szenarios ergab sich für die sieben Basiskriterien folgendes Ergebnis:

Tabelle 1 Anwendbare Kriterien aus dem Bereich OIS

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
<ul style="list-style-type: none">• OIS-05	<ul style="list-style-type: none">• OIS-01• OIS-02• OIS-03	<ul style="list-style-type: none">• OIS-04• OIS-06• OIS-07

Die hier formulierten Kriterien bewerten, wie in der Definition bereits angedeutet, die Umsetzung eines Rahmenwerkes, also eines dokumentierten Prozesses innerhalb des Unternehmens, der den Umgang mit Sicherheitsrisiken beschreibt und mögliche Handlungsanweisungen an die betreffenden Personen überträgt. Sie sind somit außer des Kriteriums OIS-05, das den Umgang mit aktuellen Bedrohungen für Dienste in der Cloud beschreibt, nicht für den Einsatz innerhalb des Szenarios zu verwenden.

2.2.2 Sicherheitsrichtlinien und Arbeitsanweisungen (SP)

Im Rahmen der Sicherheitsrichtlinien und Arbeitsanweisungen (SP) steht im Mittelpunkt das "Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen" [8, S. 16].

In Anlehnung an die Argumentation aus dem Kriterien-Bereich Organisation der Informationssicherheit (OIS) ist nach der Evaluation der Sicherheitsrichtlinien und Arbeitsanweisungen (SP) folgendes Resultat entstanden:

Tabelle 2 Anwendbare Kriterien aus dem Bereich SP

Anwendbare Kriterien	Nicht-anwendbare Kriterien
	<ul style="list-style-type: none">• SP-01• SP-02• SP-03

Innerhalb dieser Kriterien wird Bezug auf die Festlegungen aus OIS genommen. Durch Ausschluss von OIS ist somit ein Einsatz von Kriterien aus dem Bereich SP nicht ohne weiteres möglich.

2.2.3 Personal (HR)

Das Personal (HR) verfolgt die Zielsetzung des "Sicherstellen(s), dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden" [8, S. 16].

Aufgrund des gewählten Szenarios, welches eine reine technische Vorkehrung zur Prävention von Angriffen behandelt, sind auch diese Kriterien nicht für eine Anwendung geeignet:

Tabelle 3 Anwendbare Kriterien aus dem Bereich HR

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
	<ul style="list-style-type: none">• HR-01• HR-02• HR-03	<ul style="list-style-type: none">• HR-04• HR-05• HR-06

2.2.4 Asset Management (AM)

Die Zielsetzung des Asset Management (AM) verfolgt das "Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenes Schutzniveau über deren gesamten Lebenszyklus sicherstellen" [8, S. 16].

Als Asset werden in diesem Kontext Objekte bezeichnet, die "während der Erstellung, Verarbeitung, Speicherung, Übermittlung, Löschung oder Zerstörung von Informationen benötigten Objekte im Verantwortungsbereich des Cloud-Anbieters, z.B. Firewalls, Loadbalancer, Webserver, Anwendungsserver und Datenbankserver." [8, S. 50] Hierbei kann nochmals in Hardware- und Software-Objekte unterschieden werden. Hardware-Objekte sind demnach physische und virtuelle Ressourcen, wie zum Beispiel Server, und Software-Objekte beschreiben Hypervisor, Container und Datenbanken [8, S. 50]. Da es sich bei dem gewählten Szenario um einen Angriff handelt, der speziell die Software-Objekte versiert, sind somit Kriterien aus dem Bereich AM eine gute Möglichkeit zur Bewertung der vorhandenen Konzepte.

Tabelle 4 Anwendbare Kriterien aus dem Bereich AM

Anwendbare Kriterien	Nicht-anwendbare Kriterien
<ul style="list-style-type: none"> • AM-01 • AM-02 • AM-06 	<ul style="list-style-type: none"> • AM-03 • AM-04 • AM-05

2.2.5 Physische Sicherheit (PS)

Kernthema des Bereichs Nummer 5 Physische Sicherheit (PS) ist das "Verhindern von unberechtigtem physischen Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs" [8, S. 16].

Aufgrund der Carve-Out Methode, durch die der Anbieter der Infrastruktur aus der Bewertung durch den kondensierten Katalog herausfällt, sind die Kriterien aus diesem Bereich nicht relevant. Sie behandeln die Sicherheitsvorkehrungen innerhalb des Gebäudes des Rechenzentrums und sind somit nicht Teil der Mechanismen für das SaaS-Produkt.

Tabelle 5 Anwendbare Kriterien aus dem Bereich PS

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
	<ul style="list-style-type: none"> • PS-01 • PS-02 • PS-03 • PS-04 	<ul style="list-style-type: none"> • PS-05 • PS-06 • PS-07

2.2.6 Regelbetrieb (OPS)

Innerhalb des Regelbetriebs (OPS) steht das "Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern" im Mittelpunkt der Kontrolle [8, S. 16].

In diesem Szenario lässt sich zwischen Zuständigkeiten des SaaS-Anbieters und des Infrastruktur-Anbieters eine klare Linie ziehen. Aspekte wie die Sicherung und Wiederherstellung von Daten und die Härtung der verwendeten Komponenten, sind eindeutig im Zuständigkeitsbereich des Infrastruktur-Anbieters. Jedoch besteht der Regelbetrieb auch aus Themen wie der Protokollierung und Überwachung von Schwachstellen und die erforderliche Prüfung. Somit kann eine Teilmenge der Regularien für die Bewertung verwendet werden.

Dies ermöglicht eine Verwendung eines Großteils der Analysekriterien:

Tabelle 6 Anwendbare Kriterien aus dem Bereich OPS

Anwendbare Kriterien		Nicht-anwendbare Kriterien	
<ul style="list-style-type: none"> • OPS-10 • OPS-11 • OPS-12 • OPS-13 • OPS-14 • OPS-15 • OPS-16 	<ul style="list-style-type: none"> • OPS-17 • OPS-18 • OPS-19 • OPS-20 • OPS-21 • OPS-22 	<ul style="list-style-type: none"> • OPS-01 • OPS-02 • OPS-03 • OPS-04 • OPS-05 • OPS-06 	<ul style="list-style-type: none"> • OPS-07 • OPS-08 • OPS-09 • OPS-23 • OPS-24

2.2.7 Identitäts- und Berechtigungsmanagement (IDM)

Mit Hilfe von Identitäts- und Berechtigungsmanagement (IDM) wird das "Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (in der Regel privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen" gewährleistet [8, S. 16].

Dies spielt als Basis für die Handhabung von unautorisierten Zugriffen auf die Funktionalitäten des restlichen Systems eine bedeutende Rolle bei der Bewertung. Falls durch gezieltes Ausschalten das Rechtevergabesystem nicht mehr funktionieren sollte, könnte ein Angreifer das gesamte System lahmlegen. Aus diesem Grund sind alle Basiskriterien in die Grundlage für die spätere Evaluation miteingeflossen.

Tabelle 7 Anwendbare Kriterien aus dem Bereich IDM

Anwendbare Kriterien		Nicht-anwendbare Kriterien
<ul style="list-style-type: none"> • IDM-01 • IDM-02 • IDM-03 • IDM-04 • IDM-05 	<ul style="list-style-type: none"> • IDM-06 • IDM-07 • IDM-08 • IDM-09 	

2.2.8 Kryptographie und Schlüsselmanagement (CRY)

Durch Kryptographie und Schlüsselmanagement wird das "Sicherstellen eines angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen" gewährleistet [8, S. 16].

Die Gewährleistung der sicheren Übertragung von Daten spielt in diesem Szenario jedoch keine tragende Rolle und somit sind diese Bewertungskriterien nicht für die weitere Verwendung geeignet.

Tabelle 8 Anwendbare Kriterien aus dem Bereich CRY

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
	<ul style="list-style-type: none">• CRY-01• CRY-02• CRY-03	<ul style="list-style-type: none">• CRY-04

2.2.9 Kommunikationssicherheit (COS)

Der Bereich der Kommunikationssicherheit (COS) widmet sich dem "Sicherstellen des Schutzes von Informationen in Netzen und den entsprechenden informationsverarbeitenden Systemen" [8, S. 17].

Neben den reinen Sicherheitsvorkehrungen innerhalb der Netze des Cloud-Anbieters werden hier auch technische Schutzmaßnahmen beschrieben, die z.B. im Fall von COS-01 Vorkehrungen zum Schutz vor Distributed-Denial-of-Service Attacken beschreiben.

Tabelle 9 Anwendbare Kriterien aus dem Bereich COS

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
<ul style="list-style-type: none">• COS-01	<ul style="list-style-type: none">• COS-02• COS-03• COS-04• COS-05	<ul style="list-style-type: none">• COS-06• COS-07• COS-08

2.2.10 Portabilität und Interoperabilität (PI)

Das "Ermöglichen der Eigenschaft, den Cloud-Dienst über andere Cloud-Dienste oder IT-Systemen der Cloud-Kunden ansprechen zu können, die gespeicherten Daten bei Beendigung des Auftragsverhältnisses zu beziehen und beim Cloud-Anbieter sicher zu löschen" [8, S. 17] wird im Rahmen der Portabilität und Interoperabilität betrachtet.

Zusammenfassend handelt es sich hierbei um eine reine Dokumentation der vorhandenen Schnittstellen und die sichere Bereitstellung und Löschung von Daten. Für den Anwendungsfall der DoS-Angriffe sind diese Bewertungskriterien nicht relevant.

Tabelle 10 Anwendbare Kriterien aus dem Bereich PI

Anwendbare Kriterien	Nicht-anwendbare Kriterien
	<ul style="list-style-type: none">• PI-01• PI-02• PI-03

2.2.11 Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)

Die Zielsetzung im Bereich der Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) ist das "Sicherstellen der Informationssicherheit im Entwicklungszyklus von Systemkomponenten des Cloud-Dienstes" [8, S. 17].

Die in diesem Kontext beschriebenen Kriterien erlauben die Qualität der Entwicklung der einzelnen Dienste zu bewerten. Letztlich wird geprüft, ob die entwickelten Features sicher gegenüber variablen Eingaben sind. Hier spielen zum Beispiel Angriffe wie die SQL-Injection eine tragende Rolle. Werden diese böartigen Code-Schnipsel nicht vom System erkannt, bzw. als Plain-Text behandelt, ist es dem Angreifer möglich Daten in der Datenbank zu manipulieren, auszulesen oder im extremsten Fall zu löschen.

Tabelle 11 Anwendbare Kriterien aus dem Bereich DEV

Anwendbare Kriterien		Nicht-anwendbare Kriterien
<ul style="list-style-type: none">• DEV-01• DEV-02• DEV-03• DEV-04• DEV-05	<ul style="list-style-type: none">• DEV-06• DEV-07• DEV-08• DEV-09• DEV-10	

2.2.12 Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)

Die Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO) konzentriert sich auf das "Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Subdienstleister) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen" [8, S. 17].

Die Überwachung und Bewertung von Dienstleistern, die zusätzliche Dienste zur Verfügung stellen und deren Überwachung, ist aufgrund des Carve-Out aller umliegenden Organisationen außer dem Anbieter der SaaS-Lösung ausgeschlossen. Diese Kriterien gehen nicht mit in die Bewertung mit ein.

Tabelle 12 Anwendbare Kriterien aus dem Bereich SSO

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
	<ul style="list-style-type: none">• SSO-01• SSO-02• SSO-03	<ul style="list-style-type: none">• SSO-04• SSO-05

2.2.13 Umgang mit Sicherheitsvorfällen (SIM)

Mit dem "Gewährleisten eines konsistenten und umfassenden Vorgehens zur Erfassung, Bewertung, Kommunikation und Behandlung von Sicherheitsvorfällen" [8, S. 17] befasst sich der Bereich mit der Kennung Umgang mit Sicherheitsvorfällen.

Für die Implementierung einer allgemeinen Richtlinie für den Umgang mit Gefahren und Sicherheitsvorfällen bezüglich des Cloudproduktes sind diese Kriterien für eine Verwendung bei der Analyse geeignet. Sie ermöglichen Prozesse zu implementieren, die aus vergangenen Vorfällen neue Richtlinien für den Schutz des Produktes evaluieren.

Tabelle 13 Anwendbare Kriterien aus dem Bereich SIM

Anwendbare Kriterien		Nicht-anwendbare Kriterien
<ul style="list-style-type: none">• SIM-01• SIM-02• SIM-03	<ul style="list-style-type: none">• SIM-04• SIM-05	

2.2.14 Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)

Als Resultat der Domäne Kontinuität des Geschäftsbetriebs und Notfallmanagement steht das "Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement" [8, S. 17].

Beschreibt somit im Groben die Handhabung von Sicherheitsvorfällen innerhalb des Rechenzentrums, die die Verfügbarkeit der Dienste beeinträchtigen könnten. Die Prävention dieser Gefahren liegt im Zuständigkeitsbereich des Infrastrukturanbieters.

Tabelle 14 Anwendbare Kriterien aus dem Bereich BCM

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
	<ul style="list-style-type: none">• BCM-01• BCM-02• BCM-03	<ul style="list-style-type: none">• BCM-04

2.2.15 Compliance (COM)

Innerhalb der Compliance (COM) steht das "Vermeiden von Verstößen gegen gesetzliche, regulatorische, selbstaufgelegte oder vertragliche Anforderungen zur Informationssicherheit und Überprüfen der Einhaltung" [8, S. 17] im Mittelpunkt.

Dies betrifft größtenteils die Compliance bzw. die Einhaltung von Richtlinien im Informationsmanagementsystem (ISMS) aus dem Bereich OIS. Aus diesem Grund ist auch dieser Bereich nicht weiter für die nachfolgende Bewertung von Bedeutung.

Tabelle 15 Anwendbare Kriterien aus dem Bereich COM

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
	<ul style="list-style-type: none">• COM-01• COM-02• COM-03	<ul style="list-style-type: none">• COM-04

2.2.16 Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)

Das "Gewährleisten eines angemessenen Umgangs mit Ermittlungsanfragen staatlicher Stellen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten" [8, S. 17] ist die Zielsetzung des Zuständigkeitsbereichs von Umgang mit Ermittlungsanfragen staatlicher Stellen.

Rechtliche Fragestellungen wie den Zugriff von staatlichen Stellen auf Daten von Cloud-Kunden werden in diesem Szenario nicht betrachtet. Aufgrund der Beheimatung der Dienste und deren Daten im Land des Kunden, sind Zugriffe von regierungsnahen Institutionen wie z.B. in Amerika in Folge des CLOUD Acts nicht in gleichem Maße zutreffend.

Tabelle 16 Anwendbare Kriterien aus dem Bereich INQ

Anwendbare Kriterien	Nicht-anwendbare Kriterien	
	<ul style="list-style-type: none">• INQ-01• INQ-02• INQ-03	<ul style="list-style-type: none">• INQ-04

2.2.17 Produktsicherheit (PSS)

"Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden" [8, S. 17] wird durch den letzten Bereich, die Produktsicherheit (PSS), garantiert.

Im Rahmen des letzten Bereiches, der Produktsicherheit, werden nochmals wichtige Kriterien für die Absicherung von Cloud-Diensten zusammengefasst, die über das ausgewählte Szenario hinaus Möglichkeiten für den sicheren Zugang der Cloud-Kunden sorgen.

Tabelle 17 Anwendbare Kriterien aus dem Bereich PSS

Anwendbare Kriterien		Nicht-anwendbare Kriterien
<ul style="list-style-type: none">• PSS-01• PSS-02• PSS-03• PSS-04• PSS-05	<ul style="list-style-type: none">• PSS-06• PSS-07• PSS-08• PSS-09	<ul style="list-style-type: none">• PSS-10• PSS-11• PSS-12

2.3 Kriterienkatalog für die STP Cloud

Auf Basis der vorangegangenen Untersuchung des Cloud Computing Compliance Criteria Catalogue – C5:2020 auf Verwendbarkeit der einzelnen Basiskriterien für die Beurteilung der Sicherheitsmechanismen im Falle des in Kapitel 2.1 ausgewählten Szenarios, konnten 51 Basiskriterien aus den 17 unterschiedlichen Bereichen isoliert werden.

Die nachfolgende Tabelle dient zur Beurteilung und zeigt den Grad der Erfüllung der einzelnen Kriterien nach Einschätzung bzw. der Analyse im Rahmen dieser Thesis.

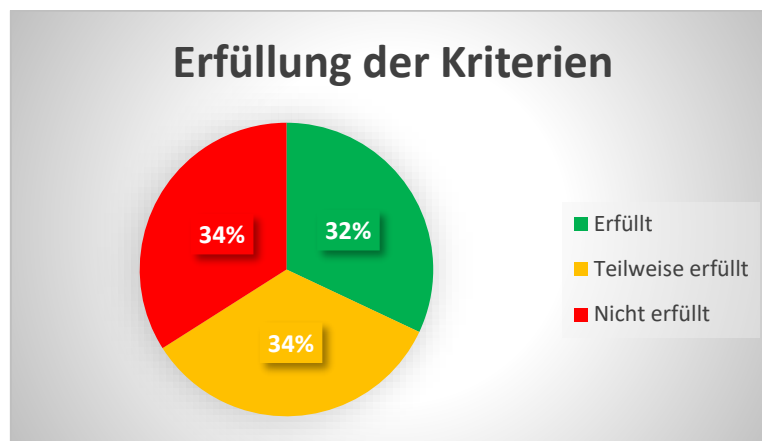
Tabelle 18 Bewertungskriterien und Erfüllungsgrad für die Bewertung der STP Cloud

Beurteilungskatalog für die Erfüllung der ausgewählten Basiskriterien für ein vordefiniertes Szenario			
Szenario		Denial-of-Service Attacke	
Anzahl an selektierten Basiskriterien		51	
Ref.	Erfüllung durch die SaaS-Lösung und deren Anbieter		
	Erfüllt	Teilweise erfüllt	Nicht erfüllt
OIS-05	X	✓	X
AM-01	X	✓	X
AM-02	X	✓	X
AM-06	X	X	✓
OPS-10	X	✓	X
OPS-11	✓	X	X
OPS-12	X	✓	X
OPS-13	X	X	✓
OPS-14	✓	X	X
OPS-15	✓	X	X
OPS-16	✓	X	X
OPS-17	X	✓	X
OPS-18	X	X	✓
OPS-19	X	✓	X
OPS-20	X	X	✓
OPS-21	X	X	✓
OPS-22	X	X	✓
IDM-01	X	✓	X
IDM-02	✓	X	X
IDM-03	X	X	✓
IDM-04	X	✓	X
IDM-05	X	X	✓
IDM-06	X	✓	X

IDM-07	X	X	✓
IDM-08	X	✓	X
IDM-09	✓	X	X
COS-01	X	X	✓
DEV-01	X	✓	X
DEV-02	X	X	X
DEV-03	X	X	✓
DEV-04	X	X	✓
DEV-05	X	X	✓
DEV-06	X	✓	X
DEV-07	✓	X	X
DEV-08	✓	X	X
DEV-09	✓	X	X
DEV-10	✓	X	X
SIM-01	X	✓	X
SIM-02	✓	X	X
SIM-03	X	X	✓
SIM-04	✓	X	X
SIM-05	X	X	✓
PSS-01	X	X	✓
PSS-02	X	✓	X
PSS-03	X	X	✓
PSS-04	X	✓	X
PSS-05	✓	X	X
PSS-06	✓	X	X
PSS-07	✓	X	X
PSS-08	✓	X	X
PSS-09	X	✓	X
Gesamt	16	17	17

Im nachfolgenden Schaubild wird die prozentuale Verteilung des Ergebnisses nochmals mit Hilfe eines Diagramms grafisch dargestellt.

Tabelle 19 Grafische Darstellung mit prozentualer Verteilung des Erfüllungsgrades



2.4 Maßnahmen zu der Optimierung des Ergebnisses

Basierend auf der Bewertung durch die zusammengestellten Basiskriterien aus dem Cloud Computing Compliance Criteria Catalogue – C5:2020 sind Lücken bzw. unvollständige Konzepte für das Betreiben der Cloud-Anwendung aufgetreten. Diese sicherheitskritischen Mängel werden mit Hilfe der nachfolgend formulierten Maßnahmen adressiert.

Die Maßnahmen zur Erfüllung der teilweise bzw. nicht erfüllten Kriterien orientieren sich hierbei eng an die Vorgaben aus dem C5 und stellen somit ein Minimum an vorhandenen Konzepten und Prozessen innerhalb des bewerteten Unternehmens bzw. der Anwendung dar. Hierbei liegt die Auslegung der einzelnen Maßnahmen auf den Annahmen des Autors und erhebt somit keinen Anspruch auf Vollständigkeit. Simultan gilt dies für den Umfang der vorangegangenen Analyse.

// TODO: Auflistung der Maßnahmen

2.5 Analyse der vorhandenen Sicherheitskonzepte

In den nachfolgenden Kapiteln wird der aktuelle Stand an Sicherheitskonzepten der Software-as-a-Service Lösung, auch „LEXolution.FLOW“ genannt, analysiert und einem möglichen Soll-Zustand gegenübergestellt. Dieser Soll-Zustand orientiert sich hierbei an den aus Kapitel 2.4 benannten Maßnahmen zur Optimierung der bestehenden Sicherheitskonzepte. Explizit wird hierbei auf die technischen Schutzmaßnahmen der Cloud-Lösung eingegangen. Diese werden als Basis für die spätere Implementierung eines Mechanismus zum Schutz der Anwendung gelegt.

2.5.1 Ist-Zustand

Die bewertete SaaS-Lösung der STP wird über einen Cloud Service Provider (nachfolgend auch CSP) zur Verfügung gestellt, bedeutet die notwendige Hardware wird nicht In-House betrieben, sondern von Außerhalb je nach Bedarf gebucht. Hierbei handelt es sich um ein deutsches Rechenzentrum, welches seine Daten ausschließlich in Standorten innerhalb von Deutschland

speichert. In Folge des Beschlusses der amerikanischen Regierung ist es mittels des CLOUD Acts (Clarifying Lawful Overseas Use of Data) regierungsnahen Institutionen, wie zum Beispiel der NSA, CIA oder FBI, möglich sich ohne Einwilligung oder vorheriges Informieren der Cloud Nutzer Zugang zu den gespeicherten Daten der Cloud Provider zu verschaffen [9]. So wäre ein Hosting bei Microsoft, Amazon Web Services oder Google Cloud Platform mit der deutschen Rechtslage für die Zielgruppe der STP nicht vereinbar.

Bei der Analyse des Ist-Zustandes steht jedoch nicht die Bewertung der Regularien zum Betreiben einer Cloud Lösung oder die Sicherheitskriterien für die Rechenzentren im Mittelpunkt, sondern die Resistenz vor gängigen Angriffen auf Cloud Softwarelösungen und Ausfalltoleranz der Anwendung selbst. Hiermit wird eine Grenze zwischen der Software und der Plattform beziehungsweise der darunterliegenden Infrastruktur gezogen (Carve-Out Methode).

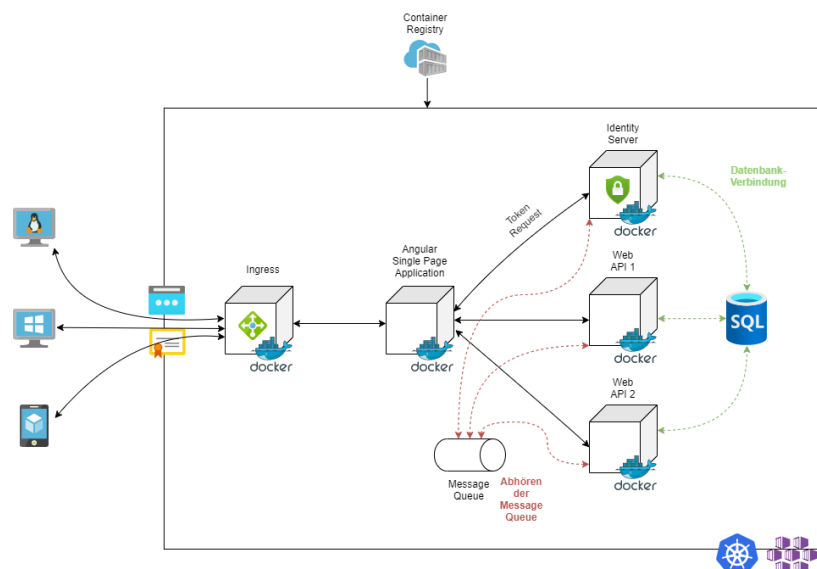


Abbildung 4 Vereinfachte Darstellung der STP Cloud SaaS-Lösung

Mithilfe der vorangegangenen vereinfachten Darstellung der STP Cloud Lösung soll nun die Bestandsaufnahme des Ist-Zustandes erfolgen. Der Anwendungsverbund besteht im übergeordneten Sinne aus unterschiedlichen Single Page Applikationen (nachfolgend auch SPA genannt), die die grafische Benutzeroberfläche der Anwendung repräsentieren. Hierbei wird je nach gewünschtem Menü über den vorgelagerten Ingress im Kubernetes Cluster die entsprechende SPA angesprochen. Somit verteilt sich die Last nicht nur auf eine einzelne Webanwendung. Über die Weboberfläche wird dem Kunden die Eingabe von für den Prozess relevanten Daten ermöglicht. Die Verarbeitung und Speicherung der Daten wird im Anschluss über Web Programmierschnittstellen (nachfolgend auch API genannt) gewährleistet. Die Implementierung der APIs ist mit dem .NET Framework und C# als Programmiersprache

umgesetzt worden. Für die sichere Übertragung der Daten vom Frontend an das Backend wird mittels TLS 1.2 der ein- und ausgehende Datenstrom verschlüsselt. Dies verhindert im ersten Schritt das ungewünschte Mitschneiden und -lesen von Datenpaketen. Bezüglich der Verwaltung von Rechten wird im Backend ein IdentityServer in der Version 4 bereitgestellt. Hierbei handelt es sich um einen Service, der das OpenID Connect und das OAuth2 Protokoll umsetzt. Die Nutzung dieses Diensts gewährleistet eine zentrale Nutzerverwaltung für alle Tenants und die Vergabe von Rechten unterschiedlicher Granularität. Bevor der Nutzer Zugriff auf die SaaS-Lösung erhält, muss es sich initial beim Identity Provider (hier IdentityServer 4) authentifizieren. Stimmen Nutzernamen und Passwörter mit den hinterlegten Anmeldedaten überein, erhält der Nutzer, die ihm zugewiesenen Rechte, er wird somit autorisiert. Im Hintergrund des Anmeldeprozesses findet der Authorization Code Flow with Proof-Key-of-Code-Exchange (nachfolgend auch Authorization Code Flow + PKCE genannt) statt. Hierbei handelt es sich um das aktuellste und sicherste im OAuth2 Protokoll spezifizierte Verfahren für den Austausch von Tokens zwischen Identity Providern und clientseitigen Webanwendungen, wie zum Beispiel SPAs.

2.5.2 Soll-Zustand

2.6 Erkennung und Prävention von Gefahren

2.6.1 Konzeption einer Testumgebung

Für die Evaluation und Umsetzung des ML.NET Proxies Dienstes wurde anhand der in Kapitel 2.5.1 beschriebenen Architektur der Anwendung eine beispielhafte Testumgebung erstellt. Diese besitzt die grundlegenden Eigenschaften des Originals und kann somit als Substitut für Testzwecke verwendet werden, ohne auf die eigentliche Anwendungslandschaft zugreifen zu müssen.

Wie im nachfolgenden Schaubild exemplarisch dargestellt, wird die Test-Lösung wie auch das Original mittels Containerisierung auf ein Kubernetes-Kluster ausgerollt. Auf die Nutzung einer Message Queue und einer relationalen Datenbank für die Persistierung der Daten wurde verzichtet. Der Fokus wird ausschließlich auf die Manipulation bzw. das Throttling der Anfragen an das Backend gelegt.

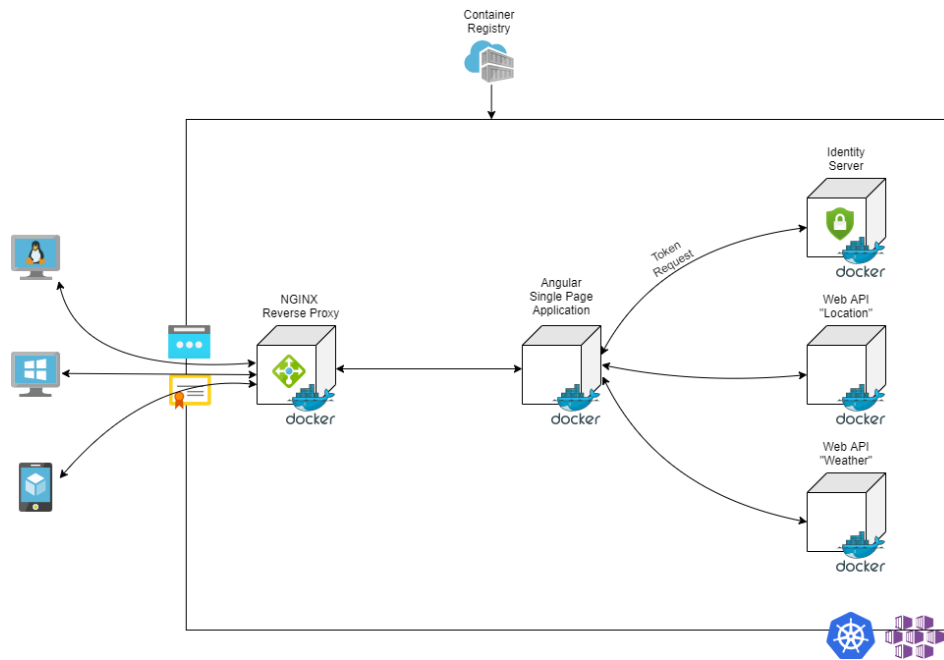


Abbildung 5 Testumgebung für die Simulation der realen Anwendungslandschaft

2.6.2 Mögliche Architektur mit ML.NET Proxy Service

Durch die Nutzung des ML.NET Proxy Service soll auf Auffälligkeiten in der Historie bzw. der aktuellen Anfragen von Außerhalb reagiert werden. Hierzu muss der Proxy jedoch zwischen Backend und dem Gateway des Klusters platziert werden. Eine mögliche Beispiel-Architektur ist im nachfolgenden Schaubild dargestellt.

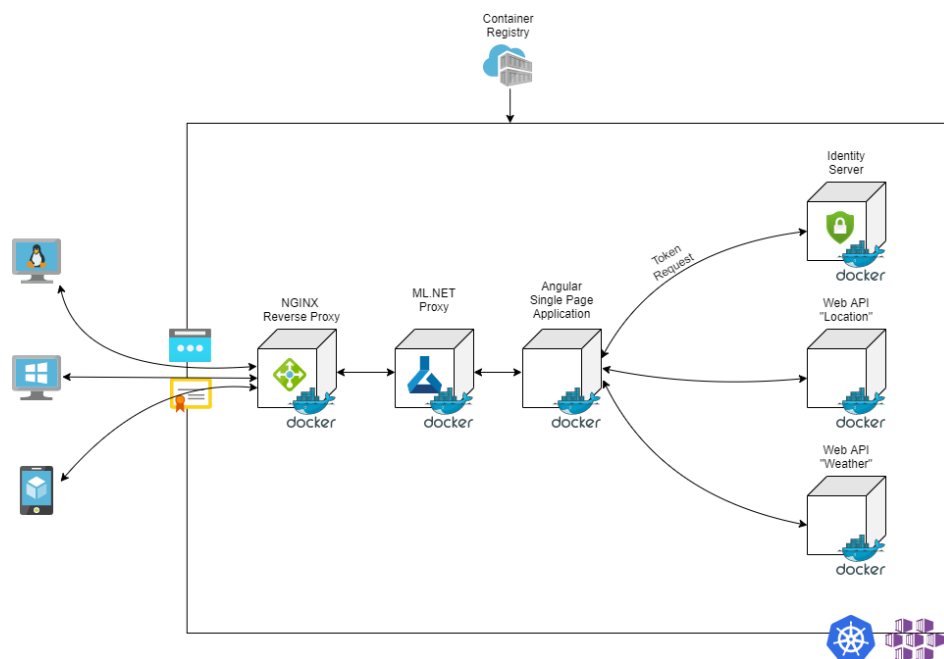


Abbildung 6 Beispiel-Architektur mit zusätzlichem Service für die Prüfung der eingehenden Requests mit Möglichkeit zum Throttling

3 Schluss

4 Literaturverzeichnis

- [1] C. Duffy, *So you're one of 533 million in the Facebook leak. What now?* [Online]. Verfügbar unter: <https://edition.cnn.com/2021/04/06/tech/facebook-data-leaked-what-to-do/index.html> (Zugriff am: 8. April 2021).
- [2] o.V., *Mehrere Schwachstellen in MS Exchange*. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=4 (Zugriff am: 8. April 2021).
- [3] o.V., *STP Informationstechnologie AG*. [Online]. Verfügbar unter: https://ka.stadtwiki.net/STP_Informationstechnologie_AG (Zugriff am: 6. Mai 2021).
- [4] Nat Sakimura, John Bradley und Naveen Agarwal, *Proof Key for Code Exchange by OAuth Public Clients*, Request for Comments. RFC Editor. Verfügbar unter: <https://rfc-editor.org/rfc/rfc7636.txt>.
- [5] A. Squicciarini, D. Oliveira und D. Lin, „Cloud Computing Essentials“ in *Cloud computing security: Foundations and challenges*, J. R. Vacca, Hg., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2021, S. 3–11.
- [6] W. Stallings, „An Overview of Cloud Computing“ in *Cloud computing security: Foundations and challenges*, J. R. Vacca, Hg., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2021, S. 13–29.

- [7] P. Pandya und R. Rahmo, „Cloud Computing Architecture and Security Concepts“ in *Cloud computing security: Foundations and challenges*, J. R. Vacca, Hg., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2021, S. 214–223.
- [8] Bundesamt für Sicherheit in der Informationstechnik, *Cloud Computing Compliance Criteria Catalogue - C5:2020: Kriterienkatalog Cloud Computing*. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html (Zugriff am: 6. Mai 2021).
- [9] Congress Government, *H.R.200 – 117th Congress (2021-2022): National Intersection and Interchange Safety Construction Program Act of 2021*. [Online]. Verfügbar unter: <https://www.congress.gov/bill/115th-congress/house-bill/4943/text> (Zugriff am: 10. Mai 2021).