HAW HAMBURG

BACHELOR THESIS
Dustin Wickert

Sicherheit einer Shared Responsibility Cloud-Infrastruktur

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Dustin Wickert

Sicherheit einer Shared Responsibility Cloud-Infrastruktur

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr.-Ing. Martin Hübner
Zweitgutachter: Prof. Dr. Stefan Sarstedt

Eingereicht am: 31. August 2023

Dustin Wickert

Thema der Arbeit

Sicherheit einer Shared Responsibility Cloud-Infrastruktur

Stichworte

Bedrohungsanalyse, Cloud, Shared Responsibility, IT-Grundschutz, Zero Trust, Vendor lock-in, Replikation, Logging, Monitoring, Alerting, Trustmanagement, Risikoanalyse, Verschlüsselung, IT-Sicherheit, Risikoanalyse

Kurzzusammenfassung

Ziel dieser Arbeit ist es, eine Bedrohungsanalyse anhand eines exemplarischen Anwendungsszenarios für den Betrieb einer Shared Responsibility Cloud-Infrastruktur durchzuführen. So werden mithilfe des IT-Grundschutzes relevante und Cloud-spezifische Bedrohungen, Schwachstellen und Angriffe gegenüber einer exemplarischen Cloud-Infrastruktur erarbeitet und analysiert. Anschließend werden entsprechende Risiken dieser Bedrohungen in Form einer Risikoanalyse für das Unternehmen analysiert. Auf Basis dessen wird ein Maßnahmenkatalog zusammengestellt, welcher die risikoreichsten Bedrohungen adressiert. Es wird zudem untersucht, in welchem Rahmen die Risiken durch eine Umsetzung des Kataloges für das Unternehmen minimiert werden können. Abschließend werden die Maßnahmen konsolidiert beziehungsweise Handlungsempfehlung für das fiktive Unternehmen ausgesprochen.

Dustin Wickert

Title of Thesis

Security of a shared responsibility cloud infrastructure

Keywords

Threat analysis, Cloud, Shared responsibility, Zero trust, Vendor lock-in, Replication, Logging, Monitoring, Alerting, Trust management, Risk analysis, Encryption, IT security, Risk analysis

Abstract

The aim of this work is to conduct a threat analysis based on an exemplary application scenario for the operation of a shared responsibility cloud infrastructure. In this way, relevant and cloud-specific threats, vulnerabilities and attacks against an exemplary cloud infrastructure are developed and analysed with the help of IT-Grundschutz. Subsequently, the corresponding risks of these threats are analysed in the form of a risk analysis for the company. Based on this, a catalogue of measures is compiled which addresses the most risky threats. It is also examined to what extent the risks can be minimised for the company by implementing the catalogue. Finally, the measures are consolidated and recommendations for action are made for the fictitious company.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

Seit den 2000er Jahren hat sich das Konzept des Cloud-Computings zu einem der größten Felder innerhalb der Informatik entwickelt. So greifen inzwischen nicht nur die großen Big Player, sondern auch zunehmend mittelständische und kleinere Unternehmen auf diese Technologie zurück. Studien legen nahe, dass schätzungsweise 90 % der exemplarisch befragten Unternehmen bereits Cloud-Computing verwenden [104]. Dabei steht nicht nur die Nutzung von Cloud-Computing für einige Services im Fokus, sondern eine breite Migration aller genutzter Services in die Cloud. Dazu geben 48 % von denselben 90 % an, über 50 % der genutzten Software in die Cloud migrieren zu wollen, falls noch nicht geschehen [57].

Die Technologie des Cloud-Computings spielt also bereits eine zentrale Rolle in vielen Unternehmensstrukturen und wird sich in Zukunft weiter manifestieren. Wie jedes Technologiekonzept bringt allerdings auch das Cloud-Computing neue Sicherheitsanforderungen und Bedrohungen mit sich, auf welche Firmen angemessen reagieren müssen, um einen sicheren Betrieb der Services in der Cloud gewährleisten zu können.

Ein weiterer Aspekt, welche die Relevanz dieser Thematik unterstreicht, ist, dass vielen Unternehmen bereits für grundlegende und lange existierende Bedrohungen ein Bewusstsein fehlt. So geben circa 50 % der Unternehmen mit einem Einkommen höher als eine Milliarde Dollar an keinen Notfallplan bei Ransomware-Angriffen zu besitzen [104]. Angesichts dieser Ausgangslage in Bezug auf die Informationssicherheit vieler Unternehmen gegenüber bereits lange existierender Bedrohungen, ist es also noch wichtiger, ein umfassendes Bewusstsein in Bezug auf Bedrohungen und Maßnahmen für ein solch neues und komplexes Konzept wie dem Cloud-Computing zu schaffen.

Ein weiterer Katalysator, welcher diesem Thema einen aktuellen Fokus verleiht, ist die Coronapandemie. Durch diese wurde beispielsweise innerhalb Deutschlands eine Homeoffice-

Pflicht erstmals gesetzlich konkret definiert. Diese resultierende Homeoffice-Quote eröffnet neue sowie katalysiert bestehende Risiken und Bedrohungen gegenüber Cloud Systemen. Unter anderem lässt dies dadurch begründen, dass insgesamt mehr mitarbeitende Personen außerhalb des geschützten Firmennetzwerkes auf einen Dienst in der Cloud oder sogar auf eine administrative Verwaltungsschnittstelle der Cloud-Umgebung zugreifen. So berichten in einer weiteren Studie 48 % der befragten deutschen Arbeitnehmer-/innen von einem Anstieg des Volumens, der Intensität und des Umfangs von Cyberangriffen in den letzten 12 Monaten *(Stand 06.2021)* [19]. Dabei handelt es sich nicht nur um ein deutsches Phänomen, sondern auch das FBI gibt an:

> „The number of cybersecurity complaints to the IC3 in the last four months has spiked from 1,000 daily before the pandemic to as many as 4,000 incidents in a day." (Federal Bureau of Investigation in [54])

Aber nicht nur Firmen, die eine Migration von bestehenden Services in die Cloud planen, benötigen ein Bewusstsein für Bedrohungen. Auch Unternehmen, die Services in einer Cloud-Umgebung bereits längerfristig betreiben, brauchen dieses. Um hierzu konkrete Zahlen zu nennen, haben 78 % von bereits angegriffenen Unternehmen in einer Studie weniger als 60 % der sensiblen Daten in der Cloud verschlüsselt [104]. Dies zeigt auf, dass auch viele von den bereits live im produktiven Betrieb eingesetzten Cloud-Systemen noch größere Sicherheitsbedrohungen aufweisen.

1.2 Problemstellung und Zielsetzung

Ziel dieser Arbeit ist die Erarbeitung einer Bedrohungsanalyse für den Betrieb einer fiktiven Anwendung in der Cloud. Dazu soll ein exemplarisches, aber möglichst realistisches Anwendungsszenario definiert und als Servicemodell eine Infrastructure as a Service Cloud verwendet werden. Die Bedrohungsanalyse soll sich am standardisierten Vorgehen der BSI-Grundschutz-Methodik orientieren, mit dem grundlegenden Ziel, dass Firmen mit einem ähnlichen Anwendungsszenario die erarbeiteten Inhalte als eine Basis beziehungsweise Werkzeug für eine eigene Bedrohungsanalyse nutzen können. Die erarbeitete Bedrohungsanalyse soll entweder vollständig genutzt werden oder dem entsprechenden System einfach angepasst beziehungsweise erweitert werden können.

Um dies zu erreichen, soll inhaltlich der Betrieb in einer Cloud bezüglich möglicher Bedrohungen, Schwachstellen, Angriffe analysiert werden. In einem nächsten Schritt sollen

Risiken dieser festgelegt und entsprechende Handlungsempfehlungen herausgearbeitet werden, um die Risiken angemessen zu behandeln. Wie im Rahmen der IT-Grundschutz-Methodik vorgesehen, soll auch das IT-Grundschutz-Kompendium [12] als Bausteinsystem genutzt werden, um relevante Bedrohungen, Schwachstellen und Angriffe für das fiktive System in der Cloud zu identifizieren. Bei der Auswahl von Inhalten soll der Fokus auf Bedrohungen, Schwachstellen oder Angriffe liegen, denen das Konzept des Cloud-Computings entweder als Ursache zugrunde liegt oder die dadurch ein erhöhtes Risiko aufweisen. Da das IT-Grundschutz-Kompendium in der Regel nur eine Basis bietet, sollen gar nicht oder nur unzureichend abgedeckte Bedrohungen mithilfe von zusätzlichen Quellen erarbeitet und Inhalte ergänzt werden. Anschließend soll für diese Bedrohungen, Schwachstellen und Angriffe das jeweilige Risiko im Rahmen einer Risikoanalyse bestimmt werden. Hier soll sich das Vorgehen am BSI-Standard 200-3 [18] orientieren, der auch in dem Gesamtprozess der IT-Grundschutz-Methodik enthalten ist [14]. Für die Bedrohungen, Schwachstellen und Angriffe mit dem höchsten Risiko sollen Maßnahmen und Handlungsempfehlung durch das IT-Grundschutz-Kompendium in Verbindung mit externen Quellen erarbeitet werden. Am Ende sollen die priorisierten Risiken derart minimiert sein, dass nach dem BSI-Grundschutz kein beziehungsweise ein deutlich verminderter Handlungsbedarf bezüglich weiterer Sicherheitsmaßnahmen für das definierte Anwendungsszenario übrig bleibt.

Auf Basis dieser Problemstellung beziehungsweise Zielsetzung lassen sich für diese Arbeit folgende Forschungsfragen festlegen:

- Welche Bedrohungen, Schwachstellen und Angriffe können sich für den Betrieb einer Anwendung in einer Infrastructure as a Service Cloud-Umgebung ohne bisherige Sicherheitsmaßnahmen ergeben?
- Welche konkreten Risiken entstehen aus den Bedrohungen, Schwachstellen und Angriffen für den Betrieb einer Anwendung in einer Infrastructure as a Service Cloud-Umgebung?
- Welche Maßnahmen und Handlungsempfehlungen sollten umgesetzt werden, um diese Risiken angemessen und effektiv zu behandeln?

1.3 Aufbau der Arbeit

Einleitend beginnt diese Arbeit mit der Definition eines exemplarischen Anwendungsszenarios. Hier werden insbesondere die Rahmenbedingungen, Sicherheitsleitlinien eines fiktiven Unternehmens und die Relevanz einer sicheren Cloud-Infrastruktur definiert. Nachfolgend wird anhand dieses Anwendungsszenarios eine dreiteilige Bedrohungsanalyse durchgeführt. Im ersten Teil werden relevante Systeme des Unternehmens identifiziert und der entsprechende Schutzbedarf festgelegt. Anschließend wird eine Übersicht an relevanten und Cloud-spezifischen Bedrohungen, Schwachstellen und Angriffen für dieses Anwendungsszenario herausgearbeitet, in verschiedene Kategorien gegliedert und die Relevanz erläutert. Als letzter Part dieser Trilogie wird eine Risikoanalyse für die jeweiligen Bedrohungen, Schwachstellen und Angriffe in Bezug auf die Eintrittshäufigkeit und Auswirkungen beziehungsweise Schadenshöhe für das fiktive Unternehmen durchgeführt. Nachdem dieser Analyseteil angeschlossen wurde, wird eine Risikobehandlung vorgenommen. Im Rahmen dessen wird eine Auswahl an verschiedenen Maßnahmen vorgestellt, sowie entsprechende Handlungsempfehlungen ausgesprochen, sodass dadurch eine möglichst hohe Informationssicherheit implementiert werden kann. Abschließend wird geprüft, ob die definierten Forschungsfragen beantwortet wurden, die Ergebnisse innerhalb eines Fazit zusammengefasst, sowie ein Ausblick auf zukünftige Entwicklungen gegeben.

1.4 Zielgruppe

Die Inhalten dieser Arbeit richten sich hauptsächlich an Personengruppen die sich mit der Einführung einer Infrastructure as a Service (IaaS) Cloud-Infrastruktur in ein bestehendes Unternehmen beschäftigen sollen. Mögliche Hintergründe hierfür könnten entwender der initiale Aufbau eines IT-Systems in der Cloud, als auch ein Umzug eines bestehenden IT-Systems von einer On-Premises-Infrastruktur in die Cloud durch verschiedenste Gründe sein. So bestehen diese Personengruppen häufig aus einer spezialisierten Gruppe von mitarbeitenden Personen, die oftmals einen detaillierten Überblick über eine bereits bestehende IT-Infrastruktur besitzen und ein entsprechendes technisches beziehungsweise fachliches Verständnis besitzen. Erste Cloud-Erfahrungen können optional vorhanden sein.

Eine weitere mögliche Personengruppe besteht aus mitarbeitenden Personen, welche die entwickelte Anwendungen als Dienstleistung in eine neue IaaS Cloud-Infratruktur von außenstehenden Firmen als Kunden migrieren beziehungsweise anschließend einen sicheren Betrieb dieser Anwendung in der Cloud sicherstellen.

Außerdem kann diese Arbeit ebenfalls zu Schulungszwecken verwendet werden, um beliebige Personengruppen für Gefahren innerhalb der Cloud zu sensibilisieren. Besonders sind hier Unternehmen angesprochen, die erst kürzlich einen initialen Kontakt mit dem Konzept des Cloud-Computings hatten und dadurch bisher nur ein beschränktes Knowhow bezüglich Cloud-Bedrohungen vorhanden ist. Relevant für Personengruppen ohne einen fachlichen Hintergrund sind insbesondere die Abschnitte zu den Gefahren der Täuschung auf sozialer Ebene beziehungsweise des Social Engineerings.

1.5 Einordnung und Abgrenzung

Diese Arbeit untersucht die Sicherheit einer IaaS Cloud-Infrastruktur am Beispiel eines fiktiven Anwendungsszenarios unter Berücksichtigung des Shared-Responsibility-Modells. Dabei orientiert sich diese Arbeit für die Bedrohungsanalyse an dem Schema und der empfohlenen Struktur der IT-Grundschutz-Methodik *(BSI-Standard 200-2 [14] und BSI-Standard 200-3 [18])* in Verbindung mit dem IT-Grundschutz-Kompendium [12] als Werkzeug. Auf die Nutzung anderer Vorgehensweisen wie beispielsweise der PASTA-Vorgehensweise[1] von GitLab oder der STRIDE-Vorgehensweise[2] von Microsoft wurde verzichtet. Dies ist hauptsächlich damit begründet, dass der IT-Grundschutz es ermöglicht, Sicherheitskonzepte insgesamt einfach und effizient zu erstellen. Insbesondere im Rahmen des BSI-Grundschutz-Kompendiums werden bereits für verschiedenste Komponenten eines Systems standardisierte Bausteine für Bedrohungen und Schwachstellen gegeben, sowie eine erste Einschätzung zur möglichen Eintrittswahrscheinlichkeit. Diese können ohne größere Aufwände entweder direkt übernommen und in Maßnahmen für das individuelle Szenario transferiert werden oder um weitere, noch nicht ausreichend abgedeckte Bedrohungen erweitert werden [14]. Insgesamt kann so der Arbeitsumfang reduziert werden und es entstehen standardisierte Arbeitsergebnisse.

[1] https://about.gitlab.com/handbook/security/threat_modeling/
[2] https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool-threats

Da diese Arbeit Bedrohungen mithilfe eines exemplarischen Anwendungsszenarios herausarbeitet, sind diese nicht gänzlich ohne Transferleistung universell auf andere Szenarien übertragbar. Allerdings wurde das Anwendungsszenario möglichst generisch, realistisch und minimal definiert, mit einer eher überdurschnittlichen Relevanz der Informationssicherheit, sodass eine Wiederverwendung der Bedrohungsanalyse für den eigenen Anwendungsfall mittels eines möglichst kleine Transferaufwands stattfinden können soll. Wie bereits erwähnt deckt der IT-Grundschutz bereits elementare Bedrohungen durch die verschiedenen Bausteine ab, sodass der Fokus auf Cloud-spezifischen Bedrohungen liegt, die bisher noch nicht ausreichend abgedeckt werden. Des Weiteren wird diese Menge insofern weiter eingeschränkt, dass hauptsächlich Bedrohungen, Schwachstellen und Angriffe analysiert werden, deren Ursache sich direkt aus dem Konzept des Cloud-Computings ergeben. Diese Eingrenzung basiert auf der Annahme, dass Unternehmen, die mit ihren IT-Systemen in eine Cloud-Infrastruktur ziehen, bereits Bedrohungsanalysen für vorherige Infrastrukturen durchgeführt haben und somit Bedrohungen, die allgemeingültig für jedes System sind, bereits ausreichend berücksichtigt wurden und in die neue Bedrohungsanalyse einfließen können. Außerdem wird diese Teilmenge dadurch weiter eingeschränkt, dass nur Bedrohungen berücksichtigt werden, die entweder dem Software as a Service Modell oder dem Plattform as a Service Modell innerhalb der Cloud zuzuordnen sind. So werden Bedrohungen bezüglich der Infrastruktur wie zum Beispiel gegenüber der Virtualisierung in Verbindung mit virtuellen Maschinen nicht berücksichtigt, da diese durch das gewählte Shared Responsibility Modell innerhalb des Zuständigkeitsbereiches des Cloud-Anbieters liegen.

Auch wenn der Fokus bereits auf Cloud-spezifischen Bedrohungen liegt, können auch mit dieser Einschränkung immer noch nicht alle Aspekte gänzlich innerhalb der Bedrohungsanalyse behandelt werden. So wurde eine Priorisierung erarbeitet und in den jeweiligen Abschnitten wird durch technische und organisatorische Argumente offen gelegt, inwiefern diese Inhalte eine ausreichende Relevanz für diese Arbeit besitzen. Trotz dessen wurden die Ergebnisse anhand des übergeordneten Ziels erarbeitet, dass hier eine möglichst hohe Abdeckung innerhalb des verfügbaren Umfangs erreicht werden soll.

2 Anwendungsszenario

2.1 MakeABank GmbH

Die MakeABank GmbH (MAB) ist ein fiktives mittelständisches Softwareunternehmen. Im Fokus steht dabei die Entwicklung und Wartung der Banksoftware „MaBCloud“. Bisher besteht das Unternehmen aus circa 200 Mitarbeitern, wovon 150 Mitarbeiter an der Entwicklung von „MaBCloud“ mitwirken. Die restlichen 50 Mitarbeiter gehören anderen Abteilungen wie dem Management, der Buchhaltung, dem Marketing, der UI/UX-Designabteilung oder dem Vertrieb an. Strukturell besteht die MakeABank GmbH aus einem Gründungsstandort in Hamburg und sechs weiteren Standorten deutschlandweit. Die Mitarbeiter sind gleichmäßig auf diese deutschlandweiten Standorte verteilt. Die Entwickler am Hauptstandort in Hamburg sind mit der Weiterentwicklung von Features für „MaBCloud“ beauftragt. Jeder weitere Standort besteht aus 2-3 Entwicklerteams, die jeweils für die Betreuung von einem festen Kontingent an Kunden zuständig sind. Diese Kunden befinden sich in der Regel in der geografischen Nähe, da die MakeABank GmbH strategisch auf einen regelmäßigen persönlichen Austausch in Form von Workshops, Schulungen und ähnlichen Formaten setzt, um eine möglichst hohe Kundenbindung zu generieren. So besteht die zweite Haupteinnahmequelle, neben dem Lizenzverkauf von „MaBCloud“, inzwischen auch aus umfangreichen Dienstleistungen im Bereich Migration, Customizing und Add-on-Entwicklung im Zusammenhang mit „MaBCloud“ für die jeweiligen Kunden. Vor der Coronapandemie verfolgte die MakeABank GmbH eine konservative Ausrichtung bezüglich des Homeoffice für Mitarbeiter. So wurde sichergestellt, dass die Kapazitäten innerhalb der verschiedenen Büros für die ansässigen Mitarbeiter ausreichend waren. Allerdings wurde anlässlich der Coronapandemie eine Trendwende der Firmenpolitik vollzogen, sodass nun den meisten MitarbeiterInnen das Homeoffice gestattet wurde. Dafür hat die MakeABank GmbH einheitliche und vorkonfigurierte Hardware in Form von Windows-Laptops ausgegeben. Zusätzlich darf für das Homeoffice standardisiertes Hardware-Zubehör beantragt werden. Mitarbeiter können jedoch weiter-

hin beliebig in der Firma an mobilen Arbeitsplätzen mit den ausgegebenen Windows-Laptops arbeiten. Die Kommunikation erfolgt größtenteils über asynchrone Kanäle wie einem zentralen Chatprogramm oder E-Mails. Für Besprechungen existiert eine externe Webanwendung für Videokonferenzen, die von einem externen Anbieter gewartet wird.

Das Hauptprodukt „MaBCloud“ hat sich bereits in der Bankenbranche etabliert und wird hauptsächlich von größeren europäischen Banken eingesetzt. Bisher wurde „MaBCloud“ als On-Premises-Software verkauft und wurde dementsprechend in kundeneigenen Rechenzentren oder Fremdrechenzentren unter Hauptverantwortung des jeweiligen Kunden betrieben. Durch die kundennahe Firmenstrategie und Rolle als Dienstleister wurden auf vielen dieser Systeme bereits diverse Wartungen, Migrationen und Installationen für den Betrieb von „MaBCloud“ durch MAB durchgeführt.

Nun kommt jedoch durch die Trendentwicklung bezüglich einer zunehmenden Cloud-Nutzung durch Unternehmen [50] innerhalb des Kundenkontingents die Nachfrage auf, „MaBCloud“ nicht mehr als On-Premises-Software zu betreiben, sondern als Anwendung in die Cloud zu migrieren. Auch hier wünschen sich die Kunden MAB als Dienstleister, um eine solche Migration und den anschließenden Betrieb von „MaBCloud“ in die Cloud zu realisieren beziehungsweise zu betreuen. So erarbeitet das Management indessen Voraussetzungen und Inhalte, um eine solche Dienstleistung in das Leistungsportfolio der MakeABank GmbH aufnehmen zu können.

Im Detail soll die neue Dienstleistung beinhalten, dass der Kunde eine Cloud-Umgebung im Rahmen eines IaaS Servicemodells bei einem beliebigen Cloud-Anbieter anmietet und MakeABank GmbH folgend die Migration von „MaBCloud“ in diese Cloud-Umgebung übernimmt. Ein vertraglich definiertes Ziel soll es sein, dass nach dem Prozess die Cloud-Umgebung so konfiguriert ist, dass ein stabiler und sicherer Betrieb von „MaBCloud“ ermöglicht ist.

2.2 Produkt „MaBCloud“

Unternehmen des Dienstleistungssektors und insbesondere Kreditinstitute beziehungsweise Banken haben eine Sorgfaltspflicht, falls diese im Rahmen von Transaktionen und Geschäftsbeziehungen Risikofaktoren für kriminelle Hintergründe, wie zum Beispiel Geldwäsche oder Terrorismus feststellen [28]. Die Bundesanstalt für Finanzdienstleistungsaufsicht schreibt hierzu:

> „Es gehört zur ordnungsgemäßen Geschäftspolitik aller verpflichteten Unternehmen im Finanzsektor, den Missbrauch des Finanzsystems durch Verschleierung und Verschiebung von Vermögenswerten illegaler Herkunft sowie Finanzierung von Terrorismus zu verhindern.“
>
> (Bundesanstalt für Finanzdienstleistungsaufsicht in [29])

MAB bietet mit „MaBCloud“ eine Anwendung, um die Banken bei der Einhaltung dieser Sorgfaltspflicht zu unterstützen. Im Detail handelt es sich bei „MaBCloud“ um eine Webanwendung, die das detaillierte Monitoring von Neukunden, Bestandskunden, sowie laufenden Transaktionen ermöglicht. „MaBCloud“ übernimmt zudem die Beschaffung aller Informationen, die für das Monitoring beziehungsweise Prüfung notwendig sind. Dabei aggregiert „MaBCloud“ nicht nur Daten aus intern vorliegenden Datenbeständen, wie zum Beispiel persönliche Daten oder gegebenenfalls Informationen über Firmenstrukturen, sondern übernimmt auch weitere Dienste zur nötigen Informationsbeschaffung wie zum Beispiel die PEP-Prüfung oder das Abgleichen von Personen mit wirtschaftlichen Sanktionslisten aus Informationsquellen externer Anbieter. Diese Daten werden letztendlich durch „MaBCloud“ aufbereitet, auf einer grafischen Oberfläche zusammengeführt und der mitarbeitenden Person zur endgültigen Prüfung vorgelegt. Parallel wertet „MaBCloud“ diese Daten auf Basis bestimmter Algorithmen aus und gibt eine unterstützende Abschätzung zum vorliegenden Risikopotenzial ab, sowie warnt, falls das Risikopotenzial als hoch berechnet wurde. Falls eine Prüfung durch die mitarbeitende Person ebenfalls als riskant in Bezug auf kriminelle Vorgänge eingestuft wird oder eine solche Warnung durch diese verifiziert wird, kann „MaBCloud“ ebenfalls bei einer Meldung an die entsprechende Aufsichtsbehörde mit allen benötigen Daten unterstützen.

Um diese Funktionalitäten zu ermöglichen, verarbeitet und speichert „MaBCloud“ dementsprechend sensible und personenbezogene Daten in einem hohen Umfang. Um einen weiteren Einblick zu geben, wurden im Zuge der Planung von „MaBCloud“ unter anderem folgender Katalog von Anwendungsfällen definiert:

- Als Bankmitarbeiter kann ich Einsicht in nötige persönliche Daten eines Kunden erhalten.
- Als Bankmitarbeiter bekomme ich Warnmeldungen bei verdächtigen Transaktionen beziehungsweise Neukundenanfragen.
- Als Administrator kann ich zu Wartungszwecken umfassende Geschäftsdaten einsehen und bearbeiten.

- Als Administrator kann ich das System umfassend konfigurieren.
- Als Bankmitarbeiter kann ich ohne großen Aufwand Verdachtsmeldungen bezüglich krimineller Vorgänge an die zuständige Aufsichtsbehörde verschicken.

Generell wird „MaBCloud“ den Endnutzern als Webanwendung zur Verfügung gestellt. Die Clients erhalten Zugriff auf die entsprechende Oberfläche mittels eines beliebigen und handelsüblichen Browsers. Die Gesamtstruktur des „MaBCloud“ Systems ist in einer 3-Schichten-Architektur aufgebaut. Aus logischer Perspektive ist diese in eine Schicht für die Weboberfläche, eine Schicht für die Geschäftslogik und eine Schicht für die Datenbankanwendung aufgebaut. Aus technischer Perspektive soll für jede Schicht eine eigene Virtualisierungszone eingerichtet werden. In jeder Virtualisierungszone laufen mehrere virtuelle Maschinen einer Schicht, die je nach Auslastung in der Anzahl hoch und herunterskaliert werden können. Die Kommunikation zwischen den Zonen wird so begrenzt, dass nur virtuellen Maschinen aus einer Zone der jeweils direkt angrenzenden logischen Schicht miteinander über das Netzwerk kommunizieren können. Zudem findet ein direktionaler Datenfluss statt. Als ein Fallbeispiel kann so die Weboberfläche also nur Anfragen an die Geschäftslogik schicken und nicht andersherum, jedoch nicht direkt mit virtuellen Maschinen aus der Zone der Datenbankanwendungen kommunizieren. Diese Trennung der Schichten, mit jeweils eigener Skalierung, sollen einen hohen Grad an Skalierbarkeit, Robustheit und Sicherheit von „MaBCloud“ als Gesamtsystem erreichen. Die 3-Schichten werden innerhalb dieser Arbeit fortführend als *Frontend* (Weboberfläche), *Backend* (Geschäftslogik) und *Persistenz* (Datenbank) bezeichnet.

Auf Anwendungsebene wird das Frontend mit der JavaScript Web-Bibliothek ReactJS[1] und verschiedenen weiteren Bibliotheken entwickelt, welche über einen Paketmanager eingebunden werden. Das Backend besteht aus einer Java Spring Boot[2] Anwendung, die dem Frontend eine Schnittstelle mittels einer REST API anbietet. Die Persistenz wird durch ein objektrelationales Datenbanksystem, wie PostgreSQL[3] realisiert. Der Austausch von Daten des Backends und der Persistenz findet über einen entstprechenden Treiber als Schnittstelle statt.

Damit „MaBCloud“ als Anwendung lauffähig ist, muss auf den virtuellen Maschinen der verschiedenen Zonen eine bestimmte Plattform gegeben sein. Deshalb wird auf jeder

[1] https://react.dev/
[2] https://spring.io/projects/spring-boot
[3] https://www.postgresql.org/

virtuellen Maschine standardisiert Linux als Betriebssystem installiert sowie weitere Abhängigkeiten, wie beispielsweise ein nginx Webserver[4] im Frontend, ein Treiber zur Verbindung mit dem objektrelationalen Datenbanksystem, sowie eine JVM[5] im Backend.

Außerdem wurden bereits einige grundlegende Anforderungen an das System „MaBCloud“ in der Cloud definiert. So soll die Administration des „MaBCloud“ Systems durch eine Cloud-Konsole des beliebigen Anbieters durchgeführt werden. Erreichbar soll diese entweder mittels der Konsolenanwendung aller gängigen Betriebssysteme sein oder durch eine Weboberfläche. Hier sollen zentrale Aspekte der Cloud wie zum Beispiel die logische Architektur und logische Netzkomponenten modelliert sowie, SSH-Schlüssel für Remote-Verbindungen auf VMs, Cloud-Dienste und weitere zentrale Aspekte beliebig konfiguriert werden können. Als Abrechnungsmodell soll erstmal die nutzungsbasierte Abrechnung verwendet werden, das nach Nutzung von Ressourcen abrechnet. Mithilfe dieses Modells soll für die anfängliche Betriebsphase am meisten Flexibilität ermöglicht werden, um Referenzdaten bezüglich der Systemauslastung und mögliche Metriken für eine optimale Skalierung in der Cloud zu sammeln. An sinnvollen Stellen sollen ausgewählte und vertrauenswürdige Cloud-Dienste für das weitere Outsourcing von Zuständigkeiten genutzt werden, um die Komplexität und den Wartungsaufwand des Systems in der Cloud möglichst gering zu halten. Bezüglich „MaBCloud“ als Anwendung soll durch das historische Wachstum als Anwendung im Rahmen der 3-Schichten Architektur, diese auch bestmöglich in der Cloud übernommen werden und bestenfalls kein kostenintensiver Umbau in eine Microservice-Architektur oder ähnliche Modelle stattfinden.

2.3 Relevanz der Informationssicherheit

Die Relevanz der Informationssicherheit ist grundsätzlich sehr hoch unter der Bezugnahme, dass alle Kunden als Bank beziehungsweise Kreditinstitut in der Finanzbranche tätig sind und es sich dabei um einen von sieben Sektoren kritischer Infrastruktur der EU handelt, der dementsprechend durch die Mitgliedstaaten unbedingt am Laufen gehalten werden muss [55]. Besonders auf Ebene der Europäischen Union existieren sowohl grundsätzlich für alle Unternehmen einzuhaltende Verordnungen, wie der DSGVO [102], als auch zusätzliche Anforderungen speziell für Finanzinstitutionen in Bezug auf die Prä-

[4] https://www.nginx.com/
[5] https://www.oracle.com/de/java/technologies/downloads/

vention von Geldwäsche, der Finanzierung von Terrorismus oder sonstiger Wirtschaftskriminalität [28].

Bereits die für EU-Unternehmen allgemeingültige DSGVO regelt den Umgang mit personenbezogenen Daten und die Rechte von Betroffenen. Hier existiert der wesentliche Grundsatz, dass alle sensiblen Informationen angemessen geschützt werden müssen. Die sogenannten „angemessenen“ Maßnahmen müssen sich am Stand der Technik, der notwendigen Kosten und den Umständen beziehungsweise Risiken orientieren [38]. Beim Nichteinhalten können schon hier Bußgelder von bis 20 Millionen Euro festgelegt werden oder für international agierende Unternehmen von bis zu 4 % des weltweiten Vorjahresumsatzes [102].

Kreditinstitute und Finanzinstitute müssen zudem das Know-Your-Customer-Prinzip erfüllen zur Prävention von Geldwäsche, Finanzierung von Terrorismus oder sonstiger Wirtschaftskriminalität, weshalb der Umfang von sensiblen Informationen besonders hoch ist. So wird im Rahmen der vierten EU-Geldwäsche Richtlinie explizit erlaubt, personenbezogene Daten zu speichern und zu verarbeiten, wenn diese benötigt werden, um verdächtige Transaktionen zu untersuchen und zu melden [105]. Dazu gehören beispielsweise die persönlichen und gegebenenfalls geschäftlichen Daten eines Konteneigentümers, sowie bei politischer Exposition die Funktion und der Ausführungsort des Amtes [97]. Diese Richtlinien gelten nicht nur europaweit, sondern müssen auch auf Zweigstellen und Tochterfirmen in Drittländern angewendet werden [105], weshalb das nahezu gesamte Kundenkontingent von der MakeABank GmbH dies umsetzen muss. Sollten diese Richtlinien nicht eingehalten werden, drohen nicht nur, wie bei der DSGVO empfindliche Geldstrafen, sondern auch Haftstrafen für leitende Mitarbeiter oder eine Entziehung der Geschäftserlaubnis [97]. Hier müssen also sensible Daten in einem hohen Umfang verarbeitet und gespeichert werden, was das entstehende Risiko für das Unternehmen durch einen Sicherheitsvorfall ansteigen lässt.

Bei den analysierten Richtlinien handelt es sich nur um einen Auszug eines breiten Anforderungskataloges, der entweder die Informationssicherheit direkt adressiert oder ein besonders hohes Maß an Informationssicherheit impliziert, um gegebene Richtlinien nicht existenzbedrohend zu verletzen. So hat die Europäische Union inzwischen einen umfangreichen generellen Maßnahmenkatalog in Form des „Digital Resilience Acts“ (DORA) oder der „Cybersecurity Strategy of the European Union: An Open, Safe and Secury Cyperspace“, aber auch weitere speziell für Finanzinstitutionen wichtige Kataloge wie beispielsweise den „Capital Requirements Regulations“ (CRR) definiert [55].

Ein weiterer Aspekt in Bezug auf die Relevanz der Informationssicherheit ist der, dass sich Vorfälle, welche die Informationssicherheit bedrohen, nicht nur juristische Folgen haben können, sondern auch einen Reputationsverlust gegenüber Kunden zufolge haben können. Da es sich bei Bankverbindungen und Details über politische Aspekte, wie im Rahmen der PEP-Prüfung, um besonders sensible Daten handelt, kann es bei einem Datenleck zu einem verhältnismäßig schnellen Vertrauensverlust des Endkunden gegenüber des Finanzinstitutes kommen. Ein Vorfall wäre direkt existenzbedrohend für das jeweilige Finanzinstitut. Von daher existiert zwischen den Finanzinstituten und der MakeABank GmbH ein hoher, aber sensibler Grad an Vertrauen in die Sicherheit des „MaBCloud“ Systems.

2.4 Aktuelles Sicherheitsszenario

Das aktuelle Sicherheitsszenario von der MakeABank GmbH zeichnet sich dadurch ab, dass bereits vor etwa zwei Jahren eine Bedrohungsanalyse inklusive einer umfangreichen Risikoermittlung mittels des IT-Grundschutzes für den Betrieb von „MaBCloud“ auf einem On-Premises System durchgeführt wurde. Diese wurde sogar derart gründlich durch eine interne Auswahl von Mitarbeitern durchgeführt, dass eine ISO 27001 Zertifizierung im Rahmen eines Audits gegenüber eines BSI zertifizierten Auditor [48] für das System erreicht werden konnte. Diese Zertifizierung wurde durch die MakeABank GmbH insbesondere als Vertrauensnachweis gegenüber neuen und bestehenden Kunden genutzt.

Da nun allerdings das On-Premises System gegen eine Cloud-Infrastruktur ausgetauscht werden soll, wurden im Zuge einer groben Vorabschätzung bereits derart neue und risikoreiche Bedrohungsfelder ermittelt, dass nun eine neue Bedrohungsanalyse mit dem Fokus auf Cloud-spezifisiche Bedrohungen, Schwachstellen und Angriffe stattfinden soll. Dazu soll ersteinmal eine minimale Cloud-Architektur betrachtet werden, auf der „MaBCloud“ lauffähig ist. Anhand dieser wird ein Basiskatalog an Bedrohungen und Maßnahmen insofern herausgearbeitet, sodass der in Nachhinein als Basis für kundenspezifische Architekturen angewendet werden kann. Das übergeordnete Schutzziel, das im Zuge der Bedrohungsanalyse durch MakeABank GmbH verfolgt werden soll, ist der „Schutz von vertraulichen und personenbezogenen Informationen in der Cloud“.

3 Grundlagen

3.1 IT-Sicherheit

Insgesamt bezeichnet die IT-Sicherheit alle Planungen, Maßnahmen und Kontrollen, die dem Schutz der Informationstechnik dienen [94]. Das amerikanische *National Institute of Standard* hat dies ausführlich in Zusammenarbeit mit dem *U.S. Department of Commernce* im Rahmen eines Anforderungskataloges für minimale Sicherheitsanforderungen von amerikanischen Regierungssysteme wie folgt definiert:

> „The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability“ in [37, S. 7]

Wie in der Definition zu erkennen, umfasst die IT-Sicherheit nicht nur den Schutz von personenbezogenen Daten und Informationen an sich, sondern auch den Schutz aller Systeme, mit denen Daten verarbeitet, genutzt und gespeichert werden. Eine Gefährdung der IT-Sicherheit liegt vor, wenn innerhalb eines Systems eine Schwachstelle existiert, die ausgenutzt werden kann um einen der Grundwerte zu verletzten. Die größte Bedrohung liegt dabei in einem lückenhaften Sicherheitskonzept, weshalb es essenziell ist eine möglichst breite Bedrohungsanalyse für bestehende IT-Systeme durchzuführen, um so Risiken und den Schutzbedarf zu analysieren, zu benennen und umzusetzen [94].

Die Grundwerte der IT-Sicherheit, die durch das Ausnutzen einer Schwachstelle verletzt werden können, setzen sich dabei aus drei Hauptzielen zusammen:

- Verfügbarkeit: Eine Information muss zu jedem Zeitpunkt für jede beliebige, aber berechtigte Person zugänglich sein. Falls ein System durch das Ausnutzen einer Schwachstelle ausfällt und so Informationen nicht mehr abgerufen werden können, wird das Ziel der Verfügbarkeit verletzt [103].

- Vertraulichkeit: Vertrauliche Daten dürfen nicht von unbefugten Personen abgerufen werden. Dieses Ziel lässt sich dahingehend erweitern, dass selbst befugte Personen eine so minimale Berechtigungsmenge erhalten, wie diese für den korrekten Abruf einer Information benötigen. Dies bezieht sich insbesondere auf verschiedene Berechtigungen zum Lesen und zum Schreiben. Dementsprechend ist dieses Schutzziel verletzt, wenn unbefugte Personen Zugriff zu vertraulichen Informationen erhalten oder Aktionen außerhalb des gewünschten Rahmens durchführen können [103].
- Integrität: Dieses Schutzziel beinhaltet gleich mehrere Anforderungen. Es gilt dabei zwischen starker und schwacher Integrität zu unterscheiden. So dürfen im Rahmen einer starken Integrität Information nicht ungewollt verändert werden. Im Rahmen einer schwachen Integrität ist dies zugelassen, aber Veränderungen müssen nachvollzogen werden können. Des Weiteren gilt für beide Arten der Integrität, dass die Verlässlichkeit von Daten und Systemen gewährleistet sein, sowie ständig eine Vollständigkeit von Informationen vorliegen muss [103].

Je nach System können diese Grundwerte um beliebige, optionale Grundwerte erweitert werden. Aufgrund des beschränkten Rahmens dieser Arbeit werden diese jedoch nicht erarbeitet, beziehungsweise weiter verfolgt.

Folgende Abkürzungen werden innerhalb dieser Arbeit für jeden Grundwert der Informationssicherheit verwendet:

Grundwert	**Abkürzung**
Verfügbarkeit	A
Vertraulichkeit	C
Integrität	I

3.2 Cloud-Computing

Laut dem *National Institute of Standards and Technology* des *U.S. Department of Commerce* ist das Cloud-Computing ein Konzept, welches es erlaubt, zeitnah, unkompliziert und anfrage basiert, den Netzwerkzugriff auf ein bestimmtes Kontingent von geteilten und konfigurierbaren Rechenressourcen zu erhalten. Diese Ressourcen bestehen dabei

aus verschiedenen Hardware- und Softwarekomponenten wie Netzwerke, Server, Speichermedien und weitere bereitgestellte Dienste des Cloud-Anbieters. Der Prozess ist dabei vollständig automatisiert, sodass während der Bereitstellung ein naher Kontakt zum Cloud-Anbieter gänzlich wegfällt [59]. Nach der Bereitstellung kann ein Kunde die Cloud-Umgebung über bestimmte Endpunkte von entsprechenden Programmierschnittstellen (APIs) konfigurieren. Alternativ dazu wird bei gängigen Cloud-Anbietern sowohl ein Kommandozeilen-Werkzeug oder als auch eine Weboberfläche mitgeliefert, welche bei Nutzung den Verwaltungsvorgang einer Cloud-Umgebung vereinfachen. Um das Konzept des Cloud-Computings zu konkretisieren, existieren einige weitere grundlegende Besonderheiten im Vergleich zu herkömmlichen On-Premises Nutzungsmodellen.

Eine erste Besonderheit des Cloud-Computing dabei ist, dass die verfügbaren Ressourcen des Cloud-Anbieter im Rahmen eines Multi-Tenant Modells auf eine große Menge an verschiedene Kunden aufgeteilt werden können [15]. Viele verschiedene Kunden teilen sich so eine identische Infrastruktur. Dabei versuchen die Cloud-Anbieter einen derart hohen Grad an Isolation zwischen den Systemen der Kunden herzustellen, dass andere Systeme auf derselben physischen Infrastruktur für einen Kunden praktisch nicht wahrgenommen werden können [98]. Bestimmte Ressourcen müssen daher mandatenfähig sein [15].

Die zweite thematisierte Besonderheiten des Cloud-Computings erfolgt im Rahmen der Abrechnung. Hier existieren verschiedenste Modelle, die sich in zwei Ansätze gliedern lassen. So gibt es einerseits verschiedene feste Vertragsformen, in welchen die Kunden ein immer festes Kontingent an Ressourcen zur Verfügung gestellt wird und damit ein fester Preis pro Intervall gezahlt wird. Andererseits existieren dynamische Modelle, die auch innerhalb dieser Arbeit relevant sind. Im Rahmen dieser kann ein Kunde nahezu unendlich Ressourcen in Anspruch nehmen und bezahlt diese nutzungsbasiert in einem bestimmten Intervall [27]. Die Ressourcennutzung kann dabei von dem Kunden und dem Cloud-Anbieter währenddessen ständig überwacht werden. Dieses Abrechnungsmodell wird auch als nutzungsbasiertes Abrechnungsmodell beziehungsweise Pay-per-use-Modell bezeichnet [15].

Aus der Beanspruchung von nahezu unendlich Ressourcen ergibt sich eine letzte thematisierte Besonderheit des Cloud-Computings. Da in der Regel ein global verteiltes Netz an Rechenzentren mit hohen Kapazitäten hinter den Cloud-Anbietern steht, bietet die Cloud einen hohen Grad an Elastizität für ein Kundensystem. Die beanspruchbaren Ressourcenkapazitäten erscheinen einem Kunden als unendlich und können schnell, in nahezu beliebigen Ausmaße und zu jeder Zeit zugewiesen werden [59]. Dadurch entsteht ein ho-

her Grad an Flexibilität bezüglich der Skalierung eines Kundensystems. Dies stellt auch eine der hauptsächlichen Motivationen für die Nutzung des Cloud-Computings dar.

Die genutzten Technologien innerhalb einer Cloud werden häufig in drei konkrete Servicemodelle gegliedert [15]. Diese reichen von der Bereitstellung einer physischen Infrastruktur bis zur Bereitstellung einer vollständig gehosteten Anwendung. Dies kann auch, wie in vielen Quellen wiederzufinden, symbolisch als Ebene innerhalb eines 3-Schichtenmodells modelliert werden. Jede Schicht wird dabei tendenziell zu unterschiedlichen Tarifen als Service durch den Cloud-Anbieter angeboten. Die Ebenen unterscheiden sich dabei am meisten durch eine Veränderung der Zuständigkeiten zwischen dem Cloud-Anbieter und dem Kunden. Inbesondere gilt dies bezüglich der Wartung, der Herstellung einer angemessenen Sicherheit und der zuverlässigen Bereitstellung von Infrastruktur beziehungsweise Diensten [15].

3.2.1 Infrastructure as a Service

Das Infrastructure as a Service (IaaS) Servicemodell beinhaltet jegliche Hardwareelemente der Rechenzentren, im Speziellen die Server, Datenspeichermedien und die physikalische Netzwerkanbindung. Des Weiteren fällt die Virtualisierung in diese Ebene. Wird eine IaaS Cloud-Umgebung beansprucht, so werden diese Aspekte entsprechend durch den Cloud-Anbieter für den Kunden bereitgestellt. Die restliche Infrastruktur bezüglich einer geeigneten Plattform für die zu integrierende Anwendung, sowie die Anwendung selbst muss der Kunde integrieren und verwalten [10]. Dies schafft eine hohe Flexibilität, da per Lift-and-Shift Prinzip eine bereits bestehende Infrastruktur von einem anderen System ohne umfangreiche Änderungen in eine IaaS Cloud migriert werden kann [45], was auch im vorliegenden Anwendungsszenario angestrebt wird. Des Weiteren ist dies in der Regel die günstigste Vertragsform, begründet dadurch, dass hier im Vergleich zu allen anderen Servicemodellen der größte Verwaltungsaufwand beziehungsweise Zuständigkeitsbereich beim Kunden liegt.

3.2.2 Plattform as a Service

Das Plattform as a Service (PaaS) Servicemodell baut auf dem Funktionsumfang der Infrastructure as Service Servicemodells auf. So liefert hier der Cloud-Anbieter nicht nur die Infrastruktur aus, sondern ebenfalls eine fertige Entwicklungsumgebung, sodass neue

Anwendungen ohne den Einkauf neuer Hardware und Software entwickelt werden können. Dazu zählen insbesondere inkludiere Debugging-Prozesse, diverse Testframeworks, aber auch SDKs für die Entwicklung von mobilen Anwendungen, weshalb dies ein besonders weit verbreitetes Einsatzszenario von einer PaaS Cloud-Umgebung darstellt [30].

Allerdings können einzelne Plattform-Dienste oder weitere Angebote auch modular in eine IaaS Cloud-Umgebung integriert werden, um bestimmte Funktionen bereitzustellen. Liegt ein solcher Kontext vor, wird auch die Begrifflichkeit „as a Service“ genutzt [15]. Konkrete Beispiele hierfür können im Rahmen der Google Cloud, der Datenbank-Dienst Cloud SQL[1] oder die Google Kubernetes Engine[2] zum Ausführen von containerisierten Anwendungen sein. Diese Dienste werden durch den Cloud-Anbieter oder externe Anbieter gewartet, gesichert und möglichst zuverlässig bereitgestellt. Der Benutzer kann diesen Dienst ebenfalls über zusätzliche APIs verwalten. Allerdings fallen hierfür üblicherweise zusätzliche Kosten an. Im Rahmen dieser Arbeit werden diese Dienste als ein verwalteter Dienst bezeichnet. Insgesamt können diese oftmals grob dem Plattform as a Service Servicemodell zugeordnet werden, allerdings lässt sich dies nicht grundlegend pauschalisieren [15].

3.2.3 Software as a Service

Das Software as a Service (SaaS) Servicemodell stellt neben der Hardware und einer Plattform direkt eine konkrete Webanwendung zur Verfügung, die über den Browser abgerufen werden kann. Hinter diesem Servicemodell steht also nicht nur ein Cloud-Anbieter, sondern auch ein entsprechender Dienstleister, der seine Software auf der Infrastruktur beziehungsweise Plattform zur Nutzung zur Verfügung stellt. Für Firmen ergibt sich daraus der Vorteil, dass die Software nicht installiert werden muss und nicht permanent gekauft werden muss, sodass eine gewisse Flexibilität bezüglich genutzter Anwendungen entsteht [31]. Dieses Servicemodell besitzt im Rahmen dieser Arbeit jedoch keine nähere Relevanz.

3.2.4 Shared-Responsibility-Modell

Um die thematisierten Zuständigkeiten pro Servicemodell nun vertraglich zu konkretisieren wird in der Regel das Shared-Responsibility-Modell verwendet. Dieses Modell bietet

[1] https://cloud.google.com/sql
[2] https://cloud.google.com/kubernetes-engine

eine Methode, um Zuständigkeiten klar zwischen Cloud-Anbieter und Kunden aufzuteilen zu können. Insbesondere im Fokus stehen hierbei die Zuständigkeit bezüglich der Sicherheit, welche dementsprechend auch im Rahmen dieser Arbeit besonders relevant sind. Das Modell bezieht sich dabei auf konkrete Komponenten einer Cloud-Umgebung, definiert hier die Zuständigkeit pro Servicemodell und kann als Matrix dargestellt werden, wie in Abbildung 3.1 abgebildet. In der Regel bildet das Shared Responsibility ebenfalls die vertragliche Grundlage bezüglich der Zuständigkeiten im Bereich der Sicherheit.

Table 2 Mapping responsibility for data Security & privacy requirements to cloud service models: (developed from Microsoft, Techtalk, IBM, and Amazon)
C= Client; CSP = Cloud Service Provider

Responsibility	On-premise	SaaS		PaaS		IaaS	
Data Governance	C		C		C		C
Endpoints Protection	C		C		C		C
User Access Management	C		C		C		C
Identity Infrastructure	C	CSP	C	CSP	C		C
Application	C	CSP		CSP	C		C
Network Control	C	CSP		CSP	C		C
OS Security	C	CSP		CSP			C
Host	C	CSP		CSP		CSP	
Network	C	CSP		CSP		CSP	
Data Centre	C	CSP		CSP		CSP	

Abbildung 3.1: Matrix des Shared-Responsibility-Modells für gängige Cloud-Anbieter. Quelle: [56]

4 Bedrohungsanalyse

4.1 Methodik

Nachdem nötige Grundlagen für das Thema erarbeitet wurden, widmet sich dieses Kapitel nun der Bedrohungsanalyse. Die Methodik der Bedrohungeanalyse basiert dabei auf der IT-Grundschutz-Methodik aus den BSI Standards 200-2 [14] und 200-3 [18]. In diesen wird durch das BSI eine Vorgehensweise beschrieben, mit der sich die Informationssicherheit eines Unternehmens steuern lässt, indem ein Managementsystem für die Informationssicherheit aufgebaut wird [14].

Dazu wird zu Beginn eine Initialisierung des Sicherheitsprozesses mit der Definition von Sicherheitsleitlinien und diverser Hintergrundinformationen vorgenommen. Hier werden Kernpunkte zu allgemeinen Einflussfaktoren, internen beziehungsweise externen Rahmenbedingungen wie Geschäftsziele, Organisationsstruktur oder ein strategischer Kontext definiert [14]. Diese Initialisierung wurde bereits im Rahmen der Definition des Anwendungsszenarios innerhalb des 2. Kapitels bearbeitet.

Nach einer abgeschlossenen Initialisierung bietet der IT-Grundschutz verschiedene Vorgehensweisen an. So gibt es die Möglichkeit einer Basis-Absicherung, die eine grundlegende Absicherung der Geschäftsprozesse und Ressourcen einer Institution mit einem dafür zeitlich niedrigen Aufwand ermöglicht. Eine weitere Möglichkeit wäre eine Kern-Absicherung, bei der eine Konzentration auf den Schutz von essenziellen Geschäftsprozessen und Ressourcen vorgenommen wird. Die dritte, vom BSI präferierte und auch hier verwendete Vorgehensweise der Standard-Absicherung zielt darauf ab, mittelfristig ein vollständiges Sicherheitskonzept zu erreichen [14]. Diese wurde für das vorliegende Anwendungsszenario ausgewählt, da es sich bei der Migration von „MaBCloud“ in die Cloud um keinen besonders zeitkritischen Vorgang handelt. Zudem ist eines der Ziele von der MakeABank GmbH auch für den Betrieb in der Cloud eine ISO 27001 Zertifizierung zu erhalten, wofür

ein vollständiges Sicherheitskonzept im Rahmen der Standard-Absicherung eine Option darstellt [48].

Die BSI-Grundschutz-Methodik sieht nun im Rahmen der Standard-Absicherung eine Strukturanalyse des zu analysierenden Systems vor, um den Geltungsbereich für eine Bedrohungsanalyse zu konkretisieren. Dieser Geltungsbereich wird innerhalb des IT-Grundschutzes als *Informationsverbund* bezeichnet. Dazu werden betroffene Geschäftsprozesse, Anwendungen, Netzkomponenten, IT-Systeme und weitere relevante Objekte benannt, einer Bezeichnung zugewiesen und organisatorische Verantwortlichkeiten festgelegt. Da die Systeme vor allem bei der Anwendung von Virtualisierungskonzepten im Zuge von Cloud-Computing schnell an großer Komplexität gewinnen und oft mehreren virtuellen Maschinen mit gleichen technischen Komponenten beziehungsweise Anwendungen parallelisiert betrieben werden, ist eine Komplexitätsreduktion durch eine Gruppenbildung als erforderlich genannt [14]. Diese wird dementsprechend auch im Rahmen dieser Arbeit umgesetzt. Das BSI konkretisiert hierzu in [14], dass Objekte dann ein und derselben Gruppe zugeordnet werden können, wenn die Objekte alle:

- vom gleichen Typ sind,
- ähnliche Aufgaben haben,
- ähnlichen Rahmenbedingungen unterliegen,
- den gleichen Schutzbedarf aufweisen.

Nachdem die Strukturanalyse abgeschlossen ist, folgt eine Schutzbedarfsfeststellung. In dieser gilt es für jedes innerhalb der Strukturanalyse identifiziertes Zielobjekt festzulegen, welchen Schutzbedarf dieses in Bezug auf das jeweilige Schutzziel der Informationssicherheit aufweist. Wie bereits innerhalb der Grundlagen erwähnt, geht es dabei vornehmlich um die Vertraulichkeit, Integrität und Verfügbarkeit. Dadurch kann für jedes Objekt ein Monitoring stattfinden wie hoch die Relevanz des Objektes innerhalb der Analyse von Bedrohung, Schwachstellen und Angriffen und der daraus resultierende Ableitung von Schutzmaßnahmen ist. Das BSI gibt hier exemplarisch die Schutzbedarfskategorien von „normal“ über „hoch“ bis „sehr hoch“ vor. Diese werden auch innerhalb dieser Arbeit verwendet. Da das grundlegende Ziel der Standard-Absicherung die Erzielung eines normalen Schutzbedarfes ist, müssen Objekte mit einem normalen Schutzbedarf in allen Schutzzielen nicht weiter betrachtet werden. Dies geschieht unter der Annahme, dass sich die hier bereits bestehenden Schutzmaßnahmen als ausreichend erweisen [14].

Für Objekte, die mindestens einen hohen Schutzbedarf aufweisen, wird mithilfe des IT-Grundschutzkompendiums nun eine Sicherheitskonzeption erstellt. Als Basis werden vordefinierte und standardisierte Bausteine aus dem IT-Grundschutzkompendium verwendet. Diese enthalten Sicherheitsanforderungen, die sich nach dem aktuellen Stand der Technik orientieren sollen [12] und sich dabei jeweils auf typische Komponenten eines Gesamtsystems wie Anwendungen, IT-Systeme, organisatorische Prozesse et cetera beziehen. Durch das IT-Grundschutzkompendium unzureichend abgedeckte Sicherheitsanforderungen beziehungsweise Bedrohungen müssen individuell und eigenständig ergänzt werden [14]. So wird jedem Objekt des Informationsverbunds eine Gesamtmenge an relevanten Bedrohungen und Sicherheitsanforderungen zugeordnet. Daraus resultiert eine Gefährdungsübersicht.

Auf der Schutzbedarfsermittlung und der Gefährdungsübersicht aufbauend wird insbesondere mithilfe des BSI-Standard 200-3 [18] eine Risikoanalyse durchgeführt. Hier werden die relevanten Bedrohungen aus der Gefährdungsübersicht durch eine Risikoeinstufung auf das konkrete Risiko für das System untersucht. Anschließend gilt es, anhand der festgestellten Risiken geeignete Sicherheitsmaßnahmen festzulegen und mithilfe dieser eine Risikobehandlung vorzunehmen, sodass ein normaler Schutzbedarf erreicht oder das Risiko in bestimmten Szenarien akzeptiert werden kann. Abschließend werden diese Maßnahmen in das bestehende Sicherheitskonzept integriert beziehungsweise Handlungsempfehlungen ausgesprochen und damit die Bedrohungsanalyse abgeschlossen.

Durch den beschränkten Umfang dieser Arbeit werden nicht alle Bedrohungen, welche für die analysierten Objekte im Kompendium aufgeführt werden, detailliert herausgearbeitet, weshalb hier vom BSI-Vorgehen abgewichen werden muss und sich diese Arbeit nur auf Cloud-spezifische Bedrohungen beschränkt. Ähnliches gilt für die ausführlichen Begründungen der Risiken im Rahmen der Risikoeinstufung, sowie für die abgeleiteten Sicherheitsmaßnahmen.

4.2 Strukturanalyse der verwendeten Systeme

Als einer erster Schritt innerhalb der Bedrohungsanalyse folgen nun die konkreten Ergebnisse der durchgeführten Strukturanalyse. Einleitend erscheint dazu eine generelle Übersicht der Systeme, welche für das vorliegende Anwendungsszenario innerhalb der Strukturanalyse erarbeitet wurden. Die hier genutzten Kategorien wurden aus dem BSI-Standard 200-2 übernommen [14].

1. **Anwendungen**

   A001: MaBCloud Frontend VM[1]

   A002: MaBCloud Backend VM[2]

   A003: objektrelationale Datenbanksystem VM[3]

   A004: virtuelle Firewall[4]

   A005: Cloud-Konsole / Web-Administrationsoberfläche für die Cloud-Umgebung

   A006: virtuelle Loadbalancer[5]

2. **Kommunikationsverbindungen**

   K001: Verbindung zwischen Cloud-Netzkomponenten

   K002: Verbindung zwischen Clients und Cloud-Endpunkt

3. **IT-Systeme**

   C001: Windows-Clients

   S001: Virtualisierungsserver

Wie bereits erwähnt bezieht sich diese Bedrohungsanalyse auf eine vereinfachte und minimale Beispielarchitektur der Cloud, die sich bei gängigen Cloud-Anbietern umsetzen lässt und auf der „MaBCloud“ als Anwendung lauffähig ist. Wie in Abbildung 4.1 zu erkennen zeichnet sich die Netztopologie grundlegend durch zwei Netze aus. Das erste Netz ist das Netz des Endnutzers. Hier wird die Annahme getroffen, dass dieses in Bezug auf den direkten Zugriff auf „MaBCloud“ aus Windows-Clients (C001) besteht, bei denen es sich in der Regel um die firmeneigenen und einheitlichen Windows-Laptops handelt. Das zweite Netz ist das interne Netz des Cloud-Anbieters. Die Verbindung zwischen dem Client und dem Cloud-Endpunkt (K002), im Netz des Cloud-Anbieters, verwendet das öffentliche Internet zur Kommunikation. Der Cloud-Enpunkt besteht in der modellierten Cloud-Architektur dabei aus einer Firewall-Komponente (A004), die durch einen

[1] zu Vereinfachung werden auch Abhängigkeiten wie ein entsprechender Webserver, das Java Runtime Environment oder das Betriebssystem inkludiert.
[2] siehe Fußnote 1.
[3] siehe Fußnote 1.
[4] Wird von einem externen Anbieter als fremd verwalteter Dienst in Anspruch genommen.
[5] Wird von dem Cloud-Diensteanbieter als fremd verwalteter Dienst in Anspruch genommen.

Firewall-as-a-Service Dienst eines externen Anbieters realisiert wird. Hier wird insbesondere der eingehende Netzverkehr mithilfe von konfigurierten Regeln überwacht und soll so gesichert werden.

Da „MaBCloud“ in einer 3-Schichten-Architektur konzeptioniert wurde, wurde eine durch das BSI empfohlene Segmentierung der virtuellen Maschinen in verschiedenen Sicherheitszonen angewandt [14]. Aus technischer Perspektive sollen so möglichst nur homogene Anwendung einer Schicht auf derselben physischen Infrastruktur beziehungsweise demselben Virtualisierungsserver (S001) laufen. Auch in der Cloud soll so ein Vorgehen bestmöglich umgesetzt werden.

Sollte der eingehende Netzverkehr die virtuelle Firewall (A004) passieren, so wird dieser über eine erste Instanz des virtuellen Loadbalancers (A006) an eine jeweilige virtuelle Maschine mit einer MaBCloud Frontend Anwendung (A001) weitergeleitet. Diese stellen bei Bedarf weitere Anfragen über eine zweite Instanz des virtuellen Loadbalancers (A006) an virtuelle Maschinen mit dem MaBCloud Backend (A002), sowie dieses entsprechend über eine dritte Instanz an die virtuellen Maschinen mit der objektrelationalen Datenbankanwendung (A003). Die Kommunikation zwischen den virtuellen Maschinen geschieht über eine Verbindung zwischen Cloud-Netzkomponenten (K001).

Im Zuge der durchgeführten Strukturanalyse wurden einige Einschränkungen aufgrund des ansonsten zu hohen Umfanges für diese Arbeit durchgeführt. So hätten innerhalb der Strukturanalyse für die Anwendungen jegliche zur Plattform dazugehörige Dienste wie zum Beispiel ein Webserver oder das zugrundeliegende Betriebssystem als eigenständige Anwendung modelliert werden müssen. Jedoch hat auch hier eine Komplexitätsreduktion durch eine Gruppenbildung stattgefunden, sodass diese in die entsprechenden Anwendungen der jeweiligen Schicht von „MaBCloud“ inkludiert sind.

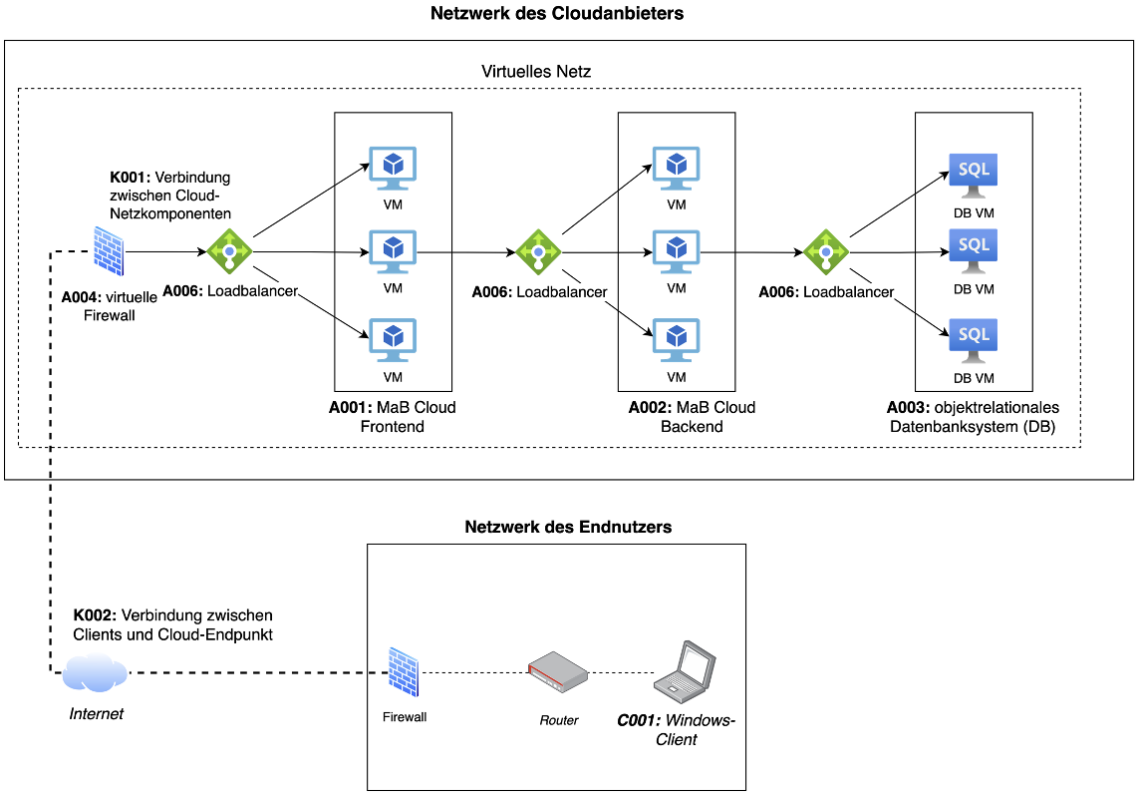

Abbildung 4.1: Netzplan der minimalen Cloud-Architektur mit entsprechenden Komponenten, für die eine Bedrohungsanalyse durchgeführt wird.

4.3 Schutzbedarfsfeststellung

Die vollständige Schutzbedarfsfeststellung für das vorliegende Anwendungsszenario kann im Anhang A.1 gefunden werden. Um eine vollständige Transparenz der Arbeitsergebnisse zu schaffen, sollten allerdings vorher einige berücksichtigte Prinzipien erwähnt und Besonderheiten des IT-Grundschutzes diesbezüglich offen gelegt werden. Bei der Schutzbedarfsfeststellung im Kontext von Systemen mit virtualisierten Elementen spielen die Konzepte des Maximumprinzips und des Verteilungsprinzips eine besondere Rolle. Das Maximumprinzip definiert hier, dass sich der Schutzbedarf eines Objektes aus der Summe von möglichen Schäden relevanter Teilobjekte ergibt [14] und ist im Rahmen des vorliegenden Systems besonders für die Kommunikationsverbindungen relevant. Das liegt darin begründet, dass diese verschiedenste Objekte verbinden und diese deshalb als ein Teilobjekt angesehen werden können. Ein zweites, für das vorliegende Anwendungsszenario

relevantes Prinzip ist das Verteilungsprinzip. Dieses greift, wenn für ein Objekt derartige Redundanzen existieren, dass ein identisch gespiegeltes Ersatzsystem auf einem weiteren physischen Server kurzfristig als Ersatz gestartet werden kann [14]. Dies gilt auch im vorliegenden System für jedes virtualisierte Objekt wie zum Beispiel jegliche virtuelle Maschinen im Zusammenhang mit „MaBCloud“ oder für die bereitgestellten Dienste des Cloud-Anbieters, wie zum Beispiel die virtuellen Loadbalancer.

Wie bereits erwähnt werden im Zuge der Standard-Absicherung keine Komponenten des Systems weiter betrachtet, die mit den aktuellen Sicherheitsmaßnahmen bereits einen normalen Schutzbedarf aufweisen. Diese gelten damit als bereits ausreichend gesichert [14]. Konkret gilt dies für drei Komponenten, die im Zuge der Strukturanalyse mit erarbeitet wurden. Unter anderem werden so die Windows-Clients (C001) im weiteren Verlauf nicht mehr berücksichtigt, unter der Annahme, dass auf den Arbeitsrechnern keine sensiblen Informationen gespeichert werden und ein Ausfall von bis zu 4 Stunden in der Regel tolerierbar ist. Des Weiteren werden ebenfalls die virtuellen Loadbalancer (A006) nicht weiter berücksichtigt unter der Annahme, dass diese zwar mit konfigurierten Regeln für die Lastverteilung auf verschiedene Gruppen von virtuellen Maschinen verknüpft sind, aber ebenfalls keine besonders sensiblen Informationen enthalten. Außerdem greift hier bezüglich der Verfügbarkeit das Verteilungsprinzip. Als drittes Objekt wird die virtuelle Firewall (A004) nicht weitere betrachtet unter der Annahme, dass die Konfigurationseigenschaften zwar vertrauliche Daten darstellen, aber der größte Teil an entsprechenden Zuständigkeiten bezüglich der Sicherheit an den Diensteanbieter der Firewall abgegeben werden. Zudem stellt dieser bezüglich der Integrität in der Regel ein ausreichendes Logging zur Verfügung und eine ausreichende Ausfallsicherheit sollte ebenfalls durch den Provider sichergestellt werden.

Auch der Virtualisierungsserver (S001) wird nicht weiter gesondert betrachtet, da sich hier der Schutzbedarf der darauf betriebenen Anwendungen vererbt. Falls mehrere Anwendungen auf diesem betrieben werden, ist die Anwendung mit dem höchsten Schutzbedarf in der Vererbung zu berücksichtigen. Dadurch wird es auch durch das BSI als ausreichend beschrieben, lediglich die Anwendungen weiter zu berücksichtigen [14].

4.4 Ermittlung von Bedrohungen

Nach dem sowohl die Strukturanalyse, als auch die Schutzbedarfsfeststellung für das vorliegende Anwendungsszenario abgeschlossen wurde, folgt nun die Ermittlung von re-

levanten Bedrohungen, Angriffe und Schwachstellen. Diese werden jeweils den betroffenen Zielobjekten innerhalb des Informationsverbundes zugeordnet und beeinträchtige Grundwerte der Informationssicherheit konkretisiert. Im Anschluss erfolgt jeweils eine Erläuterung der Relevanz für das vorliegende Szenario. Insgesamt wurde dabei versucht, thematisierte Bedrohungen in sieben angemessene Kategorien zu gliedern, um so eine klare Struktur zu verfolgen.

4.4.1 Organisatorische Bedrohungen

Organisatorische Bedrohungen beziehen sich auf die größte Einheit eines Unternehmens: das Unternehmen an sich. Im Zuge dessen werden Schwachstellen und Bedrohungen thematisiert, die aus Problemen in den Strukturen sowie Geschäftsprozessen des Unternehmens entstehen. Beispiele hierfür können entweder die mangelnde Durchführung von Schulungen bezüglich eines richtigen Umganges mit den neuen Konzepten des Cloud-Computings sein oder ein unzureichendes Notfallmanagement bis hin zu einer fehlenden Exit-Strategie.

Nr.	**Bedrohung**	**identifiziertes System**	**beinträchtigte Grundwerte**
1	Unzureichendes Notfallmanagement für die Cloud	Informationsverbund / übergeordneter Aspekt	A, C, I
2	Fehlende Exit-Strategie	Informationsverbund / übergeordneter Aspekt	A, C, I
3	Fehlende Schulungen im Umgang mit Sicherheitsbedrohungen in der Cloud	Informationsverbund / übergeordneter Aspekt	A, C, I

Tabelle 4.1: Übersicht der organisatorischen Bedrohungen

B1: Unzureichendes Notfallmanagement für die Cloud

Eine erste direkte Bedrohung für den initialen Betrieb des Systems in einer Cloud-Umgebung kann ein unzureichendes Notfallmanagement sein. Definiert wird ein Notfallmanagement dabei als ein Managementprozess, der lebensgefährdende Risiken für eine Institution frühzeitig erkennen und geeignete Maßnahmen etablieren soll. So enthält ein Notfallmanagement sowohl Alarmierungsprozesse, Sofortmaßnahmen und Wiederanlaufs-

beziehungsweise Wiederherstellungsmaßnahmen nach der Wahrnehmung eines sicherheitskritischen Vorfalls als auch die Planung und den Betrieb von Vorsorgemaßnahmen [17].

Existiert nun solch ein Notfallmanagement innerhalb eines Unternehmens gar nicht, so entstehen Sicherheitslücken beispielsweise dadurch, dass Mitarbeiter schlichtweg nicht wissen, wie bei einem sicherheitskritischen Vorfall zu reagieren ist. Als direkte Folge kann mehr Zeit verloren gehen, in der -je nach Szenario- gegebenenfalls weitere sensible Daten an die Angreifenden abfließen beziehungsweise bösartig verschlüsselt werden können. In anderen Szenarien könnte das System schlichtweg länger nicht mehr erreichbar sein, bevor es zu einer Wiederherstellung der Verfügbarkeit kommt. Dadurch könnten alle drei Grundwerte der IT-Sicherheit direkt negativ beeinträchtigt werden. Durch das BSI wird ein unzureichendes Notfallmanagement als massive Gefahr eingestuft [12].

Aber auch falls ein Notfallmanagement existiert, kann dieses für den Betrieb in einer Cloud gänzlich ungeeignet sein. Dies ergibt sich oftmals aus einem Notfallmanagement, das nicht auf die neuen Konzepte bezüglich der Infrastruktur und neuen Prozesse des Cloud-Computings angepasst wurde. Ein konkreter Grund, weshalb die Anpassung des Notfallmanagements in der Cloud nötig sein kann, ist die fehlende Berücksichtigung des nun geltenden Shared-Responsibility-Modells. Speziell gilt dies, wenn sich ein Sicherheitsvorfall auf Ebene der physischen Infrastruktur ereignet. Bei einer nicht erfolgten Anpassung des Notfallmanagements könnte hier immer noch der Prozess einer Krisenbewältigung angestoßen werden, obwohl die Zuständigkeiten diesbezüglich an den Cloud-Diensteanbieter abgegeben wurden und dieser indessen die Krisenbewältigung im Rahmen des eigenen Notfallmanagements vornehmen muss.

Des Weiteren können viele bisher festgelegte Maßnahmen und Prozesse des Notfallmanagements, insbesondere auf technischer Ebene, mit der neuen Cloud-Umgebung inkompatibel sein. Ein Grund hierfür kann der fehlende Zugriff auf die Infrastruktur der Cloud sein, was damit einhergeht, dass die kontextabhängige Erkennung von Sicherheitsvorfällen nur noch über zugelieferte Events von einer entsprechenden API des Cloud-Anbieters möglich ist. Dafür müssen gegebenenfalls neue Konzepte bezüglich des Loggings, Monitorings, sowie Alertings von sicherheitsrelevanten Vorfällen eingearbeitet werden. Werden solche veränderten technischen Grundlagen im Notfallmanagement nicht berücksichtigt, könnten Alarmierungsprozesse und entsprechende Maßnahmen erst spät greifen, da sicherheitsrelevante Vorfälle gegebenenfalls gar nicht ausreichend als Auslöser des Notfallmanagements erkannt werden.

Eine weitere Schwierigkeit für das angemessene Notfallmanagement in der Cloud liegt darin, dass in der Cloud die meisten sicherheitsrelevanten Komponenten als virtualisieren Anwendung bereitgestellt werden und nicht mehr als Hardwarekomponente wie in vielen On-Premises Systemen [95]. Ein Beispiel ist häufig in den Firewalls zu finden, die dem Benutzer in der Cloud lediglich als virtualisierte Komponente zur Verfügung stehen und nicht mehr in eigener Verantwortung als Hardwarekomponente in das Gesamtsystem eingebaut werden können. Zudem werden sowohl für jede solcher virtualisierten Komponenten, als auch für jeden vom Cloud-Diensteanbieter zur Verfügung gestellten Dienst, Kosten generiert. Konsumieren also Prozesse beziehungsweise Maßnahmen im Rahmen des Notfallmanagement unnötig viele Ressourcen - so kann dies dauerhaft zu überhöhten finanziellen Kosten für das bezahlende Unternehmen führen und den Betrieb des ganzen Systems in der Cloud gefährden.

B2: fehlende Exit-Strategie

Falls längerfristige Probleme mit einer Cloud bestehen und diese durch die Ausführung eines angemessenen Notfallmanagements nicht ausreichend behandelt werden können, sind in der Regel Exit-Strategien als eine weitere Eskalationsstufe der Problembehandlung vorgesehen. Insgesamt bildet das vorausschauende Ausarbeiten von Exit-Strategien einen essenziellen Baustein auf dem Weg zu einer erfolgreichen Nutzung von Cloud-Computing. Im Kontext von Cloud-Computing stellt eine Exit-Strategie dabei einen Plan dar, der festlegt beziehungsweise organisiert, wie ein Wechsel zu einem anderen Cloud-Anbieter oder die gänzliche Rückkehr zu einem On-Premises System aussehen könnte. Typische Themenblöcke einer solchen Exit-Strategie sind oftmals der Ablauf von Datenmigrationen, die Rekonfiguration von Anwendungen und das Training von Mitarbeitern für die Nutzung eines anderen Systems, sowie Strategien zur Minimierung der Ausfallzeit [111]. Zum Einsatz kommen Exit-Strategien in der Regel, wenn der Einsatz von Cloud-Computing in Verbindung mit einem bestimmten Cloud-Anbieter oder aber grundsätzlich gescheitert ist. Zum Beispiel, wenn sich Anforderungen derart verändert haben, dass diese vom Cloud-Anbieter nicht mehr erfüllt werden können, im Voraus eine grundlegende finanzielle Verkalkulation bezüglich einer Cloud-Nutzung stattgefunden hat oder der Cloud-Anbieter seine Dienste spontan gänzlich einstellt. Ein historisches Beispiel zeigt, dass solche Szenarien möglich sind. So hat der ehemalige Cloud-Speicher Anbieter *Nirvanix*, der eng mit den Cloud-Diensten von IBM kooperierte und Ende 2013 lediglich circa 14 Tage im Voraus die Schließung der eigenen Dienste bekannt gegeben hat [93]. Aufgrund solcher möglichen Szenarien hat auch die *European Banking Authority (EBA)* eine Exit-Strategie als einen essenziellen Baustein angesehen und 2019 festgelegt, dass

Finanzinstitution eine solche ausarbeiten müssen, sobald wichtige oder sogar kritische Funktionen in die Cloud ausgelagert werden [66].

Wird also im Vorhinein für die Nutzung von Cloud-Computing keine Exit-Strategie mit ausgearbeitet, so können einerseits behördliche Regularien möglicherweise nicht erfüllt werden. Dies hätte gegebenenfalls juristischen Folgen, beispielsweise in Form von bis zu 10 Millionen Euro Bußgeld [16]. Andererseits könnte es durch eine fehlende Strategie nach dem Exit zu einem desolaten Übergangszustand kommen, mit unklaren Zuständigkeiten, falsch konfigurierten Anwendungen und mit für die neue Infrastruktur inkompatiblen beziehungsweise verlorenen Datenbeständen. Mögliche Folgen dadurch, wären hohe finanzielle Verluste für das Unternehmen und möglicherweise hohen Ausfallzeiten des Systems, die besonders in einer Infrastruktur-kritischen Branche nicht tolerierbar sind. Außerdem kommt es in solchen Szenarien nicht selten zu einem Reputationsverlust gegenüber Kunden beziehungsweise anderen externen Akteuren.

Allerdings können solche Szenarien nicht nur durch eine gänzlich fehlende Exit-Strategie entstehen, sondern ebenfalls durch das unzureichende Testen von bestehenden Exit-Strategien, sodass eine Nichtbenutzbarkeit durch fehlende Aktualität nicht auffällt. Findet zudem kein Einbezug einer Exit-Strategie in die frühen und grundlegenden Planungen der Systemarchitektur sowie Auswahl an Technologien statt, so könnte ebenfalls ähnliche Folgen auftreten. Insbesondere wenn Cloud-Anbieter spezifische Komponenten in die Systemarchitektur integriert werden oder Datenspeicherformate genutzt werden, die ebenfalls nur in Cloud-Umgebungen eines bestimmten Providers genutzt werden können.

B3: Fehlende Schulungen im Umgang mit Sicherheitsbedrohungen in der Cloud

Aber nicht nur bei Szenarien nach sicherheitskritischen Vorfällen, wie im Rahmen des Notfallmanagements und der Exit-Strategie, trägt eine unzureichende Streuung von Fachkenntnissen zu einer Bedrohung bei. Auch schon während des Betriebes einer Cloud im Rahmen des Alltagsgeschäftes können solche unzureichenden Fachkenntnisse zu einer Gefahr werden. Konkret gilt dies, falls der mit dem System von „MaBCloud“ interagierende Personenkreis für Sicherheitsbedrohungen in der Cloud nicht ausreichend geschult und sensibilisiert wird. So kann es einerseits passieren, dass durch fehlende Fachkenntnisse sicherheitsrelevante Ereignisse als ein solches nicht angemessen von Mitarbeitenden identifizierte werden können oder neue Sicherheitserweiterungen durch Unwissenheit nicht genutzt werden. Außerdem können Aufgaben insbesondere in Verbindung mit neuen

Konfigurationsmechanismen in der Cloud-Umgebung von „MaBCloud“ durch fehlende Fachkenntnisse oftmals nicht in derart angemessen erfüllt werden, dass daraus ein sicheres Ergebnis resultiert [12]. Das kann sich dementsprechend negativ auf das Schutzniveau des gesamten Informationsverbundes auswirken, sowie Chancen für sicherheitskritische Vorfälle erhöhen, die alle drei Schutzziele verletzen können. Ein konkretes Beispiel kann hier eine sichere Konfiguration von Nutzerberechtigungen in der Cloud-Umgebung liefern, da diese oftmals anbieterabhängige Fachkenntnisse erfordert. Weitere Probleme treten auf, wenn die Perspektive auf die MakeABank GmbH als ein dynamisch-wachsendes Unternehmen dazu gezogen wird. Situationen wie Kündigungen und Personalmangel sind gängige Szenarien, sodass Mitarbeitende in Situationen geraten können, in denen diese plötzlich andere oder zusätzliche Aufgaben innerhalb des Systems übernehmen müssen. Wird lediglich eine zu begrenzte Auswahl an mitarbeitenden Personen ausreichend geschult, können durch solche Situationen Wissenslücken entstehen, die ebenfalls zu den angeführten Problemen führen [12].

Des Weiteren besteht durch die fehlende Schulung eine höhere Gefahr für einen sorglosen Umgang mit sicherheitsrelevanten Informationen. Bereits alltägliche Situationen bieten das Potenzial, zu einem Sicherheitsvorfall in der Cloud zu führen. Beispielsweise könnte bereits der sorglose Umgang in einer solchen Situation dazu führen, dass unter anderem während einer Zugfahrt die Zugangsdaten für einen Administrationsbenutzer der Cloud-Konsole eingegeben und durch Dritte mitgelesen werden oder ausgedruckte sicherheitsrelevante Informationen durch Unachtsamkeit an einem Drucker liegen bleiben [12]. Im schlimmsten Falle könnten diese durch unberechtigte Personen mit Fachkenntnissen genutzt werden, um mittels der Cloud-Konsole grundlegende Änderungen an allen Komponenten in der Cloud-Umgebung durchführen.

4.4.2 Bedrohungen durch mangelhaftes Anforderungsmanagement

Falls eine Institution sich dazu entscheidet den Dienst eines Cloud-Anbieters zu nutzen, sind in der Regel viele Erwartungen daran geknüpft. So erhoffen sich mitarbeitende Personen oftmals einen höheren Funktions- und Leistungsumfang bei geringeren Kosten. Diesbezüglich müssen jedoch im vorhinhein diverse Anforderungen umgesetzt beziehungsweise auf eine bereits erfolgte Umsetzung überprüft werden. Ansonsten kann es passieren, dass eine Cloud nicht den gewünschten Mehrwert, zum Beispiel in Bezug auf eine bessere Verfügbarkeit der Anwendung liefert [14].

Nr.	Bedrohung	identifiziertes System	beinträchtigte Grundwerte
4	Unzureichende Partition von Entwicklungsumgebungen	Informationsverbund / übergeordneter Aspekt	A,C,I
5	Unzureichende Partition der Anwendung	A001: MaBCloud Frontend, A002: MaBCloud Backend, A003: objektrelationales Datenbanksystem	A

Tabelle 4.2: Übersicht der Bedrohungen durch mangelhaftes Anforderungsmanagement

B4: Unzureichende Partition von Entwicklungsumgebungen

Eine erste Cloud-spezifische Bedrohung im Rahmen des mangelhaften Anforderungsmanagements stellt eine unzureichende Partitionierung der Entwicklungsumgebungen dar, die für die Entwicklung von „MaBCloud“ in der Cloud genutzt werden sollen. Dabei spielen Entwicklungsumgebungen im Rahmen der Softwareentwicklung eine zentrale Rolle. In diesem Kontext ist eine Entwicklungsumgebung ein System, das ein vollständiges Set an Hardware und Software zur Verfügung stellt, also eine lauffähige Plattform, damit eine spezifische Anwendung auf diesem System entwickelt werden kann [34]. In vielen Unternehmen gibt es häufig ein Mindestkontingent an verschiedene Umgebungen, für das produktive System (Prod), das System zum Testen beziehungsweise zur Abnahme von neuen Funktionen durch Kunden (Test) und das System zum Entwickeln (Dev). Der oft erkannte Vorteil dabei ist, dass die Nutzung von jeweils isolierten Entwicklungsumgebungen ein Testen von neuen Funktionen ermöglicht, ohne das Produktivsystem zu involvieren. Dadurch existiert auf dem produktiven System immer ein funktionsfähiger, getesteter und idealerweise sicherer Stand der Anwendung, sodass fehlerhafte Funktionen und eine einhergehende Beeinträchtigung der Verfügbarkeit im Betrieb minimiert werden können.

In der Realität zeigen sich häufig grundlegende Unterschiede in der Organisation von den verschiedenen Entwicklungsumgebungen. Während empfohlen wird innerhalb der Entwicklungsumgebung des Produktivsystems den Kreis der Benutzer möglichst einzuschränken [68], jegliche Änderungen nur noch per automatisierte DevOps-Pipelines zu installieren [51] und dementsprechend tendenziell nur noch wenige menschlich geführte Benutzerkonten existieren, kann dies auf den anderen Entwicklungsumgebungen anders aussehen. Im Kontrast dazu existieren hier oftmals nicht nur eine vergleichsmäßig hohe

Anzahl an Benutzern, sondern auch Authentifizierungsrichtlinien werden für diese Umgebungen oftmals ebenfalls weniger strikt definiert beziehungsweise stärker durchgesetzt als auf dem Produktivsystem. Dies basiert häufig auf der Annahme, dass die Isolation der Entwicklungsumgebung bereits so stark sei, sodass ein Sicherheitsvorfall keine Auswirkungen auf die Live-Daten und die Verfügbarkeit des produktiven Systems haben kann.

Allerdings hat sich historisch gezeigt, dass solche offenen Dev und Test Entwicklungsumgebung oftmals bei Angriffen als Einstiegspunkt in ein System dienen [87]. Herrscht also eine schwache Authentifizierungspolitik in Kombination mit einer unzureichenden Partition der Entwicklungsumgebungen, so senkt dies das Schutzniveau des Systems. Eine unzureichende Partition in dem Kontext kann zum Beispiel das Verwenden einer einzigen Cloud-Umgebung für alle Entwicklungsumgebungen darstellen. Sowohl Benutzer für die Dev-Entwicklungsumgebung, als auch Benutzer für das produktive System wären dann in dieser einen Umgebung angelegt und haben Zugriff auf dieselbe Cloud-Umgebung. Dadurch würde ebenfalls die Konfigurationen im Rahmen der Benutzerverwaltung bezüglich Rechte und Rollen deutlich komplexer gestaltet werden, sodass Fehler hier einem unberechtigten Benutzer in schlimmsten Falle Zugriff auf Ressourcen einer anderen Entwicklungsumgebung gestatten könnten. Dies könnte es angreifenden Personen leichter ermöglichen, einen schlecht gesicherter Benutzer zu übernehmen, der eigentlich nur für das Dev- oder Test-System angelegt wurde, aber durch einen Konfigurationsfehler Zugriff auf Ressourcen einer anderen Umgebung erhalten hat. So können diese im schlimmsten Falle bis in die Entwicklungsumgebung des produktiven Systems eindringen und produktive Daten stehlen beziehungsweise die Verfügbarkeit beeinträchtigen. Eine starke Isolation zwischen den Umgebungen fällt so also schwer und entspricht wie beschrieben nicht den Best Practises der Cloud-Entwicklung [36]. Auch andere Angriffstechniken haben es so einfacher, die Isolation zwischen den Umgebungen zu durchbrechen und können so potenziell den gesamten Informationsverbund bezüglich aller Schutzziele der Informationssicherheit beeinträchtigen, da verschiedenste Angriffsszenarien möglich sind.

B5: Unzureichende Partition der Anwendung

Doch nicht nur die unzureichende Partitionierung von Entwicklungsumgebungen stellt eine Bedrohungen für das System dar. Auch die unzureichende Partitionierung der selbst entwickelten Anwendungen in einer Entwicklungsumgebung kann eine Bedrohung für das System darstellen. Das liegt vor allem an den festen technischen Limitierungen, die gängige Cloud-Anbieter pro Cloud-Umgebung festgelegt haben. Beispielsweise ist bei

Microsoft im Rahmen von einem IaaS-Cloud Abonnement des Cloud-Produktes Azure[6] nur die gleichzeitige Verbindung von 1982 Benutzern des verwalteten Datenbankdienstes erlaubt [65]. Durch eines der unternehmerischen Ziele längerfristig möglichst viele Zuständigkeiten an externe Diensteanbieter auszulagern, kann die Verwendung eines ähnlichen Cloud-Datenbankdienstes kann auch für das „MaBCloud“ System zukünftig nicht gänzlich ausgeschlossen werden. Weitere exemplarische Limitierungen gelten in der Regel ebenfalls für Leistungen, wie zum Beispiel für allgemeine Speicherkapazitäten, für die Anzahl der Regeln zur Zugriffsbeschränkung des Systems zum Beispiel durch die eine Firewall oder für die maximale Anzahl an Instanzen an virtuellen Maschinen, die für die Skalierung einer Anwendung genutzt werden können.

Aus diesem Umstand entsteht nun eine konkrete Bedrohung, wenn solche Limitierung eines Cloud-Anbieters nicht als Anforderungen innerhalb der umgesetzten Anwendungsarchitektur berücksichtigt wurden. Denn während sich im Rahmen eines selbst gehosteten On-Premises System gegebenenfalls die Hardware ausbauen lässt um solche Limitierungen zu erhöhen, ist dies im Rahmen des Cloud-Computings durch den fehlenden Zugriff auf die Infrastruktur unmöglich. So müssen andere Strategien umgesetzt werden, wie zum Beispiel ein Zuschnitt in Microservices oder eine andersweitig geeignete Partition der Anwendung auf verschiedene Cloud-Umgebungen. Geschieht dies nicht und werden trotz der Limitierungen große monolithische Anwendungen in die Cloud migriert, kann diese Anwendung im schlimmsten Falle nicht mehr ausreichend skaliert werden, da der Anbieter keine weiteren Ressourcen zur Verfügung stellt. Dadurch können Anfragen nicht mehr ausreichend beantwortet werden und es kann zu Einschränkungen in der Verfügbarkeit des Systems kommen. Historische Beispiele für ein solches Szenario boten komplexe Datenverarbeitungsanwendungen für Datenanalysen, wie zum Beispiel Apache Spark[7] [109]. Unter der Annahme, dass diese Limitierungen bereits in den Anforderungen von verwendeten Cloud-Diensten berücksichtigt wurden, betrifft dies primär die Verfügbarkeit von selbst entwickelten Anwendungen. Innerhalb des vorliegenden Szenarios wäre dies also das „MaBCloud“ Frontend (A001) und Backend (A002). Allerdings ist auch das objektrelationale Datenbanksystem (A003), als selbstverwaltete Anwendung, hiervon betroffen.

Ein weiterer Seiteneffekt bezüglich der unzureichenden Partitionierung kann außerdem sein, dass Teile einer Anwendung mit skaliert werden, die eigentlich nicht mit skaliert

[6] https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-is-azure/azure-iaas/
[7] https://spark.apache.org/

werden müssten. Dies gilt beispielsweise für Anwendungen, die übermäßig viel Geschäftslogik in das Frontend integrieren, die jedoch nicht für die Grundfunktionalität nötig ist. Dadurch werden in der Cloud zusätzlich unnötige Ressourcen in Anspruch genommen, sodass im Rahmen der nutzungsbasierten Abrechnung teils deutliche Mehrkosten für den Rechnungsträger der Cloud-Umgebung entstehen können. Eine ungeeignete Partitionierung der Anwendung im Rahmen der Architekturmodellierung kann also bereits verschiedene Bedrohungen und Probleme mit sich bringen und muss anhand von den Limits des jeweiligen Cloud-Anbieters aureichend geplant beziehungsweise umgesetzt werden.

4.4.3 Bedrohungen durch das Outsourcen von Daten

Die folgenden Bedrohungen beziehen sich auf das dem Cloud-Computing zugrundeliegenden Konzept des Data Outsourcings. Data Outsourcing bezeichnet eine immer häufiger angewendeten Vorgehensweise im Zuge welcher der Eigentümer von Daten Zuständigkeiten für die Verwaltung an externe Dienstleister abgibt [20]. Im zugrunde liegenden Kontext geben die Kunden der MakeABank GmbH als Eigentümer die Zuständigkeiten bezüglich des Datenmanagements zum großen Teil an die Infrastrukturen des Cloud-Anbieters ab. Daraus entstehen neue Probleme und Sicherheitsherausforderungen für die jeweiligen Cloud-Systeme, welche im Folgenden adressiert werden.

Nr.	**Bedrohung**	**identifiziertes System**	**beinträchtigte Grundwerte**
6	Cloud Outages	Informationsverbund / übergeordneter Aspekt	A
7	Inkompatible Monitoring-Lösungen	Informationsverbund / übergeordneter Aspekt	I
8	Vendor lock-in	Informationsverbund / übergeordneter Aspekt	C, I
9	Unzureichendes Datenamangement	Informationsverbund / übergeordneter Aspekt	C

Tabelle 4.3: Übersicht der Bedrohungen durch das Outsourcen von Daten

B6: Cloud Outages

Eine erste Bedrohung im Zusammenhang mit dem Outsourcing von Daten sind Cloud Outages beziehungsweise Ausfälle von externen Cloud-Diensten. Genauer gesagt, wird als Cloud Outage eine Zeitspanne bezeichnet, in der die Dienste eines Cloud-Anbieters gar nicht oder nicht vollständig verfügbar sind [80]. Dementsprechend könnte ein solches Szenario einerseits eine vollständige Nichterreichbarkeit des gesamten Systems von „MaBCloud“ zur Folge haben. Andererseits können Cloud-Dienste ein Fehlverhalten aufweisen durch welches die unvollständige Verfügbarkeit der Funktionalität, zum Beispiel bei Abhängigkeiten zu anderen Diensten, die gänzlich nicht erreichbar sind. Selbst mit Cloud-Diensteanbieter geschlossene Service-Level-Agreements, die oftmals eine Verfügbarkeit der Dienste von 99,9 % garantieren sollen, schützen in der Regel nicht vor solchen Szenarien [80].

Im Prinzip unterscheidet sich der Ausfall von einem On-Premises Systems im Vergleich zu einer Cloud-Umgebung in Bezug auf die Verfügbarkeit nicht grundlegend. Das Cloud-Umfeld beinhaltet allerdings einige zusätzliche Schwierigkeiten und zu berücksichtigende Aspekte. So erhält einerseits der jeweilige Cloud-Nutzer bei einem Ausfall in der Regel keine Sichtbarkeit über den Fehler beziehungsweise den Grund für den aktuellen Ausfall. Andererseits greift zur Wiederherstellung der Funktionalität in solchen Fällen das Notfallmanagement des Cloud-Anbieters. Dadurch liegt der Prozess außerhalb der eigenen Zuständigkeiten, es kann also keinen Einfluss auf den Wiederherstellungsprozess genommen werden. Damit bleibt sowohl den Nutzern von „MaBCloud“ als auch den Rechnuntsträgern der Cloud-Umgebung oft unklar, wann die betroffenen Dienste wieder verfügbar sind beziehungsweise ordnungsgemäß funktionieren [110]. Es existiert bezüglich der Wiederherstellung und Verfügbarkeit des Systems also eine vollständige Abhängigkeit zum Cloud-Anbieter beziehungsweise Anbieter der entsprechenden Cloud-Dienste. Außerdem kann es bei unzureichender Trennung von Stakeholdern durch den Cloud-Diensteanbieter auf der Cloud-Infrastruktur dazu führen, dass bei erfolgreichen Angriffen auf Systeme, die nicht der MakeABank GmbH zuzuordnen sind, auch die MakeABank GmbH ihre zugesicherten Dienstleistungen nicht mehr in den Anspruch nehmen kann [12].

Das ein solches Szenario die Verfügbarkeit von „MaBCloud“ auch bei größeren Providern bedroht, lässt sich mit Zahlen statistisch belegen. So haben über 60 % der Firmen die eine Public-Cloud nutzen Verluste durch Cloud-Outages zu vermelden [110]. So war beispielsweise der Amazon EC2 Service[8] im April 2011 für vier Tage nicht erreichbar [78].

[8] https://aws.amazon.com/de/ec2/

Ein anderes Beispiel ist ein Google Cloud[9] Outage im November 2021, während dem für über 2 Stunden viele Dienste nur noch mit dem HTTP-Statuscode 404 erreichbar waren [110].

B7: Inkompatible Monitoring-Lösungen

Eine weitere Bedrohung für den Betrieb von „MaBCloud“ in der Cloud, die bereits erwähnt wurde, sind inkompatible Monitoring-Lösungen. Unter Bezugnahme des Kontextes, dass bisher ein On-Premises System mit einer entsprechenden Monitoring-Lösung verwendet wurde, müssen in der Cloud weitaus komplexere Anforderungen berücksichtigt werden, die viele Monitoring-Lösungen nicht angemessen umsetzen können.

Dabei stellt das Monitoring in der Cloud eine Schlüsselkomponente für die Verwaltung von Hardware- und Softwarekomponenten dar. Durch ein für die Cloud angemessenes Monitoring-System kann einerseits die Auslastungen der Systeme überwacht werden und so stetige Optimierungen vorgenommen werden. Andererseits lassen sich damit ebenfalls Mechanismen zur Prävention von Sicherheitsvorfallen umsetzen, die zusätzlich bei der Herstellung eines Systems nach einem Sicherheitsvorfall unterstützen können. Eine angemessene Monitoring-Lösung für die Cloud zeichnet sich durch einen hohen Grad an Umsetzung von Eigenschaft wie Skalierbarkeit, Aktualität, Elastizität, Anpassungsfähigkeit, Autonomie, Erweiterbarkeit, Widerstandsfähigkeit beziehungsweise Verfügbarkeit und Präzision beim Bereitstellen der Daten aus [1]. Erfüllt die bisher eingesetzte Monitoring-Lösung diese Kriterien nicht in einem hohen Umfang, können daraus verschiedene Bedrohungen für den Betrieb von „MaBCloud“ entstehen. Ein Beispiel dafür kann die Eigenschaft der Aktualität einer Monitoring-Lösung in der Cloud sein. Da es sich bei einer Cloud-Umgebung um ein verteiltes System handeln, in dem die virtuellen Maschinen physisch außergewöhnlich weit entfernt sein können, kann es beim Einsatz von ungeeigneten Lösungen dazu kommen, dass die vergangene Zeit zwischen dem tatsächlichen Auftreten eines sicherheitskritischen Events und der Benachrichtigung an den Nutzer so hoch sein kann, dass eine sofortige Reaktion verhindert wird und Schäden anwachsen können. Eine weitere konkrete Cloud-spezifische Bedrohung entsteht, sobald die bisher verwendete Lösung die Elastizität des Cloud-Computings nicht berücksichtigt. Da in der Cloud häufiger und eine höhere Anzahl an virtuelle Maschinen zur Skalierung hinzugefügt, abgeschaltet oder getauscht werden ohne dass ein konkreter Fehlerfall besteht, muss eine Monitoring-Lösung diese Flexibilität ebenfalls berücksichtigen. Das schnelle ein- und ausklinken von einer vergleichsweise hohen Anzahl an virtuellen Maschinen an

[9] https://cloud.google.com/

die Monitoring-Prozedur muss unkompliziert ermöglicht werden. Diese Eigenschaft muss von Monitoring-Lösung für ein On-Premises System derart ausgeprägt nicht umgesetzt werden und so ist die Gefahr hoch, dass vorher genutzte Lösungen auch bezüglich dieses Aspektes inkompatibel sein können. So kann eine solche inkompatible Lösung keine dynamischen Veränderungen des Kontingenz der zu überwachenden Ressourcen in der Cloud-Umgebung verarbeiten und neu erstellte Ressourcen werden nicht überwacht oder das dynamische Entfernen von Ressourcen führt zu einem fehlerhaften Monitoring [1].

B8: Vendor lock-in

Das Bedrohungspotenzial vom Vendor lock-in steigt mit der Komplexität und der Größe des Systems von „MaBCloud“. Vendor lock-ins bezeichnen dabei eine Situation in der ein Kunde abhängig von einem Diensteanbieter geworden ist und der Wechsel zu anderen Anbietern ohne einen hohen monetären Aufwand, rechtlichen Problemen oder technischen Schwierigkeiten nicht möglich ist. Der Grund hierfür sind die grundlegenden semantischen Unterschiede der jeweiligen APIs der Cloud-Diensteanbieter, die einen Umzug von Anwendungen und Daten sehr komplex gestalten können [83].

Daraus lassen sich vier konkrete Teilbedrohungen für die MakeABank GmbH und den Betrieb von „MaBCloud“ ableiten. Grundlegend kann die Servicequalität des Cloud-Diensteanbieters abnehmen oder das Produktangebot könnte sich so drastisch ändern, dass es nicht mehr den Anforderungen der MakeABank GmbH entspricht. Zudem könnten massive Preiserhöhungen für die Cloud-Umgebung stattfinden oder im schlimmsten Falle könnte die Geschäftstätigkeit eines Anbieters eingestellt werden [22]. Ein weiterer problematischer Aspekt sind hier die hohen Anforderungen an den Datenschutz, bedingt durch den Betrieb innerhalb des stark regulierten Banksektors. Durch die oft international-agierenden Cloud-Diensteanbieter kann es passieren, dass durch die stark variierenden nationalen Regularien bezüglich des Datenschutzes die Anforderungen nicht mehr erfüllt werden und die Kunden der MakeABank GmbH hohen juristischen Folgen als primär-verantwortliche Institution ausgesetzt werden [12]. Das stellt sowohl eine direkte Bedrohung für den Betrieb beziehungsweise Verfügbarkeit des gesamten Systems dar, als auch für die Integrität und Vertraulichkeit von Daten, falls Datenschutz- oder ähnliche Anforderungen bezüglich der Datensicherheit nicht mehr erfüllt werden und kein sofortiger Wechsel des Anbieters stattfinden kann.

In jedem der genannten Szenarien wäre ein schneller Wechsel des Anbieters für die MakeABank GmbH durch ein Vendor lock-in nicht möglich. So stellt dies dementsprechend

eine Bedrohung für den Betrieb der gesamten Cloud-Umgebung und somit für den gesamten Informationsverbund dar.

B9: Unzureichendes Datenmanagement

Durch das Outsourcing von Daten an den Cloud-Anbieter ist nur ein eingeschränktes Datenmanagement seitens des Cloud-Kundens möglich. Besonders in Bezug auf das vollständige Löschen von sensiblen Daten erhält der Kunde durch den Cloud-Anbieter in der Regel nur ein visuelles Feedback. Allerdings kann der Kunde aber nicht selbst auf technischen Ebene verifizieren, ob die Daten wirklich vollständig vernichtet wurden, da kein direkter Zugang zu physischen Komponenten der Infrastruktur wie zum Beispiel Festplatten besteht. Zudem ist die Infrastruktur eines Cloud-Systems oftmals ein hochkomplexes verteiltes System mit diversen Herausforderungen wie unter anderem dem Multi-Tenancy Konzept, Elastizität, Virtualisierung, Datensicherungen über verschiedene geografische Standorte, sodass eine Überprüfung als auch vollständige Löschung seitens der Cloud-Anbieters keine triviale Aufgabe ist und einen hohen Grad an Fehleranfälligkeit bieten kann. Obwohl eine vollständige Datenlöschung oftmals durch Erwähnungen innerhalb des Service-Level-Agreement garantiert werden soll, kann der Kunde hier also nur dem Cloud-Anbieter vertrauen, dass dieser den Anforderungen einer vollständigen Löschung gerecht wird [86]. Falls der Cloud-Anbieter zwar eine vollständige Datenlöschung verspricht, aber nicht umsetzt kann, so können als Resultat sensible Daten in den Besitz von unberechtigten Drittparteien gelangen. Diesbezüglich existieren bereits Beispiele in denen durch einen Fehler seitens des Cloud-Anbieters, neue Kunden durch Nutzung derselben physischen Infrastruktur Zugriff auf die Daten des vorherigen Kunden hatten, weil der Cloud-Anbieter die Festplatte nicht ordnungsgemäß geleert hat [86]. Auch das BSI beschreibt diesen Fall in Form einer nicht geregelte Datenlöschung nach Vertragsende als eine konkrete Bedrohung um Rahmen der Nutzung von Cloud-Computing [12].

Des Weiteren nutzen Cloud-Diensteanbieter für die Bereitstellung des eigenen Dienstes oft Dienste von Dritten. Werden solche Situationen nicht vertraglich genau geregelt und Abhängigkeiten zwischen dem Cloud-Diensteanbieter und der dritten Partei nicht offengelegt, kann sich dies ebenfalls negativ auf die Informationssicherheit der Institution auswirken [12]. Das liegt daran, dass sensible Daten nun möglicherweise von weiteren Parteien verarbeitet beziehungsweise gespeichert werden und nun auch hier die Umsetzung des Datenmanagements nicht überprüft werden kann.

Eine weitere Bedrohung bezüglich des Datenmanagements kann sein, dass Cloud-Anbieter oft eigene unabhängige Richtlinien bezüglich einer Datenwiederherstellung besitzen und

ausführen. Diese sollen gewährleisten, dass im Rahmen eines Totalausfalls oder Notfalls die Daten schnell wiederhergestellt werden können, um den Kunden die betroffenen Infrastruktur schnellstmöglich wieder bereitstellen zu können. Dazu wird durch den Cloud-Anbieter die Datensicherung von ganzen Rechenzentren vorgenommen. Dadurch ist allerdings gegebenenfalls unklar, wo und in welchem Rahmen sich diesbezüglich durchgeführte Kopien der eigenen Geschäftsdaten beim Cloud-Anbieters befinden und ob diese garantiert ausreichend gesichert sind.

Ein weiterer Aspekt welcher mit den Rechenzentren der Cloud-Anbieter und einem unzureichenden Datenmanagement zusammenhängt, ist die Wartung von Hardware. Diese werden durch Personal der Cloud-Anbieter durchgeführt. Auch Datenträger werden ausgetauscht und es bleibt oft unklar, ob eine solche Wartung einerseits durch vertrauenswürdige Personen durchgeführt und ob andererseits der alte physische Datenträger mit Geschäftsdaten wirklich unwiederherstellbar vernichtet wird.

Ein Datenleck, verursacht durch die angeführten Situationen, würde primär den Grundwert der Vertraulichkeit verletzten. Die Integrität sowie Vertraulichkeit ist weniger betroffen, da es sich bei gelöschten Daten um Daten handelt, die im System nicht mehr genutzt werden und deshalb eine Veränderung beziehungsweise fehlende Verfügbarkeit keine kritischen Auswirkungen hätte.

4.4.4 Bedrohungen durch fehlerhafte Konfigurationen

Konfigurationen spielen in der Cloud eine zentrale Rolle. Da in der Cloud kein Zugriff auf die physische Infrastruktur wie zum Beispiel Server oder Netzwerkleitungen besteht, kann die Systemarchitektur lediglich bezüglicher einer logischen Topologie modelliert werden. Dies geschieht im Kontext des Cloud-Computings über logische Konfiguration und mittels Nutzung entsprechender Schnittstellen des Cloud-Anbieters. Es ist nicht möglich, wie in eigenen Rechenzentren, die Systemarchitektur durch das eigenständige Zuschalten von Hardwarekomponente oder eine Integration in ein bestehendes Netzwerk mittels eines physischen Kabels durchzuführen.

Aber auch in Bezug auf die Performance eines Systems hat das Konzept des Cloud-Computings hinsichtlich der Konfigurationen einen Paradigmenwechsel ausgelöst. Während durch begrenzte Ressourcen bei herkömmlichen On-Premises Systemen eher die Anwendung auf ein Virtualisierungscluster zugeschnitten wurde, wird in der Cloud die Konfiguration für einen Workload zugeschnitten. Dies wird dadurch begründet, dass in

der Cloud beziehungsweise besonders im Rahmen der nutzungsbasierten Abrechnung das Konzept der Elastizität eine Rolle spielt und deshalb scheinbar unendlich Ressourcen zur Verfügung stehen können. Voraussetzungen dabei ist, wie bereits vorhergehend als Bedrohung erläutert, dass die Anwendungsarchitektur die technischen Limits des Cloud-Anbieters pro Umgebung berücksichtigt. Wichtige Konfigurationen diesbezüglich stellen die Anzahl der Prozessorkerne, des zugewiesenen Speichers und der Knoten dar. Falls hier eine schlechte Konfiguration vorliegt kann ein Workload beispielsweise bis zu 20-mal länger benötigen oder das Durchlaufen 10-mal mehr kosten als bei einer optimalen Konfiguration für den Anwendungsfall [39].

Nr.	**Bedrohung**	**identifiziertes System**	**beinträchtigte Grundwerte**
10	Ungeignete Topologie der Systemarchitektur	Informationsverbund / übergeordneter Aspekt	A, C, I
11	Unreichende Konfiguration von Replikation	A001: MaBCloud Frontend, A002: MaBCloud Backend, A003: objektrelationales Datenbanksystem	A
12	Unreichende Backup- und Recoverystrategie	A001: MaBCloud Frontend, A002: MaBCloud Backend, A003: objektrelationales Datenbanksystem	A, C, I
13	Unzureichende Konfiguration von Kontingenten	Informationsverbund / übergeordneter Aspekt	A
14	Unzureichende Konfiguration von Logging	Informationsverbund / übergeordneter Aspekt	A, C, I
15	Unzureichende Konfiguration von Alerting	Informationsverbund / übergeordneter Aspekt	A, C, I

Tabelle 4.4: Übersicht der Bedrohungen durch fehlerhafte Konfigurationen

B10: Ungeeignete Topologie innerhalb der Systemarchitektur

Die Cloud-Umgebung kann aus architektonischer Perspektive als eine verteilte Zusammenstellung angesehen werden, die Cloud-native Dienste enthält beziehungsweise zur Verfügung stellt. Diese Zusammenstellung kann dynamisch verwaltet werden, sodass auf Änderung innerhalb der Anforderungen von Systemen, sowie nötiger Plattform reagiert werden kann. Ein bestimmter Stil der Systemarchitektur in der Cloud mit diversen Grundprinzipien ist allerdings notwendig, um einen sicheren Betrieb einer Anwendung zu ermöglichen [84]. Wie bereits einleitend erwähnt, kann in Bezug auf die Architektur des Gesamtsystems lediglich eine logische Topologie konfiguriert werden, da im Rahmen des Cloud-Computings kein Einfluss auf die Architektur der physischen Infrastruktur des Anbieters ausgeübt werden kann. Nichtdestotrotz ergeben sich auch hier Bedrohungen für den Betrieb von „MaBCloud“ in der Cloud. Da für alle Teilaspekte einer ungeeigneten Netzwerktopologie in der Cloud allerdings auch kein Vollständigkeitsanspruch im Rahmen dieser Arbeit gewährt werden kann, wird ein Auszug an möglichst Cloud-spezifischen Aspekten bezüglich dieser Bedrohung vorgestellt.

Die erste Cloud-spezifische Besonderheit sind System-Netzwerkrouten, die üblicherweise automatisch vom Cloud-Anbieter innerhalb des virtuellen Netzes angelegt werden, damit Anfragen neue virtuelle Maschinen garantiert erreichen können. Administrative Interaktionen mit diesen System-Netzwerkrouten sind häufig stark beschränkt. So können diese beispielsweise im Rahmen der Microsoft Azure Cloud nicht selbst gelöscht oder erstellt werden. Allerdings können diese in einem gewissen Rahmen durch die Konfiguration von eigenen Netzwerkrouten überschrieben werden [73]. Wird dieses Best Practice in der logischen Modellierung eines Cloud-Netzwerkes nicht berücksichtigt, so können virtuelle Maschinen gegebenenfalls gewünschte Barrieren durch konfigurierte Subnetze durchbrechen und sich global über die System-Netzwerkrouten mit beliebigen anderen virtuellen Maschinen verbinden. Unter diesen Umständen gelingt ein starkes Sicherheitskonzept also nur begrenzt und kann in der Netzwerktopologie gegebenenfalls nicht beziehungsweise nur unzureichend umgesetzt werden [63]. Ähnliche Szenarien sind auch bei anderen Cloud-Anbietern wahrscheinlich und beschränken sich nicht nur auf die Microsoft Azure Cloud. Insofern kann sich dies generell negativ auf das allgemeine Schutzniveau und alle Grundwerte der Informationssicherheit auswirken.

Eine zweite Cloud-spezifische Bedrohung, die hier entstehen kann, ist die mangelnde Modellierung von Komponenten zur Lastverteilung an strategisch sinnvollen Positionen im Netzwerk. Insbesondere für Systeme in kritischen Infrastrukturen, wie also im vorliegen-

den Szenario zutreffend, ist eine ständige Verfügbarkeit essenziell. Wie bereits erwähnt, wird in der Cloud die Verfügbarkeit primär durch einen hohen Grad an Fehlertoleranz sichergestellt und nicht durch eine gänzliche Vermeidung von Ausfällen. Werden nun also in der Topologie an strategisch wichtigen Punkten des Netzes kein Loadbalancer oder andere Cloud-Dienste mit einer Funktion für die Lastenverteilung integriert, können Ausfälle von einzelnen Komponenten möglicherweise nicht mehr ausreichend durch ein alternatives Routing kompensiert werden. Dies kann sich dementsprechend grundlegend negativ auf die Verfügbarkeit des Systems auswirken [63].

Ein letzter Aspekt, welcher Relevanz in Bezug auf die Topologie und des vorliegenden Anwendungsszenarios besitzt, ist eine doppelte Modellierung von Diensten und Netzwerkrouten. Anders als innerhalb der nachfolgenden Replikation, werden hier keine zwei gleichen Cloud-Dienste genutzt, sondern verschiedene, welche aber eine möglichst hohe Schnittmenge an gleicher Funktionalität ausüben können [71]. Wird dies innerhalb von Subnetzen, in denen besonders kritische Geschäftsprozesse durchgeführt werden, nicht praktiziert, so kann ein Cloud-Dienst schnell als Single Point Of Failure die Verfügbarkeit des ganzen Systems durch den eigenen Ausfall negativ beeinträchtigen. Ähnliches gilt für die Netzwerkrouten, die ein Routing der Anfragen zwischen den verschiedenen Cloud-Diensten ermöglichen. Sobald zwei verschiedene Cloud-Dienste die ständige Verfügbarkeit von demselben Geschäftsprozess sicherstellen sollen, müssen entsprechende Netzwerkrouten, möglicherweise individuell zugeschnitten auf die Anforderungen des jeweiligen Cloud-Dienstes doppelt modelliert sowie getestet werden [71]. Geschieht dies nicht, so wird durch einen doppelten Einsatz von verschiedenen Cloud-Diensten kein Vorteil gewonnen und dies wirkt sich sogar ebenfalls negativ auf die Verfügbarkeit aus. Dies liegt vor allem darin begründet, dass so durch die ineffiziente Integration von mehreren Instanzen eines Cloud-Dienstes lediglich Mehrkosten entstehen, die unter Umständen ein zusätzliches Risiko für den Betrieb des gesamten Systems darstellen können.

B11: Unzureichende Konfiguration von Replikation

Weitere Bedrohungen entstehen, wenn innerhalb der Architektur keine beziehungsweise lediglich unzureichende Replikationsstrategien berücksichtigt werden. Auch der Einsatz von Replikationsstrategien, die für eine On-Premises-Infrastruktur konzeptioniert und als ausreichend angesehen wurden, kann zu Bedrohungen führen. Grund hierfür ist das unterschiedliche Verständnis der Entwicklung eines zuverlässigen Systems auf einer herkömmlichen Infrastruktur wie einem On-Premises-System sowie in der Cloud. Während in Systemen auf On-Premises Infrastrukturen oftmals in redundante High-End-Hardware in-

vestiert wird, um einen Ausfall von Komponenten möglichst komplett zu vermeiden, wird in der Cloud ein solcher Ausfall akzeptiert und stattdessen der Fokus auf das Minimieren der Auswirkungen bezüglich der Funktionalität gesetzt [61]. Um diese Auswirkungen zu minimieren, wird in der Regel Replikation als ein Werkzeug genutzt. Im Kontext von Cloud-Computing bedeutet Replikation also, dass Komponenten exakt auf andere Systeme kopiert und in einem gewissen Intervall mit dem „Original“ synchronisiert werden. Bei einem Ausfall können diese Kopien auf einem anderen unabhängigen System gestartet werden und entsprechende Funktionalitäten weiterhin sicherstellen [25]. Ziel dabei ist es, dass der Endnutzer gänzlich nichts von dem Ausfall bemerkt. Konkrete Bedrohungen entstehen nun, wenn bezüglich der Verfügbarkeit unbedingt zu schützende und damit zu replizierende Komponenten nicht ausreichend identifiziert werden und keine Replikation dieser innerhalb der Systemarchitektur berücksichtigt wird [69]. Dadurch könnte beispielsweise schon der Ausfall einer Loadbalancer-Instanz (A006) dafür sorgen, dass der dahinterliegende Teil des Systems nicht mehr erreicht werden kann. Da die Schichten im System von „MaBCloud“ aufeinander angewiesen sind, hätte dieses Szenario wahrscheinlich ein Ausfall des gesamten Systems zur Folge. Aber auch wenn zu replizierende Komponenten ausreichend identifiziert wurden und ein entsprechender Replikationsmechanismus sichergestellt wurde, kann dieser weiterhin Schwachstellen aufweisen. Dies passiert beispielsweise, wenn ein Replika nicht innerhalb einer anderen Verfügbarkeitszone beziehungsweise Region des Cloud-Anbieters angelegt werden. Falls eine solche Zone des Cloud-Anbieters gänzlich ausfällt, so wäre auch die Anwendung trotz Replikation nicht mehr erreichbar, da sowohl die „originale“ Instanz einer Komponente als auch das Replika nicht mehr erreichbar sind [69]. Des Weiteren ist oft unklar, wann eine solche Zone wieder funktionsfähig ist, da dies im Zuständigkeitsbereich des Cloud-Anbieters liegt. Da durch die Cloud-Anbieter verwaltete Dienste oft als hochverfügbar verkauft werden und damit bereits eine Replikationsstrategie umgesetzt ist[10], betrifft diese Bedrohungen primär die Verfügbarkeit der virtuellen Maschinen der eigenen Anwendung.

B12: Unreichende Backup- und Recoverystrategie

Ein Datenverlust kann in verschiedenen Dimensionen auftreten und wird oftmals durch eine unzureichende Datensicherung herbeigeführt. Falls Daten durch einen Sicherheitsvorfall verloren gehen und keine Datensicherung durchgeführt wurde, kann dies direkt existenzbedrohend für ein Unternehmen sein [12]. Allerdings kann ebenfalls eine zwar durchgeführte, aber mangelhaft umgesetzte Datensicherung das Schutzniveau des Systems senken. Wird beispielsweise durch Tests nicht regelmäßig sichergestellt, dass die ge-

[10]Siehe zum Beispiel Cloud SQL von Google: https://cloud.google.com/sql

sicherten Daten überhaupt wieder einspielbar sind, so können ebenfalls essenzielle Daten trotz durchgeführter Sicherungen verloren gehen. Auch falls die Menge der zu sichernden Daten schlichtweg so groß ist, dass genutzte Speichermedien und oder die genutzte Datensicherungsgeschwindigkeit nicht ausreicht, kann dies in einem Verlust von Daten resultieren [12].

Im Kontext von Cloud-Computing kommen weitere spezifische Aspekte zu dieser Bedrohung dazu. Viele Cloud-Diensteanbieter bieten eine Datensicherung als verwalteten Cloud-Dienst an, im welchem eine gewünschte Backup-Strategie bezüglich zeitlicher Abstände und Umfänge von Sicherungen konfiguriert werden kann. Die Datensicherung und das Wiedereinspielen von Daten wird dann bei Bedarf von dem Cloud-Anbieter durchgeführt. Hier bietet jedoch jeder Cloud-Anbieter andere und möglicherweise sehr spezifische Konfigurationsmöglichkeiten, sowie Umfang der gebotenen Funktionalitäten und Art und Weise der Benutzung an. Dementsprechend kann die Wahrscheinlichkeit von Konfigurations- beziehungsweise Anwenderfehler zunehmen. Werden also insbesondere hinsichtlich dessen keine regelmäßigen Tests bezüglich einer richtigen Konfiguration durchgeführt, kann daraus im Rahmen eines entsprechenden Vorfalls ein akuter Verlust von Geschäftsdaten stattfinden. Kann nachgewiesen werden, dass der Datenverlust einem Konfigurationsfehler zugrunde liegt, so gibt es im Rahmen des Shared-Resoponsibility-Modells keine Unterstützung seitens des Cloud-Anbieters bei einer Wiederherstellung.

Im Zuge der Nutzung eines verwalteten Cloud-Dienstes für die Datensicherung muss außerdem damit gerechnet werden, dass ein gewisser Grad an Kontrolle über die Sicherungen der eigenen Geschäftsdaten abgegeben wird. Dies gilt speziell im Hinblick darauf, dass so Angriffe auf den Backup-Dienst des Cloud-Anbieters auch die eigenen Datensicherungen betreffen können. Aufgrund dessen dass die Implementierung und die Daten der Datensicherungen so vollständig in einem System des Diensteanbieters liegen, könnte eine Institution gegebenenfalls nicht beziehungsweise erst verzögert über einen kritischen Sicherheitsvorfall in Kenntnis gesetzt werden. Ebenso besteht zusätzlich die Gefahr, dass durch bestimmte vertragliche Konditionen die Datensicherung erst nach einer bestimmten Zeitspanne wieder eingespielt werden, die für das Anwendungsszenario nicht tragbar sind [12]. Zudem werden bestimmte Funktionen oft gezielt eingeschränkt. So ist es zum Beispiel im Zuge des Backup-Cloud-Dienstes von Microsoft für die Azure-Cloud nicht möglich die dort hinterlegten Datensicherungen, ohne Umwege auf ein lokales Gerät herunterzuladen [62], um mittels einer lokalen Datensicherung eine Kopie mit vollständiger eigener Kontrolle zu erhalten. Diese Umstände können sich negativ auf die Verfügbarkeit der in der Cloud entwickelten Anwendungen auswirken.

Als ein weiterer Aspekt kann es auch bei Cloud-Diensten für Datensicherungen vorkommen, dass gesetzliche Vorschriften nicht eingehalten werden [12]. Dies kann sich unter Umständen negativ aus das Sicherheitsniveau auswirken, falls eine Institution ansonsten eine sichere lokale Datensicherung gewährleisten könnte. Neben der Verfügbarkeit würde dies auch die Grundwerte der Vertraulichkeit und Integrität von Geschäftsdaten negativ beeinflussen.

B13: Unzureichende Konfigurationen von Kontingenten

Besonders im Zuge der nutzungsbasierten Abrechnungen ist die Konfiguration von Kontingenten wichtig, um eine Cloud-Umgebung vorteilhaft für das eigene Unternehmen einsetzen zu können. Insbesondere gilt dies hinsichtlich der Autoskalierung von Komponenten und dem damit verbundenen Ressourcenverbrauch. Cloud-Anbieter bieten mit der Autoskalierung in der Regel ein Mechanismus an, der die Anzahl von Instanzen automatisch steuern kann. Im Beispiel von Microsoft Azure werden dazu bestimmte Metriken, wie zum Beispiel Antwortzeit auf Anfragen, CPU-Nutzung oder Speichernutzung verwendet, um die Anzahl der Instanzen von einer Komponente automatisch zu erhöhen oder zu verringern [60]. Dies geschieht mit dem Ziel, die Anfragen bedarfsgerecht bei einem möglichst niedrigen Ressourcenverbrauch verarbeiten zu können. Kommt es nun jedoch zu einem plötzlichen Anstieg von Anfragen durch verschiedenste Hintergründe, wie zum Beispiel durch bösartige Angriffstechniken wie einem Denial of Service Angriff oder durch anderweitige Ereignisse, so kann das System bis an die harten technischen Limits des Cloud-Anbieters autoskaliert werden. Dadurch können potenziell tausende von Instanzen einer Komponente, wie zum Beispiel dem „MaBCloud“ Frontend laufen, einen hohen Ressourcenverbrauch und damit hohe Kosten verursachen [60]. Werden hier also keine Kontingente für die automatische Skalierung festgelegt, so können deutlich erhöhte finanzielle Kosten für den Rechnungsträger entstehen. Als Folge könnte gegebenenfalls der Betrieb des Systems in der Cloud aufgrund eines zu hohen existenziellen Risikos aufgegeben werden, was eine Bedrohung für die Verfügbarkeit des gesamten Informationsverbundes darstellt.

B14: Unzureichende Konfigurationen von Logging

Schränken solche Limitierungen allerdings das Logging durch Komponenten und Anwendungen in der Cloud-Umgebung ein, so können sich daraus maßgebliche Bedrohungen für den Betrieb des gesamten Informationsverbundes in der Cloud ergeben. Logging in der Cloud ist eine dauerhafte Aktivität, die jedes Event des Systems dokumentiert und

besonders im Rahmen von forensischen Untersuchungen vor, während oder nach einem Sicherheitsvorfall zur Verhinderung oder Nachuntersuchung von sicherheitskritischen Vorfällen essenziell sind. So sind beispielsweise Reportings aus Log-Analysen entscheidend für juristische Verfahren gegen angreifende Parteien [58].

Um ein sinnvolles Logging zu implementieren, müssen Logs an einer zentralen Stelle gespeichert beziehungsweise für Analysen abrufbar sein und gegebenenfalls Relationen zwischen geloggten Ereignissen verschiedener Komponenten analysierbar sein. Unter Bezugnahme der komplexen und dezentralen Komposition von Komponenten innerhalb der Infrastruktur in der Cloud, sind dies keine trivialen Anforderungen. Damit hier der Nutzer entlastet wird, bieten gängige Cloud-Anbieter in der Regel einen Cloud-Dienst für das Logging an, wie zum Beispiel bei Microsoft Azure der Dienst Azure Monitor[11] oder dem Cloud Logging beziehungsweise Log-Explorer[12] in der Google Cloud. In einem solchen Dienst werden Logs aus verschiedenen konfigurierbaren Quellen, wie Anwendungen oder anderen genutzten Cloud-Diensten, zugeliefert. Diese sind dann an diesem zentralen Ort abrufbar und erste kompatible Analysewerkzeuge werden direkt bereitgestellt. Die Nutzung eines solchen Dienstes bietet sich besonders an, da jeder Cloud-Anbieter sein eigenes Logging-Format besitzt und damit direkt und mit wenig Aufwand ein kompatibler Dienst zur Verfügung steht.

Im Kontrast dazu stellt die reine Nutzung eines solchen Cloud-Dienstes ohne Konfigurationen allerdings eine direkte Bedrohung für das Schutzniveau des gesamten Systems dar. Ein Beispiel hierfür bietet die Azure Cloud von Microsoft mit dem Azure Monitor Dienst. Hier werden ohne Konfigurationen dem Dienst keinerlei Logs zugeliefert und dementsprechend sind diese für Analysen auch nicht ohne Weiteres zentral abrufbar [64]. Bei Analysen müssten hier die Logs aus jeder Ressource und Komponenten selbst gesammelt und in eigener Verantwortung analysierbar dargestellt und werden. Dadurch können gegebenenfalls Log-Dateien verloren gehen oder Analysen durch Cloud-Anbieter spezifische Formate kompliziert sein.

Weitere Bedrohungen ergeben sich aus dem zu konfigurierenden Umfang an Ereignissen, welche geloggt werden sollen. Hier entsteht ein Spannungsfeld zwischen wirtschaftlichen Interessen und der Sicherheit des Systems, da nach einem gewissen kostenlosen Kontingent häufig zusätzliche Kosten pro Gigabyte an gesammelten Log-Dateien anfallen. Im

[11] https://azure.microsoft.com/de-de/products/monitor
[12] https://cloud.google.com/logging

Interesse des Managements kann es also sein, hier das loggen von Ereignissen und damit verbundene Kosten eher gering zu halten. Für solche Szenarien können bei gängigen Cloud-Anbietern Regeln erstellt werden, die konfigurieren welche Ereignisse berücksichtigt und in den Logs gesammelt werden sollen. Beispielsweise können bei Microsoft Azure Filterkriterien angegeben werden, wie eindeutige Event-Identifier, Prozessnamen, oder einen kategorischen Schweregrad der Ereignisse beziehungsweise ob es sich lediglich um eine Warnung handelt oder eine kritische Fehlermeldung [67].

Haben es geloggte Events durch die konfigurierten Filter geschafft, so gilt ähnliches für die Aufbewahrungsdauer von Log-Dateien. Da auch die Speicherung von Log-Daten durch die Cloud-Anbieter häufig ab dem 31. Tag pro Gigabyte Geld kostet, kann sich ein selbes Spannungsfeld bilden.

Werden also aus Kostengründen entweder Filter zu eng definiert, sodass relevante Ereignisse nicht mehr zugeliefert oder Logs nicht ausreichend lange aufbewahrt werden, können sicherheitskritische Vorfälle unentdeckt bleiben beziehungsweise nicht mehr rekonstruiert werden. Dies kann sich potenziell negativ auf alle Schutzziele der Informationssicherheit auswirken. Als weitere Seiteneffekte durch solche Szenarien können Schwachstellen des Systems für angreifende Personen offen bleiben, sowie juristische Folgen für angreifende Personen durch fehlende gerichtsverwertbare Beweise ausbleiben.

B15: Unzureichende Konfigurationen von Alerting

Nicht nur eine unzureichende Konfiguration von Logging in der Cloud kann dafür sorgen, dass sicherheitskritische Ereignisse nicht erkannt werden, sondern auch eine unzureichende Konfiguration von Alerting-Mechanismen kann dafür verantwortlich sein. Denn selbst wenn sicherheitskritische Ereignisse angemessen geloggt werden, müssen verantwortliche Stellen möglichst zeitnah in Kenntniss gesetzt werden, damit angemessene Reaktionen möglich sind und Schäden effektiv begrenzt werden können.

Eine solche Funktion erfüllen Alert-Dienste, die in der Regel ebenfalls durch den Cloud-Anbieter bereitgestellt werden können. Dieser Dienst benachrichtigt proaktiv konfigurierte Aktionsgruppen, falls möglicherweise Probleme mit der Infrastruktur besteht. Je nach Konfiguration können Aktionsgruppen dabei entweder Benachrichtigungskanäle wie E-Mail oder SMS, aber auch Instanzen, die nach einer Benachrichtigung automatisierte Aktionen ausführen sein.

Eine solche Konfiguration kann mittels Regeln vorgenommen werden. Exemplarisch innerhalb der Microsoft Azure Cloud enthalten diese einerseits die zu überwachende Res-

source, andererseits mitzusendende Daten aus der Ressource und Vorbedingungen zum Informieren jeweiliger Aktionsgruppen [74]. Eine unzureichende Konfiguration von diesen Regeln kann zu einer Bedrohung führen, wenn innerhalb des Cloud-Systems ein sicherheitskritischer Vorfall stattfindet, der zwar angemessen geloggt wird aber für den keine Aktionsgruppe proaktiv benachrichtigt wird. Als Folge, könnten die Benachrichtigungen von den verantwortlichen Stellen innerhalb des Unternehmens nicht oder nur verspätet wahrgenommen werden. So erhöht sich also die Chance, dass dieser Vorfall erstmal unentdeckt bleibt und eine angemessene Reaktion ausbleibt.

Werden zwar Regeln konfiguriert, aber dabei eine unzureichende Strategie bezüglich der benachrichtigten Aktionsgruppen verfolgt, kann sich dies ebenfalls negativ auf das Schutzniveau des gesamten Systems auswirken. Ein konkretes Beispiel diesbezüglich kann ein nächtlicher Angriff auf ein System sein, der möglicherweise sofortiges Handeln bedarf. Allerdings sind in der allermeisten Unternehmen nachts keine administrierenden beziehungsweise mitarbeitenden Personen verfügbar. Wird nun die Aktionsgruppe so konfiguriert, dass lediglich Benachrichtigungen an hinterlegte Kontaktmöglichkeiten verschickt werden und nicht an technische Komponenten, die automatisierte Maßnahmen einleiten, so kann einige Zeit vergehen bis eine Reaktion stattfindet. Je nach Ziel des Angriffes kann sich dies sowohl negativ auf die Verfügbarkeit des gesamten Systems auswirken, als auch auf die Integrität und Vertraulichkeit der Daten.

4.4.5 Bedrohungen in Kommunikation

Nr.	**Bedrohung**	**identifiziertes System**	**beinträchtigte Grundwerte**
16	Denial of Service	Informationsverbund / übergeordneter Aspekt	A
17	Betrügerische Ressourcenverbrauch	A001: MaB Cloud Frontend	A
18	Unzureichende Separierung von Komponenten	Informationsverbund / übergeordneter Aspekt	A, C, I
19	Unnötiges Öffnen von Cloud-Komponenten für das öffentliche Internet	Informationsverbund / übergeordneter Aspekt	A, C, I

Tabelle 4.5: Übersicht der Bedrohungen durch die Kommunikation

B16: Denial of Service

Eine Studie des *Neustar International Security Council* durch Sicherheitsexperten aus diversen EU-Ländern sowie der USA hat gezeigt, dass Denial of Service Angriffe einer der am höchsten einzustufenden Gefahren für ein IT-System eines Unternehmens sind [11]. Dabei wird als Denial of Service Angriff eine Angriffstechnik bezeichnet, die eine vorhergesehene Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte verhindern soll. Dies kann auf physischer Ebene, sollten beispielsweise Eingangstüren von einer für das Unternehmen essenziellen Infrastruktur blockiert werden, als auch auf technischer Ebene gegen IT-Systeme erfolgen [12]. Im Rahmen eines Denial of Service gegen ein IT-System versucht ein Angreifer in der Regel Netzwerkinfrastrukturen und Rechenressourcen derart mit Anfragen zu überfordern, dass ein uneingeschränkter Betrieb nicht mehr möglich ist. Wie in Abbildung 4.2 zu erkennen kann dafür ein Netz aus verschiedensten internetfähigen Geräten verwendet werden. Falls ein solcher Denial of Service Angriff direkt gegen einen Webdienst wie beispielsweise dem „MaBCloud“ Frontend gerichtet wird, kann dieser für Benutzer nur noch eingeschränkt oder sogar gar nicht mehr verfügbar sein [12] (ebenfalls erkennbar in Abbildung 4.2).

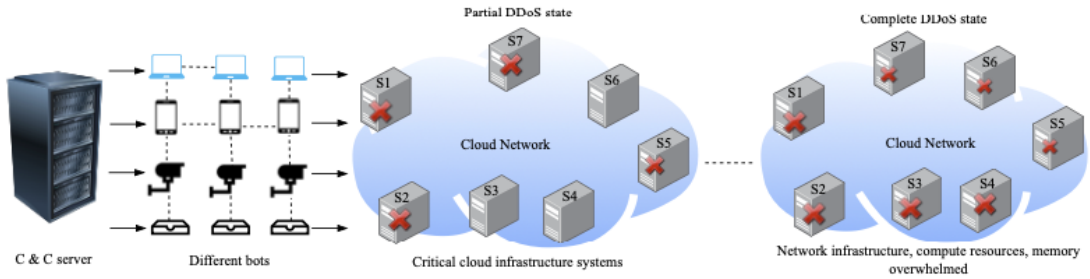

Abbildung 4.2: Mögliche Szenarien eines Denial of Service Angriffes auf eine Cloud-Umgebung. Quelle: [11]

Ein anderes Beispiel wäre ein Denial of Service Angriff gegen Firewalls, die oft als erste Instanz solchen Angriffen von außen über das Netzwerk ausgesetzt sind. Wird diese durch zu viele Anfragen so weit belastet, dass sie ausfällt, so kann im schlimmsten Szenario das ganze dahinterliegende Netzwerk nicht mehr erreichbar sein und die dem Netzwerk angehörende Dienste können vom Endnutzer ebenfalls nicht mehr verwendet werden [12]. Die Nichtbenutzbarkeit von Systemen innerhalb solcher Szenarien für den Endnutzer, sei es durch den Totalausfall oder einer schlechten Benutzererfahrung durch eine eingeschränkte Erreichbarkeit, kann für ein Unternehmen viele Gefahren mit sich bringen. Als Folge kann

neben einer Rufschädigung auch ein hoher finanzieller Schaden auftreten, sowie Mehrkosten für Abwehrmaßnahmen und Wiederherstellung der Verfügbarkeit der Systeme [11]. Während dieses allgemeingültige Bedrohungen für die meisten IT-Systeme sind, kommen bei Denial of Service Angriffe gegen IT-Systeme in der Cloud noch weitere Gefahren dazu. Da im Rahmen der nutzungsbasierten Abrechnung oftmals eine flexible Skalierung von Ressourcen nach Bedarf stattfindet, kann im Rahmen eines Denial of Service ein Szenario entstehen, das Ressourcen automatisch hoch skaliert werden, um die Überflutung der Anfragen bedarfsgerecht zu verarbeiten. Durch diese Skalierung und dem entstehenden Mehrverbrauch von Ressourcen können deutliche Mehrkosten für ein Unternehmen entstehen. Zusätzlich bringt das Multi-Tenant-Modell des Cloud-Computings eine weitere Bedrohung im Zusammenhang mit Denial of Serive Angriffen gegen Cloud-Anwendungen mit sich. Da sich mehrere Kunden des Cloud-Anbieters dieselbe physische Infrastruktur teilen und dadurch Systeme von mehreren Kunden auf beispielsweise denselben physischen Server betrieben werden, oder zumindest die physischen Netzwerkleitungen nutzen, kann auch ein Denial of Service Angriff auch bei anderen Kunden Kollateralschäden und Beeinträchtigungen verursachen. Gleiches gilt ebenfalls in einem umgekehrten Szenario. Falls ein anderer Kunde des Cloud-Anbieters mit einem Denial of Service Angriff angegriffen wird, können sich die Folgen auch auf den Betrieb der eigenen Anwendung in der Cloud auswirken [99]. Alle genannten Szenarien hätten dabei primär einen negativen Einfluss auf den Grundwert der Verfügbarkeit innerhalb des ganzen Systems. Dies lässt sich primär mit der Abhängigkeit zwischen den verschiedenen Anwendungen erklären, um die gewünschte Funktionlität zu ermöglichen.

B17: Betrügerischer Ressourcenverbrauch

Der Bedrohung von betrügerischer Ressourcennutzung unterliegen ähnliche Funktionsweisen wie einem Denial of Service Angriff in Bezug auf bösartige Zugriffe auf den Cloud-Endpunkt. Im Zuge einer betrügerischen Ressourcennutzung werden jedoch nur wenige HTTP-Zugriffe an das MaBCloud Frontend (A001) gestellt, um so einen legitimen Benutzer vorzuspielen. Eine konkrete Bedrohung für die MakeABank GmbH entsteht nun unter der Bezugnahme des angestrebten nutzungsbasierten Abrechnungsmodells der Cloud-Umgebung. Dadurch können durch die zusätzlichen bösartigen Anfragen teils deutliche Mehrkosten für die MakeABank GmbH generiert werden. Durch den damit verbundenen finanziellen Merhaufwand für das rechnungstragende Unternehmen kann der generelle Betrieb von „MaBCloud“ in der Cloud bedroht werden, weshalb sich dieser Angriff ebenfalls gegen die Verfügbarkeit des Systems richtet. Primär wird hier das „MaBCloud“ Frontend als identifiziertes Systems definiert, da diese Teilanwendung die Endpunkte für

einen betrügerischen Ressourcenverbrauch zur Verfügung stellt. Zudem wird der Bedrohungsgrad dadurch weiter erhöht, dass durch die verhältnismäßig wenigen Anfragen eine Klassifizierung des Angriffes besonders schwierig ist [2].

B18: Unzureichende Separierung von Komponenten

Ebenso schwierig kann eine Klassifikation bei Angriffen auf das System in der Cloud sein, was durch eine unzureichende Separierung von Cloud-Komponenten in Bezug auf Netzwerkverbindungen begünstigt wird. Konkret geht es hier um Angriffstechniken wie den Advanced Persistence Threads oder Lateral Movements. Unterstützt durch den Umstand, dass die Schutzmaßnahmen eines Systems oft auf starke Außengrenzen der Netze fokussiert sind und die innere Sicherheit tendenziell vernachlässigt wird [79], wurden bereits viele Unternehmen zum Opfer und haben pro Angriff solcher Art durchschnittliche Verluste von 100.000 bis 500.000 USD verzeichnen müssen [21]. Im Detail zielen beide Gruppen der Angriffstechniken darauf ab, nach einem erfolgreichen Eindringen in ein Netzwerk über eine unzureichend gesicherte Komponente, eine Eskalation der Berechtigungen, beziehungsweise einen Zugang zu weiteren Komponenten des Systems zu erwirken. Dafür folgt nach einer Analyse des Netzwerkes die Ausbreitung des Angriffes bei der weitere Hosts angegriffen werden. Primäres Ziel dabei ist es, Daten für den Zugang zu weiteren Komponenten und insbesondere zu den Kronjuwelen in Form von sensiblen Geschäftsdaten zu erhalten. Im Rahmen von Advanced Persistence Threads verbleiben Angreifer meistens sogar längerfristig im System, um jede neue Komponente im Netzwerk anzugreifen bis ein Zugang zu den sensiblen Daten besteht [21].

Auch wenn, im Gegensatz zu On-Premises Systemen, kein Einfluss auf die Verbindungen zwischen Komponenten auf Ebene der Infrastruktur besteht, können Kommunikationskanäle zwischen Komponenten trotzdem umfangreich konfiguriert, geöffnet, sowie geschlossen und die Kommunikation der Netze auf logischer Ebene modelliert werden. Werden also innerhalb dieser nicht essenzielle Verbindungen zwischen Cloud-Komponenten offen gelassen und kritische Geschäftsprozesse nicht ausreichend voneinander durch jeweils eigene und unabhängige Netze isoliert, kann dies die Effektivität und den Erfolg von genannten Angriffstechniken unterstützen. So können angreifende Personen schneller durch die Netze traversieren, Komponenten anderer essenzieller Geschäftsprozesse im Netz angreifen und die Gefahr erhöhen, dass in einer der vielen Komponenten Konfigurationsfehler gefunden und bösartig ausgenutzt werden.

Insgesamt wird den angreifenden Personen also mehr Angriffsfläche zur Verfügung gestellt, was sich dementsprechend negativ auf das Schutzniveau des gesamten Systems

auswirkt. Da es sich besonders im Rahmen der Advanced Persistence Threads um Angriffstechniken handelt, die Daten von Systemen ausspähen und manipulieren, für die es aber eher günstig ist möglichst lange unentdeckt zu bleiben, steht die Beeinträchtigung der Verfügbarkeit nicht allzu stark im Fokus. Vorrangig werden die Schutzziele der Vertraulichkeit und Integrität von Geschäftsdaten verletzt.

B19: Unnötiges Öffnen von Cloud-Komponenten für das öffentliche Internet

Ein weiterer Faktor, welcher ein solches Eindringen und Verbreiten im Netzwerk begünstigen kann, ist ein unnötiges Öffnen von Cloud-Komponenten und Ressourcen für das öffentliche Internet. Um einen externen Zugriff aus dem öffentlichen Internet zu verhindern, können auch in der Cloud verschiedene Blockaden konfiguriert werden.

Bereits beim Erstellen von Ressourcen in Form eines virtuellen Speichermediums oder virtuellen Maschinen kann in der Regel konfiguriert werden, ob ein externer Zugriff erlaubt, beziehungsweise ob diesem Objekt eine öffentliche Adresse zugewiesen werden soll. Werden diese Einstellungen unzureichend verifiziert, ist ein Speichermedium oder eine virtuelle Maschine fälschlicherweise für externe Zugriffe erreichbar und liegen zusätzlich andere begleitende Mängel wie eine schwache oder gänzlich keine Verschlüsselung vor, so können Angreifer im schlimmsten Falle einfach unberechtigt auf Daten zugreifen, diese verändern oder aus dem aktuellen Betrieb löschen. Um zu verdeutlichen, dass solche Szenarien in der Realität durchaus Relevanz besitzen und sich in Unternehmen realistisch abspielen können, gibt es historische Beispiele wie die türkische Airline *Pegasus Air* und die *US Intelligence and Security Command* Behörde. Im Detail wurde bei *Pegasus Air* ein Speichermedium fälschlicherweise für einen Zugriff aus dem Internet offen gelassen, sodass 6.5 Terrabyte an sensiblen Daten öffentlich zugänglich waren. Gleiches spielte sich mit 1000 Gigabyte an Daten bei der *US Intelligence and Security Command* Behörde ab, die in Strukturen der US-Arme und NSA operiert und dementsprechend sensible Daten händelt [33]. Spielen sich durch Konfigurationsfehler ähnliche Szenarien wie beschrieben ab, so können die alle Grundwerte der Informationssicherheit betroffen sein, je nachdem ob lediglich ein unberichtigter Zugriff erfolgt oder weitere Operationen auf die Daten stattfinden können. Außerdem können diesbezüglich verschiedene Komponenten im System falsch konfiguriert werden, was schwerwiegende Folgen für das ganze System beziehungsweise den ganzen Informationsverbund nach sich ziehen kann.

4.4.6 Authentifikation/Trust-Bedrohungen

Bedrohungen dieser Kategorie resultieren aus einem mangelhaften Authentifikationsprozess sowie Trustmanagements in der Cloud. Authentifikation bedeutet hierbei ein Sicherheitsprozess, der entweder die Erlaubnis einer Datenübertragung, einer Nachricht, eines Urhebers oder die Gültigkeit eines Benutzers überprüfen, um eine bestimmte Kategorie an Daten empfangen zu dürfen [9]. Trust besitzt hingegen keine einheitliche Definition im Kontext von Cloud-Computing. Wichtig ist es trotzdem für folgende Abschnitte zwei Definitionsansätze festzuhalten. Ein Definitionsansatz auf allgemeinster Ebene wäre hier der Grad des Vertrauens in etwas oder jemanden. Für spätere thematische Analysen innerhalb des Kapitels ist es wichtig, diesen Definitionsansatz sowohl aus der unternehmerischen Sicht als auch aus der transaktionalen Sicht zwischen technischen Komponenten weiter zu konkretisieren. So lässt sich aus der unternehmerischer Perspektive Trust als den Grad der Zufriedenheit oder Vertrauen definieren, den ein Nutzer in den Diensten eines Cloud-Anbieters hat [81]. Die transaktionale Perspektive definiert Trust hingegen eher als eine Entität A, die einer Entität B Trust ausspricht, sobald A fest davon ausgeht, dass sich Entität B wie erwartet beziehungsweise benötigt verhält [115].

Nr.	**Bedrohung**	**identifiziertes System**	**beinträchtigte Grundwerte**
20	Unzureichende Authentifizierungsrichtlinien	Informationsverbund / übergeordneter Aspekt	A,C,I
21	Social Engineering	Informationsverbund / übergeordneter Aspekt	A,C,I
22	Schlechtes Trustmanagement	Informationsverbund / übergeordneter Aspekt	A, C, I
23	Schlechtes Keymanagement	Informationsverbund / übergeordneter Aspekt	A, C, I

Tabelle 4.6: Übersicht der Bedrohungen entstehend durch Authentifikation beziehungsweise Trust

B20: Unzureichende Authentifizierungsrichtlinien

Die Passwort-basierte Authentifikation ist auch heute durch die Einfachheit der beliebteste Weg sich in einem System zu authentifizieren. Auch wenn sich die Technik stetig weiterentwickelt, bleibt die ständige Schwachstelle des Menschen erhalten [13]. Um die Schwach-

stelle des menschlichen Verhaltens hier größtmöglich einzuschränken, werden einerseits Passwortrichtlinien und andererseits zusätzliche Authentifizierungsschritte im Rahmen einer Multi-Faktor-Authentifizierung eingesetzt. Im Kontext von Cloud-Computing lassen sich sowohl die Passwortrichtlinien als auch eine Multi-Faktor-Authentifizierung meistens in der Cloud-Konsole des Cloud-Anbieters konfigurieren. Durch die Passwortrichtlinien wird dann bestimmt, welche Passworteigenschaften die Benutzerkonten der Cloud-Konsole erfüllen müssen, um ein Konto registrieren beziehungsweise sich zukünftig anmelden zu dürfen. Die Multi-Faktor-Authentifizierung fügt nach erfolgreicher Eingabe des Passwortes einen zusätzlichen Authentifizierungsschritt hinzu. Dieser kann beispielsweise aus der Nutzung von Hardware-Schlüsseln, Prüfung von biometrischen Merkmalen oder der Eingabe eines Sicherheitscodes bestehen, welcher an ein mobiles Gerät gesendet wurde. Die Authentifizierungsrichtlinien beschränken sich dabei jedoch oftmals nicht nur auf die Cloud-Konsole. Viele Cloud-Anbieter bieten Proxy-Dienste an, um Zugriff auf Anwendungen und VMs anhand der Identität zu beschränken. Diese Proxys agieren dabei wie eine Vermittlungskomponente zwischen dem Endnutzer und dem Endpunkt der VM. Diese Komponente sorgt dafür, dass sich der Endnutzer dann über eine Weboberfläche mit einem autorisierten Benutzerkonto des Cloud-Anbieters anmelden muss und erst nach erfolgreicher Anmeldung mit dem Endpunkt der VM kommunizieren kann. Aus sich des Cloud-Nutzers muss so unter Umständen keine eigener Authentifizierungsmechanismus implementiert werden, um den Zugriff auf das System zu beschränken, zu können. Speziell Anwendung, welche öffentlich erreichbar sein sollen, wie dem MaBCloud Frontend (A001) können damit gesichert werden. Daher kommen konfigurierte Authentifizierungsrichtlinien häufig in breiten Anwendungsszenarien innerhalb der Cloud zum Einsatz.

Die konkreten Bedrohungen durch mangelhafte Authentifizierungsrichtlinien entstehen nun aus der Schwachstelle Mensch und Angriffstechniken, die darauf abzielen Passwörter zu knacken. So hat eine Studie herausgefunden, dass 72 % der befragten Personen überall dasselbe Passwort nutzen und 50 % keinen Wert auf die Sicherheit bei der Passwortwahl legen [42]. Angenommen eine freie Wahl des Passwortes wäre zulässig, so kann davon ausgegangen werden, dass ein solches Verhalten ohne Einschränkungen durch Richtlinien auch bei der Wahl des Passwortes im eigenen System genutzt werden würde. Berücksichtigt man nun die entsprechenden Angriffstechniken, wie einen Brute-Force-Angriff oder einen Dictionary-Angriff, welche eine schwache Passwortvergabe gezielt ausnutzen, dann wirkt sich dies negativ auf das gesamte Schutzniveau des Systems aus. So werden im Rahmen eines Brute-Force-Angriffes automatisiert alle möglichen Passwortkombina-

tionen ausprobiert, während ein Dictionary-Angriff Statistiken zu den am meisten verwendeten Passwörtern berücksichtigt und abarbeitet. Der Aufwand für solche Angriffe ist verhältnismäßig niedrig, da bereits frei erhältliche Open Source Werkzeuge wie beispielsweise Hashcat[13] verwendet werden können. Im Rahmen eines Experimentes konnte beispielsweise durch einen Brute-Force-Angriff 10-stellige englische Passwörter, bestehend aus Kleinbuchstaben, in durchschnittlich 50 Minuten errechnet werden [13]. Bei einer besseren Hardware kann dies in einer noch kürzeren Zeit geschehen. Falls zusätzlich in den Authentifizierungsrichtlinien keine Multi-Faktor-Authentifizierung vorgesehen ist, können kompromittierte Passwörter von angreifenden Personen verwendet werden, um sich möglicherweise mit einem autorisierten Benutzerkonto in der Cloud-Konsole zu authentifizieren und umfassende Aktionen durchzuführen. In einem solchen Szenario können alle Schutzziele verletzt werden.

B21: Social Engineering

Als Social Engineering wird eine Methode bezeichnet, um durch soziale Handlungen einen unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen. Dabei werden menschliche Eigenschaften wie Hilfsbereitschaft, Angst oder Autorität gezielt ausgenutzt. Diese Angriffe können auch sehr komplexe Formen annehmen, indem beispielsweise vorher längere Beziehungen zu den Opfern aufgebaut oder gesammelte Informationen aus vorherigen Stufen für eine intensivere Täuschung genutzt werden. Werden bei diesen Angriffen Passwörter oder andere Authentifierungsmerkmal beschafft, spricht man von Phishing [12]. Oft werden Social Engineering Attacken als die effektivsten überhaupt bezeichnet, da sich diese gegen alle Systeme und das gesamte Netzwerk richten können und durch Hardware- sowie Software-basierte Sicherheitsmechanismen nicht verhindert werden können [91]. So stellt das Social Engineering, insbesondere das Phishing, auch eine Bedrohung für das vorliegende Anwendungsszenario dar.

Beispielsweise könnten angreifende Personen an die mitarbeitenden Personen E-Mails versenden mit der Aufforderung, sich auf der Webseite des folgenden Links mit dem eigenen Benutzernamen und Passwort anzumelden, um eine bestimmte Aktion durchzuführen. Der Link leitet auf eine gefälschte Seite weiter, die im Design und der Adresse ähnlich der echte Weboberfläche des Cloud-Anbieters erscheint, aber die eingegebenen Zugangsdaten an die angreifenden Personen weitersendet. Dadurch können sich angreifende Personen mithilfe dieser Zugangsdaten in der echten Cloud-Konsole anmelden und gegebenenfalls umfangreiche Aktionen durchführen, wie zum Beispiel das System herunterzufahren und

[13] https://hashcat.net/hashcat/

die Wiederherstellungsmechanismen außer Kraft zu setzen. Außerdem können zusätzlich sensible Daten, die zum Beispiel in einer Datenbank in der Cloud gespeichert sind, gestohlen werden. Fälschen angreifenden Personen zusätzlich den Absender und geben sich als eine Autoritätsperson im Rahmen eines Spear Phishing Angriff aus oder fälschen ein besonders glaubwürdiges Szenario im Rahmen eines Pretexting Phishing Attacks so erhöht sich die Gefahr zusätzlich [91]. Dies wird zusätzlich dadurch ergänzt, dass Opfer oftmals nicht merken, dass sie einem Angriff ausgesetzt wurden, Täter oft nicht mit Strafverfolgung rechnen müssen und die angreifenden Personen so gegebenenfalls einen dauerhaften Angriffsvektor gefunden haben, um bei Bedarf weitere Informationen durch weitere Täuschungsstrategien zu erlangen [12].

Dieses beschriebene Szenario ist dabei nur eines von vielen Taktiken, dem mitarbeitende Personen zur Täuschung ausgesetzt werden können und das dem Teilgebiet des Social Engineerings entspringt.

B22: Schlechtes Trustmanagement

Oft wird der Begriff Trust als ein Synonym für Sicherheit und Privatsphäre verwendet. Eine allgemeingültige Definition existiert allerdings nicht [41]. Zur folgenden Analyse der aus einem schlechten Trustmanagements resultierenden Bedrohungen, wird ein Definitionsansatz verwendet, der sich hauptsächlich innerhalb der Sozialwissenschaft entwickelt hat.

> "Trust is a mental state comprising: (1) expectancy - the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); (2) belief - the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill; (3) willingness to take risk - the trustor is willing to take risk for that belief." aus [40, S.2]

Trust im Gesamtkontext des Cloud-Computings ist eine komplexe Struktur aus verschiedenen Beziehungen, sodass im Rahmen dieser Arbeit lediglich ein symbolischer Auszug auf einer grundlegenden Ebene behandelt werden kann. Insgesamt spielt Trust in der Cloud dabei einerseits eine relevante Rolle in technischen Beziehungen zwischen Cloud-Diensten und eigenen Anwendungen, sowie andererseits auf organisatorischer Ebene zwischen verschiedenen involvierten Institutionen. Solche Vertrauensflüsse innerhalb der Beziehungen werden als Trust-Chain bezeichnet und können sich über mehrere Komponen-

ten beziehungsweise Akteure erstrecken [41]. Ein exemplarischer Auszug an nennenswerten Trust-Chains existiert dabei in der Cloud zwischen:

- (1) eigene Anwendungen und Anwendungen beziehungsweise Dienste von Dritten in der eigenen Cloud-Umgebung (technisch)
- (2) eigene Anwendungen und Anwendungen beziehungsweise Dienste von Dritten in externen Systemen (technisch)
- (3) dem eigenen Unternehmen und einem Cloud-Anbieter (organisatorisch, siehe auch Abbildung 4.3)
- (4) gegebenenfalls dem eigenen Unternehmen und einer dritten Institution wie zum Beispiel einem Cloud Broker oder Cloud Auditor (organisatorisch, siehe auch Abbildung 4.3)

Im Folgenden werden insbesondere zwei Gefahren näher erläutert, die aus den Trust-Chains (1) und (3) in Verbindung mit einem schlechten Trustmanagement entstehen. Die erste Schwachstelle aus einem unangemessen hohen Vertrauensfluss in der Trust-Chain (1) bezieht sich auf eine technische Perspektive und entsteht, wenn Komponenten von externen Anbietern ein zu hoher Grad an Vertrauen eingeräumt wird. Die zweite Schwachstelle bezieht sich auf einen unangemessen hohen Vertrauensfluss in der Trust-Chain (3) und verursacht die vermeintlich existentiellste Bedrohung aus der Sicht eines Unternehmens bei der Adoption einer Cloud. Dabei handelt es sich um die Wahl eines gänzlich unangemessenen Cloud-Anbieters. Da dieser Vorgang ebenfalls auf einer Trust-Chain (3) basiert, wird diese Entscheidung direkt und ausschließlich durch das Trust-Management beeinflusst.

Wird also im Rahmen von (1) einem externen Dienst in der eigenen Cloud-Umgebung zu viel Trust eingeräumt, ohne dass dieses ausreichend verifiziert wird, so können sich daraus verschiedenste Folgen ergeben. Beispielsweise könnte ein als vertrauensvoll eingestufter Dienst unerlaubte Kopien von sensiblen Geschäftsdaten anlegen, Daten kompromittieren, unerlaubte Datenoperationen vornehmen, wirtschaftlich schwächeln oder schlichtweg unzuverlässig sein.

Darüber hinaus lässt sich diese Problemstellung in der Cloud in eine noch viel größere Dimension spannen. Das liegt primär an dem Umstand, dass externen Dienste oftmals weitere Dienste von Drittanbietern in Anspruch nehmen, um ihre eigenen Funktionalitäten zu implementieren. Dadurch kann sich die zu verifizierende Trust-Chain nahezu

unendlich erweitern und eine so hohe Komplexität gewinnen, dass dem Cloud-Nutzer eine solche Verifizierung der gesamten Trust-Chain unmöglich wird [4]. Zudem werden Abhängigkeiten von den Diensten eines Cloud-Anbieters zu weiteren Diensten häufig nicht ausreichend transparent offen gelegt beziehungsweise vertraglich geregelt [12], sodass selbst mit einem hohen Engagement diesbezüglich die Trust-Chain nicht mehr bis zum Ende verfolgt werden kann. Dies kann dementsprechend das Potenzial für beschriebene negative Folgen weiter begünstigen. Da hier verschiedenste Szenarien möglich wären wie ein nicht vertrauenswürdiger Dienst sich negativ auf die Sicherheit des Systems auswirken kann, kann sich dies potenziell negativ auf alle Grundwerte der Informationssicherheit innerhalb des gesamten Systems auswirken.

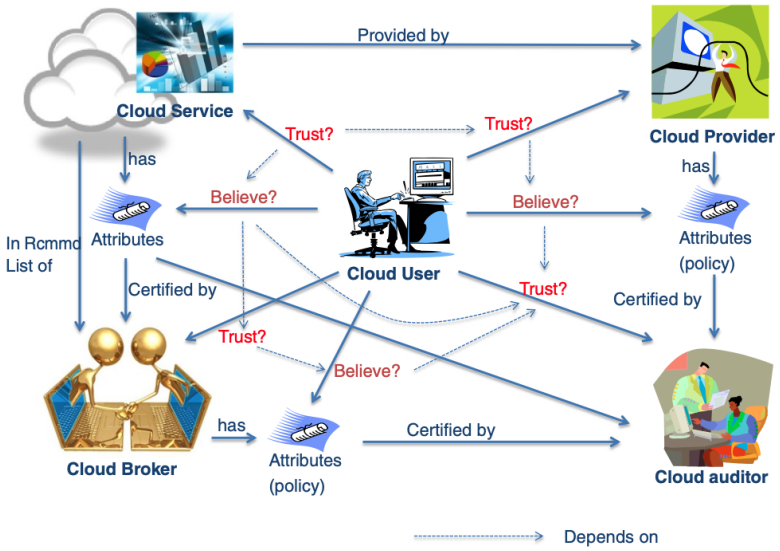

Abbildung 4.3: Beispielhafte Vertrauensketten im Cloud-Kontext mit möglichen Akteuren, wenn ein Ansatz basierend auf Attributen ausgewählt wird. Quelle: [41].

Auf der organisatorischen Ebene, wie in Abbildung 4.3 zu erkennen, gibt es weitere relevante Trust-Chains bei der Nutzung von Cloud-Computing. Besonders der Cloud-Nutzer muss dabei viele Trust-Chains evaluieren, zum Beispiel in Richtung eines Cloud-Dienstes, eines Cloud Broker oder eines Cloud-Anbieters. Während Cloud-Anbieter und Broker inzwischen weitere Institutionen wie zum Beispiel Cloud-Auditoren nutzen, um ihre Vertrauenswürdigkeit mithilfe bestimmter Attribute zu verifizieren, ergeben sich dadurch für den Cloud-Nutzer nur noch weitere Trust-Chains und ein komplexes Konstrukt entsteht. Hinsichtlich dessen ist ein fundiertes Trust-Management also essenziell, um den Vertrau-

ensfluss innerhalb der vielen verschiedenen Ketten angemessen steuern und das Risiko für Fehlentscheidungen minimieren zu können.

Insbesondere die Trust-Chain zwischen dem Cloud-Nutzer und dem Cloud-Anbieter (3) kann bei einem Vertragsabschluss und der Migration der eigenen Anwendungen in dessen Systeme eine entscheidende Rolle einnehmen [81]. Um hier einen möglichst risikoarmen Vertrauensfluss zu schaffen, wenden Firmen verschiedene Systeme des Trustmanagements an, wie zum Beispiel Service-Level-Agreement-basierte Ansätze, Reputation-basierte Ansätze oder Ansätze basierend auf Empfehlungen [41]. Wird allerdings ein falscher Ansatz gewählt und falsche Vertrauensflüsse entstehen, so kann eine Cloud-Umgebung ausgewählt und genutzt werden, die möglicherweise nicht den eigenen Anforderungen entspricht. Dies kann vorwiegend kritische Auswirkungen haben, wenn die Anforderungen im Bereich der allgemeinen Sicherheit, des Datenschutzes oder der Verfügbarkeit nicht erfüllt werden. Da hier verschiedenste Szenarien das Schutzniveau des Systems negativ beeinträchtigen können, können als Folge auch die Grundwerte der Informationssicherheit in Rahmen des gesamten Systems negativ beeinflusst werden.

Weil es sich hierbei lediglich um einen Auszug an Bedrohungen und deren mögliche Folgen für das System handelt, ist es essenziell, dass eine solche Analyse detailiert für das individuelle Anwendungsszenario fortgeführt wird und Vertrauensflüsse mit einem geeigneten Ansatz des Trust-Managements gesteuert werden.

B23: Schlechtes Keymanagement

Auch wenn möglicherweise ein hoher Grad von Trust zwischen dem Cloud-Anbieter und dem Stakeholder einer Cloud-Umgebung (hier Kunden der MakeABank GmbH) besteht, sollten sensible Daten in der Cloud unbedingt verschlüsselt werden. Geschieht dies nicht, könnte es einerseits passieren, dass bei der Kompromittierung sensibler Daten diese nach einem Angriff den Angreifern in Klartextform in die Hände fallen und damit zu bösartigen Zwecken verwendet werden können. Andererseits könnten auch bei Fehlern des Cloud-Anbieters bezüglich einer vollständigen Datenlöschung oder Datenisolation zwischen den Nutzern unberechtigte Dritte diese ohne größere Hürden abfangen und missbrauchen.

Jedes System, welches mit Schlüsseln für eine solche Datenverschlüsselung arbeitet, kann als Keymanagementsystem bezeichnet werden. Das System führt dabei im Rahmen des Keymanagements Aufgaben aus wie die Erstellung, das Teilen und das Nutzen von Schlüsseln zur Verschlüsselung beziehungsweise Entschlüsselung von Daten. Zudem werden Schlüssel auch durch Überschreibung zerstört. Die Übertragung sicherheitsrelevanter

Schlüsselinformation im Rahmen von Verschlüsselungsprotokollen gehört ebenfalls dazu. Begründet durch den hohen funktionellen Umfang basiert die Sicherheit eines Systems, welches kryptografische Methoden zur Datenverschlüsselung einsetzt, immer auf den Fähigkeiten und der Sicherheit des Keymanagements [96].

Im Zuge der Umsetzung eines Key-Management Systems lassen sich zwei Strategien für die Verschlüsselung verfolgen. Einerseits gibt es die Möglichkeit der clientseitigen Verschlüsselung. Hier werden die Daten direkt beim Client verschlüsselt und somit bereits vollständig verschlüsselt zum Endpunkt der Cloud geschickt [114]. Andererseits gibt es die Möglichkeit einer serverseitigen Verschlüsselung. Im Zuge dieser, treffen die Daten unverschlüsselt[14] am öffentlichen Endpunkt der Cloud ein, werden durch das Netzwerk des Cloud-Anbieters zum endgültigen Speichermedium weitergeleitet und dort verschlüsselt. Diese Verschlüsselung und dazugehörige Schlüssel werden durch den Cloud-Anbieter durchgeführt beziehungsweise verwaltet [70].

Werden Anforderungen des Keymanagements bezüglich einer Verschlüsselungsstrategie falsch eingeschätzt und beispielsweise auf eine clientseitige Verschlüsselung verzichtet, so können sensible Daten während der Übertragung im Netzwerk des Cloud-Anbieters von den physischen Komponenten wie zum Beispiel dem Server problemlos entschlüsselt und in Klartext gelesen werden. Selbst wenn eine Ende-zu-Ende-Verschlüsselung wie beispielsweise ein Transport der Daten mittels des Verschlüsselungsprotokolls TLS umgesetzt wird, so sind die Daten lediglich während der Übertragung zwischen zwei Komponenten verschlüsselt. In diesem Fall können beide an der Kommunikation teilnehmende Komponenten jedoch die Daten für sich entschlüsseln [24]. Da der Server des Cloud-Endpunktes in der Regel nicht gleichfalls der Speicherort der Daten ist, sondern Daten im Netzwerk des Cloud-Anbieters über mehrere Komponenten geschickt werden können, werden angreifenden Personen mehrere Angriffspunkte geboten. Zudem ist es so für den Cloud-Anbieter möglich, die Daten mitzulesen. Diese Sachlage kann sich dies negativ auf das Sicherheitsniveau in Bezug auf die Vertraulichkeit und Integrität von Daten innerhalb des Systems auswirken. Insbesondere bezüglich Daten, die als rechtlich besonders schützenswert deklariert sind, können sich juristische Probleme ergeben. Dies liegt vor allem darin begründet, dass ein Cloud-Anbieter so potenziell die Möglichkeit eines Zugriffs auf die unverschlüsselten und schützenswerten Geschäftsdaten ausüben kann. Insbesondere falls es sich dabei um einen amerikanischen Cloud-Anbieter mit grundlegend anderen

[14] Unverschlüsselt bedeutet hier, dass Daten trotzdem durch eine End-to-End Verschlüsselung, zum Beispiel im Rahmen von den Kommunikationsprotokoll HTTPS beziehungsweise TLS geschützt sind, aber vom Kommunikationspartner problemlos entschlüsselt werden können.

Datenschutzbestimmungen handelt, reicht dies schon für entsprechende juristische Folgen aus, solange ein Unternehmen nicht beweisen kann, dass bisher garantiert noch kein Zugriff stattgefunden hat. Die mögliche Relevanz dieser Problematik kann mittels des amerikanische *CLOUD Acts* aufgezeit werden. Diese Regelung soll es US-Behörden ermöglichen, auf Daten von US-Unternehmen zur Strafverfolgung außerhalb des eigenen Hoheitsgebiets zugreifen zu dürfen. Durch die DSGVO wird dies allerdings verboten und ein solcher Datenabfluss unter hohe Strafen gestellt [3]. Geschieht jedoch nun ein solcher Datenabfluss und es fallen hier hohe Strafen an, kann eine zusätzlich eine Gefahr für den generellen Betrieb in der Cloud entstehen, was sich dementsprechend negativ auf den Grundwert der Verfügbarkeit auswirkt.

Auch wenn Cloud-Anbieter einen vollständig verwalteten Cloud-Dienst mit einer starken Verschlüsselung und ein Keymanagement anbieten, so gilt dies oftmals nur für ruhende Daten. Ruhende Daten sind Daten, die auf dem endgültigen physischen Speichermedium liegen, also bereits vollständig zum Zielort übertragen wurden [23]. Hier gilt das Prinzip der serverseitigen Verschlüsselung. Falls ein solcher Cloud-Dienst verwendet wird, kommt zusätzlich der Aspekt dazu, dass oftmals unklar ist wo sich verwendete Schlüssel im System befinden, welche Schlüssel verwendet wurden und ob diese wirklich den Sicherheitsansprüchen genügen. Die Kontrolle über die Schlüssel und Verschlüsselungsalgorithmen, ferner über jegliche verschlüsselte Daten, liegt damit nicht mehr in der eigenen Institution.

4.4.7 Dienstnahe Bedrohungen

Nr.	**Bedrohung**	**identifiziertes System**	**beinträchtigte Grundwerte**
24	Ungesicherte Cloud-Anbieter API	A001: MaBCloud Frontend, A002: MaBCloud Backend, A003: objektrelationales Datenbanksystem	A,C,I
25	Malware	A001: MaBCloud Frontend, A002: MaBCloud Backend, A003: objektrelationales Datenbanksystem	A,C,I

Tabelle 4.7: Übersicht der dienstnahen Bedrohungen

B24: Ungesicherte API von Cloud-Diensten

In der Regel stellen Cloud-Anbieter den Kunden eine bestimmte Menge an sogenannten Application Programming Interfaces (APIs) zur Verfügung. Das sind festgelegte Interfaces beziehungsweise Schnittstellen, über die zwei Software-Komponenten miteinander kommunizieren können. Eine Schnittstelle kann dabei als eine Art Servicevertrag angesehen werden, der definiert wie die Anfrage und Antwort aussehen müssen. Zudem besitzt jede Schnittstelle einen Endpunkt wie zum Beispiel eine URL, an die entsprechende Daten geschickt und empfangen werden können und die als Berührungspunkt der Komponente gilt [5].

Aus diesem Application Programming Interfaces entstehen konkrete Bedrohungen für das System, wenn diese nicht ausreichend gesichert sind. Um hier ein konkretes Szenario zu nennen liegt nun eine Software-Komponente als Client in Form eines Webbrowser vor, die andere Komponente wird als ein beliebiger Cloud-Dienst modelliert. Als Fallbeispiel für diesen Cloud-Dienst kann beispielsweise der durch Google bereitgestellte Datenbankdienst Cloud-SQL[15], der im Rahmen eines Google Cloud Abonnement erhältlich ist, exemplarisch verwendet werden. Dies ist ein durch Google verwalteter Datenbankdienst, der für Kunden nutzbare Datenbanken und einige weitere Funktionalitäten bereitstellt. Der Kunde kann für diesen Cloud-Dienst indessen konfigurieren, welche Nutzer, mit welchen Anmeldedaten, über welche Authentifizierungstechnologie und auf welche Funktionalität der API von Cloud-SQL zugreifen darf. Bei entsprechender Konfiguration könnte ein autorisierter Client beispielsweise Live-Daten durch Anfragen an den Endpunkt der Cloud SQL API löschen, ebenso wie durchgeführte Datensicherungen [35].

In diesem exemplarischen Szenario besteht also einerseits ein Abhängigkeitsverhältnis zu dem Dienst-Anbieter insofern, als dieser die API bereits ausreichend gegen jegliche Browser-basierte Angriffe abgesichert hat. Andererseits kann im Zuständigkeitsbereich des Kunden keine oder nur eine unzureichende Autorisierung eingerichtet, eine zu breite Rechtevergabe für das Nutzen von Funktionalitäten konfiguriert, sowie Anmeldedaten unverschlüsselt zwischen den beiden Software-Komponenten verschickt werden [78].

Die beschriebenen Szenarien können zur Folge haben, dass ein Angreifer unautorisierten Zugriff auf Schnittstellen von Cloud-Diensten erhält und so unautorisiert bösartige Aktionen durchführen kann, die ein Leck von sensiblen Daten als Folge haben oder einen vollständigen Datenverlust nach sich ziehen können [78]. Dadurch können alle Grundwerte der Informationssicherheit innerhalb des gesamten Systems verletzt werden. Insgesamt

[15] https://cloud.google.com/sql

hängt damit die Sicherheit der Cloud sehr eng mit der Sicherheit der API zusammen [98].

Eine weitere Bedrohung im Zusammenhang mit unsicheren APIs liegt in der Art und Weise der Nutzung durch Dienste, welche nicht direkt vom Cloud-Anbieter bereitgestellt werden, sondern von weiteren Externen. Haben Unternehmen nun also so spezifische beziehungsweise umfangreiche Anforderungen an die Funktionalitäten eines Dienstes, dass ein Cloud-Anbieter dies mit dem eigenen Repertoire an Diensten nicht mehr bedienen kann, so kann unter Umständen ein externer Dienst genutzt werden. In einem solchen Szenario involviert eine weitere Institution mit ihrem Dienst eine weitere Ebene in die Zugriffskaskade, sodass ein gewisser Grad an Kontrolle verloren geht, die Komplexität steigt und der externe Dienst möglicherweise die API eines Cloud-Dienstes auf eine unsichere Art und Weise nutzen könnte [98]. Auch in einem solchen Szenario wären Szenarien möglich, welche die Integrität, Vertraulichkeit und Verfügbarkeit gefährden können.

B25: Malware

Als Malware wird Software bezeichnet, die mit dem Ziel entwickelt wurde, unerwünschte und meist schädliche Funktionen auf einem IT-System aufzuführen. In der Regel soll dies ohne das Wissen des Benutzers geschehen. Installierte Malware kann dabei verschiedene Ziele verfolgen. Einerseits kann eine Ransomware direkt auf die Ressourcen eines IT-Systems abzielen, diese verschlüsseln und vom Besitzer der Daten eine finanzielle Leistung zur Entschlüsselung verlangen, andererseits kann Malware in Form von Spionagesoftware still Systeme bezüglich sensibler Daten ausspionieren [49]. Ein drittes existierendes Szenario ist die Installation von sogenannter Botware, um die Cloud-Umgebung in ein Botnetz zu integrieren.

Angreifer kontrollieren in einem Botnetz häufig tausende von IT-Systemen und können dies verwenden, um Denial-of-Service-Angriffe zu starten oder Spam zu versenden, beispielsweise durch das massenhafte Versenden von böswilligen E-Mails. In der Regel wird dadurch die eigene Institution nicht direkt geschädigt, aber trotzdem können sich Folgen negativ auf die Verfügbarkeit und Integrität des eigenen Systems auswirken und sogar in rechtliche Probleme resultieren. Dies beschreibt das BSI im Zuge des Kompendium für den generellen Betrieb eines IT-Systems [14]. Im Kontext des Cloud-Computings findet hier trotzdem eine direkte Schädigung gegen die Institution statt, da für das Mitwirken in einem Botnetz einerseits generell Ressourcen durch die Angreifer beansprucht werden und andererseits können diese Ressourcen durch die Elastizität einer Cloud sogar potenziell bis an die Limits hochskaliert werden. Dadurch könnte eine Cloud-Umgebung

dem Botnetz für missbräuchliche Zwecke so tendenziell mehr Ressourcen zur Verfügung stellen als die meisten On-Premises Infrastrukturen. Für die MakeABank GmbH können durch die nutzungsbasierte Abrechnung hohe Mehrkosten entstehen, die möglicherweise den Betrieb von „MaBCloud“ in der Cloud gefährden.

Zusätzliches Bedrohungspotenzial entsteht des Weiteren unter dem Aspekt, dass tagtäglich schätzungsweise 1 Million neue Varianten von Malware-Software entstehen. Die meisten davon sind verbesserte Versionen von bereits existierenden Malware-Anwendungen [7]. Diese verbesserten Versionen implementieren immer neue Kaschierungstechniken in Bezug auf Verschleierung und eine nach außen täuschende Präsentation des Schadprogramms. So ist es nahezu unmöglich für konventionelle Erkennungsmethoden komplexe Malware-Anwendungen als solche richtig zu klassifizieren [7]. Malware kann dadurch länger beziehungsweise gänzlich unerkannt agieren und die Vertraulichkeit, Integrität und Verfügbarkeit direkt und zunehmend bedrohen. Auch für die Cloud-Umgebung der MakeABank GmbH sind solche Szenarien möglich.

4.5 Risikoeinstufung

Nachdem nun die Gefährdungsübersicht für ausgewählte Bedrohungen abgeschlossen wurde, erfolgt die Einstufung des dazugehörigen Risikos. In der Risikoeinstufung werden konkrete Risiken für die jeweiligen Bedrohungen und Zielobjekte erarbeitet. Mit einem solchen Risiko soll primär für jedes Zielobjekt des Informationsverbundes bestimmt werden, welcher Handlungsbedarf in Bezug auf eine vorliegende Bedrohung besteht. In einem nächsten Schritt sollen damit entsprechende Maßnahmen erarbeitet werden, damit die vorliegenden Informationssicherheitsrisiken ausreichend behandelt werden können. Auch hier stützen sich das durchgeführte Vorgehen und folgende Inhalte größtenteils an der empfohlenen Vorgehensweise des IT-Grundschutzes. Insbesondere der BSI Standard-200-3 nimmt diesbezüglich eine zentrale Rolle ein [18].

Wie durch das BSI, im Rahmen des Standards empfohlen, wird auch in dieser Arbeit das Risiko maßgeblich durch zwei Parameter bestimmt. Einerseits werden dazu die Eintrittshäufigkeit ohne zusätzliche Maßnahmen und andererseits die Auswirkungen ohne zusätzliche Maßnahmen in Betracht gezogen werden. Dabei werden die Eintrittshäufigkeit und die Auswirkungen individuell anhand der jeweiligen Bedrohung für jedes Zielobjekt des Informationsverbunds bestimmt. Während im Rahmen der Eintrittshäufigkeit häufig Statistiken bei einer Einschätzung unterstützend verwendet werden können, kann

der Risikoanteil der Schadenshöhe lediglich individuell durch die MakeABank GmbH für das vorliegende Anwendungsszenario bestimmt werden.

Nachdem die genutzten Parameter für die Risikoeinstufung innerhalb dieser Arbeit festgelegt wurden, können nach IT-Grundschutz, Risiken nun entweder qualitativ oder quantitativ bestimmt werden. Für eine quantitative Vorgehensweise ist jedoch umfangreiches statistisches Material nötig, weshalb im Rahmen dieser Arbeit eine qualitative Vorgehensweise genutzt wird [18]. Für eine solche empfiehlt das BSI indessen sowohl für den Parameter der Eintrittshäufigkeit als auch für den Parameter der Auswirkungen verschiedene Kategorien. Auch diese werden im Rahmen dieser Arbeit vollständig übernommen. Dazu erscheint im Folgenden eine erste Übersicht mit den hier verwendeten Kategorien der Eintrittshäufigkeit und der damit verbundenen konkreten Eintrittshäufigkeit.

Eintrittshäufigkeit (Kategorie)	**konkrete Eintrittshäufigkeit**
selten	Höchstens alle 5 Jahre
mittel	Einmal alle 5 Jahre bis einmal im Jahr
häufig	Einmal im Jahr bis einmal im Monat
sehr häufig	Mehrmals im Monat

Tabelle 4.8: Genutzte Kategorien für den Parameter der Eintrittshäufigkeit. Übernommen aus: [18]

In Bezug auf den zweiten Parameter, der Auswirkungen beziehungsweise Schadenshöhe, folgt ebenfalls eine Übersicht mit den hier verwendeten Kategorien und der damit verbundenen konkreten Schadensauswirkung.

Schadenshöhe (Kategorie)	Schadenauswirkung
vernachlässigbar	Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadenauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadenauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 4.9: Genutzte Kategorien für den Parameter der potenziellen Schadenshöhe. Übernommen aus: [18]

Mithilfe der festgelegten Kategorien für beide genannten Parameter wird nun mithilfe einer Matrix eine konkrete Risikokategorie abgeleitet, die letztendlich das Risiko definiert. Auch hierfür wird durch das BSI, im Rahmen des BSI Standard 200-3 [18], eine mögliche Matrix gegeben. Wie schon jegliche Parameter und mögliche Kategorien, wird auch diese hier vollständig übernommen und angewendet. Zur Veranschaulichung erfolgt eine Darstellung in nachfolgender Abbildung 4.4.

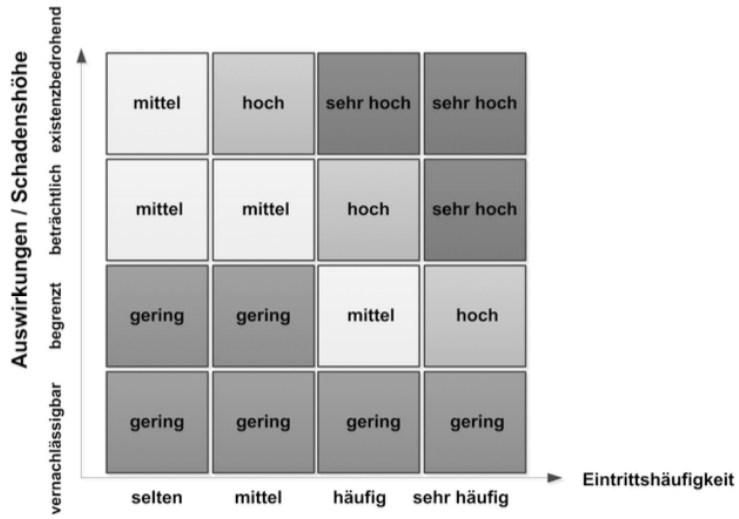

Abbildung 4.4: Vom BSI im Rahmen des BSI Standard 200-3 gegebene Matrix zur Bewertung einer Risikokategorie. Übernommen aus: [18]

Abschließend folgt eine konkrete Übersicht zu genannten Risikokategorien, welche durch die Matrix pro Zielobjekt und Bedrohung bestimmt werden. Jede Risikokategorie definiert dabei einen Richtwert bezüglich des Handlungsbedarfs und zeigt auf, ob und wie gravierend dieser vorliegt. Auch die im Rahmen dieser Arbeit ausgewählten Maßnahmen und Handlungsempfehlungen orentieren sich an diesen ermittelten Risikokategorien.

Risikokategorien	
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die Schadenauswirkungen können ein existenziell bedrohliches, katastrophales Außmaß erreichen.

Tabelle 4.10: Genutzte Risikokategorien mit entsprechender Beschreibung. Übernommen aus: [18]

Als Ergebnis dieser Risikoeinstufung sollte also mithilfe der Parameter und der gegebenen Matrix, für jede Bedrohung pro Zielobjekt des Informationsverbundes eine konkrete Risikokategorie bewertet worden sein. Schon umgesetzte Sicherheitsmaßnahmen sollten dabei bereits berücksichtigt werden. Mithilfe des bestimmten Risikos soll so der konkrete Handlungsbedarf pro Bedrohung in Bezug auf die Umsetzung von Sicherheitsmaßnahmen festgestellt werden [18] und direkt in die Auswahl von Maßnahmen und Handlungsempfehlungen einfließen. Jedoch muss auch dieses Ergebnis durch den beschränkten Rahmen dieser Arbeit eingeschränkt werden. So können nicht alle klassifizierten Risiken der 25 Bedrohungen ausführlich begründet werden. Dementsprechend wird lediglich eine Auswahl an Risiken für den gesamten Informationsverbund näher begründet, welche mit der höchsten Risikokategorie „sehr hoch“ klassifiziert wurden. Eine vollständige Risikoeinstufung für alle andere Risiken pro Bedrohungen und Zielobjekt ist bei Bedarf jedoch im Anhang A.2 zu finden. Dort können mithilfe entsprechender Beschreibungen und Bewertungen die jeweiligen Risikokategorien in ihrer Gesamtheit nachvollzogen werden.

Als eine weitere Einschränkung wird der gesamte Informationsverbund wie ein konkretes Zielobjekt innerhalb der Risikoeinstufung behandelt, obwohl dieser eigentlich lediglich die abstrakte Menge aller erarbeiteten Zielobjekten aus der Strukturanalyse darstellt. Dadurch ist dieser bezüglich einer Risikoeinstufung nach IT-Grundschutz kein gewöhnliches Zielobjekt für eine Risikoeinstufung. Durch diese Vereinfachung fällt eine explizite Risikoeinstufung speziell für Zielobjekte der Kommunikationsverbindungen (K001 und K002) sowie der IT-Systeme (S001) gänzlich weg, da diese somit bereits in der Risikoeinstufung für den gesamten Informationsverbund berücksichtigt werden. Aus diesem Grund können diese auch innerhalb der vollständigen Risikoeinstufung im Anhang A.2 nicht als ein konkretes Zielobjekt wiedergefunden werden. Diese Entscheidung wurde innerhalb dieser Arbeit getroffen, da sich im Kontext des Cloud-Computings sehr viele Bedrohungen gegen den gesamten Informationsverbund richten und so hier eine höhere Vollständigkeit erreicht werden kann.

4.5.1 gesamter Informationsverbund

Im Folgenden werden die Bedrohungen gegen den gesamten Informationsverbund mit einer als *sehr hoch* klassifizierten Risikokategorie für das vorliegende Anwendungsszenario näher erläutert.

1. **B1: Unzureichendes Notfallmanagement** Die erste Bedrohung mit der Risikokategorie *sehr hoch* ist *B1: Unzureichendes Notfallmanagement*. Ein Notfallmanagement wurde zwar durch die MakeABank GmbH nach bestem Wissen für alle bekannten Notfallszenarien bezüglich des Betriebs von „MaBCloud“ in der Cloud ausgearbeitet, konnte allerdings bisher nicht in einem realen Betrieb getestet werden. Zudem kann angenommen werden, dass nach einem Umstieg von einem On-Premises System in eine Cloud-Umgebung möglicherweise das breite Fachwissen für Bedrohungen im Zusammenhang mit dem Cloud-Computing fehlt. So erhöht sich die Gefahr, dass nicht alle Cloud-spezifische Angriffsszenarien ausreichend berücksichtigt sind und dass das Notfallmanagement diesbezüglich in den ersten Versionen Lücken enthält. Zudem erstreckt sich das Notfallmanagement durch das Dienstleistungsverhältnis mit den Kunden über mehrere Institutionen. Dementsprechend kann auf die Umsetzung des Notfallmanagements auf Seite des Kunden lediglich beschränkter Einfluss genommen werden. Jedoch kann aus historischen Erfahrungswerten abgeleitet werden, dass gerade in Bezug auf Präventionsmaßnahmen wie einem Notfallmanagement, Ressourcen tendenziell eingespart werden. So

kann möglicherweise keine angemessenen Integration des erarbeiteten Notfallmanagements in die Prozesse des Kunden stattfinden. Um hier von dem schlimmsten Fall auszugehen, erhält diese Bedrohung präventiv eine Eintrittshäufigkeit der Kategorie *häufig*. Die Auswirkungen eines unzureichenden Notfallmanagements werden als *existenzbedrohend* klassifiziert. Liegt kein Notfallmanagement vor oder wurde es nur unzureichend umgesetzt, so steht Angreifenden schlichtweg mehr Zeit zur Verfügung, um weitere Komponenten zu infizieren, mehr schützenswerte Geschäftsdaten zu entwenden, Datensicherungen zu löschen oder andere negative Einflüsse auf die Infrastruktur auszuüben. Die Vertraulichkeit und Integrität der Daten kann so derart verletzt werden, dass dies existenzbedrohende Konsequenzen nach sich ziehen kann. Des Weiteren kann sich die Zeitspanne, in der ein System nicht verfügbar ist, ebenfalls verlängern, sodass im schlimmsten Falle insgesamt alle Grundwerte *existenzbedrohend* geschädigt werden können.

2. **B8: Vendor lock-in** Eine zweite Bedrohung mit der Risikokategorie *sehr hoch* ist *B8: Vendor lock-in*. Bereits die Eintrittshäufigkeit kann als *sehr häufig* kategorisiert werden. Wie schon im Zuge der Bedrohungsübersicht erwähnt, vertreten Cloud-Anbieter selbst ein spürbares Interesse an einem Vendor lock-in. Dementsprechend werden mit hoher Wahrscheinlichkeit auch bei dem ausgewählten Cloud-Anbieter der MakeABank GmbH diverse Funktionen gezielt durch Vendor Lock-in Mechanismen des Anbieters restriktiert sein. Im Falle von „MaBCloud“ dürfte dies bereits bei der Integration beziehungsweise Nutzung von geplanten Cloud-Diensten wie beispielsweise der virtuellen Firewall (A004) oder den virtuellen Loadbalancern (A006) eintreffen. Hier kann die MakeABank GmbH die Konfigurationen dieser Dienste in der Regel nicht automatisiert in Umgebungen von anderen Cloud-Anbietern übertragen. Noch weiter gefasst müsste bereits die grundlegende Netztopologie bei der Nutzung von anbieterspezifischen Cloud-Diensten jeweils händisch rekonfiguriert und angepasst werden, bevor diese in die Umgebung eines anderen Cloud-Anbieters integriert werden kann. Anhand dieser wenigen Beispiele ist bereits davon auszugehen, dass das Vendor lock-in mit einer Eintrittshäufigkeit der Kategorie *sehr hoch* klassifiziert werden kann. Des Weiteren können auch hier die Auswirkungen *beträchtlich* sein. Angenommen ein Cloud-Anbieter verändert die Rahmenbedingungen bezüglich des Datenschutzes, sodass die Anforderungen nicht mehr erfüllt werden, kann ein schneller Umstieg auf eine andere Cloud-Umgebung verhindert werden. Da die Verfügbarkeit von „MaBCloud“ allerdings um jeden Preis sichergestellt werden muss, kann es zu einer Übergangsphase kommen, in der so möglicher-

weise beträchtlichen Auswirkungen bezüglich der Vertraulichkeit und Integrität von schützenswerten Geschäftsdaten auftreten können. Zusammenfassend ergeben die beiden Parameter damit eine Einstufung des Risikos innerhalb der Risikokategorie *sehr hoch*.

3. **B16: Denial of Service** Die Bedrohung *B16: Denial of Service* stellt aus verschiedenen Gründen die Risikokategorie *sehr hoch* für das System dar. Einerseits lässt sich statistisch belegen, dass global agierende Unternehmen im letzten Quartal von 2022 durchschnittlich 29,3 Denial of Service Attacken pro Tag auf die IT-Infrastruktur zu verzeichnen hatten [85]. Andererseits kann im vorliegenden Szenario angenommen werden, dass dieser Durchschnittswert wahrscheinlich noch höher ausfallen wird, da es sich um ein Anwendungsszenario innerhalb der kritischen Infrastruktur der EU handelt und damit möglicherweise als Angriffsziel in einem besonderen Fokus steht. Von daher trifft für diese Bedrohung eine *sehr häufige* Eintrittswahrscheinlichkeit ohne weitere Maßnahmen ein. Allerdings sind auch die möglichen Auswirkungen *beträchtlich*. Aus dem öffentlichen Internet ist der Loadbalancer (A006) für die virtuellen Maschinen des „MaBCloud“ Frontends (A001) beziehungsweise die davor geschaltete Firewall (A004) erreichbar. Sollte diese Firewall im Rahmen eines Denial of Service Angriffes beispielsweise derart mit Anfragen überflutet werden, dass diese selbst im Rahmen einer maximalen Skalierung die Anfragen nicht mehr verarbeiten kann, so können auch keine regulären Anfragen mehr das dahinterliegende System erreichen. Damit wäre das System nicht mehr verfügbar, was in Anbetracht des vorliegenden Sektors innerhalb der kritischen Infrastruktur zu *beträchtlichen* Auswirkungen führen kann. Die Risikokategorie ist damit ebenfalls *sehr hoch*.

4. **B21: Social Engineering** Auch die Bedrohung *B21: Social Engineering* erhält eine *sehr hohe* Risikokategorie. Bereits die Häufigkeit des Angriffes gibt hier einen ersten Anhaltspunkt. So erlebt ein durchschnittliches Unternehmen circa 2,7 Angriffe im Zusammenhang mit Social Engineering pro Tag [89]. Wie bereits erwähnt, ist im vorliegenden Anwendungsszenario auch hier ein tendenziell höherer Durchschnitt erwartbar. Eine *sehr häufige* Eintrittshäufigkeit ist damit gegeben. Aufgrund des Unsicherheitsfaktors Mensch können auch hier die die Auswirkungen *beträchtlich* sein. So lassen sich Social Engineering Angriffe nur begrenzt mit technischen Sicherheitsmaßnahmen präventiv verhindern. Sollten Angreifende durch das Social Engineering Zugangsdaten für ein Benutzerkonto von „MaBCloud“ erhalten und ebenfalls durch komplexe Täuschungsstrategien durch die Multi-Faktor-

Authentifizierung des Identitätsdienstes des Cloud-Anbieters kommen, so können zwar keine direkten Änderungen an der Infrastruktur, sowie Datensicherungen oder Konfigurationen der Cloud-Umgebung vorgenommen, es könnten aber besonders schützenswerte Geschäftsdaten in einem hohen Umfang eingesehen sowie verwaltende Aktionen durchgeführt werden. Insbesondere die Auswirkungen bezüglich der Vertraulichkeit und Integrität von Geschäftsdaten wäre beträchtlich. Damit ergibt sich auch hier eine insgesamt *sehr hohe* Risikokategorie.

5. **B22: Schlechtes Trustmanagement** Die letzte Bedrohung mit einem sehr hohen Risiko für den gesamten Informationsverbund ist *B22: Schlechtes Trustmanagement*. Dadurch, dass eine hohe Anzahl von sehr weitläufigen Trust-Chains innerhalb des Informationsverbunds sowohl auf technischer als auch auf organisatorischer Ebene existieren, kann das Trustmanagement als ein komplexes Konstrukt angesehen werden. Da es sich bei „MaBCloud“ um eine Anwendung handelt, die viele Abhängigkeiten in der Implementierung verwendet und das Gesamtsystem auf viele verwaltete Cloud-Dienste wie zum Beispiel der virtuellen Firewall (A004) oder die virtuellen Loadbalancern (A006) zurückgreift, kann davon ausgegangen werden, dass es nicht möglich ist, für jede Abhängigkeit den Vertrauensfluss durch ein angemessenes Trustmanagement zu steuern. Insbesondere unter der zusätzlichen Annahme, dass Abhängigkeiten vermutlich weitere Ketten von externen Abhängigkeiten für die eigene Funktionalität verwenden, kann kein angemessenes Trustmanagement für alle Ketten umgesetzt werden und damit wird die Eintrittshäufigkeit hier als *hoch* eingeschätzt. Bezüglich der Auswirkungen gilt hier das Maximumprinzip, sodass der schlimmst-mögliche Fall angenommen wird. Falls in diesem durch ein unangemessenes Trustmanagement, ein zu hoher Vertrauensfluss zu einem bösartigen Cloud-Anbieter aufgebaut wird, können verschiedenste Auswirkungen möglich sein. Cloud-Anbieter könnten beispielsweise gegen den Datenschutz verstoßen, Konfigurationen speziell bezüglich der Datensicherung und Replikation nicht umsetzten, versteckte Kosten in Rechnung stellen oder andere versprochene Sicherheitsstandards nicht einhalten. Die Auswirkungen können sich so, je nach Szenario, *existenzbedrohend* auf alle Grundwerte der Informationssicherheit auswirken.

Nach Abschluss der Risikoeinstufung erfolgt nun eine Risikobehandlung auf Basis der herausgearbeiteten Risikokategorien. Unter der Annahme, dass von einer Institution in der Regel nur „geringe“ Risiken akzeptiert werden, gibt das BSI verschiedene Strategien

vor, wie Risiken entsprechend behandelt werden können. Diese stammen aus [18] und im Detail können Risiken hier

- **vermieden** werden, indem beispielsweise die Risikoursache ausgeschlossen wird,
- **reduziert** werden, indem die Rahmenbedingungen, die zur Risikoeinstufung beigetragen haben, modifiziert werden,
- **transferiert** werden, indem die Risiken mit anderen Parteien geteilt werde,
- **akzeptiert** werden, beispielsweise weil die mit dem Risiko einhergehenden Chancen wahrgenommen werden sollen.

Durch die hohe Relevanz einer angemessenen Informationssicherheit für das vorliegende Anwendungsszenario, wird eine Akzeptanz von Risiken als Strategie möglichst vermieden. Wie bereits erwähnt, können lediglich geringe Risiken akzeptiert werden, weshalb es im folgenden Kapitel darum gehen wird, die ermittelten Risikokategorien so weit zu behandeln, dass ein solch niedriges Niveau erreicht werden kann.

Um dieses übergeordnete Ziel zu erreichen, werden im Nachfolgenden geeignete Sicherheitsmaßnahmen vorgestellt. Im Zuge dessen wird zudem eine Empfehlung ausgesprochen, in welchem Rahmen und zeitlicher Reihenfolge die vorgestellten Maßnahmen umgesetzt werden sollten, um das Risiko optimal zu behandeln.

4.6 Evaluation

4.6.1 Maßnahmen

So erfolgt nun die angesprochene Vorstellung der ausgewählten Sicherheitsmaßnahmen für das vorliegende Anwendungsszenario. Dabei besteht auch hier, durch den begrenzten Rahmen dieser Arbeit, kein gänzlicher Vollständigkeitsanspruch. Stattdessen wird eine Auswahl der vermeintlich effektivsten Maßnahmen für die Cloud-Nutzung im vorliegenden Anwendungsszenario vorgestellt.

Nummer	Maßnahme
1	Globale Zero-Trust-Strategie implementieren
2	Nutzung von clientseitiger Verschlüsselung
3	Single Sign-on
4	Multi-Faktor-Authentifizierung
5	Nutzung von Infrastructure as Code
6	Automatisierte Reaktion auf sicherheitskritische Vorfälle
7	Berücksichtigung des Well-Architected Framewoks
8	Sensibilisierung im Rahmen von regelmäßigen Schulungen
9	Erstellung eines Datensicherungskonzeptes
10	Angemessenes Patch- und Änderungsmanagement
11	Durchführung von Monitoring
12	Einrichten von Konten für den Notfallzugriff
13	Erstellung eines Notfallmanagements mittels BSI-Standard 100-4
14	Frühe Ausarbeitung einer Exit-Strategie
15	Nutzung einer Hybrid-Cloud beziehungsweise Multi-Cloud-Architektur
16	Ausreichende Vorausplanung einer Strategie
17	Festlegung der Sensibilität von auszulagernden Daten und Diensten
18	Kommunikationskanäle mit dem Cloud-Anbieter etablieren
19	Möglichst breiter Einsatz von Firewalls

Tabelle 4.11: Übersicht der thematisierten Maßnahmen.

M1: Globale Zero-Trust-Strategie implementieren

Bereits seit 2010 hat sich der Begriff Zero Trust etabliert und stellt seitdem ein großes Forschungsgebiet innerhalb der Informationssicherheit dar [92]. Zero Trust kann dabei als keine konkrete Architektur oder Technologie beschrieben werden, sondern eher als ein Paradigma in Bezug auf den Schutz von Ressourcen in der Cloud angesehen werden [90]. Insgesamt verfolgt Zero Trust den Ansatz, dass keiner Entität im Netzwerk explizit vertraut werden darf, sondern vor jeder Interaktion mit einer Ressource die Autorität und Authentizität geprüft werden muss. Ziel dabei soll es sein, dass lediglich bei absoluter Notwendigkeit auf eine Ressource zugegriffen wird, mit stets möglichst eingeschränkten Rechten [90]. Zudem wurde das Zero-Trust-Paradigma unter der Annahme entwickelt, dass jeder Zugriff bösartig sein und hohen Schaden verursachen kann [92]. Das

sogenannte Worst-Case-Szenario wurde also bereits in den grundlegenden Konzeptionen berücksichtigt, sodass ein insgesamt robustes Konzept entwickelt wurde.

Um nun eine solche und effektive Zero Trust Strategie in der Cloud umzusetzen, müssen einige Komponenten, wie in Abbildung 4.5 schematisch dargestellt, realisiert werden. Dabei wird jeder Zugriff auf eine Ressource durch einen *Policy Enforcement Point (PEP)* geleitet, der diesen Zugriff überwacht und gegebenenfalls unterbindet. Dabei wird mit einem *Policy Decision Point (PDP)* kommuniziert, in dem evaluiert werden muss, ob der Zugriff stattfindet darf oder nicht [90]. Hier findet also die Authentifizierung des Zugriffes beziehungsweise des zugreifenden Kommunikationsteilnehmers statt. Um eine solche Authentifizierung zu implementieren, können verschiedene Algorithmen und Frameworks genutzt werden. Ein exemplarisches Beispiel für die Cloud könnte hier der Ansatz von Google für die Google Cloud im Rahmen der ByondCorp[16] Implementierung sein.

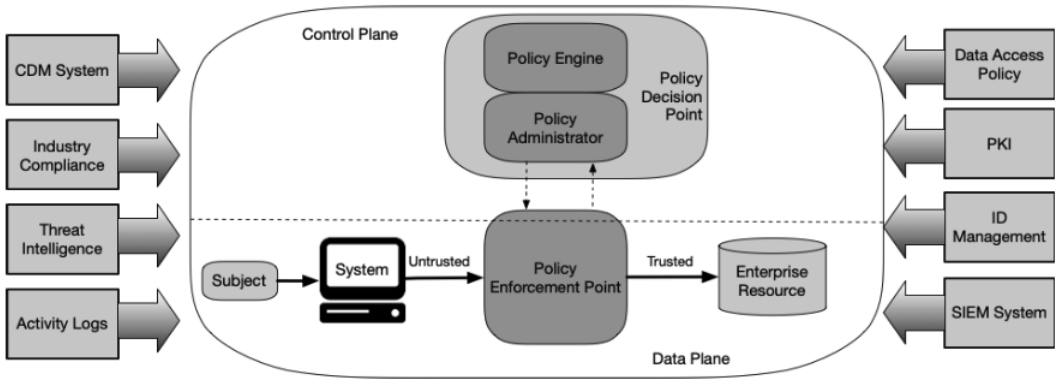

Abbildung 4.5: Notwendige Komponenten für ein schematisches Zero-Trust-Modell. Quelle: [90]

Wird ein solcher Ansatz auch durch die MakeABank GmbH in der Cloud verfolgt, so kann innerhalb der eigenen Cloud-Umgebung die Sicherheit deutlich erhöht werden. Selbst wenn Angreifende durch, mittels Firewall stark gesicherte, Außengrenzen des Systems ins Netz eindringen konnten, so müssen sich diese nun für jeden Zugriff auf eine beliebige Ressource authentifizieren. Dadurch können diese nicht mehr ohne weitere Blockaden auf interne Ressourcen zugreifen, beziehungsweise über verschiedene Ressourcen durch das Netzwerk traversieren. Als ein Resultat können hier Angriffe schneller unterbunden und aufgedeckt werden. Angreifenden fällt es schwer sich so effektiv durch das Netz zu bewegen, dieses auszuspähen und Daten abfließen zu lassen [90]. Zudem wäre

[16] https://cloud.google.com/beyondcorp

die Cloud-Umgebung hier tendenziell robuster gegenüber anderweitigen Konfigurationsfehlern, die einen unautorisierten Zugriff auf Ressourcen ermöglichen könnten. Dementsprechend kann so das Schutzniveau des Systems in Bezug auf alle Grundwerte erhöht werden.

M2: Nutzung von clientseitiger Verschlüsselung

Eine zweite Maßnahme, um das Schutzniveau des Systems zu erhöhen und Risiken zu minimieren, ist die Umsetzung einer clientseitigen Verschlüsselung von Geschäftsdaten. Im Rahmen einer clientseitigen Verschlüsselung werden Geschäftsdaten noch in den internen Strukturen der MakeABank GmbH verschlüsselt und anschließend erst, durch das öffentliche Internet, in die Cloud übertragen. Die Schlüssel werden dabei intern aufbewahrt und durch ein eigenes Keymanagement der MakeABank GmbH verwaltet. Bei der Umsetzung eines solchen Ansatzes muss zwar angenommen werden, dass ein tendenziell hoher Verwaltungsaufwand durch ein eigenes Keymanagement entsteht, in Anbetracht der Sensibilität von den verwendeten Geschäftsdaten dürften hier allerdings die Vorteile tendenziell überwiegen. So kann sichergestellt werden, dass ein Zugriff des Cloud-Anbieters auf unverschlüsselte Daten ausgeschlossen ist, was ansonsten im Rahmen der Datenschutzgrundverordnung rechtliche Folgen nach sich ziehen kann [3]. Andererseits behält die MakeABank GmbH so weiterhin einen hohen Grad an Kontrolle über die Verschlüsselung der Daten und kann die Sicherheit der Verschlüsselung technisch selbst verifizieren. Insbesondere geht es hier um die regelmäßige Rotation von Schlüsseln und die Verwendung eines definitiv sicheren Verschlüsselungsmechanismus, wie zum Beispiel AES, RSA oder Triple DES. So können im Endeffekt ebenfalls alle Grundwerte der Informationssicherheit gestärkt und das Schutzniveau des Systems angehoben werden.

M3: Single Sign-on

Eine weitere Maßnahme stellt die Umsetzung eines Single Sign-on (SSO) Authentifizierungsschemas dar. Dieses Schema erlaubt den Benutzern sich einmal zu authentifizieren, um anschließend verschiedene Dienste im System nutzen zu können [32]. Insgesamt basiert SSO dabei auf einer Trust-Chain zwischen verschiedenen Anwendungen, einem Identitätsprovider beziehungsweise einer SSO-Lösung. Meldet sich der Benutzer bei einer solchen Anwendung mit seinen Zugangsdaten an, so wird durch die SSO-Lösung ein Token generiert und ausgehändigt. Dieser Token liegt in der Regel entweder im JSON oder XML-Format vor und kann anschließend zur automatischen Authentifizierung gegenüber anderen Anwendungen genutzt werden, indem der Token durch die SSO-Lösung verifiziert und ein Zertifikat für die Echtheit ausgestellt wird. Ein solcher Token wird pro

Sitzung im Browser des Benutzers oder auf einem SSO-Server gespeichert und wird nach Ablauf dieser ungültig. Trotz des globalen Authentifizierungsschemas gibt es aber auch weiterhin die Möglichkeit, für bestimmte Anwendungen weitere Authentifizierungsmerkmale zu verlangen, sodass trotz der Verbindung mittels SSO weitere dieser Authentifizierungsmerkmale durch den Benutzer angegeben werden müssen [43]. Im Hinblick auf die Sensibilität von verwendeten Geschäftsdaten im Rahmen von „MaBCloud“ sollte, neben der Nutzung von SSO an sich, auch eine solche Konfiguration evaluiert werden. Durch SSO lässt sich so insgesamt die Nutzbarkeit und Sicherheit des Systems, bei einem richtigen Einsatz, teils deutlich erhöhen. Dies lässt sich einerseits aus der Perspektive des Benutzers damit begründen, dass ein Benutzer so keine größere Menge an Zugangsdaten mehr verwalten beziehungsweise sichern muss und die Wahrscheinlichkeit eines Verlustes beziehungsweise einer Kompromittierung damit sinkt. Aus der administrativen Perspektive andererseits müssen zudem weniger Benutzerkonten verwaltet werden. Insbesondere ist dies in Bezug auf die Stilllegung von nicht mehr notwendigen Benutzerkonten eine der größten Vorteile.

Jedoch müssen für ein sicheres SSO weitere Maßnahmen implementiert werden, da das Risiko besteht, dass Angreifende bei der Fälschung eines Tokens, entsprechend direkten Zugriff auf alle Anwendungen ausüben können. Als Gegenmaßnahme sollten zusätzlich starke Passwörtern der SSO Zugangsdaten und eine Multi-Faktor-Authentifizierung erzwungen werden, welche dieses Risiko deutlich minimieren und die Vorteile von SSO für „MaBCloud“ in der Cloud vollständig ausnutzen [43].

M4: Multi-Faktor-Authentifizierung

Eine solche Multi-Faktor-Authentifizierung sieht vor, dass im Rahmen der Authentifizierung eine Kombination aus zwei Faktoren angegeben werden muss. Dementsprechend reicht eine Single-Faktor-Authentifizierung mittels einer klassischen Benutzernamen-Passwort-Kombination hier nicht mehr aus. Stattdessen muss zusätzlich ein weiterer Faktor, wie zum Beispiel der Besitz eines bestimmten Smartphones, Hardwareschlüssels oder einer E-Email-Adresse nachgewiesen werden. Alternativ wäre hier auch der Einsatz eines biometrischen Faktors wie eines Fingerabdruckes oder einer Gesichtserkennung möglich. Durch den Einsatz eines solchen zweiten Faktors innerhalb des Authentifizierungsvorganges kann das allgemeine Schutzniveau angehoben und besonders kritische Dienste besser geschützt werden [82]. Jedoch müssen hierfür einige Aspekte bezüglich der Wahl eines zweiten besitzenden Faktors beachtet werden. Wird hier beispielsweise das Verifizieren mittels eines Links und der eigenen E-Email-Adresse als zweiter Faktor genutzt und

ein SSO Mechanismus wurde umgesetzt *(vgl. M3: Single Sign-on)*, so können Angreifende gegebenenfalls bereits Zugriff auf das E-Email-Postfach besitzen und den zweiten Faktor selbst bestätigen. Auch der Nachweis über eine SMS Verifizierung kann unsicher sein, genau dann, wenn Angreifende per Social Engineering den Mobilfunkanbieter beeinflusst haben, sodass dieser eine neue SIM-Karte zu der richtigen Nummer an die Angreifenden verschickt hat. Dadurch erhalten auch hier Angreifende Zugang zu diesem Authentifizierungsfaktor. Die vermeintlich sicherste Möglichkeit, um solche Szenarien im Rahmen der Multi-Faktor-Authentifizierung zu vermeiden, ist die Nutzung eines physischen Hardwareschlüssels in Form eines USB-Schlüssels. Hier liegt lediglich das Risiko eines Verlustes vor. Sollten Angreifende an einen solchen verlorenen Schlüssel gelangen, würde immer noch der erste Faktor in Form der Zugangsdaten für eine Authentifizierung fehlen.

M5: Nutzung von Infrastructure as Code

Eine weitere Maßnahme, um unter bestimmten Bedingungen das sehr hohe Risiko des Vendor lock-ins zu behandeln, ist die breite Verwendung von Infrastructure-as-Code-Werkzeugen. Exemplarisch werden hier die Auswirkungen eines Einsatzes von Terraform[17] und Kubernetes[18] näher betrachtet.

Bei Terraform handelt es sich um ein Open-Source Infrastructure-as-Code-Werkzeug, mit dem durch die Konfigurationssprache HCL die Infrastruktur einer Cloud als Code definiert werden kann. Terraform erstellt aus diesem Code einen Plan und führt diesen zur Bereitstellung von Infrastruktur in der Cloud aus. So kann die als Code modellierte Infrastruktur beziehungsweise Systemarchitektur in der Cloud konsistent und wiederholt bereitgestellt werden [46]. Dadurch kann einerseits die Geschwindigkeit einer Bereitstellung deutlich erhöht werden, da keine manuellen Konfigurationen jeder Komponenten in der Infrastruktur mehr benötigt wird. Andererseits geht damit eine höhere Zuverlässigkeit des Systems einher da insbesondere im Rahmen von größeren Infrastrukturen, Konfigurationsfehler durch eine automatisierte Bereitstellung eher vermieden werden können. Insgesamt erhöht sich dadurch das Schutzniveau des Systems gegenüber verschiedenster Konfigurationsfehler. Des Weiteren wird das Risiko eines Vendor lock-ins verringert, da der Terraform Code bei anderen Cloud-Anbieters wiederverwendet werden kann, um eine gleiche Infrastruktur bereitzustellen. Lediglich Konfigurationen bezüglich verwalteter Cloud-Dienste müssten gegebenenfalls angepasst werden, da Cloud-Anbieter jeweils eine

[17] https://www.terraform.io/
[18] https://kubernetes.io/

andere API für die Nutzung vorsehen. Zudem sollte die Nutzung von spezifischen Diensten, die es in ähnlicher Art bei anderen Cloud-Anbietern nicht gibt, vermieden werden.

Kubernetes dagegen ist ein System zur Bereitstellung und Skalierung von Containern beziehungsweise containerisierten Anwendungen. Ein Container ist dabei eine Zusammenfassung von Softwarecode und allen nötigen Abhängigkeiten beziehungsweise Betriebssystembibliotheken, die zur vollständigen Ausführung der Anwendung benötigt werden. Container sind dabei insgesamt als portabler und ressourceneffizienter anzusehen als virtuelle Maschinen, da keine direkte Abhängigkeit mehr zu einem spezifischen Betriebssystem zur Virtualisierung besteht [44]. Solche Container können durch Kubernetes dann verwaltet, skaliert und bereitgestellt werden. Ein Vorteil dabei ist, dass Kubernetes mit nahezu jeder Cloud-Infrastruktur kompatibel ist und teilweise sogar als ein durch den Cloud-Anbieter verwalteter Dienst angeboten wird. So kann sich auch durch den Einsatz von Kubernetes insgesamt das Risiko eines Vendor lock-in verringern, da Container zwischen Cloud-Umgebungen von verschiedenen Cloud-Anbietern, beziehungsweise zwischen einer Cloud und einem On-Premises System ohne grundlegende Anpassungen verschoben werden können [47]. Hier gilt jedoch dasselbe wie im Rahmen von Terraform bezüglich einer unterschiedlichen Konfiguration von verwalteten Cloud-Diensten pro Provider.

Im Bereich der Infrastructure-as-Code-Werkzeuge existieren viele weitere Technologien, wie zum Beispiel Ansible[19] oder SaltStack[20]. Weitere Werkzeuge sollten gegebenenfalls geprüft und von Beginn an konsequent integriert und genutzt werden.

M6: Automatisierte Reaktion auf sicherheitskritische Vorfälle

Als nächste Maßnahme werden automatisierte Reaktionen gegenüber sicherheitskritischen Vorfällen thematisiert. Durch automatisierte Reaktionen kann die Zeit zwischen dem Erkennen eines sicherheitskritischen Vorfalls und den ersten Maßnahmen teils deutlich verringert werden, sodass die Wahrscheinlichkeit der sofortigen und effektiven Einleitung von Maßnahmen höher liegt [52]. Da hier allerdings noch keine breite Menge an praktikablen Werkzeugen existiert, muss besonders auf eine angemessene Auswahl geachtet werden. Viele der bisher existenten Lösungen, wie zum Beispiel der IBM QRadar SOAR-Plattform[21] oder Sumo Logic Cloud SOAR[22] nutzen beispielsweise KI basierte Ansätze für die Erkennung von Vorfällen sowie einer Auswahl an geeigneten Maßnahmen.

[19] https://www.ansible.com/
[20] https://saltproject.io/
[21] https://www.ibm.com/de-de/products/qradar-soar
[22] https://www.sumologic.com/de/loesungen/cloud-soar/

Allerdings ist es auch möglich, Matrizen wie die D3FEND[23] und ATT&CK[24] Matrix zu nutzen. Diese bündeln jeweils breite Wissensdatenbanken über Angriffsmöglichkeiten und Verteidigungsmaßnahmen frei verfügbar in einer Art Graphensystem. Über entsprechende Algorithmen kann hier eine Graphentraversierung durch diese Wissensdatenbanken implementiert werden, um so entsprechende Reaktionsmechanismen aufzubauen [52]. Falls die breite Integration oder Implementierung eines solchen Werkzeuges zu aufwendig erscheint, sollten zumindest grundlegende Basis-Maßnahmen definiert werden. Die Basis-Maßnahmen sollten dann im Zuge jedes Sicherheitsvorfalles automatisiert umgesetzt werden.

Wird eine solche automatisierte Reaktion auf sicherheitskritische Vorfälle angemessen implementiert, so können Ausfälle verhindert, mögliche Schäden minimiert und das System schneller wiederhergestellt werden.

M7: Berücksichtigung des Well-Architected Frameworks

Als eine weitere Maßnahme kann die Berücksichtigung des Well-Architected Frameworks[25] empfohlen werden. Insbesondere gilt diese Empfehlungen, da im vorliegenden Anwendungsszenario bisher keinerlei Erfahrung mit dem Einsatz einer Cloud und einer entsprechenden Architektur vorhanden sind. Dieses Framework wurde ursprünglich von Amazon Web Services entwickelt, wird in Grundzügen allerdings ebenfalls und identisch von diversen anderen größeren Cloud-Anbietern, wie Microsoft oder Google, ebenfalls angeboten. Mithilfe des Frameworks können die Best Practices für eine sichere, zuverlässige, effiziente, kosteneffektive und nachhaltige Cloud-Architektur erlernt werden. Genauer dient das Framework als eine Art Schema, um die geplante Architektur in der Cloud hinsichtlich von Best Practices in der Cloud zu verifizieren und gegenzuprüfen [6]. Das Framework wird dabei in sechs Säulen aufgebaut, die unter anderem aus Themen wie der Sicherheit oder Performance bestehen. Innerhalb dieser Säulen werden mögliche Fragestellungen angeführt, mithilfe dessen ein Unternehmen bei der Definition von Anforderunge für eine geeigenete Cloud-Architektur unterstützt werden kann. Zusätzlich werden erste Erläuterungen zu den verschiedenen Best Practices der jeweiligen Säule geliefert. Im Anhang befindet sich, anschließend zu jedem dieser thematisieren Best Practices, ein weiter Block mit ausführlichen Inhalten wie Implementierungshinweisen, Anti-Patterns, Benefits und einer schrittweisen Umsetzungsanleitung.

[23] https://d3fend.mitre.org/
[24] https://attack.mitre.org/
[25] https://aws.amazon.com/de/architecture/well-architected/

Zwar gibt dieses Framework so einen soliden Überblick über Cloud-spezifische Best Practices und Eigenheiten der Cloud, allerdings sollte die MakeABank GmbH die Inhalte mit einem gewissen Grade an Skepsis in die eigene Architektur einarbeiten. Da das Framework von den jeweiligen Cloud-Anbietern erarbeitet wurde und Lösungsstrategien beziehungsweise Best Practices vorgestellt werden, die in der Regel auf einem verwalteten Cloud-Dienst des Providers basieren, könnte es im Zuge einer identischen Umsetzung passieren, dass mehr verwaltete Cloud-Dienste berücksichtigt werden und sich somit der Effekt des Vendor Lock-in erhöht. Daher empfiehlt es sich, Grundstrukturen und Prinzipien der Best Practices zu übernehmen und nebenbei zu prüfen, ob der verwaltete Cloud-Dienst des Providers gegebenenfalls sinnvoll durch eine alternative Open-Source Lösung ersetzt werden kann. Um hier ein konkretes Beispiel zu liefern, könnte es zum Beispiel als sinnvoll erscheinen im Rahmen des Identitäts- und Zugriffsmanagements eher die Open-Source Lösung Keycloack[26] zu nutzen, statt wie empfohlen, ein verwalteter Dienst des Cloud-Anbieters.

M8: Sensibilisierung im Rahmen von regelmäßigen Schulungen

Zudem sollten Schulungen durchgeführt werden, um Cloud-spezifisches Fachwissen möglichst breit innerhalb einer Institution zu streuen. Dazu sollte im allerersten Schritt die Unterstützung des Managements eingeholt werden, da diese in der Regel monetäre Mittel und Ressourcen freigeben müssen, um eine solche Maßnahme zu ermöglichen. Des Weiteren sollte ein beauftragte Person für die Informationssicherheit ernannt werden, die eine Durchführung von regelmäßigen Schulungen im Rahmen der Empfehlungen des BSI-Grundschutzes überwacht. Diese sollte ebenfalls den Prozess anregen, konkrete Zielgruppen von Schulungen zu identifizieren und individuelle Themenschwerpunkte zu setzen [12].

Beispielsweise erscheint es hier möglicherweise als sinnvoll, den Schwerpunkt für Schulungen innerhalb der Kunden von der MakeABank GmbH eher auf die Gefahren des Social Engineerings zu legen. Denn da die Kunden durch das vereinbarte Dienstleistungsmodell mit der MakeABank GmbH per se kaum Berührungspunkte mit der Verwaltung der Cloud-Infrastruktur besitzen, würde dementsprechend ein technischer Schwerpunkt tendenziell lediglich unternehmerische Ressourcen verschwenden.

Nach abgeschlossener Schulung sollten zudem mögliche Erfolge gemessen beziehungsweise verifiziert werden und bei Bedarf nachgeschult werden [12].

[26] https://www.keycloak.org

Als unterstützende Maßnahme bieten auch viele Cloud-Anbieter teilweise kostenlose Schulungen in einem Selbstkurs-Format an. Hier können gegen Aufpreis häufig sogar offizielle Zertifikate erworben werden. Die Integration solcher Schulungen und Zertifikate in die eigenen Schulungsstrukturen wird ebenfalls empfohlen, da so der Aufwand in der Vorbereitung minimiert werden kann und offizielle Zertifikate möglicherweise für eine höhere Reputation gegenüber des Kunden sorgen können.

M9: Erstellung eines Datensicherungskonzeptes

Das Erstellen und Berücksichtigen eines Datensicherungskonzepts für die Cloud ist eine weitere wichtige Maßnahme, um die Risiken des Anwendungsszenarios zu minimieren. In einem ersten vorbereitenden Schritt, um ein angemessenes Datensicherungskonzept zu erstellen, sollten die Anforderungen in enger Kooperation mit fachverantwortlichen Personen abgestimmt werden [12]. Speziell im Kontext der Cloud sollte hier ein besonderer Fokus auf der Definition von Anforderungen hinsichtlich der Vertraulichkeit, des Rechts, des Datenmanagements und des Umfangs der zu sichernden und der zu löschenden Daten liegen. Des Weiteren sollen im Rahmen der Vorbereitung zeitliche Intervalle für eine automatische Datensicherung bestimmt werden und mehrere voneinander unabhängige Speicherorte evaluiert, im Konzept berücksichtigt und für spätere Datensicherungen genutzt werden. Die meisten Cloud-Anbieter bieten hierfür einen verwalteten Datensicherungsdienst an, welcher als einer von drei Speicherorten genutzt werden und häufig bereits einen hohen Grad an Skalierung beziehungsweise Redundanz von Datensicherungen für eine Hochverfügbarkeit bereitstellen kann. Durch einen solchen verwalteten Datensicherungsdienst können Datensicherungen in der Regel simpel, beziehungsweise automatisiert angelegt und nach Belieben konfiguriert werden. Ein konkretes Beispiel hierfür und mit den beschriebenen Eigenschaften stellt der Azure Backup Dienst von Microsoft dar [75]. Hinsichtlich des Stellenwertes der Verfügbarkeit im vorliegenden Anwendungsszenario reicht es jedoch gegebenenfalls nicht aus, sich lediglich auf die Zuverlässigkeit eines einzigen Datensicherungsdienstes des Cloud-Anbieters zu verlassen. Daher sollte zusätzlich eine eigene Redundanz geschaffen werden, indem Datensicherungen ebenfalls sowohl auf lokalen Dateiträgern, die anschließend vom Netz getrennt werden können, als auch bei einem weiteren externen Anbieter für Speicherkapazitäten hinterlegt werden. Da es sich hierbei jedoch um ein weiteres Outsourcing von sensiblen Geschäftsdaten handelt, sollten jegliche Datensicherungen grundsätzlich immer sicher verschlüsselt werden. Zudem sollten für Schlüssel getrennte Datensicherungen angelegt werden und die Anbieter keinen Zugriff auf die Schlüssel erhalten.

Inbesondere bei Nutzung des Datensicherungsdienstes eines Cloud-Anbieters nimmt dieser eine zentrale Rolle ein, sodass im Rahmen dieser Maßnahme einige zusätzliche Aspekte berücksichtig werden müssen. So müssen möglicherweise auch im Rahmen von Datensicherungen die technischen Limitierungen eines Providers innerhalb des Konzeptes berücksichtigt werden. Beispielsweise ist es im Rahmen der Microsoft Azure Cloud nur 3-mal am Tag möglich eine Datensicherung von derselben virtuellen Maschine anzulegen [76]. Ähnliche Limitierungen sollten im Voraus präzise geprüft werden. Zudem werden pro Datensicherung in der Regel zusätzliche Kosten für die rechnungstragende Institution fällig. Strategien zur Kostenoptimierung sollten dementsprechend auch von Anfang an innerhalb eines Datensicherungskonzeptes berücksichtigt werden. Ein Ansatz zur Kostenoptimierung kann das regelmäßige und zeitnahe Löschen von alten Datensicherungen darstellen. Des Weiteren sollte evaluiert werden, inwiefern eine differenzielle Datensicherung der vollständigen Datensicherung vorgezogen werden kann, um dessen Größe zu minimieren. Als ein letzter Ansatz, erlauben es viele Datensicherungsdienste lediglich bestimmte Bereiche einer Festplatte zu sichern, was möglicherweise auch genutzt werden könnte. Diese Aspekte bezüglich einer Kostenoptimierung wurden ebenfalls anhand einer Quelle für die Microsoft Azure Cloud erarbeitet [8], lassen sich allerdings in der Regel auch auf andere Cloud-Anbieter transferieren, solange eine nutzungsbasierte Abrechnung verwendet wird.

M10: Angemessenes Patch- und Änderungsmanagement

Innerhalb des Systems sollten für die Abhängigkeiten der Anwendung regelmäßig Updates und Patches eingespielt werden [12]. Speziell im Fokus sollten hier die Anwendung mit eher vielen Abhängigkeiten, wie der Frontend Webanwendung (A001), der Backend Spring-Anwendung (A002) und weiterer entsprechender Anwendungen des „MaBCloud“ Systems sein. Dabei sollte geprüft werden, inwiefern automatische Mechanismen beim Patchen von sicherheitskritischen Schwachstellen genutzt werden können.

Des Weiteren sollte ständig geprüft werden, ob verwendete Bibliotheken und Dienste Dritter noch unterstützt werden. Wenn dies nicht der Fall ist, sollten zeitnah geeignete Alternativen gesucht werden [12].

M11: Durchführung von Monitoring

Ein erster Baustein zu einem angemessenen Monitoring des IT-Systems ist das Etablieren eines angemessenen Log-Managements. Eine Anforderung für alle Systeme ist es hier, dass Ereignismeldungen sofort an ein zentrales Logging-System übermittel werden [12].

Besonders in der Cloud bietet sich hierfür eine Logging-as-a-Service-Lösung an, die in der Regel bereits durch gängige Cloud-Anbieter zur Verfügung gestellt wird. Alternativ können auch Dienste von Dritten, wie zum Beispiel *Data Dog*[27] oder *Solarwinds Loggly*[28] verwendet werden. Dies ist besonders essenziell für spätere forensische Analysen, da viele Ansätze auf einer Analyse von zentral gesammelten Log-Dateien basieren, und um eine effektive Überwachung und Analyse von Ereignissen aller Ressourcen während des Betriebes sicherzustellen [58].

Zudem sollten Logs ausreichend lange aufbewahrt werden, da sicherheitskritische Vorfälle nicht immer sofort wahrgenommen werden. Außerdem sollte ein ähnlicher Ansatz wie im Rahmen des Datensicherungsmanagements konzipiert werden mit dessen Hilfe Log-Dateien sicher verschlüsselt und an mehreren unabhängigen Speicherorten aufbewahrt werden. Ein übergeordnetes Ziel muss es hier sein, eine nachträgliche Manipulation von Log-Dateien zu verhindern.

Auf Basis eines angemessenen Log-Managements sollte die Überwachung des Systems im Rahmen eines IT-Monitorings umgesetzt werden. Zu prüfen ist hier, ob entweder der hauseigene Dienst des Cloud-Anbieters den technischen Ansprüchen genügt, eine externe Anwendung für das Monitoring in die Cloud integriert oder eine Monitoring-as-a-Service-Anwendung genutzt werden soll. Verschiedene dieser Lösungsmöglichkeiten und damit verbundene Produkte sollten mit den technischen Anforderungen abgeglichen werden und eine möglichst hohe Schnittmenge bieten. Zudem sollten ein fester Plan für das Monitoring erarbeitet werden, in dem geeignete Metriken und entsprechende Schwellenwerte für Warnungen beziehungsweise Alarme ermittelt und dokumentiert werden. Entsprechende Reports mit aktuellen Lageberichten und Trendentwicklungen sollten ebenfalls erstellt werden. Des Weiteren sollte das Monitoring stetig aktualisiert und an Veränderungen der Systemarchitektur angepasst werden [12].

M12: Einrichten von Konten für den Notfallzugriff

Besonders im Kontext des Cloud-Computings ist es empfehlenswert, mindestens zwei Benutzer für einen Notfallzugriff auf das System anzulegen. In der Cloud besteht in der Regel immer eine Abhängigkeit zu einem externen Identitätsdienst oder einem Dienst für die Multi-Faktor-Authentifizierung, um eine Authentifizierung zu implementieren. Dies gilt im vorliegenden Szenario auch für die MakeABank GmbH. Dadurch kann es passieren,

[27] https://www.datadoghq.com/
[28] https://www.loggly.com/

dass beim Ausfall dieser möglicherweise nicht mehr auf die Cloud-Umgebung beziehungsweise die Ressourcen zugegriffen werden kann. Falls sich in dieser Zeit ein sicherheitskritischer Vorfall ereignet, könnte dadurch eine sofort benötigte Reaktion ausbleiben. Um dieses Problem zu behandeln, sollten besondere Konten für einen Notfallzugriff eingerichtet werden, die dabei bestimmte Kriterien zu erfüllen haben [72]. So sollte keiner der Konten einer expliziten Person zugeordnet werden und umfassende administrative Privilegien für die Cloud-Umgebung besitzen, sodass dementsprechend administrative Aktionen durchgeführt werden könnten. Zudem sollten beide Benutzer, sowohl untereinander als auch gegenüber jeglichen anderen Benutzerkonten, andere und unabhängige Zugangsdaten beziehungsweise Authentifizierungsmethoden benutzen [72]. Dadurch kann das Risiko gestreut werden, und es müssten verschiedene, voneinander unabhängige Dienste ausfallen, um ein identisches Ausschlussszenario zu erzeugen. Nach der abgeschlossenen Konfiguration sollte hier ebenfalls eine regelmäßige Prüfung stattfinden, ob diese noch Benutzer existent und nutzbar sind.

M13: Erstellung eines Notfallmanagements mittels BSI-Standard 100-4

Da sich, wie bereits im Zuge der Bedrohungsübersicht herausgearbeitet, durch der Cloud Nutzung ebenfalls neue Anforderungen an ein Notfallmanagement ergeben, muss das Notfallmanagement dementsprechend angepasst werden. Grundlegende Schritte, wie die Erstellung eines neuen Notfallhandbuches, sollten hier unbedingt vorgenommen werden. Dabei sollten von Anfang an alle betroffenen Mitarbeiter integriert werden. Eine Streuung des Wissens kann hier auch im Rahmen von Schulungen *(vgl. M8: Sensibilisierung im Rahmen von regelmäßigen Schulungen)* erfolgen.

Zudem kann eine Nutzung des BSI-Standard 100-4 als sinnvoll erscheinen. Im Rahmen dessen wird durch das BSI eine Methodik vorgegeben, um ein Notfallmanagement zu erarbeiten. Dieser Standard erweitert die Reihe des IT-Grundschutzes, baut auf dem BSI-Standard 200-3 beziehungsweise der beschriebenen Risikoanalyse auf und bietet daher ein kompatibles Werkzeug [17].

M14: Frühe Ausarbeitung einer Exit-Strategie

Während ein Notfallmanagement mittels des BSI-Standards 100-4 erarbeitet werden kann, sollte der Fokus auch auf die frühe Ausarbeitung einer Exit-Strategie gelegt werden. Auch hier bietet das BSI ein konkretes Werkzeug beziehungsweise Methodik zur Orientierung. So kann zur Ausarbeitung einer Exit-Strategie das durch das BSI veröffentlichte Dokument mit Empfehlungen zur Vorbereitung einer Exit-Strategie bei Nutzung von

Cloud-Diensten verwendet werden [107]. Um hier einen kurzen Einblick zu geben, werden die drei Phasen untersucht, die sich auf den Inhalt einer möglichen Exit-Strategie auswirken. Innerhalb der Phasen werden mögliche Risiken untersucht und Anforderungen an den Auftraggeber *(hier Kunden der MakeABank GmbH)* und den Auftragnehmer *(hier beliebiger Cloud-Anbieter)* genannt. Die beschriebenen Anforderungen sollten im Rahmen einer angemessenen Exit-Strategie berücksichtigt beziehungsweise umgesetzt werden. Insgesamt wurde die Methodik mit einem besonderen Fokus auf Unternehmen entwickelt, die zur kritischen Infrastruktur gehören [107]. Daher ist die Nutzung dieser Vorgehensweise für die MakeABank GmbH besonders relevant und sollte als Werkzeug für die Entwicklung einer Exit-Strategie unbedingt etabliert werden.

M15: Nutzung einer Hybrid-Cloud beziehungsweise Multi-Cloud-Architektur

Eine weitere Maßnahme ist die Absicherung von kritischen Dienstleistungen mittels einer Hybrid-Cloud-Architektur beziehungsweise Multi-Cloud-Architektur. Insbesondere mit dem Fokus auf den hohen Stellenwert einer dauerhaften Verfügbarkeit des Systems sollte diese Maßnahme umgesetzt werden. Dabei bedeutet Hybrid-Cloud in diesem Kontext, die Nutzung eines eigenen On-Premises Systems sowie einer externen Cloud und Multi-Cloud die Nutzung zwei verschiedener Cloud-Anbieter für einen Service, um so die ständige Verfügbarkeit bestmöglich sicherzustellen [107]. Hier ist allerdings davon auszugehen, dass diese Maßnahme durchaus mit einem höheren Wartungsaufwand einhergeht. Dies lässt sich primär durch die nicht existente Kompatibilität unter den Cloud-Anbietern begründen. Deswegen sollte diese Maßnahme vornehmlich im Kontext mit einer kritischen Infrastruktur in Erwägung gezogen und die Verhältnismäßigkeit für andere Bereiche individuell geprüft werden. Wird diese Maßnahme umgesetzt, sollten unbedingt verschiedene Cloud-Anbieter beziehungsweise Infrastrukturen verwendet werden, die jeweils unabhängig voneinander eine Hochverfügbarkeit garantieren.

M16: Ausreichende Vorausplanung einer Strategie

Diverse Anforderungen sollten in der Strategie bezüglich der Wahl eines Cloud-Anbieters klar definiert werden. Einerseits sollten konkrete Voraussetzungen definiert werden, wie Zertifikaten, Testate oder ähnliche Anforderungen, die ein Cloud-Anbieter erfüllen sollte und die sich in der Regel verhältnismäßig leicht prüfen lassen [107]. Andererseits müssen technischen Anforderungen evaluiert und mit den Leistungen eines Cloud-Anbieters in Bezug auf die Cloud-Umgebung sowie jeglicher bereitgestellter Dienste gegengeprüft werden. Entsprechende Ergebnisse sollten in einer konkreten Machbarkeitsstudie dokumentiert werden [12]. Insbesondere durch Cloud-spezifische Bedrohungen wie dem Vendor

lock-in sollte in diese Planungen zu präventiven Zwecken ein hoher Umfang an Ressourcen einfließen.

Als ein weiterer Baustein sollten wirtschaftliche Ziele des Unternehmens in Bezug auf eine Cloud-Nutzung definiert und bestmöglich daraufhin überprüft werden, ob diese mit der aktuellen Strategie erreicht werden können. Jegliche Entscheidungen sollten dabei stets ausführlich dokumentiert werden und nebenbei Roadmaps beziehungsweise Schemen ausgearbeitet werden, um zu einem späteren Zeitpunkt einheitlich und präziser bestimmten zu können, wann und wie ein neuer verwalteter Cloud-Dienst in das System integriert werden sollte [12]. Dies gilt speziell hinsichtlich zu nutzender Schnittstellen oder dem benötigten Level an implementierter Sicherheit beziehungsweise Performance des Dienstes.

M17: Festlegung der Sensibilität von auszulagernden Daten und Diensten

Im Vorhinein sollte insbesondere bei Betreibern einer kritischen Infrastruktur geprüft werden, ob Geschäftsprozesse existieren, die nach gesetzlichen Regularien entweder gar nicht in einer Cloud betrieben werden dürfen oder nur unter bestimmten Auflagen [107]. Solch identifizieren Geschäftsprozesse sollten gegebenenfalls weiterhin ausschließlich auf der On-Premises Infrastruktur betrieben werden und damit in folgenden Planungen für eine Cloud-Nutzung nicht mehr berücksichtigt werden.

M18: Kommunikationskanäle mit dem Cloud-Anbieter etablieren

Im Kontext des Cloud-Computings wird das System durch den Cloud-Anbieter als weiter involvierte Institution ergänzt. Dabei kann es durchaus vorkommen, dass während der Nutzung der Infrastruktur sowie von verwalteten Diensten des Cloud-Anbieters diverse technische Probleme auftreten können. Verschiedene Szenarien sind hier möglich, die jeweils verschiedene Grundwerte negativ beeinträchtigen können. Da derartige Probleme nicht in die Zuständigkeit der eigenen Institution fallen, sollte hier eine möglichst schnelle beziehungsweise effiziente Problemlösung in Kooperation mit dem Cloud-Anbieter angestrebt werden. Auch in dem Szenario, falls sich beim Cloud-Anbieter für die MakeABank GmbH sicherheitskritische Vorfälle ereignen, sollte ein solcher Kommunikationskanal für einen schnellen Informationsfluss definiert werden [106]. Um diesen Prozess seitens der eigenen Institution zu optimieren, sollten Ansprechpartner und entsprechende Kommunikationskanäle für verschiedene Problemkategorien evaluiert und festgelegt werden [12].

Zudem sollten diese ausführlich und für mitarbeitende Personen des eigenen Unternehmens dokumentiert werden, sowie schnell beziehungsweise unkompliziert und an einer zentralen Stelle zugänglich sein.

Optional kann diese Liste ebenfalls mit beliebigen Ansprechpersonen des eigenen Unternehmens für diverse wichtige Anliegen erweitert werden, sodass alle Kommunikationsprozesse insgesamt optimiert werden können.

M19: Möglichst breiter Einsatz von Firewalls

Vor dem Einsatz einer Firewall-Lösung sollte auch hier ein Konzept entworfen und dokumentiert werden, welche die Regeln für den Datenverkehr genaustens definiert [12]. Anschließend sollte innerhalb der Cloud-Umgebung insgesamt ein möglichst breiter Einsatz von verschiedenen Firewalls erfolgen. Einerseits sollten sowohl die Außengrenzen des Systems über eine angemessene Firewall-Lösung abgesichert werden und andererseits kann es auch sinnvoll sein, die virtuellen Maschinen im System durch jeweilige Firewalls des Betriebssystems zu sichern. So können mehrere Barrieren gegen Angriffe errichtet werden. Zudem sollten jegliche Datenströme über festgelegte Endpunkte der Firewall erfolgen. Andere Komponenten sollten nicht über das öffentliche Internet erreichbar sein und nur unbedingt benötigte Ports sollten geöffnet werden.

Da bereits der Einsatz einer Firewall im Rahmen eines Firewall-as-a-Service-Servicemodells im vorliegenden Anwendungsszenario festgehalten wurde, sollte die Anbieterwahl nach technischen Voraussetzungen und Zertifizierungen erfolgen. Das BSI empfiehlt hier im Rahmen des Common Criteria Standards eine Zertifizierung von mindestens EAL4. Zudem sollte der Dienst eine vertraglich zugesicherte Hochverfügbarkeit umsetzen [12].

Wurde durch die Empfehlungen eine angemessene Firewall-Lösung ausgewählt, so sollten zusätzlich einige Konfigurationsaspekte umgesetzt werden, um einen möglichst hohen Schutz des Systems zu ermöglichen.

- TLS-Proxy der Firewall sollte stets die Zertifikate auf ihre Gültigkeit überprüfen.
- Setzen von Limits für offene Verbindungen gegen Denial of Service durch TCP SYN Flooding.
- Setzen von Rate-Limits für UDP-Datenströme.
- Dynamisches Routing deaktivieren.

- Paketfilter sollte genaustens konfiguriert werden und stets Zustands-behaftet Pakete filtern.
- Schutzmechanismen gegen IPv4- und IPv6-Fragmentierungsangriffe sollten aktiviert werden.
- Ungenutzte Erweiterungen sollten deaktiviert werden.

Die ausgeführten Empfehlungen stammen dabei gänzlich aus dem IT-Grundschutz Kompendium [12].

4.6.2 Empfehlungen

Da im Rahmen dieser Arbeit nicht alle Sicherheitsmaßnahmen im Detail ausgeführt werden können und im vorliegenden Anwendungsszenario bisher wenig Cloud-Erfahrung vorliegt, sollte geprüft werden, ob zur Absicherung vor dem Live-Gang des Systems ein Cloud Audit der Cloud-Umgebung durchgeführt werden kann. Ein vollständiger Penetrationstest sollte im Kontext der Cloud vermieden, beziehungsweise das Vorgehen genauestens auf Rechtsmäßigkeit geprüft werden, da hier die Infrastruktur mit angegriffen wird und dies ohnehin durch die Cloud-Provider in der Regel untersagt ist. Beispielsweise sind im Rahmen der Azure Cloud jegliche Penetrationstests verboten, welche andere Kunden negativ beeinträchtigen könnten, wie zum Beispiel Denial of Service oder jegliche Tests, die Zugriff auf fremde Daten gewähren können [77]. Ein solcher Cloud Audit kann durch zertifizierte Fachkräfte von externen Firmen als Dienstleistung durchgeführt werden und zur schnelleren Streuung von Fachwissen bezüglich einer sicheren Cloud-Nutzung innerhalb der MakeABank GmbH beitragen. Insbesondere hinsichtlich der Bedeutung der Informationssicherheit sollte dies unbedingt in Erwägung gezogen werden.

Um nun auf die vorgestellten Maßnahmen einzugehen, sollten durch den Betrieb einer Anwendung innerhalb der kritischen Infrastruktur alle Maßnahmen umgesetzt werden. Auch wenn dies möglicherweise mit einem hohen Arbeitspensum einhergeht, ist eine unvollständige Umsetzung trotzdem nicht zu empfehlen. Dennoch erscheint es hier sinnvoll eine Strategie zu verfolgen, um als sehr hoch klassifizierte Risiken für Bedrohungen, die den gesamten Informationsverbund betreffen, möglichst effizient zu behandeln. So empfiehlt es sich *B1: Unzureichendes Notfallmanagement* grundsätzlich durch *M13: Erstellung eines Notfallmanagements mittels BSI-Standard 100-4* vorzubeugen. Da hier das

Risiko, wie bereits erwähnt, aufgrund mangelnder Erfahrungswerte nicht gänzlich vermieden werden kann, kann dies durch eine kombinierte Umsetzung von *M6: Automatisierte Reaktion auf sicherheitskritische Vorfälle*, *M16: Ausreichende Vorausplanung einer Strategie* und *M14: Frühe Ausarbeitung einer Exit-Strategie* weiter reduziert werden. Auch eine frühe Umsetzung von *M18: Kommunikationskanäle mit dem Cloud-Anbieter etablieren* wirkt sich generell positiv auf ein mögliches Notfallmanagement aus, da so ein Cloud-Anbieter in bestimmten Szenarien effizienter unterstützen kann.

Auch das Bedrohungspotenzial des als sehr hoch klassifizierten Risikos von *B8: Vendor lock-in*, kann nicht gänzlich vermieden werden. Um das Risiko jedoch möglichst zu reduzieren, empfiehlt es sich hier ebenfalls die möglichst frühe Umsetzung von *M1: Globale Zero-Trust-Strategie implementieren*, um bereits bei der Auswahl eines Cloud-Anbieters keinen unangemessenen Vertrauensfluss entstehen zu lassen. Währenddessen sollte ebenfalls möglichst früh mit *M14: Frühe Ausarbeitung einer Exit-Strategie* begonnen werden, da eine solche Strategie möglicherweise grundlegende Architekturentscheidungen beeinflussen kann. Ebenso sollte von Anfang an *M15: Nutzung einer Hybrid-Cloud beziehungsweise Multi-Cloud-Architektur* umgesetzt werden, damit so unverzüglich und mittels eines möglichst niedrigen Aufwandes zwei Cloud-Umgebungen synchronisiert aufgebaut werden können. Sobald die Wahl der Provider beziehungsweise der Architektur gefallen ist und eine bereitgestellte Cloud-Umgebung existiert, sollte *M5: Nutzung von Infrastructure as Code* umgesetzt werden, um nicht manuell angelegt und erst später mit zusätzlichem Aufwand in einen Code transferiert werden zu müssen.

Das sehr hohe Risiko für den gesamten Informationsverbund durch *B16: Denial of Service* sollte reduziert werden, indem möglichst früh *M19: Breiter Einsatz von Firewalls* in Verbindung mit *M16: Ausreichende Vorausplanung einer Strategie* umgesetzt wird, sodass von Anfang an eine angemessene Firewall-Lösung mit einer richtigen Konfiguration an strategisch sinnvollen Punkten eingesetzt wird. Wenn die primären Maßnahmen der andere Bedrohungen *M6: Automatisierte Reaktion auf sicherheitskritische Vorfälle* und *M15: Nutzung einer Hybrid-Cloud beziehungsweise Multi-Cloud-Architektur* angemessenen umgesetzt werden, können diese auch hier das restliche Risiko zusätzlich reduzieren.

Um anschließend das sehr hohe Risiko von *B21: Social Engineering* zu reduzieren, sollte der Fokus unbedingt auf einer Vermeidung mittels *M8: Sensibilisierung im Rahmen von regelmäßigen Schulungen* liegen. Auf technischer Seite sollte zudem von Anfang an *M4: Multi-Faktor Authentifizierung* umgesetzt werden in einer direkten Verbindung mit *M3: Single Sign-on*. Andere Maßnahmen, die bereits in Verbindung mit anderen Bedrohungen

genannt wurden, wie *M1: Globale Zero-Trust-Strategie implementieren* und *M13: Erstellung eines Notfallmanagements mittels BSI-Standard 100-4* können dieses Risiko weiter reduzieren.

Die anderen thematisierte Maßnahmen, welche hier nicht direkt in Verbindung mit den risikoreichsten Bedrohungen genannt wurden wie: *M2: Nutzung clientseitiger Verschlüsselung*, *M7: Berücksichtigung des Well-Architected Frameworks*, *M9: Erstellung eines Datensicherungskonzeptes*, *M10: Angemessenes Patch- und Änderungsmanagement* sowie *M11: Durchführung von Monitoring* sollten ebenfalls umgesetzt werden und zwar bevor das System in der Cloud in Betrieb geht. Auch wenn hiermit nicht in erster Linie Bedrohungen mit einem sehr hohen Risiko adressiert werden, reduzieren diese Maßnahmen dennoch ein hohes Kontingent an Bedrohungen mit einem als hoch klassifizierten Risiko. Daher sollten nach Umsetzung der vorherigen Empfehlungen auch diese Maßnahmen im vollen Umfang durchgeführt werden.

Nach der Umsetzung dieser Handlungsempfehlung kann angenommen werden, dass alle Bedrohungen mit einem sehr hohen Risiko grundsätzlich behandelt wurden. Die Risiken können durch eine Umsetzung insgesamt vermieden beziehungsweise reduziert werden. Insgesamt kann davon ausgegangen werden, dass die Kategorien der begründeten Risiken dadurch in mittel bis gering gesenkt werden konnten. Ähnliches gilt für Bedrohungen mit einem hohen Risiko, welche durch den beschränkten Rahmen dieser Arbeit nicht weiter thematisiert werden können.

5 Schlussbetrachtung

Nachdem nun die Bedrohungsanalyse durch eine Darstellung von Handlungsempfehlungen abgeschlossen wurde, findet nachfolgend ein Abschluss der gesamten Arbeit im Rahmen eines Fazits statt. Insbesondere werden Arbeitsergebnisse abschließend diskutiert, zusammengefasst und geprüft, ob beziehungsweise inwiefern die aufgestellten Forschungsfragen *(vgl. Kapitel 1)* beantwortet wurden. Zusätzlich wird ein Ausblick auf zukünftige Entwicklungen und damit verbundene weiterführende Forschungsthemen gegeben.

5.1 Diskussion

Im Rahmen dieser Arbeit wurden die Bedrohungen aus dem Betrieb einer exemplarischen Anwendung in einer IaaS Cloud-Umgebung betrachtet. Dazu wurde die Methodik des IT-Grundschutzes verwendet. So wurde ein Informationsverbund festgelegt und die dazugehörigen Zielobjekte im Rahmen einer Strukturanalyse herausgearbeitet und nach Empfehlungen des BSI gruppiert. Anschließend wurde der jeweilige Schutzbedarf festgestellt, um so mittels des IT-Grundschutzes für Zielobjekte mit einem hohen Schutzbedarf relevante Bedrohungen innerhalb einer Bedrohungsübersicht herauszuarbeiten.

Obwohl der IT-Grundschutz an eine Verwendung des IT-Grundschutzkompendiums geknüpft ist, womit durch standardisierte und wiederverwendbare Bausteine eine Aufwandsreduktion der Bedrohungsanalyse ermöglicht werden soll, konnten insgesamt nur wenige Bausteine für das vorliegende Anwendungsszenario in der Cloud wiederverwendet werden. Zwar existiert im IT-Grundschutz-Kompendium ein eigenes Unterkapitel für die Cloud-Nutzung *(vgl. OPS.2.2 Cloud-Nutzung in [12, S.277])*, jedoch werden hier lediglich Bausteine für Cloud-spezifische Bedrohungen auf einer organisatorischen Ebene gegebenen. Bausteine für Bedrohungen mit einem technischen Hintergrund werden zwar in anderen Kapiteln innerhalb des IT-Grundschutzkompendiums thematisiert, jedoch ohne dabei Cloud-spezifische Aspekte zu berücksichtigen. So musste ein Großteil des Inhaltes

aus externer Fachliteratur bezogen werden, weshalb das IT-Grundschutz-Kompendium hier insgesamt lediglich ein begrenzt-nutzbares Werkzeug darstellt, um die angestrebte Aufwandsreduktion zu erreichen. Zudem konnte kein Anspruch auf Vollständigkeit für die Bedrohungsübersicht erfüllt werden, obwohl das im Zuge der Cloud-Nutzung geltende Shared-Responsibility-Modell sowie die Integration von verwalteten Cloud-Diensten bereits viele Zuständigkeiten an den Cloud-Anbieter beziehungsweise Dienste-Anbieter auslagert haben. Jedoch ergibt sich selbst für den Betrieb der Anwendung innerhalb einer minimalen Systemarchitektur ein schlichtweg zu hoher Umfang an möglichen Bedrohungen. Aus diesem Grund konnten nur eine Auswahl an priorisierten Bedrohungen behandelt werden, sodass diese Arbeit als eine Basis für weitere Bedrohungsanalysen dienen kann, aber nicht unverändert übernommen werden sollte. Ähnliches gilt für die erarbeiteten Maßnahmen.

Auch eine vollständige Risikoeinstufung beläuft sich auf einen zu hohen Umfang für diese Arbeit, sodass lediglich ein Auszug im relevanten Text dargestellt werden konnte. Hier können jedoch zusätzliche Informationen dem Anhang entnommen werden.

5.2 Fazit

Ziel dieser Arbeit war es, eine Bedrohungsanalyse anhand eines exemplarischen Anwendungsszenarios für den Betrieb einer Shared Responsibility Cloud-Infrastruktur mittels des IT-Grundschutzes durchzuführen.

Dazu wurde, wie bereits erwähnt, ein exemplarisches Anwendungsszenario für den Betrieb einer Anwendung in der Cloud definiert. Zudem wurde mittels des IT-Grundschutzes ein Informationsverbund ausgearbeitet und einzelne Systeme beziehungsweise Zielobjekte festgelegt. Für diese Zielobjekte wurden insgesamt 25 relevante Bedrohungen herausgearbeitet. Außerdem die Relevanz für das vorliegende Anwendungsszenario erläutert, beeinträchtige Grundwerte der IT-Sicherheit genannt und die betroffene Zielobjekte des festgelegten Informationsverbundes konkretisiert. Damit konnte einerseits sowohl gezeigt werden, dass relevante Bedrohungen existieren und andererseits welche konkreten Bedrohungen auf den Informationsverbund einwirken. Dadurch konnte die erste Forschungsfrage, welche Bedrohungen, Schwachstellen und Angriffe für den Betrieb in einer IaaS Cloud-Umgebung ohne bisherige Sicherheitsmaßnahmen ergeben, im vorderen Teil dieser Arbeit beantwortet werden.

Des Weiteren wurde eine Risikoanalyse für diese Bedrohungen durchgeführt. Im Rahmen dieser konnten mittels des empfohlenen Vorgehens aus dem IT-Grundschutz für die 25 Bedrohungen pro Zielobjekt entsprechende Risiken definiert werden. Diesen wurden mittels entsprechenden Beschreibungen und Bewertungen für das vorliegende Anwendungsszenario begründet. Insbesondere konnten dabei für den gesamten Informationsverbund fünf Bedrohungen mit einer als sehr hoch klassifizierten Risikokategorie herausgearbeitet werden und diverse weitere Bedrohungen mit einer hohen Risikokategorie. Dadurch konnte die Beantwortung der zweiten Forschungsfrage, welche konkreten Risiken aus den Bedrohungen, Schwachstellen und Angriffen für den Betrieb einer Anwendung in einer IaaS Cloud-Umgebung entstehen, erzielt werden.

Im Anschluss wurden insgesamt 19 Sicherheitsmaßnahmen definiert, um diese Risiken zu behandeln. Besonders bezüglich Cloud-spezifischer Maßnahmen, wie beispielsweise der Durchsetzung Zero-Trust-Ansatz, wurden zusätzliche Hintergrundinformationen gegeben, die relevant sind, um einen solchen Ansatz im eigenen System etablieren zu können. Abschließend wurden Handlungsempfehlungen für eine effektive Umsetzung der Maßnahmen erläutert, sodass speziell die als sehr hoch klassifizierten Risiken angemessen behandelt werden können. Des Weiteren wurden Einschätzungen gegeben, inwiefern die vorgegebenen Handlungsempfehlungen die Risiken vermieden, reduziert oder transferiert werden. So konnte hiermit auch die letzte Forschungsfrage beantwortet werden, welche Maßnahmen und Handlungsempfehlungen umgesetzt werden sollten, um die vorliegenden Risiken angemessen zu behandeln.

5.3 Ausblick

Da im Rahmen dieser Arbeit der Fokus auf eine minimale Systemarchitektur lag, kann das Anwendungsszenario für weiteren Forschungen beliebig erweitert werden. Beispielsweise setzten immer mehr Unternehmen eine Multi-Cloud beziehungsweise Hybrid-Cloud-Architektur ein. Der Einsatz einer solchen Architektur hätte deutlichen Einfluss auf eine Bedrohungsanalyse und könnte in nachfolgenden Arbeiten untersucht werden.

Des Weiteren können verschiedene Schwerpunkte gesetzt werden, insofern dass Systeme betrachtet werden, in denen einige Cloud-spezifische Sicherheitsmaßnahmen bereits umgesetzt wurden. Beispielsweise könnte ein System untersucht werden, in welchem eine Zero-Trust-Strategie bereits implementiert wurde. Damit könnte der direkte Einfluss von den hier genannte Maßnahmen auf das Bedrohungsszenario untersucht werden.

Da außerdem das Konzept des Cloud-Computings mit einem Aufwärtstrend einhergeht, werden Konzepte stetig weiterentwickelt. Insbesondere hinsichtlich des sich etablierenden Internet of Things, neuer 5G/6G-Netzwerke und Blockchain-Technologien entstehen neue Herausforderungen, um innerhalb der Cloud eine angemessene Informationssicherheit zu implementieren. Von daher ist zu erwarten, dass diese Bedrohungsanalyse möglicherweise in regelmäßigen Abständen mit dem neusten Stand der Forschungen aktualisiert werden sollte. Auch dies kann im Rahmen von nachfolgenden Arbeiten umgesetzt werden.

Ergänzend kommt dazu, dass sich nicht nur die technologischen Aspekte stetig weiterentwickeln. Auch das IT-Grundschutz-Kompendium wird jährlich aktualisiert. So könnten zukünftig neue Bausteine bezüglich Cloud-spezifischer Bedrohungen und Maßnahmen ergänzt werden. So sollte diese Bedrohungsanalyse also nicht nur bezüglicher technischer Fortschritte aktualisiert werden, sondern Inhalte neuer Auflagen des IT-Grundschutz-Kompendiums beziehungsweise des IT-Grundschutzes sollten in späteren Forschungen identifiziert und ebenfalls inkludiert werden.

Literaturverzeichnis

[1] Aceto, Guiseppe ; Botta, Alessio ; Donato, Walter de ; Pescape, Antonio: Cloud monitoring: A survey / University of Napoli. URL http://dx.doi.org/10.1016/j.comnet.2013.04.001, 2013. – Forschungsbericht. Zugriffsdatum: 2023-05-13

[2] Agarwal, Abhishek ; Prasad, Ayush ; Rustogi, Rishabh ; Mishra, Sweta: Detection and mitigation of fraudulent resource consumption attacks in cloud using deep learning approachAuthor links open overlay panel. In: Journal of Information Security and Applications 56 (2021), Februar. – URL https://doi.org/10.1016/j.jisa.2020.102672. – Zugriffsdatum: 2023-05-14

[3] Ahlborn, Karl-Wilhelm: LfD: Der CLOUD Act – Zugriff von US-Behörden auf Daten in der EU. (2020), September. – URL https://datenschutz.nibis.de/2020/09/07/der-cloud-act-zugriff-von-us-behoerden-auf-daten-in-der-eu/. – Zugriffsdatum: 2023-08-23

[4] Aligarh Muslim University (Veranst.): Trust Management Issues in Cloud Computing Ecosystems. URL https://dx.doi.org/10.2139/ssrn.3358749, 2020. – Zugriffsdatum: 2023-05-21

[5] Amazon: Was ist eine API? (o. D.). – URL https://aws.amazon.com/de/what-is/api/. – Zugriffsdatum: 2023-06-11

[6] Amazon Web Services: AWS Well-Architected Framework. (2023), April. – URL https://docs.aws.amazon.com/pdfs/wellarchitected/latest/framework/wellarchitected-framework.pdf. – Zugriffsdatum: 2023-07-22

[7] Aslan, Ömer ; Ozkan-Okay, Merve ; Gupta, Deepti: Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. In: IEEE Access 9 (2021), S. 83252–83271. – Zugriffsdatum: 2023-06-12

[8] Balaji, Aditya: 5 ways to optimize your backup costs with Azure Backup. (2020), September. – URL https://azure.microsoft.com/en-us/blog/5-ways-to-optimize-your-backup-costs-with-azure-backup/. – Zugriffsdatum: 2023-07-26

[9] Barker, William C.: Guideline for Identifying anInformation System as aNational Security System / National Institute of Standards and Technology. URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf, August 2003. – Forschungsbericht. Zugriffsdatum: 2023-05-15

[10] Bharadwaj, Deepak ; Bhattacharya, Anamika ; Chakkaravarthy, Manivannan: Cloud Threat Defense – a Threat Protection and Security Compliance Solution, URL https://ieeexplore.ieee.org/document/8648627, 2018. – Zugriffsdatum: 2022-11-21

[11] Bhardwaj, Aanshi ; Mangat, Veenu ; Vig, Renu ; Halder, Subir ; Conti, Mauro: Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. In: Computer Science Review 39 (2021), S. 100332. – URL https://www.sciencedirect.com/science/article/pii/S1574013720304329. – Zugriffsdatum: 2023-06-08. – ISSN 1574-0137

[12] Bottenberg, Petra ; Didier Essoh, Alex ; Förster, Stefanie ; Gilles, Daniel ; Göhler, Florian ; Hillebrand, Florian ; Hoffmann, Brigitte ; Jung, Cäcilia ; Klein, Birger ; Nöhles, Alexander ; Oppelt, Johannes ; Wiemers, Christoph: IT-Grundschutz-Kompendium. Bundesamt für Sicherheit in der Informationstechnik, 2023. – ISBN 978-3-8462-0906-6

[13] Bošnjak, L. ; Sreš, J. ; Brumen, B.: Brute-force and dictionary attack on hashed real-world passwords. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, S. 1161–1166. – Zugriffsdatum: 2023-06-16

[14] Bundesamt für Sicherheit in der Informationstechnik (Veranst.): BSI-Standard 200-2. Bundesamt für Sicherheit in der Informationstechnik, November 2017. – URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2. – Zugriffsdatum: 2023-03-13

[15] Bundesamt für Sicherheit in der Informationstechnik: Cloud Computing Grundlagen. (o. D.). – URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html. – Zugriffsdatum: 2023-07-12

[16] Bundesamt für Sicherheit in der Informationstechnik: Fragen und Antworten zu Bußgeldern (§ 14 BSIG). (o. D.). – URL https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-Bussgelder/faq-bussgelder_node.html. – Zugriffsdatum: 2023-08-26

[17] Bundesamt für Sicherheit und Informationstechnik (Veranst.): BSI-Standard 100-4. Bundesamt für Sicherheit und Informationstechnik, 2008. – URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2. – Zugriffsdatum: 2023-05-11

[18] Bundesamt für Sicherheit und Informationstechnik (Veranst.): BSI-Standard 200-3. Bundesamt für Sicherheit und Informationstechnik, November 2017. – URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2. – Zugriffsdatum: 2023-03-13

[19] businesswire: Die Mehrheit der Unternehmen hat auch ein Jahr nach der Pandemie noch Bedenken bezüglich der Cybersicherheit im Homeoffice. (2021), Juni. – URL https://www.businesswire.com/news/home/20210602005101/de/. – Zugriffsdatum: 2023-06-14

[20] Carminati, Barbara: Secure Data Outsourcing. S. 2523–2528. In: LIU, LING (Hrsg.) ; ÖZSU, M. T. (Hrsg.): Encyclopedia of Database Systems. Boston, MA : Springer US, 2009. – URL https://doi.org/10.1007/978-0-387-39940-9_328. – Zugriffsdatum: 2023-05-12. – ISBN 978-0-387-39940-9

[21] Chen, Mingyi ; Yao, Yepeng ; Liu, Junrong ; Jiang, Bo ; Su, Liya ; Lu, Zhigang: A Novel Approach for Identifying Lateral Movement Attacks Based on Network Embedding. In: 2018 IEEE Intl Conf on Parallel & Distributed

Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), URL https://ieeexplore.ieee.org/abstract/document/8672383, 2018, S. 708–715. – Zugriffsdatum: 2023-07-02

[22] CLOUDFLARE: Was ist Anbieter-Lock-in? | Anbieter-Lock-in und Cloud Computing. – URL https://www.cloudflare.com/de-de/learning/cloud/what-is-vendor-lock-in/. – Zugriffsdatum: 2023-05-14

[23] CLOUDFLARE: Was sind Data-at-Rest? (o.D.). – URL https://www.cloudflare.com/de-de/learning/security/glossary/data-at-rest/. – Zugriffsdatum: 2023-08-17

[24] COMCRYPTO: TLS: Die Technologie für sichere Verschlüsselung und Kommunikation im Netz. (o.D.). – URL https://www.comcrypto.de/wissensecke/einfach-erklaert/was-ist-tls-verschluesselung.html. – Zugriffsdatum: 2023-08-24

[25] COMMVAULT: Replication of Virtual Machines. (2022), April. – URL https://documentation.commvault.com/v11/essential/87228_replication_of_virtual_machines.html. – Zugriffsdatum: 2023-06-05

[26] DRILLING, Thomas ; OSTLER, Ulrike: Was ist ein Cluster? (2017), März. – URL https://www.datacenter-insider.de/was-ist-ein-cluster-a-588715/. – Zugriffsdatum: 2023-05-23

[27] FADLALLAH, Hadi: Pricing on the Cloud. (2018), November. – URL https://towardsdatascience.com/pricing-on-the-cloud-9a2d3f61b67f. – Zugriffsdatum: 2023-08-09

[28] FINANZDIENSLEISTUNGSAUFSICHT, Bundesanstalt für: Thema Geldwäschebekämpfung: Zentrale Pflichten. o. D.. – URL https://www.bafin.de/dok/11481556. – Zugriffsdatum: 2023-05-22

[29] FINANZDIENSTLEISTUNGSAUFSICHT, Bundesanstalt für: Thema Geldwäschebekämpfung: Prävention von Geldwäsche und Terrorismusfinanzierung. 2018. – URL https://www.bafin.de/dok/7845892. – Zugriffsdatum: 2023-05-22

[30] Floyd, Blue: Was ist Platform as a Service? 2017. – URL https://www.cloudcomputing-insider.de/was-ist-platform-as-a-service-a-624296/?cflt=rdt&_lt=Y29udGVudF90ZWFzZXJ-YXJ0aWNsZX42MDUwNzF-c2VsZg. – Zugriffsdatum: 2023-03-04

[31] Floyd, Blue: Was ist Software as a Service? 2017. – URL https://www.cloudcomputing-insider.de/was-ist-software-as-a-service-a-622859/?cflt=rdt&_lt=Y29udGVudF90ZWFzZXJ-YXJ0aWNsZX42MjQyOTZ-c2VsZg. – Zugriffsdatum: 2023-03-04

[32] Frederiksen, Tore K. ; Hesse, Julia ; Poettering, Bertram ; Towa, Patrick: Attribute-based Single Sign-On: Secure, Private, and Efficient. (2023). – URL https://eprint.iacr.org/2023/915. – Zugriffsdatum: 2023-07-19

[33] Glover, Claudia: https://techmonitor.ai/technology/cybersecurity/pegasus-airline-data-breach-aws-bucket. (2022), August. – URL https://techmonitor.ai/technology/cybersecurity/pegasus-airline-data-breach-aws-bucket. – Zugriffsdatum: 2023-07-11

[34] Gonzales, Jason: Why Software Development Environments are Important and How to Manage them Effectively. (2022). – URL https://www.devzero.io/blog/why-software-development-environments-are-important-and-how-to-manage-them-effectively. – Zugriffsdatum: 2023-06-26

[35] Google: Cloud SQL Admin API. (2023). – URL https://cloud.google.com/sql/docs/mysql/admin-api/rest. – Zugriffsdatum: 2023-06-11

[36] Google: Naming Developer Environments. (2023), Juni. – URL https://cloud.google.com/appengine/docs/legacy/standard/php/creating-separate-dev-environments. – Zugriffsdatum: 2023-07-04

[37] Gutierrez, Carlos M. ; Jeffrey, William: Minimum Security Requirements for FederalInformation and Information Systems / U.S. Department of commerce and National institute of standards and technology. URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf, März 2006. – Forschungsbericht. Zugriffsdatum: 2023-03-02

[38] Haucke, Annika: Mit personenbezogenen Daten DSGVO-konform umgehen. 2023. – URL https://www.e-recht24.de/artikel/datenschutz/12808-was-sind-personenbezogene-daten.html. – Zugriffsdatum: 2023-05-26

[39] Hsu, Chin-Jung ; Nair, Vivek ; Menzies, Tim ; Freeh, Vincent W.: Scout: An Experienced Guide to Find the Best Cloud Configuration. In: CoRR abs/1803.01296 (2018). – URL http://arxiv.org/abs/1803.01296. – Zugriffsdatum: 2023-06-06

[40] Huang, Jingwei ; Nicol, David: A Formal-Semantics-Based Calculus of Trust. In: IEEE Internet Computing 14 (2010), 09, S. 38–46. – URL https://www.researchgate.net/publication/220490854_A_Formal-Semantics-Based_Calculus_of_Trust. – Zugriffsdatum: 2023-05-20

[41] Huang, Jungwei ; M Nicol, David: Trust mechanisms for cloud computing. In: Journal of Cloud Computing: Advances, Systems and Applications 2 (2013), Nr. 9. – URL https://doi.org/10.1186/2192-113X-2-9. – Zugriffsdatum: 2023-02-22

[42] Hussain, Muhammad I. ; He, Jingsha ; Zhu, Nafei ; Sabah, Fahad ; Zardari, Zulfiqar A. ; Hussain, Saqib ; Razque, Fahad: AAAA: SSO and MFA Implementation in Multi-Cloud to Mitigate Rising Threats and Concerns Related to User Metadata. In: Applied Sciences 11 (2021), Nr. 7. – URL https://www.mdpi.com/2076-3417/11/7/3012. – Zugriffsdatum: 2023-06-16. – ISSN 2076-3417

[43] IBM: Single Sign On (SSO). (o.D.). – URL https://www.ibm.com/de-de/topics/single-sign-on. – Zugriffsdatum: 2023-07-19

[44] IBM: Was ist Containerisierung? (o.D.). – URL https://www.ibm.com/de-de/topics/containerization. – Zugriffsdatum: 2023-07-21

[45] IBM: Was ist Lift-and-shift? (o.D.). – URL https://www.ibm.com/de-de/topics/lift-and-shift. – Zugriffsdatum: 2023-08-16

[46] IBM: Was ist Terraform? (o.D.). – URL https://www.ibm.com/de-de/topics/terraform. – Zugriffsdatum: 2023-07-21

[47] IBM Cloud Education: Top 7 Benefits of Kubernetes. (2022). – URL https://www.ibm.com/cloud/blog/top-7-benefits-of-kubernetes. – Zugriffsdatum: 2023-07-21

[48] Informationstechnik, Bundesamt für Sicherheit in der: ISO 27001 Zertifizierung auf Basis von IT-Grundschutz. o. D.. – URL https://www.bsi.bund.de/dok/6604686. – Zugriffsdatum: 2023-05-26

[49] Informationstechnik, Bundesamt für Sicherheit in der: Was ist Malware? (o. D.). – URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Malware/malware_node.html. – Zugriffsdatum: 2023-06-12

[50] insider.de cloudcomputing: Was ist On-Premises? 2017. – URL https://www.cloudcomputing-insider.de/was-ist-on-premises-a-f20cfc9b4abfecaacd6b88ef817b2993/. – Zugriffsdatum: 2023-05-22

[51] jetbrains: CI/CD Best Practices. (o.D.). – URL https://www.jetbrains.com/teamcity/ci-cd-guide/ci-cd-best-practices/. – Zugriffsdatum: 2023-07-04

[52] Kaiser, Florian K. ; Andris, Leon J. ; Tennig, Tim F. ; Iser, Jonas M. ; Wiens, Marcus ; Schultmann, Frank: Cyber threat intelligence enabled automated attack incident response. In: 2022 3rd International Conference on Next Generation Computing Applications (NextComp), 2022, S. 1–6. – Zugriffsdatum: 2023-07-21

[53] Karlsetter, Florian ; Srocke, Dirk: Was sind Regionen und Availability Zones? (2018), Juli. – URL https://www.cloudcomputing-insider.de/was-sind-regionen-und-availability-zones-a-ff600314864f9bb829360230ea72b60b/. – Zugriffsdatum: 2023-06-14

[54] Kass, Howard: FBI: Covid-19 Cyberattacks Spike 400 % in Pandemic. 2020. – URL https://www.msspalert.com/cybersecurity-news/fbi-covid-19-cyberattacks-spike-400-in-pandemic/. – Zugriffsdatum: 2023-03-07

[55] Krüger, Phillip S. ; Brauchle, Jan-Phillip: The European Union, Cybersecurity, and the Financial Sector: A Primer. In: Cyber Policy Initiative Working Paper Series 9 (2021), März. – URL https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055. – Zugriffsdatum: 2023-05-26

[56] Lane, Michael ; Shrestha, Anup ; Omar, Ali: Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client Organisation, URL https://www.researchgate.net/publication/322049523_Managing_the_Risks_of_Data_Security_and_Privacy_in_the_Cloud_A_Shared_Responsibility_between_the_Cloud_Service_Provider_and_the_Client_Organisation, Dezember 2017. – Zugriffsdatum: 2023-03-02

[57] Loukides, Mike: The Cloud in 2021:Adoption Continues / O'Reilly. URL https://get.oreilly.com/ind_the-cloud-in-2021-adoption-continues.html, 2021. – Forschungsbericht. Zugriffsdatum: 2023-02-17

[58] Manral, Bharat ; Somani, Gaurav ; Choo, Kim-Kwang R. ; Conti, Mauro ; Gaur, Manoj S.: A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. In: ACM Comput. Surv. 52 (2019), nov, Nr. 6. – URL https://doi.org/10.1145/3361216. – Zugriffsdatum: 2023-06-28. – ISSN 0360-0300

[59] Mell, Peter ; Grance, Timothy: The NIST Definition of Cloud Computing / National Institute of Standards and Technology. URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, 2011. – Forschungsbericht. Zugriffsdatum: 2022-12-03

[60] Microsoft: Autoscaling. (2022). – URL https://learn.microsoft.com/en-us/azure/architecture/best-practices/auto-scaling. – Zugriffsdatum: 2023-06-15

[61] Microsoft: Reliability design principles. (2022). – URL https://learn.microsoft.com/en-us/azure/well-architected/resiliency/principles. – Zugriffsdatum: 2023-06-04

[62] Microsoft: Azure Backup - Frequently asked questions. (2023). – URL https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq#how-can-i-move-data-from-the-recovery-services-vault-to-on-premises. – Zugriffsdatum: 2023-06-15

[63] Microsoft: Azure best practices for network security. (2023), März. – URL https://learn.microsoft.com/en-us/azure/security/fundamentals/network-best-practices. – Zugriffsdatum: 2023-07-11

[64] Microsoft: Azure Monitor Logs overview. (2023), Juni. – URL https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs. – Zugriffsdatum: 2023-07-01

[65] Microsoft: Azure subscription and service limits, quotas, and constraints. (2023), Mai. – URL https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits. – Zugriffsdatum: 2023-06-04

[66] Microsoft: Cloud exit planning guidelines for financial services institutions. (2023). – URL https://www.microsoft.com/en-us/industry/blog/financial-services/2020/11/23/cloud-exit-planning-guidelines-for-financial-services-institutions/. – Zugriffsdatum: 2023-06-24

[67] Microsoft: Collect events and performance counters from virtual machines with Azure Monitor Agent. (2023). – URL https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent. – Zugriffsdatum: 2023-07-02

[68] Microsoft: Deployment pipelines best practices. (2023), Mai. – URL https://learn.microsoft.com/en-us/power-bi/create-reports/deployment-pipelines-best-practices. – Zugriffsdatum: 2023-07-04

[69] Microsoft: Design reliable Azure applications. (2023), Mai. – URL https://learn.microsoft.com/en-us/azure/well-architected/resiliency/app-design. – Zugriffsdatum: 2023-06-04

[70] Microsoft: Key management in Azure. (2023), März. – URL https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management. – Zugriffsdatum: 2023-06-17

[71] Microsoft: Mission-critical global HTTP ingress. (2023), April. – URL https://learn.microsoft.com/en-us/azure/architecture/guide/networking/global-web-applications/mission-critical-global-http-ingress. – Zugriffsdatum: 2023-07-12

[72] Microsoft: Verwalten von Konten für den Notfallzugriff in Azure AD. (2023), März. – URL https://learn.microsoft.com/de-de/azure/active-

directory/roles/security-emergency-access. – Zugriffsdatum: 2023-07-28

[73] Microsoft: Virtual network traffic routing. (2023). – URL https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview. – Zugriffsdatum: 2023-07-11

[74] Microsoft: Was sind Azure Monitor-Warnungen? (2023), Juni. – URL https://learn.microsoft.com/de-de/azure/azure-monitor/alerts/alerts-overview. – Zugriffsdatum: 2023-07-02

[75] Microsoft: What is the Azure Backup service? (2023), April. – URL https://learn.microsoft.com/en-us/azure/backup/backup-overview. – Zugriffsdatum: 2023-07-26

[76] Microsoft: Azure Backup - Frequently asked questions. (o.D.). – URL https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq. – Zugriffsdatum: 2023-07-26

[77] Microsoft: Penetration Testing Rules of Engagement. (o.D.). – URL https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement. – Zugriffsdatum: 2023-08-28

[78] Modi, Chirag ; Patel, Dhiren ; Borisaniya, Bhavesh ; Patel, Avi ; Rajaran, Muttukrishnan: A Survey on Security Issues and Solutions at Different Layers of Cloud Computing / City University London. URL https://doi.org/10.1007/s11227-012-0831-5, 2013. – resreport. Zugriffsdatum: 2023-05-12

[79] National Cyber Security Centre: Preventing Lateral Movement. (2018), Februar. – URL https://www.ncsc.gov.uk/guidance/preventing-lateral-movement. – Zugriffsdatum: 2023-07-02

[80] Neville, Lois: What is a Cloud Outage? A Beginner's Guide. 2022. – URL https://www.divio.com/blog/what-is-a-cloud-outage-a-beginners-guide/. – Zugriffsdatum: 2023-05-12

[81] Odun-Ayo, Isaac ; Ehi Idoko, Blessing: Cloud Trust Management – Issues and Developments, URL https://www.researchgate.net/publication/332143965_Cloud_Trust_Management, Oktober 2018. – Zugriffsdatum: 2023-05-16

[82] Ometov, Aleksandr ; Bezzateev, Sergey ; Mäkitalo, Niko ; Andreev, Sergey ; Mikkonen, Tommi ; Koucheryavy, Yevgeni: Multi-Factor Authentication: A Survey. In: Cryptography 2 (2018), Nr. 1. – URL https://www.mdpi.com/2410-387X/2/1/1. – Zugriffsdatum: 2023-07-20. – ISSN 2410-387X

[83] Opara-Martins, Justice ; Sahandi, Reza ; Tian, Feng: Critical analysis of vendor lock-in and itsimpact on cloud computing migration: abusiness perspective / Bournemouth University. URL https://doi.org/10.1186/s13677-016-0054-z, April 2016. – Forschungsbericht. Zugriffsdatum: 2023-05-13

[84] Pahl, Claus ; Jamshidi, Pooyan ; Zimmermann, Olaf: Architectural Principles for Cloud Software. In: ACM Trans. Internet Technol. 18 (2018), feb, Nr. 2. – URL https://doi.org/10.1145/3104028. – Zugriffsdatum: 2023-06-01. – ISSN 1533-5399

[85] Radware: Radware Full Year 2022 Report: Malicious DDoS Attacks Rise 150 (2023), Februar. – URL https://www.radware.com/newsevents/pressreleases/2023/radware-full-year-2022-report-malicious-ddos-attacks/. – Zugriffsdatum: 2023-07-16

[86] Ramokapane, Marvin ; Rashid, Awais ; Such, Jose M.: Assured deletion in the cloud:requirements, challenges and future directions, URL https://doi.org/10.1145/2996429.2996434, Mai 2016. – Zugriffsdatum: 2023-05-14

[87] rapid7: Best Practices für die Cloud Network Security. (o.D.). – URL https://www.rapid7.com/de/cybersecurity-grundlagen/cloud-network-security/. – Zugriffsdatum: 2023-06-25

[88] redhat: Was sind virtuelle Maschinen (VM) und wie funktionieren sie? (2023), März. – URL https://www.redhat.com/de/topics/virtualization/what-is-a-virtual-machine. – Zugriffsdatum: 2023-06-24

[89] Reed, Catherine: https://firewalltimes.com/social-engineering-statistics/. (2022), Mai. – URL https://firewalltimes.com/social-engineering-statistics/. – Zugriffsdatum: 2023-07-16

[90] Rose, Scott ; Borchert, Oliver ; Mitchell, Stu ; Sean, Connelly: Zero Trust Architecture. (2020), August. – URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. – Zugriffsdatum: 2023-07-18

[91] Salahdine, Fatima ; Kaabouch, Naima: Social Engineering Attacks: A Survey. In: Future Internet 11 (2019), Nr. 4. – URL https://www.mdpi.com/1999-5903/11/4/89. – Zugriffsdatum: 2023-06-05. – ISSN 1999-5903

[92] Sarkar, Sirshak ; Choudhary, Gaurav ; Shandilya, Shishir K. ; Hussain, Azath ; Kim, Hwankuk: Security of Zero Trust Networks in Cloud Computing: A Comparative Review. In: Sustainability 14 (2022), Nr. 18. – URL https://www.mdpi.com/2071-1050/14/18/11213. – Zugriffsdatum: 2023-07-18. – ISSN 2071-1050

[93] Schaffer, Henry: Will You Ever Need an Exit Strategy? In: IT Professional 16 (2014), Nr. 2, S. 4–6. – Zugriffsdatum: 2023-06-24

[94] Schonschek, Oliver ; Schmitz, Peter: IT-Security umfasst die Sicherheit der ganzen IT. 2017. – URL https://www.security-insider.de/it-security-umfasst-die-sicherheit-der-ganzen-it-a-578480/. – Zugriffsdatum: 2023-03-05

[95] Shackleford, Dave: Cloud incident response: Frameworks and best practices. (2023). – URL https://www.techtarget.com/searchsecurity/tip/Cloud-incident-response-Frameworks-and-best-practices. – Zugriffsdatum: 2023-05-11

[96] Shahnawaz, Ahmand ; Mehfuz, Shabana ; Beg, Javed: Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. In: The Journal of Supercomputing 79 (2022), November. – URL https://doi.org/10.1007/s11227-022-04964-9. – Zugriffsdatum: 2023-06-16

[97] Siller, Helmut: Know-your-Customer-Prinzip (KYC). 2018. – URL https://wirtschaftslexikon.gabler.de/definition/know-your-customer-prinzip-kyc-53389/version-276482. – Zugriffsdatum: 2023-05-26

[98] Sing, Ashish ; Chatterjee, Kakali: Cloud security issues and challenges: A survey / National Institute of Technology Patna. URL https://www.sciencedirect.com/science/article/abs/pii/S1084804516302983, 2016. – Forschungsbericht. Zugriffsdatum: 2022-11-24

[99] Somani, Gaurav ; Gaur, Manoj S. ; Sanghi, Dheeraj ; Conti, Mauro: DDoS attacks in cloud computing: Collateral damage to non-targets. In: Computer Networks 109 (2016), S. 157–171. – URL https://www.sciencedirect.com/science/article/pii/S1389128616300901. – Zugriffsdatum: 2023-06-10. – ISSN 1389-1286

[100] Sophos: Ransomware-Report 2023. (2023). – URL https://www.sophos.com/de-de/content/state-of-ransomware. – Zugriffsdatum: 2023-08-25

[101] Standards, National I. of ; Technology: Cloud Auditor. – URL https://csrc.nist.gov/glossary/term/cloud_auditor. – Zugriffsdatum: 2023-05-21

[102] Suske, Sophia: DSGVO: Was sollten Webseitenbetreiber und Unternehmer über die Datenschutz-Grundverordnung wissen? 2022. – URL https://www.e-recht24.de/datenschutzgrundverordnung.html. – Zugriffsdatum: 2023-03-06

[103] Säckel, André: Schutzziele der Informationssicherheit und ihre Bedeutung. 2022. – URL https://www.dqsglobal.com/de-de/blog/schutzziele-der-informationssicherheit-und-ihre-bedeutung. – Zugriffsdatum: 2023-03-05

[104] Thalesgroup: 2022 ThalesData Threat Report / Thales. URL https://mb.cision.com/Public/20506/3530950/b55a39d9e52a4074.pdf, 2022. – Forschungsbericht. Zugriffsdatum: 2023-02-17

[105] Union, Europäisches P. und Rat der europäischen: RICHTLINIE (EU) 2015/849 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. ASP 02G354,Rue Wiertz 60, B-1047 Brüssel: Europäisches Parlament und Rat der europäischen Union (Veranst.), Mai 2015. – URL https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L0849. – Zugriffsdatum: 2023-05-22

[106] UP KRITIS: Empfehlungen zur Nutzung von CloudDienstleistungen in Kritischen Infrastrukturen. (2020), November. – URL https://www.bsi.bund.de/dok/upk-empfehlungen-cloudnutzung. – Zugriffsdatum: 2023-07-31

[107] UP KRITIS: Empfehlungen zur Vorbereitung einer Exit-Strategie bei Nutzung von Cloud-Dienstleistungen. (2022), März. – URL https://www.bsi.

bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-exit-strategie-cloud-dienstleistungen.html. – Zugriffsdatum: 2023-07-30

[108] Validatis: Politisch exponierte Personen. (o.D.). – URL https://www.validatis.de/kyc-prozess/news-fachwissen/politisch-exponierte-personen/. – Zugriffsdatum: 2023-04-19

[109] Varghese, Blesson ; Buyya, Rajkumar: Next Generation Cloud Computing: New Trends and Research Directions. In: CoRR abs/1707.07452 (2017). – URL http://arxiv.org/abs/1707.07452. – Zugriffsdatum: 2023-06-04

[110] Velimirovic, Andreja: Cloud Outage: Why and How Does It Happen? 2022. – URL https://phoenixnap.com/blog/cloud-outage. – Zugriffsdatum: 2023-05-12

[111] Volhøj, Jens C.: The importance of a Cloud Exit Strategy. (2023). – URL https://www.linkedin.com/pulse/importance-cloud-exit-strategy-qa-part-1-jens-christian-volh\T1\oj/. – Zugriffsdatum: 2023-06-24

[112] Wikipedia: Cloud-native Computing. (o.D.). – URL https://de.wikipedia.org/wiki/Cloud-native_Computing. – Zugriffsdatum: 2023-08-28

[113] Wikipedia contributors: Differential backup — Wikipedia, The Free Encyclopedia. 2022. – URL https://en.wikipedia.org/w/index.php?title=Differential_backup&oldid=1127301806. – Zugriffsdatum: 2023-08-28

[114] Wikipedia contributors: Client-side encryption — Wikipedia, The Free Encyclopedia. 2023. – URL https://en.wikipedia.org/w/index.php?title=Client-side_encryption&oldid=1135743450. – Zugriffsdatum: 2023-08-28

[115] Zissis, Dimitrios ; Lekkas, Dimitrios: Addressing cloud computing security issues. In: Future Generation Computer Systems 28 (2012). – URL https://doi.org/10.1016/j.future.2010.12.006. – Zugriffsdatum: 2023-05-17

A Anhang

A.1 Strukturanalyse und Schutzbedarfsfeststellung

A.1.1 Anwendungen im System der MakeABank GmbH

Bezeichnung: A001	**Beschreibung der Gruppe der Zielobjekte:** MaBCloud Frontend
Plattform/Baustein: individuelle Webanwendung	**Verantwortlich/Administrator:** IT-Betrieb, Mitarbeiter*innen

Vertraulichkeit: Normal	**Begründung für Vertraulichkeit:** Besonders sensible Kundendaten werden zwar temporär angezeigt und Eingaben ans Backend geschickt, aber nichts permanent gespeichert. Es besteht außerdem keine direkte Anbindung zur Datenbank.
Integrität: Hoch	**Begründung für Integrität:** Anwendung enthält nur temporär sensible Kundendaten. Eingaben, die Datenveränderung bewirken, müssen trotzdem nachvollziehbar- und zuordenbar sein.
Verfügbarkeit: Hoch	**Begründung für Verfügbarkeit:** Verteilungsprinzip greift (falls VM ausfällt, kann andere einfach dazu geschaltet werden). Trotzdem ist Verfügbarkeit des Frontends essenziell für den Betrieb des ganzen „MaBCloud“ Systems.

Bezeichnung: A002	**Beschreibung der Gruppe der Zielobjekte:** MaBCloud Backend
Plattform/Baustein: individuelle Java Anwendung	**Verantwortlich/Administrator:** IT-Betrieb

Vertraulichkeit: Sehr hoch	**Begründung für Vertraulichkeit:** Die Backend-Anwendung kann direkt mit der Datenbank kommunizieren und hat deshalb einen direkten Zugriff auf besonders sensible beziehungsweise schützenswerte Daten.
Integrität: Sehr hoch	**Begründung für Integrität:** Verweis Vertraulichkeit. Derart sensible Daten dürfen nicht unberechtigt verändert werden. Da vollständige Sicherstellung unrealistisch, muss zumindest jede Datenveränderung nachvollziehbar sein.
Verfügbarkeit: Hoch	**Begründung für Verfügbarkeit:** Verteilungsprinzip (falls VM ausfällt, kann andere einfach dazu geschaltet werden). Trotzdem ist Verfügbarkeit des Backends essenziell für den Betrieb des ganzen „MaBCloud“ Systems

Bezeichnung: A003	**Beschreibung der Gruppe der Zielobjekte:** Objektrelationales Datenbanksystem
Plattform/Baustein: Datenbank	**Verantwortlich/Administrator:** IT-Betrieb

Vertraulichkeit: Sehr hoch	**Begründung für Vertraulichkeit:** Speichert und führt Operationen auf einen großen Teil von besonders schützenswerten Geschäftsdaten aus.
Integrität: Sehr hoch	**Begründung für Integrität:** Verweis Vertraulichkeit. Derart sensible Daten dürfen nicht unberechtigt verändert werden. Da vollständige Sicherstellung unrealistisch, muss zumindest jede Datenveränderung unbedingt nachvollziehbar sein.
Verfügbarkeit: Hoch	**Begründung für Verfügbarkeit:** Verteilungsprinzip (falls VM ausfällt, kann andere einfach dazu geschaltet werden). Trotzdem ist Verfügbarkeit der Datenbankanwendung essenziell für den Betrieb des ganzen „MaBCloud“ Systems

Bezeichnung: A004	**Beschreibung der Gruppe der Zielobjekte:** Virtuelle Firewall
Plattform/Baustein: Dienst eines externen Anbieters	**Verantwortlich/Administrator:** IT-Betrieb (Konfiguration), externer Firewall as a Service Anbieter

Vertraulichkeit: Normal	**Begründung für Vertraulichkeit:** Konfigurationseigenschaften sollten vertraulich bleiben, stellen allerdings aus der Perspektive einer Priorisierung weniger schützenswerte Daten dar. Zuständigkeit bezüglich der Sicherheit liegt zudem zum größten Teil bei dem Anbieter des Firewall-Dienstes.
Integrität: Normal	**Begründung für Integrität:** Konfigurationen dürfen nicht unberechtigt verändert werden. Zuständigkeit bezüglich der Sicherstellung dessen liegt allerdings ebenfalls zum größten Teil bei dem Anbieter des Firewall-Dienstes.
Verfügbarkeit: Normal	**Begründung für Verfügbarkeit:** Ein Ausfall der Firewall würde zwar das System gegenüber Angriffen von außen öffnen allerdings wird Verfügbarkeit des Firewall-Dienstes in der Regel ebenfalls durch den Anbieter sichergestellt.

Bezeichnung: A005	**Beschreibung der Gruppe der Zielobjekte:** Cloud-Konsole/Cloud-Web-Administrationsoberfläche
Plattform/Baustein: Dienst eines externen Anbieters	**Verantwortlich/Administrator:** IT-Betrieb (Konfiguration), Cloud-Anbieter

Vertraulichkeit: Hoch	**Begründung für Vertraulichkeit:** Hier können sämmtliche administrative Konfigurationen eingesehen und bearbeitet werden. Auch administrative Verwaltungsoptionen zur Infrastruktur können vorgenommen werden. Ein großer Teil der Zuständigkeiten bezüglich der Sicherheit liegen allerdings beim Cloud-Anbieter.
Integrität: Hoch	**Begründung für Integrität:** Durch die Möglichkeit grundlegende administrative Konfigurationen vorzunehmen zu können, dürfen keine Änderungen unberechtigt stattfinden, sonst ist die Funktionalität des Systems bedroht. Zumindest muss jede Änderung genau nachvollziehbar sein, besonders in Bezug auf Wiederherstellungsmaßnahmen. Hier liegt allerdings ebenfalls ein großer Teil der Zuständigkeiten beim Cloud-Anbieter.
Verfügbarkeit: Hoch	**Begründung für Verfügbarkeit:** Aufgrund fehlender Administrationsmöglichkeiten besonders in Fehlersituationen kann ein Ausfall den Betrieb des gesamten Systems gefährden und ist nicht tolerierbar. Die Ausfallsicherheit wird allerdings in der Regel durch den Cloud-Anbieter sichergestellt.

Bezeichnung: A006	**Beschreibung der Gruppe der Zielobjekte:** Virtuelle Loadbalancer
Plattform/Baustein: Dienst eines externen Anbieters	**Verantwortlich/Administrator:** IT-Betrieb (Konfiguration), Cloud-Anbieter

Vertraulichkeit: Normal	**Begründung für Vertraulichkeit:** Enthält zwar Regeln zur Lastverteilung auf verschiedene Gruppen von virtuellen Maschinen, allerdings sind diese aus Perspektive einer Priorisierung keine besonders sensiblen Informationen.
Integrität: Normal	**Begründung für Integrität:** Keine besonders sensiblen Informationen. Trotzdem dürfen Konfiguration nicht unberechtigt verändert werden. Zuständigkeit bezüglich der Sicherstellung dessen liegt allerdings ebenfalls zum größten Teil bei dem Cloud-Anbieter beziehungsweise Anbieter des Loadbalancer-Dienstes.
Verfügbarkeit: Normal	**Begründung für Verfügbarkeit:** Verteilungsprinzip gilt. Andere Loadbalancer können dynamisch dazugeschaltet werden. Zuständigkeit bezüglich einer hohen Verfügbarkeit liegt hier ebenfalls beim Diensteanbieter.

Tabelle A.1: Strukturanalyse und Schutzbedarfsfeststellung für Anwendungen im System der MakeABank GmbH nach BSI-Standard 200-2 [14]

A.1.2 Kommunikationsverbindungen im System der MakeABank GmbH

Bezeichnung: K001	**Beschreibung der Gruppe der Zielobjekte:** Verbindung zwischen Cloud-Netzkomponenten
Plattform/Baustein: Netz und Kommunikation	**Verantwortlich/Administrator:** IT-Betrieb (Konfiguration), Cloud-Anbieter

Vertraulichkeit: Hoch	**Begründung für Vertraulichkeit:** Maximumsprinzip greift, da Komponenten mit einem sehr hohen Schutzbedarf Daten über diese Verbindung schicken. Jedoch wird die Infrastruktur auf physischer Ebene durch den Cloud-Anbieter abgesichert.
Integrität: Hoch	**Begründung für Integrität:** Siehe Vertraulichkeit.
Verfügbarkeit: Normal	**Begründung für Verfügbarkeit:** Ohne eine funktionierende Verbindung zwischen den Komponenten ist das gesamte System nicht funktionsfähig. Allerdings kann durch Redundanz der Ausfall einzelner Verbindungen toleriert werden und große Teile der Zuständigkeit liegen beim Cloud-Anbieter.

Bezeichnung: K002	**Beschreibung der Gruppe der Zielobjekte:** Verbindung zwischen Clients und Cloud-Endpunkt
Plattform/Baustein: Netz und Kommunikation	**Verantwortlich/Administrator:** IT-Betrieb (teilweise)

Vertraulichkeit: Hoch	**Begründung für Vertraulichkeit:** Derart sensible Daten müssen zwingend ohne Einsicht von Dritten zwischen dem Cloud-Endpunkt und dem Endnutzer transportiert werden.
Integrität: Sehr hoch	**Begründung für Integrität:** Siehe Vertraulichkeit.
Verfügbarkeit: Hoch	**Begründung für Verfügbarkeit:** Ohne Verbindung zwischen den Clients und einem Cloud-Endpunkt kann keine Administration stattfinden. Das System ist ohne möglichen Zugriff sich selbst überlassen, was nicht tolerierbar ist. Allerdings liegt die Infrastruktur des öffentlichen Internets als Kommunikationskanal außerhalb des Zuständigkeitsbereiches der MakeABank GmbH.

Tabelle A.2: Strukturanalyse und Schutzbedarfsfeststellung für Kommunikationsverbindungen im System der MakeABank GmbH nach BSI-Standard 200-2 [14]

A.1.3 IT-Systeme im System der MakeABank GmbH

Bezeichnung: C001	**Beschreibung der Gruppe der Zielobjekte:** Windows-Clients
Plattform/Baustein: Clients unter Windows	**Verantwortlich/Administrator:** IT-Betrieb, alle mitarbeitende Personen

Vertraulichkeit: Normal	**Begründung für Vertraulichkeit:** Auf Arbeitsrechnern werden keine sensiblen Informationen gespeichert.
Integrität: Normal	**Begründung für Integrität:** Auf Arbeitsrechnern werden keine sensiblen Informationen gespeichert.
Verfügbarkeit: Normal	**Begründung für Verfügbarkeit:** Ein Ausfall bis zu 4 Stunden kann toleriert werden.

Bezeichnung: S001	**Beschreibung der Gruppe der Zielobjekte:** Virtualisierungsserver
Plattform/Baustein: Server	**Verantwortlich/Administrator:** IT-Betrieb (Konfiguration), Cloud-Anbieter (Infrastruktur)

Vertraulichkeit: Sehr hoch	**Begründung für Vertraulichkeit:** Da sich entweder A001 bis A003 jeweils auf einem Virtualisierungsserver befinden können, wird der höchste Wert für die Vertraulichkeit hier übernommen (Maximumsprinzip) und vererbt sich auf den zugrundeliegenden Server.
Integrität: Sehr hoch	**Begründung für Integrität:** Ein selbes Schema gilt für die Integrität, wie für den Grad der Vertraulichkeit.
Verfügbarkeit: Hoch	**Begründung für Verfügbarkeit:** Ein selbes Schema gilt für die Verfügbarkeit, wie für den Grad der Vertraulichkeit.

Tabelle A.3: Strukturanalyse und Schutzbedarfsfeststellung für IT-Systeme im System der MakeABank GmbH nach BSI-Standard 200-2 [14]

A.2 Risikoanalyse

A.2.1 Risikoeinstufung für Bedrohungen gegen den gesamten Informationsverbund

<table>
<tr><td colspan="3">Gesamter Informationsverbund</td></tr>
<tr><td colspan="2">Gefährdung: B1: Unzureichendes Notfallmanagement für die Cloud</td><td>Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)</td></tr>
<tr><td>Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig</td><td>Auswirkungen ohne zusätzliche Maßnahmen: existenzbedrohend</td><td>Risiko ohne zusätzliche Maßnahmen: sehr hoch</td></tr>
<tr><td colspan="3">Beschreibung: Ein Notfallmanagement, welches existenzbedrohende Risiken frühzeitig erkennen und eine angemessene Behandlung initialisieren soll, wird nicht definiert. Falls ein Notfallmanagement existieren sollte, kann dieses für die neue Cloud-Umgebung ungeeignet sein, da noch veraltete Bausteine für die vorher verwendete On-Premise Infrastruktur enthalten sind. In beiden Fällen kann gegebenenfalls nicht angemessen auf Sicherheitsvorfälle reagiert werden.
Bewertung: Vergleich 4.5.1</td></tr>
</table>

<table>
<tr><td colspan="2">Gefährdung: B2: Fehlende Exit-Strategie</td><td>Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)</td></tr>
<tr><td>Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel</td><td>Auswirkungen ohne zusätzliche Maßnahmen: existenzbedrohend</td><td>Risiko ohne zusätzliche Maßnahmen: hoch</td></tr>
<tr><td colspan="3">Beschreibung: Im Rahmen der Nutzung des Cloud-Computings wurde keine Exit-Strategie definiert. Falls der Einsatz von Cloud-Computing generell oder in Verbindung mit einem Cloud-Provider gescheitert ist, kann es zu desolaten Übergangszuständen kommen, die alle Grundwerte der IT-Sicherheit betreffen können.</td></tr>
</table>

Bewertung: Im Rahmen der fehlenden Exit-Strategie wird angenommen, dass ein grundsätzliches Scheitern eher selten vorkommt, solange ausreichende Ressourcen in die Auswahl eines geeigneten Cloud-Providers investiert wurden. Auch bei der MakeABank GmbH wurde im Vorhinein ein solch hoher Umfang an Ressourcen in die angemessene Auswahl eines größeren und bekannten Cloud-Providers investiert, der ebenfalls von den Kunden akzeptiert wird. So werden viele auslösende Faktoren für einen möglichen Exit wie zum Beispiel eine grundlegende Änderung von Anforderungen minimiert. Jedoch besteht immer noch die realistische Möglichkeit einer grundlegenden Fehlkalkulation, da eine Planung der Kosten im Voraus schwierig ist und keine Referenzdaten aus einem vorherigen Betrieb in der Cloud vorliegen. Ein Eintreten ist also trotzdem möglich, jedoch tendenziell unwahrscheinlicher. Die Eintrittshäufigkeit wird damit als mittel klassifiziert. Die Auswirkungen können jedoch potenziell existenzbedrohend sein, da im Falle einer hohen Fehlkalkulation, die Kosten nicht mehr tragbar sein könnten und daraus im schlimmsten Falle ein existenzielles Risiko für den Rechnungsträger entstehen könnte. Falls sich außerdem Rahmenbedingungen des Cloud-Providers negativ auf den Datenschutz auswirken, können gegebenenfalls sogar juristische beziehungsweise behördliche Konsequenzen drohen, falls kein schneller und vollständiger Wechsel des Cloud-Providers durch eine Exit-Strategie möglich ist. Aus einer mittleren Eintrittshäufigkeit und existenzbedrohenden Auswirkungen ohne weitere Maßnahmen entsteht ein hohes Risiko aus einer fehlenden Exit-Strategie.

Gefährdung: **B3: Fehlende Schulung im Umgang mit Sicherheitsbedrohungen in der Cloud**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

Beschreibung Das Personal wird entweder gar nicht im Rahmen von Schulungen für den Umgang mit Sicherheitsbedrohungen in der Cloud sensibilisiert oder lediglich ein zu kleiner Personenkreis für das jeweilige Szenario. In den Strukturen der MakeABank GmbH werden beispielsweise intern keine regelmäßigen und breitflächigen Schulungen durchgeführt. Dies basiert auf der Annahme, dass hier als IT-Dienstleister sowie ausschließlich Personal mit bereits grundlegenden Fachkenntnissen bezüglich der allgemeinen Informationssicherheit mit der Cloud-Umgebung arbeiten wird. Für besonders Cloud-spezifische Bedrohungen soll trotzdem ein ausgewählter Fachkreis an Personen eine externe Schulung erhalten. Dieser ausgewählte Personenkreis soll das Fachwissen in alternativen Formen des Zusammenarbeitens wie zum Beispiel des Pair-Programmings innerhalb der MakeABank GmbH streuen. Für Kunden bietet die MakeABank GmbH jedoch breite Schulungen an. Damit sollen mitarbeitende Personen der Finanzinstitution, die keine Fachkenntnisse in der IT beziehungsweise Informationssicherheit besitzen, für Bedrohungen sensibilisiert werden. Diese ist jedoch nur eine Empfehlung, nicht verpflichtend und nur wenige Kunden haben sich vorab angemeldet.

Bewertung: Im Zusammenhang mit „MaBCloud“ sind Sicherheitsvorfälle durch eine fehlende Sensibilisierung von Sicherheitsbedrohungen in der Cloud möglicherweise des Häufigeren auf Seite der Kunden zu erwarten. Insbesondere da, wie bereits erwähnt, Finanzinstitution vermutlich in einem besonderen Fokus von angreifenden Institutionen liegen werden. Werden zudem keine umfangreichen Schulungen angenommen, so kann davon ausgegangen werden, dass mindestens Angriffstechniken im Bereich des Social Engineerings häufiger erfolgreich sein können. Standardmäßig verwaltet beziehungsweise wartet die MakeABank GmbH die Cloud-Umgebungen vollständig, weshalb ein Zugriff auf die Infrastruktur durch Kundenmitarbeiter, die keine Schulung für Sicherheitsbedrohungen erhalten, nicht möglich ist. Allerdings bieten bereits kompromittierte Zugangsdaten für die Web-Oberfläche von „MaBCloud“ gegebenenfalls Zugang zu umfangreichen sensible Daten, weshalb die Auswirkungen von fehlenden Schulungen möglicherweise beträchtlich sein können. Daraus ergibt sich ohne zusätzliche Maßnahmen insgesamt ein hohes Risiko.

Gefährdung: **B4: Unzureichende Partition von Entwicklungsumgebungen**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

Beschreibung Die Entwicklungsumgebungen werden nicht in verschiedene Cloud-Umgebung aufgeteilt, sodass eine Isolation dieser innerhalb derselben Cloud-Umgebung durch komplexe Konfigurationskonstrukte innerhalb des Zugriffsmanagements erfolgen muss. Zudem herrschen bezüglich der Authentifizierungsrichtlinien von Benutzerkonten häufig grundlegend unterschiedliche Paradigmen pro Entwicklungsumgebung, sodass Konfigurationsfehler im Zusammenhang mit dem Zugriffsmanagement durch Angreifenden möglicherweise einfach ausgenutzt werden können. Bei der MakeABank GmbH werden die Entwicklungsumgebung dahingegen in verschiedenen Cloud-Umgebungen betrieben. Zudem gibt es bis auf wenige Benutzerkonten, die durch bestimmte Personen in Ausnahmesituationen genutzt werden, keine menschlich geführten Benutzerkonten. Lediglich Benutzer für DevOps Pipelines sind eingerichtet und im Tagesgeschäft aktiv, um eine neue Version automatisiert zu installieren. Diese sind durch sichere Passwörter bestmöglich geschützt.
Bewertung: Die MakeABank GmbH besitzt bereits langfährige Erfahrung mit der agilen Softwareentwicklung, dementsprechend werden Entwicklungsumgebungen genutzt und breite CI/CD Kenntnisse sind vorhanden. Von daher kann davon ausgegangen werden, dass die Idee einer möglichst hohe Partition von Entwicklungsumgebungen durch verschiedene Cloud-Umgebungen intuitiv scheint. Ein ähnliches Ziel wurde vermutlich auf einer On-Premises Infrastruktur ebenfalls bereits verfolgt. Ein Transfer auf das Konzept des Cloud-Computings lässt sich tendenziell als trivial bewerten. Aufgrund fehlender Statistiken wird, basierend auf diesen Annahmen, eine eher seltene Eintrittshäufigkeit klassifiziert. Die Auswirkungen können jedoch unter Umständen beträchtlich sein. Falls schlecht gesicherte Benutzer, die eigentlich nur für die Dev-Umgebung zu Testzwecken vorgesehen waren beispielsweise durch einen Konfigurationsfehler im Zugriffsmanagement auf Ressourcen des produktiven Systems zugreifen können, sind verschiedenste Szenarien möglich. Das Schutzniveau des Systems kann massiv negativ beeinflusst werden. Basieren auf den beiden Parametern, wird das Risiko hier als mittel klassifiziert.

Gefährdung: **B6: Cloud Outages**		Beeinträchtigte Grundwerte: Verfügbarkeit (A)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: Dienste des gewählten Cloud-Anbieters fallen aus, sodass entweder die ganze Cloud-Umgebung oder Teilfunktionalitäten nicht mehr erreichbar sind, sodass das System nicht mehr funktioniert. **Bewertung:** Der Ausfall von Rechenzentren beziehungsweise Verfügbarkeitszonen eines Cloud-Anbieters kommt in regelmäßigen Abständen vor, belegbar durch historische Daten. Diese Abstände sind schwer vorauszusagen, aber ungefähr in den Bereich einer mittleren Eintrittshäufigkeit einzugliedern. Insbesondere Naturkatastrophen sind hierfür ein Auslöser, die zukünftig bedingt durch den Klimawandel tendenziell häufiger auftreten können. Von daher wird die Eintrittshäufigkeit als mittel, mit Tendenz in Richtung häufig klassifiziert. Speziell in einem Sektor der kritischen Infrastruktur, dem Finanzinstitutionen angehören, muss die Verfügbarkeit auf jeden Fall gewährleistet werden. Ein Ausfall könnte mit behördlichen Folgen oder einem Reputationsverlust einhergehen. Ein solches Szenario könnte im schlimmsten Falle existenzbedrohend für die MakeABank GmbH sein.		

Gefährdung: **B7: Inkompatible Monitoring-Lösung**		Beeinträchtigte Grundwerte: Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: Nach dem Umzug von einem On-Premises System in die Cloud wird das Monitoring gegebenenfalls nicht angemessen angepasst. So kann es zur Nutzung einer inkompatiblen Monitoring-Lösung kommen. Insbesondere die Elastizität und breitere geografische Verteilung der unterliegenden Infrastruktur in der Cloud kann so beispielsweise ein angemessenes Monitoring verhindern.		

Bewertung: Da die durch die MakeABank GmbH auf dem On-Premises System verwendete Monitoring-Lösung bereits eine sogenannte Full-Stack IT-Infrastruktur Monitoring Lösung ist, bringt diese eine Unterstützung für das Monitoring in der Cloud mit und muss lediglich umfassend neu konfiguriert werden. Generell ist davon auszugehen, dass seitdem aufstrebenden Trend bezüglich der Nutzung von Cloud Computing viele Monitoring-Lösungen das Monitoring von einer Cloud-Umgebung bereits unterstützen. Konkrete Statistiken diesbezüglich konnten nicht gefunden werden, allerdings wurden im Rahmen dieser Arbeit eine Auswahl von 18 momentan beliebten Monitoring-Lösungen untersucht und dabei keine gefunden, die laut Hersteller nicht Cloud-kompatibel ist. Jedoch ist die Nutzung einer für die Cloud inkompatiblen Monitoring-Lösung nicht ausgeschlossen, weshalb eine seltene Eintrittshäufigkeit klassifiziert wird. Die Auswirkungen einer inkompatiblen Monitoring-Lösung können für die MakeABank GmbH allerdings beträchtlich sein. Es können falsche Warnungen auftreten, obwohl die Workloads in Cloud-Umgebung ordnungsgemäß laufen oder sicherheitskritische Ereignisse beziehungsweise Vorgänge werden gar nicht abgebildet. Auch die Performance des Systems kann gegebenenfalls nicht überwacht und optimiert werden, was sich letztendlich negativ auf die Verfügbarkeit des Systems auswirken kann. Aus diesen beiden Parametern entsteht ein mittleres Risiko ohne zusätzliche Maßnahmen.

Gefährdung: **B8: Vendor lock-in**		Beeinträchtigte Grundwerte: Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **sehr hoch**
Beschreibung: Cloud-Provider stellen mit verschiedenen Maßnahmen eine gezielte Abhängigkeit her, sodass ein Wechsel des Cloud-Providers erschwert werden soll. Dies kann sowohl auf technischer Ebene mithilfe von eigenen Datenformanten, sowie auf organisatorischer Ebene geschehen. **Bewertung:** *Vergleich 4.5.1*		

Gefährdung: **B9: Unzureichendes Datenmanagement**		Beeinträchtigte Grundwerte: Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: Cloud-Provider implementieren kein ausreichendes Datenmanagement. Dies gilt insbesondere hinsichtlich einer angemessenen beziehungsweise vollständigen Vernichtung von gelöschten Daten, sowie einer unzureichenden Offenlegung von der Nutzung dritter Dienste für die Funktionalität der eigenen Dienste. **Bewertung:** Im Prinzip ist vor dieser Bedrohung kein Unternehmen, außer der Cloud-Provider selbst, ausgeschlossen, da nicht auf technischer Ebene verifiziert werden kann, ob Daten wirklich gelöscht werden und welche weiteren dritten Akteure involviert sind. Auch für die MakeABank GmbH trifft dies zu. Allerdings ist das Cloud-Computing inzwischen sehr verbreitet und so häufig genutzt, dass zumindest hinsichtlich großer und bekannter Provider angenommen werden kann, dass ein angemessenes Datenmanagement solide umgesetzt wird. Unter der Annahme, dass ein solcher größerer und bekannter Cloud-Provider von der MakeABank GmbH ausgewählt wird, wird so die Eintrittshäufigkeit als selten eingeschätzt. Dies geschieht unter dem Vorbehalt einer Korrektur, sobald konkrete Fälle eines unzureichenden Datenmanagements bekannt werden. Die Auswirkungen ohne weitere Maßnahmen können hier allerdings beträchtlich für die MakeABank GmbH sein, da so sensible Geschäftsdaten an unberechtigte Dritte gelangen können, möglicherweise ohne dass die MakeABank GmbH oder ein anderer Eigentümer der Daten Information darüber erhält. Das Risiko erhält somit eine mittlere Kategorie.		

Gefährdung: **B10: Ungeeignete Topologie der Systemarchitektur**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Bestimmte Grundprinzipien innerhalb der konfigurierten Topologie für das System werden im Kontext des Cloud Computings nicht angemessen umgesetzt. Dies kann beispielsweise in Bezug auf Netzwerkrouten oder einer Lastverteilung an strategischen Positionen geschehen. Auch die Modellierung eines schützenswerten Geschäftsprozesses mittels zwei unabhängiger Cloud-Dienste und entsprechender Routen kann dazu gehören.		

Bewertung: Die Eintrittshäufigkeit dieser Bedrohung wird als häufig klassifiziert. Grund hierfür sind einerseits das möglicherweise begrenzte Fachwissen der MakeABank GmbH. Andererseits existieren viele Teilaspekte, die im Rahmen einer ungeeigneten Topologie in der Cloud eine Rolle spielen, Ursache dieser Bedrohung sein können und im Rahmen dieser Arbeit auch nicht gänzlich behandelt werden können. Zudem lassen sich viele dieser Ursachen als Cloud-spezifisch kategorisieren und mussten in der Art nicht häufig im Kontext einer On-Premises Infrastruktur berücksichtigt werden. So ist davon auszugehen, dass die Folgen aus der Modellierung einer ungeeigneten Systemarchitektur zumindest anfänglich eher häufig auftreten können. Die Auswirkungen können zudem beträchtlich sein, wenn zum Beispiel durch die nicht überschriebenen Systemrouten die gewünschte Isolation von Subnetzen durchbrochen werden kann und so Angreifende leichter über mehrere Geschäftsprozesse hinweg an sensible Daten gelangen können. Bezüglich der Verfügbarkeit kann sich dies ebenfalls negativ auswirken, wenn zum Beispiel die Last nicht optimal verteilt wird oder lediglich ein Cloud-Dienst integriert wird, sodass ein Prozess im Rahmen eines Ausfalls nicht mehr funktionsfähig ist. Solche Folgen können auch die MakeABank GmbH treffen. So entsteht ohne zusätzliche Maßnahmen ein insgesamt hohes Risiko.

Gefährdung: **B13: Unzureichende Konfiguration von Kontingenten**		Beeinträchtigte Grundwerte: Verfügbarkeit (A)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Kontingente bezüglich der Nutzung von Ressourcen werden nicht angemessen konfiguriert. Im Zuge der ressourcenbasierten Abrechnung kann es so zur überhöhten und vermeidbaren Mehrkosten kommen.		

Bewertung: Die MakeABank GmbH hat bereits ein festes Kontingent festgelegt. Insbesondere gilt dieses für die maximale Anzahl an virtuellen Maschinen pro Schicht von „MaBCloud“. Zudem wurde ein Kontingent bezüglich der maximalen Anzahl an Prozessorkernen pro virtuelle Maschine definiert. Ein Kontingent an Zugriffe auf die API des Cloud-Providers wurde jedoch noch nicht festgelegt, da hier noch keine Referenzwerte bezüglich sinnvoller Grenzwerte gesammelt werden konnten. Da die unzureichende Konfiguration eine häufig thematisierte Bedrohung in der Cloud ist und möglicherweise aufgrund von mangelnden Fachwissen komplexe Konfigurationen bezüglich eines Kontingents für die Zugriffe auf die API eines spezifischen Cloud-Dienstes nicht angemessen durchgeführt werden, wird die Eintrittshäufigkeit als mittel eingestuft. Die Auswirkungen können durch den finanziellen Schaden gegebenenfalls beträchtlich ausfallen. Für die MakeABank GmbH entsteht dadurch ein insgesamt hohes Risiko.

Gefährdung: **B14: Unzureichende Konfiguration von Logging**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: existenzbedrohend	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Logging wird nicht richtig konfiguriert. So werden gegebenenfalls sicherheitsrelevante Ereignisse nicht als Log-Eintrag an eine zentrale Stelle zugeliefert, sodass diese nicht sinnvoll ausgewertet werden können. Davon können sowohl Cloud-Dienste als auch eigene Anwendungen auf virtuellen Maschinen betroffen sein.		

Bewertung: Angenommen wird, dass das Logging mithilfe der Dokumentation des Cloud-Providers angemessen konfiguriert wurde. Insgesamt wird hier durch die MakeABank GmbH ein Logging-Dienst des Cloud-Providers verwendet. Alle Cloud-Dienste sowie virtuelle Maschinen mit eigenen Anwendungen wurden nach dem eigenen Kenntnisstand bestmöglich angeschlossen. Dafür wurde insbesonders darauf geachtet, dass die Logs der eigenen Anwendungen in einem für den Logging-Dienst kompatiblen Format vorliegen. Allerdings wurde auch hier der reale Betrieb noch nicht erprobt, sodass nicht ausgeschlossen werden kann, dass bestimmte Ereignisse noch nicht korrekt zugeliefert werden. Zudem ist die Erweiterung des Systems um neue Dienste oder Anwendungen mittelfristig nicht ausgeschlossen, sodass hier ebenfalls das Potenzial für eine unzureichende Konfiguration von Logging in der Zukunft bestehen kann. Aus diesem Grund wird die Eintrittshäufigkeit auf mittel geschätzt. Auswirkungen können allerdings gegebenenfalls existenzbedrohend sein, da ohne die vollständige Zulieferung von sicherheitsrelevanten Events, sicherheitskritische Vorfälle im schlimmsten Falle unerkannt bleiben könnten. Je nach Angriffsszenario könnten damit die Grundwerte derart verletzt werden, dass dieses existenzbedrohend Auswirkungen zur Folge hat.

Gefährdung: **B15: Unzureichende Konfiguration von Alerting**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: existenzbedrohend	Risiko ohne zusätzliche Maßnahmen: **hoch**

Beschreibung: Alerting wird nicht richtig konfiguriert. So werden sicherheitsrelevante Ereignisse möglicherweise zwar an einer zentralen Stelle geloggt und sichtbar, allerdings wird keine Aktionsgruppe beim Erfassen eines sicherheitskritischen Ereignisses benachrichtigt. Falls also keine ständige manuelle Überwachung der Logs durchgeführt wird, können auch so sicherheitsrelevante Ereignisse untergehen und eine menschliche oder automatisierte Reaktion zeitnah ausbleiben.
Bewertung: Angenommen wird, dass das Alerting mithilfe der Dokumentation des Cloud-Providers angemessen konfiguriert wurde. Dazu wurden mögliche sicherheitsrelevante Ereignisse in verschiedene Prioritätsklassen eingeteilt und ein Konzept herausgearbeitet, welche Aktionsgruppen definiert werden. Wurden bestimmte Ereignisse als besonders risikoreich bewertet, so wird nicht nur eine bestimmte Gruppe an mitarbeitenden Personen informiert, sondern auch ein Dienst, der sofort eine automatisierte Reaktion initiiert.

Gefährdung: **B16: Denial of Service**		Beeinträchtigte Grundwerte: Verfügbarkeit (A)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **sehr hoch**
Beschreibung: Im Rahmen eines Denial of Service Angriff wird die vorhergesehene Nutzung bestimmter Dienstleistung, Funktionen und Geräte verhindert. Die Cloud-Infrastruktur wird gezielt mit bösartigen Anfragen überflutet, mit dem Ziel, dass Cloud-Dienste beziehungsweise die gesamte Cloud-Umgebung nicht mehr funktionsfähig ist. **Bewertung:** *Vergleich 4.5.1*		

Gefährdung: **B18: Unzureichende Separierung von Komponenten**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Die Sicherheit im inneren Netz wird tendenziell vernachlässigt, indem Komponenten nicht ausreichend separiert werden. Separiert bedeutet in diesem Kontext die Konfiguration von einer logischen Topologie, in der Geschäftsprozesse in eigene Subnetze integriert werden und Komponenten nur bei zwingender Notwendigkeit untereinander kommunizierten dürfen. **Bewertung:** Die MakeABank GmbH plant jede Schicht von „MaBCloud“ Cloud in einem eigenen Subnetz zu modellieren. Diese Subnetze erhalten einen bestimmten Dienstendpunkt und es werden Sicherheitsgruppen konfiguriert, die eine Kommunikation innerhalb der Cloud-Umgebung zwischen den Komponenten gezielt einschränken. So kann beispielsweise, wie geplant, nur das Frontend mit dem Backend kommunizieren, aber nicht mit der Datenbank. Auf einer solchen Modellierung liegt zwar ein besonderer Fokus der MakeABank GmbH, jedoch sind auch hier die Konfigurationen möglicherweise derart komplex und Anbieter-spezifischen, dass präventiv eine häufige Eintrittshäufigkeit angenommen wird. Die Auswirkungen solcher Konfigurationsfehler können als beträchtlich angesehen werden, da dies als Katalysator für Schäden durch Angriffstechniken wie einem Lateral Movement Angriff wirken kann, da für Angreifer kaum eine interne Barriere besteht. Aus beiden Parametern ergibt sich ein hohes Risiko.		

Gefährdung: **B19: Unnötiges Öffnen von Cloud-Komponenten für das öffentliche Internet**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: Durch Fehler in der Konfiguration werden Cloud-Komponenten beziehungsweise Ressourcen eine öffentliche Adresse zugewiesen und externe Zugriffe durch die Firewall der Cloud-Umgebung beziehungsweise des Betriebssystems der einzelnen virtuellen Maschine erlaubt.		

Bewertung: Nicht immer sind neu angelegte Komponenten beziehungsweise Ressourcen in der Cloud standardmäßig für externe Zugriffe geschlossen. Dies kann auch bei dem Cloud-Anbieter der MakeABank GmbH nicht ausgeschlossen werden. Allerdings ist der externe Zugriff ein leicht testbares Szenario und mitarbeitende Personen der MakeABank GmbH wurden bereits bezüglich einer besonderen Achtsamkeit gegenüber dieser Bedrohung sensibilisiert. Trotzdem gibt es, wie erarbeitet im Rahmen der Gefährdungsübersicht, historische Beispiele von großen Unternehmen, in denen es trotzdem zu einer solchen Bedrohung gekommen ist. Deshalb wird eine Eintrittshäufigkeit vorsorglich als mittel eingestuft. Falls ein solches Szenario allerdings eintritt, können unbefugte Personen möglicherweise ohne eine Hürde an sensible Geschäftsdaten gelangen. Es wird allerdings angenommen, dass zumindest eine Verschlüsselung von ruhenden Daten umgesetzt wurde, weshalb die Auswirkungen zwar beträchtlich, aber nicht existenzbedrohend wären.

Gefährdung: **B20: Unzureichende Authentifizierungsrichtlinien**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: Lediglich eine schwache Politik bezüglich der Wahl von Benutzerpasswörtern wird konfiguriert. So sind beispielsweise eine Multi-Faktor-Authentifizierung oder starke Passwörter nicht verpflichtend. Ein starkes Passwort kann sich in dem Kontext durch diverse Sonderzeichen oder einer Mindestlänge auszeichnen.		

Bewertung: Unter der Annahme, dass zur Authentifizierung ein sicherer Identitätsanbieter des Cloud-Providers verwendet wird, lässt sich eine Passwortpolitik in der Regel global für alle Nutzer festlegen. Dies erscheint sinnvoll für alle existenten Benutzerkonten, unabhängig von der Entwicklungsumgebung, und kann in Sicherheitsstandards einmalig konfiguriert werden. Die Eintrittshäufigkeit von Konfigurationsfehlern wird hier eher als selten eingeschätzt. Im Kontext von der Multi-Faktor-Authentifizierung ist jedoch eine genauere Konfiguration nützlich. So kann es sinnvoll sein für Administratoren lediglich Hardware-Schlüssel zuzulassen, während für Konten mit keinen verwaltenden Berechtigungen, die lediglich zur Nutzung von „MaBCloud“ dienen, zum Beispiel eine SMS als zweiter Faktor ausreicht. Bestimmte Konten sollten zudem keine Multi-Faktor Authentifikation besitzen, um sicherzustellen, dass, auch wenn der MFA-Dienst oder Identitätsdienst des Cloud-Providers nicht funktioniert, ein Zugriff auf die Cloud-Umgebung weiterhin möglich ist. Durch die mögliche Komplexität werden Konfigurationsfehler als möglich eingeschätzt, mit einer mittleren Eintrittshäufigkeit. Sollten allerdings durch schwache Authentifizierungsrichtlinien Angreifende Zugriff auf ein Konto erhalten, so können bereits bei einfachen Nutzerkonten für „MaBCloud“ schützenswerte Geschäftsdaten eingesehen werden. Die Auswirkungen hier können bereits beträchtlich sein. Ein insgesamt mittleres Risiko liegt vor.

Gefährdung: **B21: Social Engineering**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **sehr hoch**
Beschreibung: Durch soziale Manipulation wird ein unberechtigter Zugang zum System geschaffen. Dabei werden durch teilweise komplex ausgearbeitete Täuschungsstrategien menschliche Werte gezielt ausgenutzt, um beispielsweise Zugangsdaten zu erhalten. **Bewertung:** *Vergleich 4.5.1*		

Gefährdung: **B22: Schlechtes Trustmanagement**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: existenzbedrohend	Risiko ohne zusätzliche Maßnahmen: **sehr hoch**
Beschreibung: Vertrauensflüsse bei der Nutzung einer Cloud-Umgebung werden unzureichend gesteuert. So kann zum Beispiel auf unternehmerischer Ebene dem falschen Cloud-Provider oder dritten Institutionen vertraut werden, sodass im schlimmsten Falle eine unangemessene Wahl des Cloud-Providers stattfindet. Aus technischer Sicht kann im Rahmen eines schlechten Trustmanagements, Cloud-Diensten oder Anwendungen beziehungsweise Bibliotheken Dritter vertrauen werden, die ebenfalls das Schutzniveau des Systems in verschiedenen Aspekten negativ beeinflussen können. **Bewertung:** *Vergleich 4.5.1*		

Gefährdung: **B24: Schlechtes Keymanagement**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: exixtenzbedrohend	Risiko ohne zusätzliche Maßnahmen: hoch
Beschreibung: Ein schlechtes Keymanagement wurde etabliert, in dem zum Beispiel Daten entweder nicht ausreichend früh oder sicher genug verschlüsselt werden. Auch Schlüssel können schneller verloren gehen oder es ist unklar, wie sicher verwendete Schlüssel beziehungsweise Algorithmen überhaupt sind.		

Bewertung: Die MakeABank GmbH setzt grundsätzlich, wenn möglich, auf eine clientseitige Verschlüsselung für Daten der eigenen Anwendungen. Dabei wird auf die Verwendung von sicheren Algorithmen und Schlüsseln geachtet. Jedoch sind dabei Ereignisse wie der Verlust von Schlüsseln oder ähnlichem dabei nicht gänzlich ausgeschlossen, aber lediglich mit einer mitteleren Eintrittshäufigkeit zu erwarten. Außerdem werden Cloud-Dienste verwendet und hier kann das Keymanagement nicht überprüft werden, sodass auch hier ein schlechtes Management seitens des Cloud-Anbieters möglich wäre, aber tendenziell unwahrscheinlich ist durch den drohenden Reputationsverlust. Präventiv wird so eine mittlere Eintrittshäufigkeit klassifiziert. Durch die hohe Sensibilität der Geschäftsdaten von der MakeABank GmbH wäre ein schlechtes Keymanagement allerdings existenzbedrohend. Werden Daten nicht ausreichend verschlüsselt oder Schlüssel gehen verloren, könnte die eine Daten Kompromittierung beziehungsweise einen existenzbedrohenden Datenverlust bedeuten. Daraus entsteht ein hohes Risiko.

Tabelle A.4: Risikobewertung von Gefährdungen gegen den gesamten Informationsverbund nach Vorlage aus dem BSI-Standard-200-3 [18]

A.2.2 Risikoeinstufung für Bedrohungen gegen das MaBCloud Frontend (A001)

MaBCloud Frontend (A001)		
Gefährdung: **B5: Unzureichendes Partition der Anwendung**	Beeinträchtigte Grundwerte: Verfügbarkeit (A)	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: Eine Anwendung wird in die Cloud migriert, ohne die festgelegten technischen Limits eines Cloud-Providers zu berücksichtigen. Wird hier eine Anwendung bei Bedarf nicht ausreichend partitioniert, kann die Funktionalität eingeschränkt werden.		

Bewertung: Eine allgemeingültige Eintrittshäufigkeit zu bestimmen ist in diesem Falle nicht möglich. Ob eine Anwendung die Limitierungen des Cloud-Providers ausreizt, hängt in der Regel nicht nur von der Größe einer Anwendung an sich ab, sondern auch von der Anzahl der Benutzer, die Last auf eine Anwendung ausüben und Ressourcen beanspruchen. Da die Kunden der MakeABank GmbH ein sehr variierendes Benutzerkontingent bedienen müssen, muss hier jeweils individuell über eine entsprechende Partitionierung von „MaB-Cloud“ nachgedacht werden. Allerdings ist das vorliegenden Szenario nicht als Regelfall zu erwarten. Eine mittlere Eintrittshäufigkeit wird geschätzt. Werden Limitierungen erreicht, so kann dies allerdings die Verfügbarkeit der Anwendung negativ beeinflussen. In Anbetracht der Relevanz des vorliegenden Szenarios hätte dies beträchtliche Auswirkungen. Ein hohes Risiko liegt also vor.

Gefährdung: **B:11 Unzureichendes Konfiguration von Replikation**		Beeinträchtigte Grundwerte: Verfügbarkeit (A)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Replikation wird nicht angemessen konfiguriert, beziehungsweise es wird keine synchronisierte Kopie einer Komponente angelegt, die im Rahmen eines Ausfalles derart die Anfragen übernehmen kann, dass dieser nicht wahrgenommen wird. Diese Kopie sollte dabei innerhalb einer anderen Verfügbarkeitszone angelegt werden. **Bewertung:** Die MakeABank GmbH setzt eine Replikationsstrategie bereits nach bestem Wissen um. Jedoch extisieren oftmals verschiedene Replikationstypen und es können teilweise im Rahmen einer Notfallwiederherstellung mit Repliken ganze Workflows konfiguriert werden. Von daher wird hier ebenfalls angenommen, dass im Rahmen einer fehlenden Erfahrung mit der Cloud, auch hier negative Folgen aus Konfigurationsfehlern mit einer eher hohen Eintrittshäufigkeit eintreten können. Da diese Folgen primär die Verfügbarkeit des Systems negativ beeinträchtigen, können die Auswirkungen beträchtlich sein. Es besteht damit ein hohes Risiko.		

Gefährdung: **B12: Unzureichende Backup- und Recoverystrategie**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: existenzbedrohend	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung Eine Backup- und Recoverystrategie wird nicht erstellt beziehungsweise angemessen konfiguriert, sodass keine Datensicherungen existieren, beziehungsweise nach einem sicherheitskritischen Vorfall zur Wiederherstellung eingespielt werden können. **Bewertung:** Durch die MakeABank GmbH wurde die Backup- und Recoverystrategie von dem On-Premises System bezüglich des Intervalls und Umfang der Sicherungen übernommen. Allerdings kann eine angemessene Konfiguration möglicherweise anspruchsvoll sein, da kein direktes Abbild von Daten auf der physischen Ebene durchgeführt werden kann und durchgeführte Datensicherungen oft durch die Cloud-Provider gehalten werden. Durch diese möglicherweise anspruchsvolle und spezifischen Konfigurationen wird die Eintrittshäufigkeit präventiv als mittel eingestuft. Die Auswirkungen können allerdings existenzbedrohend sein. Konfiguriert die MakeABank GmbH beispielsweise keine umfangreiche und regelmäßig Sicherung der Datenbank, so kann ein vollständiger Datenverlust auftreten. Daraus ergibt sich ein insgesamt hohes Risiko.		

Gefährdung: **B17: Betrügerischer Ressourcenverbrauch**		Beeinträchtigte Grundwerte: Verfügbarkeit (A)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig	Auswirkungen ohne zusätzliche Maßnahmen: begrenzt	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Bösartige Zugriffe mit einer niedrigeren Frequenz als im Rahmen eines klassischen Denial of Service Szenarios finden auf das System statt, um Ressourcen zu beanspruchen und somit einen finanziellen Schaden zu verursachen.		

Bewertung: Bösartige Zugriffe im Rahmen eines betrügerischen Ressourcenverbrauchs können nur schwierig klassifiziert beziehungsweise eine dementsprechende Eintrittshäufigkeit definiert werden. Jedoch ist davon auszugehen, dass sich dies in einem ähnlichen Rahmen wie Denial of Service bewegen kann. Die Auswirkungen können durch den finanziellen Schaden im Rahmen der verwendeten nutzungsbasierten Abrechnung potenziell beträchtlich sein. Allerdings wird davon ausgegangen, dass der finanzielle Schaden möglicherweise erstmal nicht so hoch ausfällt, da aus Gründen der Verschleierung die Frequenz an bösartigen Anfragen eher niedrig gehalten wird.

Gefährdung: **B24: ungesicherte Cloud-Anbieter API**	Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)

Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**

Beschreibung: Die Application Programming Interfaces des Providers sind nicht ausreichend gesichert. Dies kann geschehen, indem der Cloud-Provider diese nicht angemessen absichert, durch den Nutzer keine angemessene Authentifizierung implementiert wird, beziehungsweise zu breite Rechte vergeben werden oder Dritte diese API in einer unsicheren Art und Weise nutzen.
Bewertung: Die Eintrittshäufigkeit kann hier als häufig eingeschätzt werden. Dies liegt daran, dass hier verschiedene Ursachen für eine ungesicherte Cloud-Anbieter-API existieren. Damit wird die Wahrscheinlichkeit insgesamt erhöht. Die Auswirkungen können beträchtlich sein, da über die Cloud-API auch umfassende Änderung an der Systemarchitektur beziehungsweise Datensicherungen und weiteren Diensten vorgenommen werden können, allerdings eine Teilabsicherung durch den Cloud-Anbieter stattfindet. Dadurch ergibt sich ein als hoch zu klassifizierendes Risiko.

Gefährdung: **B25: Malware**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Software gerät in die Cloud-Umgebung und führt unerwünschte sowie meist schädliche Funktionen aus. So können beispielsweise Daten erpresserisch verschlüsselt, Ressourcen der Cloud-Umgebung für Denial of Service Angriffe gegen andere Systeme missbraucht oder Daten unbemerkt ausspioniert werden. **Bewertung:** Bereits die Eintrittshäufigkeit kann als häufig klassifiziert werden. Anhalt dazu gibt eine Studie des Cybersecurity-Anbieters Sophos, in welcher 3000 IT-Entscheider von Unternehmen befragt wurden, ob diese im letzten Jahr von Malwaren beziehungsweise insbesondere von Ransomware betroffen waren. Insgesamt erlebten 66 % einen solchen Vorfall innerhalb dieser Zeitspanne [100]. So sind auch im vorliegenden Szenario hier mindestens genauso hohe Zahlen zu erwarten. Die Auswirkungen hingegen können zunächst existenzbedrohend erscheinen, speziell, wenn Daten ausspioniert oder gar unwiederherstellbar durch nicht-erfüllbare Lösegeldforderungen eines Ransomware-Angriffes verloren gehen. Jedoch wird diese Kategorie im vorliegenden Fall vermindert, da viele Cloud-Anbieter verwaltete Dienste anbieten, die dabei unterstützen, die Auswirkungen von Malware im System zu minimieren. Auch die MakeABank GmbH strebt die Nutzung beziehungsweise Integration solcher Dienste in das System an. Von daher werden die Auswirkungen von existenzbedrohend auf beträchtlich herabgestuft. Durch diese beiden Parameter entsteht ein hohes Risiko.		

Tabelle A.5: Risikobewertung von Gefährdungen gegen das MaBCloud Frontend (A001) nach Vorlage aus dem BSI-Standard-200-3 [18]

A.2.3 Risikoeinstufung für Bedrohungen gegen das MaBCloud Backend (A002)

MaBCloud Backend (A002)		
Gefährdung: **B5: Unzureichendes Partition der Anwendung**	Beeinträchtigte Grundwerte: Verfügbarkeit (A)	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B5: Unzureichendes Partition der Anwendung, Beschreibung* **Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B5: Unzureichendes Partition der Anwendung, Bewertung*		

Gefährdung: **B11: Unzureichendes Konfiguration von Replikation**	Beeinträchtigte Grundwerte: Verfügbarkeit (A)	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B11: Unzureichendes Konfiguration von Replikation, Beschreibung* **Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B11: Unzureichendes Konfiguration von Replikation, Bewertung*		

Gefährdung: **B24: ungesicherte Cloud-Anbieter API**	Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B24: ungesicherte Cloud-Anbieter API, Beschreibung* **Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B24: ungesicherte Cloud-Anbieter API, Bewertung*		

Gefährdung: **B25: Malware**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B25: Malware, Beschreibung* **Bewertung: Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B25: Malware, Bewertung*		

Tabelle A.6: Risikobewertung von Gefährdungen gegen das MaBCloud Backend (A002) nach Vorlage aus dem BSI-Standard-200-3 [18]

A.2.4 Risikoeinstufung für Bedrohungen gegen das objektrelationale Datenbanksystem (A003)

Objektrelationales Datenbanksystem (A003)		
Gefährdung: **B5: Unzureichendes Partition der Anwendung**		Beeinträchtigte Grundwerte: Verfügbarkeit (A)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**
Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B5: Unzureichendes Partition der Anwendung, Beschreibung* **Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B5: Unzureichendes Partition der Anwendung, Bewertung*		

Gefährdung: **B11: Unzureichendes Konfiguration von Replikation**		Beeinträchtigte Grundwerte: Verfügbarkeit (A)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B11: Unzureichendes Konfiguration von Replikation, Beschreibung* **Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B11: Unzureichendes Konfiguration von Replikation, Bewertung*		

Gefährdung: **B24: ungesicherte Cloud-Anbieter API**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B24: ungesicherte Cloud-Anbieter API, Beschreibung* **Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B24: ungesicherte Cloud-Anbieter API, Bewertung*		
Gefährdung: **B25: Malware**		Beeinträchtigte Grundwerte: Verfügbarkeit (A), Vertraulichkeit (C), Integrität (I)
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **hoch**
Beschreibung: Beschreibung: *Vergleich A.2.2, MaBCloud Frontend A001, B25: Malware, Beschreibung* **Bewertung: Bewertung:** *Vergleich A.2.2, MaBCloud Frontend A001, B25: Malware, Bewertung*		

Tabelle A.7: Risikobewertung von Gefährdungen gegen die objektrelationale Datenbankanwendung (A003) nach Vorlage aus dem BSI-Standard-200-3 [18]

Glossar

Cloud Audit Eine regelmäßige Prüfung, um den Cloud-Anbieter hinsichtlich verschiedener Parameter wie der Sicherheit oder Performance zu bewerten. Auch eigene Konfigurationsfehler werden in der Regel so aufgedeckt.

Cloud Auditor Eine Institution, die eine unabhängige Bewertungen von Cloud-Diensten eines Providers in Bezug von Leistung und Sicherheit vornehmen kann [101].

Cloud Broker Cloud Broker vermitteln im Rahmen einer beratenden Tätigkeit zwischen Cloud-Anbietern und Auftragsgebern. Cloud Brooker sollen dabei dafür sorgen, dass die Cloud-Umgebung den Anforderungen eines Unternehmens entspricht in Bezug auf Aspekte wie Sicherheit, Performance oder Auswahl des richtigen Servicemodells.

Cloud-nativer Dienst Cloud-native Dienste bieten Entwicklern eine umfassende und standardisierte Plattform für die Erstellung und Verwaltung von Anwendungen. Dabei handelt es sich um Anwendungen, die optimiert sind, um in automatisierten Umgebung mit minimaler Interaktion eines Administrators betrieben werden können [112]. Dadurch können Entwickler operative Aufgaben minimieren und Anwendungen schneller erstellen.

differenzielle Datensicherung Im Rahmen der differenziellen Datensicherung werden nur Daten gesichert, die sich seit der letzten vollständigen Datensicherung verändert haben [113].

DSGVO Abkürzung für Datenschutz-Grundverordnung beziehungsweise eine Verordnung der Europäischen Union, mit deren Richtlinien die Verarbeitung beziehungsweise der Schutz von personenbezogenen Daten EU-weit vereinheitlich werden.

FBI Abkürzung für Federal Bureau of Investigation.

Feature Unterscheidungsmerkmal oder spezielle Funktion einer Software, die durch vorher definierte Anforderungen entstanden ist.

HTTP-Statuscode 404 Ein Fehlercode, der anzeigt, dass der Browser zwar einen bestimmten Server erreichen konnte, jedoch die angeforderte Information nicht auffindbar ist. Eine Seite als angeforderte Information kann beim Empfangen dieser Fehlermeldung dementsprechend nicht angezeigt werden.

Java Runtime Environment Zusammenstellung aus Anwendungen, die eine Ausführung von in Java entwickelten Anwendungen auf einem System ermöglichen.

Know-Your-Customer-Prinzip Eine Prüfung der persönlichen Daten und Geschäftsdaten von Neukunden eines Kreditinstituts zur Prävention von Geldwäsche und Terrorismusfinanzierung [97].

Lift-and-Shift Ein Prozess zur Migration einer exakten Anwendungskopie. Insbesondere geht es dabei um Datenspeicher, Betriebssysteme und andere IT-Umgebungen [45].

On-Premises Bezeichnet ein Lizenz- und Nutzungsmodell für serverbasierte Anwendungen. Ein Kunde kauft oder mietet Software und betreibt diese unter eigener Verantwortung in einem eigenen Rechenzentrum oder auf angemieteten Server eines Fremdrechenzentrums [50].

PEP-Prüfung Eine Prüfung, ob eine Person ein hochrangiges wichtiges öffentliches Amt auf internationaler, nationaler oder unterhalb der nationalen Ebene, aber in Bezug auf die Bedeutung vergleichbares Amt ausübt oder ausgeübt hat. Auch dessen direkte Familienmitglieder gelten als politisch exponiert [108]. Die Prüfung findet in der Regel mittels Listen von verschiedenen Anbietern statt.

Region Mit Regionen beschreibt ein Cloud-Anbieter die echten geografischen Positionen, in denen Ressourcen durch Kunden in Anspruch genommen werden können. Eine Region besteht aus mehreren Verfügbarkeitszonen [53].

Service-Level-Agreement Ein Vertrag, welcher die Rahmenbedingungen zwischen einem Auftraggeber und dem Dienstleister für vereinbarte Dienstleistungen regelt.

SSH-Schlüssel Schlüssel um sich im Rahmen von SSH zu Authentifizierung. SSH ist dabei ein Protokoll, welches eine Remote-Verbindung auf andere Computer oder virtuelle Maschinen ermöglicht.

Verfügbarkeitszone Eine Verfügbarkeitszone stellt ein jeweils physisch getrennter Standort dar. Zu dieser gehört jeweils mindestens ein Rechenzentrum mit einer jeweils unabhängigen Stromversorgung und Netzwerkanbindung, um so großflächige Ausfälle zu minimieren [53].

Virtualisierungscluster Als Virtualisierungscluster wird ein Verbund von zusammengeschlossenen Hardware und Software-basierten Lösungen (auch Nodes beziehungsweise Knoten genannt) definiert, der für die Virtualisierung von bestimmten virtuellen Maschinen zuständig ist. Dieser Verbund zeichnet sich dadurch aus, dass Knoten über einen speziellen Kanal über ihren Gesundheitszustand kommunizieren und dadurch beispielsweise mittels automatischer Skalierung eine ständige Optimierung bezüglich der Verfügbarkeit und Lastverteilung stattfinden kann [26].

VM Eine virtuelle Maschine ist eine Anwendungsumgebung, die als virtuelles Betriebssystem aggiert und auf einem physischen Hardwaresystem erstellt wurde [88].

Workload Als Workload wird eine Anwendung mit den dazugehörigen Eingabewerten bezeichnet [39].

Erklärung zur selbstständigen Bearbeitung

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

Ort	Datum	Unterschrift im Original