Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Michael Bulinski

Analyse von Instant-Messengern in sicherheitsrelevanten Unternehmensbereichen

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Michael Bulinski

Analyse von Instant-Messengern in sicherheitsrelevanten Unternehmensbereichen

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr.-Ing. Hübner
Zweitgutachter: Prof. Dr. Kossakowski

Eingereicht am: 22. Januar 2018

Michael Bulinski

Thema der Arbeit
Analyse von Instant-Messengern in sicherheitsrelevanten Unternehmensbereichen

Stichworte
Authentifizierung, Autorisierung, IT-Sicherheit, Mattermost, Nachrichtensofortversand, Nachrichtenverschlüsselung, Nutzwertanalyse, Protokollierung, Rocket.Chat, Verfügbarkeit, Zulip

Kurzzusammenfassung
Die vorliegende Bachelorarbeit thematisiert Instant-Messenger-Applikationen und inwieweit sie in sicherheitsrelevanten Unternehmensbereichen eingesetzt werden können. Im ersten Teil wird ein fiktives Beispielunternehmen vorgestellt, das eine Liste an Ausschlusskriterien vorgibt. Diese Ausschlusskriterien dienen zur Vorauswahl vor der eigentlichen Nutzwertanalyse. Im zweiten Teil werden sicherheitsrelevante Kriterien ausgearbeitet, anhand derer die Nutzwertanalyse die Sicherheitsstandards der Applikationen bewertet.
Michael Bulinski

Title of the paper
Analysis of Instant Messaging Applications for Usage in Security-related Business Areas

Keywords
Authentification, Authorization, IT-Security, Mattermost, Instant Messaging, Message Encryption, Cost-benefit analysis, Logging, Rocket.Chat, Availability, Zulip

Abstract
This bachelor thesis deals with instant messenger applications and their usefulness in security-related environments. The first section introduces a fictional company that specifies a list of exclusion criteria. These criteria are used for pre-selection before a cost-benefit analysis is used to evaluate the provided applications. In the second section, safety criteria are outlined, which are applied in the cost-benefit analysis to evaluate security standards in instant messaging applications.

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

Im Laufe des letzten Jahrzehnts haben Instant-Messenger einen rasanten Aufstieg erlebt. Spätestens mit der Veröffentlichung der mobilen Applikation Whatsapp im Jahr 2009, ist diese Art der Kommunikation zum Quasistandard geworden[1]. Es ist zu beobachten, dass sehr viele Menschen Instant-Messenger-Applikationen in ihrer Freizeit, zur Kommunikation, verwenden.

Instant-Messenger gab es schon vor der mobilen Verbreitung. Die Software ICQ, veröffentlicht im Jahr 1996, gilt als erster populärer Instant-Messaging-Dienst. Die Teilnehmer im Netzwerk waren durch eine einmalige ID identifizierbar, was in der damaligen Zeit eine neue Idee darstellte. Der Vorteil lag darin, dass Anwender direkt und sofort miteinander kommunizieren konnten. Im Vergleich zum Telefon musste der Gesprächspartner nicht angerufen werden. Eine Nachricht konnte auch hinterlassen werden, falls der Gesprächspartner nicht verfügbar war. Zusätzlich konnten neben Nachrichten auch Bilder oder Dateien versendet werden, was die Verwendung der Applikation für die damalige Zeit multifunktional machte [2].

Der Durchbruch im privaten Bereich ist belegt, doch wie sieht die Verbreitung im Geschäftsbereich aus? Die Unternehmen sind, was die Einführung neuer Technologien betrifft, meistens konservativ eingestellt.(vgl. [KON2015]) Im Gegensatz zum privaten Anwender betrifft die Einführung neuer Software nicht einen Nutzer sondern alle Mitarbeiter des Unternehmens. Sicherheitsrelevante Fragen sind schwieriger zu beantworten, weil sie das ganze Unternehmen betreffen bzw. abdecken müssen. Folgende Fragen sind bei der Evaluierung von Instant-Messenger-Applikation in Unternehmen zu beantworten:

- Sind vertrauliche Unternehmensdaten in einer externen Applikation sicher vor dem Zugriff Unbefugter?

[1] [STA2017] bietet eine Übersicht von Statistiken zur Verbreitung von Instant-Messenger-Applikationen
[2] [ICQ2016] gibt einen interessanten Rückblick auf die letzten 20 Jahre von ICQ

- Bietet die Applikation Möglichkeiten zur Authentifikation und Autorisierung des Anwenders an?
- Wird dem Kunden eine Ausfallsicherheit bzw. Verfügbarkeit der Applikation vom Hersteller garantiert?
- Arbeitet der Hersteller transparent gegenüber seinen Kunden?

Die Beantwortung dieser allgemein gestellten Fragen, ist das Hauptziel dieser Ausarbeitung. Das nachfolgende Kapitel konkretisiert die Zielvorgabe.

1.2 Ziel der Arbeit

Ziel dieser Bachelorarbeit ist das Erstellen und Anwenden eines Entscheidungsmodells zur Evaluierung von Instant-Messenger-Applikationen in sicherheitsrelevanten Unternehmensbereichen.

Im ersten Teil werden für ein fiktives aber realitätsnahes Unternehmen Ausschlusskriterien definiert, die sich aus der firmeninternen IT-Infrastruktur ableiten lassen. Ziel dieser Vorauswahl sind die Lokalisierung und die Ausschließung von ungeeigneten Applikationen vor der Durchführung einer Nutzwertanalyse.

Im zweiten Teil werden sicherheitsrelevante Entscheidungskriterien erarbeitet, anhand derer die Nutzwertanalyse durchgeführt wird. Ziel der Nutzwertanalyse ist die Findung der bestmöglichen Instant-Messenger-Applikation unter Einhaltung der sicherheitsrelevanten Entscheidungskriterien.

1.3 Abgrenzung der Arbeit

Die in Kap. 4.4 durchgeführte Nutzwertanalyse umfasst nur Entscheidungskriterien aus dem Bereich IT-Sicherheit. Nachfolgende Themen werden nicht bewertet, können aber als Ausschlusskriterien in Kap. 3.2 eine Rolle spielen:

- Kosten der Applikation,
- Umfang der Applikation,

- Bereitstellung der Applikation,
- Benutzerfreundlichkeit der Applikation,
- Rechtliche Anforderungen an die Applikation.

Der Fokus dieser Bachelorarbeit liegt im Bereich der sicherheitsrelevanten Entscheidungskriterien, die dafür im gegebenen Rahmen im Detail betrachtet werden können und den Umfang der Nutzwertanalyse darstellen.

1.4 Gliederung der Arbeit

Zu Beginn wird in Kap. 2 benötigtes Grundlagenwissen vermittelt. Den Anfang macht die Nutzwertanalyse, auf deren Vorgehensweise die Bachelorarbeit, im weiteren Verlauf in Kap. 3 und in Kap. 4 aufgebaut ist. Des Weiteren stellt dieses Kapitel die Schutzziele vor, auf denen die in Kap. 3.4 verwendeten sicherheitsrelevanten Entscheidungskriterien anknüpfen.

In Kap. 3 wird das Entscheidungsmodell bzw. die Vorgehensweise dieser Bachelorarbeit ausgearbeitet. Zu Beginn wird die IT-Infrastruktur des fiktiven Unternehmens vorgestellt, auf deren Grundlage in Kap. 3.2 die entscheidenden Ausschlusskriterien definiert werden. Diese stellen die essentiellen Anforderungen dar, die das Produkt aus Sicht des fiktiven Unternehmens erfüllen muss. Das Kap. 3.3 erläutert die für die Nutzwertberechnung in Kap. 4.5 benötigten sicherheitsrelevanten Entscheidungskriterien. Das Kap. 3 schließt mit dem Kap. 3.4, der Gewichtung der Entscheidungskriterien, ab.

Das Kap. 4 beginnt mit der Vorstellung der Vorauswahl von Entscheidungsalternativen in Kap. 4.1. Anschließend werden die gewählten Entscheidungsalternativen in Kap. 4.2 einem Ausschlussverfahren ausgesetzt. Das Ergebnis dieser Vorauswahl stellt die Entscheidungsalternativen für die nachfolgende Nutzwertanalyse dar. Die in Kap. 4.5 durchgeführte Nutzwertberechnung basiert auf den in Kap. 4.4 bewerteten Entscheidungskriterien. Das Kap. 4 wird mit einer Ergebnisbewertung in Kap. 4.6 abgeschlossen.

In Kap. 5 werden die gewonnenen Erkenntnisse dieser Bachelorarbeit zusammengefasst. Auf Basis dieser Erkenntnisse wird anschließend ein Ausblick auf die weiterführende Thematik gegeben.

2 Grundlagen

2.1 Nutzwertanalyse

Die Nutzwertanalyse wurde im deutschsprachigen Raum als erstes von Christof Zangemeister im Jahr 1976 erwähnt. Er definierte sie folgendermaßen:

Definition (Nutzwertanalyse)
„*Die Nutzwertanalyse ist die Analyse einer Menge komplexer Handlungsalternativen mit dem Zweck, die Elemente dieser Menge entsprechend den Präferenzen des Entscheidungsträgers bezüglich eines multidimensionalen Zielsystems zu ordnen. Die Abbildung der Ordnung erfolgt durch die Angabe der Nutzwerte (Gesamtwerte) der Alternativen.*“[ZAN1976, S. 45]

Bei der Nutzwertanalyse handelt es sich um ein Instrument, der Entscheidungsfindung. Die verwendete Fragmentierung hilft dabei, das Gesamtproblem in Teilprobleme zu zerlegen, um somit eine komplexe Entscheidungsfindung zu vereinfachen.(vgl. [KUH2004, S. 1]) Folgende Umstände können nach (vgl. [KUH2004, S. 2-3]) dazu führen, das die Umsetzung einer Nutzwertanalyse ein sinnvolles Unterfangen zur Entscheidungsfindung darstellen kann:

- Eine hohe Anzahl an Bewertungskriterien liegt vor.
- Eine hohe Anzahl an Entscheidungsalternativen liegt vor.
- Die Bewertungskriterien haben eine unterschiedliche Gewichtung.
- Eine eindeutige Reihenfolge der Bewertungskriterien ist nicht möglich.
- Mehrere Mitarbeiter, mit unterschiedlichen Kompetenzen, nehmen am Entscheidungsprozess teil.
- Eine Entscheidung auf Basis von Erfahrungen ist nicht möglich.

Eine umfangreiche Einleitung zur Vorgehensweise der Nutzwertanalyse gibt Jörg Kühnapfel mit seiner Ausarbeitung *Nutzwertanalysen in Marketing und Vertrieb.*[KUH2004] Im weiteren Verlauf wird seine Ausarbeitung als Grundlage genutzt und an entsprechenden Stellen auf diese verwiesen.

2.2 Schutzziele der Informationssicherheit

Mit den Schutzzielen der Informationssicherheit werden allgemeine Anforderungen vorgestellt, die vom einzusetzenden System umgesetzt sein müssen, um einen definierten Sicherheitsstandard gewährleisten zu können. In der folgenden Auflistung wird eine Auswahl an Schutzzielen beschrieben, die bei der Bewertung von Instant-Messenger-Applikationen eine bedeutende Rolle spielen.

1. **Schutzziel Informationsvertraulichkeit**

   Definition (Informationsvertraulichkeit)
   „*Wir sagen, dass das System die Informationsvertraulichkeit (engl. confidentiality) gewährleistet, wenn es keine unautorisierte Informationsgewinnung ermöglicht.*“[ECK2013, S.10]

   Die Informationsvertraulichkeit garantiert im ersten Fall, dass die Nachrichten des Subjektes nur durch autorisierte Subjekte gelesen werden können. Das kann zwischen den Systemen der Subjekte durch eine Nachrichtenverschlüsselung gewährleistet werden. Die Nutzung des SSL/TLS-Protokolls ist eine Möglichkeit die Informationsvertraulichkeit auf dem Übertragungsweg, z.B über das Internet, zu ermöglichen.

   Neben der Vertraulichkeit auf dem Übertragungsweg, sagt die Informationsvertraulichkeit aus, dass z. B. innerhalb einer Applikation oder Infrastruktur, Subjekte nur auf die jeweils für sie autorisierten Informationen zugreifen können. Eine mögliche Umsetzung der Zugriffskontrolle basiert auf der Idee der rollenbasierten Zugriffskontrolle (RBAC).

   Auf Grundlage dieses Schutzzieles, werden in Kap. 3.3.1 und in Kap. 3.3.3 die Nachrichtenverschlüsselung und die Autorisierung des Anwenders als Entscheidungskriterien ausgearbeitet.

2. **Schutzziel Authentizität**

Definition (Authentizität)
„Unter der Authentizität eines Objekts bzw. Subjekts (engl. authenticity) verstehen wir die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist.“[ECK2013, S.8]

Mit einer erfolgreichen Authentifizierung bestätigt das Subjekt, in diesem Fall der Anwender der Applikation, seine Identität unter der er im System gespeichert ist. Im ersten Schritt gibt das Subjekt dem System seine Identität durch seinen Benutzernamen oder seine E-Mail-Adresse bekannt. Im zweiten Schritt bestätigt das Subjekt seine Identität durch eine der drei möglichen Faktoren:

- Das Subjekt hat die Kenntnis einer geheimen Information, z.B. eines Passwortes.
- Das Subjekt ist im Besitz eines einzigartigen Objektes, z.B. eines Schlüssels.
- Es wird ein biometrisches Merkmal des Subjektes, z. B. ein Fingerabdruck, verwendet.

Bei der Verwendung eines der Faktoren wird von einer Ein-Faktor-Authentifizierung gesprochen. Werden ein oder mehrere Faktoren hinzugefügt, handelt es sich um eine Zwei-Faktor- bzw. Multifaktor-Authentifizierung.

Auf Grundlage dieses Schutzzieles, wird in Kap. 3.3.2 die Authentifizierung des Anwenders als Entscheidungskriterium ausgearbeitet.

3. **Schutzziel Verfügbarkeit**

Definition (Verfügbarkeit)
„Wir sagen, dass das System die Verfügbarkeit (engl. availability) gewährleistet, wenn authentifizierte und autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.“[ECK2013, S.12]

Die Verfügbarkeit sagt also in diesem konkreten Fallbeispiel aus, wie das Verhältnis zwischen der Zeit, in der Hersteller der Applikation einen problemlosen Zugriff gewährleistet und der Zeit in der die Applikation nicht verfügbar ist. Dabei wird unterscheiden zwischen der Verfügbarkeit der Applikation, die vom Hersteller selbst betrieben wird

und der Verfügbarkeit der Applikation, die firmenintern beim Kunden betrieben werden kann. Für den ersten Fall ist der Hersteller zuständig, der die Verfügbarkeit in einem Service-Level-Agreement fixiert. Für den zweiten Fall ist der Kunde, in diesem Fallbeispiel das fiktive Unternehmen verantwortlich.

Auf Grundlage dieses Schutzzieles, wird in Kap. 3.3.4 die Verfügbarkeit der Applikation als Entscheidungskriterium ausgearbeitet.

4. **Schutzziel Datenintegrität**

   Definition (Verfügbarkeit)
   „*Wir sagen, dass das System die Datenintegrität (engl. integrity) gewährleistet, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.*“[ECK2013, S.9]

   Bei der Datenintegrität wird zwischen der schwachen und der starken Integrität unterschieden. Von einer schwachen Integrität wird gesprochen, falls Daten manipuliert werden können, dies aber nicht unbemerkt geschieht. Die starke Integrität verhindert zusätzlich die Manipulation, in diesem Fallbeispiel den Nachrichtenaustausch zwischen den Anwendern der Applikation.(vgl.[INT2017])

   Das TLS-Protokoll, das in Kap. 3.3.1 verwendet wird, garantiert eine Datenintegrität der Kommunikationsdaten. Somit ist dieses Schutzziel durch dessen Verwendung gewährleistet.

5. **Hilfsziel Transparenz**

   Im Gegensatz zu den vorherigen Schutzzielen ist die Umsetzung der Transparenz kein primäres Schutzziel eines Unternehmens im eigentlichen Sinne. Das Hilfsziel hat die Aufgabe, Klarheit, Erkennbarkeit und Nachverfolgbarkeit bei der Verwendung des Objektes zu garantieren. Die Instant-Messenger-Applikation und ihr technischer Aufbau sollen demnach durchschaubar und ihre Funktionsweise soll nachvollziehbar sein.(vgl.[BAS2010, S.324])

Dies wird z.B. dadurch erreicht, dass der Quellcode der Applikation unter einer freien Lizenz zur Verfügung steht und somit für jedermann kostenlos zugänglich ist. Des Weiteren hilft eine umfangreiche Dokumentation des Herstellers die Bedingungen der Transparenz bestmöglich zu erfüllen.(vgl.[BAS2010, S.324])

Auf Grundlage dieses Hilfszieles, wird in Kap. 3.3.4 die Verfügbarkeit der Applikation als Entscheidungskriterium ausgearbeitet.

3 Ausarbeitung des Entscheidungsmodells

3.1 Die IT-Infrastruktur des fiktiven Unternehmens

Die fiktive Next-Drive GmbH, mit Sitz in Hamburg, wurde im Jahr 2014 als Startup gegründet und hat laut aktuellem Stand 24 eingestellte Mitarbeiter. Next-Drive stellt seinen Kunden die mobile Applikation Drive zur effektiven Personenbeförderung zur Verfügung. Als Zielsysteme werden sowohl Android als auch iOS-Smartphones bedient.

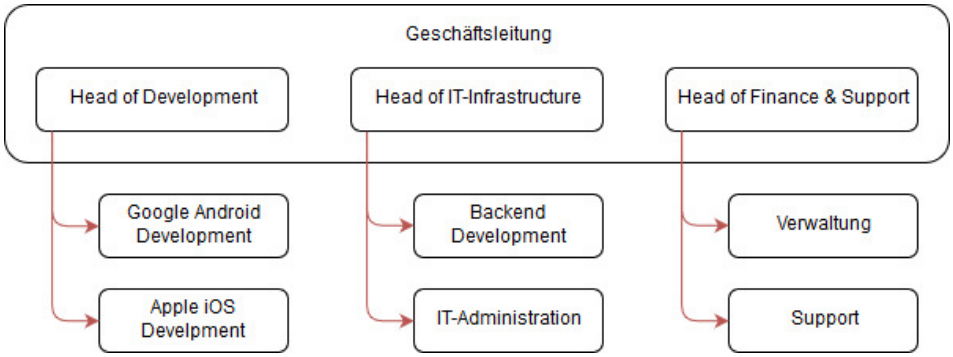

Abbildung 3.1: Abteilungsaufbau des Unternehmens

Wie der Abb. 3.1 zu entnehmen ist, setzt sich das Unternehmen aus sieben Abteilungen zusammen. Dabei hat jeder der drei Geschäftsführer die Verantwortung über jeweils zwei Abteilungen.

- **Head of Development**
  Verantwortet die Frontend-Entwicklung der mobilen Applikation für Google-Android- bzw. Apple-iOS-Smartphones.
- **Head of Infrastructure**
  Verantwortet die Backend-Entwicklung der mobilen Applikation. Des Weiteren liegt die gesamte IT-Infrastruktur des Unternehmens in seiner Verantwortung.

- **Head of Finance & Support**
  Verantwortet die Finanzen des Unternehmens und ist zuständig für die Abteilungen Verwaltung und Support.

Das Unternehmen benötigt für die Arbeit seiner Mitarbeiter verschiedene Betriebssystem-Clients, was die folgende Abb. 3.2 verdeutlichen soll.

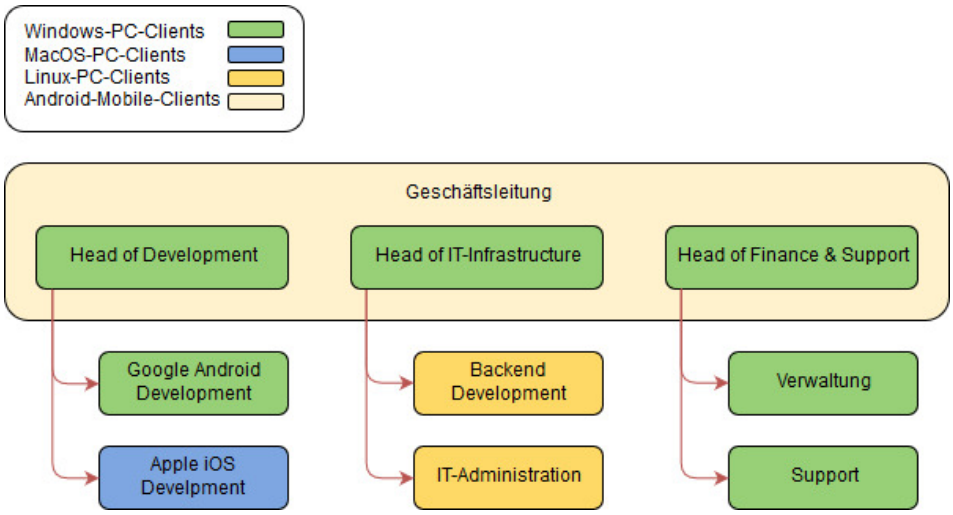

Abbildung 3.2: Verwendete Clients im Unternehmen

- **MacOS-PC-Clients**
  Apple iOS Entwickler sind auf Clients vom Typ MacOS angewiesen.
- **Linux-PC-Clients**
  Für die Verwaltung der Linux-Server in den Bereichen Backend Development und IT-Administration setzen die Mitarbeiter Linux-PC-Clients ein.
- **Windows-PC-Clients**
  In den anderen Abteilungen werden aus Kosten- und Bedienungsgründen Windows-PC-Clients eingesetzt.
- **Android-Mobile-Clients**
  Die Geschäftsführer besitzen Diensttelefone, die auf dem mobilen Betriebssystem Android basieren.

Die Abb. 3.3 des Kap. 3.1 beschreibt die IT-Komponenten, die dezentral im Unternehmen verwendet werden. In der linken Spalte werden interne IT-Komponenten aufgelistet, die am Sitz des Unternehmens betrieben werden und für dessen Verfügbarkeit die Mitarbeiter verantwortlich sind.

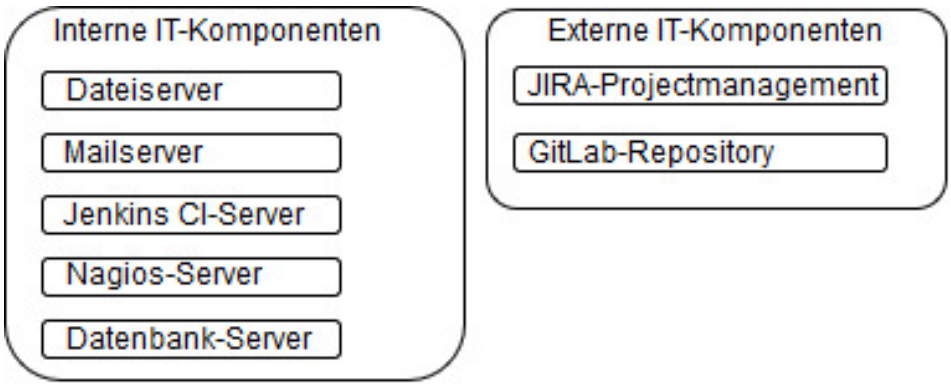

Abbildung 3.3: Verwendung von dezentralen IT-Komponenten

- **Dateiserver**
  Das Unternehmen stellt einen firmeninternen Dateiserver zur Verfügung, auf dem alle unternehmensrelevanten Dateien gespeichert werden können. Alle Mitarbeiter haben bestimmte Zugriffsrechte für das firmeninterne Netzwerk.
- **Mailserver**
  Das Unternehmen stellt seinen Mitarbeitern einen Mailserver zur Verfügung, der firmenintern betrieben wird.
- **Jenkins CI-Server**
  Für die Kontinuierliche Integration der Drive-Applikation, verwenden die Entwickler einen Jenkins CI-Server, der firmenintern betrieben wird.
- **Nagios-Server**
  Der Nagios-Server wird zum Monitoring des firmeninternen Netzwerks und der externen Amazon EC2 Cloud verwendet.

In der rechten Spalte werden externe IT-Komponenten aufgelistet, die bei einem Fremdanbieter genutzt werden und bei denen der Fremdanbieter für die Verfügbarkeit zuständig ist.

- **JIRA-Projektmanagement**
  Mit JIRA setzt das Unternehmen eine Projektmanagement-Applikation ein, mit deren Hilfe die Abteilungen ihre Projekte verwalten können. Alle nicht-technischen Bereiche wie die Fehlerverwaltung oder das Aufgabenmanagement, werden durch diese Applikation abgedeckt.

- **GitLab-Repository**
  Mit GiLab setzt das Unternehmen eine Applikation zur Versionsverwaltung in der App-Entwicklung ein. Dabei wird der, für die Versionsverwaltung, zuständige Server beim Hersteller in der Cloud betrieben.

3.2 Ausarbeitung von Ausschlusskriterien

Die in diesem Kapitel beschriebenen Ausschlusskriterien beschreiben elementare Voraussetzungen des Unternehmens. Sollten diese Eigenschaften nicht erfüllt sein, wird die Instant-Messenger-Applikation von der weiteren Analyse ausgeschlossen. Die Ausschlusskriterien werden weder gewichtet noch fließen sie in die in Kap. 4.5 durchgeführte Nutzwertberechnung mit ein. Im Rahmen eines Team-Meetings haben sich die Verantwortlichen auf folgende Ausschlusskriterien festgelegt:

- **Kostenlose und zeitlich unbegrenzte Nutzung**
  Die Geschäftsführer des Unternehmens haben eine Richtlinie festgelegt, überall auf kostenfreie Programme zu setzen, wo es als sinnvoll erachtet wird. Dementsprechend wird der Fokus auf Instant-Messenger-Applikationen gelegt, die eine kostenfreie aber voll funktionsfähige Grundversion anbieten. Die mögliche Umwandlung der Applikation in eine erweiterte kostenpflichtige Version stellt für das Unternehmen ein erstrebenswertes Merkmal dar, hat aber keinen Einfluss auf die Bewertung als K.o.-Kriterium. Des Weiteren wurde von Voraus beschlossen, auf zeitbeschränkte Probeversionen zu verzichten.

- **Unabhängigkeit der Applikation**
  Mit der Unabhängigkeit wird ein gewünschter Aspekt der Applikation beschrieben, der besagt, dass die Instant-Messenger-Applikation als eigenständiges Programm die gewünschte Funktionalität bereitstellt. Die Applikation soll weder Teil einer Software-Suite sein, noch auf andere Applikationen angewiesen sein um eine Grundfunktionalität gewährleisten zu können.

- **Plattformunabhängigkeit**
  Wie der Abb. 3.2 zu entnehmen ist, setzt das Unternehmen verschiedene Betriebssysteme in den jeweiligen Abteilungen ein. Dementsprechend bekommt die Instant-Messenger-Applikation die Vorgabe, alle verwendeten Systeme nativ zu unterstützen. Sollte eine native Umsetzung nicht möglich sein, soll die Applikation über einen Webbrowser als Webclient bereitgestellt werden.

- **Externe API-Anbindung**
  Eine externe API-Anbindung ermöglicht den Anwendern über die Messaging-Applikation mit anderen Applikationen zu kommunizieren. Für die Applikationen in Abb. 3.3 sollen folgende Erweiterungen in Betracht gezogen werden:

  - **Nagios-Erweiterung**
    Eine Nagios-Erweiterung versendet netzwerkrelevante Informationen direkt an die Instant-Messenger-Applikation und kann somit von jedem berechtigten IT-Administrator gelesen werden.

  - **Jenkins-Erweiterung**
    Eine Jenkins-Erweiterung versendet Statusberichte über erfolgreiche oder fehlgeschlagene Deployments auf dem Jenkins-CI-Server.

  - **GitLab-Erweiterung**
    Eine GitLab-Erweiterung versendet Informationen über Veränderungen im GitLab-Repository.

  - **JIRA-Erweiterung**
    Eine JIRA-Erweiterung kann die jeweiligen Gruppen über Veränderungen im Projektmanagement unterrichten.

  Die Realisierung einer nicht existierenden Erweiterung, soll mit Hilfe eines offenen API möglich sein.

- **Ende-zu-Ende Verschlüsselung**
  Der Abb. 3.2 ist zu entnehmen, dass die Geschäftsführer Smartphones vom Typ Android als Geschäftstelefon verwenden. Durch die Nutzung setzen sie voraus auch außerhalb des firmeninternen Netzwerkes, mit der bestmöglichsten Sicherheit, die Instant-Messaging-Applikation des Unternehmens verwenden zu können. Eine Ende-zu-Ende-Verschlüsselung wird nur dann als Pflicht und somit als ein K.o.-Kriterium angesehen,

wenn der Anbieter der Instant-Messenger-Applikation nur ein anbieterinternes Serverhosting bereitstellt.

- **Gruppenchat-Funktion**
  Die Gruppenchat-Funktion stellt eine elementare Eigenschaft der Instant-Messenger-Applikation dar. Wie der Abb. 3.1 zu entnehmen ist, setzt sich das Unternehmen aus sieben heterogenen Abteilungen zusammen. Somit benötigt das Unternehmen sieben Gruppenchats, die den jeweiligen Abteilungen zur Verfügung stehen. Ein zusätzlicher Gruppenchat wird benötigt, der allen Mitarbeitern als allgemeiner Chat zur Verfügung steht.

3.3 Ausarbeitung von sicherheitsrelevanten Entscheidungskriterien

Im Gegensatz zu den, im vorherigen Kapitel, erwähnten Ausschlusskriterien, sind bei sicherheitsrelevanten Entscheidungskriterien genauere Bewertungsabstufungen notwendig. Hierfür dient die Tab. 3.1 als allgemeine Bewertungsskala, mit deren Hilfe die Ergebnisse nach einem einfachen Punktesystem bewertet werden können.

Punkte	Beurteilung
4	Das Kriterium ist sehr gut erfüllt.
3	Das Kriterium ist gut erfüllt.
2	Das Kriterium ist in befriedigendem Maße erfüllt.
1	Das Kriterium ist ausreichend erfüllt.
0	Das Kriterium ist nicht erfüllt.

Tabelle 3.1: Allgemeine Bewertungsskala

3.3.1 Nachrichtenverschlüsselung

Dieses Entscheidungskriterium basiert auf dem im Kap. 2.2 vorgestellten Schutzziel der Vertraulichkeit. In diesem Anwendungsfall betrifft das den Nachrichtenaustausch zwischen dem Messenger-Client des Anwenders und dem Server, der die jeweilige Nachricht an einen Empfänger oder eine Gruppe von Empfängern schickt. Diese Nachricht soll sowohl innerhalb des

Unternehmens als auch beim externen Zugriff von außen nur durch autorisierte Subjekte gelesen werden können. Zu diesem Zweck beschäftigt sich dieses Kriterium mit der Umsetzung einer Client-zu-Server Verschlüsselung auf Grundlage des SSL/TLS-Protokolls.

- **0 Punkte - Bewertungsrichtlinien**
  Eine Applikation, die keine Client-zu-Server-Verschlüsselung umsetzt, bietet keinen Schutz vor dem unautorisierten Lesen des Nachrichtenaustausches. Innerhalb des Unternehmens könnten beliebige Mitarbeiter die gesamte Kommunikation der anderen Kollegen mitschneiden und lesen. Des Weiteren könnten Angreifer auf die gesamte Kommunikation zugreifen, sobald sie Zugang zum Firmennetz erlangt haben. Ist das Internet der unverschlüsselte Übertragungskanal haben Angreifer keinerlei Hürde die Übertragung mitzulesen.

- **1 Punkt - Bewertungsrichtlinien**
  Beim Nachrichtenaustausch zwischen den Clients und dem Server kommt das SSL/TLS-Protokoll zum Einsatz. Bei der Verwendung dieses Protokolls sind sicherheitsrelevante Vorkehrungen zu treffen. Nachfolgend werden unsichere SSL/TLS-Versionen vorgestellt.

  – **SSL 2.0 und SSL 3.0**
    SSL 3.0 gilt als Erweiterung von SSL 2.0 und wurde 2014 durch die POODLE-Attacke (vgl.[POO2014]) gebrochen. SSL 3.0 und dessen Vorgänger gelten somit als unsicher und sollten nicht mehr verwendet werden.

  – **TLS 1.0**
    TLS 1.0 gilt seit 2011, durch den BEAST-Angriff (vgl.[SAS2013, S. 2]), als gebrochen. Somit sollte diese Version in sicherheitsrelevanten Applikationen nicht mehr eingesetzt werden.

  TLS 1.1 und TLS 1.2 bieten neben sicheren Algorithmen auch unsichere Verfahren an, deren Verwendung möglichst vermieden werden sollte.

  – **Message-Digest-Algorithm 5 (MD5)**
    Das BSI stuft mit (vgl.[BSIES2017, S.19]) die Nutzung von MD5 als Hashfunktion, als unsicher ein. Die Nutzung in TLS 1.1 und TLS 1.2 ist möglich, sollte aber vermieden werden und durch eine aktuellere Hashfunktion wie SHA256 ersetzt werden.

  – **Ron's Code 4 (RC4)**
    Die IETF (Internet Engineering Task Force) untersagte mit dem [RFC7465] im Jahr 2015 die Nutzung der RC4-Stromverschlüsselung in TLS-Protokollen.

  - **Secure Hash Algorithm 1 (SHA-1)**
    Genau wie bei MD5 wird die Nutzung von SHA-1 als Hashfunktion durch das BSI als unsicher eingestuft. (vgl.[BSIES2017, S.19]) Die Möglichkeit der Nutzung ist bei TLS 1.1 und TLS 1.2 gegeben, sollte aber z.B. durch SHA256 ersetzt werden.

  Von der Verwendung eines unsicheren Verfahrens in Geschäftsbereichen wird abgeraten, dies stellt aber eine bessere Nachrichtenverschlüsselung dar, als wenn gar keine Verschlüsselung verwendet wird.

- **2 bis 4 Punkte - Bewertungsrichtlinien**
  Die TLS-Versionen 1.1 und 1.2 bieten eine Vielzahl an Cipher-Suite-Kombinationen an. Zur Veranschaulichung des Aufbaus wird exemplarisch eine mögliche Cipher-Suite und deren Zusammensetzung betrachtet.

  TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384

  - **TLS**
    Die Cipher-Suite steht dem TLS-Protokoll zur Verfügung.
  - **ECDH**
    Für den Schlüsselaustausch wird das asymmetrische Elliptic-Curve-Diffie-Hellman-Verfahren verwendet.
  - **RSA**
    Für die Authentifizierung wird das asymmetrische RSA-Verfahren verwendet.
  - **AES_256**
    Für die Verschlüsselung der Nachricht wird das symmetrische AES-Verfahren mit 256 Bit verwendet.
  - **GCM**
    Als Betriebsart der AES-Verschlüsselung wird der Galois/Counter-Modus verwendet.
  - **SHA384**
    Als kryptographische Hashfunktion wird der Secure-Hash-Algorithm mit 384 Bit verwendet.

Beim Aufbau der Cipher-Suites wird zwischen drei möglichen Verfahren unterschieden:

- symmetrischer Schlüsselaustausch,
- asymmetrischer Schlüsselaustausch ohne Perfect Forward Secrecy,
- asymmetrischer Schlüsselaustausch mit Perfect Forward Secrecy.

Beim ersten Verfahren, das auch als Pre-Shared Key bekannt ist, müssen beide Teilnehmer dafür sorgen, dass vor der eigentlichen Kommunikation der Schlüssel für die Verschlüsselung ausgetauscht und somit beiden Teilnehmern bekannt ist. Dieses symmetrische Verfahren stellt sich als Nachteil dar, weil der Schlüssel im Geheimen über einen möglicherweise unsicheren Kanal ausgetauscht werden muss. Des Weiteren wird sowohl für die Verschlüsselung als auch für die Entschlüsselung derselbe geheime Schlüssel benötigt.

Das BSI stellt mit Abb. 3.4 (vgl.[BSIKV2017, S.9]) eine Auswahl an Cipher-Suites vor, die das symmetrische Verfahren verwenden und für einen längeren Zeitraum als sicher bewertet werden.

	Schlüsseleinigung und -authentisierung		*Verschlüsselung*	*Betriebs-modus*	*Hash*	*Verwendung bis*
TLS_	ECDHE_PSK_	WITH_	AES_128_	CBC_	SHA256	2023+
			AES_256_		SHA384	2023+
	DHE_PSK_	WITH_	AES_128_	CBC_	SHA256	2023+
				GCM_		2023+
			AES_256_	CBC_	SHA384	2023+
				GCM_		2023+
	RSA_PSK_	WITH_	AES_128_	CBC_	SHA256	2023+
				GCM_		2023+
			AES_256_	CBC_	SHA384	2023+
				GCM_		2023+

Abbildung 3.4: Empfohlene Cipher-Suiten mit sym. Schlüsselaustausch

Eine bessere Möglichkeit die Sicherheit des Schlüsselaustausches zu gewährleisten, bietet die Nutzung von asymmetrischen Verfahren. Bei diesem Verfahren, das auch als Public-Key-Verfahren bekannt ist, müssen sich beide Teilnehmer vor der Kommunikation nicht auf einen geheimen Schlüssel zur Verschlüsselung einigen, sondern erzeugen jeweils ein

Schlüsselpaar, bestehend aus einem privaten Schlüssel und einem öffentlichen Schlüssel. Der Versender benötigt den öffentlichen Schlüssel des Empfängers um die Nachricht zu verschlüsseln. Die Nachricht kann dann nur noch durch den privaten Schlüssel des Empfängers entschlüsselt werden. Klaus Schmeh gibt in seinem Buch *Kryptografie: Verfahren, Protokolle, Infrastrukturen* einen genauen Einblick in das asymmetrische Verfahren des Schlüsselaustausches.[KRY2016, S. 189, S. 561]

Das BSI stellt mit Abb. 3.5 (vgl.[BSIKV2017, S.8]) eine Auswahl an Cipher-Suites vor, die das asymmetrische Verfahren verwenden und für einen längeren Zeitraum als sicher bewertet werden.

	Schlüsseleinigung und -authentisierung		***Verschlüsselung***	***Betriebs-modus***	***Hash***	***Verwendung bis***
TLS_	ECDH_ECDSA_	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_ GCM_	SHA384	2023+
	ECDH_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_ GCM_	SHA384	2023+
	DH_DSS_	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_	SHA256	2023+
				GCM_	SHA384	2023+
	DH_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_	SHA256	2023+
				GCM_	SHA384	2023+

Abbildung 3.5: Empfohlene Ciper-Suiten mit asym. Schlüsselaustausch

Durch die Nutzung von Perfect Forward Secrecy (PFS) kann die Sicherheit von asymmetrischen Verfahren verbessert werden. Mit PFS ist es nicht möglich aus dem geheimen Langzeitschlüssel auf vorherige verwendete und abgelaufene Sitzungsschlüssel zu schließen oder diese zu einem späteren Zeitpunkt auszulesen.(vgl.[PFS2014])

Das BSI stellt mit Abb. 3.6 (vgl. [BSIKV2017, S.7]) eine Auswahl an Cipher-Suites vor, die das asymmetrische Verfahren verwenden, Perfect Forward Secrecy umsetzen und für einen längeren Zeitraum als sicher bewertet werden.

	Schlüsseleinigung und -authentisierung		*Verschlüsselung*	*Betriebs-modus*	*Hash*	*Verwendung bis*
TLS_	ECDHE_ECDSA_	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_ GCM_	SHA384	2023+
	ECDHE_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_ GCM_	SHA384	2023+
	DHE_DSS_[1]	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_	SHA256	2023+
				GCM_	SHA384	2023+
	DHE_RSA_[1]	WITH_	AES_128_	CBC_ GCM_	SHA256	2023+
			AES_256_	CBC_	SHA256	2023+
				GCM_	SHA384	2023+

Abbildung 3.6: Empfohlene PFS-Ciper-Suiten mit asym. Schlüsselaustausch

Punkte	**Beurteilung**
4	Verwendung einer Cipher-Suite aus der Abb. 3.6
3	Verwendung einer Cipher-Suite aus der Abb. 3.5
2	Verwendung einer Cipher-Suite aus der Abb. 3.4
1	Die Nutzung eines als unsicher geltenden Verfahrens
0	Der Nachrichtenaustausch findet unverschlüsselt statt Die Art der Verschlüsselung ist unbekannt oder nicht einsehbar

Tabelle 3.2: Bewertungsskala: Nachrichtenverschlüsselung

3.3.2 Authentifizierung des Anwenders

Dieses Entscheidungskriterium basiert auf dem im Kap. 2.2 vorgestellten Schutzziel der Authentizität. Bei der Authentifizierung des Anwenders wird unterschieden zwischen den Anwendern im firmeninternen Netzwerk und den mobilen Anwendern außerhalb des Netzwerkes. Zu diesem Zweck wird dieses Kriterium in zwei Bewertungsskalen aufgeteilt.

- **0 Punkte - Bewertungsrichtlinien**
  Eine Applikation, die keine Authentifizierung vorsieht, kann von jedem Anwender genutzt werden, sobald er die Adresse des Servers kennt. Dabei spielt es keine Rolle, ob der Anwender ein Mitarbeiter des Unternehmens ist oder ein Angreifer, der dem Unternehmen schaden möchte. Die Applikation kann ohne eine Authentifizierung die Anwender nicht unterscheiden und bietet somit keinen Schutz vor unautorisiertem Zugriff auf die Instant-Messenger-Applikation.

- **1 Punkt - Bewertungsrichtlinien**
  Mit der Ein-Faktor-Authentifizierung ist in der Regel die Authentifizierung des Anwenders mit Hilfe seines Benutzernamens bzw. seiner E-Mailadresse und seines Passworts gemeint. Sie stellt die am weitesten verbreitete Form der Authentifizierung dar und wird als Ein-Faktor-Authentifizierung bezeichnet.

Abbildung 3.7: Beispiel für eine Ein-Faktor-Authentifizierung

- **2 Punkte - Bewertungsrichtlinien**
  Eine Authentifizierung bestehend aus Benutzername, Passwort und Versand des Tokens über die SMS stellt eine weit verbreitete, aber die unsicherste Art der Zwei-Faktor-Authentifizierung dar. Das National Institute of Standards and Technology (NIST) rät von der Authentifizierung mit Hilfe externer SMS-Provider ab.(vgl. [FMA2017]) Sie wird zwar als unsicher und veraltet betrachtet, bietet aber trotzdem einen höheren Schutz als die Ein-Faktor-Authentifizierung.

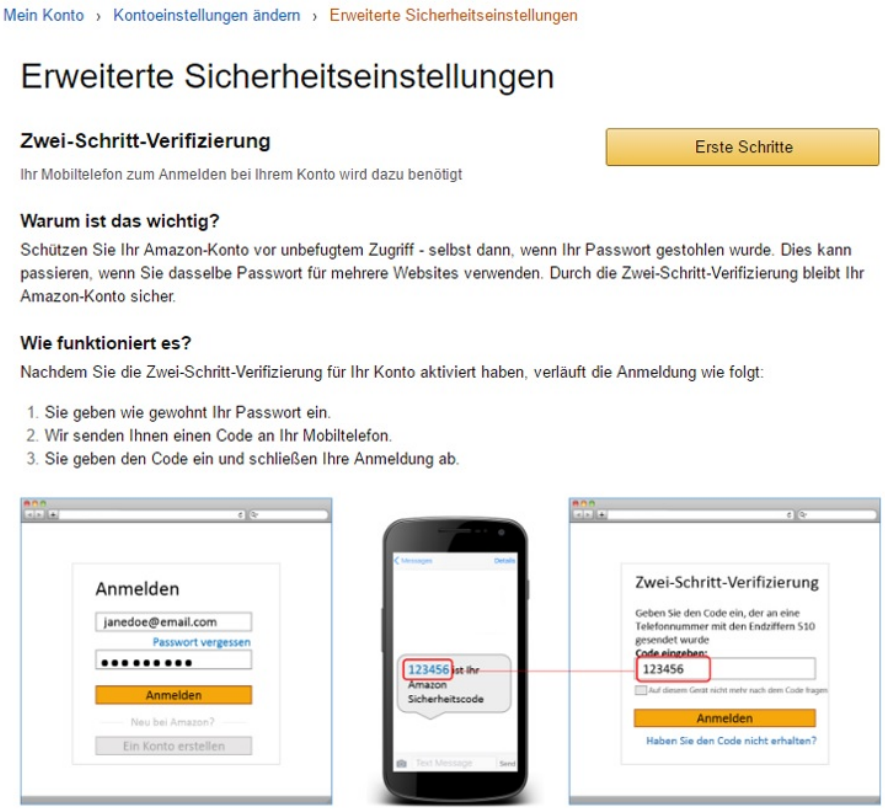

Abbildung 3.8: Beispiel für eine SMS-Zwei-Faktor-Authentifizierung

- **3 bis 4 Punkte - Bewertungsrichtlinien**
  Bei der Bewertung mit drei bzw. vier Punkten wird unterschieden zwischen dem internen Anwender innerhalb des Unternehmensnetzwerkes und dem externen Anwender, der über das offene Internet Zugriff auf die Instant-Messenger-Applikation benötigt.

Die Beispielanwendung in Abb. 3.9 zeigt eine mögliche Umsetzung der Zwei-Faktor-Authentifizierung mit Hilfe der persönlichen E-Mail-Adresse. Diese Art der Anmeldung stellt für die Verwendung innerhalb des Unternehmens die sicherste Methode dar. Sie hat den Vorteil, dass der komplette Prozess innerhalb des Unternehmensnetzwerkes durchgeführt wird und somit keine weiteren externen Dienstleister benötigt werden.

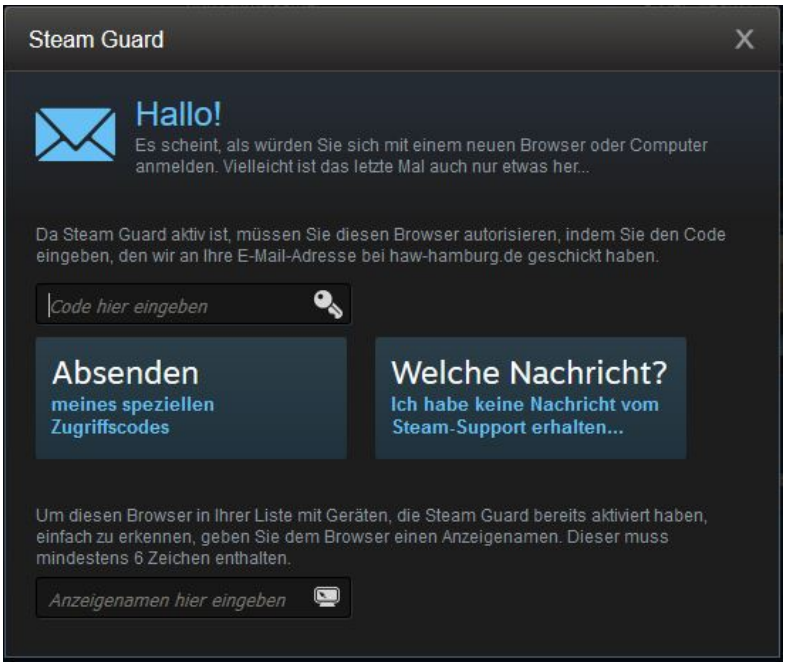

Abbildung 3.9: Beispiel für eine Mail-Zwei-Faktor-Authentifizierung

Die in Abb. 3.10 vorgestellte Zwei-Faktor-Authentifizierung mit Hilfe eines Software-Tokens ist sinnvoll für Mitarbeiter, die von außerhalb, z. B. von ihren Smartphones, auf den Messenger zugreifen wollen. Sie ist die beste Möglichkeit für die externe Verwendung, weil sie im Gegensatz zur E-Mail keinen zusätzlichen Übertragungskanal benötigt. Zum generieren des Tokens, wird eine mobile Applikation auf dem Smartphone der Geschäftsleitung verwendet.

Somit wird im internen Bereich die Authentifizierung per mobiler Authentikator-Applikation mit drei Punkten und die Authentifizierung per E-Mail-Adresse mit vier Punkten bewertet.

Bei der Bewertung der externen Authentifizierung, wird die Bewertungsreihenfolge bei den zwei höchsten Punktevergaben getauscht.

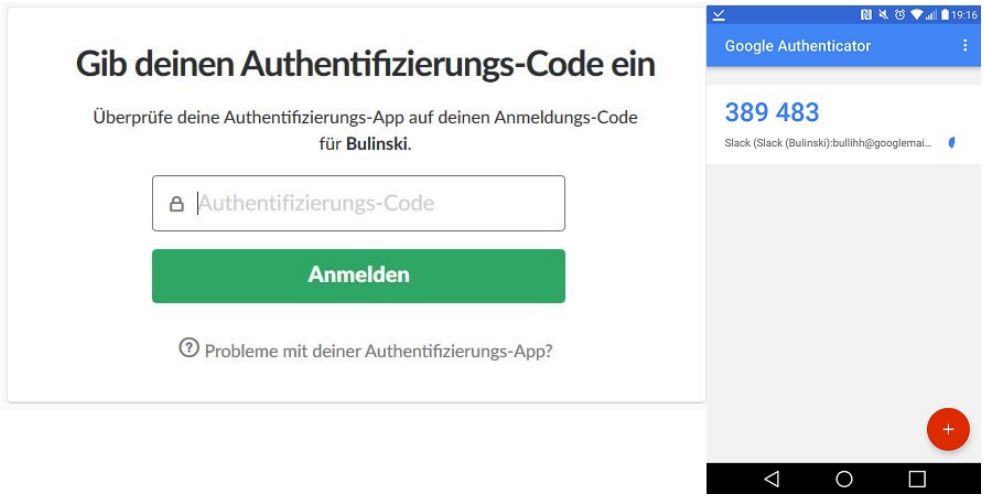

Abbildung 3.10: Beispiel für eine Token-Zwei-Faktor-Authentifizierung

Punkte	Beurteilung
4	Zwei-Faktor-Authentifizierung bestehend aus E-Mail-Adresse, Passwort und Token per E-Mail-Versand
3	Zwei-Faktor-Authentifizierung bestehend aus E-Mail-Adresse, Passwort und Token per Authentifizierungs-Applikation
2	Zwei-Faktor-Authentifizierung bestehend aus E-Mail-Adresse, Passwort und Token per SMS-Versand
1	Ein-Faktor-Authentifizierung bestehend aus E-Mail-Adresse und Passwort
0	Keine Authentifizierung vorhanden

Tabelle 3.3: Bewertungsskala: Interne Authentifizierung

Punkte	Beurteilung
4	Zwei-Faktor-Authentifizierung bestehend aus E-Mail-Adresse, Passwort und Token per Authentifizierungs-Applikation
	Weiter auf der nächsten Seite

Tabelle 3.4 – Fortsetzung von vorheriger Seite

Punkte	Beurteilung
3	Zwei-Faktor-Authentifizierung bestehend aus E-Mail-Adresse, Passwort und Token per E-Mail-Versand
2	Zwei-Faktor-Authentifizierung bestehend aus E-Mail-Adresse, Passwort und Token per SMS-Versand
1	Ein-Faktor-Authentifizierung bestehend aus E-Mail-Adresse und Passwort
0	Keine Authentifizierung vorhanden

Tabelle 3.4: Bewertungsskala: Externe Authentifizierung

3.3.3 Autorisierung des Anwenders

Dieses Entscheidungskriterium basiert auf dem im Kap. 2.2 vorgestellten Schutzziel der Vertraulichkeit. Die Autorisierung legt fest, in welcher Art und Weise dem Anwender Rechte gewährt werden.

- **0 Punkte - Bewertungsrichtlinien**
  Der Worst Case im Bereich Autorisierung, ist eine Instant-Messenger-Applikation ohne Rechtevergabe. Die nachfolgende Aufzählung schildert Problemfälle, die ohne eine Autorisierung des Anwenders entstehen.
  - Jeder Mitarbeiter, vom Geschäftsführer bis zum Studenten, hätte kompletten Zugriff auf die Applikation und somit auch auf die Konfiguration.
  - Die Erstellung von privaten Gruppenchats wäre unmöglich, da jeder Anwender administrative Rechte besitzt.
  - Angreifer könnten jeden beliebigen Zugang nutzen, um maximalen Schaden anzurichten.
  - Frustrierte Mitarbeiter könnten vor ihrem letzten Arbeitstag noch Schaden verursachen.

  Es ist unwahrscheinlich, dass eine Applikation, die für den Geschäftsbereich konzipiert wurde, keine Rechtevergabe vorsieht.

- **1 Punkt - Bewertungsrichtlinien**
  Die Standardlösung ist die Verwendung eines Administratorenkontos, über das die Applikation verwaltet wird und Nutzerrechte erteilt werden können.
  - Nur das Administratorenkonto kann Benutzer- und Gruppen anlegen bzw. löschen.
  - Nur das Administratorenkonto kann Benutzer- und Gruppenrechte vergeben bzw. annehmen.

- **2 bis 4 Punkte - Bewertungsrichtlinien**
  Bei der Vergabe von Rechten stehen dem Administrator drei Möglichkeiten zur Verfügung, die in dieser Ausarbeitung unterschiedlich bewertet werden.
  - **2 Punkte - einzelne Rechtevergabe**
    Hierbei muss jedem Anwender der Applikation jedes Recht einzelnd erteilt werden. Das kann bei größeren System mit vielen Anwendern viel Zeit und Arbeit kosten.
  - **3 Punkte - Rechtevergabe mit Hilfe von Gruppen**
    Hierbei werden die Anwender in Benutzergruppen eingeteilt, denen die Rechte zugewiesen werden. Dies hat den Vorteil, dass nur den Gruppen die Rechte zugewiesen werden müssen, was Zeit und Arbeit spart. Der Anwender kann aber weiterhin individuelle Einzelrechte anfordern.
  - **4 Punkte - Rechtevergabe mit Hilfe von Rollen**
    Der Unterschied zwischen Rollen und Benutzergruppen liegt darin, dass der Anwender nur die Rechte einer Rolle erhält, deren Funktion er im Unternehmen einnimmt. Ein Student erhält dann z.B nur die Rechte, die der Rolle Student zugewiesen sind und ein Geschäftsführer die Rechte der Rolle Geschäftsführer. Die Vergabe von einzelnen Rechten ist anders als bei den Benutzergruppen nicht möglich.

Punkte	Beurteilung
4	Die zentrale Benutzerverwaltung unterstützt die rollenbasierte Rechtevergabe.
3	Die zentrale Benutzerverwaltung verwaltet die Anwender mit Hilfe von Benutzergruppen.
2	Die zentrale Benutzerverwaltung muss jedem einzelnen Anwender dessen Rechte zuweisen.
	Weiter auf der nächsten Seite

Tabelle 3.5 – Fortsetzung von vorheriger Seite

Punkte	Beurteilung
1	Verwendung einer zentralen Benutzerverwaltung durch einen Administrator.
0	Der Messenger unterstützt keine Rechtevergabe. Jeder Benutzer hat die selben Rechte und kann auf jede Funktionalität der Applikation zugreifen oder sie sogar verändern.

Tabelle 3.5: Bewertungsskala: Autorisierung des Anwenders

3.3.4 Verfügbarkeit der Applikation

Dieses Entscheidungskriterium basiert auf dem in Kap. 2.2 vorgestellten Schutzziel der Verfügbarkeit und dem Hilfsziel der Transparenz.

- **0 Punkte - Bewertungsrichtlinien**
  Ein Applikationsserver, der nur in der Cloud des Herstellers betrieben werden kann, stellt Unternehmen, die auf Sicherheit Wert legen, vor einige Problemstellungen. David Molnar und Stuart Schechter führen in [MOS2010, S. 3-5] verschiedene Argumente an, die Bedenken an die Sicherheit einer Cloud-Lösung geben können. Nicht alle in der Quelle angegebenen Punkte, können auf eine Instant-Messenger-Applikation übertragen werden Die nachfolgende Auflistung erfasst aber einige grundlegende Fragen.
  - Kann der Hersteller firmeninterne Nachrichten mitlesen?
  - Was passiert mit persönlichen Daten, falls das Unternehmen zahlungsunfähig wird?
  - Kann der Hersteller einen bestimmten Prozentsatz an Verfügbarkeit garantieren?
  - Wie schnell reagiert der Hersteller bei Ausfällen?
  - Welche Hard- und Software setzt der Hersteller ein, um Daten zu speichern?
  - Was passiert mit Daten, falls das Unternehmen durch einen Mitbewerber aufgekauft wird?
  - Werden rechtliche Anforderungen eingehalten?

  Die Ablage von firmeninternen Daten in der Hersteller-Cloud ist für das sicherheitsbewusste Unternehmen Next-Drive ein Sicherheitsrisiko.

  Eine proprietäre Software kann mit einer Blackbox verglichen werden. Der Hersteller bietet die Applikation an, gibt aber nicht preis wie die Applikation umgesetzt wurde und

ob sie Sicherheitsrichtlinien einhält. Der Kunde, in diesem Fall das fiktive Unternehmen muss dem Hersteller vertrauen ohne dessen Software auf Schwachstellen überprüfen zu können.

- **1 Punkt - Bewertungsrichtlinien**
  Sicherheitsunternehmen bieten sogenannte Audits an, die feststellen, ob eine Software einen bestimmten Sicherheitsstandard einhält. Dies kann das Vertrauen in eine bestimmte Applikation erhöhen. Der Vorteil für den Hersteller liegt darin, dass er eine offizielle Bestätigung erhält, die die Sicherheit seiner Software bestätigt. Er behält aber die volle Kontrolle über seine Software und gibt weiterhin keinen Einblick in deren Innenleben. Ein Beispiel für ein IT-Sicherheitsaudit gibt [ITA2017], das für die Applikation Slack durchgeführt wurde.

- **2 Punkte - Bewertungsrichtlinien**
  Ein Applikationsserver, der firmenintern betrieben werden kann, bietet einige interessante Vorteile.
  - Die Chat-Nachrichten werden nicht auf fremden IT-Systemen gespeichert.
  - Für die Betreibung der Applikation kann das Unternehmen selbstständig die passende Hard- und Software auswählen und sie optimal für ihre eigene IT-Infrastruktur integrieren.
  - Bei Ausfällen kann das Unternehmen sofort unabhängig reagieren.
  - Das Unternehmen kann ein eigenes Logging betreiben.

- **3 Punkte - Bewertungsrichtlinien**
  Die Applikation erreicht drei Punkte in der Wertungsskala, wenn sich der Applikationsserver firmenintern aufsetzten lässt und der Quellcode jedem Interessierten zugänglich gemacht wurde. Das Ziel ist z. B. dann erfolgreich umgesetzt, wenn eine der kostenlosen Hosting-Plattformen wie z. B. GitLab genutzt wurde.

- **4 Punkte - Bewertungsrichtlinien**
  Die Applikation erreicht die volle Punktzahl, falls sich der Applikationsserver firmenintern aufsetzen lässt und der Quellcode der Applikation unter einer anerkannten freien Lizenz läuft. Einen Überblick über verschiedene Anbieter von Open-Source-Lizenzen gibt [OSL2017].

Punkte	Beurteilung
4	Der Applikationsserver lässt sich firmenintern betreiben und der Quellcode der Applikation ist quelloffen. Des Weiteren stehen alle Teile der Applikation unter einer gültigen und anerkannten Lizenz.
3	Der Applikationsserver lässt sich firmenintern betreiben und der Quellcode der Applikation ist quelloffen.
2	Der Applikationsserver lässt sich firmenintern betreiben und der Quellcode der Applikation ist proprietär. Des Weiteren fanden externe Audits der Applikation statt.
1	Der Applikationsserver lässt sich nicht firmenintern betreiben und der Quellcode der Applikation ist proprietär. Des Weiteren fanden externe Audits der Applikation statt.
0	Der Applikationsserver lässt sich nicht firmenintern betreiben und der Quellcode der Applikation ist proprietär. Des Weiteren fanden keine externe Audits der Applikation statt.

Tabelle 3.6: Bewertungsskala: Verfügbarkeit der Applikation

3.4 Gewichtung der sicherheitsrelevanten Entscheidungskriterien

Nachdem die sicherheitsrelevanten Entscheidungskriterien im vorherigen Kap. 3.3 festgelegt wurden, müssen sie als Teil der Nutzwertanalyse gewichtet werden. In[KUH2004][S.10 - S.16] wird ausführlich beschrieben, welche Verfahren zur Gewichtung angewendet werden können. Da nur fünf Entscheidungskriterien vorliegen, bietet sich das Prozentverfahren zur Gewichtung an.

- **Nachrichtenverschlüsselung [30% von 100%]**
  Die Vertraulichkeit in Form der Nachrichtenverschlüsselung stellt ein wesentliches Sicherheitsmerkmal für das Unternehmen dar. Da neben dem firmeninternen Netzwerk auch das unsichere Internet als Übertragungsmedium genutzt werden soll, erwartet das Unternehmen die Umsetzung des bestmöglichen Sicherheitsstandards und gewichtet das Kriterium mit einem hohen Prozentsatz.

- **Authentifizierung des internen Anwenders [10% von 100%]**
  Der internen Authentifizierung wird mit 10% eine weniger bedeutende Rolle zugeschrieben. Zum einen ist eine Brute-Force-Attacke innerhalb des Unternehmens ,durch einen Mitarbeiter sehr unwahrscheinlich. Zum anderen würde ein Angriff auf die interne Authentifizierung, durch eine vorhandene Protokollierung des Applikationsservers, schnell auffallen.

- **Authentifizierung des externen Anwenders [25% von 100%]**
  Im Gegensatz stellt die externe Authentifizierung ein bedeutendes Sicherheitsmerkmal dar, das mit 25% gewichtet wird. Das Unternehmen erwartet sowohl bei der Authentifizierung bei herstellereigenen Cloud-Servern als auch bei der Authentifizierung von außerhalb des unternehmerischen Netzwerkes, den bestmöglichen Sicherheitsstandard.

- **Autorisierung des Anwenders [15% von 100%]**
  Die Autorisierung innerhalb einer Instant-Messenger-Applikation ist dem Unternehmen weniger bedeutend. Zum einen sieht das Unternehmen bei der Autorisierung der Applikation ein geringes Sicherheitsrisiko, zum anderen stellt eine Zuweisung, von aktuell 24 Anwenderrechten, kein Problem dar.

- **Verfügbarkeit der Applikation [20% von 100%]**
  Die Verfügbarkeit der Applikation geht mit den restlichen 20% in die Wertung mit ein. Dem Unternehmen ist es von Bedeutung, wo die Nachrichten gespeichert werden und ob der Hersteller bezüglich der Entwicklung seines Produktes transparent ist.

4 Anwendung des Entscheidungsmodells

4.1 Auswahl von Entscheidungsalternativen

Bei der Auswahl der Entscheidungsalternativen wurde der Fokus auf team-basierte Instant-Messenger-Applikationen gelegt. Folgende Artikel haben zur Findung der Entscheidungsalternativen beigetragen:

- *Slack-Alternativen: Diese Team-Messenger sind einen Blick wert* [SLA2017]
- *The Top 11 Slack Alternatives* [TTS2016]

In der nachfolgenden Tab. 4.1 werden die für die Nutzwertanalyse vorübergehend verwendeten Alternativen vorgestellt.

Produktname	**Hersteller**	**Lizenz**
Azendoo	Azendoo	Proprietäre Software
Bitrix24	Bitrix, Inc.	Proprietäre Software
Circuit	Unify Software & Solutions GmbH & Co.KG	Proprietäre Software
eXo Platform	eXo Platform	Proprietäre Software
Fleep	Fleep Technologies	Proprietäre Software
Hipchat	Atlassian	Proprietäre Software
Jostle	Jostle Corporation	Proprietäre Software
Let's Chat	SD Elements,Inc.	Freie Software
Keybase Teams	Keybase ,Inc.	Freie Software
Mattermost	Mattermost,Inc.	Freie Software
Office 365[1]	Microsoft	Proprietäre Software
Riot.im	Vector Creations Ltd	Freie Software
Rocket.Chat	Rocket.Chat	Freie Software
Weiter auf der nächsten Seite		

Tabelle 4.1 – Fortsetzung von vorheriger Seite

Produktname	Hersteller	Lizenz
Sid	Spherebox UG	Proprietäre Software
Slack	Slack Technologies	Proprietäre Software
Stride	Atlassian	Proprietäre Software
Twist	Doist Limited	Proprietäre Software
Watson Workspace	IBM	Proprietäre Software
Wickr Pro	Wickr, Inc.	Proprietäre Software
Zulip	Dropbox, Inc.	Freie Software

Tabelle 4.1: Vorauswahl von Entscheidungsalternativen

4.2 Bewertung anhand der Ausschlusskriterien

Mit Hilfe der in Kap. 3.2 vorgestellten Ausschlusskriterien wird eine Vorauswahl aus den in Kap. 4.1 vorgestellten Entscheidungsalternativen getroffen.

- **Ausschlusskriterium: Kostenfreie Grundversion**
  Von den 20 verfügbaren Applikationen haben sieben Applikationen das erste K.o.-Kriterium nicht erfüllt.

  1. **Azendoo** - Die Azendoo-Applikation bietet nur eine kostenlose 30-Tage Testversion an.
  2. **Bitrix 24** - Bitrix 24 bietet zwar eine kostenlose Version an, bietet aber nur Platz für maximal 12 Benutzer.
  3. **exo Platform** - Die Testversion von exo Platform ist in ihrer Funktionalität so stark eingeschränkt, dass sie schon mit dem ersten K.o.-Kriterium ausgeschieden ist.
  4. **Jostle** - Die Jostle Applikation bietet nur eine kostenlose 30-Tage-Testversion an.
  5. **Office 365** - Office 365 der Firma Microsoft ist nur als gebührenpflichtige Applikation verfügbar.

[1] Zum Umfang der Office 365 Suite gehören die Instant-Messenger-Applikationen Skype for Business und Microsoft Teams

6. **Stride** - Die Applikation Stride ist der offizielle Nachfolger der Applikation Hipchat. Mit dem jetzigen Stand (20.11.2017) ist nur eine zugangsbeschränkte Testversion verfügbar.
7. **Wickr Pro** - Die Wickr-Pro-Applikation bietet nur eine kostenlose 30-Tage-Testversion an.

- **Ausschlusskriterium: Unabhängigkeit der Applikation**
  Von den dreizehn verfügbaren Applikationen erfüllen alle das zweite K.o.-Kriterium.
- **Ausschlusskriterium: Platformunabhängigkeit**
  Von den dreizehn verfügbaren Applikationen erfüllen alle das dritte K.o.-Kriterium.
- **Ausschlusskriterium: Externe API-Anbindung**
  Von den dreizehn verfügbaren Applikationen haben acht das vierte K.o.-Kriterium nicht erfüllt.
  1. **Circuit** - Die Applikation bietet keine Erweiterung an, die vom Unternehmen vorgegeben wurde. Die Implementierung eigener Erweiterungen, ist der Dokumentation unter [CIR2017] nicht zu entnehmen.
  2. **Hipchat** - Die Applikation Hipchat bietet keine JIRA-Anbindung an. Da es sich um proprietäre Software handelt, ist eine eigene Implementierung einer Anbindung nicht möglich.
  3. **Keybase Teams** - Die Applikation Keybase Teams befindet sich momentan in der Entwicklung und wurde noch nicht in einer finalen Version veröffentlicht. Zum momentanen Zeitpunkt ist eine API-Anbindung noch nicht integriert.
  4. **Let's Chat** Die Applikation bietet keine Erweiterung an, die vom Unternehmen vorgegeben wurde. Die Implementierung eigener Erweiterungen, ist der Dokumentation unter [LET2017] nicht zu entnehmen.
  5. **Riot.im** - Die Applikation Riot.im bietet keine JIRA- oder GitLab-Anbindung an. Des Weiteren stellt die Homepage des Entwicklers keinerlei Informationen darüber bereit, in wie weit sich eigene Erweiterungen realisieren lassen.
  6. **Sid** - Die Applikation Sid stellt kein API zur Verbindung mit externe Software zur Verfügung.

7. **Twist** - Von den erforderlichen Erweiterungen ist nur die GitLab-Erweiterung verfügbar. Die eigene Implementierung von Erweiterungen ist nicht möglich.
8. **Watson Workspace** - Die Applikation bietet keine geforderte Erweiterung an. Die Implementierung eigener Erweiterungen ist nicht möglich.

- **Ausschlusskriterium: Ende-zu-Ende Verschlüsselung**
  Von den fünf verfügbaren Applikationen haben zwei das fünfte K.o.-Kriterium nicht erfüllt.
  1. **Fleep** - Die Applikation Fleep ist proprietär und somit von diesem Kriterium betroffen. Auf der Webseite des Herstellers finden sich keine Informationen über eine Implementierung einer Ende-zu-Ende-Verschlüsselung.
  2. **Slack** - Die Applikation Slack ist proprietär und somit von diesem Kriterium betroffen. Wie bei der Applikation Fleep, stellt die Webseite des Herstellers keine Informationen über eine Ende-zu-Ende-Verschlüsselung bereit.

- **Ausschlusskriterium: Gruppenchat-Funktion**
  Von den drei übrig gebliebenen Applikationen erfüllen alle das sechste K.o.-Kriterium.

4.3 Zwischenfazit

Von den in Kap. 4.1 vorgestellten Applikationen haben siebzehn die K.o.-Kriterien nicht erfüllt. Die drei übrig gebliebenen Alternativen erfüllen alle erforderlichen K.o.-Kriterien und sind somit für die Nutzwertanalyse von Sicherheitseigenschaften in Kap. 4.4 zugelassen. Alle drei Alternativen sind unter einer freien Lizenz veröffentlicht worden, was ein umfangreiches Testszenario für die Nutzwertanalyse ermöglicht.

Produktname	Hersteller	Lizenz
Mattermost	Mattermost, Inc.	Server: MIT-Lizenz Clients: Apache-Lizenz v2.0 Doc: Creative-Common-CC-BY-NC-SA-3.0-Lizenz
Rocket.Chat	Rocket.Chat	Freie Software, steht unter MIT-Lizenz
Zulip	Dropbox, Inc.	Freie Software, steht unter Apache-Lizenz v2.0

Tabelle 4.2: Alternativen für die Nutzwertanalyse

4.4 Bewertung anhand der sicherheitsrelevanten Entscheidungskriterien

Um die Entscheidungskriterien bewerten zu können, ist eine manuelle Konfiguration und Bereitstellung der Applikationen erforderlich. Zu diesem Zweck wurde eine Testumgebung, bestehend aus einem Windows10-Client und einem Ubuntu-Server, vorbereitet. Jeder Applikationsserver hat eine eigene Ubuntu-Instanz, die mit der Applikation Vagrant realisiert wurde. Die Überprüfung der verwendeten Cipher-Suites wurde mit der Applikation Wireshark gewährleistet.

4.4.1 Nachrichtenverschlüsselung

Bewertung der Mattermost-Applikation

Verwendete Software auf der Seite des Clients

- Betriebssystem: Windows 10 Professional 64-Bit
- IPv4-Adresse: 192.168.178.80
- Applikation: Mattermost-Windows-Client v3.7.1

Verwendete Software auf der Seite des Servers

- Betriebssystem: Ubuntu 16.04 LTS 64-Bit
- IPv4-Adresse: 192.168.178.55
- Applikationen: Mattermost-Server v4.4.3, Nginx Webserver v1.10.3

Um die TLS-Funktionalität nutzen zu können, muss auf der Seite des Servers, Nginx als Webserver vor den Mattermost-Server vorschalten werden. Ruft der Client die Adresse des Applikationsservers auf, wird sein Aufruf durch Nginx abgefangen und an den Mattermost-Server weitergeleitet. Somit kann durch den Webserver garantiert werden, dass unverschlüsselte HTTP-Aufrufe automatisch in verschlüsselte HTTPS-Aufrufe umgewandelt werden. Das Betriebssystem des Clients bietet eine vollständige TLS-1.2-Funktionalität an. Dementsprechend können bei der Konfiguration des Webservers alle TLS/SSL-Versionen, außer der aktuellsten Version 1.2, deaktiviert werden.

Die Abb. 4.1 zeigt eine erfolgreiche Festlegung einer Cipher-Suite zwischen dem Client und dem Server mit Hilfe des TLS-Protkolls. Der Client verschickt eine ‚Client Hello' Nachricht an den Server und bietet diesem 16 verschiedene Cipher-Suite Kombinationen an. Der Server antwortet mit einer ‚Server Hello' Nachricht und teilt dem Client mit, das er die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 verwenden möchte. Zum Abschluss bestätigt der Client den Wunsch des Servers mit einer ‚Change Cipher Spec' Nachricht. Die Verwendung dieser Cipher-Suite wird mit der maximalen Punktzahl bewertet.

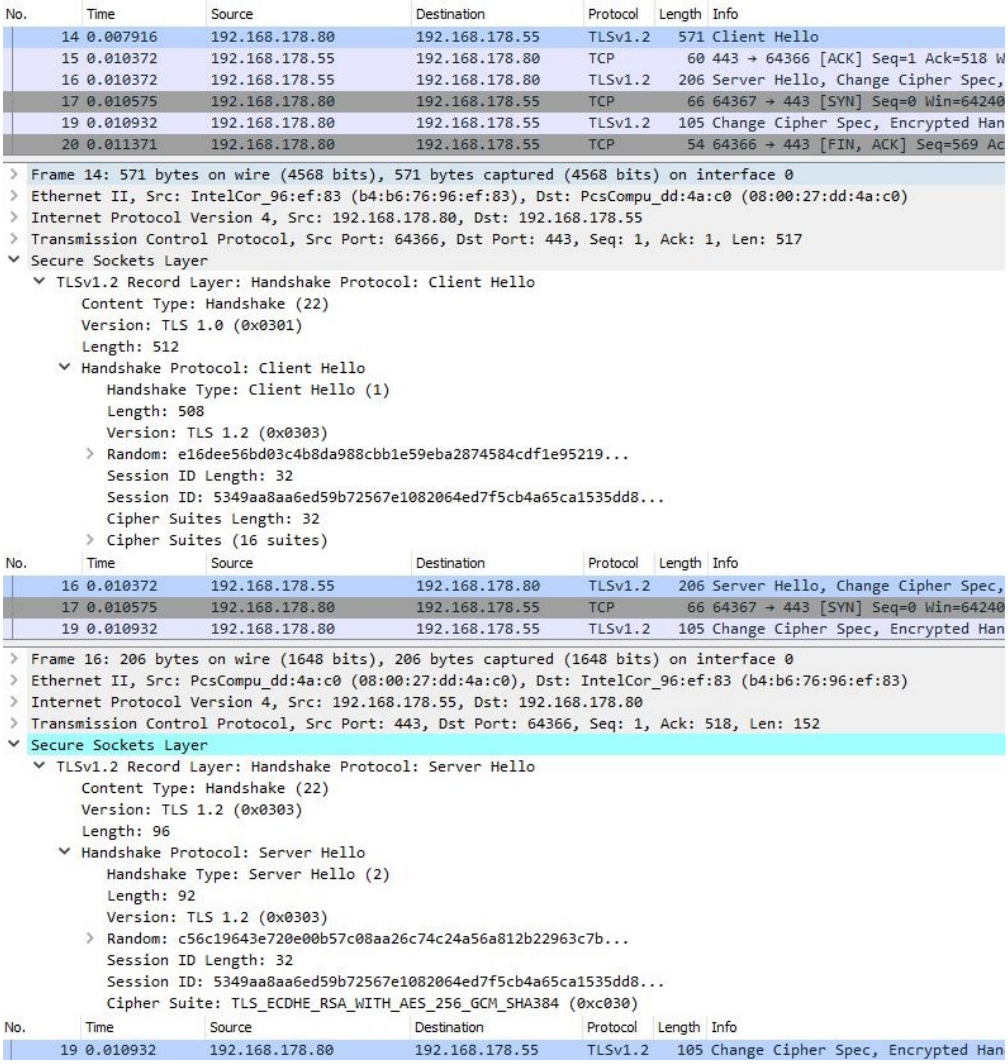

Abbildung 4.1: Nachrichtenverschlüsselung unter Mattermost

Punkte	Beurteilung
4	Mit TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 wird eine Cipher-Suite verwendet, die einer Empfehlung aus Abb. 3.6 entspricht.

Bewertung der Rocket.Chat-Applikation

Verwendete Software auf der Seite des Clients

- Betriebssystem: Windows 10 Professional 64-Bit
- IPv4-Adresse: 192.168.178.80
- Applikation: Rocket.Chat-Windows-Client v2.9.0

Verwendete Software auf der Seite des Servers

- Betriebssysteme: Ubuntu 16.04 LTS 64-Bit
- IPv4-Adresse: 192.168.178.56
- Applikationen: Rocket.Chat-Server v0.59.6, Nginx-Webserver v1.10.3

Die Applikation Rocket.Chat kann den selben Sicherheitsstandard der Nachrichtenverschlüsselung anbieten, wie die zuvor bewertete Applikation Mattermost. Um die TLS-Funktionalität nutzen zu können, muss auch hier ein Webserver zwischen die Kommunikation schalten werden. Im Unterschied zu Mattermost, wo die Installation des Webservers manuell durchgeführt wird, wird hier der Webserver mit dem Serverpaket mitinstalliert. Als Betriebssystem wird wieder Windows 10 Professional 64-Bit eingesetzt, was ermöglicht, die Verbindung auf TLS 1.2 zu beschränken.

Die Abb. 4.2 zeigt eine erfolgreiche Festlegung einer Cipher-Suite zwischen dem Client und dem Server mit Hilfe des TLS-Protokolls. Der Client verschickt eine ‚Client Hello' Nachricht an den Server und bietet diesem 14 verschiedene Cipher-Suite Kombinationen an. Der Server antwortet mit einer ‚Server Hello' Nachricht und teilt dem Client mit, das er die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 verwenden möchte. Zum Abschluss bestätigt der Client den Wunsch des Servers mit einer ‚Change Cipher Spec' Nachricht. Die Verwendung dieser Cipher-Suite wird mit der maximalen Punktzahl bewertet.

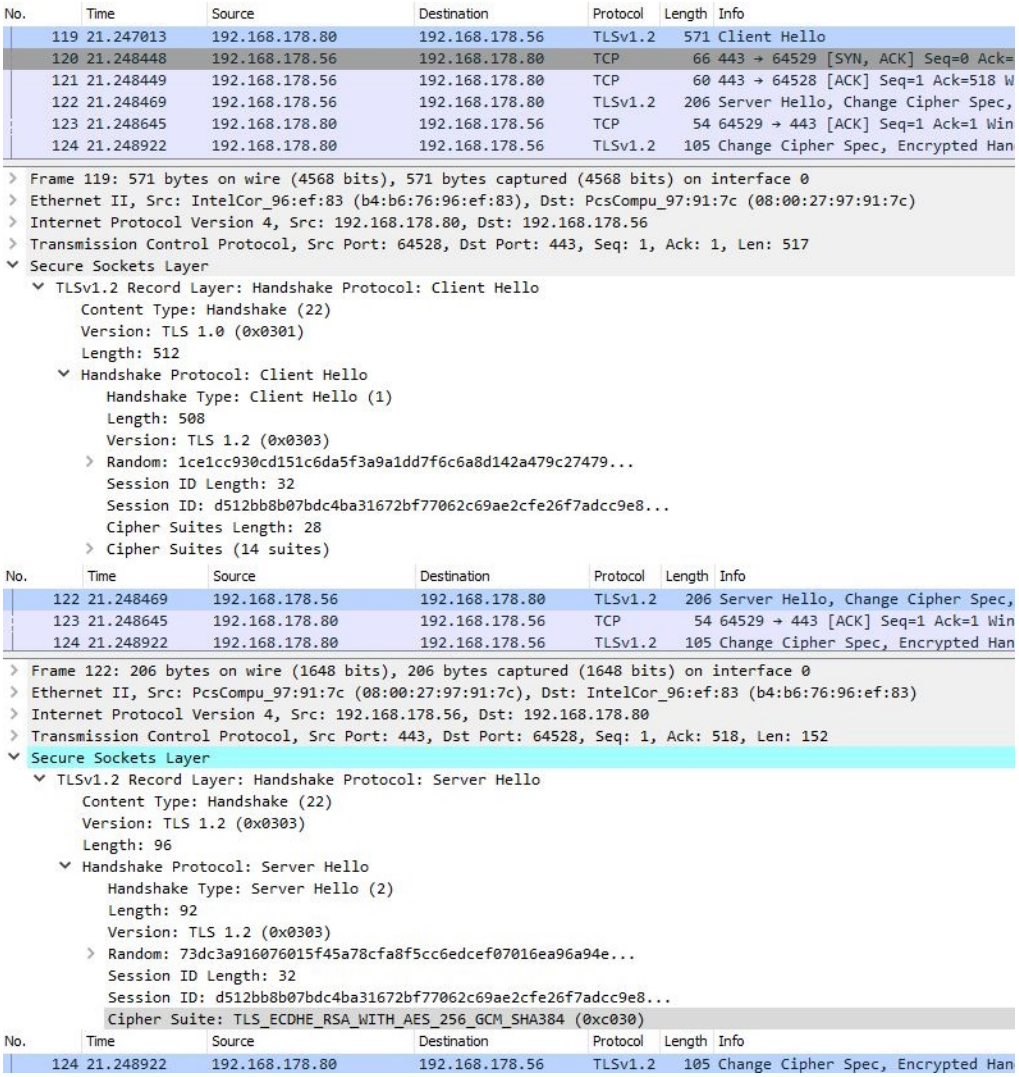

Abbildung 4.2: Nachrichtenverschlüsselung unter Rocket.Chat

Punkte	Beurteilung
4	Mit TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 wird eine Cipher-Suite verwendet, die einer Empfehlung aus Abb. 3.6 entspricht.

Bewertung der Zulip-Applikation

Verwendete Software auf der Seite des Clients

- Betriebssystem: Microsoft Windows 10 Professional 64-Bit
- IPv4-Adresse: 192.168.178.80
- Applikation: Zulip-Windows-Client v1.7.0

Verwendete Software auf der Seite des Servers

- Betriebssystem: Ubuntu 16.04 LTS 64-Bit
- IPv4-Adresse: 192.168.178.57
- Applikationen: Zulip-Server v1.7.1, Nginx-Webserver v1.10.3

Die Applikation Zulip lässt sich auf die selbe Art und Weise einrichten wie die zuvor bewertete Applikation Rocket.Chat. Die TLS-Funktionalität wird mit dem Webserver gewährleistet, der mit dem Serverpaket mitinstalliert wird. Windows 10 Professional 64-Bit bietet die selbe TLS-1.2-Funktionalität, wie in den beiden vorigen Applikationen.

Die Abb. 4.3 zeigt eine erfolgreiche Festlegung einer Cipher-Suite zwischen dem Client und dem Server mit Hilfe des TLS-Protokolls. Der Client verschickt eine ‚Client Hello' Nachricht an den Server und bietet diesem 16 verschiedene Cipher-Suite Kombinationen an. Der Server antwortet mit einer ‚Server Hello' Nachricht und teilt dem Client mit, das er die Cipher-Suite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 verwenden möchte. Zum Abschluss bestätigt der Client den Wunsch des Servers mit einer ‚Change Cipher Spec' Nachricht. Die Verwendung dieser Cipher-Suite wird mit der maximalen Punktzahl bewertet.

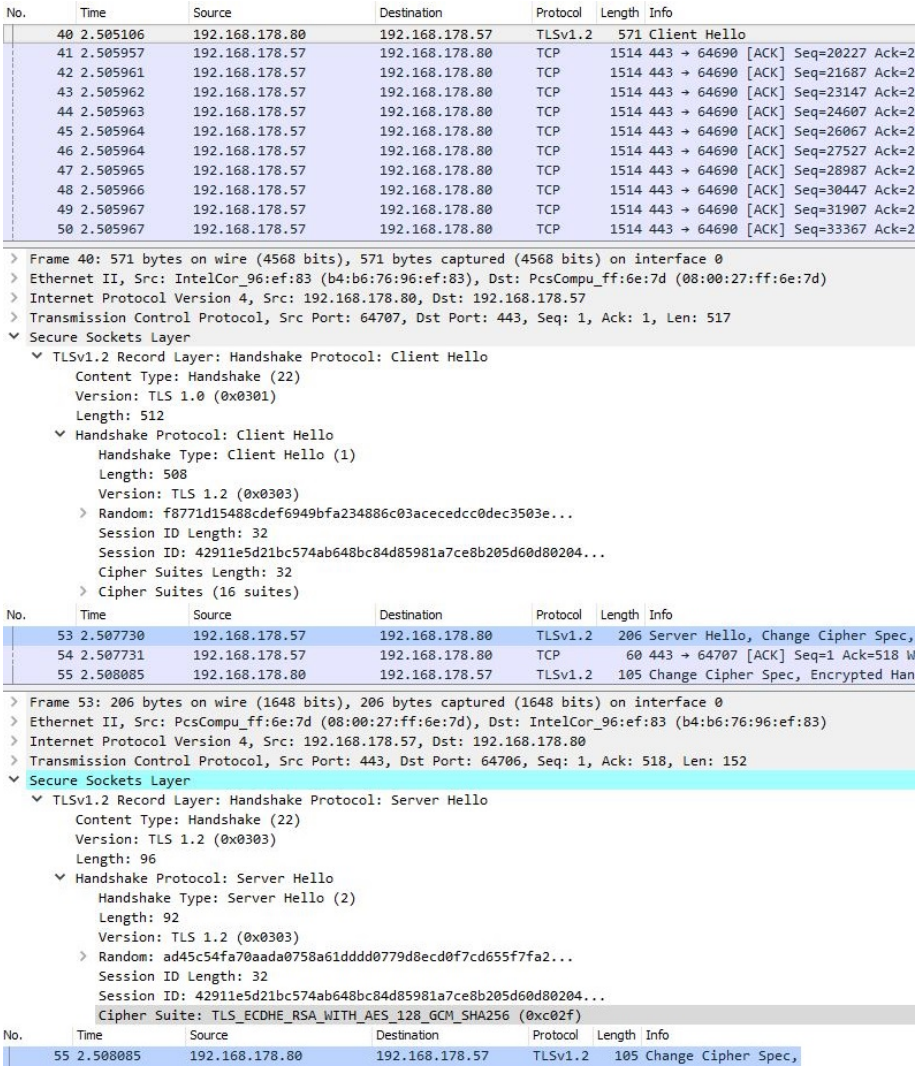

Abbildung 4.3: Nachrichtenverschlüsselung unter Zulip

Punkte	Beurteilung
4	Mit TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 wird eine Cipher-Suite verwendet, die einer Empfehlung aus Abb. 3.6 entspricht.

4.4.2 Authentifizierung des Anwenders

Bewertung der Mattermost-Applikation

Aus den zu bewertenden Möglichkeiten aus Tab. 3.3 und Tab. 3.4, bietet die Applikation nur die Ein-Faktor-Authentifizierung, bestehend aus Benutzername bzw. E-Mail-Adresse und Passwort, an. Sowohl die Dokumentation unter [MAU2017] als auch die Konfigurationsmöglichkeiten des Administrators, bieten keine weitere Möglichkeit der Authentifizierung an, die durch die Bewertungsskala abgedeckt wird.

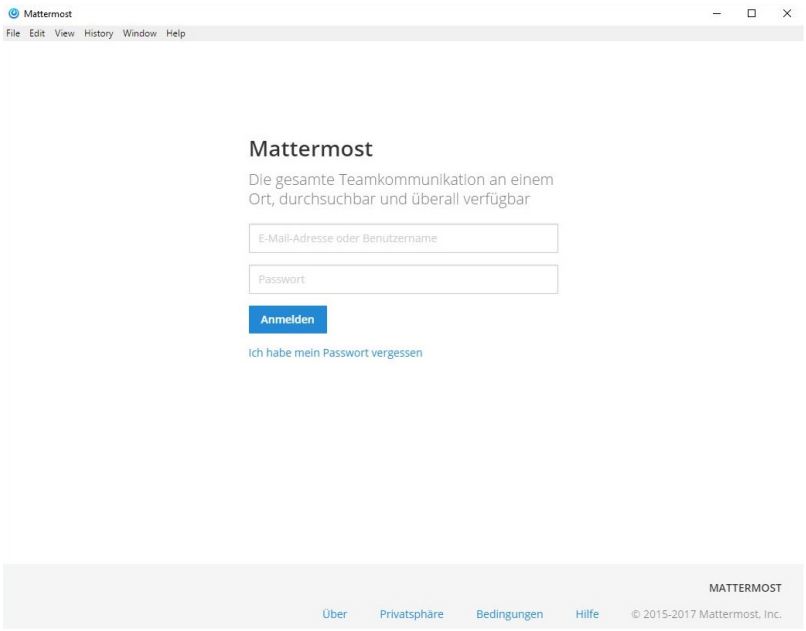

Abbildung 4.4: Ein-Faktor-Authentifizierung unter Mattermost

Somit wird sowohl die interne als auch die externe Authentifizierung mit einem Punkt bewertet.

Punkte	Interne Beurteilung
1	Ein-Faktor-Authentifizierung bestehend aus Email-Adresse und Passwort

Punkte	Externen Beurteilung
1	Ein-Faktor-Authentifizierung bestehend aus Email-Adresse und Passwort

Bewertung der Rocket.Chat-Applikation

Die Applikation bietet sowohl eine Ein-Faktor Authentifizierung bestehend aus Benutzername bzw. E-Mail-Adresse und Passwort, als auch die Möglichkeit der Zwei-Faktor-Authentifizierung mit Hilfe eines Software-Tokens. Dazu wird die mobile Applikation Google Authenticator, in diesem Fall die Android-Version aus dem Play Store[2]verwendet. Mit Hilfe der mobilen Token-Generierung kann die in Abb. verwendete Zwei-Faktor Authentifizierung erfolgreich abgeschlossen werden.

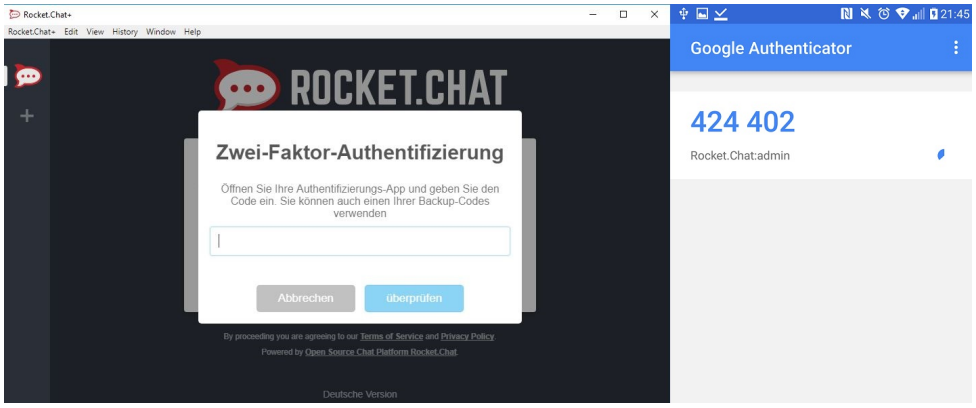

Abbildung 4.5: Zwei-Faktor-Authentifizierung unter Rocket.Chat

Somit wird die Authentifizierung für den internen Anwender mit drei Punkten und für den externen Anwender mit 4 Punkten bewertet.

Punkte	Interne Beurteilung
3	Zwei-Faktor-Authentifizierung bestehend aus Email-Adresse, Passwort und Token per Authentifizierungs-Applikation

Punkte	Externe Beurteilung
4	Zwei-Faktor-Authentifizierung bestehend aus Email-Adresse, Passwort und Token per Authentifizierungs-Applikation

[2] https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=de

Bewertung der Zulip-Applikation

Aus den zu bewertenden Möglichkeiten aus Tab. 3.3 und Tab. 3.4, bietet die Applikation nur die Ein-Faktor-Authentifizierung, bestehend aus Benutzername bzw. E-Mail-Adresse und Passwort, an. Sowohl die Dokumentation unter [ZAU2017] als auch die Konfigurationsmöglichkeiten des Administrators, beschreiben keine weitere Möglichkeit der Authentifizierung, die durch die Bewertungsskala abgedeckt wird.

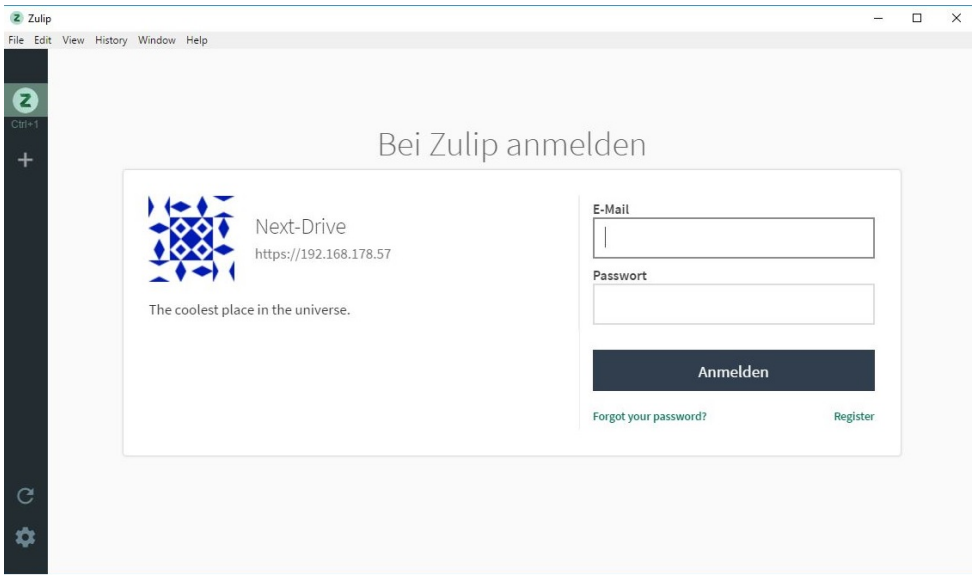

Abbildung 4.6: Ein-Faktor-Authentifizierung unter Zulip

Punkte	Interne Beurteilung
1	Ein-Faktor-Authentifizierung bestehend aus Email-Adresse und Passwort

Punkte	Externen Beurteilung
1	Ein-Faktor-Authentifizierung bestehend aus Email-Adresse und Passwort

4.4.3 Autorisierung des Anwenders

Bewertung der Mattermost-Applikation

Die Applikation bietet nur eine eingeschränkte Rechtevergabe an. Die Abb. 4.7 stellt die Rechtevergabe der Applikation Mattermost dar.

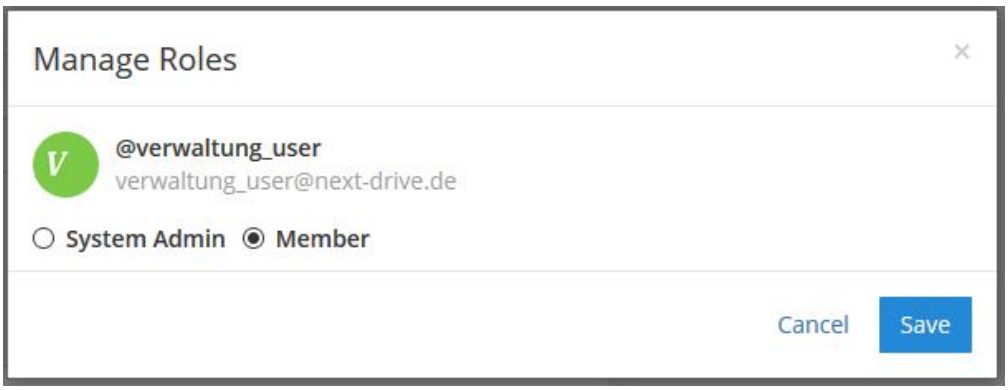

Abbildung 4.7: Rechteverwaltung unter Mattermost

Der Abbildung ist zu entnehmen, dass die Applikation zwei feste Rollen vorsieht. Das Erstellen von weiteren Rollen ist nicht möglich. Es ist zudem nicht bekannt, welche Berechtigungen im Detail beide Rollen besitzen. Der Systemadministrator hat Zugriff auf alle Teile der Applikation und kann sie beliebig konfigurieren. Die Rolle Member hat nur die Möglichkeit, Direktnachrichten an Kollegen zu verschicken oder private Kanäle zu erstellen. Diese können für temporäre Projekte genutzt werden, an denen z.B. mehrere Mitarbeiter aus verschiedenen Abteilungen beteiligt sind. Um die Gruppenchats der Abteilungen zu sehen, muss der Anwender vom Systemadministrator eingeladen werden.

Die Applikation kann nur mit Administratorrechten verwaltet werden und bietet keine Vergabe von Berechtigungen an. Aus diesem Grund wird die Applikation mit einem Punkt bewertet.

Punkte	Beurteilung
1	Verwendung einer zentralen Benutzerverwaltung durch einen Administrator

Bewertung der Rocket.Chat-Applikation

Im Gegensatz zur vorherigen Applikation, wird die Rechtevergabe mit einer großen Auswahl an vordefinierten Rollen gelöst. Wie der Abb. 4.8 zu entnehmen ist, stellt die Applikation eine große Anzahl an verschiedenen Berechtigungen bereit, die den unterschiedlichen Rollen erteilen werden können. Des Weiteren ist es möglich, eigene Rollen hinzuzufügen und zu konfigurieren. Die Applikation erfüllt das Kriterium im vollen Umfang und wird somit mit vier Punkten bewertet.

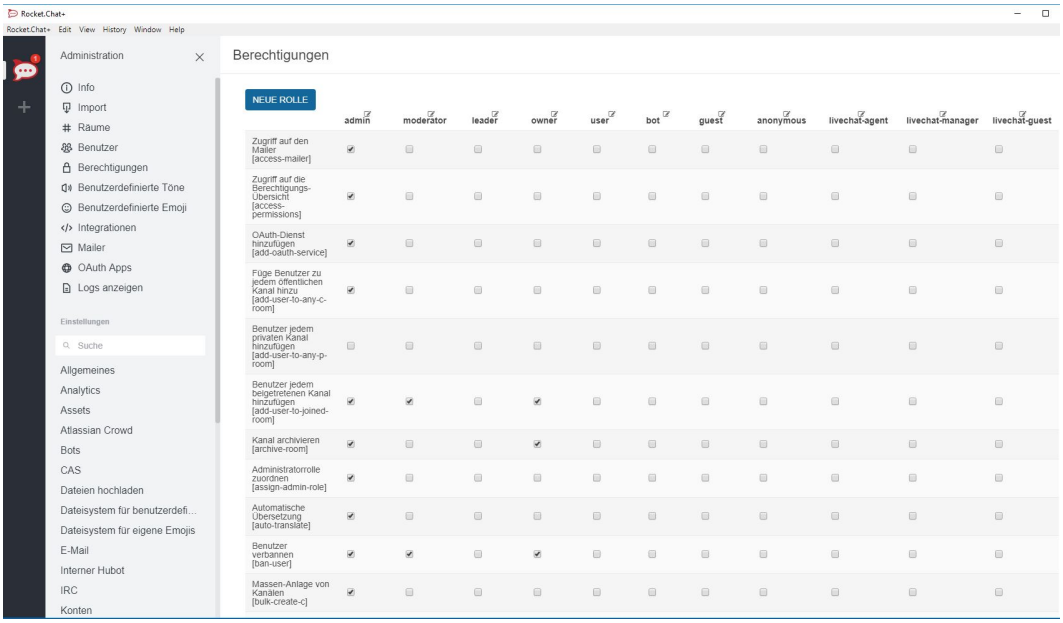

Abbildung 4.8: Rechteverwaltung unter Rocket.Chat

Punkte	Beurteilung
4	Die zentrale Benutzerverwaltung unterstützt die rollenbasierte Rechtevergabe.

Bewertung der Zulip-Applikation

Wie bei der Mattermost-Applikation unterscheidet Zulip nur zwischen den Rechten des Administrators und den Rechten des einfachen Anwenders. Die Abb. 4.9 zeigt exemplarisch, dass für die Rechtevergabe nur zwischen den Buttons ‚Admin entfernen'und ‚Zum Admin machen'unterschieden wird.

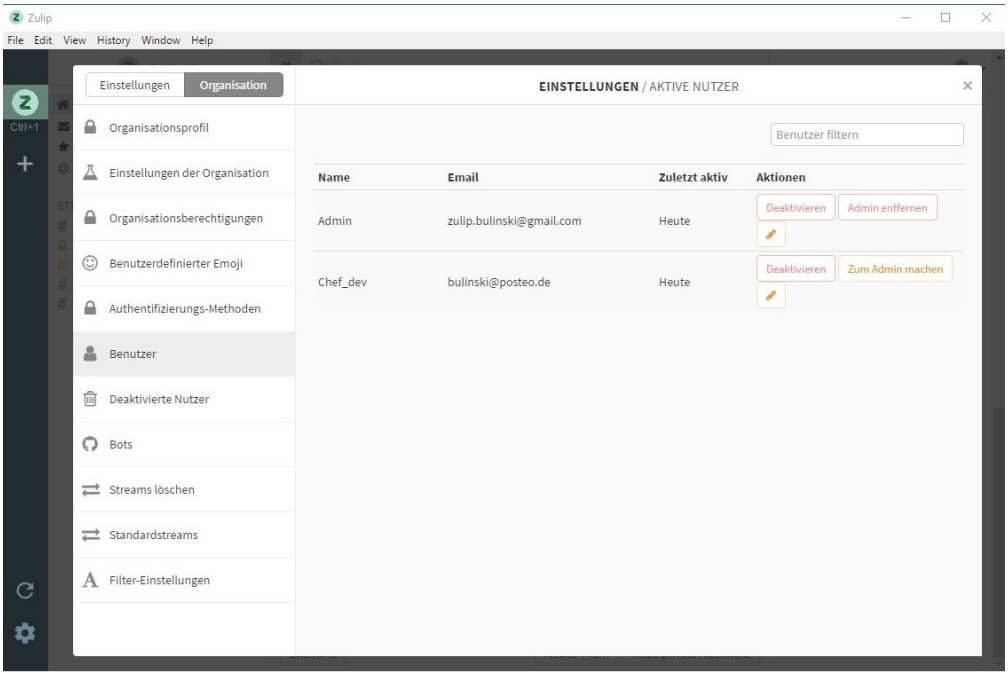

Abbildung 4.9: Rechteverwaltung unter Zulip

Das Erstellen von weiteren Rollen ist nicht möglich. Zudem ist nicht bekannt, welche Berechtigungen im Detail beide Rollen besitzen. Des Weiteren lassen sich keine Berechtigungen einzeln oder an Benutzergruppen vergeben. Somit wird dieses Kriterium mit einem Punkt bewertet.

Punkte	Beurteilung
1	Verwendung einer zentralen Benutzerverwaltung durch einen Administrator.

4.4.4 Verfügbarkeit der Applikation

Bewertung der Mattermost-Applikation

Die für die Auswertung verwendete kostenfreie Team-Edition von Mattermost lässt sich firmenintern betreiben. Die benötigen Installationsdateien und eine umfangreiche Anleitung sind unter [3]zu finden. Neben der manuellen Installation stehen dem Anwender weitere Möglichkeiten zur Verfügung. So kann er mit Hilfe eines Automatisierungswerkzeugs, die Installation durchführen lassen. Dafür stehen Anleitungen für Heroku, Puppet, Chef und Ansible bereit. Des Weiteren ist es mit Hilfe des Bitnami-Projekts möglich, einen Applikationsserver in der eigenen Cloud z. B. auf Amazon-Web-Services, Azure oder Google-Cloud-Platform aufzusetzen. Alle Teile der Applikation sowohl die unterschiedlichen Clients als auch der Server werden als Quellcode auf GitHub gehostet und stehen somit jedem Interessierten zur Verfügung.

Wie der Abb. 4.2 zu entnehmen ist, wurde Teile der Applikation unter unterschiedlichen Lizenzen veröffentlicht. Der Applikationsserver steht unter MIT-Lizenz, somit sind die unter [MIT2017] angegebenen Rechte und Pflichten bei der Verwendung gültig. Die verwendeten Clients der Applikation stehen unter Apache-v2.0-Lizenz, somit sind die unter [APA2004] angegeben Rechte und Pflichten bei der Verwendung gültig. Die Dokumentation steht unter der Creative-Common-BY-NC-SA-3.0-Lizenz. Die Abb. 4.10 gibt einen genauen Einblick, welche Rechte und Pflichten bei dieser Lizenz einzuhalten sind.

- Der Nutzer ist bei Verwendung verpflichtet, den Autor des Werkes anzugeben.
- Die Vervielfältigung, die Verbreitung und die öffentliche Zugänglichmachung sind gestattet.
- Die Abwandlung, die Bearbeitung und die kommerzielle Nutzung sind nicht gestattet.

Somit erfüllt die Applikation Mattermost das Entscheidungskriterium im vollen Umfang und wird mit 4 Punkten bewertet.

[3] https://about.mattermost.com/download/

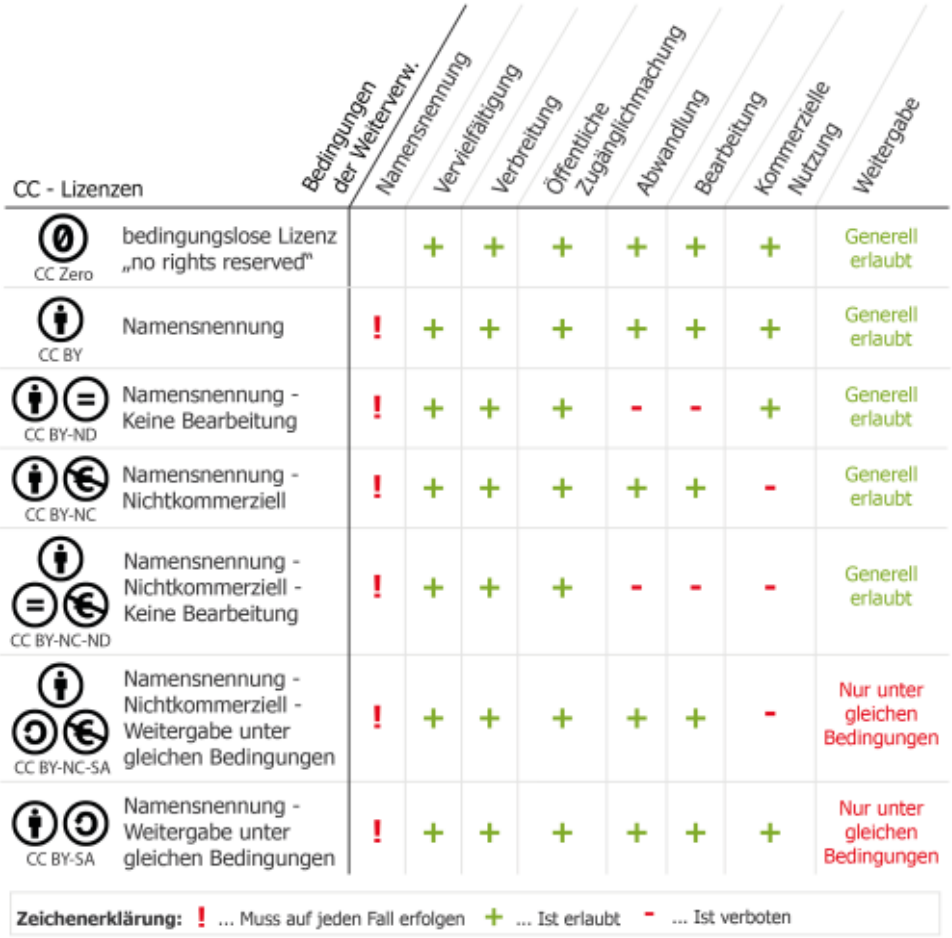

Abbildung 4.10: Überblick der CC-Lizenzen[4]

Punkte	Beurteilung
4	Der Applikationsserver lässt sich firmenintern betreiben und der Quellcode der Applikation ist quelloffen.Des Weiteren stehen alle Teile der Applikation unter einer gültigen und anerkannten Lizenz.

[4] https://www.e-learning.tu-darmstadt.de/media/elc/__relaunch/werkzeuge/openlearnware_3/lehrmaterialien_veroeffentlichen/cc-lizenzen_ueberblick_ueberarb040817.png

Bewertung der Rocket.Chat Applikation

Die für die Auswertung verwendete Rocket.Chat-Applikation, lässt sich firmenintern betreiben und steht somit nicht unter Verwaltung des Herstellers. Die benötigten Installationsdateien und die der Dokumentation sind unter den Quellen [5] und [6]zu finden. Alle Teile der Applikation, sowohl die unterschiedlichen Clients als auch der Server, werden als Quellcode auf GitHub gehostet und stehen somit jedem Interessierten zur Verfügung. Die Rocket.Chat-Applikation steht komplett unter MIT-Lizenz, somit sind die unter [MIT2017] angegeben Rechte und Pflichten bei der Verwendung gültig. Somit erfüllt die Applikation Rocket.Chat das Entscheidungskriterium im vollen Umfang und wird mit vier Punkten bewertet.

Punkte	Beurteilung
4	Der Applikationsserver lässt sich firmenintern betreiben und der Quellcode der Applikation ist quelloffen. Des Weiteren stehen alle Teile der Applikation unter einer gültigen und anerkannten Lizenz.

Bewertung der Zulip Applikation

Der Applikationsserver von Zulip lässt sich firmenintern betreiben und kann mit Hilfe der Anleitung unter [7]installiert werden. Alle Teile der Applikation werden als Quellcode auf GitHub gehostet und stehen somit jedem Interessierten zur Verfügung. Die Zulip-Applikation steht komplett unter Apache-v2.0-Lizenz, daher sind die unter [APA2004] angegeben Rechte und Pflichten bei der Verwendung gültig. Somit erfüllt die Applikation Zulip das Entscheidungskriterium im vollen Umfang und wird mit vier Punkten bewertet.

Punkte	Beurteilung
4	Der Applikationsserver lässt sich firmenintern betreiben und der Quellcode der Applikation ist quelloffen.Des Weiteren stehen alle Teile der Applikation unter einer gültigen und anerkannten Lizenz.

[5] https://rocket.chat/download
[6] https://rocket.chat/docs/
[7] http://zulip.readthedocs.io/en/latest/production/install.html

4.5 Nutzwertberechnung

Die im vorherigen Kap. 4.4 durchgeführte Punktevergabe wird in der Tab. 4.18 zusammengefasst.

Entscheidungskriterium	Mattermost	Rocket.Chat	Zulip
Kap. 3.3.1 Nachrichtenverschlüsselung	4	4	4
Kap. 3.3.2 Authentifizierung des int. Anwenders	1	3	1
Kap. 3.3.2 Authentifizierung des ext. Anwenders	1	4	1
Kap. 3.3.3 Autorisierung des Anwenders	1	4	1
Kap. 3.3.4 Verfügbarkeit der Applikation	4	4	4

Tabelle 4.18: Übersicht der Punktevergabe ohne Gewichtung

Auf Basis dieser Punktevergabe und der in Kap. 3.4 vergebenen Gewichtung, stellt die folgende Tab. 4.19 die modifizierte Punktevergabe dar. Die bisher vergebenen Punkte werden mit dem Prozentsatz der Gewichtung multipliziert.

Entscheidungskriterium	Gew.	Mattermost	Rocket.Chat	Zulip
Kap. 3.3.1 Nachrichtenverschlüsselung	30 %	120	120	120
Kap. 3.3.2 Authentifizierung des int. Anwenders	10 %	10	30	10
Kap. 3.3.2 Authentifizierung des ext. Anwenders	25 %	25	100	25
Kap. 3.3.3 Autorisierung des Anwenders	15 %	15	60	15
Kap. 3.3.4 Verfügbarkeit der Applikation	20 %	80	80	80
Endergebnis		250	390	250

Tabelle 4.19: Übersicht der Punktevergabe mit Gewichtung

4.6 Ergebnisbewertung

Die im vorherigen Kap. 4.5 abgebildete Tab. 4.19 stellt das Endergebnis dieser Nutzwertanalyse dar. Die Applikation Rocket.Chat hat, mit insgesamt 390 von möglichen 400 Punkten, die höchste Punktzahl erreicht. Die beiden anderen Applikationen haben die gleiche Anzahl an Punkten erreicht und teilen sich mit 250 von möglichen 400 Punkten den gemeinsamen zweiten Platz. Das Ergebnis der Nutzwertanalyse wird nachfolgend für jedes Entscheidungskriterium erläutert.

- **Nachrichtenverschlüsselung**
  Die freie Verwendbarkeit des Applikationsservers aller drei Alternativen, rechtfertigt eine volle Punktzahl bei der Bewertung. Die Konfiguration der Nachrichtenverschlüsselung ist vollständig dem Anwender überlassen. Mit Hilfe eines Webservers, wie z. B. Nginx, ist es dem Anwender möglich die sicherste Cipher-Suite unter Verwendung der aktuellsten TLS-Version zu verwenden.

- **Authentifizierung des Anwenders**
  Mattermost und Zulip bieten, unter Berücksichtigung der Bewertungsskalen aus Kap. 4.4.2, bestenfalls die E-Faktor-Authentifizierung an. Die Applikation Rocket.Chat lässt sich hingegen mit einer Zwei-Faktor-Authentifizierung, zusätzlich zu der Ein-Faktor-Authentifizierung, erweitern. Dies wird mit Hilfe eines Software-Tokens gelöst, das mit der mobilen Google-Authenticator-Applikation generiert werden kann. Dementsprechend wird Rocket.Chat höher bewertet als die beiden anderen Applikationen, die nur das minimale Ziel von einem Punkt erreicht haben.

- **Autorisierung des Anwenders**
  Mattermost und Zulip bieten eine minimalistische Rechtevergabe an. Sie unterscheiden nur zwischen dem Administrator und dem einfachen Anwender. Rocket.Chat hingegen bietet eine umfangreiche Rechtevergabe mit Hilfe von vorgegebenen Rollen und umfangreichen Berechtigungen an. Des Weiteren lassen sich eigene Rollen definieren, denen man verschiedene Berechtigungen erteilen werden können. Dementsprechend erzielt Rocket.Chat die volle Punktzahl in dieser Kategorie, wo hingegen Mattermost und Zulip nur das minimale Ziel von einem Punkt erreicht haben.

- **Verfügbarkeit der Applikation**
  Das letzte Entscheidungskriterium schließen alle drei Alternativen mit der vollen Punktzahl ab. Beim Hosting des Applikationsservers haben die Anwender die freie Wahl, wo und wie sie die Applikation aufsetzen möchten. Für alle drei Alternativen gibt es eine umfangreiche Dokumentation, die bei der Installation oder bei Problemen mit der Applikation behilflich ist. Alle Hersteller setzen auf Open-Source und stellen den Quellcode der Applikation unter einer gültigen und anerkannten freien Lizenz auf dem Filehoster GitHub bereit.

Die Nutzwertanalyse fand in keiner der drei Applikationen eine Schwachstelle, die ein Sicherheitsrisiko für den Gebrauch in Unternehmen darstellen würde. Jede Applikation hat mindestens einem Bewertungspunkt in jeder sicherheitsrelevanten Kategorie erreicht.

5 Fazit und Ausblick

Die Evaluierung von Instant-Messenger-Applikationen in sicherheitsrelevanten Unternehmensbereichen konnte, mit Hilfe der Anforderungen eines repräsentativen fiktiven Unternehmens, im vollen Umfang gelöst werden.

Das fiktive Unternehmen wurde soweit angepasst, um ein praxisnahes Beispiel geben zu können. Die Angaben zur Unternehmensstruktur ermöglichten eine umfangreiche und zielgenaue Ausarbeitung von Ausschlusskriterien. Dies half dabei, den Fokus auf genau die Instant-Messenger-Applikationen zu legen, die sich für die Unternehmensstruktur als passend erweisen würden.

Mit den sicherheitsrelevanten Entscheidungskriterien wurde versucht, relevante Themen der IT-Sicherheit für die Evaluierung von Instant-Messenger-Applikationen abzudecken. Die Schwierigkeit lag darin, die Entscheidungskriterien auf fünf Bewertungspunkte zu begrenzen. Um ein einheitliche Bewertung zu gewährleisten, mussten alle Entscheidungskriterien diese Bewertungsskala einhalten, was sich als schwierig herausstellte. Ein nicht-fiktives Unternehmen wird sich bei der Evaluierung voraussichtlich die Frage stellen, ob eine Fünf-Stufen-Bewertung ausreichend ist.

Eine weitere Schwierigkeit der Evaluierung lag darin, eine möglichst große und aktuelle Anzahl von Instant-Messenger-Applikation abzudecken. Der Markt dieser Applikationen ist in ständiger Bewegung. Beinahe täglich gibt es Meldungen über neue oder verbesserte Applikationen. Das stellt den privaten Anwender vor keine großen Probleme. Ein Unternehmen muss bei der Evaluierung allerdings genau hinschauen, um eine aktuelle bzw. die bestmögliche Anwendung in die IT-Infrastruktur integrieren zu können.

Des Weiteren wurde bei der Evaluierung nur der Bereich der IT-Sicherheit abgedeckt. Wie in der Abgrenzung am Anfang der Arbeit beschrieben wurde, waren andere entscheidende Aspekte nicht Bestandteil dieser Ausarbeitung. Ein nicht fiktives Unternehmen wird aber genau diese Themen in die Entscheidungsfindung mit aufnehmen, um alle relevanten Themen in der Evaluierung mit abdecken zu können. Durch die Abdeckung aller Themen kann sich allerdings das Endergebnis zu Gunsten einer anderen Instant-Messenger-Applikation verändern.

Diese Bachelorarbeit gibt dem Leser einen Einblick, wie eine Entscheidungsfindung mit Hilfe der Nutzwertanalyse aussehen kann. Auf Grundlage dieser Ausarbeitung kann eine eigene Evaluierung mit eigenen Entscheidungskriterien durchgeführt werden. Dabei ist es nicht von Bedeutung, welche Art von Objekt evaluiert werden muss. Die Nutzwertanalyse eignet sich für jede Art von Objekten, um eine Evaluierung nach einer systematischen Vorgehensweise durchzuführen.

Literaturverzeichnis

[APA2004] Apache Licens Version 2.0 - Januar 2004 - https://github.com/mattermost/mattermost-mobile/blob/master/LICENSE.txt - Letzter Aufruf am 18.01.2018

[BAS2010] Schutzziele der IT-Sicherheit - 2010 - https://link.springer.com/content/pdf/10.1007/s11623-010-0096-1.pdf - Letzter Aufruf am 18.01.2018

[BSIES2017] Bundesamt für Sicherheit in der Informationstechnik - TR-02102-1 Kryptographische Verfahren:Empfehlungen und Schlüssellängen Teil1 - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile - Letzter Aufruf am 18.01.2018

[BSIKV2017] Bundesamt für Sicherheit in der Informationstechnik - TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil2 - Verwendung von Transport Layer Security (TLS) - Letzter Aufruf am 18.01.2018 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile

[CIR2017] Circuit Support und Dokumentation - 2017 - https://www.circuit.com/support - Letzter Aufruf am 18.01.2018

[ECK2013] Claudia Eckert - IT - Sicherheit - 2013 - 8.Auflage - De Gruyter Oldenbourg Verlag

[FMA2017] Figuring out multifactor authentication - 7.August 2017 - https://fcw.com/Articles/2017/08/07/multi-factor-authentication-for-agencies.aspx?m=1&Page=1 - Letzter Aufruf am 18.01.2018

[ICQ2016] 20 Jahre ICQ Die Mutter aller Messenger feiert Geburstag - 16.November 2016 - https://www.mobilegeeks.de/artikel/20-jahre-icq-die-mutter-aller-messenger-feiert-geburtstag/ - Letzter Aufruf am 18.01.2018

[INT2017] Schutzziele der Informationssicherheit - 10.03.2017 - http://www.kryptowissen.de/schutzziele.php#integritaet - Letzter Aufruf am 18.01.2018

[ITA2017] System and Organization (SSOC") for Service Organizations: Trust Service Principles Report Relevant to Security, Availability, and Confidentiality Related to the Team Communitcation Platform Reffered to as Slack - For the period 02.01.2017 to 09.30.2017 - https://a.slack-edge.com/f9c4a/marketing/downloads/security/Slack_SOC_3_Report.pdf - Letzter Aufruf am 18.01.2018

[KON2015] IT-Verantwortliche in Deutschland sind zu konservativ - 16.März 2015 - https://www.springerprofessional.de/it-strategie/industrie-4-0/it-verantwortliche-in-deutschland-sind-zu-konservativ/6607138 - Letzter Aufruf am 18.01.2018

[KRY2016] Klaus Schmeh - Kryptografie: Verfahren, Protokolle, Infrastrukturen - 2016 - 6.Auflage - dpunkt.verlag GmbH

[KUH2004] Jörg Kuehnapfel - Nutzwertanalysen in Marketing und Vertrieb - 2014 - 1.Auflage - Springer Gabler Verlag - http://www.springer.com/de/book/9783658055080#aboutAuthors - Letzter Aufruf am 18.01.2018

[LET2017] Let's Chat Wiki - 2017 - https://github.com/sdelements/lets-chat/wiki/Configuration - Letzter Aufruf am 18.01.2018

[MAU2017] Mattermost Authentification Methods - 2017 - https://docs.mattermost.com/overview/auth.html#basic-authentication - Letzter Aufruf am 18.01.2018

[MIT2017] MIT-Lizenz - Letzte Änderung 29.12.2017 - https://de.wikipedia.org/wiki/MIT-Lizenz - Letzter Aufruf am 18.01.2018

[MOS2010] David Molnar Stuart Schechter - 2010 - Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.2908&rep=rep1&type=pdf - Letzter Aufruf am 18.01.2018

[OSL2017] Open Source Licenses by Category - 2017 - https://opensource.org/licenses/category - Letzter Aufruf am 18.01.2018

[PFS2014] Perfect Forward Secrecy - An Introduction - 10.Mai 2014 - https://scotthelme.co.uk/perfect-forward-secrecy/ - Letzter Aufruf am 18.01.2018

[POO2014] US-Cert - 2014 - Alert (TA14-290A) SSL 3.0 Protocol Vulnerability and POODLE Attack - https://www.us-cert.gov/ncas/alerts/TA14-290A - Letzter Aufruf am 18.01.2018

[RFC7465] Internet Engineering Task Force (IETF) - Februar 2015 - Prohibiting RC4 Cipher Suites - https://tools.ietf.org/html/rfc7465 - Letzter Aufruf am 18.01.2018

[ROC2017] Rocket.Chat Dokumentation - 2017 - https://docs.rocket.chat/ - Letzter Aufruf am 18.01.2018

[SAS2013] Pratik Guha Sarkar Shawn Fitzgerald - 2013 - Attacks on SSL A comprehensive study of Beast, Crime, Time, Breach, Lucky 13 & RC4 Biases - https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/ssl_attacks_survey.pdf - Letzter Aufruf am 18.01.2018

[SLA2017] Slack Alternativen: Diese Team-Messenger sind einen Blick wert - 26.10.2017 - http://t3n.de/news/slack-alternativen-584284/ - Letzter Aufruf am 18.01.2018

[STA2017] Statistiken zu Instant Messaging - 2017 - https://de.statista.com/themen/1973/instant-messenger/ - Letzter Aufruf am 18.01.2018

[TTS2016] The Top 11 Slack Alternatives - 24.10.2016 - https://blog.capterra.com/the-top-13-slack-alternatives/ - Letzter Aufruf am 18.01.2018

[ZAN1976] Christof Zangemeister - Nutzwertanalyse in der Systemtechnik - Eine Methodik zur multidimensionalen Bewertung und Auswahl von Projektalternativen - 1976 - Zangemeister und Partner Verlag

[ZAU2017] Zulip Authentification Methods - 2017 - https://zulip.readthedocs.io/en/latest/production/authentication-methods.html - Letzter Aufruf am 18.01.2018

Tabellenverzeichnis

Abbildungsverzeichnis

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

Hamburg, 22. Januar 2018 Michael Bulinski