



Bachelorarbeit HS 18/19

Chatbot Charli

Version 1.0

Autoren Giuliano De Gani
Denis Hodzic

E-Mail gdegani@hsr.ch
dhodzic@hsr.ch

Betreuer Ivan Bütler
Experte Mark Cieliebak
Gegenleser Markus Stolze
Studiengang Informatik

Erstellt am: 18.11.2018
Letzte Änderung: 21.11.2018



1. VORWORT

Wir bedanken uns herzlich bei Ivan Bütler, unserem Betreuer, für seine engagierte und fordernde Betreuung und Unterstützung.

Besonderer Dank geht auch an Cyrill Bannwart, der unermüdlich Hilfestellung bei Deployment Angelegenheiten geboten hat.



2. ABSTRACT

2.1 EINLEITUNG

In dieser Bachelorarbeit wurde ein Chatbot für Compass Security entwickelt. Dazu wurde das Bot Framework "Dialogflow" von Google verwendet, um den Neukunden online und digital zu beraten und in der Wahl der Compass Dienstleistung zu unterstützen.

2.2 ERGEBNIS

Als Ergebnis steht ein funktionierender Chatbot bereit, der die Grundanforderungen der Aufgabenstellung beherrscht. Der Chatbot reagiert auf Texteingaben des Benutzers, indem er seine Aussagen aufnimmt, mittels Texterkennungsalgorithmen verarbeitet und damit den Neukunden berät und ein Beratungsgespräch führt.

Die Umsetzung gliedert sich dabei in einen Frontend Teil, der die Inputs des Neukunden entgegennimmt und ein Backend, welches diese verarbeitet und Gesprächszustände abspeichern kann. Zusätzlich kann im Backend auf Datenbanken zugegriffen oder eigene Businesslogik ausgeführt werden. Der Chatbot bietet die Möglichkeit, mit zusätzlichen Gesprächsdaten weiter trainiert zu werden, um die Qualität des Gesprächs zu verbessern.

2.3 FAZIT

Für die Umsetzung eines Chatbots, der mehr können soll als einen gewöhnlichen Bestellablauf zu durchlaufen, ist die Technologie ungeeignet, weil in einem offenen Gespräch die Anzahl möglicher Gesprächspfade kombinatorisch explodiert. Eine Gesprächsmodellierung mittels klassischem Entscheidungsbaum oder Zustandsautomat ist deswegen keine Lösung.

Nur wenn das Gespräch strikt geführt wird, indem vorgefertigte Antwortmöglichkeiten angeboten werden, kann ein befriedigendes Kundenerlebnis ermöglicht werden.



3. MANAGEMENT SUMMARY

3.1 AUSGANGSLAGE

Im Zeitalter der Digitalisierung drängen immer mehr KMUs mit neuen Lösungen und Dienstleistungen in den digitalen Raum. Auch der Kundendienst passt sich den neuen Ansprüchen der Kunden an und entwickelt sich weiter. So werden zunehmend künstliche Intelligenzen in Form von Chatbots im Kundendienst eingesetzt, um die Servicezeit auszuweiten und Unternehmensressourcen einzusparen.

Die vorliegende Thesis befasst sich mit der Realisierung eines Chatbots. Grundlagen der Aufgabenstellung liefert der Industriepartner, die Compass Security AG, ein Anbieter von Dienstleistungen im Rahmen der Cyber Security.

Es geht darum, einen Chatbot zu realisieren, der die erste Kontaktaufnahme mit potenziellen Neukunden übernimmt und ein Beratungsgespräch führt.

3.2 VORGEHEN UND TECHNOLOGIE

Für die Entwicklung des Chatbots wurden zunächst Grundlagen im Bereich der Machine Learning Algorithmen erarbeitet und eine Evaluation verfügbarer Bot Frameworks durchgeführt. Anschliessend wurde ein Prototyp realisiert, wo alle Komponenten und deren Zusammenspiel zum Einsatz kommen. Im Verlaufe der Umsetzungsphase wurden mit Hilfe von Trainingssessions und Usability Tests Gesprächspfade und Textantworten optimiert, um die Nutzererfahrung zu verbessern.

Als Technologie Stack wurde Dialogflow für die Textverarbeitung und Gesprächsmodellierung eingesetzt. Zusätzlich wurde ein .NET Backend für das Verwalten und Halten von Informationen realisiert.

3.3 ERGEBNIS

Das Ergebnis der Thesis ist ein lauffähiger Chatbot.

Er ist in der Lage, Texteingaben des Benutzers entgegen zu nehmen und die Absicht dahinter zu verstehen. Der Chatbot wurde im Hinblick auf einfache Wart- und Erweiterbarkeit realisiert. Eine eingebaute Trainingsfunktion ermöglicht es dem Betreiber des Chatbots, neue Texteingaben zu erkennen und einzutrainieren. Mit einer Kommunikation zum Chatbot Backend kann der Chatbot Informationen speichern und verarbeiten.

Die Realisierung des Chatbots hat gezeigt, dass die aktuell verfügbare Technologie noch nicht ausgereift ist, um ein komplexes Beratungsgespräch vollständig abzubilden, weil viele Aspekte der menschlichen Kommunikation noch nicht modelliert werden können oder die Anzahl Möglichkeiten zu gross sind. Die Verwendung eines Chatbots eignet sich deshalb vor allem für interaktive FAQ Anwendungen oder einfache Bestellvorgänge.

3.4 AUSBLICK

Mit der Umsetzung eines eigenen User Interfaces können in Zukunft weitere Funktionen angeboten werden wie zum Beispiel Auswahlboxen, Bild- oder Videoantworten. Auch die nahtlose Übernahme des Gesprächs durch eine echte Person könnte damit realisiert werden. Mit Hilfe von Client Korrelationsservices können in Zukunft auch bestehende Kunden von Neukunden automatisch unterschieden werden, um so ein besseres Benutzererlebnis und eine bessere Beratung anbieten zu können.



INHALTSVERZEICHNIS

- 1. VORWORT 2**
- 2. ABSTRACT..... 3**
- 2.1 EINLEITUNG 3
- 2.2 ERGEBNIS 3
- 2.3 FAZIT..... 3
- 3. MANAGEMENT SUMMARY 4**
- 3.1 AUSGANGSLAGE 4
- 3.2 VORGEHEN UND TECHNOLOGIE 4
- 3.3 ERGEBNIS 4
- 3.4 AUSBLICK 4
- 4. AUFGABENSTELLUNG 11**
- 4.1 AUSGANGSLAGE 11
- 4.2 BUSINESS IDEE..... 11
- 4.3 BESCHREIBUNG DER AUFGABE 11
- 4.4 ZIELE 12
- 4.5 ZIELGRUPPE..... 13
- 4.6 LIEFEROBJEKTE..... 14
- 5. PROJEKTPLAN 15**
- 5.1 PROJEKT ÜBERSICHT 15
- 5.1.1 ZWECK UND ZIEL..... 15
- 5.1.2 LIEFEROBJEKTE 15
- 5.1.3 ANNAHMEN UND EINSCHRÄNKUNGEN 15
- 5.2 PROJEKTORGANISATION 15
- 5.2.1 PERSONELLE ORGANISATION..... 15
- 5.2.2 BETEILIGTE PERSONEN 15
- 5.2.3 ROLLEN..... 16
- 5.3 MANAGEMENT ABLÄUFE 16
- 5.3.1 KOSTENVORANSCHLAG 16
- 5.3.2 ZEITLICHE PLANUNG 17
- 5.3.3 BESPRECHUNGEN..... 19
- 5.4 RISIKOMANAGEMENT..... 20
- 5.4.1 RISIKEN 20
- 5.4.2 VERFAHREN 20
- 5.5 ARBEITSPAKETE 20
- 5.6 ENTWICKLUNGSUMGEBUNG..... 21
- 5.6.1 ÜBERBLICK 21
- 5.6.2 ÜBERSICHT DER TOOLS 22
- 5.6.3 RÄUMLICHKEITEN 22
- 5.6.4 COMPUTER, SERVER UND GADGETS 22



5.7 QUALITÄTSMASSNAHMEN	23
5.7.1 DOKUMENTATION	24
5.7.2 PROJEKTMANAGEMENT	24
5.7.3 ENTWICKLUNG	24
5.7.4 CODE REVIEWS	24
5.7.5 TESTEN	24
6. EVALUATION	26
6.1 GRUNDLAGEN	26
6.2 MACHINE LEARNING VON DIALOGFLOW	26
6.2.1 MATCH-MODUS	26
6.2.2 ML THRESHOLD FÜR INTENTKLASSIFIZIERUNG	26
6.2.3 AUTOMATISCHE RECHTSCHREIBKORREKTUREN	26
6.2.4 WARNUNGEN UND BEST-PRACTICES-VERFAHREN	27
6.3 EVALUATIONSKRITERIEN BOT FRAMEWORKS DIALOGFLOW	27
6.3.1 EINLEITUNG	27
6.3.2 KRITERIENKATALOG	27
6.4 AUSWAHL BOT FRAMEWORKS	28
6.5 EINFÜHRUNG BOT BUILDER FRAMEWORK	29
6.6 BEURTEILUNG BOT BUILDER FRAMEWORK	29
6.6.1 DOKUMENTATION UND SUPPORT	29
6.6.2 WERKZEUGE	30
6.6.3 SCHNITTSTELLEN	30
6.6.4 SKALIERBARKEIT	30
6.6.5 COGNITIVE CAPACITIES	30
6.6.6 FLEXIBILITÄT, MODELLIERUNG GESPRÄCHSABLAUF	30
6.6.7 INBETRIEBNAHME UND DEPLOYMENT	31
6.6.8 MEHRSPRACHIGKEIT	31
6.6.9 KOSTEN	31
6.7 AUSWERTUNG BOT BUILDER FRAMEWORK	33
6.7.1 BEWERTUNGSMATRIX	33
6.7.2 FAZIT	33
6.8 EINFÜHRUNG DIALOGFLOW	34
6.9 BEURTEILUNG DIALOGFLOW	34
6.9.1 DOKUMENTATION UND SUPPORT	34
6.9.2 WERKZEUGE	34
6.9.3 SCHNITTSTELLEN	35
6.9.4 SKALIERBARKEIT	36
6.9.5 COGNITIVE CAPACITIES	36
6.9.6 FLEXIBILITÄT, MODELLIERUNG GESPRÄCHSABLAUF	36
6.9.7 INBETRIEBNAHME UND DEPLOYMENT	37
6.9.8 MEHRSPRACHIGKEIT	37
6.9.9 KOSTEN	38
6.10 AUSWERTUNG DIALOGFLOW	38
6.10.1 BEWERTUNGSMATRIX	38
6.10.2 FAZIT	39
6.11 GESAMTERGEBNIS	39
6.11.1 ERGEBNISÜBERBLICK	39
6.11.2 ERGEBNIS FAZIT	40
7. ANFORDERUNGSSPEZIFIKATION	41



7.1 EINLEITUNG 41

7.1.1 ANFORDERUNGSERMITTLUNG 41

7.1.2 ANFORDERUNGSANALYSE UND BESCHREIBUNG 41

7.1.3 ANFORDERUNGSREVISION 42

7.2 USE CASES 43

7.2.1 USE CASE DIAGRAM 43

7.2.2 USE CASE BESCHREIBUNGEN 44

7.2.3 USE CASES FÜR KUNDEN 45

7.2.4 USE CASES FÜR COMPASS SECURITY MITARBEITER 46

7.3 NICHT FUNKTIONALE ANFORDERUNGEN (NFR) 47

7.3.1 EINLEITUNG 47

7.3.2 BEGRIFFE 47

7.3.3 NICHT FUNKTIONALE ANFORDERUNGEN 49

7.3.4 VERHALTENSGRUNDSÄTZE 50

7.3.5 TESTEN DER VERHALTENSGRUNDSÄTZE 50

8. SOFTWARE DESIGN 54

8.1 EINLEITUNG 54

8.2 ARCHITEKTUR 54

8.2.1 ARCHITEKTUR VARIANTEN 54

8.2.2 ÜBERBLICK ARCHITEKTUR VARIANTE 1 54

8.2.3 ÜBERBLICK ARCHITEKTUR VARIANTE 2 55

8.2.4 VARIANTENVERGLEICH 55

8.2.5 ARCHITEKTUR ENTWURFSMUSTER 56

8.3 DEPLOYMENT 58

8.3.1 DEPLOYMENT ABSICHT 58

8.4 DOMAINANALYSE 59

8.5 KONVERSATIONSABLAUF 59

8.5.1 SEQUENZEN 59

8.6 GESPRÄCHSMODELLIERUNG 63

8.6.1 GESPRÄCHSMODELL KONZEPT 63

8.6.2 BEGRÜSSUNG 63

8.6.3 BEDÜRFNISSE KLÄREN 63

8.6.4 BERATUNGSGESPRÄCH 64

8.6.5 AUFKLÄRUNG PENETRATION TEST 64

8.6.6 DIENSTLEISTUNGEN 64

8.6.7 EVENTS 64

8.6.8 COMPASS SECURITY KENNENLERNEN 64

8.6.9 ABSCHLUSS MIT / OHNE KONTAKTDATEN 64

8.6.10 KONZEPTE ZUR MODELLIERUNG IN DIALOGFLOW 65

8.6.11 INTENTS 65

8.6.12 ENTITIES 66

8.6.13 CONTEXTS 66

8.6.14 GESPRÄCHSVERZWEIGUNGEN 66

8.6.15 FULFILLMENT 67

9. REALISIERUNG 68

9.1 ÜBERSICHT 68

9.2 DIALOGFLOW GESPRÄCHSMODELLIERUNG ÜBERSICHT 68



9.3 DIALOGFLOW CHARLI INTENTS	68
9.3.1 COMPANY.INFOs	68
9.3.2 GLOBAL.CONSULTING.....	68
9.3.3 GLOBAL.CONTACT.PERSON	70
9.3.4 GLOBAL.DFIR	70
9.3.5 GLOBAL.DISCOVER	71
9.3.6 GLOBAL.EVENTS	71
9.3.7 GLOBAL.KILLER.QUESTIONS.....	72
9.3.8 GLOBAL.NEEDS.....	72
9.3.9 PT	72
9.3.10 GLOBAL.PT.ENTLIGHTENMENT	72
9.3.11 GLOBAL.SECURITY.REVIEW	72
9.3.12 GLOBAL.SECURITY.TRAINING.....	73
9.3.13 GLOBAL.SERVICE.....	73
9.3.14 GLOBAL.WELCOME	73
9.3.15 FALLBACKS.....	73
9.3.16 DEFAULT FALLBACK.....	73
9.3.17 FOLLOW-UP FALLBACK.....	73
9.4 DIALOGFLOW CHARLI ENTITIES.....	74
9.5 BACKEND	75
9.5.1 API	76
9.5.2 SERVICE	79
9.5.3 DATA.....	79
9.5.4 DEPLOYMENT.....	80
9.5.5 BACKEND HIBERNATE	80
9.5.6 RICH RESPONSES WEB UI LIMITATIONEN.....	80
9.5.7 CONTEXT WERDEN NICHT RESETEd	80
9.5.8 @LAST-NAME ENTITY.....	81
9.5.9 WEBHOOK CONTROLLER MIT SWAGGER INKOMPATIEL	81
9.5.10 SLOT FILLING ANWENDUNG.....	81
9.5.11 FULFILLMENT EINSATZ	81
<u>10. TESTING.....</u>	<u>82</u>
10.1 EINLEITUNG	82
10.2 VORGEHEN	82
10.3 TEST CASES	82
10.4 BEWERTUNGSRASTER CHARAKTER UND VERHALTEN.....	84
10.5 AUSWERTUNG	85
<u>11. ERGEBNISSE.....</u>	<u>86</u>
11.1 ZUSAMMENFASSUNG	86
11.2 RESULTATE	86
11.2.1 FUNKTIONALE ANFORDERUNGEN.....	86
11.2.2 NICHT-FUNKTIONALE ANFORDERUNGEN.....	88
11.3 SCHLUSSFOLGERUNGEN	90
<u>12. WEITERENTWICKLUNG</u>	<u>91</u>
12.1 WEITERENTWICKLUNGEN	91



12.2 ARCHITEKTURWECHSEL AUF VARIANTE 2	91
12.3 USERINTERFACE	91
12.4 TRAININGSDATEN AGGREGATION	91
12.5 BERATUNG ÜBER DAS BACKEND.....	91
12.6 CREDENTIALMANAGEMENT	91
12.7 DIENSTLEISTUNGSANGEBOTE ERWEITERN.....	91
12.8 TESTABDECKUNG.....	91
12.9 AUSBLICK	92
<u>13. PROJEKTMONITORING.....</u>	94
13.1 EINLEITUNG	94
13.2 AUFWAND PRO WOCHE	94
13.3 GESAMTAUFWAND.....	95
13.4 MEILENSTEINE SOLL/IST VERGLEICH	95
13.5 CODESTATISTIK	96
13.6 DIALOGFLOW ANALYTICS	97
13.7 SESSION FLOW ÜBERSICHT	98
<u>14. VERZEICHNISSE</u>	100
14.1 GLOSSAR	100
14.2 TABELLENVERZEICHNIS	103
14.3 ABBILDUNGSVERZEICHNIS	105
<u>15. ERKLÄRUNG ZUR URHEBERSCHAFT.....</u>	107
<u>16. ANHANG.....</u>	108
<u>A. DIALOGFLOW GESPRÄCHSMODELLIERUNG</u>	109
<u>B. ZUGANGSDATEN</u>	110
<u>C. EIGENSTÄNDIGKEITS-ERKLÄRUNG</u>	112
<u>D. DIALOGFLOW BENUTZERANLEITUNG.....</u>	113
<u>1. EINLEITUNG</u>	113
1.1 ZWECK.....	113
<u>2. DIALOGFLOW EINFÜHRUNG</u>	114
2.1 VORAUSSETZUNGEN	114
2.2 LOGIN / REGISTRIERUNG.....	114
2.3 AGENT	115
2.4 EINSTELLUNGEN	116
2.5 INTENTS	117



2.5.1 CREATE INTENT	117
2.5.2 FOLLOW-UP INTENT	121
2.5.3 CONTEXT VERWENDUNG	123
2.5.4 DEFAULT FALLBACK	125
2.6 ENTITIES.....	126
2.6.1 SYSTEM ENTITIES	126
2.6.2 EIGENE ENTITIES ERSTELLEN	127
2.6.3 VERWENDUNG EINES ENTITIV	129
2.7 KNOWLEDGE BASES	130
2.8 FULFILLMENT	130
2.9 INTEGRATIONS.....	131
2.10 ANLEITUNG INTEGRATION	132
2.11 TRAINING	132
2.12 HISTORY.....	133
2.13 ANALYTICS.....	134
<u>3. ERWEITERUNGEN</u>	<u>136</u>
3.1 NEUE DIENSTLEISTUNG HINZUFÜGEN	136
3.1.1 KONZEPT	136
3.1.2 DIENSTLEISTUNGSINTENT ERSTELLEN	136
3.1.3 DIENSTLEISTUNG ENLIGHTENMENT ERSTELLEN	137
3.1.4 BERATUNG ERWEITERN	137
3.1.5 CONTEXTS SETZEN.....	137
3.1.6 ANTWORTEN ANPASSEN.....	137
<u>E. SYSTEM TESTS.....</u>	<u>138</u>
<u>F. USABILITY TESTS</u>	<u>147</u>
<u>G. PERSÖNLICHER BERICHT GIULIANO DE GANI</u>	<u>165</u>
<u>H. PERSÖNLICHER BERICHT DENIS HODZIC.....</u>	<u>167</u>
<u>I. CHARLI API DOCUMENTATION.....</u>	<u>169</u>
<u>J. RISIKOMANAGEMENT</u>	<u>170</u>



4. AUFGABENSTELLUNG

4.1 AUSGANGSLAGE

Im Zeitalter der Digitalisierung drängen immer mehr KMUs mit neuen Lösungen und Dienstleistungen in den digitalen Raum. Für die Betreiber ist es von strategischer Bedeutung, dass sie die Verwundbarkeiten und technischen Sicherheitsaspekte ihrer Lösungen kennen.

Die Compass Security AG¹ bietet in diesem Rahmen Security Reviews an. Sie erlauben es, eine Gesamtaussage über diese Verwundbarkeiten zu machen und dienen als Entscheidungsgrundlage für die Freigabe allfälliger Dienstleistungen.

Sicherheitsüberprüfungen werden in engem Kontakt mit dem Kunden durchgeführt und auf seine individuellen Bedürfnisse angepasst. Dabei findet in einer ersten Phase ein Offertengespräch statt, welches das Scoping, also das Festlegen der Art und des Umfangs des Security Reviews, festlegt.

4.2 BUSINESS IDEE

Im Rahmen der Bachelorarbeit von Denis Hodzic und Giuliano De Gani geht es darum, einen Chatbot Prototypen zu realisieren, welcher den Erstkontakt zu potenziellen Kunden herstellt, diese durch die erste Phase dieses Offertengesprächs führt, Informationen zum Kunden sammelt und schliesslich die gesammelten Informationen für einen menschlichen Mitarbeiter der Compass Security AG zur Übergabe bereitstellt.

Diese erste Kontaktaufnahme und Vorsondierung mit dem Kunden, welche üblicherweise telefonisch oder persönlich durchgeführt wird und bis zu 30 Minuten dauert, wird in Zukunft teilautomatisiert ablaufen. Die Beratung des Kunden wird damit effizienter und ökonomischer.

4.3 BESCHREIBUNG DER AUFGABE

Es wird ein interaktiver Chatbot auf der Webseite der Compass Security AG implementiert, der den ersten Kontakt zum Kunden herstellt.

¹ Siehe <https://www.compass-security.com/services/security-reviews/>



4.4 ZIELE

Die Ziele, mit Prioritäten von 1 bis 3 (von hoch bis niedrig), beschreiben die einzelnen Aufgaben, die es zu lösen gilt:

ZIEL	BESCHREIBUNG	PRIORITÄT
Evaluation Bot Frameworks	Zu Beginn des Projektes soll aus mindestens zwei Bot Frameworks dasjenige ausgewählt werden, welches die Qualität der Konversation am besten erfüllt. Die Evaluationskriterien sind im Kapitel 6.3.2 einsehbar.	1
Konversation	<p>Jede Konversation muss ein Gesprächsanfang und ein Gesprächsende haben. Abbrüche seitens des Kunden (z.B. Browser schliessen, Fenster wegklicken o. Ä.) müssen erkannt werden.</p> <p>Abgeschlossene Konversationen sollen nicht wieder geöffnet werden, stattdessen muss eine neue Konversation mittels Gesprächsanfang gestartet werden.</p>	1
Qualität der Konversation / Verständnisgrad des Chatbots	<p>Der Chatbot muss die Absichten des Gesprächspartners hinreichend genau erkennen können, damit ein natürlicher Gesprächsverlauf stattfinden kann. Das bedeutet, der Verständnisgrad, also die Zuordnung eines Textes zu einer Absicht soll im Durchschnitt einer Konversation 75% nicht unterschreiten.</p> <p>Es muss möglich sein, den Verständnisgrad hinsichtlich der Erkennung der Absicht dynamisch zu verbessern. Dies soll mit dem Trainieren der Natural Language Understanding Komponenten unter Aufsicht und mit Trainingsdaten geschehen.</p> <p>Die Konversation muss dynamisch angepasst werden können, d.h. es müssen Mechanismen eingerichtet sein, so dass die Struktur und der Ablauf eines Gesprächs angepasst werden können.</p>	1
UI / Chatbot Clients	Textbasiertes Userinterface (UTF8 Zeichensatz) für die Mensch- Maschine Konversation. Der Client muss in einem HTML5 fähigen Browser umgesetzt sein. Der Client wird von der Compass Security AG gehostet.	2
Zugriff auf Konversationen	Alle laufenden und gespeicherten Konversationen müssen für den Compass Security Mitarbeiter ersichtlich sein.	1



ZIEL	BESCHREIBUNG	PRIORITÄT
Übergabe des Gesprächs	<p>Der Compass Security Mitarbeiter soll in der Lage sein, jederzeit in die Konversation einzusteigen und das Gespräch zu übernehmen.</p> <p>Der Compass Security Mitarbeiter muss notifiziert werden können, wenn eine Gesprächsübergabe stattfinden muss. Dies beinhaltet auch eine gewünschte Kontaktaufnahme nach einem Gesprächsende.</p>	2
Kundenidentifikation	<p>Kunden sollen anhand ihrer Kundenmetadaten wiedererkannt werden können.</p> <p>Als Kundenmetadaten gelten z.B. ClientIP oder UserAgent, sowie sämtliche Parameter, welche mit Hilfe von Client Correlation Services (fingerprint2.js), erfasst werden.</p>	2
Sicherheit	<p>Die Kommunikation von Mensch zu Maschine muss über SSL/TLS erfolgen.</p> <p>Kunden dürfen keinen Zugang zu fremden Konversationen haben.</p>	1
Backend Web Application	<p>Das Chatbot Backend muss eine RESTful http API anbieten, über welche die Kommunikation zu den Chatbot Clients stattfindet.</p> <p>Allfällige Verwaltungsaufgaben für die Organisation oder Visualisierung der Kundendaten müssen ebenfalls über eine RESTful http API angeboten werden.</p> <p>Chatverläufe, sowie Metadaten der Kunden, müssen persistiert werden.</p>	1
Management Application	<p>Die Verwaltung der gespeicherten Konversationen (persistierte Daten der Chatbot Anwendung) müssen über eine Management Applikation abgerufen werden können.</p>	3

Tabelle 1 Produktziele für den Chatbot

4.5 ZIELGRUPPE

Zielgruppe sind potenzielle Neukunden für cyber-sicherheitsbezogene Dienstleistungen. Dazu gehören auch Personen, die im Auftrag Ihres Unternehmens Security-Reviews oder Trainings durchführen lassen möchten.



4.6 LIEFEROBJEKTE

Im Rahmen dieser Projektarbeit werden folgende Lieferobjekte, in lösungsneutraler Form, definiert:

DELIVERABLE	BESCHREIBUNG	FORM
Aufgabenstellung	Enthält die Aufgabenstellung für die Bachelorarbeit	Textdokument
Projektplan	Beschreibt die Organisation des Projekts, den zeitlichen Ablauf, das Risiken- und Qualitätsmanagement	Textdokument
Sitzungsprotokolle	Protokolle der Sitzungen mit dem Betreuer. Enthält die Beschlüsse, wichtige Entscheidungen und Termine	Text
Abstract	Kurze Beschreibung der Projektarbeit inkl. Ergebnisse	Text, 1 A4 Seite
Management Summary	Beschreibung des Produkts, dessen Möglichkeiten und Mehrwertgenerierung	Text, 1 A4 Seite
Glossar	Erläuterung von Fachbegriffen und Fremdwörtern oder Anglizismen	Textdokument
Software Anforderungsspezifikation	Enthält die Anforderungsdokumente für die zu realisierende Softwarekomponenten	Textdokument
Technischer Bericht	Beschreibt die Umsetzung und die verwendeten Technologien	Bericht
Persönlicher Bericht	Persönliche Schilderung der Entwickler zum Projekt. Inhaltlich frei	Bericht
Evaluation AI/ML	Ein reduzierter Evaluationsbericht über die verwendete AI Engine / Bot Framework	Bericht
PoC / Prototyp	Lauffähiger Prototyp auf Docker Basis für die Präsentation an Dritte	Docker Compose Software, Code
UI	Frontend für die Konversation mit dem Chatbot	Code
Backend Web Application	Chatbot RESTful API für die Kommunikation von und zu den Chatbot Clients sowie Drittsystemen.	Code

Tabelle 2 Lieferobjekte der Bachelorarbeit



5. PROJEKTPLAN

5.1 PROJEKT ÜBERSICHT

5.1.1 ZWECK UND ZIEL

Im Rahmen der Projektarbeit wird ein Prototyp eines Chatbots realisiert, welcher über ein textbasiertes UI in Form eines Chats den Kontakt zu potenziellen Kunden herstellt, diese durch die erste Phase eines Offertengesprächs für Dienstleistungsangebote der Compass Security führt und schliesslich die gesammelten Informationen für einen menschlichen Mitarbeiter zur Übergabe bereitstellt.

5.1.2 LIEFEROBJEKTE

Die Lieferobjekte sind im Kapitel 4.6 dokumentiert.

5.1.3 ANNAHMEN UND EINSCHRÄNKUNGEN

1. Die Weiterführung von Dienstleistungen Dritter, welche für die Realisation verwendet werden, kann nach Ablauf des vorgegebenen Projektzeitraums nicht gewährleistet werden.
2. Es gelten im Übrigen die Rahmenbedingungen der Hochschule für Technik HSR in Rapperswil SG bezüglich der Durchführung einer Bachelor-Arbeit im Bachelor Studiengang Informatik.

5.2 PROJEKTORGANISATION

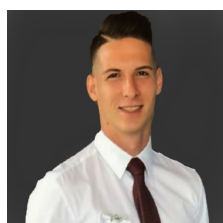
5.2.1 PERSONELLE ORGANISATION

Das Projekt wird aufgrund der Anzahl Teammitglieder flach und ohne Hierarchie organisiert. Entscheide werden im Kollektiv gefällt, weil die Entscheidungswege kurz sind. Teammitglieder haben zugewiesene Rollen mit Zuständigkeiten. Rollen können getauscht werden.

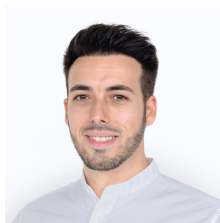
5.2.2 BETEILIGTE PERSONEN



**IVAN
BÜTLER**
ibuetler



**DENIS
HODZIC**
dhodzic



**GIULIANO
DE GANI**
gdegani



**MARKUS
STOLZE**
mstolze



**MARK
CIELIEBAK**
ciel



5.2.3 ROLLEN

ROLLE	PERSON	ZUSTÄNDIGKEIT
Betreuer	ibuetler	<ul style="list-style-type: none"> Betreut Bewertet Unterstützt Ist Ansprechpartner für Externe
Entwickler	dhodzic gdegani	<ul style="list-style-type: none"> Realisiert Dokumentiert Sichert Qualität und testet
Protokollführer	dhodzic	<ul style="list-style-type: none"> Bereitet vor und nach, führt und verteilt Sitzungsprotokolle
DevOps Projektadministrator	gdegani	<ul style="list-style-type: none"> Verwaltet und regelt den Zugang zur DevOps Projektseite
Gegenleser	mstolze	<ul style="list-style-type: none"> Kontrolliert die Durchführung und Fairness
Experte	ciel (@zhaw.ch)	<ul style="list-style-type: none"> Unterstützt bei der Bewertung Beurteilt inhaltlich Arbeit, Ergebnis und Analyse

Tabelle 3 Rollenübersicht

5.3 MANAGEMENT ABLÄUFE

5.3.1 KOSTENVORANSCHLAG

Die Realisierung des Chatbots erfolgt im Herbstsemester 2018/2019 über eine Zeitspanne von 14 Wochen. Mit einem zeitlichen Budget von 360 Mannstunden pro Entwickler ergibt sich eine Kapazität von ca. 720 Mannstunden.

BESCHREIBUNG		ZEIT
Zeitraum	HS18/19	14 Wochen
Teammitglied 1	Giuliano De Gani	360 Stunden
Teammitglied 2	Denis Hodzic	360 Stunden
Total		720 Stunden



Tabelle 4 Kapazität

5.3.2 ZEITLICHE PLANUNG

Für die Zeitverwaltung und Planung der Arbeitsschritte wird Azure DevOps ²(ehemals team services) verwendet. Das Projekt ist agil. Das agile Planungskonzept erlaubt es, besser auf unerwartete Begebenheiten reagieren zu können und mit wechselnden oder neuen Anforderungen im Verlaufe des Projekts besser umzugehen.

5.3.2.1 PHASEN / ITERATIONEN / MEILENSTEINE

Auf der folgenden Seite befindet sich die Timeline des Projektes. Alle Phasen, Iterationen und Meilensteine sind festgehalten. Tritt ein Meilenstein oder ein Review-Termin auf, sollen alle oberhalb genannten Punkte erledigt sein. Die folgende Tabelle zeigt die Aufteilung der Phasen verteilt über die 14 Kalenderwochen.

38	39	40	41	42	43	44	45	46	47	48	49	50	51
----	----	----	----	----	----	----	----	----	----	----	----	----	----

Tabelle 5 Kalenderwochen und Phasen

Nachfolgend sind die Phasen, ihre Iterationen und die groben Arbeitspakete den einzelnen Iterationen zugeordnet:

	ITERATION	DAUER	AUFTÄGE
Inception	0	17.09.2018 – 21.09.2018	<ul style="list-style-type: none"> • Kickoff • Projektmanagementtools ausgewählt und eingerichtet • IDE eingerichtet • Scope grob abgesteckt
	A	24.09.2018 – 05.10.2018	<ul style="list-style-type: none"> • Aufgabenstellung schriftlich festgehalten • Projektplan erstellt • Risikomanagement • Projektname • Bot Framework Hands-on (mind. 3) • Bot Frameworks Evaluationsbericht • Anforderungen festgelegt • User stories grob erstellt • Logo erstellt • Design für die Dokumente festlegen • Code Guidelines festlegen
	M1	04.10.2018	Meilenstein 1: Infrastruktur
Elaboration	B	08.10.2018 – 19.10.2018	<ul style="list-style-type: none"> • Evaluationen AI/ML Engine • Software Anforderungsspezifikation (Use cases, Sequenzdiagramme, NFR, Domainanalyse) • Entscheidung Technologiestack für Frontend und Backend

² <https://visualstudio.microsoft.com/de/team-services/>



	ITERATION	DAUER	AUFTÄGE
			<ul style="list-style-type: none"> • Ablauf / Chatfluss dokumentieren und verstehen in Zusammenarbeit mit Compass Security • End of Elaboration Checklist
	M2	17.10.2018	Meilenstein 2: End of Elaboration
Construction	C	22.10.2018 – 09.11.2018	<ul style="list-style-type: none"> • RESTful http web API • End zu End Verschlüsselung • Grundsätzlicher Gesprächsablauf Business Logic abbilden • Impl. / Einsatz der NLU services • Lauffähiger Architekturprototyp (Kommunikation zum Backend, Persistenz, „vertikaler Durchstich“)
	M3	07.11.2018	Meilenstein 3: Prototyp Alpha
	D	12.11.2018 – 23.11.2018	<ul style="list-style-type: none"> • Erweiterter Gesprächsablauf Business Logic abbilden (Übergabe Zeitpunkt, Feststellen, wann vorzeitige menschliche Interaktion notwendig ist) • Konzeptionierung Management Applikation • Chat-Verläufe speichern
	M4	21.11.2018	Meilenstein 4: Prototyp Beta
	E	26.11.2018 - 07.12.2018	<ul style="list-style-type: none"> • Testprotokolle • Usability Tests durchgeführt • Optionale Features • Source Code / API Dokumentation finalisieren
	M5	05.12.2018	Meilenstein 5: End of Construction
Transition	F	10.12.2018 – 21.12.2018	<ul style="list-style-type: none"> • Technischer Bericht fertigstellen • Präsentation erstellen • Abgabe Abstract • Abgabe Poster
	M6	21.12.2018	Meilenstein 6: Abgabe Bachelorarbeit

Tabelle 6 Iterationen



5.3.2.2 MEILENSTEINE

MEILENSTEIN	DATUM	BESCHREIBUNG
M1: Infrastruktur	04.10.2018	Projektplan erstellt, Infrastruktur bereit-gestellt
M2: End of Elaboration	17.10.2018	Anforderungen festgelegt, EoE Checkliste ³ erfüllt
M3: Prototyp Alpha	07.11.2018	Prototyp Alpha („vertikaler Stich“) bereitgestellt
M4: Prototyp Beta	21.11.2018	Prototyp Beta bereitgestellt
M5: End of Construction	05.12.2018	End of Construction
M6: Schlussabgabe	21.12.2018	Endprodukt als Ganzes funktioniert, Technischer Bericht fertiggestellt und abgabebereit

Tabelle 7 Meilensteine

5.3.3 BESPRECHUNGEN

Besprechungen mit dem Betreuer werden einmal wöchentlich, in der Regel mittwochs oder donnerstags durchgeführt.

Ziele der Besprechungen sind:

- STANDORTBESTIMMUNG DES PROJEKTS
- ADMINISTRATIVES KLÄREN
- AKTUELLE UND GEPLANTE ARBEITEN BESPRECHEN
- PROBLEME UND HINDERNISSE BESPRECHEN UND BESEITIGEN
- REVIEWS DURCHFÜHREN
- MEILENSTEINE BESPRECHEN

Zu jeder Sitzung wird ein Protokoll geführt, bei der die wichtigsten Punkte dokumentiert werden. Die Sitzungsprotokolle werden spätestens 48 Stunden im Anschluss dem Betreuer zugesendet und auf der Projektseite online zur Verfügung gestellt.

Zusätzlich findet mindestens einmal pro Woche eine Synchronisation unter den Entwicklern statt. Diese findet von Angesicht zu Angesicht statt, um Unklarheiten vorzubeugen und die Teambildung zu fördern. Es werden aktuelle Tätigkeiten, geplante Tätigkeiten und Probleme besprochen. Ergebnisse dieser Sitzungen werden nicht protokolliert.

³ Siehe dazu im DevOps Repository unter «/docu/eoe_checkliste.pdf »



5.4 RISIKOMANAGEMENT

5.4.1 RISIKEN

Eine Bewertung der Risiken und der Umgang damit sind im Anhang J dokumentiert.

5.4.2 VERFAHREN

Das Risikomanagement ist ein kontinuierlicher Prozess. In regelmässigen Abständen, mindestens alle zwei Wochen, wird die Lage neu beurteilt und entsprechende Anpassungen vorgenommen. Dies beinhaltet das Identifizieren von neuen Risiken, das Beurteilen von bestehenden Risiken und die Überprüfung des Massnahmenkatalogs für die Prävention sowie den Eintrittsfall.

Wird ein neues Risiko mit hohem⁴ gewichteten Schaden identifiziert, wird der Betreuer unverzüglich benachrichtigt.

5.5 ARBEITSPAKETE

Das Management der Arbeitspakete und deren Einplanung ist über die DevOps Projektseite https://dev.azure.com/dedi1199/ChatBot/_workitems/ einsehbar.

Für die Einsicht in das Projekt sind ein Microsoft Login und eine Einladung des DevOps Projektadministrators notwendig.

⁴ Gefährdung eines erfolgreichen Abschluss des Projekts. Ein Schaden gilt als hoch, wenn er mindestens 10% der Teamkapazität beträgt.

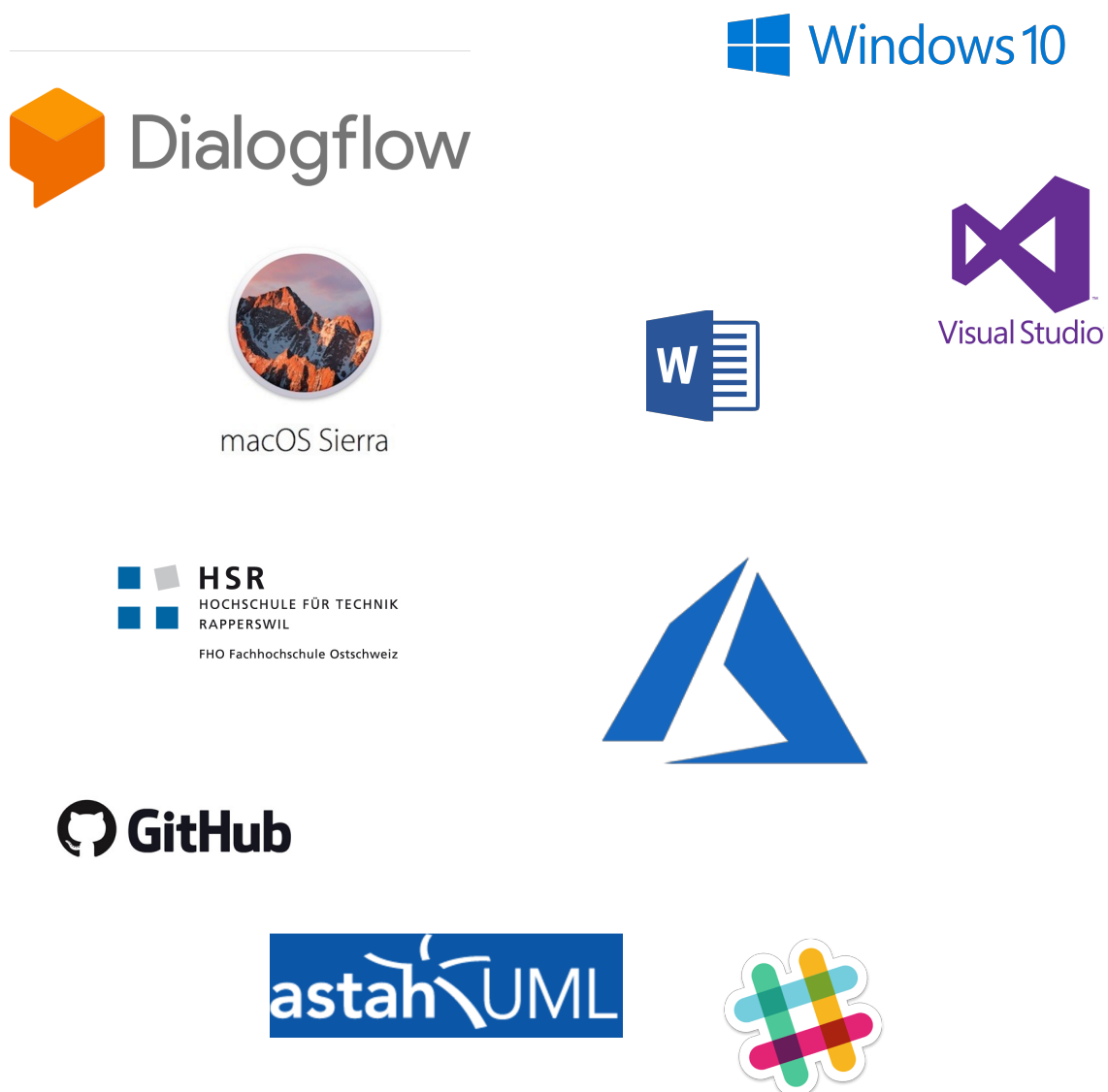


5.6 ENTWICKLUNGSUMGEBUNG

5.6.1 ÜBERBLICK

Die folgende Seite zeigt einen Überblick der wichtigsten Technologien und Organisationen, welche im Zuge dieser Projektarbeit zum Einsatz kommen.

Die wichtigsten Komponenten werden im nächsten Kapitel genauer beschrieben.





5.6.2 ÜBERSICHT DER TOOLS

BEZEICHNUNG	BESCHREIBUNG	ZUSÄTZLICHE INFORMATIONEN
Dialogflow 	Dialogflow (ehemals Api.ai, Speaktit) ist ein Google-eigener Entwickler von Human-Computer-Interaktionstechnologien, die auf natürlichsprachlichen Gesprächen basieren.	https://dialogflow.com/
Visual Studio 2017 	Eine von Microsoft angebotene Entwicklungsumgebung für verschiedene Hochsprachen	https://www.visualstudio.com/
DevOps Azure 	DevOps Azure führt Menschen, Prozesse und Technologie zusammen und automatisiert die Softwarebereitstellung, um Ihren Benutzern einen gleichbleibend hohen Mehrwert zu bieten.	https://azure.microsoft.com/de-de/solutions/devops/
AstahUML 	UML Modeling Tool	https://azure.microsoft.com/de-de/solutions/devops/
Slack 	Slack ist ein Ort, an dem dein Team einfach zusammenarbeiten kann.	https://slack.com/intl/de/

Tabelle 8 Übersicht Tools

5.6.3 RÄUMLICHKEITEN

Für die Arbeit während der Unterrichtszeiten werden, die von der HSR zur Verfügung gestellten freien Räumlichkeiten benutzt. Den Umständen entsprechend kann ein Teil der Arbeit auch Zuhause verrichtet werden.

5.6.4 COMPUTER, SERVER UND GADGETS

Jedes Teammitglied verfügt über einen Laptop und/oder einen Computer zu Hause mit dem die Arbeit verrichtet wird.

Während der Entwicklung werden für Test und Usability Zwecke die eigenen Notebooks, ein MacBook und ein Dell PC verwendet.

Für das Persistieren der Daten, wird in Absprache mit Compass Security, die entsprechende Infrastruktur bereitgestellt.



5.7 QUALITÄTSMASSNAHMEN

Es werden folgende Massnahmen zur Erreichung und Erhaltung der Qualität getroffen:

MASSNAHMEN	ZIEL	BESCHREIBUNG	ZEITRAUM
Automatisierte Tests	Bugs erkennen und beseitigen	<p>Die Continuous Integration Umgebung führt die Code Tests nach jedem Build aus. Die CI Umgebung notifiziert die Entwickler mittels Email, wenn ein Test fehlschlägt.</p> <p>Zusätzlich können die (Unit / System) Tests lokal ausgeführt werden.</p> <p>Als Test Runner kommen Microsoft Technologien zum Einsatz.</p> <p>Für das Testen der JS Komponenten behält sich das Team vor, weitere Testing Frameworks einzusetzen.</p>	Fortlaufend während der gesamten Entwicklungsphase
Code Analyse	Qualitativ hochwertigen Code sicherstellen, Komplexität minimieren	Die CI Umgebung oder die integrierten Tools in Visual Studio 2017 Professional berechnen auf Verlangen statische Codemetriken. Weiter können auch Code Testabdeckungen berechnet werden.	Kontinuierlich
Code Guidelines	Einheitlicher und gut lesbarer Code.	Wird durch Visual Studio und Projektsettings eingestellt. Wenn über das Team gesehen die Einheitlichkeit nicht mehr gewährleistet ist, kann mittels DevOps Extensions, die Einheitlichkeit in der CI Umgebung erzwungen werden.	Kontinuierlich
Team Reviews	Standortbestimmung Lösungen für aufgetretene Probleme suchen	<p>Mittels vier Augen Prinzip und im Gespräch, können Lösungen erarbeitet werden.</p> <p>Durch regelmässige (daily) Kurzmeetings, können Hindernisse früh erkannt und zusammen behoben werden.</p>	Täglich während der Entwicklungsphase oder bei Bedarf

Tabelle 9 Qualitätsmassnahmen



5.7.1 DOKUMENTATION

Die Dokumente werden während der Bearbeitung in DevOps Azure abgelegt. Dies ermöglicht allen Mitgliedern die Dokumente zeitgleich zu bearbeiten und die aktuellsten Versionen einzusehen. Nach Fertigstellung der Dokumente werden diese als PDF abgespeichert.

Um die Qualität der Dokumente hochzuhalten, werden diese vor der Abgabe einem Team-Review unterzogen. Unklarheiten werden mit dem Betreuer über Slack oder in Sitzungen besprochen.

5.7.2 PROJEKTMANAGEMENT

Für das Projektmanagement wird DevOps Azure verwendet. DevOps Azure lässt sich unabhängig vom Standort immer abrufen und ist für alle verfügbar. Der Betreuer erhält Zugang mit dem Status Reader. DevOps Azure wird auch für die Verwaltung von Arbeitspaketen und die Zeiterfassung gebraucht.

5.7.3 ENTWICKLUNG

Die CI / CD Umgebung für die Entwicklung befindet sich auf DevOps. Für die Entwicklung wird der git workflow⁵ verwendet.

5.7.4 CODE REVIEWS

Durch den Pull-Request-Flow informieren sich die Teammitglieder über die Fertigstellung verschiedener Code Abschnitte. Sobald ein Branch soweit ist wird ein Pull-Request abgesetzt. Damit ist sichergestellt, dass gemäss dem vier Augen Prinzip, Code gereviewed wurde, bevor er in den produktiven Einsatz gelangt.

5.7.4.1 CODE STYLE GUIDELINES

Es gelten die Coding Conventions⁶ von Microsoft. Die DevOps Umgebung und die einheitlichen Entwicklerumgebungen stellen sicher, dass die Coding Conventions jederzeit eingehalten sind.

5.7.5 TESTEN

5.7.5.1 UNIT TESTING

Alle implementierten Klassen und Funktionen werden fortlaufend durch automatisierte Unit Tests geprüft. Für die Business Logik Komponenten und das Backend wird eine Testabdeckung von mindestens 80% angestrebt.

5.7.5.2 INTEGRATION TESTING

Nach Fertigstellung jeder Komponente, wird diese durch die CI Umgebung und durch den Entwickler auf Integration getestet. Eine Komponente gilt erst als abgeschlossen, wenn auch die Integration-Tests erfolgreich sind.

5.7.5.3 SYSTEM TESTING

Als Grundlage für Systemtests werden Use Cases herangezogen. Systemtests werden am Ende der Construction Iterationen durchgeführt. Ergebnisse werden mittels Testprotokollen dokumentiert. Konsequenzen und Verbesserungen werden iterativ in die kommenden Iterationen eingeplant.

⁵ Siehe <https://de.atlassian.com/git/tutorials/comparing-workflows>

⁶ Siehe <https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/inside-a-program/coding-conventions>





6. EVALUATION

6.1 GRUNDLAGEN

Im folgenden Kapitel werden die Grundlagen von Machine Learning erläutert.

6.2 MACHINE LEARNING VON DIALOGFLOW⁷

Dialogflow Agenten verwenden maschinelle Lernalgorithmen, um natürliche Sprachäußerungen (NLU) zu verstehen, sie mit den Intents abzugleichen und strukturierte Daten zu extrahieren.

Ein Agent lernt sowohl von den bereitgestellten Trainingsphrasen vom Chatbot als auch von den in Dialogflow integrierten Sprachmodellen. Basierend auf diesen Daten baut es einen Algorithmus auf, um Entscheidungen darüber zu treffen, welche Intents mit einer Benutzeräußerung abgeglichen werden soll. Dialogflow aktualisiert den maschinellen Lernalgorithmus des Agenten jedes Mal, wenn Änderungen an Intents und Entitäten vorgenommen werden, ein Agent importiert, wiederhergestellt oder trainiert wird.

6.2.1 MATCH-MODUS

Match-Mode definiert die Algorithmen, die für alle Zwecke verwendet werden sollen, in denen Machine Learning aktiviert ist. Folgende Modi stehen zur Auswahl:

- Hybrid (empfohlen): Dieser Modus versucht zunächst eine regelbasierte Grammatikübereinstimmung. Wenn eine Übereinstimmung nicht hergestellt wird, wechselt sie zu ML-Matching.
- Nur ML: Dieser Modus verwendet nur ML-Matching.

6.2.2 ML THRESHOLD FÜR INTENTKLASSIFIZIERUNG

Um falsch-positive Ergebnisse herauszufiltern und dennoch eine Vielzahl von passenden Eingaben für den Agenten zu erhalten, kann der Schwellwert beim Klassifizieren der Intents für das maschinelle Lernen angepasst werden.

Intent Matches haben einen Confidencescore von 0 (völlig unsicher) bis 1 (völlig sicher). Wenn der Confidencescore kleiner als der Threshold ist, wird der Fallback Intent aufgerufen.

6.2.3 AUTOMATISCHE RECHTSCHREIBKORREKTUREN

Wenn die automatische Rechtschreibkorrektur aktiviert ist und die Benutzereingabe einen Rechtschreib- oder Grammatikfehler aufweist, wird in einen Intent gewechselt, der mit dem korrigierten Text korreliert. Die Detect Intent Response enthält die korrigierte Benutzereingabe. Wenn ein Benutzer beispielsweise "Ich will ein Apfel" eingibt, wird es so verarbeitet, als ob der Benutzer "Ich will einen Apfel" eingegeben hätte. Dies gilt auch für Übereinstimmungen, an denen sowohl System- als auch Entwickler-Entitäten beteiligt sind.

Die Rechtschreibkorrektur ist für alle von Dialogflow unterstützten Sprachen verfügbar.

⁷ Quelle: <https://dialogflow.com/docs/agents/machine-learning>



6.2.4 WARNUNGEN UND BEST-PRACTICES-VERFAHREN

- Die Rechtschreibkorrektur kann ASR-Fehler (automatische Spracherkennung) nicht korrigieren, daher wird nicht empfohlen sie für Agenten zu aktivieren, die ASR-Eingänge verwenden.
- Es ist möglich, dass korrigierte Eingaben mit der falschen Intention übereinstimmen. Sie können dies beheben, indem Sie häufig unpassende Phrasen zu Negativbeispielen hinzufügen.
- Die Rechtschreibkorrektur erhöht die Reaktionszeit des Agenten leicht.
- Die Rechtschreibkorrektur wird auf allgemeine Benutzerfragen trainiert. Wenn ein Agent mit domänenspezifischem Fachjargon definiert ist, können die Korrekturen unerwünscht sein.

6.3 EVALUATIONSKRITERIEN BOT FRAMEWORKS DIALOGFLOW

6.3.1 EINLEITUNG

Im Zentrum der Projektarbeit steht der Einsatz eines Chatbots. Um die Ziele, die in der Aufgabenstellung beschrieben sind, zu erreichen, ist es aufgrund der zeitlichen und personellen Ressourcen dieser Bachelorarbeit zwingend, dass ein bestehendes Bot Framework eingesetzt wird.

Zum Zeitpunkt der Projektarbeit im Herbst 2018 stehen zahlreiche Bot Frameworks zur Verfügung.

6.3.2 KRITERIENKATALOG

Für die Kurzevaluation werden die Kriterien mit entsprechender Gewichtung definiert:

KRITERIUM	GEWICHTUNG	BESCHREIBUNG
Dokumentation, Support	0.15	Sind die Dokumentation und Beispiele aktuell? Gibt es genügend Unterstützung online? Sind die Nutzerzahlen gross?
Werkzeuge	0.1	Wie sind die Anzahl und die Qualität der verfügbaren Werkzeuge?
Schnittstellen	0.1	Welche Schnittstellen sind unterstützt? Welche Möglichkeiten für die Integration bestehen?
Skalierbarkeit	0.05	Können die eingesetzten Services skalieren?
Cognitive Capacities	0.2	Wie gut erkennt der Bot den Intent aus einer Textphrase? Gibt es Möglichkeiten, die Genauigkeit zu verbessern? Welche weiteren Services können verwendet werden?
Flexibilität Modellierung Gesprächsablauf	0.2	Welche Mittel gibt es, um den "Flow" abzubilden? Wie komplex ist es, eine Modellierung zu machen?



KRITERIUM	GEWICHTUNG	BESCHREIBUNG
Inbetriebnahme / Deployment	0.1	Wie schwierig ist es, den Bot in Betrieb zu nehmen?
Mehrsprachigkeit	0.05	Sind Mechanismen eingerichtet, so dass der Bot mehrere Sprachen unterstützen kann?
Kosten	0.05	Was sind die Betriebskosten des Bots und dessen Services? Gibt es einmalige Kosten? Ist das Kostenmodell Pay per use?

Tabelle 10 Kriterienkatalog

6.4 AUSWAHL BOT FRAMEWORKS

Es wurde entschieden, die Anzahl der zu evaluierenden Frameworks auf zwei zu beschränken. Damit wurde das Schwergewicht auf die Umsetzung und weniger auf die Evaluationen gebildet.

Eine erste Onlinerecherche⁸ hat folgende populären Frameworks gelistet⁹:

BOT FRAMEWORK NAME	BESCHREIBUNG
IBM Watson	Chatbot builder von IBM. Bietet SDKs für node.js, Java, Unity und weitere.
Bot Builder Framework (Bot Builder SDK und LUIS)	Microsofts Bot Framework. Enthält im Wesentlichen das SDK und «cognitive services». Diese Services werden als «Azure Bot Service» zusammengefasst.
Dialogflow	Ehemals Api.ai, nun zu Google gehörend. Bietet Tools, um für den Google Assistant Applikationen zu entwickeln.
Amazon Lex	Service für die Entwicklung von Konversationsschnittstellen für Sprache und Text. Greift auf die gleichen Deep Learning Technologien zurück wie auch Amazon Alexa.
ManyChat	Bekannt dafür, sehr einfach und schnell einen Facebook Messenger Bot zu realisieren.

Tabelle 11 Überblick populäre Bot Frameworks

Für die nähere Evaluation wurden das «Bot Builder Framework» von Microsoft sowie «Dialogflow» von Google ausgewählt.

Gründe für die Auswahl:

- Rasches Erfolgserlebnis («HelloWorld») mit Dialogflow und Bot Builder Framework
- Saubere, aktuell gehaltene und verständliche Dokumentation

⁸ Googlesuche mit «popular chat bot frameworks»

⁹ Siehe auch <https://www.newgenapps.com/blog/top-5-chatbot-platforms-develop-bots-sdk-solution-tools>



- Die gesetzten Anforderungen in dieser Projektarbeit können gemäss den Dokumentationen von Bot Builder Framework und Dialogflow erfüllt werden
- ManyChat fällt wegen der Nähe zu Facebook weg
- Amazon und IBM wurden hinter Microsoft und Google priorisiert, was den persönlichen (positiven) Erfahrungswerten der Entwickler geschuldet ist

6.5 EINFÜHRUNG BOT BUILDER FRAMEWORK

Das Bot Builder V4 SDK¹⁰, in diesem Dokument fortan «Bot Builder SDK» genannt, ist Hauptbestandteil des Bot Frameworks, welches von Microsoft entwickelt wird. Grosse Teile des Sourcecodes sind auf Github verfügbar.

Die SDK's sind für zahlreiche Plattformen wie .NET / C#, Java, Python oder JS verfügbar.

Alle Services im Zusammenhang mit dem Bot Builder Framework werden unter den «Azure Bot Services¹¹» zusammengefasst.

Zum aktuellen Zeitpunkt, Oktober 2018, werden verschiedene Begriffe verwendet, wie zum Beispiel «Microsoft Bot Framework», «Azure Bot Service» oder «Bot Builder SDK». Bot Builder Framework enthält dabei das Bot Builder SDK und weitere Services, welche wiederum unter Azure gehostet werden unter dem Überbegriff «Azure Bot Service».

6.6 BEURTEILUNG BOT BUILDER FRAMEWORK

6.6.1 DOKUMENTATION UND SUPPORT

Die «Azure Bot Services» sind sehr gut dokumentiert. Es gibt zahlreiche, aktuell gehaltene Samples, mit welchen der Entwickler rasch einen Ersterfolg erzielen kann.

Die Benennung der einzelnen Services ist nicht immer einheitlich, was zur Verwirrung führen kann.

Das «Bot Builder SDK» wird aktiv weiterentwickelt. Besonders die Beispielanwendungen werden aktuell gehalten, damit der Einstieg leichtfällt:



Abbildung 1 Contributions am Bot Builder Samples Projekt

Ein Blick in die Issue Liste zeigt, dass zeitnahe auf Probleme eingegangen wird und Bugs gefixt werden.

Die Menge an Tutorials, welche aktuell gehalten und einfach zu folgen sind, ist gross. Die meisten Anwendungsfälle werden durch Tutorials bereits abgedeckt, was die «time to market» enorm verbessern kann.

¹⁰ Siehe dazu: <https://github.com/Microsoft/BotBuilder-Samples> oder <https://dev.botframework.com/>

¹¹ Siehe dazu: <https://docs.microsoft.com/en-us/azure/bot-service/bot-service-quickstart?view=azure-bot-service-4.0>



6.6.2 WERKZEUGE

Es gibt viele Tools. Es ist etwas schwierig für Einsteiger zu beurteilen, welche davon benötigt werden und welche nur «Convenience» sind. Um die Geschwindigkeit beim Entwickeln zu steigern, gibt es das Bot Framework Emulator App, welches lokal installiert werden kann. Zusätzlich gibt es viele «Cognitive Services», welche für die Konfiguration webbasierte Uls anbieten.

Die Werkzeuge sind frei verfügbar und einfach zu benutzen.

Eine Beurteilung der Güte dieser Werkzeuge kann aber erst gemacht werden, wenn diese intensiv genutzt werden. Es könnte sich herausstellen, dass einige Tools (bewusst) zu simpel gehalten sind und man bei komplexeren Anforderungen an seine Grenzen stösst.

6.6.3 SCHNITTSTELLEN

Microsoft versucht, das Gesamtpaket anzubieten. Entsprechend sind alle benötigten Services, welche vom Bot verwendet werden könnten, ebenfalls auf Azure verfügbar. Ein erster Test hat gezeigt, dass die Services gut miteinander orchestrierbar sind.

Zusätzlich sind viele Services über normale RESTful http web APIs verfügbar, was die Interoperabilität verbessert.

6.6.4 SKALIERBARKEIT

Microsoft bietet zwei Möglichkeiten für das Deployment der Bots an:

- Gehostet auf Azure
- On Premise

Werden Bots und deren verwendete Services in der Cloud bei Azure gehostet, sind diese (gegen entsprechende Kosten) beliebig skalierbar.

6.6.5 COGNITIVE CAPACITIES

Zu den wichtigsten «Cognitive Services» gehören LUIS¹² und QnAMaker¹³. Diese sind für Testzwecke kostenlos verfügbar und lassen sich problemlos als Services über das Bot Builder SDK anbinden.

Unter der URL <https://azure.microsoft.com/en-us/services/cognitive-services/> sind weitere Services wie das «Vision API» verfügbar, die für die Umsetzung des Chatbots weniger relevant sind.

6.6.6 FLEXIBILITÄT, MODELLIERUNG GESPRÄCHSABLAUF

Das Kernkonzept zur Modellierung eines Gesprächsablaufs in Bot Builder SDK sind Dialoge. Dialoge verarbeiten eingehende Aktivitäten (welche die Nachrichten enthalten) und erzeugen Antworten. Das SDK enthält vordefinierte Dialogtypen¹⁴ wie «prompts», «waterfall» und «component dialogs». Dialoge können neue Dialoge starten. Dies wird «Conversation Branching» genannt. Die Abfolge dieser Dialoge bestimmt den Gesprächsfluss. Die Business Logik zur Bestimmung des Dialogs kann mittels «Cognitive Services» wie QnAMaker oder LUIS realisiert werden.

Der Gesprächsablauf muss grundsätzlich per Code abgebildet werden. Es existieren jedoch Hilfswerkzeuge, wie zum Beispiel «Chatdown¹⁵», welche aus einfachem Markdown «Chat» ein Transkript erzeugen können.

¹² Language Understanding Intelligent Service: <https://www.luis.ai/>

¹³ Siehe dazu: <https://www.qnamaker.ai/>

¹⁴ Siehe: <https://docs.microsoft.com/en-us/azure/bot-service/bot-builder-concept-dialog?view=azure-bot-service-4.0>

¹⁵ Siehe: <https://github.com/Microsoft/botbuilder-tools>

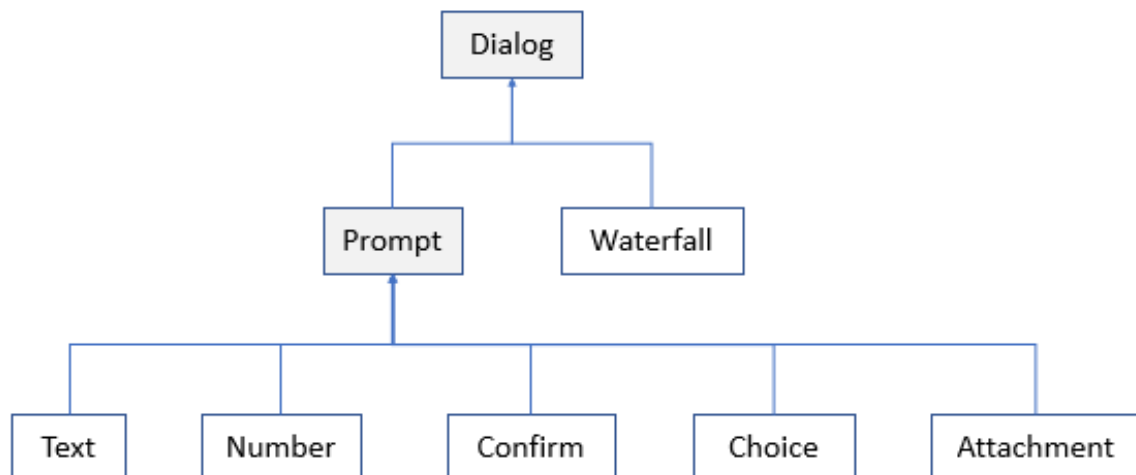


Abbildung 2 Dialogtypen in Bot Builder SDK

6.6.7 INBETRIEBNAHME UND DEPLOYMENT

Aus den Samples können direkt lauffähige Prototypen realisiert werden. Diese können auf Azure deployed werden (Account mit Zahlungsinformation hinterlegt ist nötig). Alternativ kann der Bot, umgesetzt als ASP .NET Core 2 Web Backend Projekt, lokal oder on premise deployed werden. Die Schwierigkeiten dieses Deployment unterscheiden sich dann nicht mehr von anderen Deployments mit ASP .NET Core.

6.6.8 MEHRSPRACHIGKEIT

Microsoft Translator Service kann eingebunden werden.

6.6.9 KOSTEN

Der «Azure Bot Service» ist mit Standard Channels kostenlos im Azure verfügbar. Standard Channels¹⁶ beinhalten Microsofts first-party Services wie Skype, Cortana oder öffentlich verfügbare Bot APIs, wie Facebook oder Slack. Für die Zwecke der Bachelorarbeit ist dieses Angebot hinreichend.

Zusätzlich fallen weitere Kosten an.

Es wird zwischen «Functions Bots» und «Web App Bots» unterschieden. Functions Bots sind «serverless», kommen also ohne Backend aus, bieten das Bezahlung pro Nutzungszeit Zahlungsmodell und sind tendenziell etwas günstiger als das Web App Service Pendant, weil dort ein Backend und allenfalls Datenbank Server verfügbar sind.

Weiter fallen unterschiedliche Kosten je nach Verwendung von LUIS oder QnAMaker an.

Folgende Tabelle gibt einen groben Überblick über die erwarteten Kosten pro Monat auf:

¹⁶ Weitere Informationen: <https://azure.microsoft.com/en-us/pricing/details/bot-service/>



SERVICE	DETAILS	BEZAHLMODELL	KOSTEN PRO MONAT IN CHF
Azure Bot Service	Standard channels	Flatrate	kostenlos
+ Functions	Nutzungsabhängige Bezahlung	Execution Time ¹⁷ und Anzahl Executions	CHF 0.000016/GB-s, (400,000 GB-s kostenlos) CHF 0.197 pro Million executions (1 Mio executions kostenlos)
+ Web App	BASIC ¹⁸ mit einem 4 Core, 7 GB RAM, 10GB Storage Backend In der Region «West Europe»	Abgestuft nach Leistung	Ca. CHF 215.52
+ LUIS	«FREE» Instanz; (West Europe). Textbasierter Input möglich	Nutzungsabhängig	Kostenlos mit max. 5 TPS ¹⁹ , max. 10000 Transaktionen, danach wechselt die Instanz auf «STANDARD» mit CHF 1.477 pro 1000 Transaktionen (Text Requests)
+ QnAMaker	«FREE» Instanz	Jeweils bis zu 1MB pro Dokument (z.B. ein FAQ URL oder Seite in *.pdf, *.docx)	3 TPS, die ersten 3 Dokumente kostenlos
+ Application Insight	Nur Log Analytics mit Data Ingestion und Retention,	Nutzungsabhängig	CHF 2.943 pro GB, die ersten 5 GB kostenlos CHF 0.128 pro GB, die ersten 31 Tage kostenlos

Tabelle 12 Kosten Azure Bot Service

Es ist grundsätzlich möglich, im Rahmen einer Evaluation oder Testphase sämtliche Services kostenlos zu verwenden. Bedingung dafür ist ein Azure Account mit hinterlegten Kreditkarteninformationen. Für das produktiv im Einsatz stehende Produkt werden monatliche Kosten von minimal CHF 300.00 geschätzt. Für das Abschätzen der maximalen zu

¹⁷ Ein Funktionsaufruf gilt als eine Execution. Siehe für weitere Details: <https://azure.microsoft.com/en-us/pricing/details/functions/>

¹⁸ Pricing details unter der URL: ersichtlich: <https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

¹⁹ Transactions per Second (TPS); eine Transaktion ist ein API Call mit textbasierter query Länge von max. 500 Zeichen oder sprachbasierter query Länge von max 15 Sekunden. Siehe dazu: <https://azure.microsoft.com/en-us/pricing/details/cognitive-services/language-understanding-intelligent-services/>



erwartenden monatlichen Kosten müssen Faktoren wie Datenaufkommen, Skalierung und der mögliche Einsatz von weiteren Services (wie zum Beispiel Application Insight Metrics o.Ä.) in Betracht gezogen werden. Die Kosten skalieren grundsätzlich mit Benützung der Services, also gemäss dem Prinzip «pay per use».

6.7 AUSWERTUNG BOT BUILDER FRAMEWORK

6.7.1 BEWERTUNGSMATRIX

KRITERIUM	GEWICHTUNG	BENOTUNG 1 BIS 6 (UNBRAUCHBAR BIS HERVORRAGEND)	GEWICHTETE NOTE
Dokumentation, Support	0.15	6	0.9
Werkzeuge	0.1	5.	0.5
Schnittstellen	0.1	5	0.5
Skalierbarkeit	0.05	6	0.3
Cognitive Capacities	0.2	5	1
Flexibilität Modellierung Gesprächsablauf	0.2	4.5	0.9
Inbetriebnahme / Deployment	0.1	5.5	0.55
Mehrsprachigkeit	0.05	5.5	0.275
Kosten	0.05	4	0.2
Gesamtnote	1.0		5.125

Tabelle 13 Bewertungsmatrix Bot Builder Framework

6.7.2 FAZIT

Bot Builder SDK eignet sich als Bot Framework für die Realisierung des Chatbot «Charli» gut.

Die Stärken liegen im Bereich der Dokumentation und Skalierbarkeit, dank des «global players» Microsoft. Weiter sind die Anzahl und Maturität der Werkzeuge gut und – vorausgesetzt man bleibt im Microsoft Garten—ist die Interoperabilität der verschiedenen Services garantiert.



Schwächen sind im Bereich der Modellierung des Gesprächsablaufs ersichtlich und im Bereich Kosten. Das Gespräch wird konzeptionell mittels Dialogen umgesetzt, welche im Code abgebildet werden müssen. Vereinfachungen für diesen Prozess konnten zum Zeitpunkt der Evaluation nicht ausgemacht werden. Die Kostenstruktur ist, obwohl transparent, nicht übersichtlich gestaltet. Es ist schwierig, die Kosten nach oben abzuschätzen, ohne ein bereits lauffähiges Produkt im Einsatz zu haben und die Nutzungszahlen zu kennen.

6.8 EINFÜHRUNG DIALOGFLOW²⁰

Dialogflow, ehemals API.ai, ist eine auf Mensch-Computer-Interaktionen spezialisierte Technologie, basierend auf natürlichen Sprachkonversationen. Es ermöglicht App-Entwicklern neue Möglichkeiten der Interaktion mit ihren Benutzeroberflächen durch Sprach- und Textaustausch auf Basis künstlicher Intelligenz anzubieten.

Mit Dialogflow haben Entwickler Zugang zu integrierten Technologien für maschinelles Lernen und natürliche Sprachverarbeitung. Auf diese Weise können sie sich auf andere integrale Bestandteile der App-Erstellung konzentrieren und nicht auf die Beschreibung detaillierter Grammatikregeln.

Dialogflow verfügt über vorgefertigte Agenten, mit denen Benutzer ihre Anwendungen schneller erstellen können. Darüber hinaus verfügt die überarbeitete API über einen Inline-Code-Editor, so dass Programmierer mehrere Aufgaben direkt von der Konsole aus ausführen können. Durch den Einsatz dieser Inline Code Editoren für sogenannte Actions, kann, bei hinreichend einfachen Chatbots, auf ein eigenes Backend vollständig verzichtet werden

6.9 BEURTEILUNG DIALOGFLOW

6.9.1 DOKUMENTATION UND SUPPORT

Dialogflow ist sehr gut dokumentiert und aktuell gehalten, was den Einstieg erleichtert. Funktionen werden auch mit YouTube Videos verständlich erklärt. Dank der grossen Google Community existieren auch Hilfestellungen zu Fragen, die nicht von der Dokumentation beantwortet wurden.

6.9.2 WERKZEUGE

Dialogflow bietet die grundlegenden Werkzeuge an, um rasch einen simplen Chatbot zu erstellen. Die Werkzeuge werden über einfach zu bedienende Web UIs, wie zum Beispiel die «Dialogflow Console», genutzt.

Es kann auch auf die Funktionalität des Google Assistent zurückgegriffen werden.

²⁰ Quelle: <https://en.wikipedia.org/wiki/Dialogflow>

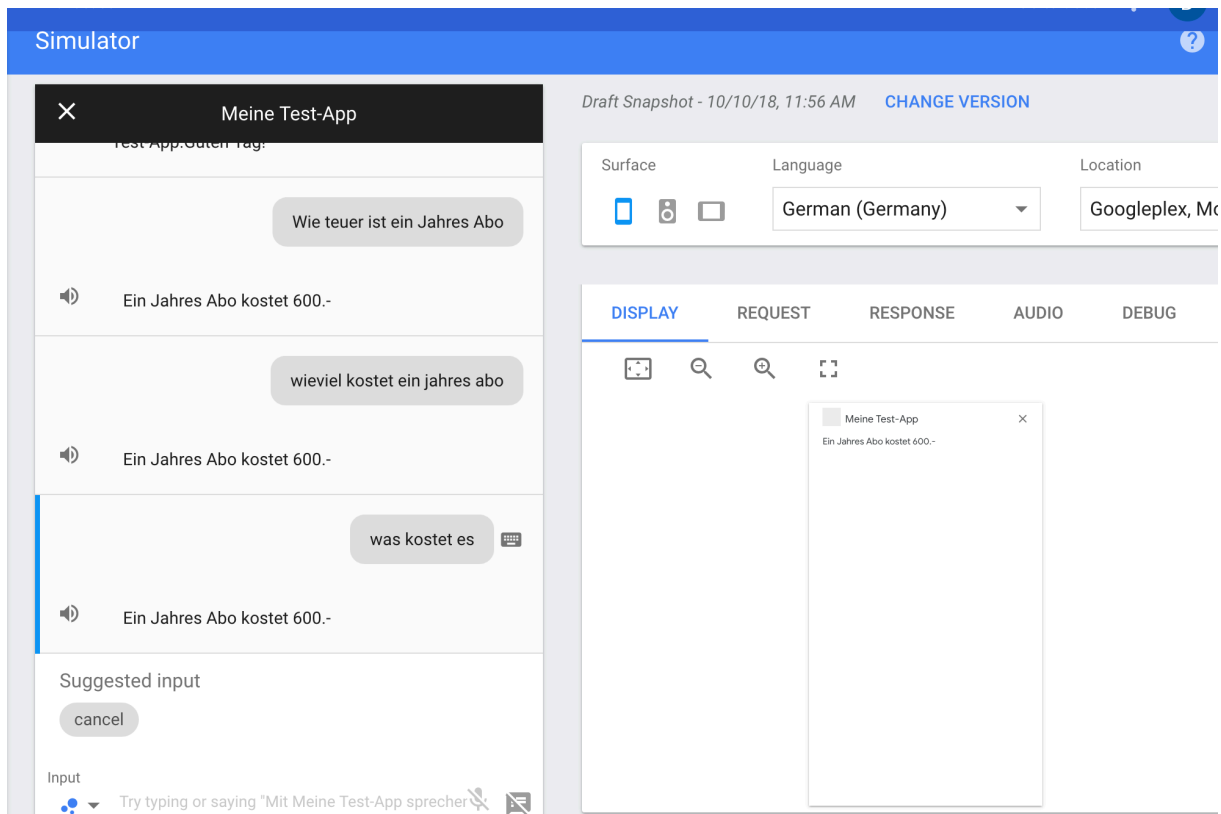


Abbildung 3 Google Assistent inkl. Simulator User Interface

6.9.3 SCHNITTSTELLEN

Google bietet das Gesamtpaket an. Entsprechend sind alle benötigten Services, welche vom Bot verwendet werden könnten, ebenfalls auf Google Cloud Platform (GCP) verfügbar. Ein erster Test hat gezeigt, dass die Services gut miteinander orchestrierbar sind. Beim Test wurde die Authentifizierung von Firebase für die Datenbank verwendet.

Zusätzlich sind viele Services über normale RESTful http web APIs verfügbar, was die Interoperabilität verbessert.

Der Chatbot kann auf zahlreichen Plattformen integriert werden. Für die Bekannteren existieren bereits fertige Integrationen, welche sich einfach einrichten lassen.

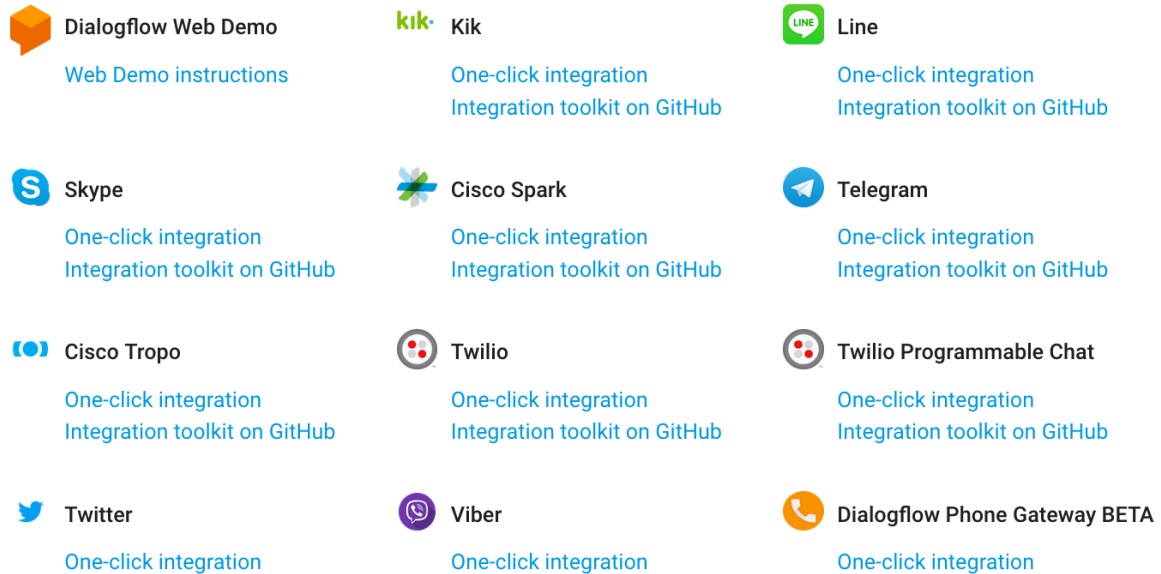


Abbildung 4 Plattformen

6.9.4 SKALIERBARKEIT

Mit Dialogflow und den auf GCP basierten Services kann der Bot frei skaliert werden. In der Standard Edition von Dialogflow bleiben diese Services kostenlos. Diese Services besitzen jedoch Kontingente und Beschränkungen²¹:

Option	Dialogflow Standard Edition	Dialogflow Enterprise Edition
Textanfragen pro Minute	180	600
Audioanfragen pro Minute*	100**	300
Audioanfragen pro Tag*	1.000**	100.000
Audioanfragen pro Monat	15.000**	Unbegrenzt
Maximale Audiolänge pro Anfrage	60 Sekunden	60 Sekunden
Alle anderen Anfragen pro Minute (z. B. Bearbeitung von Intents)	60	60

Abbildung 5 Beschränkungen Standard Edition Dialogflow

6.9.5 COGNITIVE CAPACITIES

Die wichtigsten cognitive Capacities sind bereits in Dialogflow integriert ohne, dass ein externer Service benötigt wird. So sind zum Beispiel die NLP Services, basierend auf Machine Learning Algorithmen, nutzbar und trainierbar.

6.9.6 FLEXIBILITÄT, MODELLIERUNG GESPRÄCHSABLAUF

Das Kernkonzept zur Modellierung eines Gesprächsablaufs in Dialogflow sind Intents. Intents verarbeiten eingehende Aktivitäten (welche die Nachricht enthalten) und enthalten Antworten. Man kann eine beliebige Anzahl von Intents erstellen, welche den ganzen Gesprächsablauf modellieren. Intents können miteinander verknüpft werden, um ein Gespräch zu modellieren.

²¹ Siehe dazu: <https://cloud.google.com/dialogflow-enterprise/>

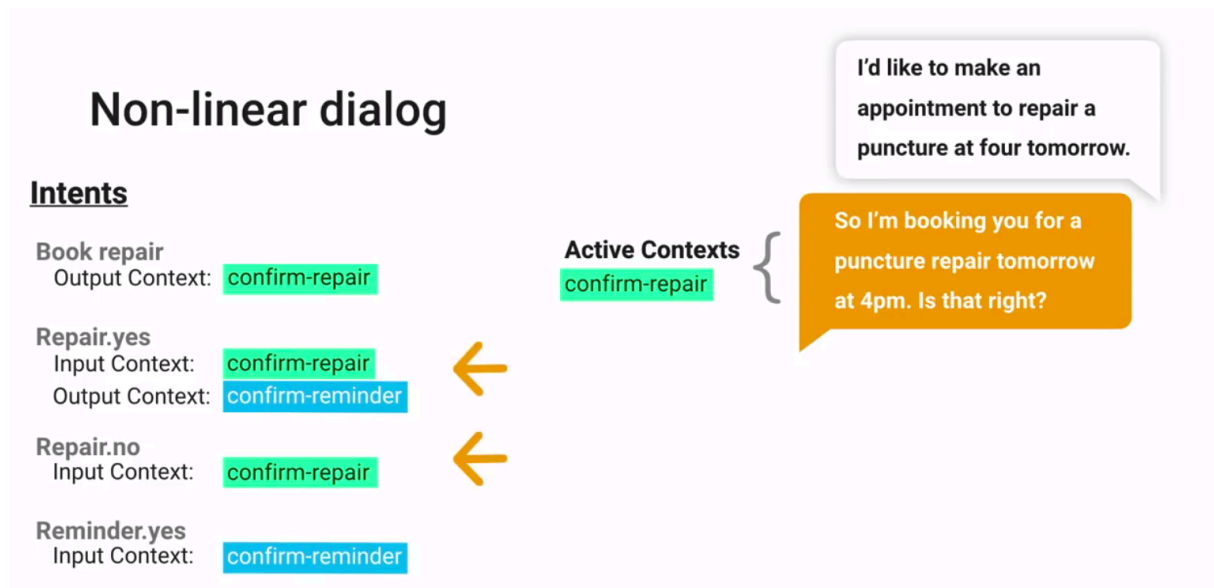


Abbildung 6 Non-Linear Dialog

6.9.7 INBETRIEBNAHME UND DEPLOYMENT

Das Erstellen oder Integrieren von Agents ist einfach gehalten. Zum Testen können vorgefertigte Agents verwendet werden. Für zahlreiche Endpunkte existieren vorgefertigte Integrationslösungen für Slack, Twitter oder ähnliche Plattformen, welche mit wenigen Klicks durchgeführt werden können. Für das Einbinden des Chat UIs wird ein <iframe> basiertes Codefragment angeboten, welches auf der eigenen Website integriert werden kann.

6.9.8 MEHRSPRACHIGKEIT

Dialogflow enthält Konfigurationsmöglichkeiten, um Mehrsprachigkeit zu unterstützen. Die entsprechenden Übersetzungen werden vom Entwickler bereitgestellt.



6.9.9 KOSTEN

Viele Funktionen von Dialogflow sind in begrenzten Mengen kostenlos. Services, welche als unbegrenzt markiert sind unterliegen den im Kapitel «Skalierbarkeit» beschriebenen Kontingenten und Einschränkungen (im Rahmen der Standard Edition).

	Free Standard Edition	Pay as you go Enterprise Edition	
		Essentials	Plus
Knowledge Connectors (Beta)	Limited	Limited	Unlimited*
Text or Google Assistant	Unlimited*	Unlimited* \$0.002 per request	Unlimited* \$0.004 per request
Audio Includes speech recognition and synthesis (Beta)	Limited	Unlimited* \$0.0065 per 15 sec of audio	Unlimited* \$0.0085 per 15 sec of audio
Phone Call (Beta) Includes phone connectivity, speech recognition, natural language understanding, speech synthesis	Limited	Unlimited* \$0.05 per min of phone call processed	Unlimited* \$0.065 per min of phone call processed
Toll-free phone call (Beta)	None	\$0.06 per min of phone call processed	\$0.075 per min of phone call processed
Service Level Agreement	None	SLA	
Support	Community support and email	Eligible for Cloud Support package with committed response times for supporting production applications	
Terms of Service	Dialogflow ToS	Google Cloud Platform ToS	

Abbildung 7 Kosten Dialogflow Standard vs Enterprise Edition

6.10 AUSWERTUNG DIALOGFLOW

6.10.1 BEWERTUNGSMATRIX

KRITERIUM	GEWICHTUNG	BENOTUNG 1 BIS 6 (UNBRAUCHBAR BIS HERVORRAGEND)	GEWICHTETE NOTE
Dokumentation, Support	0.15	6	0.9
Werkzeuge	0.1	5.	0.5
Schnittstellen	0.1	5	0.5
Skalierbarkeit	0.05	6	0.3
Cognitive Capacities	0.2	5	1



KRITERIUM	GEWICHTUNG	BENOTUNG 1 BIS 6 (UNBRAUCHBAR BIS HERVORRAGEND)	GEWICHTETE NOTE
Flexibilität Modellierung Gesprächsablauf	0.2	5	1
Inbetriebnahme / Deployment	0.1	6	0.6
Mehrsprachigkeit	0.05	5.5	0.275
Kosten	0.05	5	0.25
Gesamtnote	1.0		5.325

Tabelle 14 Bewertungsmatrix Dialogflow

6.10.2 FAZIT

Das Arbeiten mit Dialogflow ist intuitiv und simpel. Die Dokumentationen sind ausführlich und verständlich. Die grosse Anzahl von Benutzern und die Community von Google helfen bei der Lösung von Problemen.

Die bereitgestellten «Agents» inklusive Integrationen in populäre Anwendungen wie Twitter, Slack, Telegram oder Ähnliche ersparen viel Arbeit für die Inbetriebnahme oder Entwicklung des Frontends. Dank sogenannter «Webhooks» können, wo nötig, gezielt API Calls in ein eigenes Backend gemacht werden.

Die Intent Erkennung ist dank ML²² basierten Algorithmen konkurrenzfähig und kann mit Training von geeigneten Trainingsdatensätzen weiter verbessert werden.

6.11 GESAMTERGEBNIS

6.11.1 ERGEBNISÜBERBLICK

Die folgende Tabelle zeigt noch einmal die beiden Frameworks und deren Bewertung gegenübergestellt:

KRITERIUM	BOT BUILDER FRAMEWORK (MICROSOFT)	DIALOGFLOW (GOOGLE)
Dokumentation, Support	0.9	0.9
Werkzeuge	0.5	0.5

²² Machine Learning: https://de.wikipedia.org/wiki/Maschinelles_Lernen



KRITERIUM	BOT BUILDER FRAMEWORK (MICROSOFT)	DIALOGFLOW (GOOGLE)
Schnittstellen	0.5	0.5
Skalierbarkeit	0.3	0.3
Cognitive Capacities	1	1
Flexibilität Modellierung Gesprächsablauf	0.9	1
Inbetriebnahme / Deployment	0.55	0.6
Mehrsprachigkeit	0.275	0.275
Kosten	0.2	0.25
Gesamtnote	5.125	5.325

Tabelle 15 Ergebnisgesamtüberblick

6.11.2 ERGEBNIS FAZIT

Beide evaluierten Bot Frameworks erhalten eine gute Bewertung. Mit leichten Vorzügen bei der Flexibilität und Einfachheit für das Modellieren der Konversationen und einfacherem Deployment setzt sich «Dialogflow» leicht gegenüber dem Bot Builder Framework von Microsoft durch.



7. ANFORDERUNGSSPEZIFIKATION

7.1 EINLEITUNG

Die Anforderungsspezifikation wird in vier Schritten festgelegt:

- Anforderungen ermitteln
- Analyse der Anforderungen
- Beschreibung der Anforderungen
- Revision der Anforderungen (zu einem späteren Zeitpunkt, falls notwendig)

7.1.1 ANFORDERUNGSERMITTLUNG

Das Ermitteln der Anforderungen wurde in Gesprächen mit dem Industriepartner sowie Betreuer und unter Festlegen der Aufgabenstellung durchgeführt.

Die Ergebnisse sind im separaten Dokument «Aufgabenstellung²³» einsehbar.

7.1.2 ANFORDERUNGSANALYSE UND BESCHREIBUNG

Aus den Zielsetzungen der Aufgabenstellung ergeben sich folgende Anforderungen:

ID	ANFORDERUNG	BESCHREIBUNG	PRIORITÄT [1-3]
1	Modellierung Gespräch	Ein Akteur ist in der Lage, den Gesprächsverlauf zu modellieren. Das heisst, er kann Antworten auf Fragen erstellen, anpassen oder löschen und Übergänge von einem Gesprächsthema in ein anderes Gesprächsthema ändern, erstellen oder löschen	1
2	Training	Ein Akteur kann den Verständnisgrad des Systems bei der Erkennung der Absicht anhand einer «Utterance ²⁴ » (Textphrase) verbessern, indem Trainingsdaten eingesetzt werden	1
3	Notification	Ein Akteur kann vom System benachrichtigt werden	2
4	UI	Ein Akteur kann über ein textbasiertes Userinterface (UTF8 Zeichensatz) mit dem System kommunizieren	1
5	Konversationsübernahme	Ein Akteur kann in einer laufenden Konversation einsteigen und das Gespräch aufnehmen	2

²³ Siehe: https://dev.azure.com/dedi1199/ChatBot/_git/Charli-Documentation?path=%2Fdocu&version=GBmaster

²⁴ Siehe dazu: <https://dialogflow.com/docs/training-analytics/training>



ID	ANFORDERUNG	BESCHREIBUNG	PRIORITÄT [1-3]
6	Persistieren der Konversationen	Das System kann Konversationen persistieren.	1
7	Monitoring	Ein Akteur kann laufende Konversationen einsehen	2
8	Management	Ein Akteur kann Konversationen einsehen oder löschen, Kundeninformationen erstellen, auslesen, ändern oder löschen und Konfigurationen für den Betrieb des Systems erstellen, auslesen, ändern oder löschen (CRUD)	3
9	Identifikation	Das System kann anhand von Metadaten und persistierten Kundeninformationen Clients wiedererkennen	3

Tabelle 16 Übersicht funktionale Anforderungen

7.1.3 ANFORDERUNGSREVISION

Im Rahmen der Bachelorarbeit wird zugunsten der Entwicklungszeit und mangels Ressourcen auf ein formelles Änderungsverfahren (Change Management) bewusst verzichtet. Allfällige Anpassungen der Anforderungen werden iterativ mit dem Betreuer kommuniziert, abgesegnet und angepasst.

7.2 USE CASES

Aus Sicht der Aktoren und Systeme ergeben sich Anwendungsfälle wie im folgendem Diagramm ersichtlich.

7.2.1 USE CASE DIAGRAM

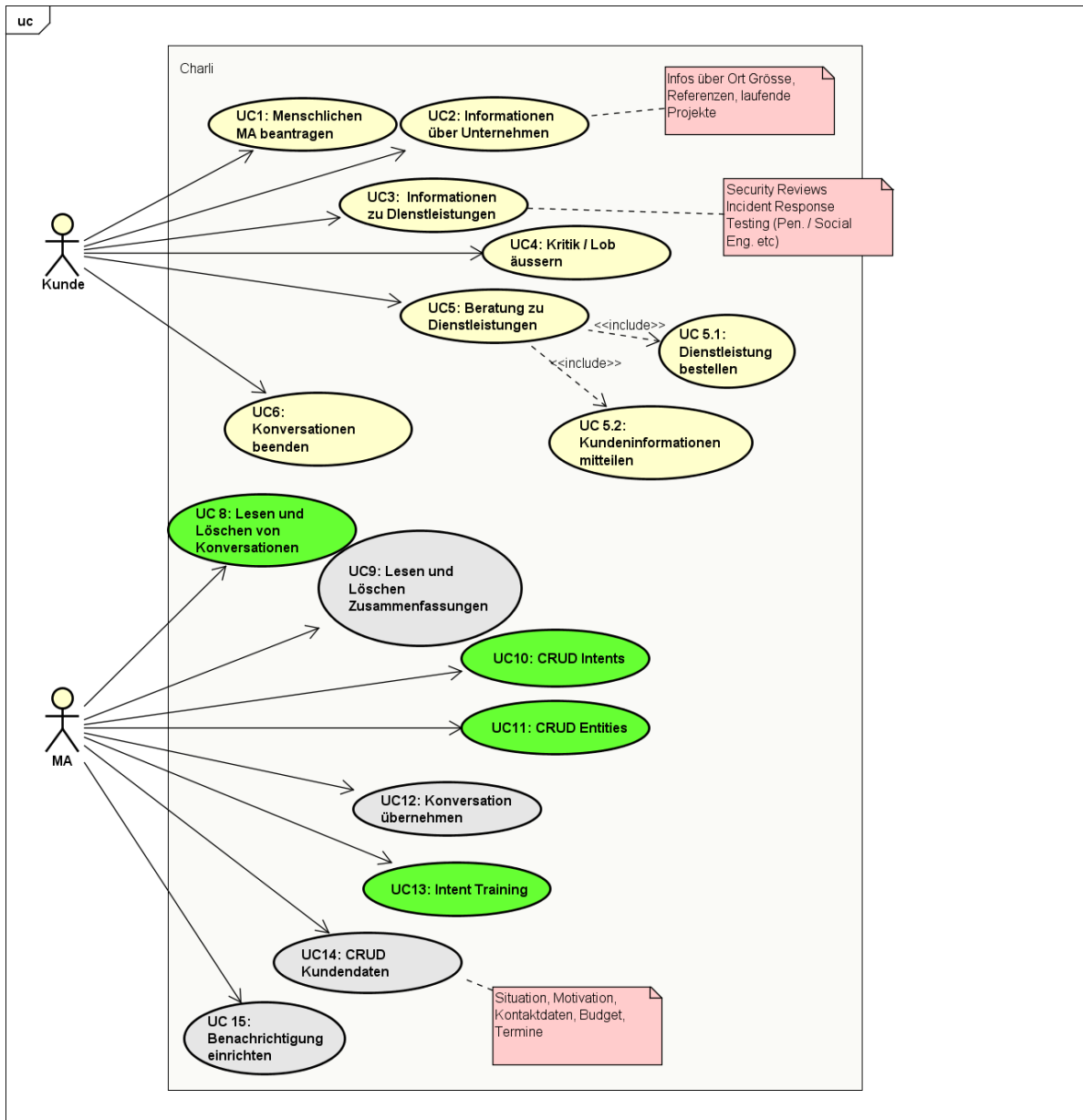


Abbildung 8 Use Case Diagramm



7.2.2 USE CASE BESCHREIBUNGEN

7.2.2.1 ÜBERBLICK

ID	USE CASE NAME	PRIORITÄT [1-3]
1	Menschlichen Mitarbeiter beantragen	1
2	Informationen über Unternehmen	1
3	Informationen über Dienstleistungen	1
4	Kritik / Lob äussern	1
5	Beratung zu Dienstleistung	1
5.1	Dienstleistung bestellen	1
5.1	Kundeninformationen mitteilen	1
6	Konversation beenden	1
8	Lesen und Löschen von Konversationen	1
9	Lesen und Löschen Zusammenfassungen	2
10	CRUD Intents	1
11	CRUD Entities	1
12	Konversation übernehmen	2
13	Intent Training	1
14	CRUD Kundendaten	3



ID	USE CASE NAME	PRIORITÄT [1-3]
15	Benachrichtigung einrichten	2

Tabelle 17 Überblick Use Cases

Die Use Cases (UC) werden in zwei Gruppen unterteilt:

- UC des Aktors «Kunde»
- UC des Aktors «Compass Security Mitarbeiter» (MA).

7.2.2.2 RAHMENBEDINGUNGEN

Im Folgenden können «System» und «Chatbot Charli» oder «Charli» als Synonyme betrachtet werden.

Die UC sind im «Brief» Format beschrieben (UC Name, Aktoren und Beschreibung).

7.2.3 USE CASES FÜR KUNDEN

7.2.3.1 AUSGANGSLAGE

Für alle UC des Kunden ist folgende Ausgangslage geschaffen:

Der Kunde surfte auf der Website von Compass Security und gelangte auf die Seite, auf welcher der Chatbot Charli läuft. Der Kunde hat den Messenger gesehen und eine Konversation mit dem Chatbot gestartet.

Da der Kunde lediglich über eine textbasierte Schnittstelle mit dem Chatbot interagiert, werden Informationen auch nur in Textform übermittelt.

7.2.3.2 UC 1: MENSCHLICHEN MITARBEITER BEANTRAGEN

Der Kunde äussert die Absicht, mit einem richtigen, menschlichen Mitarbeiter zu kommunizieren. Dies wird zum Beispiel über den Wunsch nach einem Telefonat zum Ausdruck gebracht.

Charli wird daraufhin Kontaktinformationen einfordern, den Aktor MA benachrichtigen und die Konversation beenden.

7.2.3.3 UC 2: INFORMATIONEN ÜBER UNTERNEHMEN

Der Kunde möchte Informationen über die Compass Security AG. Das können Entitäten wie Niederlassungsort, Mitarbeiteranzahl, Referenzen oder aktuelle Projekte sein.

Charli gibt Auskunft.

7.2.3.4 UC 3: INFORMATIONEN ÜBER DIENSTLEISTUNGEN

Der Kunde möchte Informationen über die Angebote und Dienstleistungen der Compass Security AG.

Charli gibt Informationen weiter und startet ein Beratungsgespräch, wo versucht wird, die Motivation des Kunden zu erfassen. Es geht darum, sich für die Bedürfnisse des Kunden zu interessieren.

7.2.3.5 UC 4: KRITIK / LOB ÄUSSERN

Der Kunde teilt Charli seine Meinung mit. Dies kann in Form von positiver oder negativer Kritik geschehen.



Charli erkennt positive oder negative Äusserungen. Sie reagiert auf die Kritik, indem sie positive Punkte hervorhebt und nicht auf negative Punkte eingeht. Weiter benachrichtigt Charli den MA.

7.2.3.6 UC 5: BERATUNG ZU DIENSTLEISTUNGEN

Der UC 5 ist eine zentrale Aufgabe des Chatbots.

Folgende Punkte sind während des Beratungsgesprächs wichtig:

- Motivation des Kunden erkennen
- Eine persönliche Beziehung aufbauen
- Terminologie des Kunden übernehmen
- Verstehen, gegen was sich der Kunde schützen möchte
- Den Kunden über Bedrohungen und Gefahren aufklären
- Aufklären und Orientieren über mögliche Dienstleistungen
- Zusagen des Kunden erkennen und sich merken («Pflöcke setzen»)
- Rahmenbedingungen erfragen wie Termine oder Budget
- MA benachrichtigen

Der UC 5 setzt sich aus zwei Sub UC zusammen:

SUB USE CASE	BESCHREIBUNG
5.1 Dienstleistung bestellen	Der Kunde zeigt Interesse an bestimmten Dienstleistungen. Charli wird zu dieser Dienstleistung weitere Fragen stellen und Informationen sammeln (Slot Filling).
5.2 Kundeninformationen mitteilen	Der Kunde kann Informationen bereitstellen. Dies können Entitäten wie Kontaktdaten, Name, Ortschaft, Firma, Motivation, Budget oder Terminvorstellungen sein. Charli kann diese Informationen auslesen und sich im Kontext einer Konversation merken.

Tabelle 18 Sub Usecases 5

7.2.3.7 UC 6: KONVERSATION BEENDEN

Der Kunde kann die Konversation regulär beenden, das heisst er kann sich vom Gesprächspartner Charli verabschieden.

Charli erkennt die Absicht zum Gesprächsende und verabschiedet sich freundlich. Abhängig vom Verlauf der Konversation kann Charli noch nach den Kontaktdaten des Kunden fragen.

7.2.4 USE CASES FÜR COMPASS SECURITY MITARBEITER

7.2.4.1 UC 8: LESEN UND LÖSCHEN VON KONVERSATIONEN

Der MA kann Konversationen lesen oder löschen. Dazu zählen die noch laufenden als auch die bereits geschlossenen Konversationen.

7.2.4.2 UC 9: LESEN UND LÖSCHEN ZUSAMMENFASSUNGEN

Der MA kann von Charli erzeugte Zusammenfassungen von Konversationen lesen oder löschen.



7.2.4.3 UC 10: CRUD INTENTS

Der MA kann Intents erstellen, lesen, aktualisieren oder löschen. Ein Intent enthält dabei mögliche Textphrasen des Kunden und dazugehörige Antworten. Die Textphrasen können mit Hilfe von Entities formatiert werden, um so Informationen zu extrahieren. Weiter kann der MA Input und Output Contexts bestimmen, um so den Konversationsfluss zu steuern.

7.2.4.4 UC 11: CRUD ENTITIES

Der Ma kann Entities erstellen, lesen, aktualisieren oder löschen. Eine Entity enthalten dabei spezifische Informationen, wie zum Beispiel Orte, Dinge, Mengen, Zeitangaben, Produktnamen und vieles mehr.

7.2.4.5 UC 12: KONVERSATION ÜBERNEHMEN

Der MA kann in laufende Konversationen einsteigen und Charli als Gesprächspartner ablösen. Dies geschieht ohne Konversationsunterbruch aus Sicht des Kunden.

7.2.4.6 UC 13: INTENT TRAINING

Der MA kann die Intenterkennung verbessern, indem er in alten Konversationen die falsch erkannten Intents korrigiert, neue Trainingstextphrasen für bestehende Intents erstellt oder neue Intents definiert (UC 10).

7.2.4.7 UC 14: CRUD KUNDENDATEN

Der MA kann Kundendaten erstellen, auslesen, aktualisieren oder löschen. Kundendaten enthalten Informationen zu Kunden wie Kontaktdaten, Namen, Fingerprints und weitere Metadaten.

7.2.4.8 UC 15: BENACHRICHTIGUNG EINRICHTEN

Der MA kann im System einrichten, wo er auf welche Weise benachrichtigt werden möchte.

7.3 NICHT FUNKTIONALE ANFORDERUNGEN (NFR)

7.3.1 EINLEITUNG

Nicht funktionale Anforderungen sind spezifische, messbare Qualitätsmerkmale, die grossen Einfluss auf die Architektur- und Technologieentscheide haben. Die nachfolgende Analyse der nichtfunktionalen Anforderungen ist angelehnt an das „(F)URPS+(Functionality, Usability, Reliability, Performance, Supportability)“ Modell.

7.3.2 BEGRIFFE

Es werden zunächst einige Begriffe definiert. Zwecks der Einfachheit und Verständlichkeit sind diese in Englisch mit deutscher Übersetzung in Klammern beschrieben:

BEGRIFF	ZUORDNUNG NFR	BEDEUTUNG
Safety (Betriebssicherheit)	Functionality	Sicherheit aus Anwendersicht, beispielsweise End- zu End verschlüsselte Kommunikationskanäle
Auditability (Protokollierung)	Functionality	Protokollierung wichtiger, interner Daten zur Systemausführung



BEGRIFF	ZUORDNUNG NFR	BEDEUTUNG
Operability (Bedienbarkeit)	Usability	Beispielsweise die Geschwindigkeit, in welcher ein User Daten erhalten kann
Accuracy (Genauigkeit)	Reliability	Umfasst die Richtigkeit und Genauigkeit von durchgeführten Berechnungen. Im Kontext eines Chatbots kann das zum Beispiel der Intenterkennungsgrad sein
Recoverability (Fehlertoleranz)	Reliability	Die Reaktion, mit welcher die Anwendung auf einen Fehler antwortet (Fehlererholungsprozess)
Security (Angriffssicherheit)	Reliability	Im Gegensatz zu Safety bezieht sich in diesem Fall die Sicherheit auf den Schutz des Objektes vor seiner Umgebung. Konkret bedeutet dies, dass für den Betrieb des Chatbots notwendige Dienste und Infrastrukturen geschützt werden.
Throughput (Durchsatz)	Performance	Beispielsweise die Anzahl Transaktionen pro Sekunde, Datenraten oder Verzögerungszeiten
Capacity (Kapazität)	Performance	Bezieht sich auf die Anzahl (paralleler) Transaktionen, gleichzeitig ausführender Benutzer sowie die zu speichernden Daten
Maintainability (Wartbarkeit)	Supportability	Die Leichtigkeit, mit der das System betrieben und gewartet werden kann
Extendability (Erweiterbarkeit)	Supportability	Die Leichtigkeit, mit der das System erweitert werden kann
Localizability (Lokalisierbarkeit)	Supportability	Die Unterstützung von Sprachen und örtlichen Einstellungen

Tabelle 19 Begriffsdefinitionen



7.3.3 NICHT FUNKTIONALE ANFORDERUNGEN

ZUORDNUNG	ANFORDERUNG
Safety	Die Kommunikation des Users mit dem Bot ist mittels SSL/TLS gesichert
Safety	User haben keinen Zugang zu fremden Konversationen
Safety	Das Chatbot UI ist gegen Script-injection basierte Angriffe geschützt (zum Beispiel XSS)
Auditability	Alle Konversationen müssen in für einen Menschen lesbaren Form persistiert oder auslesbar sein
Operability	Das Chatbot UI erlaubt die Eingabe von Text und das Abschicken von Text mittels der Eingabetaste
Accuracy	Der Confidence-score bei der Intenterkennung des Bots innerhalb einer Konversation ist im Durchschnitt mindestens 75%
Recoverability	Der Chatbot kehrt bei Unverständnis in einen definierten «Non Intent» Zustand zurück oder übergibt an einen (menschlichen) Supporter
Security	Die Zugriffe zum Backend, Datenbanken oder Verwaltungsplattform des Chatbots sind nur für Berechtigte möglich. Zugriffsberechtigungen werden vom Projektteam verwaltet
Throughput	Der Chatbot kann bis zu 5 Transaktionen pro Sekunde verarbeiten. Eine Transaktion beschreibt einen Textbasierten Input mit einer maximalen Zeichenlänge von 500 Zeichen
Capacity	Es können bis zu 5 User gleichzeitig mit dem Chatbot interagieren. Es können bis zu 5 Konversationen gleichzeitig betrieben werden
Maintainability	Die Intenterkennung ist mittels Trainingsdaten verbesserungsfähig. Die Trainingsdaten werden vom (menschlichen) Betreiber vorbereitet
Extendability	Der Chatbot bietet die Möglichkeit, nachträglich neue Intents zu trainieren und den groben Gesprächsablauf zu ändern
Localizability	Der Chatbot bietet die Möglichkeit, weitere Sprachen einzubinden, ohne dass Quellcode geändert werden muss

Tabelle 20 Nichtfunktionale Anforderungen



7.3.4 VERHALTENSGRUNDSÄTZE

Um ein gutes Beratungsgespräch zu erreichen, soll Charli als Chatbot mit folgenden Charakterzügen und Verhaltenskodizes modelliert werden:

CHARAKTER/ VERHALTEN	ERLÄUTERUNG
Menschlich	<ul style="list-style-type: none">• Freude am Kontakt zeigen
Kundenbedürfnis-orientiert	<ul style="list-style-type: none">• Offene Fragen stellend• Kundenbedürfnis erkennend• Terminologie des Gesprächspartners übernehmen• Informationen Kundengerecht aufbereitet, keine zu langen Antworttexte
freundlich	<ul style="list-style-type: none">• Nicht auf negative Äusserungen eingehen• Keine Kraftausdrücke, keine wertenden Aussagen über Kunde• Verständnis zeigend
klar	<ul style="list-style-type: none">• Die gelieferten Informationen sind klar und einfach verständlich• Antworten sind, wenn möglich kurz
Nicht angeberisch	<ul style="list-style-type: none">• Kein Prahlen,• keine Vergleiche anstellen mit Mitbewerbern
Nicht über Geld sprechend	<ul style="list-style-type: none">• Preise oder Kosten nur auf explizite Anfrage ansprechen• Keine Rabattverhandlungen

Tabelle 21 Verhaltensgrundsätze

7.3.5 TESTEN DER VERHALTENSGRUNDSÄTZE

Die Beurteilung des Charakters und Wesen des Chatbots bringt einige Herausforderungen:

1. Der Charakter wird von der jeweiligen Testperson subjektiv wahrgenommen
2. Wesenszüge können schlecht gegen eine festgelegte Anzahl Kriterien getestet werden
3. Das Trainieren des Bots als integralen Bestandteil für die (Weiter)Entwicklung soll berücksichtigt werden

Deshalb soll manuell, beispielsweise nach Erreichen eines Meilensteins ein Beratungsgespräch durchgeführt werden. Um den Effekt der subjektiven Empfindung abzdämpfen, wird eine grosse Anzahl verschiedener Testpersonen angestrebt. Im Minimum sollen drei Testpersonen involviert werden.

Im Folgenden werden Test Cases mit festgelegter Zielsetzung für die Testperson definiert. Zu jedem Test Case wird zusätzlich in Bewertungsraster nach Abschluss des Gesprächs von der Testperson ausgefüllt.

7.3.5.1 BEISPIEL TEST CASES

Test Cases leiten sich aus den Use Cases ab. Im Folgenden sind beispielhaft einige Test Cases beschrieben, damit Testpersonen früh einbezogen werden können. Die Liste der Test Cases wird im Verlauf des Projekts ausgebaut.



BSP TEST CASE 2 KRITISIEREN	
Ziel	Dem Chatbot die Unzufriedenheit ausdrücken, dass die keine genaueren Informationen über die Preise zu den Dienstleistungen vorhanden sind
Erwartetes Verhalten	Der Chatbot nimmt die Kritik auf, geht aber nicht darauf ein

Tabelle 22 Beispiel Test Case 2

BSP TEST CASE 3 DIENSTLEISTUNGSBERATUNG ZU PENETRATION TEST	
Ziel	Zum Thema Penetration Test alle relevanten Fragen stellen, bis kein Bedürfnis nach weiteren Informationen besteht
Erwartetes Verhalten	Der Chatbot informiert über Penetration Testing und beantwortet die Fragen der Testperson. Mit Rückfragen wird der Chatbot feststellen, ob alle Fragen beantwortet wurden und wird eine Kontaktaufnahme anstreben

Tabelle 23 Beispiel Test Case 3

BSP TEST CASE 4 INFORMIEREN ÜBER NÄCHSTEN ANLASS	
Ziel	Auskunft darüber erhalten, wann und wo der nächste Anlass der Compass Security stattfindet
Erwartetes Verhalten	Der Chatbot liefert Informationen darüber, wann der nächste Anlass stattfindet

Tabelle 24 Beispiel Test Case 4



BSP TEST CASE 5 MENSCHLICHEN MITARBEITER ANFORDERN	
Ziel	Dem Chatbot mitteilen, dass ein menschlicher Kontakt erwünscht oder gefordert wird
Erwartetes Verhalten	Der Chatbot erkennt das Bedürfnis der Testperson, dass diese lieber einen echten menschlichen Mitarbeiter sprechen möchte. Der Chatbot versucht noch, Kontaktinformationen zu sammeln und beendet das Gespräch

Tabelle 25 Beispiel Test Case 5

7.3.5.2 BEWERTUNGSRASTER CHARAKTER UND VERHALTEN

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

Zu jedem Test Case wird das Verhalten anhand dieses Rasters mitbewertet.

CHARAKTER / VERHALTEN	BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	
Stellt offene Fragen	
Übernimmt die Terminologie des Gesprächspartners bei Nomen	
Die Antworten sind nicht unnötig lange	
Die Antworten sind hilfreich	
Die Antworten und Informationen sind einfach verständlich	
Geht nicht auf negative Äusserungen ein	
Verwendet keine Kraftausdrücke und Fluchwörter	

Tabelle 26 Bewertungsraster für Charakter



7.3.5.3 UMGANG MIT BESONDEREN FRAGEN

Einige besondere «Killer Fragen», welche im Rahmen eines Beratungsgesprächs auftreten können, erfordern eine besondere Behandlung.

Der Chatbot soll sinngemäss auf folgende Aussagen mit entsprechenden Antworten reagieren:

AUSSAGE / FRAGE	ANTWORT / REAKTION
Ihr seid viel zu teuer	Wir bringen viel Erfahrung mit und Qualität hat ihren Preis
Ich habe schlechte Erfahrungen mit euch gemacht	Das tut uns leid. Wir nehmen Ihr Feedback ernst. Können Sie uns sagen, was wir verbessern können?
Ich möchte mit einem richtigen Menschen sprechen.	Danke. Wie können wir Sie erreichen?
Ich habe nichts Gutes gehört über euch	Danke für Ihr Feedback. Haben Sie selbst negative Erfahrungen gemacht?

Tabelle 27 Killerfragen mit Antworten

7.3.5.4 ERFÜLLUNGSKRITERIEN

Für die Erfüllung der Anforderungen müssen drei Kriterien erfüllt sein:

1. Ziele, in den Test Cases beschrieben, müssen erreicht sein
2. Die Bewertung hinsichtlich des Charakters und Verhalten des Chatbots muss im Mittel über die letzten zehn Testdurchläufe (rolling average) durch drei unterschiedliche Testpersonen mindestens 2.0 (befriedigend) betragen.
3. Die Antworten zu den «Killer Fragen» stimmen sinngemäss mit den erwarteten Antworten, gemäss Kapitel «Umgang mit besonderen Fragen», überein.

8. SOFTWARE DESIGN

8.1 EINLEITUNG

Im Folgenden wird beschrieben, wie die Anforderungen umgesetzt werden. Die Kernfragen wie, wo und warum werden in diesem Kapitel geklärt.

8.2 ARCHITEKTUR

8.2.1 ARCHITEKTUR VARIANTEN

Die Architekturdiskussion bringt im Wesentlichen zwei unterschiedliche Entwürfe zu Tage, die in den folgenden Unterkapiteln erläutert werden.

8.2.2 ÜBERBLICK ARCHITEKTUR VARIANTE 1

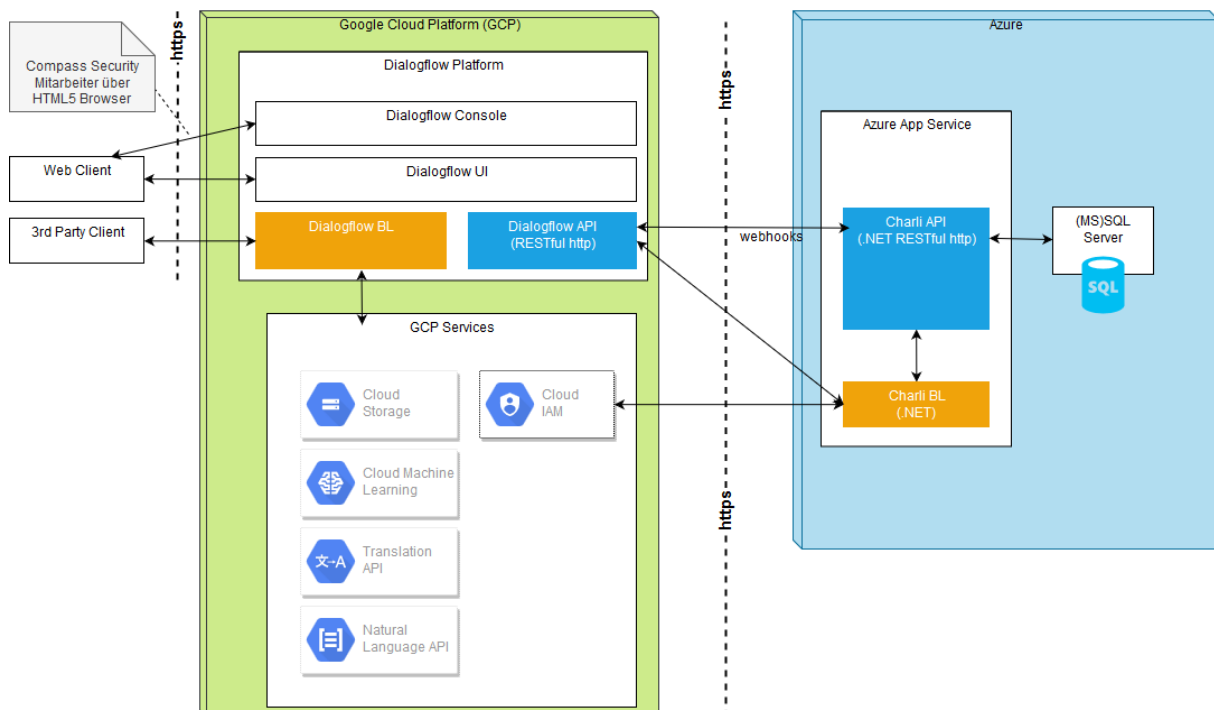


Abbildung 9 Überblick Architektur Variante 1

8.2.3 ÜBERBLICK ARCHITEKTUR VARIANTE 2

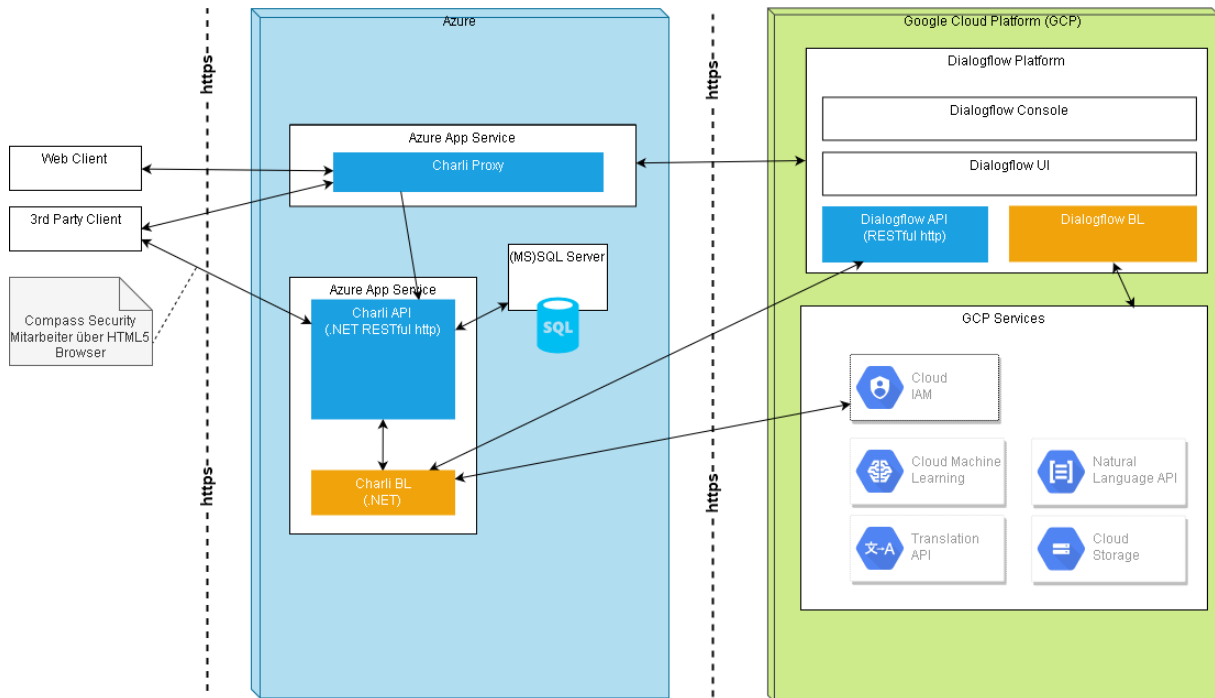


Abbildung 10 Überblick Architektur Variante 2

Es gilt zu beachten, dass die bidirektionalen Kommunikationspfeile keinen Rückschluss darauf geben, von wem die Kommunikation lanciert wird.

8.2.4 VARIANTENVERGLEICH

Variante 1 zeigt, dass die Clients direkt mit Dialogflow kommunizieren. Dialogflow selbst entscheidet wiederum, wann mittels Webhooks mit dem Charli Backend kommuniziert werden soll. Die Entscheidung, ob ein Webhook Aufruf stattfindet, wird vom Inbetriebnehmer oder Charli Supportbeauftragten direkt über das Dialogflow UI konfiguriert.

Variante 2 zeigt, dass die Clients über einen vorgeschalteten Proxy entweder mit Dialogflow oder mit dem Charli Backend kommunizieren. Der Unterschied ist, dass nun die Charli Proxy Anwendung entscheidet, wann ein clientseitiger Aufruf an Dialogflow weiter delegiert wird oder vom Charli Backend behandelt werden soll.

Gegenüberstellung der Varianten:

VARIANTE 1	VARIANTE 2
Einfachere Kommunikation, weniger verteilt und damit weniger komplex	Höherer Kommunikationsaufwand, weil für die Intenterkennung NLP Services innerhalb von Dialogflow aufgerufen werden müssen, bevor überhaupt entschieden werden kann, wie der User Request behandelt werden soll
Einfacheres Deployment, nur ein Web App Service notwendig	Zusätzliche Charli Proxy Komponente, welche hinsichtlich der Last (jeder Client spricht mit dieser Komponente) und des Deployments



VARIANTE 1	VARIANTE 2
Limitierte Möglichkeiten für Features der Prioritäten 2 und 3 gemäss der Anforderungsspezifikation, wie zum Beispiel die Gesprächsübernahme.	Bessere Kontrolle über den Programmfluss. Die Entscheidung wird selbst getroffen, was von Dialogflow bearbeitet wird (eine Form von Inversion of Control). Features wie die unterbrechungsfreie Gesprächsübernahme sind einfacher realisierbar.
Entspricht der bestehenden Prototyparchitektur (zum Zeitpunkt des Meilenstein 3 «Prototyp Alpha»), kein weiterer Aufwand notwendig	Umstellung und Neuentwicklung der Charli Proxy Komponente bringt Aufwand und Risiken für das Projekt
Fokus auf der Dialogflow Technologie mit Ausreizen der Möglichkeiten	Anteil der Eigenentwicklung grösser, damit auch Verwendung der Dialogflow Capabilities reduzierter

Tabelle 28 Gegenüberstellung Architekturvarianten

Die Umsetzung erfolgt in der Variante 1. Ausschlaggebende Gründe sind der Fokus auf Dialogflow und der damit verbundene Aufbau des Technologieknowhow und die Reduktion der Risiken, indem der Anteil der Eigenentwicklung kleiner gehalten wird.

8.2.5 ARCHITEKTUR ENTWURFSMUSTER

Charli wird mit dem relaxierten «Layers» Architektur Entwurfsmuster²⁵ realisiert:

LAYER	BESCHREIBUNG	TECHNOLOGIE
UI	User Interface, bietet Möglichkeit, textbasierten Input an Charli zu senden und textbasierten Output darzustellen	JS / Webclient
BLL	Business Logic Layer: Enthält die Konversationslogik, bildet Dialoge und Konversationsabläufe ab, trifft Entscheidungen (z.B. ob ein Compass Security Mitarbeiter benachrichtigt werden muss)	Dialogflow Google Cloud Platform Services .NET Core / C#
Charli API	Endpoints für «Webhooks ²⁶ » Schnittstelle für CRUD Operationen auf Kundendaten, Konversationszusammenfassungen	.NET RESTful http
DAL	Data Access Layer: ORM für Businessrelevante Daten	.NET/ Entity Framework Core
DL	Data Layer: Persistierte Businessrelevante Daten	SQL

²⁵ Siehe Buch «Pattern oriented Software Architecture» (POSA) 1

²⁶ Konzeptionell sind das Callbacks für usermanaged Code, die registriert werden können, welche dann vom BLL aufgerufen werden



Tabelle 29 Layerübersicht

Mit der Entscheidung einer Layering Architektur wird die Austauschbarkeit einzelner Komponenten verbessert, die Kohäsion erhöht und die Kopplung reduziert. Die damit erhöhten Laufzeitkosten aufgrund der (asynchronen) Kommunikation zwischen den Layers werden in Kauf genommen.

8.2.5.1 USER INTERFACE (UI)

Als User Interfaces können bestehende Chat Applikationen integriert werden, wie zum Beispiel Slack²⁷ oder Telegram²⁸.

Dialogflow bietet selbst ein User Interface für Techniker, um verschiedene Operationen durchzuführen, wie zum Beispiel das Einspeisen von Trainingsdaten, Erstellen oder Editieren von Intents oder Modellierung des Konversationsverlaufs.

Für eine rasche Integration bietet Dialogflow ein einfaches User Interface, welches per iframe²⁹ eingebettet werden kann. Dieses Dialogflow UI ist nur zu Demo Zwecken geeignet, da es nur einfache Textantworten erlaubt.

Die Kommunikation zum Backend findet über Https statt.

8.2.5.2 BUSINESS LOGIC LAYER (BLL)

Die Business Logik ist über mehrere Komponenten verteilt. Der Hauptanteil der Logik wird in Dialogflow mit den Konzepten des NLP³⁰, wie zum Beispiel Intents, Entities und Utterances abgebildet.

Mit Hilfe von «Webhooks» kann eigener Code für die Verarbeitung von Input eingesetzt werden. Dies kommt zum Zug, wenn Charli zusätzliche Informationen abspeichern möchte, gespeicherte Informationen übermittelt oder spezielle Entscheide abhängig von Kontext getroffen werden müssen.

8.2.5.3 CHARLI API

Das Charli API bietet Endpunkte für CRUD Operationen auf persistierten Daten und die «Webhooks», um die WebhookRequest³¹ selber zu behandeln. Das Charli API ist als RESTful http Schnittstelle umgesetzt. Die Endpunkte sind mit SSL/TLS verschlüsselt. Eine https Verbindung ist erforderlich, um das API anzusprechen. Bestimmte Endpunkte sind nur mit einer Authentisierung und / oder Autorisierung benutzbar.

Eine unvollständige (exkl. gültiger, erforderlicher oder optionaler Parameter, Datenstrukturen oder Rückgabetypen) API Definition sieht wie folgt aus:

²⁷ Siehe <https://slack.com>

²⁸ Siehe <https://telegram.org/>

²⁹ Siehe https://www.w3schools.com/tags/tag_iframe.asp

³⁰ Natural Language Processing: Extrahieren der Informationen aus einem Satz und Absicht erkennen

³¹ Siehe API Dokumentation:

<https://cloud.google.com/dialogflow-enterprise/docs/reference/rest/Shared.Types/WebhookRequest>



HTTP METHODE	ENDPUNKT	ERLÄUTERUNG
POST	api/webhook	<ul style="list-style-type: none"> • Webhook Endpunkt für Dialogflow. Akzeptiert eingehende WebhookRequest³² • Antwortet mit einer WebhookResponse
GET	api/conversations	<ul style="list-style-type: none"> • Listet alle Konversation • Autorisierung erforderlich
GET	api/conversations/<conversationId>	<ul style="list-style-type: none"> • Gibt die Konversation mit der ID conversationId zurück • Die conversationId wird anhand der aktuellen Session des Agents generiert, welcher im WebhookRequest mitgeteilt wird • Autorisierung erforderlich

Tabelle 30 API Endpunkte Entwurf

Die aktuelle und vollständige API Dokumentation wird mittels API Dokumentationswerkzeug «Swagger³³» bereitgestellt.

8.2.5.4 DATA ACCESS

Für den Zugriff auf persistente Daten wird Entity Framework Core verwendet. Dies ist der weitverbreitete und bestens integrierte OR Mapper für .NET.

8.2.5.5 DATEN

Daten werden in einer relationalen Datenbank mit MSSQL persistiert.

8.3 DEPLOYMENT

8.3.1 DEPLOYMENT ABSICHT

Der Chatbot wird mit dem «cloud first» Ansatz realisiert.

Dialogflow, das eingesetzte Bot Framework, läuft als Service innerhalb der Google Cloud Platform.

Das Backend mit der Datenhaltung und Business Logik wird als .NET Web Applikation in Azure als Azure App Service deployed.

Zusätzlich wird eine alternative Release Pipeline eingerichtet, um das Backend in einem Docker Container Image auszuführen.

Auf Angaben zur verwendeten Hardware oder Infrastruktur wird verzichtet, weil dies bei der Nutzung von SaaS oder Paas Providern Teil der Abstraktion darstellt und nicht im Fokus steht. Zudem sind Cloud Lösungen «on demand», d.h. es wird bezahlt, was benötigt wird. Die dabei verwendeten Ressourcen können variieren.

³² WebhookRequest:

https://dialogflow.com/docs/reference/v1-v2-migration-guide-fulfillment#webhook_request

³³ siehe <https://swagger.io/>

8.4 DOMAINANALYSE

Nachfolgendes Domainmodell zeigt grob die Beziehungen zwischen den für Charli relevanten Entitäten:

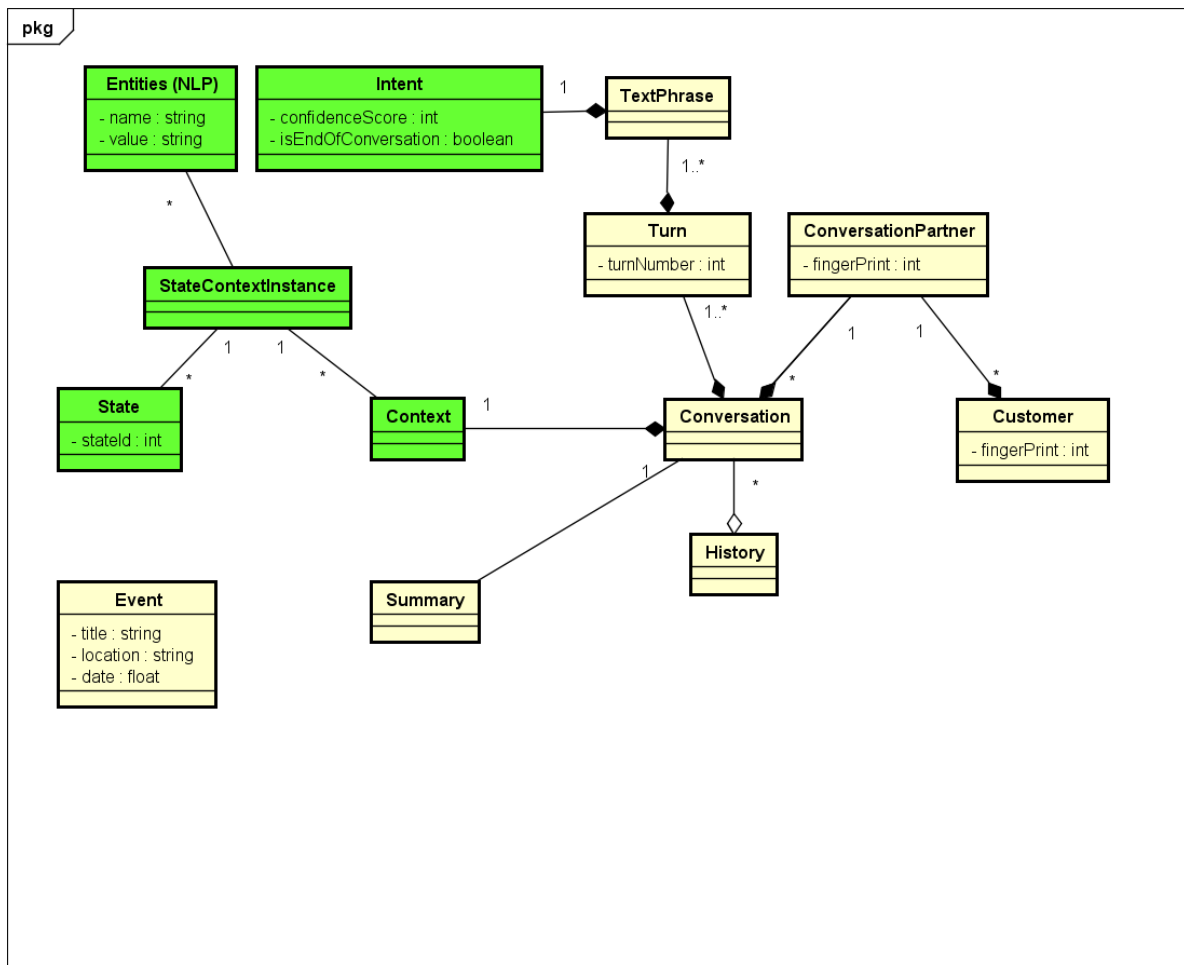


Abbildung 11 Domainmodellierung

Das Model ist bewusst einfach gehalten, Attribute und Methoden wurden zwecks Übersichtlichkeit weggelassen.

Grün eingefärbt sind die Entitäten, welche stark an die vorgegebenen Strukturen des Dialogflow SDK angelehnt sind.

Für das Erfüllen der MA Use Cases 8, 10, 11, 12 und 13 existiert bereits ein Service von Dialogflow.

Use Case 9, Lesen und Löschen von Zusammenfassungen, kann mit Hilfe der Summary Entität bewerkstelligt werden.

Use Case 14, CRUD Kundendaten, kann dadurch erfüllt werden, dass Gesprächspartner mittels «fingerprint» erkannt werden und einem bestehenden Customer zugeordnet werden können.

Use Case 15, Benachrichtigung einrichten, wird erfüllt, indem anhand des boolean «isEndOfConversation» im eingehenden Intent die Benachrichtigung ausgelöst wird.

8.5 KONVERSATIONSABLAUF

8.5.1 SEQUENZEN

Zur Veranschaulichung der wichtigsten Abläufe dienen folgende Sequenzdiagramme:

8.5.1.1 KONTAKTAUFNAHME

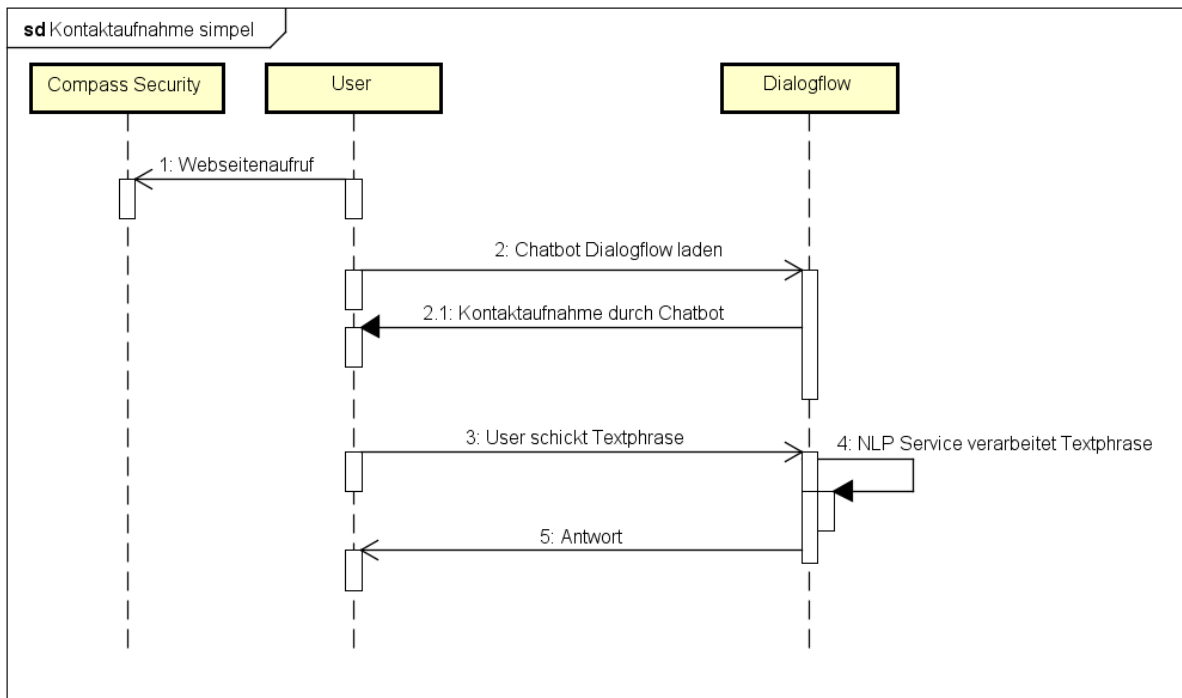


Abbildung 12 Kontaktaufnahme simpel

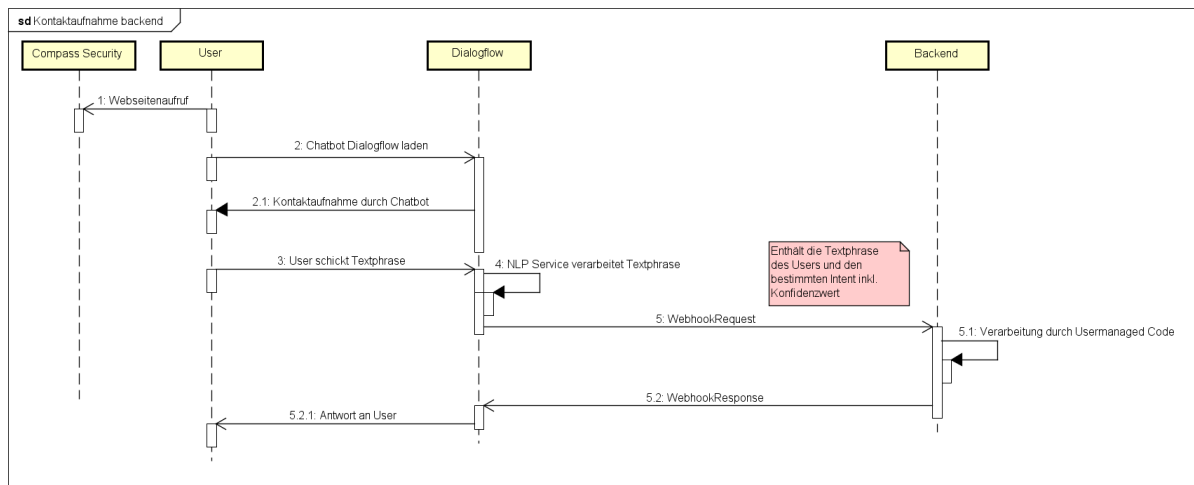


Abbildung 13 Kontaktaufnahme mit Backend

Die Kontaktaufnahme wird durch den User gestartet, indem er das Chatbot UI im Browser lädt.

8.5.1.2 SINGLE TURN CONVERSATION

Single turn Conversation beschreibt eine Sequenz einer Frage oder Aussage des Users und die dazugehörige Antwort oder Reaktion des Chatbot (Ping Pong Prinzip).

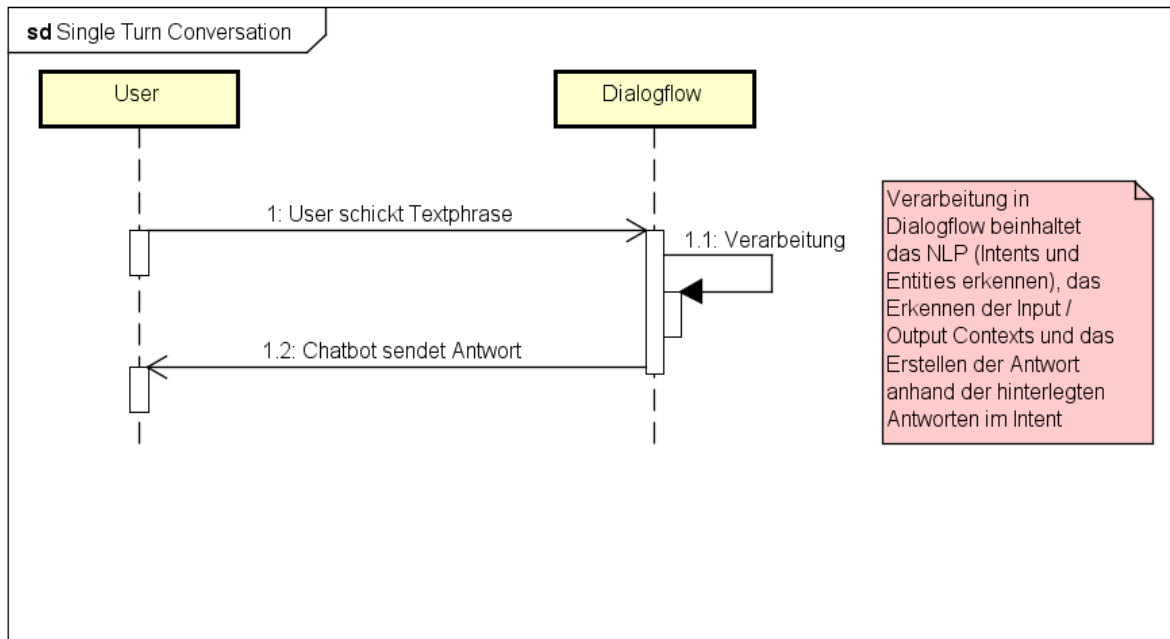


Abbildung 14 Single Turn

8.5.1.3 GESPRÄCHSABBRUCH DURCH USER

Ein Gesprächsabbruch findet statt, wenn vom User nach einer bestimmten Zeit (in Dialogflow nach 20 Minuten) keine Textphrase mehr kommt.

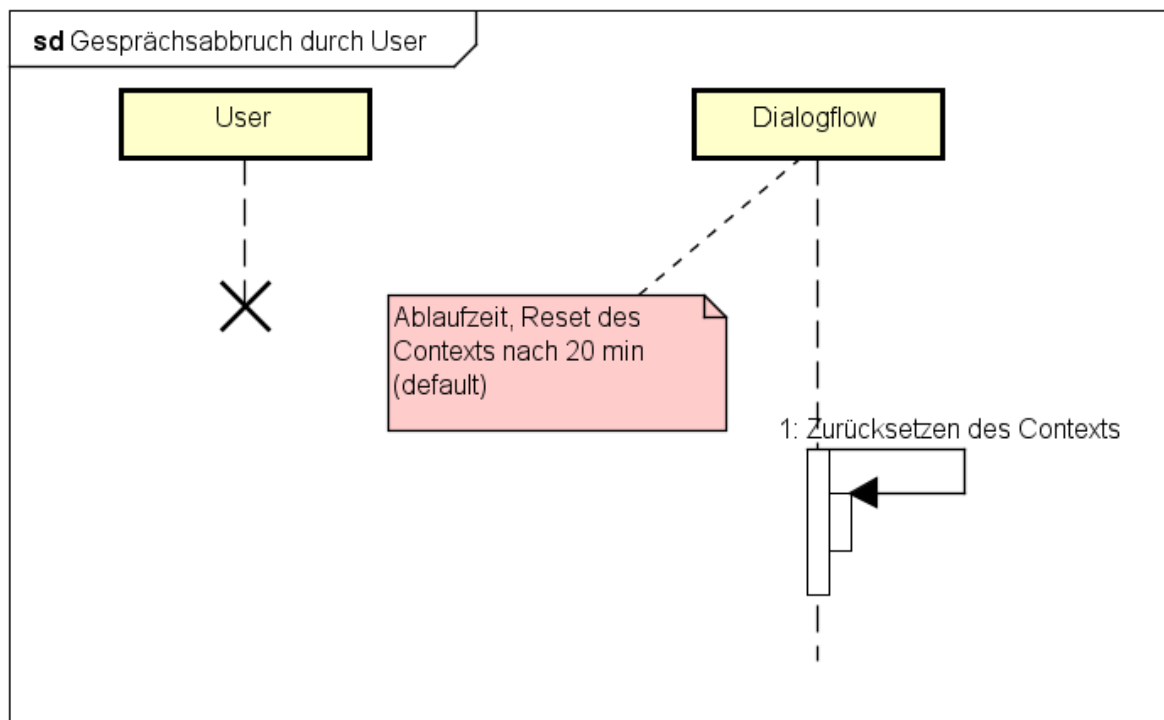


Abbildung 15 Gesprächsabbruch durch User

8.5.1.4 GESPRÄCHSÜBERNAHME

Eine Gesprächsübernahme kann grundsätzlich spontan, durch den Mitarbeiter initiiert oder durch die erkannte Absicht des Users, mit einem Menschen zu sprechen, ausgelöst werden. Bei einer Gesprächsübernahme werden alle Textphrasen ohne Verarbeitung über das Backend an den Mitarbeiter weitergeleitet und durch diesen beantwortet.

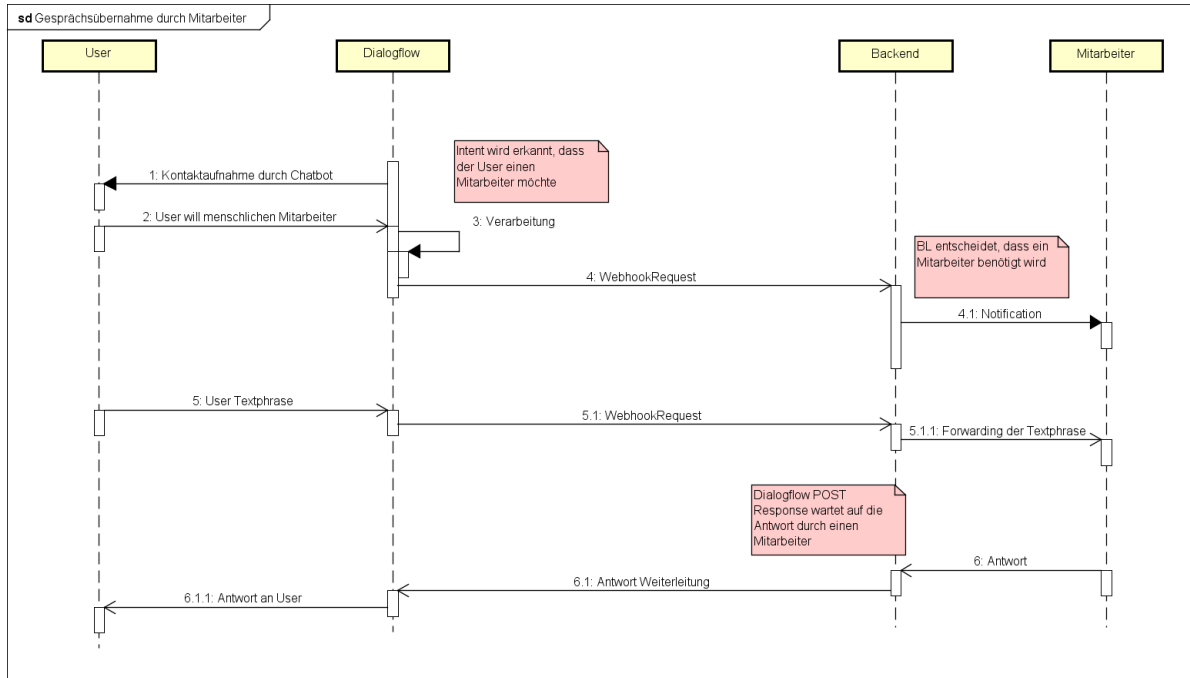


Abbildung 16 Gesprächsübernahme durch Mitarbeiter

8.6 GESPRÄCHSMODELLIERUNG

8.6.1 GESPRÄCHSMODELL KONZEPT

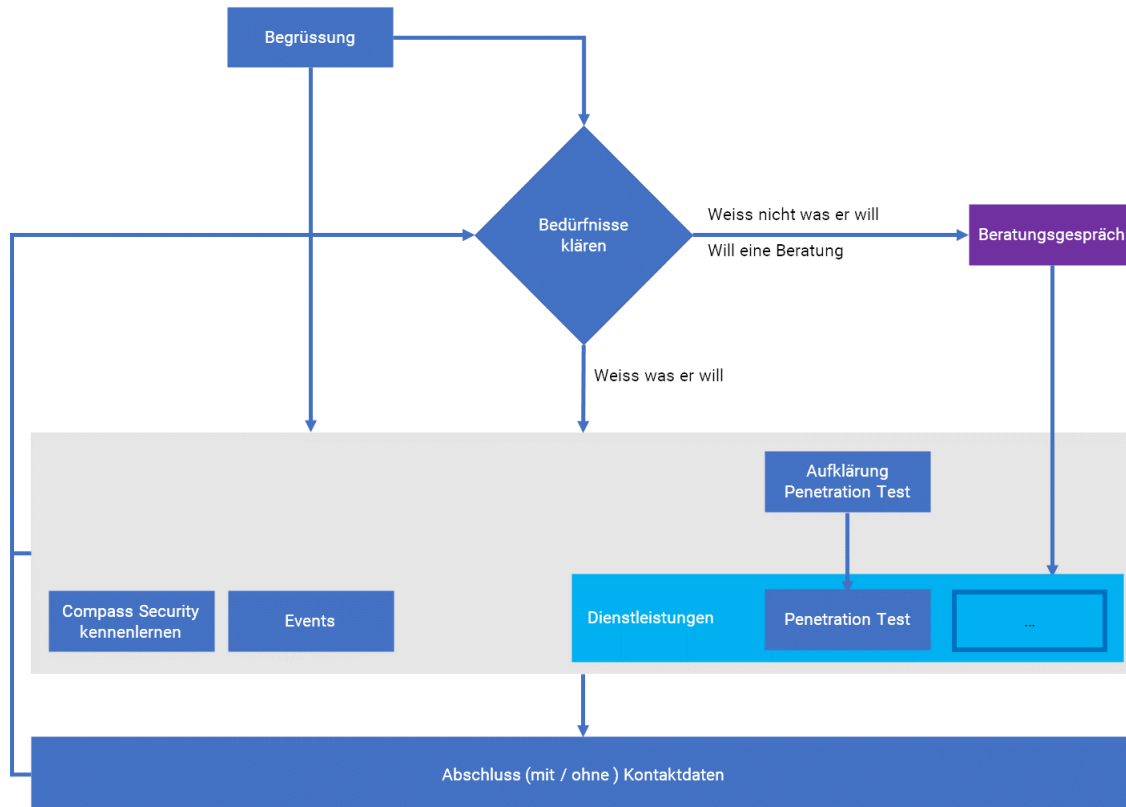


Abbildung 17 Gesprächsmodell Konzept

Die Abbildung zeigt den konzeptionellen Ablauf eines Gesprächs. Zentrale Aspekte sind das Bedürfnis klären und das Beratungsgespräch.

Erfolgreiche Durchgänge in den Boxen im grauen Kasten führen zum Abschluss und dem Sammeln von Kontaktdaten. Durch eine Rückkopplung zum «Bedürfnisse klären» können mehrere Dienstleistungen angeboten oder Informationen geteilt werden. Diese Rückkopplung kommt auch immer dann zum Zuge, wenn der User signalisiert, dass es sich um die falsche Dienstleistung oder Information handelt.

Nachfolgend werden die einzelnen Elemente des Konzeptdiagramms beschrieben.

8.6.2 BEGRÜSSUNG

Beginn der Konversation. Wenn der Kunde den Chatbot anspricht, wird er von diesem begrüsst und erklärt ihm die Möglichkeiten für das folgende Gespräch.

8.6.3 BEDÜRFNISSE KLÄREN

Beim «Bedürfnisse klären» geht es darum, zu entscheiden, ob der User ein Beratungsgespräch wünscht oder benötigt oder nicht.



8.6.4 BERATUNGSGESPRÄCH

Beim «Beratungsgespräch» geht es darum, den User mit gezielten Fragen zu klassifizieren und ihn zu den treffendsten Boxen (im grauen Kasten) weiterzuleiten, wo Slot Filling für die einzelnen Unterkategorien betrieben wird. Im Beratungsgespräch findet auch das Erklären statt. Das Ziel ist es, den User soweit aufzuklären, dass er in der Lage ist zu entscheiden, ob die vorgeschlagenen Dienstleistungen seinen Bedürfnissen entsprechen.

Eine Klassifikation kann auch zu einem Vorschlag für mehrere Dienstleistungen oder Phasen führen. Ein Beispiel dafür könnte der Vorschlag sein, in einer ersten Phase ein Security Training durchführen zu lassen und in einer zweiten Phase einen Angriff mittels Social Engineering zu fahren.

8.6.5 AUFKLÄRUNG PENETRATION TEST

Für jede Dienstleistung wird eine Aufklärungsbox vorgeschaltet, welche vom User durchschritten wird, wenn er nicht vom Beratungsgespräch kommt. Diese «Aufklärungsboxen» sind global erreichbare Zustände. Damit wird sichergestellt, dass die Dienstleistungsboxen nicht direkt angesprungen werden können. Dies hat den Vorteil, dass versehentliche Slot Filling Phasen verhindert werden. Gleichzeitig kann der Chatbot den User über die Dienstleistung aufklären und sicherstellen, dass die Dienstleistung auch wirklich das Gewünschte darstellt. In diesen Aufklärungsboxen wird also eine Zusage vom User erwartet, bevor in die eigentliche Dienstleistungsbox weitergeleitet wird.

8.6.6 DIENSTLEISTUNGEN

Alle Dienstleistungen der Compass Security.

8.6.6.1 PENETRATION TEST

Der eigentliche Penetration Test Intent, wo mit Hilfe des Slot Filling Verfahrens alle benötigten Informationen gesammelt werden.

8.6.6.2 WEITERE DIENSTLEISTUNGEN

Weitere Dienstleistungen wurden nicht oder nur teils implementiert. Konzeptionell werden weitere Dienstleistungen analog eingefügt. In der Benutzeranleitung im Anhang D wird die Vorgehensweise beschrieben.

8.6.7 EVENTS

Der Kunde erhält Informationen zu bevorstehenden Veranstaltungen oder Events, wo die Compass Security beteiligt ist oder selbst organisiert.

8.6.8 COMPASS SECURITY KENNENLERNEN

Der Kunde erhält allgemeine Informationen über das Unternehmen.

8.6.9 ABSCHLUSS MIT / OHNE KONTAKTDATEN

Jede Konversation wird mit oder ohne Kontaktdaten abgeschlossen. Dies hängt davon ab, ob sich der Kunde weiteren Kontakt wünscht.

8.6.10 KONZEPTE ZUR MODELLIERUNG IN DIALOGFLOW

Die Modellierung des Gesprächs ist auf einer konzeptionellen Ebene als Zustandsautomat abgebildet. Dabei spiegeln die Intents (Absichten des Kunden), gepaart mit den Contexts die Zustände wieder. Zustandsübergänge werden modelliert, indem zu den Intents jeweils Input- und Output Contexts miteinander verknüpft werden oder der NLP Service ein Match zu einer Trainingsphrase eines Intents erkennt.

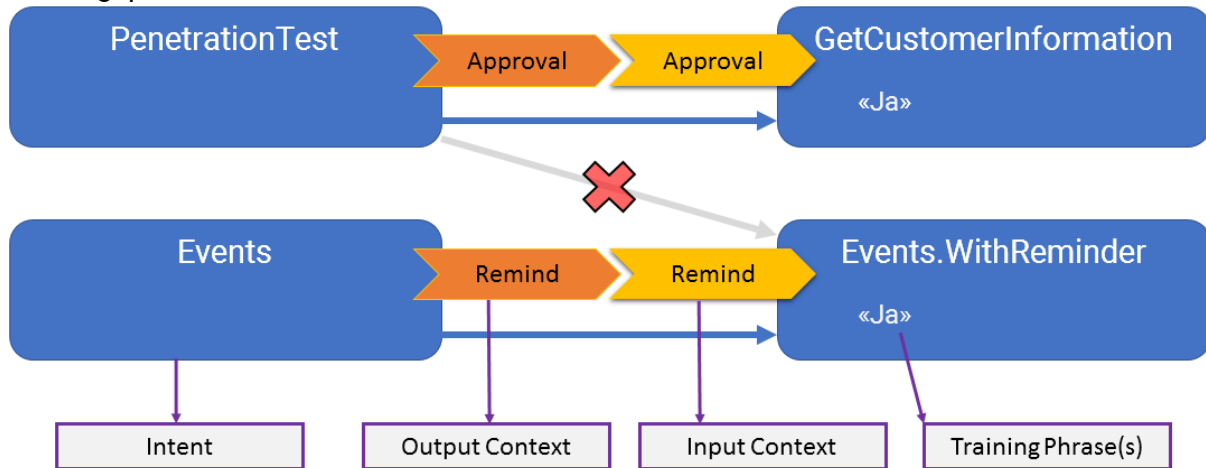


Abbildung 18 Konzept Gesprächsablauf in Dialogflow

Die Abbildung zeigt, wie mit Output- und Input Contexts die Übergänge modelliert werden. Das Verknüpfen der Intents mit Contexts ist dann notwendig, wenn sich in zwei Intents, identische Trainingsphrasen befinden. Damit wird sichergestellt, dass in den korrekten Intent gewechselt wird.

Es kann vorkommen, dass einige Informationen vom Benutzer benötigt werden, bevor das Gespräch weitergeführt werden kann. In diesem Fall werden mit dem «Slot Filling» Verfahren alle benötigten Informationen «abgefüllt», ehe in den nächsten Zustand gewechselt wird.

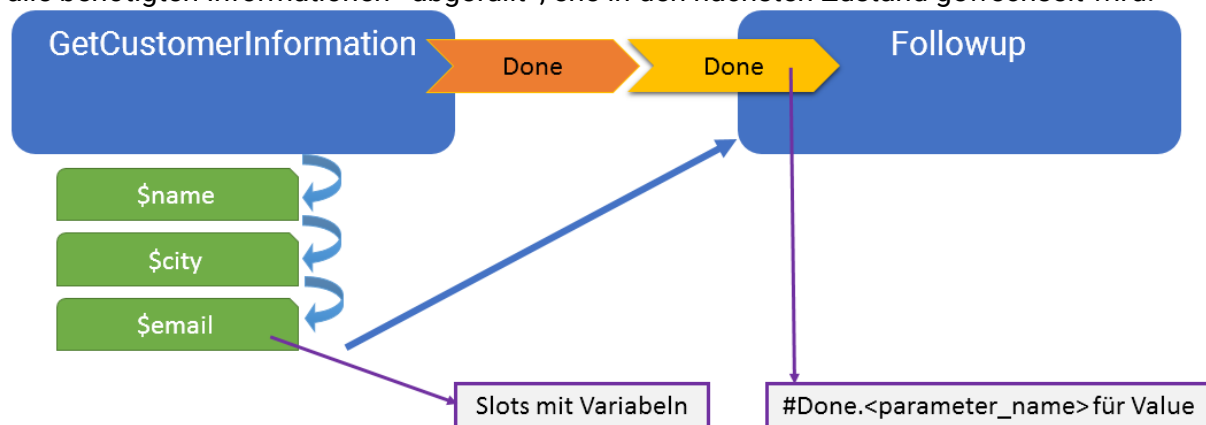


Abbildung 19 Konzept Slot Filling in Dialogflow

Damit Dialogflow einen Wert für die Variable innerhalb eines «Slots» setzen kann, werden «Entities» eingesetzt. Weitere Informationen zu Entities finden sich im Kapitel «Entities».

8.6.11 INTENTS

Damit Charli die Absichten des Kunden erkennen kann, müssen diese als Katalog mit entsprechenden Trainingsphrasen bekannt gemacht werden. Das Erfassen und Bearbeiten der Intents geschieht über die Dialogflow Benutzeroberfläche oder per Dialogflow API Aufrufe.

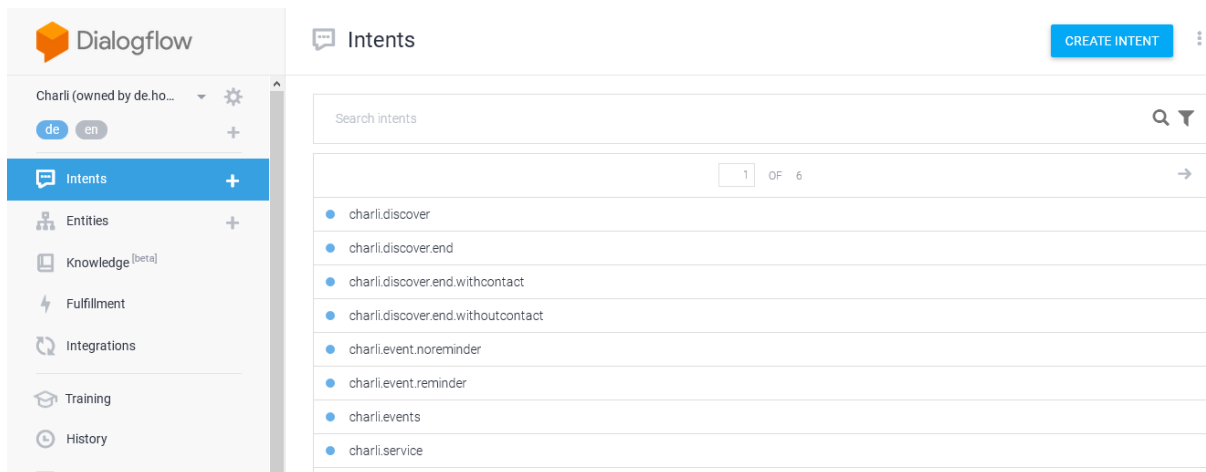


Abbildung 20 Intents in Dialogflow

Auf eine vollständige Liste der möglichen Intents wird hier bewusst verzichtet, da diese iterativ und mit überwachtem Training erfasst und verfeinert werden.

8.6.12 ENTITIES

Ein Entity beschreibt eine Sache, einen Wert oder eine Information. Dialogflow bietet vorgefertigte System Entities, wie zum Beispiel **@sys.geo-city**, welches alle grösseren Städte beinhaltet. Dialogflow prüft die Eingabe des Users und füllt den richtigen Slot aus, wenn der Wert im Katalog des Entities gefunden wurde.

Weiter können auch eigene Entities definiert werden, damit zum Beispiel Enumerationen («keine Erfahrung», «ein wenig Erfahrung», «viel Erfahrung») abgebildet werden können.

8.6.13 CONTEXTS

Dialogflow nutzt Contexts, um den Gesprächsfluss, die Gesprächsverzweigungen und den Konversationszustand zu managen.

Contexts enthalten die Werte der Entities und Parameter, welche bislang erkannt wurden. Auf die Werte zugegriffen wird mit der Syntax **#<context_name>.<parameter_name>**.

Context haben eine Lebensdauer (dargestellt als Ganzzahl). Übersteigt die Anzahl Turns mit dem Agenten die Lebensdauer oder findet über zwanzig Minuten keine Interaktion mit dem Agenten statt, werden Contexts gelöscht.

Output Contexts können auch zurückgesetzt werden, indem die Lebensdauer auf 0 gesetzt wird. Dies kann nützlich sein, wenn für Follow-up Intents bestimmte Contexts nicht mehr relevant sind.

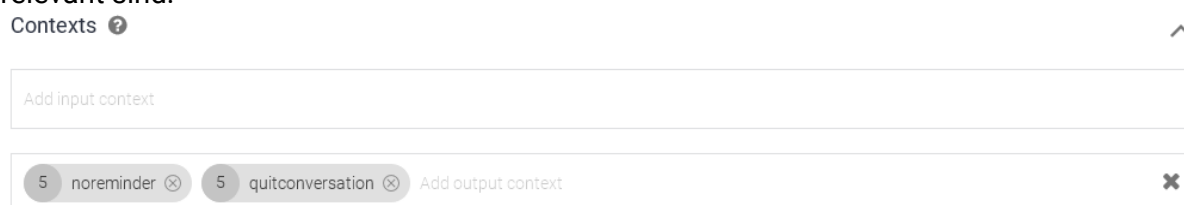


Abbildung 21 Contexts in Dialogflow

8.6.14 GESPRÄCHSVERZWEIGUNGEN

Gesprächsverzweigungen werden realisiert, indem die vorgestellten Konzepte kombiniert werden.

1. Intent matching nutzen, um in einen Intent zu springen



2. Mit Hilfe von Input- und Output Contexts den Gesprächsverlauf steuern und einschränken

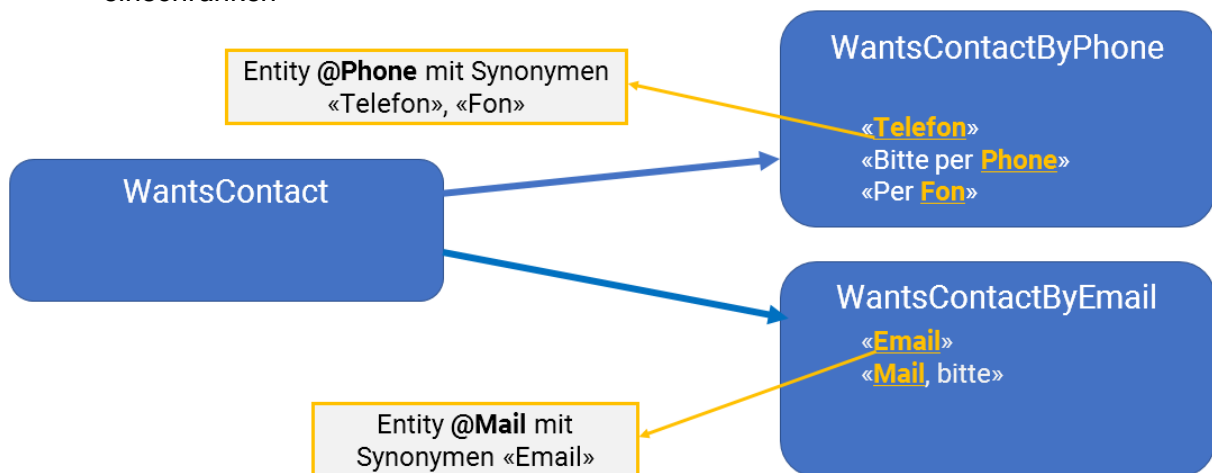


Abbildung 22 Beispiel Gesprächsverzweigung mit Intentmatching und Entities

8.6.15 FULFILLMENT

Müssen persistierte Werte zurückgegeben werden oder besteht die Notwendigkeit, Benutzercode auszuführen, wird dies mit Hilfe von Webhooks gelöst. Webhooks können pro Intent oder global eingerichtet werden. Weitere Informationen sind im Kapitel «Charli API» zu finden.



9. REALISIERUNG

9.1 ÜBERSICHT

Das folgende Kapitel geht auf die Implementierung und den IST Zustand ein. Er gliedert sich in die Teilbereiche Dialogflow (Frontend und Gesprächsmodellierung) und einem Backend unter .NET und Azure.

9.2 DIALOGFLOW GESPRÄCHSMODELLIERUNG ÜBERSICHT

Der aktuelle Stand der Gesprächsmodellierung in Dialogflow ist im Anhang A ersichtlich.

9.3 DIALOGFLOW CHARLI INTENTS

Im Kern der Gesprächsmodellierung stehen die Intents. Für die Bachelorarbeit wurde der Fokus auf die Dienstleistung «Penetration Test» gelegt. Die Intents für weitere Dienstleistungen wurden zu Testzwecken erstellt, jedoch nicht in die Tiefe umgesetzt.

9.3.1 COMPANY.INFO

Wird verwendet, um die Firmeninformationen des Kunden zu erhalten. Wenn alle benötigten Informationen des Kunden erhalten wurden, wird in diesen Intent gewechselt um einen Abschluss zu ermöglichen.

FOLLOW-UP	BESCHREIBUNG
person.infos	Nachdem der Chatbot die Firmeninformationen erhalten hat, benötigt er nun die Informationen zur Person selbst und schliesst das Gespräch ab.

Tabelle 31 Follow-up zu company.infos

9.3.2 GLOBAL.CONSULTING

Wird verwendet, wenn sich der Kunde eine Beratung wünscht.



● global.consulting ^
● ↳ cs.employee
🔖 ↳ global.consulting - fallback Contexts: CSconsulting-followup, globalconsulting-followup
● ↳ consulting ^
● ↳ consulting.securitytraining
● ↳ consulting.securityreview ^
🔖 ↳ consulting.security.review.fallback Contexts: consultingsecurityreview-followup
● ↳ security.review.reason.hacking ^
● ↳ security.review.recommendation
● ↳ consulting.pt ^
● ↳ pt.reason.hacking ^
● ↳ pt.recommendation ^
● ↳ consulting.contact
● ↳ pt.reason.executive.board
● ↳ pt.reason.safety.check
● ↳ pt.reason.new.product
🔖 ↳ consulting.pt.fallback Contexts: consultingpenetration-followup
● ↳ consulting.dfir
● ↳ consulting.noidea ^
● ↳ noidea.person.infos

Abbildung 23 Dialogflow Intentübersicht Screenshot

FOLLOW-UP	BESCHREIBUNG
cs.employee	Wird verwendet, wenn der Kunde sich eine Beratung per Telefon mit einem Compass Security Mitarbeiter wünscht. Anschliessender Wechsel zu «company.infos».
consulting	Wird verwendet, wenn sich der Kunde eine Beratung über Chat wünscht.
consulting.securitytraining	Wird verwendet, wenn sich der Kunde eine Beratung über die Dienstleistung Security Review wünscht. Wurde in dieser Bachelorarbeit nicht implementiert.
consulting.securityreview	Wird verwendet, wenn sich der Kunde eine Beratung über die Dienstleistung Security Review wünscht. Wurde in dieser Bachelorarbeit nicht implementiert.
security.review.reason.hacking	Wenn sich der Kunde ein Security Review wünscht, weil er gehackt wurde wird dieser Intent verwendet.



FOLLOW-UP	BESCHREIBUNG
security.review.recommendation	Gibt dem Kunden eine Empfehlung, ob dies die richtige Dienstleistung ist oder eine andere seinen Anforderungen besser entsprechen würde.
consulting.pt	Wird verwendet, wenn sich der Kunde eine Beratung über die Dienstleistung Security Review wünscht. Wurde in dieser Bachelorarbeit nicht implementiert.
pt.reason.hacking	Der Kunde gibt an, dass er gehackt wurde und deswegen eine Beratung wünscht.
pt.recommendation	Gibt dem Kunden eine Empfehlung, ob dies die richtige Dienstleistung ist oder eine andere seinen Anforderungen besser entsprechen würde.
consulting.contact	Der Kunde möchte die Dienstleistung mit einem Compass Security Mitarbeiter telefonisch bestellen.
pt.reason.executive.board	Der Kunde gibt an, dass der Vorstand sich einen Penetration Test wünscht.
pt.reason.safety.check	Der Kunde gibt an, dass er einen Sicherheitscheck benötigt.
pt.reason.new.product	Der Kunde gibt an, dass er ein neues Produkt ins Netzwerk migriert hat und nun das Netzwerk testen möchte.
consulting.dfir	Wird verwendet, wenn sich der Kunde eine Beratung über die Dienstleistung DFIR wünscht. Wurde in dieser Bachelorarbeit nicht implementiert.
consulting.noidea	Falls der Kunde nicht weiss, welche Art von Beratung er möchte, wird der Chatbot in diesen Intent wechseln.
noidea.person.infos	Der Kunde möchte telefonisch mit einem Compass Security Mitarbeiter beraten werden.

Tabelle 32 Follow-up Intents

9.3.3 GLOBAL.CONTACT.PERSON

Wird verwendet, wenn der Kunde telefonisch kontaktiert werden soll. Nach diesem Intent wird das Gespräch beendet.

9.3.4 GLOBAL.DFIR

Wird verwendet, wenn der Kunde die Dienstleistung Digital Forensics und Incident Response bestellen möchte. Wurde in dieser Bachelorarbeit nicht implementiert.



9.3.5 GLOBAL.DISCOVER

Dieser Intent informiert den Kunden über die Compass Security.

●	global.discover ^
🔖	↳ global.discover - fallback Contexts: globaldiscover-followup, discover-followup
●	↳ discover.end ^
●	↳ end.with.contact ^
●	↳ discover.person.infos
🔖	↳ discover.end - fallback Contexts: endconversation-followup, discoverend-followup
●	↳ end.without.contact

Abbildung 24 Dialogflow global.discover Screenshot

FOLLOW-UP	BESCHREIBUNG
discover.end	Wenn der Kunde das Gespräch beenden möchte, wird er gefragt, ob sich ein Compass Security Mitarbeiter bei ihm melden sollte.
end.with.contact	Der Kunde wünscht sich weiteren Kontakt.
end.without.contact	Das Gespräch wird beendet, da der Kunde keinen weiteren Kontakt wünscht.
discover.person.infos	Der Kunde gibt seine Informationen an, um später telefonisch kontaktiert zu werden. Das Gespräch wird beendet.

Tabelle 33 Intents zu discover

9.3.6 GLOBAL.EVENTS

Der Kunde erhält Informationen über den nächsten Event. Ihm wird angeboten, sich in die Mailingliste der Compass Security einzutragen.

FOLLOW-UP	BESCHREIBUNG
events.end	Das Gespräch wird beendet.

Tabelle 34 Intents zu event



9.3.7 GLOBAL.KILLER.QUESTIONS

Der Kunde wirft der Compass Security etwas Negatives vor. Der Chatbot bedankt sich fürs Feedback und beendet das Gespräch. Nur teilimplementiert, weil für alle «Killer Fragen» eine generische Antwort und keine spezifischen Antworten gemäss Killer Fragen Antwortkatalog zurückgegeben wird.

9.3.8 GLOBAL.NEEDS

Falls der Kunde Unsicherheit zeigt mit Texteingaben wie «ich denke ich bin nicht sicher», landet er in diesem Intent. Dem Kunden wird angeboten, sich beraten zu lassen. Danach sollte er in den Intent «global.consulting» wechseln.

9.3.9 PT

In diesem Intent wird der Penetration Test bestellt. Durch Slot Filling werden dem Kunden einige Fragen gestellt, welche für eine Offerte benötigt werden. Danach wechselt er in den Intent «company.infos».

9.3.10 GLOBAL.PT.ENTLIGHTENMENT

Wenn der Kunde direkt einen Penetration Test bestellen möchte, wird er zuerst gefragt, ob er Erfahrungen hat und was der Grund für seinen Wunsch ist. Die enthaltenden Fragen in diesem Intent wurden vom «pt» ausgelagert, um nicht redundante Fragen zu stellen. Wenn der Kunde durch die Beratung einen Penetration Test möchte, sollten ihm nicht die gleichen Fragen zweimal gestellt werden.

9.3.11 GLOBAL.SECURITY.REVIEW

Wird verwendet, wenn der Kunde die Dienstleistung Security Review bestellen möchte. Wurde in dieser Bachelorarbeit nur auf oberster Ebene implementiert.

FOLLOW-UP	BESCHREIBUNG
security.review.os	Nach den benötigten Informationen wechselt der Chatbot in den «company.infos» Intent.
security.review – previous	Kann den Kunden zum vorherigen Intent führen. Wurde in dieser Bachelorarbeit nicht implementiert.

Tabelle 35 Intents zu global.security.review



9.3.12 GLOBAL.SECURITY.TRAINING

Wird verwendet, wenn der Kunde die Dienstleistung Security Review bestellen möchte. Wurde in dieser Bachelorarbeit nur auf oberster Ebene implementiert.

FOLLOW-UP	BESCHREIBUNG
security.training – previous	Kann den Kunden zum vorherigen Intent führen. Wurde in dieser Bachelorarbeit nicht implementiert.

Tabelle 36 Intents zu global.security.training

9.3.13 GLOBAL.SERVICE

Der Kunde möchte sich alle Dienstleistungen der Compass Security anzeigen lassen.

FOLLOW-UP	BESCHREIBUNG
service.interestUnspecified	Falls der Kunde keine klare Antwort gibt, wird er nochmals gefragt, ob er Interesse an einer Dienstleistung hat.
service.nointerest	Falls der Kunde kein Interesse hat wird das Gespräch beendet.

Tabelle 37 Intents zu global.service

9.3.14 GLOBAL.WELCOME

In diesem Intent wird der Kunde willkommen geheissen und über die Möglichkeiten der Konversation aufgeklärt.

9.3.15 FALLBACKS

9.3.16 DEFAULT FALLBACK

Dieser globale Fallback, auch Default Fallback Intent genannt, kommt zum Zug, wenn kein anderer Intent oder Fallback Intent in Frage kommt. Dem Kunden wird zuerst mitgeteilt, dass der Chatbot ihn nicht verstanden hat. Danach fragt der Chatbot den Kunden, ob sich ein Compass Security Mitarbeiter bei ihm telefonisch melden sollte.

9.3.17 FOLLOW-UP FALLBACK

In der folgenden Tabelle wird aufgelistet, wo sich die definierten Fallbacks befinden.

FOLLOW-UP FALLBACK PARENT
company.infos

**FOLLOW-UP FALLBACK PARENT**

consulting.securityreview

consulting.pt

global.discover

discover.end

global.events

global.service

Tabelle 38 Fallback zu Follow-up Intents

9.4 DIALOGFLOW CHARLI ENTITIES

Charli verwendet zu den System Entities auch eigene Entities. Im Folgenden werden diese beschrieben.

ENTITIES	BESCHREIBUNG	INTENT
@recommendation	Wer die Compass Security dem Kunden empfohlen hat	person.infos discover.end events.end global.security.review
@service	Hier sind die Dienstleistungen der Compass Security hinterlegt	consulting.securitytraining consulting.securityreview consulting.pt global.dfir pt global.pt.enlightenment global.security.review global.security.training
@experiences	Wie viele Erfahrungen der Kunde mit Dienstleistungen hat	consulting.securitytraining consulting.securityreview consulting.pt global.pt.enlightenment consulting.dfir
@simpleresponses	Kurze Antworten	consulting.noidea



ENTITIES	BESCHREIBUNG	INTENT
@attacker	Mögliche Angreifer	pt global.security.training
@attack	Mögliche Attacken	pt global.security.training
@white-blackbox	Testing Methode	pt
@testaccount	Zugang zum Kunden Netzwerk	pt
@knowaboutit	Wer in der Firma des Kunden vom Test wissen sollte	pt
@reason	Der Grund für den Test	global.pt.enlightenment global.security.review

Tabelle 39 Eigene Entities

9.5 BACKEND

Das Backend wurde in .NET realisiert und gliedert sich in die folgenden Teilprojekte:

PROJEKTNAME	BESCHREIBUNG
poccharli.api	Implementation des RESTful http Web API
poccharli.data	Datenmodell der Charli Anwendung
poccharli.service	Implementiert den Service und Data Access Layer
poccharli.service.test	Testprojekt für den Service und Data Access Layer

Tabelle 40 Backend Projektüberblick

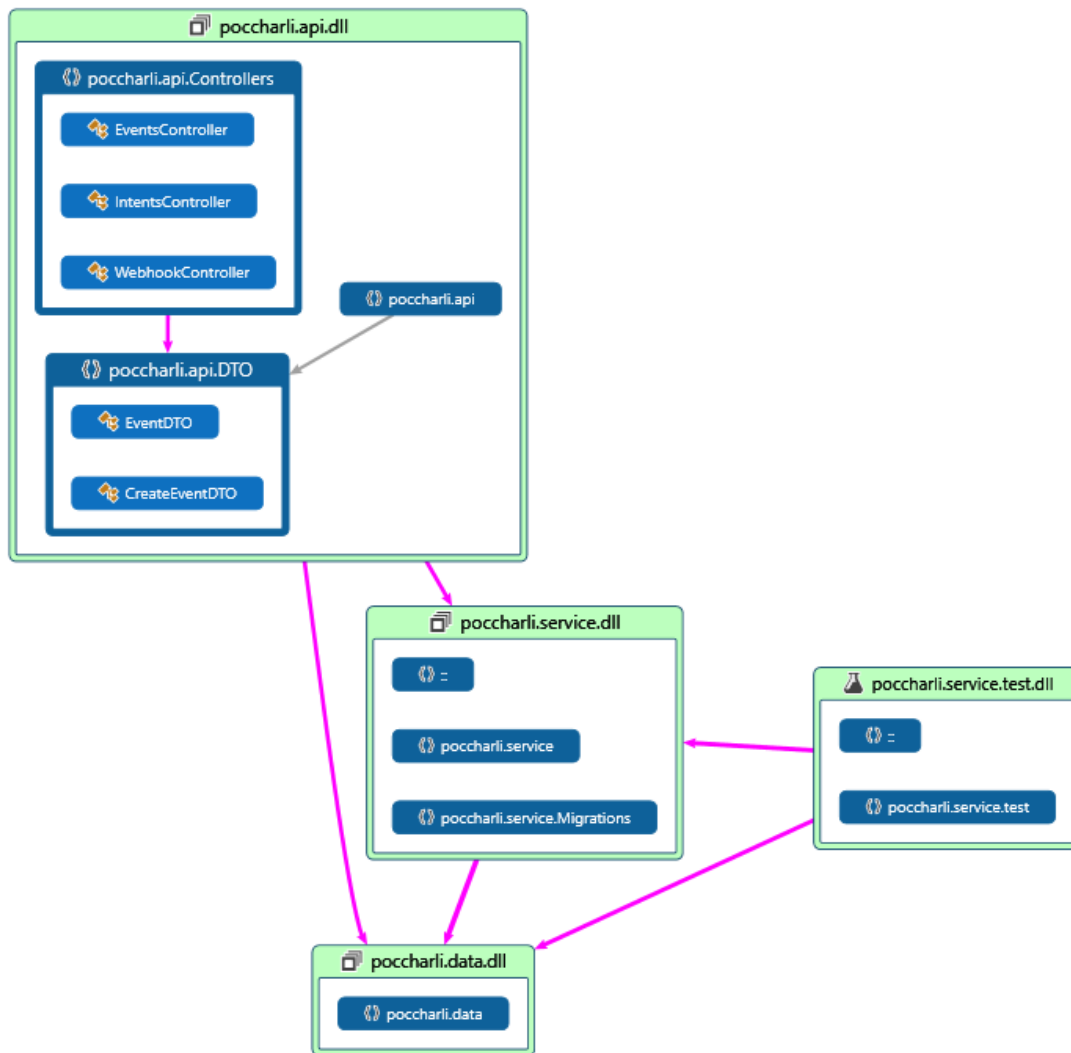


Abbildung 25 Backend Abhängigkeitsdiagramm

9.5.1 API

Das Web API wurde mit Asp.NET Core 2.x implementiert. Für die Dokumentation der API wird Swagger eingesetzt und kann über die Route /swagger aufgerufen werden. Die aktuelle API Dokumentation ist im Anhang I in Form des originalen swagger.json File hinterlegt. Die Kommunikation wird über SSL verschlüsselt.



Charli Web API ^{v1}

</swagger/v1/swagger.json>

Events

GET

`/api/Events`

POST

`/api/Events`

DELETE

`/api/Events/id`

Intents

GET

`/api/Intents`

GET

`/api/Intents/{id}`

Models

Abbildung 26 Überblick Web API Endpoints mit Swagger UI

ENDPUNKT	BESCHREIBUNG
POST /api/webhook	Empfängt WebhookRequest und antwortet mit WebhookResponse . Aufgrund der Verwendung der Google.Cloud.Dialog Klassen ist dieser Endpunkt mit Swagger inkompatibel und wurde aus der API Dokumentation exkludiert.
GET /api/Events	Listet alle bevorstehenden Events auf.
POST /api/Events	Erlaubt das Hinzufügen eines neuen Events
DELETE /api/Events	Erlaubt das Löschen eines neuen Events



ENDPUNKT	BESCHREIBUNG
GET /api/Intents	Listet alle Intents aus Dialogflow. Diese werden über den IntentsClient des Google.Cloud.Dialogflow.V2 Packages über das Dialogflow API ausgelesen. Für den API Zugang sind die Credentials (DialogflowCredentials.json) in der Projektmappe hinterlegt.
GET /api/Intents/{id}	Retourniert den Intent mit dem Bezeichner «id» (analog zu /api/Intents)

Tabelle 41 API Endpunkte Umsetzung

Nachfolgende Abbildung zeigt die eingesetzten Data Transfer Objects (DTO):

Models

UnauthorizedResult >

```
EventDTO {
  id           integer($int32)
  date         string($date-time)
  title        string
  location     string
  description  string
}
```

```
CreateEventDTO {
  date         string($date-time)
  title        string
  location     string
  description  string
}
```

BadRequestResult >

OkResult >

NotFoundResult >

Tabelle 42 DTO

Die DTO's sind trivial, weshalb nicht weiter darauf eingegangen wird.

9.5.2 SERVICE

Der Service und Data Access Layer implementiert den Hauptteil der Business Logik und enthält den OR Mapper Entity Framework Core.

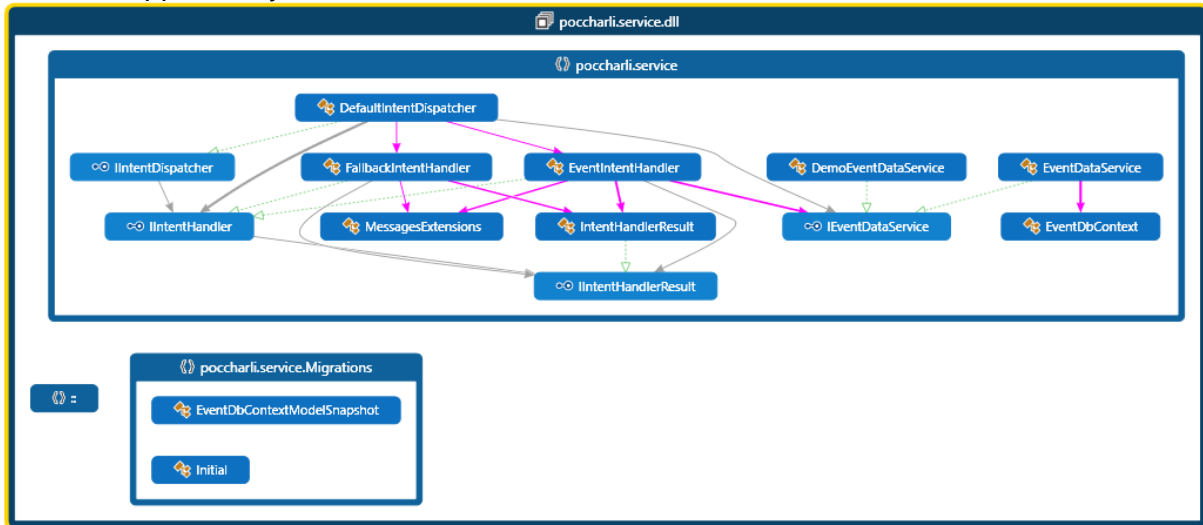


Abbildung 27 Abhängigkeiten der Service Klassen

Die Interfaces beschreiben die Funktionalität.

INTERFACE / KLASSE	BESCHREIBUNG
IIntentDispatcher	Exponiert Methoden für das Mappen von Intents und IIntentHandler
IIntentHandler	Implementieren Handle Methode, welche ein IIntentHandlerResult erzeugt
IIntentHandlerResult	Kapselt die gesamte Response, welche am Schluss der Verarbeitung an den Client zurückgegeben wird
IEventDataService	Exponiert CRUD Funktionalität für Events
EventDbContext	Entity Framework Implementation (OR Mapper)

Tabelle 43 Klassen und Interfaces im Service Layer

9.5.2.1 DATEN SCHNITTSTELLE

Die Datenhaltung und der Datenzugriff werden über **DbContextOptions** konfiguriert. Diese werden vom Konsumenten bereitgestellt, das heisst der Datenbank ConnectionString befindet sich in den Konfigurationsdateien des API Projekts. Dieser zeigt auf eine Datenbank Instanz, welche in Azure gehostet wird. Mehr dazu im Unterkapitel 9.5.4 .

9.5.3 DATA

Das Data Projekt enthält die Coderepräsentation der domänenbezogenen Daten.



Zum aktuellen Zeitpunkt existiert nur eine **Event** Klasse, welche zwecks Veranschaulichung des «vertikalen Durchstich» / Proof of Concept implementiert wurde. Das Charli Backend persistiert aktuell lediglich Events.

9.5.4 DEPLOYMENT

Das Charli Backend ist in der Azure³⁴ Cloud deployed. Alle Services werden unter der Subscription **ActionPack CSCH** mit der ResourceGroup **HSR_Students_2** verwendet. Diese Ressourcen werden vom Industriepartner Compass Security AG zur Verfügung gestellt. Folgende Abbildung liefert eine Übersicht der verwendeten Service.

Subscription ([change](#))
ActionPack CSCH

Subscription ID
6ebd55e5-6bbb-4e39-ba6b-e753db8c85...

Deployments
1 Failed,4 Succeeded

Tags ([change](#))
[Click here to add tags](#)

Filter by name... All types All locations No grouping

5 items Show hidden types

<input type="checkbox"/>	NAME ↑↓	TYPE ↑↓	LOCATION ↑↓	
<input type="checkbox"/>	charli	Application Insights	West Europe	...
<input type="checkbox"/>	charli	App Service	Central US	...
<input type="checkbox"/>	charli-dbserver	SQL server	West Europe	...
<input type="checkbox"/>	charli-db (charli-dbserver/charli-db)	SQL database	West Europe	...
<input type="checkbox"/>	ServicePlan51b62796-9000	App Service plan	Central US	...

Abbildung 28 Charli Backend Deployment Übersicht

Die Zugangsdaten für die Verwaltung sind im Anhang B. Aufgetretene Probleme während der Realisierung

9.5.5 BACKEND HIBERNATE

Die App Services auf Azure werden standardmässig nach einer gewissen Zeit ohne Nutzung heruntergefahren. Wird nun ein Webhookrequest durchgeführt, kann es sein, dass die Antwortzeit zu lange ist und Dialogflow nicht darauf wartet.

9.5.6 RICH RESPONSES WEB UI LIMITATIONEN

Durch die Auswahl der Architekturvariante 1, wie im Kapitel 8.2 beschrieben und der damit verbundenen Entscheidung auf ein eigenes UI zu verzichten, ist es nicht möglich, Rich Responses zu implementieren. Die Web Demo, welche von Dialogflow zur Verfügung gestellt wurde, ist nur für Test Zwecke geeignet und beherrscht nur Text Responses. Diese Limitation wurde erst spät in der Entwicklung festgestellt.

9.5.7 CONTEXT WERDEN NICHT RESETED

Aktive Contexts (Lifetime > 0) werden erst nach 20 Minuten gelöscht. Neu gestartete Konversationen müssen jedoch ohne die alten Contexts in die Konversationen starten, damit die richtigen Intents erreicht werden.

Die Dialogflow Console bietet eine «Reset Contexts» Möglichkeit, welche dieses Problem löst. Jedoch sind andere UI Integrationen wie z.B. Slack nicht damit ausgestattet und es gibt keine direkte Konfigurationsmöglichkeit in Dialogflow. Das Problem kann nur mit Hilfe des Backends

³⁴ <https://portal.azure.com>



und der «resetContexts=true» Property innerhalb der **outputContexts** in der WebhookResponse

9.5.8 @LAST-NAME ENTITY

Dialogflow stellt die System Entites «last-name» zur Verfügung, um Nachnamen zu erkennen. Leider gibt es keine direkte Einsicht in die System Entities. Fehlende Nachnamen werden erst im Verlaufe der Tests erkannt. Diese Entity kann auch nicht erweitert werden, weshalb der Chatbot Charli auf die Entity «any» zurückgreift, um Namen zu erkennen.

9.5.9 WEBHOOK CONTROLLER MIT SWAGGER INKOMPATIEL

Die Google.Cloud.Dialogflow.V2 Klassen sind mit der API Documentation Technologie Swagger inkompatibel. Die .NET Implementation von Swagger, Swashbuckle, konnte die API Definition nicht generieren.

9.5.10 SLOT FILLING ANWENDUNG

Slot Filling wird im Moment nur im Intent «pt» richtig verwendet. Folgende Abbildung zeigt die verwendeten Entities.

• pt SAVE

Action and parameters ^

service.service-custom ///

REQUIRED <small>?</small>	PARAMETER NAME <small>?</small>	ENTITY <small>?</small>	VALUE	IS LIST <small>?</small>	PROMPTS <small>?</small>
<input checked="" type="checkbox"/>	attacker	@attacker	\$attacker	<input type="checkbox"/>	Gegen wenn möch...
<input checked="" type="checkbox"/>	attack	@attack	\$attack	<input type="checkbox"/>	Gegen welche At...
<input checked="" type="checkbox"/>	box	@white-blackbox	\$box	<input type="checkbox"/>	Soll es ein Bla...
<input checked="" type="checkbox"/>	account	@testaccount	\$account	<input type="checkbox"/>	Welchen Zugang ...
<input checked="" type="checkbox"/>	know	@knowaboutit	\$know	<input type="checkbox"/>	Wer in der Firm...
<input type="checkbox"/>	service	@service	\$service	<input type="checkbox"/>	–
<input checked="" type="checkbox"/>	startdate	@sys.date	\$startdate	<input type="checkbox"/>	Geben Sie mir b...

Abbildung 29 Slot Filling pt

Beim Slot Filling wird erst in den nächsten Intent gewechselt, wenn alle Fragen beantwortet sind. Das hat zur Folge, dass der Benutzer gezwungen ist, sämtliche Fragen zu beantworten, bevor er weiter kommt. Ausserdem müssen die Antworten in den Wertebereichen der definierten Entities enthalten sein, da ansonsten dieselbe Frage erneut gestellt wird.

9.5.11 FULFILLMENT EINSATZ

Wenn das Backend nicht genug schnell antwortet, wird die alternative Antwort aus dem aktuellen Intent von Dialogflow zurückgegeben.



10. TESTING

10.1 EINLEITUNG

Das folgende Kapitel beschreibt das Vorgehen, die Durchführung und die Ergebnisbesprechung der durchgeführten Usability Tests. Alle Testprotokolle befinden sich im Anhang.

10.2 VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

10.3 TEST CASES

Grundlage der Usability Tests bilden die Test Cases. Sie definieren das zu erreichende Ziel, welches von der Testperson verfolgt werden soll.

TEST CASE 1	INFORMATIONEN ÜBER DIE FIRMA ERHALTEN
Ziel	Informationen über die Firma beschaffen
Erwartetes Verhalten	Die Testperson erhält einen kurzen Überblick über die Compass Security

Tabelle 44 Test Case 1

TEST CASE 2	INFORMIEREN ÜBER NÄCHSTEN ANLASS
Ziel	Auskunft darüber erhalten, wann der nächste Anlass der Compass Security stattfindet
Erwartetes Verhalten	Der Chatbot liefert Informationen darüber, wann der nächste Anlass stattfindet

Tabelle 45 Test Case 2



TEST CASE 3 PENETRATIONSTEST BESTELLEN	
Ziel	<p>Einen Penetration Test bestellen und Informationen angeben, um eine Offerte zu erhalten</p> <p>An die Testperson angegebene Informationen:</p> <ul style="list-style-type: none"> • Kennt sich mit Penetration Test aus • Führt Ihn durch, weil der Vorstand das so will • Möchte sich gegen Hacker schützen • Möchte sich gegen Injection Attacks schützen • Whitebox Test • Keinen Zugang in der Firma um den Angriff durchzuführen • Niemand sollte von diesem Angriff in der Firma wissen • Für Studenten: Arbeiten bei der Swisscom, Zürich
Erwartetes Verhalten	Der Chatbot informiert über Penetration Testing und stellt der Testperson Fragen. Danach werden die Kontaktdaten erfasst

Tabelle 46 Test Case 3

TEST CASE 4 BERATUNG ÜBER PENETRATION TESTING DURCHFÜHREN	
Ziel	<p>Testperson möchte einen Penetration Test bestellen, weiss aber nicht, ob das das richtige für Ihn ist und möchte sich erst beraten lassen</p> <p>An die Testperson angegebene Informationen:</p> <ul style="list-style-type: none"> • Kennt sich nicht mit Penetration Test aus • Möchte ein Beratungsgespräch führen • Möchte über Chat beraten werden • Führt Ihn durch, weil er gehackt wurde • Möchte Schwachstellen herausfinden • Über den Chat einen Penetration Test bestellen • Möchte sich gegen Hacker schützen • Möchte sich gegen Injection Attacks schützen • Whitebox Test • Keinen Zugang in der Firma um den Angriff durchzuführen • Niemand sollte von diesem Angriff in der Firma wissen • Für Studenten: Arbeiten bei der Swisscom, Zürich
Erwartetes Verhalten	Der Chatbot informiert über Penetration Testing und stellt der Testperson Fragen. Durch die Fragen versucht der Chatbot herauszufinden, ob der Penetration Test das richtige für Ihn ist. Der Penetration Test wird empfohlen. Dannach werden die Kontaktdaten erfasst.

Tabelle 47 Test Case 4

TEST CASE 5 MENSCHLICHEN MITARBEITER ANFORDERN	
Ziel	Dem Chatbot mitteilen, dass ein menschlicher Kontakt erwünscht oder gefordert wird.



TEST CASE 5 MENSCHLICHEN MITARBEITER ANFORDERN	
Erwartetes Verhalten	Der Chatbot erkennt das Bedürfnis der Testperson, dass diese lieber einen echten menschlichen Mitarbeiter sprechen möchte. Der Chatbot versucht noch, Kontaktinformationen zu sammeln und beendet das Gespräch.

Tabelle 48 Test Case 5

10.4 BEWERTUNGSRASTER CHARAKTER UND VERHALTEN

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

Zu jedem Test Case wird das Verhalten anhand dieses Rasters mitbewertet.

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	<Benotung von 1 bis 5>
Stellt offene Fragen	<Benotung von 1 bis 5>
Übernimmt die Terminologie des Gesprächspartners bei Nomen	<Benotung von 1 bis 5>
Die Antworten sind nicht unnötig lange	<Benotung von 1 bis 5>
Die Antworten sind hilfreich	<Benotung von 1 bis 5>
Die Antworten und Informationen sind einfach verständlich	<Benotung von 1 bis 5>
Geht nicht auf negative Äusserungen ein	<Benotung von 1 bis 5>
Verwendet keine Kraftausdrücke und Fluchwörter	<Benotung von 1 bis 5>

Tabelle 49 Bewertungsraster Charakter



10.5 AUSWERTUNG

CHARAKTER / BEURTEILUNG DER TESTPERSONEN VERHALTEN											
Zeigt Freude am Kontakt	5	5	5	4	4	4	4	5	3		4.3
Stellt Offene Fragen	3	4	4	4	3	4	4	4	4		3.8
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5	5	5	4	5	5	5	5	1		4.4
Die Antworten sind nicht unnötig lange	1	3	3	4	4	3	3	4	3		3.1
Die Antworten sind hilfreich	4	4	4	3	5	5	5	4	3		4.1
Die Antworten und Informationen sind einfach verständlich	4	4	4	5	5	5	5	5	5		4.7
Geht nicht auf negative Äusserungen ein	5	5	5	5	5	5	5	5	5		5.0
Verwendet keine Kraftausdrücke und Fluchwörter	5	5	5	5	5	5	5	5	5		5.0

Tabelle 50 Gesamtauswertung

Die Usability Tests zeigten wesentliche Punkte:

- Testpersonen geben gerne kurze Antworten im Stile von Kommandos und verzichten auf das Ausformulieren.
- Testpersonen mit geringer technischer Affinität haben sich über die vorgestellten Optionen positiv geäussert.
- Einige Testpersonen haben «Rich Responses» wie Auswahlboxen oder Hyperlinks erwartet oder hätten diese geschätzt und genutzt.
- Bei der Verwendung von Optionen war die Fehlerquote bei der Intenterkennung geringer.
- Der Chatbot fällt sehr oft in den default Fallback Intent. Dies ist auf ein mangelndes Training zurückzuführen. Für das Schliessen dieser Lücken müssen deutlich mehr Trainings durchgeführt werden. . Zusätzlich wurde als Konsequenz abgeleitet, dass innerhalb der Intents, eigene Fallback Intents eingerichtet werden müssen.
- Aus Zeitgründen wurde darauf verzichtet, jede Dienstleistung in die Tiefe zu implementieren. Bei den Tests führte dies zu Verwirrung, dass einige globale Intents nur oberflächlich umgesetzt wurden.



11. ERGEBNISSE

11.1 ZUSAMMENFASSUNG

In der nachfolgenden Tabelle wird aufgezeigt, welche Ziele erfüllt wurden und welche nicht.

Ziel	PRIO	ZUSTAND
Modellierung Gespräch	1	Erfüllt
Training	1	Erfüllt
Notification	2	Nicht erfüllt
UI	1	Erfüllt
Konversationsübernahme	2	Nicht erfüllt
Persistieren der Konversationen	1	Erfüllt
Monitoring	2	Erfüllt
Management	3	Teils erfüllt
Identifikation	3	Nicht erfüllt

Tabelle 51 Zusammenfassung der Ergebnisse der Ziele

11.2 RESULTATE

11.2.1 FUNKTIONALE ANFORDERUNGEN

In folgender Tabelle werden die Resultate der Funktionalen Anforderungen aufgelistet. Diese wurden durch die Systemtests geprüft, welches sich im Anhang befindet.

USE CASE	PRIO	STATUS
UC 1 Menschlichen Mitarbeiter beantragen	1	Teils erfüllt



USE CASE	PRIO	STATUS
UC 2 Informationen über Unternehmen	1	Erfüllt
UC 3 Informationen über Dienstleistungen	1	Erfüllt
UC 4 Kritik / Lob äussern	1	Teils Erfüllt
UC 5 Beratung zu Dienstleistungen	1	Erfüllt
UC 5.1 Dienstleistung bestellen	1	Erfüllt
UC 5.2 Kundeninformationen mitteilen	1	Erfüllt
UC 6 Konversation beenden	1	Erfüllt
UC 8 Lesen und Löschen von Konversationen	1	Erfüllt
UC 9 Lesen und Löschen Zusammenfassungen	2	Nicht erfüllt
UC 10 CRUD Intents	1	Erfüllt
UC 11 CRUD Entities	1	Erfüllt
UC 12 Konversation übernehmen	2	Nicht erfüllt
UC 13 Intent Training	1	Erfüllt
UC 14 CRUD Kundendaten	3	Nicht erfüllt
UC 15 Benachrichtigung einrichten	2	Nicht erfüllt

Tabelle 52 Ergebnisse Funktionale Anforderungen



11.2.2 NICHT-FUNKTIONALE ANFORDERUNGEN

In der nachfolgenden Tabelle sind die Ergebnisse der Nicht-Funktionalen Anforderungen ersichtlich. Viele Anforderungen wurden durch die Verwendung von Dialogflow erfüllt.

NFA	STATUS	BESCHREIBUNG
Die Kommunikation des Users mit dem Bot ist mittels SSL/TLS gesichert	Erfüllt	Durch Dialogflow gewährleistet
User haben keinen Zugang zu fremden Konversationen	Erfüllt	Durch Dialogflow gewährleistet
Das Chatbot UI ist gegen Script-injection basierte Angriffe geschützt (zum Beispiel XSS)	Erfüllt	Durch Dialogflow gewährleistet
Alle Konversationen müssen in für einen Menschen lesbaren Form persistiert oder auslesbar sein	Erfüllt	Durch Dialogflow gewährleistet
Das Chatbot UI erlaubt die Eingabe von Text und das Abschicken von Text mittels der Eingabetaste	Erfüllt	Durch Dialogflow / Slack und weiteren Integrationsmöglichkeiten gewährleistet
Der Confidence-score bei der Intenterkennung des Bots innerhalb einer Konversation ist im Durchschnitt mindestens 75%.	Ungetestet, Confidence Score wurde nicht überprüft, sofern er über dem Threshold von 0.3 liegt	Dialogflow empfiehlt 30% als Confidence-score Threshold für die Intenterkennung. Ein Wert < 0.3 führt zum Fallback Intent
Der Chatbot kehrt bei Unverständnis in einen definierten «Non Intent» Zustand zurück oder übergibt an einen (menschlichen) Supporter.	Erfüllt	Wurde durch Fallback Intents gewährleistet
Die Zugriffe zum Backend, Datenbanken oder Verwaltungsplattform des Chatbots sind nur für Berechtigte möglich. Zugriffsberechtigungen werden vom Projektteam verwaltet.	Erfüllt	Wird auf der Azure Cloud der Compass Security verwaltet
Der Chatbot kann bis zu 5 Transaktionen pro Sekunde verarbeiten. Eine Transaktion beschreibt einen Textbasierten Input mit einer maximalen Zeichenlänge von 500 Zeichen	Erfüllt	Durch Dialogflow gewährleistet



NFA	STATUS	BESCHREIBUNG
Es können bis zu 5 User gleichzeitig mit dem Chatbot interagieren. Es können bis zu 5 Konversationen gleichzeitig betrieben werden	Erfüllt	Durch Dialogflow gewährleistet
Die Intenterkennung ist mittels Trainingsdaten verbesserungsfähig. Die Trainingsdaten werden vom (menschlichen) Betreiber vorbereitet	Erfüllt	Durch Dialogflow gewährleistet
Der Chatbot bietet die Möglichkeit, nachträglich neue Intents zu trainieren und den groben Gesprächsablauf zu ändern	Erfüllt	Durch Dialogflow gewährleistet
Der Chatbot bietet die Möglichkeit, weitere Sprachen einzubinden, ohne dass Quellcode geändert werden muss	Erfüllt	Durch Dialogflow gewährleistet

Tabelle 53 Ergebnisse Nicht-Funktionale Anforderungen

11.2.2.1 VERHALTENSGRUNDSÄTZE

In der folgenden Tabelle werden die Ergebnisse der Verhaltensgrundsätze dargestellt. Die Verhaltensgrundsätze wurden mittels Usability Tests getestet. Die Durchschnittliche Bewertung der Testpersonen muss über zwei liegen, um als erfüllt zu gelten.

CHARAKTER / VERHALTEN	STATUS	DURCHSCHNITTliche BEWERTUNG
Zeigt Freude am Kontakt	Erfüllt	4.3
Stellt offene Fragen	Erfüllt	3.8
Übernimmt die Terminologie des Gesprächspartners bei Nomen	Erfüllt	4.4
Die Antworten sind nicht unnötig lange	Erfüllt	3.1
Die Antworten sind hilfreich	Erfüllt	4.1
Die Antworten und Informationen sind einfach verständlich	Erfüllt	4.7
Geht nicht auf negative Äusserungen ein	Erfüllt	5.0



CHARAKTER / VERHALTEN	STATUS	DURCHSCHNITTLICHE BEWERTUNG
Verwendet keine Kraftausdrücke und Fluchwörter	Erfüllt	5.0

Tabelle 54 Ergebnisse Verhaltensgrundsätze

11.3 SCHLUSSFOLGERUNGEN

Die gestellten Anforderungen und Zielsetzungen konnten nur teilweise erfüllt werden. Besonders der Kernaspekt, die Beratung, wurde nicht zufriedenstellend realisiert. Das zugrundeliegende Problem ist, dass ein offenes Gespräch eine sehr grosse Anzahl an Intents zur Folge hätte und dies mit Dialogflow im aktuellen Stand nicht beherrschbar ist. Nur mit einer strikten Gesprächsführung, welche mit vorgefertigten Antwortmöglichkeiten sichergestellt wird, einer grossen Menge an Trainingsdaten und einem vollwertigen Chat User Interface, sind die ambitionierten Ziele dieser Projektarbeit zufriedenstellend realisierbar.

Die Erweiterbarkeit des aktuellen Gesprächsmodell und ein lauffähiger Architekturprototyp, der alle relevanten Komponenten zum Einsatz bringt, bilden die Grundlage für zukünftige Verbesserungen.



12. WEITERENTWICKLUNG

12.1 WEITERENTWICKLUNGEN

Nachfolgend sind die wichtigsten Weiterentwicklungen gelistet, welche die Grundlage für zukünftige Arbeitspakete bilden.

12.2 ARCHITEKTURWECHSEL AUF VARIANTE 2

Gemäss dem Kapitel 8.2 sollte für die Erfüllung sämtlicher Use Cases, insbesondere für die nahtlose Gesprächsübernahme durch einen Mitarbeiter, die Architektur gemäss Variante 2 umgestellt werden.

12.3 USERINTERFACE

Im Zuge der Umstellung auf die Architekturvariante 2, wie im Kapitel 8.2 beschrieben, sollte ebenfalls ein vollwertiges User Interface implementiert werden. Damit eröffnen sich neue Möglichkeiten der Gesprächsführung durch Auswahlboxen und allgemeine Rich Response Messages.

12.4 TRAININGSDATEN AGGREGATION

Es sollten mehr Ressourcen in das Testen und Beschaffen von Trainingsdaten investiert werden. Diese ermöglichen es, die Chatbot Anwendung entlang der wichtigen Gesprächspfade robuster zu machen und neue Lücken aufzudecken.

12.5 BERATUNG ÜBER DAS BACKEND

Der «consulting» Intent sollte via Webhook mit dem Backend verknüpft werden und die Klassifizierung, wie in Kapitel 8. beschrieben wurde, selbst ausgeführt werden. Diese Business Logik wäre in der Lage, komplexe Zustände zu halten, im Gegensatz zu Dialogflow. Damit liessen sich besser auf die Bedürfnisse des Kunden eingehen und wäre aus Sicht der Produktqualität eine positive Entscheidung.

12.6 CREDENTIALMANAGEMENT

Für die API Calls zu Dialogflow V2 muss man sich zuerst gegen die Google Cloud authentisieren. Das Hinterlegen dieser Credentials sollte im Zusammenspiel mit dem Azure Active Directory und Azure Key Vault sicher hinterlegt werden, damit die Credentials nicht Teil der Applikation sind.

12.7 DIENSTLEISTUNGSANGEBOTE ERWEITERN

In Zukunft sollten die existierenden Dienstleistungsangebote vollständig umgesetzt (analog zum «pt» (und Follow-up) Intent) oder komplett aus dem Gesprächsmodell entfernt werden. Zusätzlich ist es denkbar, die Beratung um weitere Angebote zu ergänzen.

12.8 TESTABDECKUNG

Die Testabdeckung der Businesslogik Komponenten sollte verbessert werden. Zusätzlich sollten für die API automatisierte System- und Integrationstests durchgeführt werden.



12.9 AUSBLICK

Wenn ein Beratungsgespräch in hinreichender Güte erreicht werden möchte, ist eine Verlagerung der Business Logik weg von Dialogflow und hin in ein eigenes Modell unumgänglich.

Ein möglicher Ansatz für die Modellierung wäre eine hierarchische Zustandsmaschine.

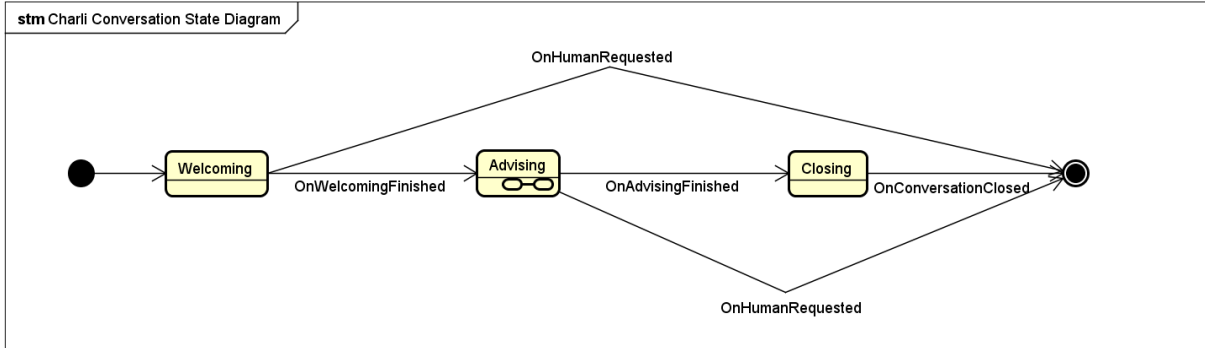


Abbildung 30 Ausblick Möglichkeit Konzept Zustandsautomat

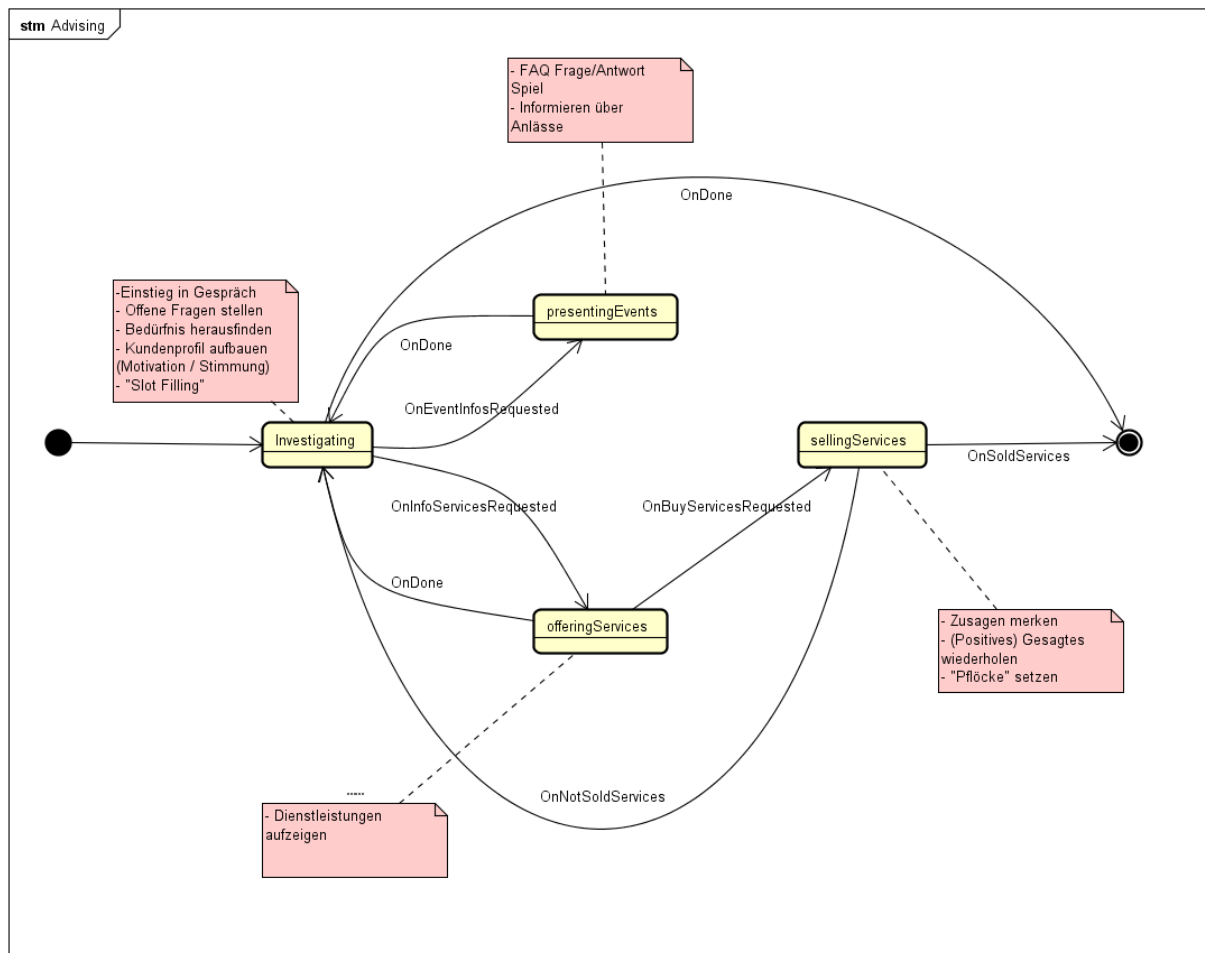


Abbildung 31 Ausblick Modellmöglichkeit Consulting

Wichtige Erfolgsfaktoren für diesen Zustandsautomaten wäre der Umgang mit sehr vielen Zuständen (Intents) und ein Fallback Management, welches nicht sofort den Kontext verwirft und es ermöglicht, nach einer «Klärung» der Situation wieder in den letzten gültigen Zustand zu wechseln (self healing).



Der Chatbot Charli kann in Zukunft, sofern er als experimentelles Feature gekennzeichnet ist, in den Compass Security AG Webauftritt integriert werden, sobald die geschilderten Weiterentwicklungspunkte in diesem Kapitel umgesetzt wurden.



13. PROJEKTMONITORING

13.1 EINLEITUNG

In diesem Kapitel erfolgt ein Vergleich des geleisteten Aufwandes mit dem geplanten Aufwand. Weiter werden die Meilensteinziele abgeglichen und weitere Metriken zum Projekt aufgezeigt.

13.2 AUFWAND PRO WOCHE

Das folgende Diagramm zeigt auf, wie viele Stunden pro Woche jedes Teammitglied in die Bachelorarbeit investiert hat.

Für den geplanten Wert von 51 Mannstunden pro Woche, wurde der erwartete Gesamtaufwand (720 Stunden) durch die zu Anzahl der Kalenderwochen (14) geteilt.

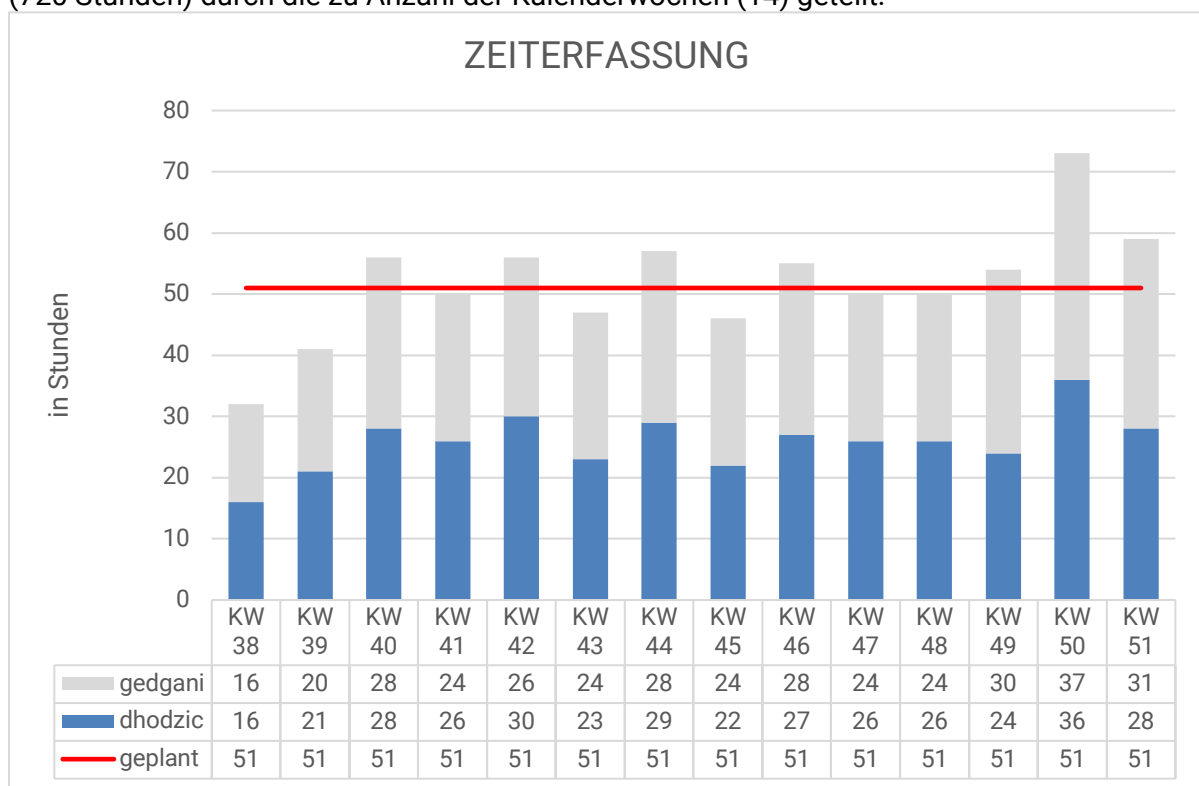


Abbildung 32 Aufwand pro Woche



13.3 GESAMTAUFWAND

TEAMMITGLIED	SOLL (in Stunden)	IST (in Stunden)
Denis Hodzic	360	362
Giuliano De Gani	360	364
Total	720	726

Tabelle 55 Gesamtaufwand

13.4 MEILENSTEINE SOLL/IST VERGLEICH

Wenn ein Arbeitspaket in einem Meilenstein nicht abgeschlossen werden kann, wird es auf den nächsten Meilenstein verschoben. Die nachfolgende Tabelle liefert einen Überblick über den Soll-/Ist-Vergleich der Meilensteine.

MEILENSTEIN	DATUM	BESCHREIBUNG
M1: Infrastruktur	04.10.2018	Projektplan erstellt, Infrastruktur bereit-gestellt
M2: End of Elaboration	17.10.2018	Anforderungen festgelegt, EoE Checkliste ³⁵ erfüllt
M3: Prototyp Alpha	07.11.2018	Prototyp Alpha („vertikaler Stich“) bereitgestellt
M4: Prototyp Beta	21.11.2018	Prototyp Beta bereitgestellt
M5: End of Construction	05.12.2018	End of Construction
M6: Schlussabgabe	21.12.2018	Endprodukt als Ganzes funktioniert, Technischer Bericht fertiggestellt und abgabebereit

Tabelle 56 Meilensteine Projektmonitoring

³⁵ Siehe dazu im DevOps Repository unter «/docu/eoe_checkliste.pdf »



MEILENSTEIN	SOLL	IST	Bemerkungen
M1:	04.10.2018	04.10.2018	
M2:	17.10.2018	17.10.2018	
M3:	07.11.2018	07.11.2018 21.11.2018	Vertikaler Architekturdurchstich erfüllt. Beim Verschieben des Backends von der privaten Entwicklersubscription in die Compass Security Azure AD Subscription, sind einige Komplikationen im Deployment aufgetreten was zu Verzögerungen und Verschiebungen von Arbeitspaketen zur Folge hatte.
M4:	21.11.2018	21.11.2018	
M5:	05.12.2018	12.12.2018	End of Construction wurde um eine Woche verschoben, um den Chatbot noch mit weiteren Trainingsdaten zu erweitern.
M6:	21.12.2018	21.12.2018	

Tabelle 57 Meilensteine Soll/Ist Vergleich

13.5 CODESTATISTIK

PROJEKT	TESTABDECKUNG	BEMERKUNGEN
.data	90%	-
.service	47.17%	Die angestrebte Testabdeckung von 80% wurde nicht erreicht.
.api	ungetestet	Keine automatisierten System- und Integrationstests, welche die API von aussen aufrufen.

Tabelle 58 Testabdeckung



13.6 DIALOGFLOW ANALYTICS

In der folgenden Tabelle ist ersichtlich in wie vielen Sessions jeder Intent erkannt wurde. Außerdem wird aufgelistet wie oft dieser aufgerufen wurde und wie viele Konversationen in diesem Intent beendet wurden. In der Tabelle sind auch Intents enthalten, welche nicht mehr vorkommen.

INTENT	SESSIONS	COUNT	EXIT %
global.welcome	31	242	5.79%
pt	3	110	3.64%
CS welcome	13	96	9.38%
global.events	20	90	32.22%
global.security.review	5	60	3.33%
global.pt.enlightenment	5	59	6.78%
person.infos	3	59	8.47%
global.consulting	7	40	0%
CS service - penetration	2	40	2.50%
global.service	9	38	2.63%
chat.consulting	7	36	2.78%
CS consulting	5	33	3.03%
consulting penetration	4	31	6.45%
welcome	5	30	13.33%
CS penetration enlightenment	3	29	0%
service - penetration	3	29	3.45%
consulting.noidea	3	27	7.41%
company.infos	3	26	11.54%
pt	3	26	0%
no.idea	3	22	0%
chat consulting	4	20	5%
test custom payload	2	19	10.53%
CS person Infos	2	17	11.76%
events end conversation	2	15	13.33%
CS company Infos	2	13	15.38%
global.discover	3	13	7.69%
global.contact.person	1	13	7.69%
service	3	11	27.27%
discover end conversation	1	10	0%
discover.end	2	10	0%
CS employee	2	10	0%
penetration reason hacking	2	9	0%
CS events	2	7	0%
penetration recommendation	2	7	0%
noidea.personinfos	1	6	0%



INTENT	SESSIONS	COUNT	EXIT %
CS discover	3	6	33.33%
pt.reason.hacking	1	6	0%
global.security.training	1	6	0%
events.end	2	6	16.67%
pt.recommendation	1	6	0%
discover.person.infos	2	5	0%
dfir	1	5	0%
discover get person data	1	4	0%
penetration enlightenment	2	4	0%
end.with.contact	2	3	0%
pt.reason.executive.board	1	3	0%
discover end without contact	1	3	0%
security.review.os	2	3	0%
global.needs	2	3	66.67%
service.nointerest	1	3	0%
discover	2	3	0%
penetration no experience	2	2	0%
discover end with contact	1	2	0%
killer.questions	1	2	0%
consulting	1	1	100%
charli.service.penetration	1	1	0%
consulting.contact	1	1	0%
service.interestUnspecified	1	1	0%
security.training	1	1	0%
events	1	1	0%
consulting contact	1	1	100%
global.killer.questions	1	1	0%

Tabelle 59 Dialogflow Analytics

13.7 SESSION FLOW ÜBERSICHT

Session flow basierend auf 30 Tagen Sitzungsdaten. Die folgende Grafik zeigt allgemeine Pfade an, die von Benutzern genommen wurden, einschließlich der Austrittspunkte.



Session flow

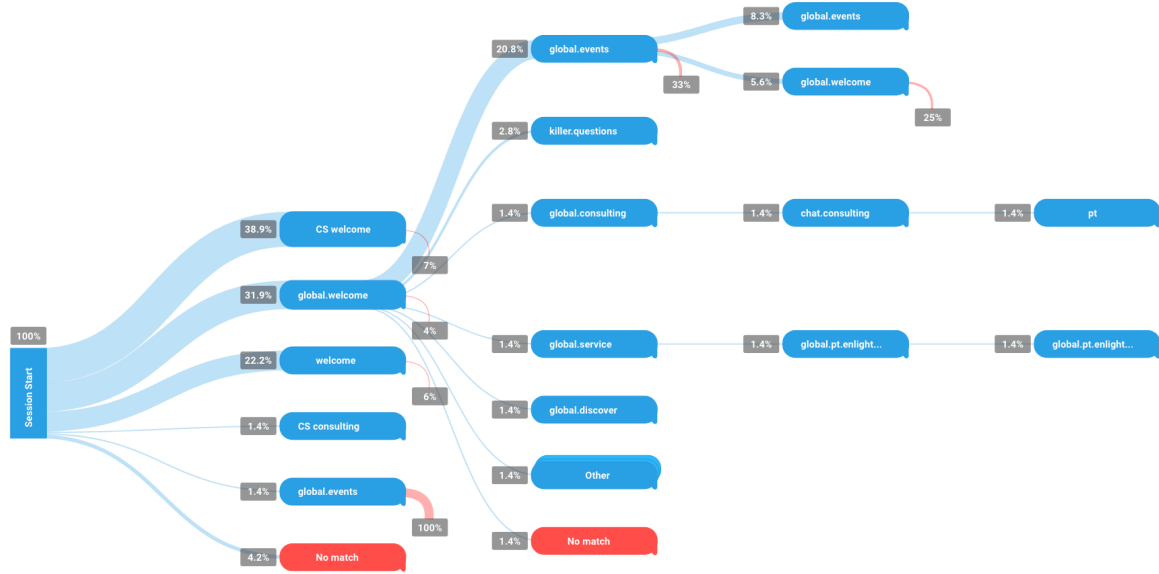


Abbildung 33 Session flow



14. VERZEICHNISSE

14.1 GLOSSAR

BEGRIFF	BEDEUTUNG / BESCHREIBUNG
Agenten	Agenten lassen sich am besten als Natural Language Understanding (NLU)-Module beschreiben. Diese Module können in eine App, Website, Produkt oder Dienstleistung integriert werden und übersetzen Text- oder gesprochene Benutzeranfragen in aussagekräftige Daten. Diese Übersetzung tritt auf, wenn die Äußerung eines Benutzers mit einer Absicht in dem Agenten übereinstimmt.
AI / ML	Künstliche Intelligenz / Machine Learning. Teilgebiete der theoretischen Informatik. Finden seit dem Aufkommen von deep neuronal networks zunehmend Anwendungen in verschiedenen Bereichen. In Bezug auf einen Chatbot wird AI / ML vor allem mit Sprach- und Texterkennungsalgorithmen in Verbindung gebracht, welche im Hintergrund mit einem neuronalen Netz arbeiten.
API	Application Programming Interface, also eine Schnittstelle für Entwickler, um externe Funktionalitäten zu verwenden. Sie erlaubt die Kommunikation zwischen verschiedenen Software Anwendungen.
Azure	Clouddienst von Microsoft. Bietet eine grosse Anzahl Services, Hosting und Deployment Optionen.
Backend	Als Backend wird der Teil eines IT-Systems bezeichnet, der sich mit der Datenverarbeitung im Hintergrund beschäftigt – typischerweise dem Service, Data Access und Data Layer.
Bot Framework	Entwicklerwerkzeuge und Sammlung von Services, welche für das Erstellen und Betreiben eines Bots benötigt werden.
Build Server	Wird auch CI Server genannt und ermöglicht den Continuous Integration Prozess. Bei jedem einzelnen Commit auf ein Repository wird durch den Build Server ein Build vom Source Code erstellt und alle Unit Tests ausgeführt.
CI / CD Umgebung	Continuous Integration / Continuous Delivery. Durch eine CI/CD Pipeline kann der Softwarebereitstellungsprozess, wie z.B. das Initiieren von automatischen Builds und das Deployment auf eine Server Instanz, automatisiert werden.
Client Correlation Services	Fingerprint Mechanismus: Anhand von Clientmetadaten werden Identitäten miteinander verknüpft



BEGRIFF	BEDEUTUNG / BESCHREIBUNG
Cognitive Services	Sammlung von AI / ML Services bei Microsoft.
Continuous Integration	Ist ein Verfahren in der Software Entwicklung, bei der Entwickler in regelmässigen Abständen Codeänderungen in einem zentralen Repository zusammenführen. Diese Änderungen werden durch den Build Server erstellt (und getestet). Das Ziel von Continuous Integration besteht darin, Software Bugs schneller zu entdecken und zu beheben. Durch das Continuous Integration Verfahren kann die Software Qualität gesteigert werden.
CRUD	Kurzform für «Create, Read, Update, Delete». Beschreibt die grundlegende Operationen mit persistierten Daten
Deployment	Als Deployment wird der Prozess zur Installation und Konfiguration von Software auf PCs und Server bezeichnet.
Detect Intent Response	Google Mechanismus, um den richtigen Intent zu matchen.
DevOps	DevOps vereint Menschen, Prozesse und Technologien – und ermöglicht Continuous Delivery. DevOps setzt sich aus «Dev» (Entwicklung) sowie «Ops» (Betrieb) zusammen und bezeichnet einen Softwareentwicklungsansatz, der genau diese beiden IT-Komponenten zusammenführt. Der Begriff steht für die Verknüpfung und Zusammenarbeit von ehemals getrennten Disziplinen.
Emulator App	Emulator App von Google, um Konversationen mit einem Agenten durchzuführen.
Entity	Im Kontext eines Chatbots beschreibt ein Entity eine nutzbare Information, wie zum Beispiel einen Ort, eine Menge, Namen oder Sachen.
Frontend	Als Frontend bezeichnet man die Präsentationsebene, das heisst den Teil einer Applikation, den der Betrachter sehen kann, zum Beispiel in Form von einer grafischen Benutzeroberfläche.
HTML 5	HTML5 ist die fünfte Fassung der Hypertext Markup Language, einer Computersprache zur Auszeichnung und Vernetzung von Texten und anderen Inhalten elektronischer Dokumente, vorwiegend im World Wide Web.
Intent	Im Kontext eines Chatbots beschreibt ein Intent die Absicht, die hinter der Utterance des Gesprächspartners steckt. Ziel eines Chatbots ist es, möglichst genau zu erkennen, welche Absicht der Gesprächspartner hegt.



BEGRIFF	BEDEUTUNG / BESCHREIBUNG
Interoperabilität	Fähigkeit unterschiedlicher Systeme, möglichst nahtlos zusammenzuarbeiten
Kundenmetadaten	Daten, die ein Kunde indirekt teilt, wie zum Beispiel die Betriebssystemversion, Browserversion, Verweildauer und Anderes. Kann verwendet werden, um den wiederkehrende Kunden auf einer Website zu identifizieren
Management Application	Ist eine Kombination aus der Entwicklung und Betreuung von Applikationen über deren gesamten Lebenszyklus. Dies beinhaltet auch eine umfassende Anwenderbetreuung (Support) und die Weiterentwicklung der Software.
NLP / NLU	Natural Language Processing oder Natural Language Understanding. Ein Service, der anhand einer Utterance ein Intent mit Confidence Score zuordnet. Es geht also darum, die Absicht hinter einem Text zu erkennen.
Paas	«Platform as a service». Ist ein Teilbereich des Cloud Computings, wo der Cloudanbieter bereits Infrastruktur und Betriebssystem bereitstellt und dem Entwickler die Möglichkeit geben, darauf aufzusetzen.
Persistieren	Ein Begriff der Informatik, um Daten über eine längere Zeit bereitzuhalten.
PoC	Im Projektmanagement ist ein Proof of Concept, auch als Proof of Principle bezeichnet, ein Meilenstein, an dem die prinzipielle Durchführbarkeit eines Vorhabens belegt ist. Vielfach ist der positive oder negative Machbarkeitsnachweis das Ergebnis einer Machbarkeitsstudie.
RESTful http API	Eine RESTful-API ist eine Schnittstelle, welche das Paradigma bzw. die Einschränkungen der repräsentativen Zustandsübertragung (REST) anwendet.
SaaS	Software as a Service (SaaS) ist ein Teilbereich des Cloud Computings. Das SaaS-Modell basiert auf dem Grundsatz, dass die Software und die IT-Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt werden.
Scoping	Scoping ist die Definition von Aufgaben- oder Untersuchungsumfängen in komplexen Planungs-, Management- und Herstellungsprozessen.



BEGRIFF	BEDEUTUNG / BESCHREIBUNG
SDK	Ein Software Development Kit (SDK) ist eine Sammlung von Programmierwerkzeugen und Programmbibliotheken, die zur Entwicklung von Software dient. Es unterstützt Softwareentwickler, darauf basierende Anwendungen zu erstellen.
Slot Filling	Ein Begriff im Bot Umfeld. Bezeichnet den Prozess, wo benötigte Informationen gesammelt und abgefüllt werden.
Social Engineering	Das Social Engineering bezeichnet das zwischenmenschliche Beeinflussen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen oder zur Freigabe von Finanzmitteln zu bewegen
SSL /TLS	Transport Layer Security (TLS, englisch für Transportschichtssicherheit), weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
Technologiestack	Als Technologiestack bezeichnet man eine Reihe von aufeinander aufbauenden Softwarekomponenten die gemeinsam eine Plattform bilden.
UI / User Interface	Das User Interface ist die Stelle oder Handlung, mit der ein Mensch mit einer Maschine in Kontakt tritt.
Utterance	Im Kontext eines Chatbots beschreibt die Utterance die Textphrase, welche vom Gesprächspartner abgesendet wird. Das sind zum Beispiel einfache Antworten wie «Ja, genau» bis hin zu längeren Sätzen.
Vertikaler Durchstich	Hierbei wird ein ausgewählter Teil umgesetzt. Dies eignet sich besonders für Fälle, in denen noch Funktionalitäts- oder Implementierungsfragen ungeklärt sind. Abgeschlossene Teile können dann bereits umgesetzt werden, bevor die Anforderungen für den Rest komplett festgelegt wurden

Tabelle 60 Glossar

14.2 TABELLENVERZEICHNIS

Tabelle 1 Produktziele für den Chatbot.....	13
Tabelle 2 Lieferobjekte der Bachelorarbeit	14
Tabelle 3 Rollenübersicht.....	16
Tabelle 4 Kapazität	17
Tabelle 5 Kalenderwochen und Phasen	17
Tabelle 6 Iterationen.....	18
Tabelle 7 Meilensteine	19
Tabelle 8 Übersicht Tools	22



Tabelle 9 Qualitätsmassnahmen.....	23
Tabelle 10 Kriterienkatalog.....	28
Tabelle 11 Überblick populäre Bot Frameworks.....	28
Tabelle 12 Kosten Azure Bot Service.....	32
Tabelle 13 Bewertungsmatrix Bot Builder Framework.....	33
Tabelle 14 Bewertungsmatrix Dialogflow.....	39
Tabelle 15 Ergebnisgesamtüberblick.....	40
Tabelle 16 Übersicht funktionale Anforderungen.....	42
Tabelle 17 Überblick Use Cases.....	45
Tabelle 18 Sub Usecases 5.....	46
Tabelle 19 Begriffsdefinitionen.....	48
Tabelle 20 Nichtfunktionale Anforderungen.....	49
Tabelle 21 Verhaltensgrundsätze.....	50
Tabelle 22 Beispiel Test Case 2.....	51
Tabelle 23 Beispiel Test Case 3.....	51
Tabelle 24 Beispiel Test Case 4.....	51
Tabelle 25 Beispiel Test Case 5.....	52
Tabelle 26 Bewertungsraster für Charakter.....	52
Tabelle 27 Killerfragen mit Antworten.....	53
Tabelle 28 Gegenüberstellung Architekturvarianten.....	56
Tabelle 29 Layerübersicht.....	57
Tabelle 30 API Endpunkte Entwurf.....	58
Tabelle 31 Follow-up zu company.infos.....	68
Tabelle 32 Follow-up Intents.....	70
Tabelle 33 Intents zu discover.....	71
Tabelle 34 Intents zu event.....	71
Tabelle 35 Intents zu global.security.review.....	72
Tabelle 36 Intents zu global.security.training.....	73
Tabelle 37 Intents zu global.service.....	73
Tabelle 38 Fallback zu Follow-up Intents.....	74
Tabelle 39 Eigene Entities.....	75
Tabelle 40 Backend Projektüberblick.....	75
Tabelle 41 API Endpunkte Umsetzung.....	78
Tabelle 42 DTO.....	78
Tabelle 43 Klassen und Interfaces im Service Layer.....	79
Tabelle 44 Test Case 1.....	82
Tabelle 45 Test Case 2.....	82
Tabelle 46 Test Case 3.....	83
Tabelle 47 Test Case 4.....	83
Tabelle 48 Test Case 5.....	84
Tabelle 49 Bewertungsraster Charakter.....	84
Tabelle 50 Gesamtauswertung.....	85
Tabelle 51 Zusammenfassung der Ergebnisse der Ziele.....	86
Tabelle 52 Ergebnisse Funktionale Anforderungen.....	87
Tabelle 53 Ergebnisse Nicht-Funktionale Anforderungen.....	89
Tabelle 54 Ergebnisse Verhaltensgrundsätze.....	90
Tabelle 55 Gesamtaufwand.....	95
Tabelle 56 Meilensteine Projektmonitoring.....	95
Tabelle 57 Meilensteine Soll/Ist Vergleich.....	96
Tabelle 58 Testabdeckung.....	96
Tabelle 59 Dialogflow Analytics.....	98
Tabelle 60 Glossar.....	103
Tabelle 61 Verwendete System Entities.....	127



14.3 ABBILDUNGSVERZEICHNIS

Abbildung 1 Contributions am Bot Builder Samples Projekt	29
Abbildung 2 Dialogtypen in Bot Builder SDK.....	31
Abbildung 3 Google Assistent inkl. Simulator User Interface.....	35
Abbildung 4 Plattformen	36
Abbildung 5 Beschränkungen Standard Edition Dialogflow	36
Abbildung 6 Non-Linear Dialog	37
Abbildung 7 Kosten Dialogflow Standard vs Enterprise Edition.....	38
Abbildung 8 Use Case Diagramm.....	43
Abbildung 9 Überblick Architektur Variante 1.....	54
Abbildung 10 Überblick Architektur Variante 2.....	55
Abbildung 11 Domainmodellierung.....	59
Abbildung 12 Kontaktaufnahme simpel.....	60
Abbildung 13 Kontaktaufnahme mit Backend.....	60
Abbildung 14 Single Turn.....	61
Abbildung 15 Gesprächsabbruch durch User.....	61
Abbildung 16 Gesprächsübernahme durch Mitarbeiter.....	62
Abbildung 17 Gesprächsmodell Konzept.....	63
Abbildung 18 Konzept Gesprächsablauf in Dialogflow.....	65
Abbildung 19 Konzept Slot Filling in Dialogflow	65
Abbildung 20 Intents in Dialogflow	66
Abbildung 21 Contexts in Dialogflow	66
Abbildung 22 Beispiel Gesprächsverzweigung mit Intentmatching und Entities.....	67
Abbildung 23 Dialogflow Intentübersicht Screenshot.....	69
Abbildung 24 Dialogflow global.discover Screenshot	71
Abbildung 25 Backend Abhängigkeitsdiagramm	76
Abbildung 26 Überblick Web API Endpoints mit Swagger UI	77
Abbildung 27 Abhängigkeiten der Service Klassen.....	79
Abbildung 28 Charli Backend Deployment Übersicht.....	80
Abbildung 29 Slot Filling pt.....	81
Abbildung 30 Ausblick Möglichkeit Konzept Zustandsautomat	92
Abbildung 31 Ausblick Modellmöglichkeit Consulting	92
Abbildung 32 Aufwand pro Woche.....	94
Abbildung 33 Session flow	99
Abbildung 34 Dialogflow Übersichtsseite.....	114
Abbildung 35 Dialogflow Console Intents.....	115
Abbildung 36 Übersicht Agent in Dialogflow	115
Abbildung 37 Neuer Agent.....	116
Abbildung 38 Dialogflow Console Einstellungen.....	116
Abbildung 39 Erstellen eines neuen Intents.....	117
Abbildung 40 Intent für Security Review	118
Abbildung 41 Slot Filling Beispiel im Security Review Intent.....	119
Abbildung 42 Prompts beim Slot Filling.....	119
Abbildung 43 Beispiel Text response.....	120
Abbildung 44 Erzeugen eines Follow-up Intent	121
Abbildung 45 Custom Follow-up Intent.....	121
Abbildung 46 Erstellter Follow-up Intent.....	122
Abbildung 47 Input Context im neuen Follow-up Intent.....	122
Abbildung 48 Output Context im Parent Intent.....	123
Abbildung 49 Ausgehende Informationen im companydata Context.....	123
Abbildung 50 eingehende Informationen im companydata Context	124
Abbildung 51 Zusammenführen nicht möglich	124
Abbildung 52 Context Sequenz	124
Abbildung 53 Erstellen des Fallback Intents.....	125



Abbildung 54 Entity erstellen	127
Abbildung 55 Beispiel Entity operatingsystem	128
Abbildung 56 Beispielanwendung eines Entity	129
Abbildung 57 Fulfillment Webhook Charli	131
Abbildung 58 Integrationsübersicht	132
Abbildung 59 Trainingsübersicht	132
Abbildung 60 Trainingsdialog mit unbekanntem Intent	133
Abbildung 61 Übersicht History	133
Abbildung 62 Protokolliertes Gespräch	134
Abbildung 63 Analyse Intent	135
Abbildung 64 Konzept beim Hinzufügen einer Dienstleistung	136



15. ERKLÄRUNG URHEBERSCHAFT

ZUR



Vereinbarung

1. Gegenstand der Vereinbarung

Mit dieser Vereinbarung werden die Rechte über die Verwendung und die Weiterentwicklung der Ergebnisse der Bachelorarbeit ChatBot von Denis Hodzic und Giuliano De Gani unter der Betreuung von Ivan Bütler geregelt.

2. Urheberrecht

Die Urheberrechte stehen den Studenten der Bachelorarbeit zu.

3. Verwendung

Die Ergebnisse der Arbeit dürfen sowohl von den Studenten der Bachelorarbeit, durch den betreuenden Professor der HSR wie auch von der Compass Security Holding oder einer ihrer Compass Tochterfirmen (Compass Schweiz, Compass Deutschland, Compass Cyber Defense, Security Competence GmbH) uneingeschränkt nach Abschluss der Arbeit verwendet und weiterentwickelt werden.

Rapperswil, den 25.10.2018

Der Student  Denis Hodzic

Rapperswil, den 25.10.2018

Der Student  Giuliano De Gani

Rapperswil, den 25.10.2018

.....
Der Betreuer der Bachelorarbeit  Ivan Bütler



16. ANHANG



A. DIALOGFLOW GESPRÄCHSMODELLIERUNG

Dialogflow Gesprächsmodell, simplifizierte Darstellung:
Knoten repräsentieren Intents, Kanten sind Verknüpfungen mit Hilfe von In- und Output Contexts.

Gelb markiert sind global zugängliche Intents (ohne Input Context)

Rot markiert sind Fallback Intents

Blau markiert sind Follow-up Intents, welche nicht direkt erreichbar sind.

Grün markierte Intents nutzen das Slot Filling Verfahren.





B. ZUGANGSDATEN

DIALOGFLOW ZUGANGSDATEN

BESCHREIBUNG	CREDENTIALS / RESOURCE
Dialogflow Einstieg	https://console.dialogflow.com/api-client/#/agent/610ac28b-8afe-492d-b80a-75a1cd8ba244/intents
Zugangsdaten	chatbotcharli@gmail.com Password: [REDACTED]



AZURE ZUGANGSDATEN

BESCHREIBUNG	CREDENTIALS / RESOURCE
Azure Einstiegsseite	https://portal.azure.com
Subscriptioninformationen	ActionPack CSCH 6ebd55e5-6bbb-4e39-ba6b-e753db8c852d Zugang muss über cyril.bannwart@compass-security.com beantragt werden
ResourceGroup	HSR_Students_2
charli-dbserver charli-dbserver.database.windows.net	Server admin: [REDACTED] Server password: [REDACTED]
charli-db	connectionstring: [REDACTED]
DevOps (ProjektManagement, Source Code)	Projekt: https://dev.azure.com/dedi1199/ChatBot Backend Repository: https://dev.azure.com/dedi1199/ChatBot/_git/Charli-Backend Documentation Repository: https://dev.azure.com/dedi1199/ChatBot/_git/Charli-Documentation Login: [REDACTED] Password: [REDACTED]



C. EIGENSTÄNDIGKEITS- ERKLÄRUNG

ERKLÄRUNG

Ich erkläre hiermit,

- dass ich die vorliegende Arbeit selber und ohne fremde Hilfe durchgeführt habe, ausser derjenigen, welche explizit in der Aufgabenstellung erwähnt ist oder mit dem Betreuer schriftlich vereinbart wurde,
- dass ich sämtliche verwendeten Quellen erwähnt und gemäss gängigen wissenschaftlichen Zitierregeln korrekt angegeben habe,
- dass ich keine durch Copyright geschützten Materialien (z.B. Bilder) in dieser Arbeit in unerlaubter Weise genutzt habe

Ort, Datum: Rapperswil, 20.12.2018

Name und Unterschrift der Verfasser

Denis Hodzic

Giuliano De Gani



D. DIALOGFLOW BENUTZERANLEITUNG

1. EINLEITUNG

1.1 ZWECK

Diese Anleitung unterstützt den verantwortlichen Compass Security Mitarbeiter bei der Wartung und Erweiterung des Chatbot Charli. Diese Anleitung erläutert nicht alle Funktionen von Dialogflow, diese sind bereits gut dokumentiert. Dort, wo Kenntnisse über Konzepte erforderlich sind, werden diese Zwecks Einfachheit direkt in dieser Anleitung erläutert, auch wenn sie bereits in anderen Erzeugnissen erklärt wurden.

2. DIALOGFLOW EINFÜHRUNG

2.1 VORAUSSETZUNGEN

Um den Chatbot zu erweitern, benötigt der zuständige Mitarbeiter einen eigenen Google-Account (eine Gmail-Email-Adresse ist ausreichend) und die entsprechende Berechtigung auf das Chatbot-Charli Dialogflow-Projekt.

2.2 LOGIN / REGISTRIERUNG

Über www.dialogflow.com gelangt man auf die Übersichtsseite von Dialogflow. In der rechten oberen Ecke auf der Webseite kann zur Konsole gewechselt werden. Nach der Authentifizierung mit dem Google Account gelangt man zur Dialogflow Console, dem Web-User-Interface von Dialogflow.

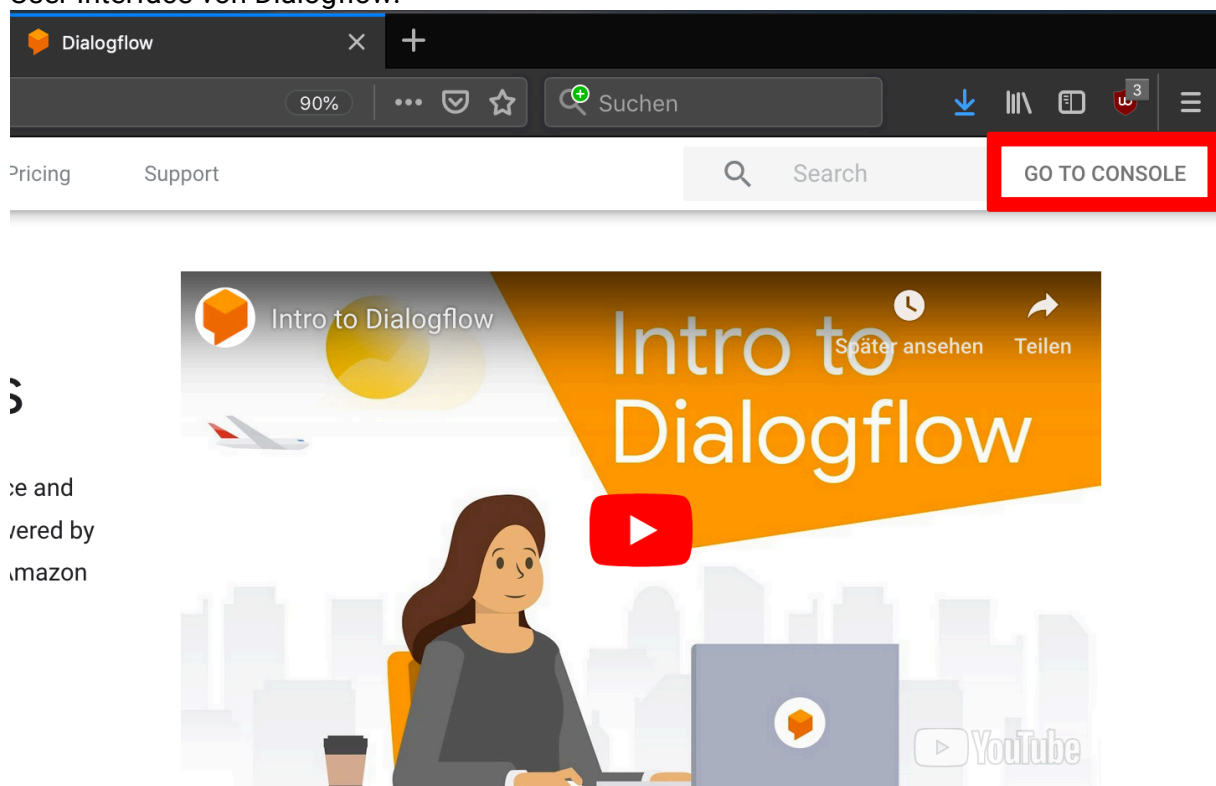


Abbildung 34 Dialogflow Übersichtsseite

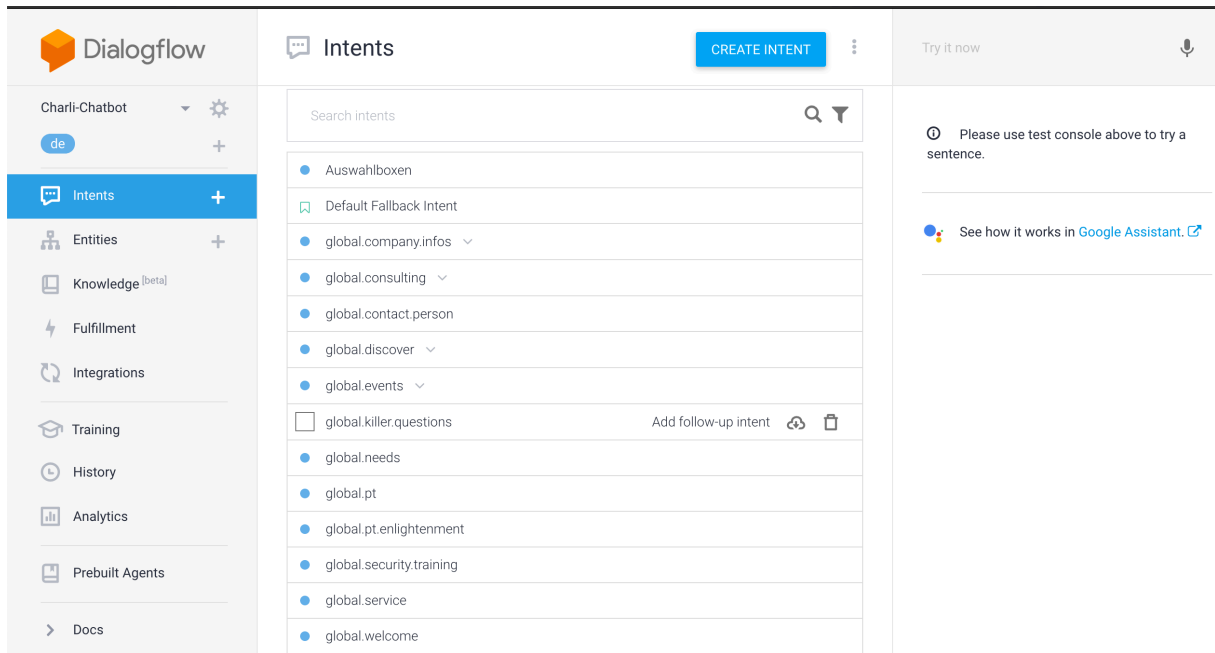


Abbildung 35 Dialogflow Console Intents

2.3 AGENT

Agenten bilden die Basis eines jeden Chatbots in Dialogflow. Sie enthalten die definierten Intents und das Gesprächsmodell.

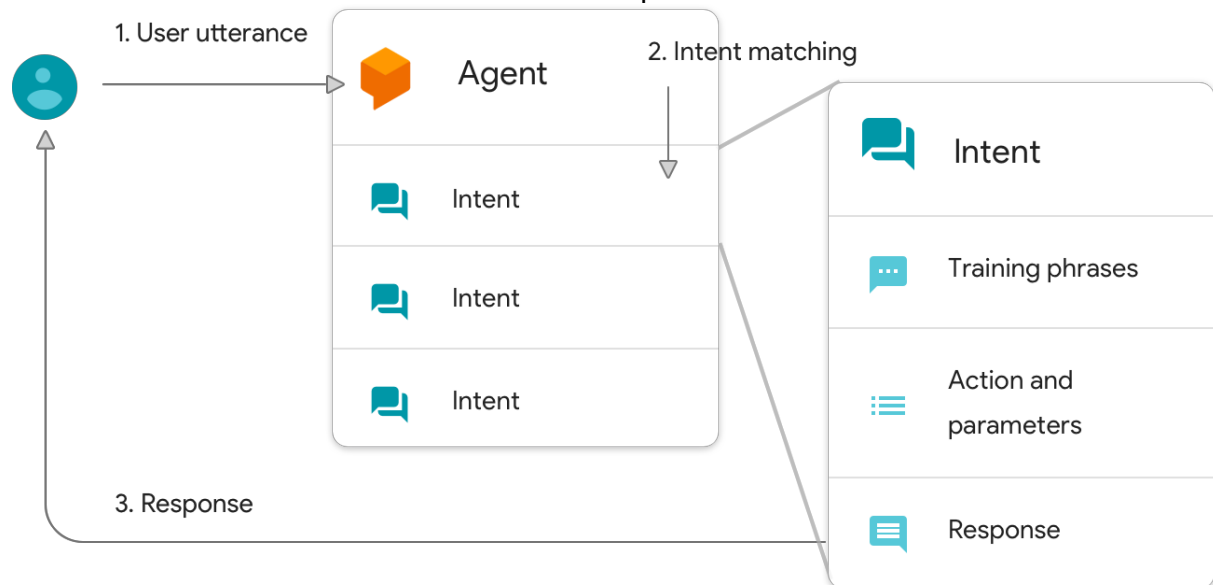


Abbildung 36 Übersicht Agent in Dialogflow³⁶

Über das Dropdown Menü auf der linken Seite kann ein neuer Agent hinzugefügt werden.

³⁶ Quelle : <https://dialogflow.com/docs/agents>

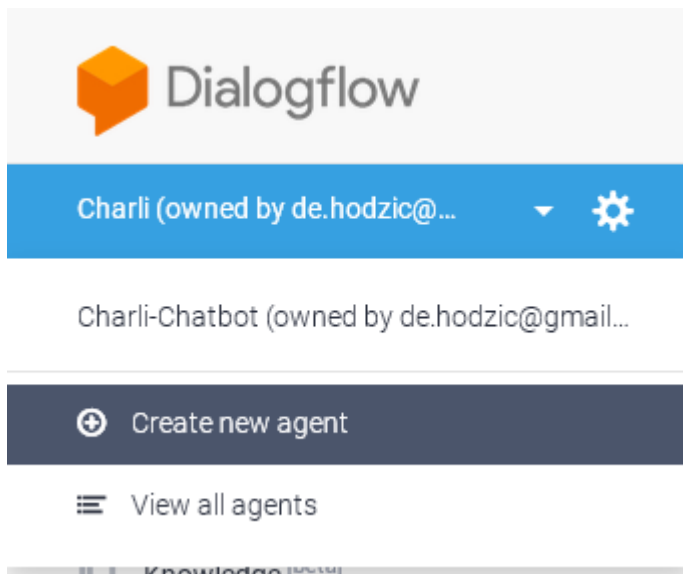


Abbildung 37 Neuer Agent

2.4 EINSTELLUNGEN

Unter Einstellungen können neue Mitglieder hinzugefügt werden und deren Rollen konfiguriert werden:

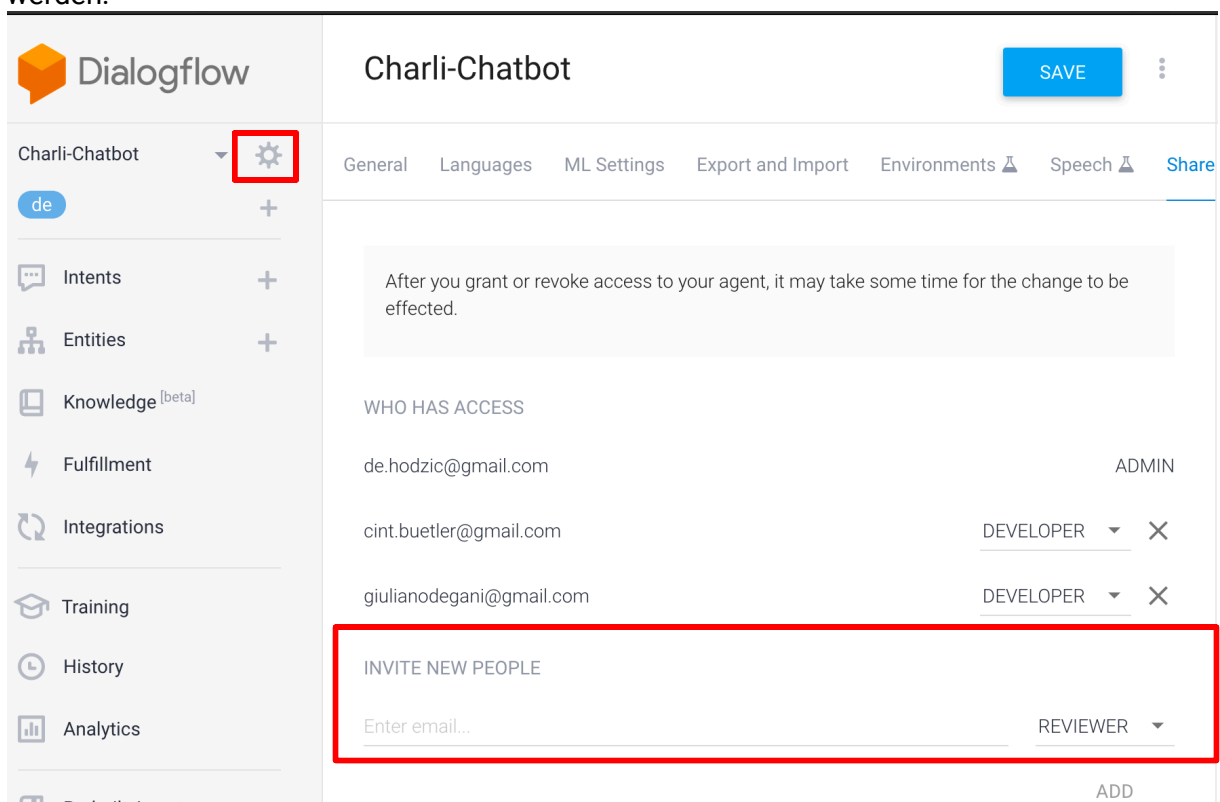


Abbildung 38 Dialogflow Console Einstellungen

2.5 INTENTS

Intents sind Zustände, in welche sich ein User versetzt, wenn er etwas Bestimmtes geschrieben hat. Sie bilden die Basis für die Gesprächsmodellierung und enthalten die Antworten und Contexts.

Mit dem Button «Create Intent» wird ein neuer Intent erstellt. Auf diesem Layer werden nur global Intents erstellt. Globale Intents sind hierarchisch auf der obersten Ebene, also keine Follow-up intent (Namenskonvention).

Jeder Intent muss eindeutig benannt werden.

2.5.1 CREATE INTENT

Intents

CREATE INTENT

Search intents

Auswahlboxen Add follow-up intent

Default Fallback Intent

global.company.infos

global.consulting

global.contact.person

global.discover

global.events

Abbildung 39 Erstellen eines neuen Intents

2.5.1.1 TRAINING PHRASES

Trainingsphrasen dienen dem Natural Language Understanding Service dazu, das neuronale Netz für die Klassifizierung der Texteingabe auf den Katalog der Intents zu trainieren. Im Beispiel dieses «Security Review» Intent, sind entsprechende Trainingsphasen eingerichtet, welche die Absicht beschreiben, ein Security Review machen zu wollen.

Das Wort «Security Review» ist gelb markiert, weil Dialogflow erkennt, dass dieses Wort zu dem selbst definierten Entity «service» gehört. Auf die Entities wird im Kapitel Entites genauer darauf eingegangen.

Training phrases ?

Search training pl

” Add user expression

” ich möchte einen Security Review bestellen

PARAMETER NAME	ENTITY	RESOLVED VALUE
service	@service	Security Review

” Security Review

” Ich brauche einen Security Review

Abbildung 40 Intent für Security Review

2.5.1.2 ACTION AND PARAMETERS / SLOT FILLING

Unter dieser Rubrik wird das Slot Filling konfiguriert.

Pro Zeile kann ein «Slot» eingerichtet werden, welcher mit einer Variablen verknüpft wird. Diese Variablen werden vom Chatbot automatisch mit Werten abgefüllt, wenn die entsprechenden Entities in den Textinputs erkannt werden.

Sind diese Parameter als «required» markiert, erscheint zusätzlich die Option «Prompts». In den Prompts werden Fragen festgelegt, die der Chatbot zwecks Abfüllen des Slots stellt. Ist Slot Filling aktiv, kann der Intent erst verlassen werden, wenn sämtliche als «required» markierte Parameter abgefüllt wurden.

Im Beispiel des «Security Review» Intents, soll der Chatbot den Grund erfahren, wieso der Kunde ein Security Review durchführen lassen möchte. «@reason» ist ein Entity, welches einen Katalog von möglichen Gründen enthält. Der Chatbot wird die Variable \$reason mit einem Wert aus dem Entity @reason abfüllen, sofern dieses erkannt wird.

In der nachfolgenden Tabelle werden die Optionen kurz beschrieben.

OPTION	BESCHREIBUNG
required	required wird ausgewählt, wenn Informationen vom Kunden benötigt werden. Diese Auswahl aktiviert das Slot Filling und die Option «Prompts».
Parameter Name	Der Name des Parameters.
Entity	Unter dem angegebenen Entity werden die zu erwartenden Antworten des Kunden zu finden sein. Nur wenn diese übereinstimmen, kann die Konversation fortgesetzt werden.
Value	Die Variable, welche den Wert enthält. Sie kann in der Antwort verwendet werden und wird mit den Output Contexts mitgegeben.



OPTION	BESCHREIBUNG
Prompts	Frage an den Kunden, um die Informationen zu erhalten.

Action and parameters

REQUIRED	PARAMETER NAME	ENTITY	VALUE	IS LIST	PROMPTS
<input type="checkbox"/>	service	@service	\$service	<input type="checkbox"/>	—
<input checked="" type="checkbox"/>	reason	@reason	\$reason	<input type="checkbox"/>	Wieso möchten Sie...
<input checked="" type="checkbox"/>	recommendation	@recommendation	\$recommendation	<input type="checkbox"/>	Wie sind Sie au...

+ New parameter

Abbildung 41 Slot Filling Beispiel im Security Review Intent

Prompts for "reason"

NAME	ENTITY	VALUE
reason	@reason	\$reason

PROMPTS

- 1 Wieso möchten Sie einen Security Review bestellen?
- 2 Enter a prompt variant

CLOSE

Abbildung 42 Prompts beim Slot Filling

Es können alternative Prompts definiert werden. Es wird zufällig eine dieser Prompts verwendet, um Abwechslung in die Fragen zu bringen.

2.5.1.3 RESPONSES

Responses enthalten die Antworten oder Rückfragen, welche vom Chatbot genutzt werden, wenn der User in den Intent gesprungen ist.

Responses können einfache Textantworten oder aber Bilder, Auswahlknöpfe bis selbstdefinierte Antwortstrukturen sein. Das Dialogflow Web UI erlaubt lediglich simple Textantworten, weshalb im Weiteren nicht mehr auf die Rich Response Möglichkeiten eingegangen werden.

Responses werden genutzt, um das Gespräch weiter zu führen. Im Beispiel des «Security Review» Intents wird mit einer Folgefrage das Gespräch am Laufen gehalten und in eine Richtung gelenkt.

Alternative Responses dienen dazu, Variation einzubringen.

Durch Auswahl des ToggleButtons «Set this intent as end of conversation» definiert man das Ende des Chats.

Responses ?

DEFAULT GOOGLE ASSISTANT +

Text response ? 🗑️

- 1 Vielen Dank für Ihre Angaben. Sie haben als Grund " \$reason " angegeben.
Können Sie mir bitte noch angeben, auf welchem Betriebssystem in Ihrer Firma gearbeitet wird?
- 2 Enter a text response variant

ADD RESPONSES

Set this intent as end of conversation ?

Abbildung 43 Beispiel Text response



2.5.2 FOLLOW-UP INTENT

Follow-up Intents sind dazu da, das Gespräch zu führen. Ein Follow-up Intent erzeugt beim «Parent» Intent einen Output-Context und den korrespondierenden Input-Context. Damit ist der Follow-up Intent nicht mehr global erreichbar.

Wenn mit Follow-up Intents gearbeitet wird, müssen sämtliche mögliche Intents abgedeckt werden, da ansonsten das Gespräch nicht weitergeführt werden kann.

Durch das Überfliegen mit der Maus über den Intent «global.security.review» erscheint die Option «Add follow-up Intent».

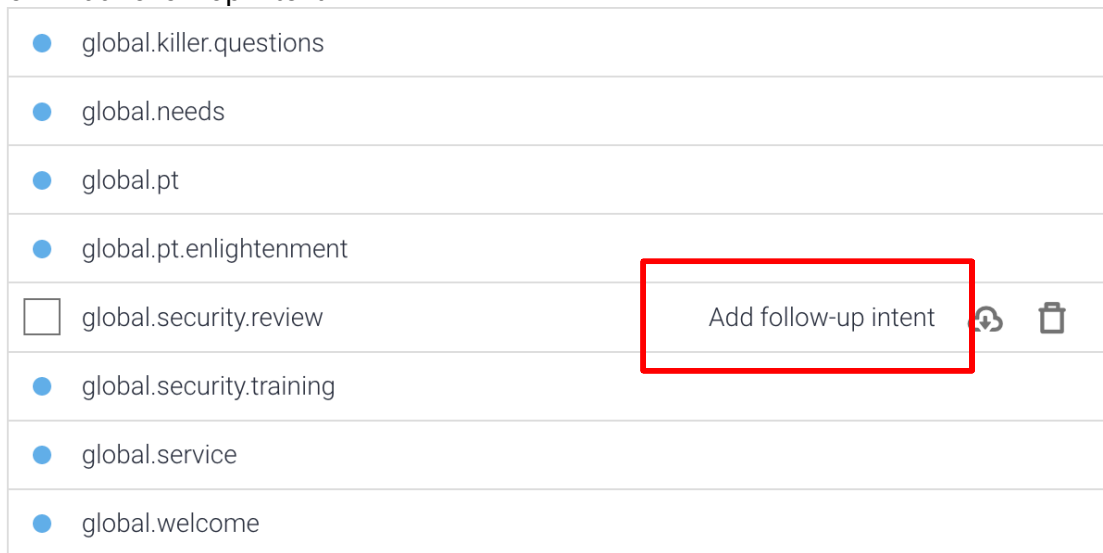


Abbildung 44 Erzeugen eines Follow-up Intent

Es gibt eine Reihe von vordefinierten Follow-up Intents. Diese sind selbsterklärend. Zum Beispiel wird durch Auswahl der «yes» Option ein Intent erstellt, welcher alle möglichen positiven Antworten auflistet, um in diesen Intent zu wechseln.

In diesem Beispiel wird ein custom Follow-up Intent erstellt:

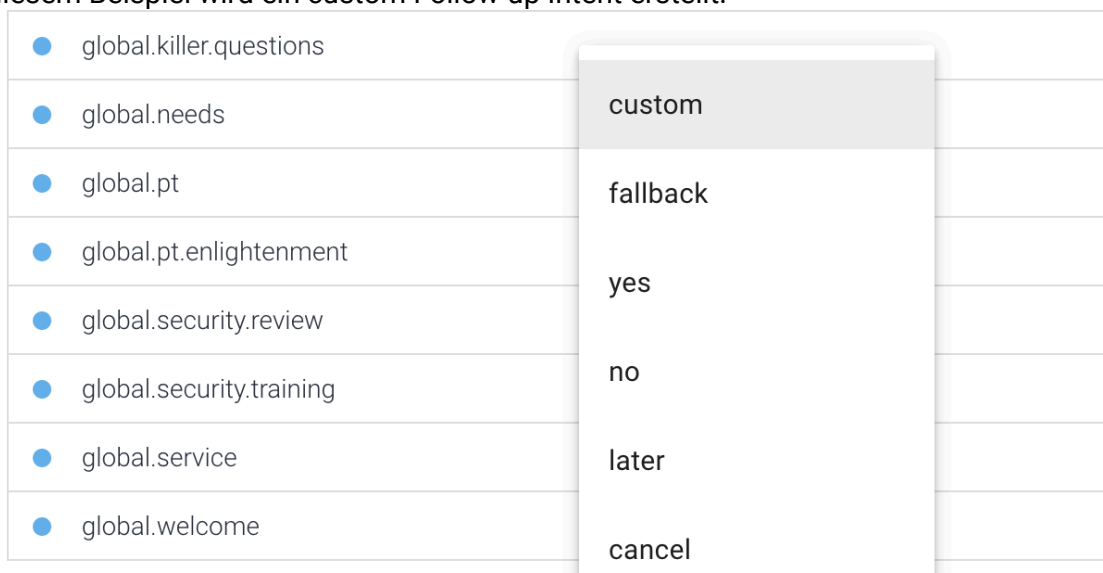


Abbildung 45 Custom Follow-up Intent



Der neu erstellte Intent kann jetzt bearbeitet werden.

- global.needs
- global.pt
- global.pt.enlightenment
- global.security.review ^
- ↪ global.security.review - custom
- global.security.training
- global.service
- global.welcome

Abbildung 46 Erstellter Follow-up Intent

Für die Namenskonvention wird empfohlen, den Intent als Erstes umzubenennen, da er nicht mehr global erreichbar ist.

Folgende Abbildung zeigt, wie ein Input Context erzeugt wurde, welcher passend zum Output Context im übergeordneten «global.security.review» passt. Damit wird der Gesprächspfad in Dialogflow modelliert.

- security.review.os SAVE ⋮

Contexts ? ^

globalsecurityreview-followup ⊗ Add input context

Add output context ⊗

Abbildung 47 Input Context im neuen Follow-up Intent



• global.security.review

SAVE



Contexts ?



Add input context

2

globalsecurityreview-followup



Add output context



Abbildung 48 Output Context im Parent Intent

2.5.3 CONTEXT VERWENDUNG

Wenn Informationen über Intents hinweg benötigt werden, kommen Output Contexts zur Anwendung.

In nachfolgenden Beispiel wurden per Slot Filling Variablen abgefüllt, welche im nächsten Intent über den «companydata» Context verfügbar sein sollen. Der Zugriff auf diese Werte erfolgt mit der Syntax #<context_name>.<parameter_name>.

Contexts ?



globalsecurityreview-followup



Add input context

5

companydata



Add output context



Abbildung 49 Ausgehende Informationen im companydata Context

• global.company.infos

SAVE

Contexts ?

companydata (X) Add input context

2 CScompanyInfos-followup (X) Add output context (X)

Abbildung 50 eingehende Informationen im companydata Context

2.5.3.1 PROBLEME MIT CONTEXT

Wenn mehrere Contexts im Input Context definiert werden, bedeutet das, dass dieser Intent nur dann erreicht werden kann, wenn beide Contexts instanziiert wurden. Das hat zur Konsequenz, dass das Gesprächsmodell keine Zusammenführung erlaubt.

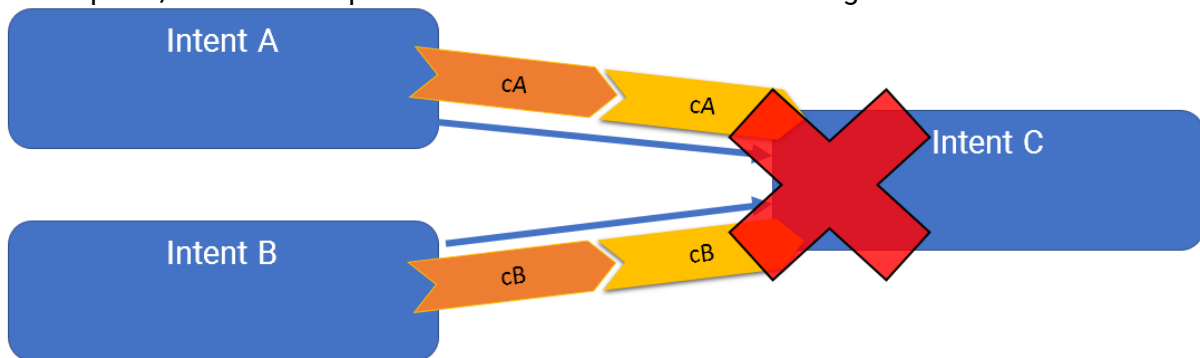


Abbildung 51 Zusammenführen nicht möglich

Eine Lösung ist, dass cA und cB als ein und derselbe Context bezeichnet wird, so dass Intent C lediglich einen Input Context besitzt.

Alternativ kann das Gespräch umstrukturiert werden, so dass sowohl cA als auch cB als Instanzen existieren:

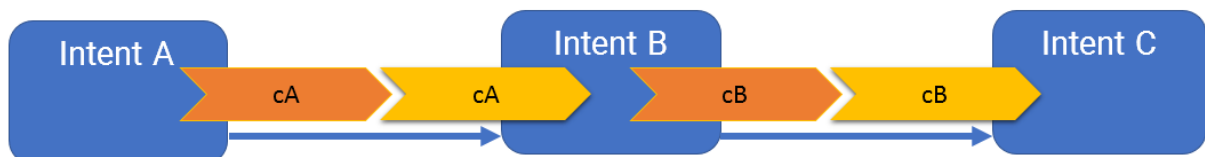


Abbildung 52 Context Sequenz

2.5.4 DEFAULT FALLBACK

Beim Erstellen eines Agenten wird ein Standard Fallback Intent erzeugt. Dieser enthält bereits eine Vielzahl von statischen Textantworten, wie zum Beispiel "Ich habe das nicht verstanden. Kannst du es noch einmal sagen?". Dieser Intent wird erreicht, wenn die Eingaben des Kunden keinem anderen Intent zugeordnet werden können.

Es ist möglich, weitere Fallbacks einzurichten. Dies bringt den Vorteil, dass die Antworten spezifischer gestaltet werden können und dass der Context nicht sofort verloren geht.

Ein Fallback Intent wird analog analog zu einem Follow-up Intent über den Button auf der rechten Seite innerhalb der Intentliste erzeugt:

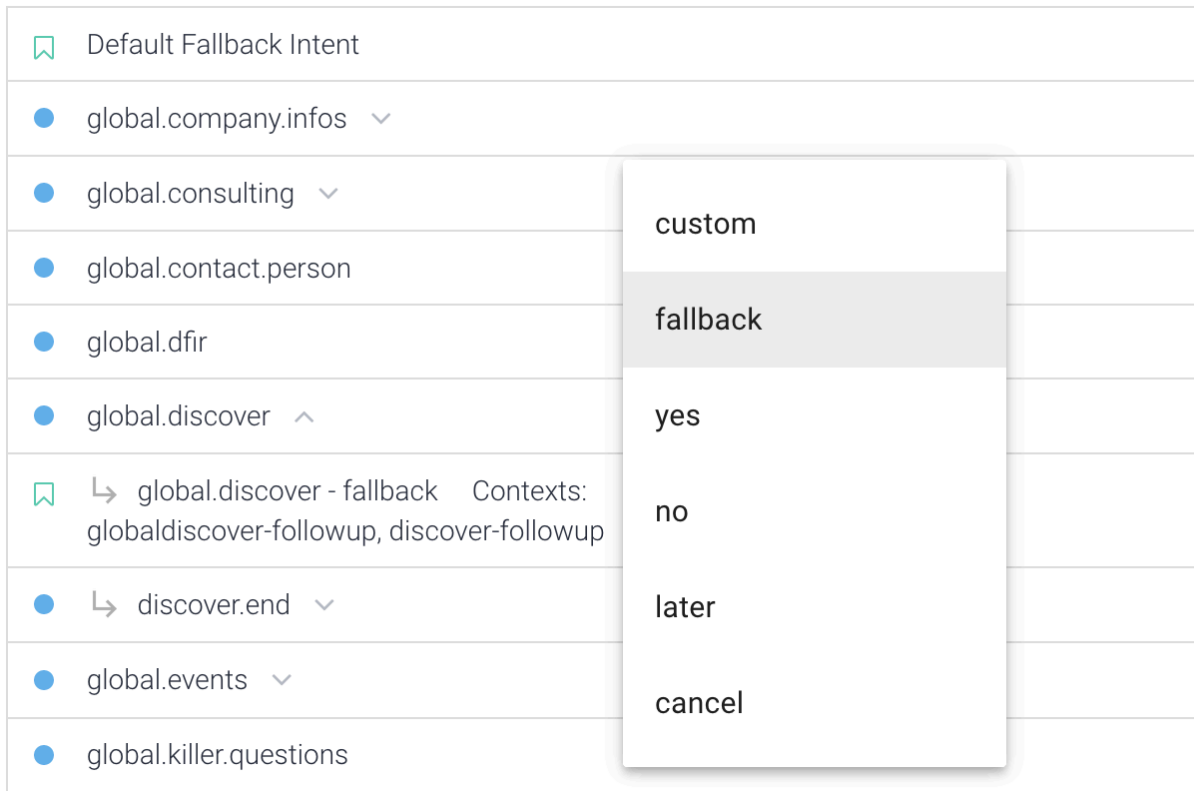


Abbildung 53 Erstellen des Fallback Intents



2.6 ENTITIES

Durch Auswahl der Entities Rubrik auf der linken Seite, wird die Übersicht der erstellten Entites aufgezeigt.

Entities definieren Wertebereiche für Variablen, welche beim Slot Filling ausgefüllt werden. Entities können mit Synonymen angereichert werden. Diese Liste der Entity Synonyme dient ebenfalls als Trainingssatz für die NLP Einheit, das heisst auch Entities werden über die Texterkennungsmechanismen erkannt. Nur wenn die Antwort des Kunden und ein Eintrag vom Entity passend sind, wird der Wert als Entity erkannt und in die Variable gesetzt.

2.6.1 SYSTEM ENTITIES

Systementities sind vorgefertigte Entities, die von Dialogflow zur Verfügung gestellt werden, um die Handhabung mit gängigen Daten wie Ortschaft oder Zeitangaben zu erleichtern. Eine Übersicht aller System Entities ist unter folgendem Link einsehbar:

<https://dialogflow.com/docs/reference/system-entities>



2.6.1.1 VERWENDETE SYSTEM ENTITES

ENTITIES	INTENT
@sys.any	company.infos person.infos noidea.person.infos discover.person.infos
@sys.location	company.infos
@sys.phone-number	person.infos noidea.person.infos discover.person.infos
@sys.email	person.infos
@sys.date	pt

Tabelle 61 Verwendete System Entities

2.6.2 EIGENE ENTITIES ERSTELLEN

Für den eigenen Anwendungsfall reichen System Entities nicht aus. Zu diesem Zweck lassen sich eigene Entities definieren.

Über das Entities Menü und dem «+» lässt sich ein Entity hinzufügen:

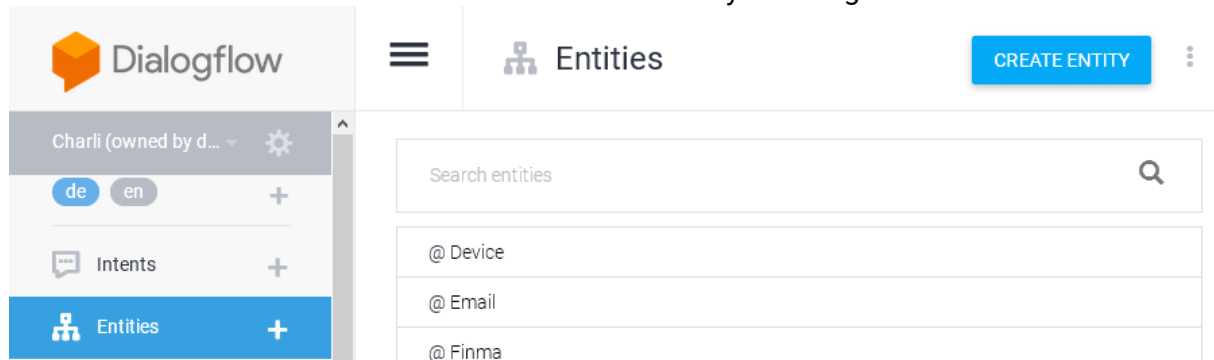


Abbildung 54 Entity erstellen

Im folgenden Beispiel wird ein «operatingsystem» Entity erstellt, welches den Wertebereich von möglichen Betriebssystemen enthalten soll:



operatingsystem

SAVE

 Define synonyms  Allow automated expansion

linux	linux
ubuntu	ubuntu
windows	windows, windows 10, windows xp, windows vista, windows server
mac os	mac os, mac, MacOS
Unix	Unix
Click here to edit entry	

[+ Add a row](#)**Abbildung 55 Beispiel Entity operatingsystem**

Das Entity erhält den Bezeichner «operatingsystem».

Zu sehen sind die möglichen Werte (erste Spalte) und ihre entsprechenden Synonyme (zweite Spalte), falls die «Define synonyms» Option aktiviert ist.

Mit der Option «Allow automated expansion» können Werte erkannt werden, die nicht explizit im Entity aufgeführt sind. Wird diese Funktion genutzt gilt es folgende Punkte zu beachten:

- Endliche Listen sollten vollständig erfasst werden. Bei Teillisten und der aktivierten Option «Allow automated expansion» können ungeeignete Einträge entstehen.
- Wenn die Option « Allow automated expansion » in mehr als einem Entity desselben Agenten aktiviert wurde, kann dies zu Konflikten und unerwarteten Klassifizierungsergebnissen führen.³⁷

³⁷ Quelle: <https://dialogflow.com/docs/entities/create-manage-entities>



2.6.3 VERWENDUNG EINES ENTITIV

Das erstellte Entity kann nun unter der «Action and parameters» Rubrik innerhalb eines Intentns verwendet werden:

● security.review.os SAVE ⋮

Action and parameters ^

globalsecurityreview.globalsecurityreview-custom ///

REQUIRED ?	PARAMETER NAME ?	ENTITY ?	VALUE	IS LIST ?	PROMPTS ?
<input checked="" type="checkbox"/>	operatin	@opera tingsyst em	\$operati ngsyste m	<input type="checkbox"/>	Bitte geben Sie...
<input type="checkbox"/>	Enter na	Enter en	Enter	<input type="checkbox"/>	—

[+ New parameter](#)

Abbildung 56 Beispielanwendung eines Entity



2.6.3.1 @ANY ENTITY

Überall dort, wo der Wertebereich zu gross werden kann, zum Beispiel bei der Anzahl von Nachnamen oder Städtenamen, ist es möglich, das «Any» Entity zu verwenden. Dieses akzeptiert jede Eingabe.

Bei der Verwendung dieses System Entity gilt es folgendes zu beachten:

Es kann sein, dass der Kunde auf die Frage nach seinem Namen wie folgt antwortet: «Mein Name ist Peter». Der abgefüllte Wert des «Any» Entity ist demnach nicht «Peter» sondern die gesamte Texteingabe.

2.6.3.2 SLOT FILLING HERAUSFORDERUNGEN

Werden mehrere Slots abgefüllt, kann es vorkommen, dass über das Matching der Entities, falsche Slots abgefüllt werden. Dies kann dann auftreten, wenn ein Städtename gleichzeitig auch ein Nachname darstellt, wie zum Beispiel «Paris». Um dieses Problem zu umgehen, sollte die Reihenfolge des Slot Fillings geschickt gewählt werden, oder die Slots auf mehrere Intents aufgeteilt werden.

2.7 KNOWLEDGE BASES

Knowledge Bases kommen zur Anwendung, wenn es bereits Dokumente in Form von «Key, Value» Paaren gibt, wie zum Beispiel FAQ's. Das Feature ist zum Zeitpunkt der Bachelorarbeit im Herbstsemester 2018 im Beta Stadium und nur für englische Agenten verfügbar.

2.8 FULFILLMENT

Fulfillment ist Code, der als Webhook bereitgestellt wird, mit dem der Dialogflow-Agent die Geschäftslogik gezielt aufrufen kann. Während eines Gesprächs ermöglicht Fulfillment, die durch die natürliche Sprachverarbeitung von Dialogflow extrahierten Informationen zu nutzen, um dynamische Reaktionen zu erzeugen oder Aktionen im Backend auszulösen.³⁸

Fulfillment wird unter anderem dazu genutzt, um

- dynamische Reaktionen basierend auf Informationen aus einer Datenbank zu generieren.
- Bestellungen auf der Grundlage von Produkten aufzugeben, die ein Kunde angefordert hat.

Um Fulfillment einzusetzen, muss ein Webhook konfiguriert werden, der in der Lage ist, POST Webhook Requests zu verarbeiten. Die Anforderungen an einen solchen Endpunkt, sind unter <https://dialogflow.com/docs/fulfillment> dokumentiert.

Für einfache Anwendungen bietet Dialogflow einen Inline Editor, in welchem simples Javascript über die «Cloud Functions» von Firebase ausgeführt werden können.

Falls der Webhook Call erfolglos war, wird stattdessen eine alternative Antwort aus den Text responses zurückgegeben.

³⁸ Quelle: <https://dialogflow.com/docs/fulfillment>



⚡ Fulfillment

Webhook

ENABLED 

Your web service will receive a POST request from Dialogflow in the form of the response to a user query matched by intents with webhook enabled. Be sure that your web service meets all the [webhook requirements](#) specific to the API version enabled in this agent.


URL*	<u>https://charli.azurewebsites.net/api/webhook</u>	
BASIC AUTH	<input type="text" value="Enter username"/>	<input type="text" value="Enter password"/>
HEADERS	<input type="text" value="Enter key"/>	<input type="text" value="Enter value"/>
	<input type="text" value="Enter key"/>	<input type="text" value="Enter value"/>
		
DOMAINS	<input type="text" value="Disable webhook for all domains"/> ▼	

Abbildung 57 Fulfillment Webhook Charli

2.9 INTEGRATIONS

Mit Integrationen wird der Chatbot verfügbar gemacht. Für eine Reihe gängiger Messaging Plattformen wie Slack, Facebook Messenger und Twitter bietet Dialogflow Ein-Klick Integrationen.

Dialogflow ermöglicht es auch, den Chatbot in andere natürliche Sprachversorgungsplattformen (NLU) wie Amazon Alexa und Microsoft Cortana zu exportieren oder von dort zu importieren.³⁹

³⁹ Quelle: <https://dialogflow.com/docs/integrations>



2.10 ANLEITUNG INTEGRATION

Das Vorgehen bezüglich der Integration hängt von der Zielplattform ab. Die entsprechenden Anleitungen sind entsprechend hinterlegt und werden beim Klick auf die Schaltflächen angezeigt.

Abbildung 58 Integrationsübersicht

2.11 TRAINING

Die natürliche Sprachverarbeitung (NLP) von Dialogflow basiert auf maschinellem Lernen. Für die Verbesserung der Erkennung, also der Klassifizierung, von Intents anhand der Texteingaben, existiert die Trainingsmöglichkeit.

Die Trainings werden anhand von protokollierten Gesprächen durchgeführt.

Über den Menüpunkt «Training» gelangt man in die Trainingsdarstellung, welche die protokollierten Gespräche auflistet.

Conversation	Requests	No match	Date	
hallo	40	4	Nov 13	>
das gespräch beenden	10	2	Nov 13	>

PREVIOUS NEXT

Abbildung 59 Trainingsübersicht



Mit einem Klick auf ein protokolliertes Gespräch öffnet sich der Trainingsdialog. Dort werden nicht erkannte Texteingaben hervorgehoben. Durch das Zuweisen eines Intents, wird die Texteingabe zum Katalog der Trainingsphrasen automatisch hinzugefügt. Nach Verlassen des Trainingsdialogs wird ein Agententraining gestartet.

hallo APPROVE

Today 32 REQUESTS 6 NO MATCH

INTENT [global.security.review](#)

CONTEXT OUTglobalsecurityreview-followup

USER SAYS

INTENT [global.needs](#)

CONTEXT OUTneeds-followup

USER SAYS

INTENT [global.welcome](#)

CONTEXT OUTsecreview sectraining pentest

USER SAYS

! INTENT [Click to assign](#)

Abbildung 60 Trainingsdialog mit unbekanntem Intent

2.12 HISTORY

Die History zeigt die protokollierten Gespräche, deren Dauer und den Zeitpunkt an. Über den Menüpunkt «History» gelangt man zur Übersicht.

Dialogflow

Charli (owned by de...)

de en

Intents

Entities

Knowledge [beta]

Fulfillment

Integrations

Training

History

History

All platforms All conversations Dec 3, 2018 - Dec 6, 2018

Conversation	Date
hi (2)	Dec 6
hi (2)	Dec 6
hi (5)	Dec 6
hallo (1)	Dec 6
hallo (1)	Dec 6
hallo (1)	Dec 6

Abbildung 61 Übersicht History



Durch Öffnen eines protokollierten Gesprächs lassen sich sämtliche Textein- und Ausgaben nachlesen.

Conversation	Date	
USER meier	Dec 17, 1:56 PM	
AGENT Und Ihre Telefonnummer unter welcher wir Sie erreichen können: (Ohne Leerzeichen)	Dec 17, 1:56 PM	⋮
USER +41788819292	Dec 17, 1:56 PM	
AGENT Unter welcher E-Mail Adresse können wir Sie kontaktieren?	Dec 17, 1:56 PM	⋮
USER kunde@hsr.ch	Dec 17, 1:56 PM	
AGENT Darf ich noch fragen wie Sie auf uns aufmerksam wurden?	Dec 17, 1:56 PM	⋮
USER durch google	Dec 17, 1:56 PM	
AGENT Vielen Dank Herr meier, wir werden die Informationen auswerten und Sie kontaktieren.	Dec 17, 1:56 PM	⋮

Abbildung 62 Protokolliertes Gespräch

2.13 ANALYTICS

Die Analyseseite ermöglicht einen Einblick in diverse Metriken und Leistungsindikatoren des Agenten. Die Analyse kann zum Beispiel dazu verwendet werden, um den kritischen Gesprächspfad ausfindig zu machen und diesen gezielt zu verbessern.

Es werden zwei Arten von Daten aufgezeigt, die sich auf den Chatbot und die Konversationen beziehen, an denen er beteiligt war:

- Nutzungsdaten: Anzahl der Sitzungen und Abfragen pro Sitzung.
- NLP-Daten: Am häufigsten verwendete Absichten und Austrittswahrscheinlichkeiten.⁴⁰

⁴⁰ Quelle: <https://dialogflow.com/docs/training-analytics/analytics>

 Analytics

Last 7 days ▾

Intents 

Intent	Sessions	Count	Exit %	Agent response time
global.welcome	19	155	8.39%	
global.security.review	5	54	1.85%	
global.events	10	49	30.61%	
global.pt	3	42	2.38%	
global.consulting	7	29	0%	
global.service	8	29	3.45%	
global.pt.enlightenment	3	28	3.57%	
chat.consulting	7	27	0%	
consulting.noidea	3	27	7.41%	

Abbildung 63 Analyse Intent

3. ERWEITERUNGEN

3.1 NEUE DIENSTLEISTUNG HINZUFÜGEN

3.1.1 KONZEPT

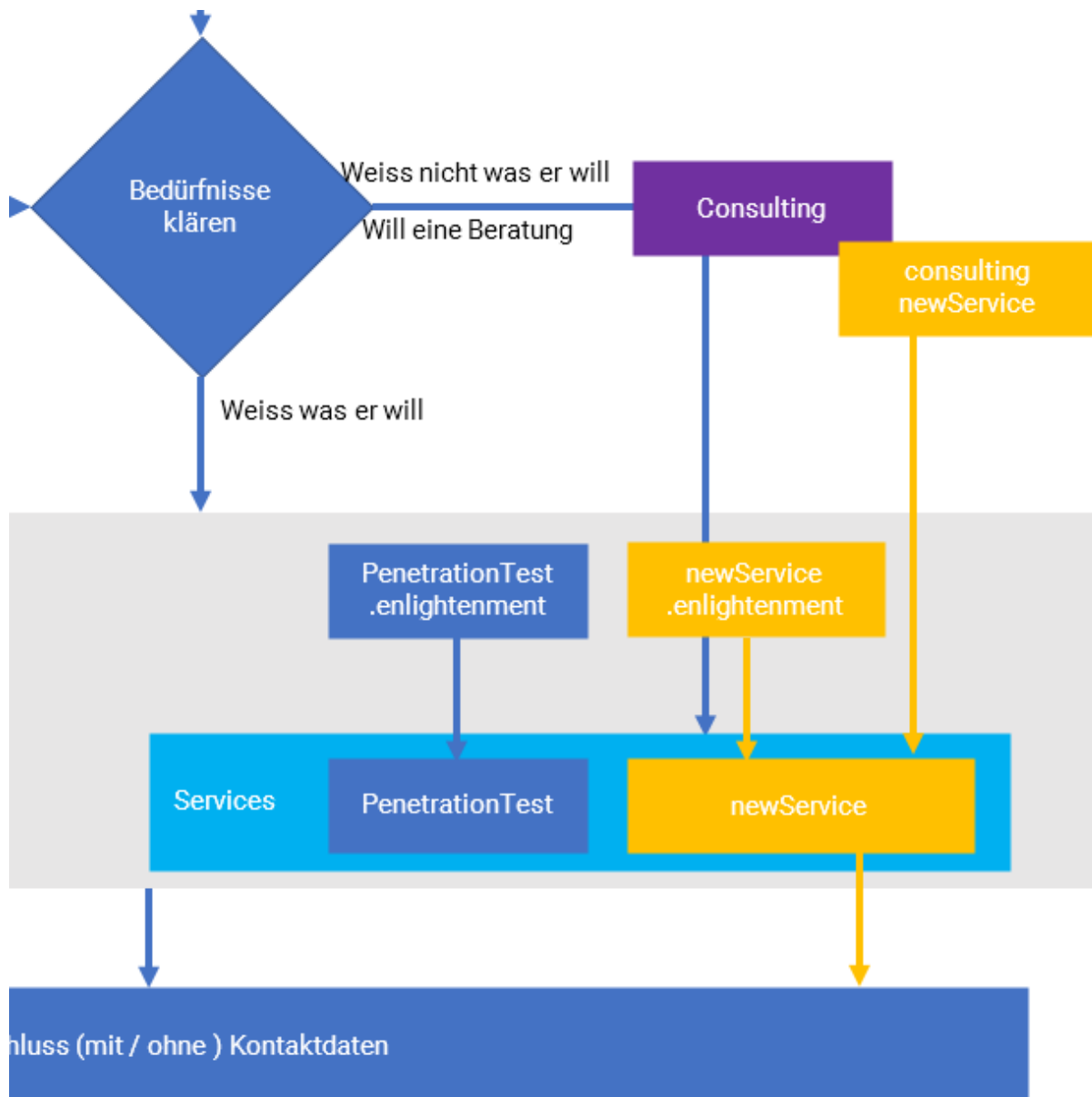


Abbildung 64 Konzept beim Hinzufügen einer Dienstleistung

Dieser Ausschnitt des Gesprächsmodellierungskonzepts zeigt die Erweiterungen in Gelb. Intents werden als Boxen, (Input- und Output) Contexts, als Pfeile abgebildet.

3.1.2 DIENSTLEISTUNGSINTENT ERSTELLEN

Um eine neue Dienstleistung hinzuzufügen erstellt man zunächst einen neuen Intent («newService»). In diesem Intent werden später mittels Slot Filling Verfahren alle benötigten Informationen gesammelt, damit für diese Dienstleistung eine Offerte erstellt werden könnte.



3.1.3 DIENSTLEISTUNG ENLIGHTENMENT ERSTELLEN

Bevor ins Slot Filling der neuen Dienstleistung «newService» gewechselt wird, muss festgestellt werden, ob der Kunde überhaupt Erfahrungen mit der Dienstleistung hat und weshalb er diese Dienstleistung bestellen möchte.

3.1.4 BERATUNG ERWEITERN

Da eine neue Dienstleistung hinzugefügt wurde, muss diese auch über ein Beratungsgespräch erreichbar sein. Zu dem Zweck wird ein neuer Follow-up Intent unter dem «consulting» Intent erstellt. In diesem Follow-up Intent werden Erklärungen zur neuen Dienstleistung bereitgestellt.

3.1.5 CONTEXTS SETZEN

Um in die neue Dienstleistung zu wechseln, müssen Contexts richtig definiert werden. Im neu erstellten «newService» Intent wird ein Input Context definiert und derselbe Context als Output Context aus den zuvor erstellten «newService.enlightenment» und «consulting.newService» konfiguriert. Der Contextname muss einmalig sein und sollte einen Bezug zum Intent herstellen.

3.1.6 ANTWORTEN ANPASSEN

Um die Userführung zu gewährleisten, werden die neuen «Pfade» in bestimmten Antworten als mögliche Option ergänzt.

In den Intents «global.service» und «consulting» werden dem Kunden alle Dienstleistungen angezeigt. Hier muss die neue Dienstleistung ergänzt werden.



E. SYSTEM TESTS

EINFÜHRUNG

ZWECK

Dieses Dokument enthält die Konversationen der Funktionalen Anforderungen.

VORRAUSSETZUNGEN

Für die Ausführung sind ein Google Account und die entsprechenden Berechtigungen auf Dialogflow erforderlich.

VORBEREITUNG

Die Systemtests werden direkt auf Dialogflow ausgeführt und bewertet. Die Konversation startet jedesmal wie folgt:

Denis [16:47 Uhr]
hallo

charli APP [16:47 Uhr]
Willkommen bei der Compass Security.

Mein Name ist Charli und ich kann Ihnen über Folgendes Auskunft geben:

- Dienstleistungen*
- Compass Security kennenlernen*
- Events*
- Beratung*

Wie kann ich Ihnen helfen?



SYSTEM TESTS PROTOKOLL

Die Systemtests werden entsprechend den verschiedenen Use Cases aufgebaut, welche im Kapitel Anforderungsspezifikation des Technischen Berichtes definiert sind.

UC 1: MENSCHLICHEN MITARBEITER BEANTRAGEN

KONVERSATION	STATUS
	NICHT ERFÜLLT
<p>Denis [16:47 Uhr] ich möchte mit jemandem telefonieren</p> <p>charli APP [16:47 Uhr] Unter folgendem Link finden Sie Ihre möglichen Ansprechpartner: https://www.compass-security.com/profil/ansprechpartner/</p>	
KONVERSATION	STATUS
	ERFÜLLT
<p>Denis [16:28 Uhr] beratung</p> <p>charli APP [16:28 Uhr] Wünschen Sie, dass Sie ein Compass Mitarbeiter kontaktiert, oder wollen Sie über diesen Chat beraten werden? Compass Mitarbeiter Chat</p> <p>Denis [16:28 Uhr] compass mitarbeiter</p> <p>charli APP [16:28 Uhr] Gerne, dann werden wir Ihre Daten erfassen und ein Compass Security Mitarbeiter wird sie kontaktieren. Wie heisst Ihre Firma?</p> <p>Denis [16:28 Uhr] siemens</p> <p>charli APP [16:28 Uhr] Wo liegt der Firmensitz?</p> <p>Denis [16:28 Uhr] zürich</p> <p>charli APP [16:28 Uhr] Vielen Dank. Könne Sie mir noch Ihren Vornamen angeben?</p> <p>Denis [16:28 Uhr] denis</p> <p>charli APP [16:28 Uhr] Und Ihren Nachnamen?</p> <p>charli APP [16:28 Uhr] Unter welcher E-Mail Adresse können wir Sie kontaktieren?</p>	



KONVERSATION	STATUS	ERFÜLLT
<p>Denis [16:28 Uhr] denis@hsr.ch</p> <p>charli APP [16:28 Uhr] Darf ich noch fragen wie Sie auf uns aufmerksam wurden?</p> <p>Denis [16:28 Uhr] durch einen kollegen</p> <p>charli APP [16:28 Uhr] Vielen Dank Herr hodzic, wir werden die Informationen auswerten und Sie kontaktieren.</p>		

UC 2: INFORMATIONEN ÜBER UNTERNEHMEN

KONVERSATION	STATUS	ERFÜLLT
<p>Denis [16:39 Uhr] compass security kennenlernen</p> <p>charli APP [16:39 Uhr] Compass Security ist ein Schweizer Unternehmen mit 45 Mitarbeitenden an den Standorten in der Schweiz(Jona, Bern und Zürich) und in Deutschland(Berlin). Im Jahre 1999 durch Walter Sprenger und Ivan Bütler gegründet, hat sich Compass Security zu einem technisch herausragenden und europaweit anerkannten IT Security Unternehmen entwickelt. Compass steht für Vertrauen, Kompetenz und Kundenorientierung. Der Verwaltungsrat besteht aus Ivan Bütler (VRP), Walter Sprenger und Bruno Wildhaber. Sie lenken und entwickeln das eigenfinanzierte und profitable Unternehmen seit ihrer Gründung. Seit 2012 ist Compass Security als Management-Holding organisiert. Compass Security ist strukturell so aufgestellt, dass sie sowohl der starken Nachfrage nach professionellen IT Security Dienstleistungen als auch dem wachsenden Bedürfnis nach Internationalisierung gerecht wird. Ich hoffe ich konnte Ihnen die Compass Security etwas näher Bringen. Wollen Sie nun etwas über unsere Dienstleistungen oder Events erfahren? Oder möchten Sie das Gespräch beenden?</p>		

UC 3: INFORMATIONEN ÜBER DIENSTLEISTUNGEN

KONVERSATION	STATUS	ERFÜLLT
<p>Denis [17:15 Uhr] was habt ihr für dienstleistungen?</p> <p>charli APP [17:15 Uhr] Wir bieten folgende Dienstleistungen an: - Penetration Tests - Security Reviews - Digital Forensics und Incident Response (DFIR) - Security Training Haben Sie Interesse an einer unserer Dienstleistungen oder möchten mehr darüber erfahren?</p> <p>Denis [17:16 Uhr] ja am penetration test</p>		



KONVERSATION	STATUS	ERFÜLLT
<p>charli APP [17:16 Uhr] Weshalb möchten Sie einen Penetration Test durchführen lassen? (Vorfall, Vorstand, Jahreskontrolle, Check, hacking, Unsicherheit, mehr Sicherheit)</p> <p>Denis [17:16 Uhr] ich möchte mehr sicherheit</p> <p>charli APP [17:16 Uhr] Welche untenstehende Beschreibung passt für Sie am besten? A Keine Erfahrung mit Penetration Tests und wünsche eine Beratung B Ich kenne mich mit Penetration Tests aus und möchte die Angaben für ein Angebot angeben</p> <p>Denis [17:16 Uhr] A</p> <p>charli APP [17:16 Uhr] Wünschen Sie, dass Sie ein Compass Mitarbeiter kontaktiert, oder wollen Sie über diesen Chat beraten werden? Compass Mitarbeiter Chat</p>		

UC 4: KRITIK / LOB ÄUSSERN

KONVERSATION	STATUS	TEILS ERFÜLLT
<p>Denis [17:20 Uhr] ihr seid zu teuer</p> <p>charli APP [17:20 Uhr] Danke für Ihr Feedback.</p>		



UC 5: BERATUNG ZU DIENSTLEISTUNGEN

UC 5.1 DIENSTLEISTUNG BESTELLEN

KONVERSATION	STATUS	ERFÜLLT
<p>Denis [17:51 Uhr] ich möchte eine beratung</p> <p>charli APP [17:51 Uhr] Wünschen Sie, dass Sie ein Compass Mitarbeiter kontaktiert, oder wollen Sie über diesen Chat beraten werden? Compass Mitarbeiter Chat</p> <p>Denis [17:51 Uhr] über chat gerne</p> <p>charli APP [17:51 Uhr] Sehr gerne. Welche Art von Beratung wünschen Sie? Wir bieten Beratung über unsere folgende Dienstleistungen an: Penetration Test: - Angreifer Simulation - Schwachstellen detektieren - Massnahmen Sicherheitsniveau Security Review: - Gesamtaussage Verwundbarkeit - Technische Sicherheitsaspekte frühstmöglich einfliessen lassen Digital Forensics und Incident Response (DFIR): - Gegen Cybereinbrüche wappnen - externe Fachspezialsiten für Ernstfälle - Verfügbarkeit und Einsatzzeiten - Permanente Erreichbarkeit von Spezialsiten und Expert Panels Security Training: - Angriffs- und Analysetechniken lernen - Theoretische Grundlagen erlernen</p> <p>Denis [17:52 Uhr] penetration test</p> <p>charli APP [17:52 Uhr] Welche Erfahrungen haben Sie bereits mit Penetration Tests gesammelt?</p> <p>Denis [17:52 Uhr] noch keine</p> <p>charli APP [17:52 Uhr] Weshalb möchten Sie einen Penetration Test durchführen lassen? (ich wurde gehackt, Vorstand, Sicherheitscheck, Neues Produkt)</p> <p>Denis [17:52 Uhr] ich wurde gehackt</p> <p>charli APP [17:52 Uhr] Oje, verstehe. Welche Aussage trifft auf Ihr Bedürfnis eher zu: Analyse: Möchte den Hacker Angriff analysieren und wissen, wer dahinter steckt Schwachstellen: Möchte allgemein die Schwachstelle von unseren IT Systemen kennen</p> <p>Denis [17:52 Uhr] möchte die schwachstellen kennen</p>		



KONVERSATION

STATUS

ERFÜLLT

charli APP [17:52 Uhr]

Dann ist ein Penetration Test die beste Lösung.

Welche Aussage trifft zu:

A:

Ich möchte mit einem Compass Security Mitarbeiter telefonisch einen Penetration Test bestellen

B:

Ich möchte einen Penetration Test über Chat bestellen

Denis [17:52 Uhr]

B

charli APP [17:52 Uhr]

Gegen wann möchten Sie sich schützen? (Script Kiddies, Hacker, Wirtschaftsspionage, Regierung)

Denis [17:53 Uhr]

gegen hacker

charli APP [17:53 Uhr]

Gegen welche Attacken möchten Sie sich schützen? (Internet Attacken, Injection, XSS etc.)

Denis [17:54 Uhr]

internet attacken

charli APP [17:54 Uhr]

Soll es ein Black- oder Whitebox Test sein?

Blackbox: Wir haben keine Insider-Informationen, Vorteil: wir können einen echten Hack-Angriff starten.

Whitebox: Wir haben Insider-Informationen, Vorteil: Wir können das Netzwerk besser testen.

Denis [17:54 Uhr]

whitebox

charli APP [17:54 Uhr]

Welchen Zugang zu Ihrem Netzwerk geben Sie uns? (z.B. Testaccount)

Denis [17:54 Uhr]

keinen

charli APP [17:54 Uhr]

Wer in der Firma sollte davon wissen? (Vorstand, IT-Abteilung, niemand)

Denis [17:54 Uhr]

nur ich

charli APP [17:54 Uhr]

Geben Sie mir bitte ein Datum an (Format: dd:mm:yyyy), wann der Test starten soll.

Denis [17:54 Uhr]

12.1.2019



UC 5.2 KUNDENINFORMATIONEN MITTEILEN

KONVERSATION	STATUS	ERFÜLLT
<p>charli APP [17:54 Uhr] Wir haben vorerst alle Angaben, welche wir für eine Offerte für einen Penetration Test brauchen. Nun brauchen wir Daten über Sie und Ihre Firma. Können Sie den Namen Ihrer Firma nennen?</p>		
<p>Denis [17:54 Uhr] siemens</p>		
<p>charli APP [17:54 Uhr] Wo liegt der Firmensitz?</p>		
<p>Denis [17:54 Uhr] in zürich</p>		
<p>charli APP [17:54 Uhr] Vielen Dank. Könne Sie mir noch Ihren Vornamen angeben?</p>		
<p>Denis [17:54 Uhr] Denis</p>		
<p>charli APP [17:54 Uhr] Und Ihren Nachnamen?</p>		
<p>Denis [17:54 Uhr] Hodzic</p>		
<p>charli APP [17:54 Uhr] Und Ihre Telefonnummer unter welcher wir Sie erreichen können: (Ohne Leerzeichen)</p>		
<p>Denis [17:54 Uhr] 0788888888</p>		
<p>charli APP [17:54 Uhr] Unter welcher E-Mail Adresse können wir Sie kontaktieren?</p>		
<p>Denis [17:54 Uhr] denis.hodzic@hsr.ch</p>		
<p>charli APP [17:54 Uhr] Darf ich noch fragen wie Sie auf uns aufmerksam wurden?</p>		
<p>Denis [17:55 Uhr] durch google</p>		
<p>charli APP [17:55 Uhr] Vielen Dank Herr Hodzic, wir werden die Informationen auswerten und Sie kontaktieren.</p>		



UC 6: KONVERSATION BEENDEN

KONVERSATION	STATUS	ERFÜLLT
<p>Denis [18:11 Uhr] compass kennenlernen</p> <p>charli APP [18:11 Uhr] Compass Security ist ein Schweizer Unternehmen mit 45 Mitarbeitenden an den Standorten in der Schweiz(Jona, Bern und Zürich) und in Deutschland(Berlin). Im Jahre 1999 durch Walter Sprenger und Ivan Bütler gegründet, hat sich Compass Security zu einem technisch herausragenden und europaweit anerkannten IT Security Unternehmen entwickelt. Compass steht für Vertrauen, Kompetenz und Kundenorientierung. Der Verwaltungsrat besteht aus Ivan Bütler (VRP), Walter Sprenger und Bruno Wildhaber. Sie lenken und entwickeln das eigenfinanzierte und profitable Unternehmen seit ihrer Gründung. Seit 2012 ist Compass Security als Management-Holding organisiert. Compass Security ist strukturell so aufgestellt, dass sie sowohl der starken Nachfrage nach professionellen IT Security Dienstleistungen als auch dem wachsenden Bedürfnis nach Internationalisierung gerecht wird. Ich hoffe ich konnte Ihnen die Compass Security etwas näher Bringen. Wollen Sie nun etwas über unsere Dienstleistungen oder Events erfahren? Oder möchten Sie das Gespräch beenden?</p> <p>Denis [18:11 Uhr] gespräch beenden</p> <p>charli APP [18:11 Uhr] Darf ich fragen wie Sie auf uns aufmerksam wurden?</p> <p>Denis [18:11 Uhr] durch einen kollegen</p> <p>charli APP [18:11 Uhr] Vielen Dank. Wollen Sie dass sich ein Compass Security Mitarbeiter später bei Ihnen meldet?</p> <p>Denis [18:11 Uhr] nein danke</p> <p>charli APP [18:11 Uhr] Ich hoffe ich konnte Ihnen weiterhelfen.</p>		

USE CASES FÜR COMPASS SECURITY MITARBEITER

UC 8: LESEN UND LÖSCHEN VON KONVERSATIONEN

KONVERSATION	STATUS	ERFÜLLT
Implizit durch Dialogflow Konsole gegeben -> History Dialogflow.		

UC 9: LESEN UND LÖSCHEN ZUSAMMENFASSUNGEN

Wurde nicht realisiert.	STATUS	NICHT ERFÜLLT
-------------------------	--------	---------------



UC 10: CRUD INTENTS

Implizit durch Dialogflow Konsole gegeben.

STATUS

ERFÜLLT

UC 11: CRUD ENTITIES

Implizit durch Dialogflow Konsole gegeben.

STATUS

ERFÜLLT

UC 12: KONVERSATION ÜBERNEHMEN

Implizit durch Dialogflow Konsole gegeben.

STATUS

ERFÜLLT

UC 13: INTENT TRAINING

Implizit durch Dialogflow Konsole gegeben.

STATUS

ERFÜLLT

UC 14: CRUD KUNDENDATEN

Wurde nicht realisiert.

STATUS

NICHT ERFÜLLT

UC 15: BENACHRICHTIGUNG EINRICHTEN

Wurde nicht realisiert.

STATUS

NICHT ERFÜLLT



F. USABILITY TESTS

VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Kai Knecht, 24, Bauingenieurswesen Student	10.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Keine Bemerkungen
Events anzeigen lassen	Ja	Keine Bemerkungen
Penetration Test bestellen	Ja	Keine Bemerkungen
Beratung über Penetration Test	Ja	Für jemanden, der sich nicht mit Penetration Tests auskennt etwas kompliziert.
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	4
Stellt offene Fragen	4
Übernimmt die Terminologie des Gesprächspartners bei Nomen	4
Die Antworten sind nicht unnötig lange	4
Die Antworten sind hilfreich	3
Die Antworten und Informationen sind einfach verständlich	5
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Argjent Kaba, 29, CEO IDosh	02.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Link mit Webseite zu über uns, oder Webseite direkt öffnen
Events anzeigen lassen	Ja	Link mit Webseite zu über uns, oder Webseite direkt öffnen
Penetration Test bestellen	Ja	Keine Bemerkungen
Beratung über Penetration Test	Ja	Wiederholende Frage, wenn man über den Penetration Test Pfad in die Beratung geht
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	5
Stellt offene Fragen	3
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5
Die Antworten sind nicht unnötig lange	1
Die Antworten sind hilfreich	4
Die Antworten und Informationen sind einfach verständlich	4
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Erol Sabotic, 24, Sachbearbeiter / Student	02.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Training phrases wurden hinzugefügt.
Events anzeigen lassen	Ja	Keine Bemerkungen
Penetration Test bestellen	Ja	Die Firma der Testperson wurde nicht erkannt.
Beratung über Penetration Test	Ja	Keine Bemerkungen
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	5
Stellt offene Fragen	4
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5
Die Antworten sind nicht unnötig lange	3
Die Antworten sind hilfreich	4
Die Antworten und Informationen sind einfach verständlich	4
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Roger Ringger, 58, CEO Twincap	10.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Weitere Training phrases wurden hinzugefügt.
Events anzeigen lassen	Ja	Keine Bemerkungen
Penetration Test bestellen	Ja	Firma der Testperson wurde nicht erkannt.
Beratung über Penetration Test	Ja	Keine Bemerkungen
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	5
Stellt offene Fragen	4
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5
Die Antworten sind nicht unnötig lange	3
Die Antworten sind hilfreich	4
Die Antworten und Informationen sind einfach verständlich	4
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Jadis Redja, 21, Marketing Social Media	05.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Weitere Antwortmöglichkeiten wurden in den Training phrases hinzugefügt.
Events anzeigen lassen	Ja	Keine Bemerkungen
Penetration Test bestellen	Ja	Keine Bemerkungen
Beratung über Penetration Test	Ja	Keine Bemerkungen
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	5
Stellt offene Fragen	4
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5
Die Antworten sind nicht unnötig lange	4
Die Antworten sind hilfreich	4
Die Antworten und Informationen sind einfach verständlich	5
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Kenan Halilovic, 24, Wirtschaftsstudent	09.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Keine Bemerkungen
Events anzeigen lassen	Ja	Keine Bemerkungen
Penetration Test bestellen	Ja	Keine Bemerkungen
Beratung über Penetration Test	Ja	Keine Bemerkungen
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	4
Stellt offene Fragen	3
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5
Die Antworten sind nicht unnötig lange	4
Die Antworten sind hilfreich	5
Die Antworten und Informationen sind einfach verständlich	5
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Armend Lesi, 23, Informatik Student	10.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Etwas zu viel Text als Antwort.
Events anzeigen lassen	Ja	Keine Bemerkungen
Penetration Test bestellen	Ja	Weitere mögliche Antworten wurden in den Entities vermerkt.
Beratung über Penetration Test	Ja	Keine Bemerkungen
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	4
Stellt offene Fragen	4
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5
Die Antworten sind nicht unnötig lange	3
Die Antworten sind hilfreich	5
Die Antworten und Informationen sind einfach verständlich	5
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Bruno Gomes, 26, Informatiker	11.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Keine Bemerkungen
Events anzeigen lassen	Ja	Weiterführung der Konversation nicht möglich.
Penetration Test bestellen	Ja	Keine Bemerkungen
Beratung über Penetration Test	Ja	Keine Bemerkungen
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Ja	Keine Bemerkungen



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	4
Stellt offene Fragen	4
Übernimmt die Terminologie des Gesprächspartners bei Nomen	5
Die Antworten sind nicht unnötig lange	3
Die Antworten sind hilfreich	5
Die Antworten und Informationen sind einfach verständlich	5
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



VORGEHEN

Die Testperson wird begrüsst und der Testfall beschrieben. Die Testperson darf fragen zum Ziel stellen bevor der Test beginnt.

Anschliessend versucht die Testperson auf ihre Art ohne Einflussnahme das geschilderte Ziel zu erreichen. Der Prüfer beobachtet die Testperson und notiert sich die Äusserungen und das Verhalten.

Wenn die Testperson das Ziel erreicht oder aufgegeben hat, wird unter der Leitung des Prüfers das Bewertungsraster selbständig ausgefüllt.

ORGANISATION

TESTPERSON (NAME, ALTER, BERUF)	DATUM DER DURCHFÜHRUNG	PRÜFER
Ivan Bütler, 48, CEO Compass Security	12.12.2018	dhodzic

TESTERGEBNISSE

TESTCASES

Die Testperson orientiert sich bei den Szenarien an den Vorgaben und Erklärungen im Usability Dokument.

TESTCASE SZENARIEN	ZIEL ERREICHT?	BEMERKUNGEN
Compass Security kennenlernen	Ja	Beschreibung stimmt nicht ganz mit der Zielsetzung überein. => TODO korrigieren.
Events anzeigen lassen	Ja	Ihn stört es, dass im letzten Absatz (letzte Text Response) vorgeschrieben wird, was es zu tun gibt (mögliche Optionen werden angezeigt). => TODO Response anpassen: Entschärfen der Formulierung oder komplett weglassen. Ivan versucht mit "zurück" zurück zu springen im Gespräch. => TODO: Konzeptionelle Lösung im techn. Bericht beschreiben.
Penetration Test bestellen	Nein	Ivan wählt den "pen test", anschliessend die Beratung per Chat. Danach wird wieder die Frage gestellt über welche Dienstleistung beraten werden soll. => Ablauf prüfen.
Beratung über Penetration Test	Nein	Firma wurde nicht erkannt. Viele weitere Antwortmöglichkeiten wurden in den Training phrases hinzugefügt.
Chat jederzeit verlassen und Kontakt mit einem Menschen herstellen	Nein	Wurde nicht ausgeführt.



BEWERTUNGSRASTER CHARAKTER

Das Bewertungsraster dient zur Qualifikation des Verhaltens.

Die Bewertung reicht von 1, unbefriedigend oder «trifft gar nicht zu» bis zu 5, hervorragend oder «trifft voll und ganz zu».

CHARAKTER / VERHALTEN	DURCHSCHNITTLICHE BEURTEILUNG VON 1 BIS 5 («GAR NICHT» BIS «VOLL UND GANZ»)
Zeigt Freude am Kontakt	3
Stellt offene Fragen	4
Übernimmt die Terminologie des Gesprächspartners bei Nomen	1
Die Antworten sind nicht unnötig lange	3
Die Antworten sind hilfreich	3
Die Antworten und Informationen sind einfach verständlich	5
Geht nicht auf negative Äusserungen ein	5
Verwendet keine Kraftausdrücke und Fluchwörter	5



G. PERSÖNLICHER BERICHT

GIULIANO DE GANI

Der persönliche Bericht bezüglich der Bachelorarbeit «Chatbot» wird in die Teilbereiche Administration und Koordination, Engineering, Lessons Learned und Danksagung gegliedert. Im Folgenden wird die eigene Erfahrung und persönliche Eindruck wiedergegeben.

ADMINISTRATION UND KOORDINATION

Mit den gegebenen Rahmenbedingungen, zwei Teilzeitstudierende mit unterschiedlichen Pensi und Arbeitszeiten für die Bachelorarbeit reserviert, war es besonders wichtig, dass ein bestimmter Kommunikationsrythmus eingehalten wurde und die Arbeiten so aufgeteilt wurden, dass keine Wartezeiten auf abhängige Aufgaben entstanden.

Die Koordination der Aufgaben und das regelmässige Treffen, mindestens einmal pro Woche, meist Donnerstags, sind uns gut gelungen. Die Arbeiten wurden zweckmässig verteilt. Denis, als Systemengineer, befasste sich mehrheitlich mit der Dialogflow Console, während ich die Softwareentwicklung im .NET Backend und grosse Teile der Softwareanforderungsdokumente und Softwaredesigndokument erstellt habe.

Trotz Einführung der Microsoft DevOps Plattform als Projektmanagement Tool und CI / CD Umgebung, wurde kein richtiges Scrum oder Kanban als agile Methode gelebt. Grund dafür sehe ich hauptsächlich darin, dass der Management Overhead den Vorteilen überwiegte. Die Tasks wurden also nicht für die Aufwandschätzung und Kapazitätsplanung eingesetzt, wohl aber als Issueboard oder als «Offene Punkte Liste».

Die Organisation und Kommunikation im Team ist reibungslos verlaufen.

ENGINEERING

In diesem Abschnitt möchte ich über das Handwerk als Softwareentwickler im engeren und als Entwickler eines Produktes oder Prototyps im weiteren Sinn einige Beobachtungen und Eindrücke schildern.

VORGEHEN

In diesem Projekt ging es darum, in kürzester Zeit sich in die Thematik einzuarbeiten, die theoretischen Grundlagen zu erfassen, Kurzevaluation bestehender Technologien durchzuführen und schliesslich ein Produkt zu entwickeln.

Unter diesen Voraussetzungen wurde für die Evaluation der Technologien wenig Zeit aufgewendet. Wir sind bewusst das Risiko eingegangen, dass im Verlaufe des Projekts sich die Technologie als ungeeignet für unsere Anforderungen erweisen könnte.

PRODUKT

Im Verlaufe des Projekts wurden einige Entscheide getroffen, die sich im Nachhinein als negativ für das Produkt ausgewirkt haben. Obwohl die Entscheide begründet und nachvollziehbar sind, hätten wir mit etwas mehr Mut, Risikobereitschaft und Aufwand einige Anpassungen machen können. Ich denke dabei vor allem an drei Punkte:

- **Software Architekturentscheidung:** Variante 2 hätte zwar deutlich mehr Entwicklungsaufwand mitgebracht, jedoch die Grundlage gelegt, um sämtliche Use Cases und Anforderung zu lösen.
- **Chat Userinterface:** Das UI spielt eine zentrale Rolle, wenn es um die Wahrnehmung des Produkts geht. Hier hätten wir noch stärker Wert darauf legen sollen, auf welcher Plattform wir das User Interface integrieren. Das Demo Web UI von Dialogflow hat mit seinen Limitationen negativ zum Produkt beigetragen und wirft ein schlechtes Licht auf die Arbeit.



- **Ambitionierte Zielsetzungen:** Die hochgesteckten Anforderungen an den Chatbot haben dazu geführt, dass wir sehr lange versucht haben, das Bestmögliche mit den bestehenden Mitteln zu erreichen. Wir haben meiner Meinung nach versucht, mit einem Hammer eine Schraube einzudrehen. Auch hier hätten wir mit etwas mehr Mut und Initiative früher den Kurs korrigieren können.

LESSONS LEARNED

- **Deployment Aufgaben:** Hier muss genügend Reservezeit eingeplant werden
- **Tooling:** Die Werkzeuge müssen früh eingerichtet und einheitlich im Team verfügbar sein. Stichwort git/ vs for Mac mit unvorhergesehenen Problemen. Die Werkzeuge müssen beherrscht sein (Stichwort git workflow)
- **Risikomanagement:** Fokus noch stärker auf technische Schwierigkeiten richten. Mehr Wert auf das «Denken in Varianten» legen, um schneller reagieren zu können.
- **Die Expertenmeinung einholen und berücksichtigen:** Der Experte hat ein unmissverständliches und deutliches Statement abgegeben, was die Zielsetzungen dieses Projekts betreffen. Dies hat zur Anpassung der Anforderungen geführt. In Zukunft möchte ich darauf achten, dass der Experte so früh wie möglich mit einbezogen wird, weil spätere «Kurskorrekturen» im Projekt um ein Vielfaches teurer werden.
- **Mut:** Mutiger sein, wenn risikoreiche Entscheidungen getroffen werden müssen.

DANKSAGUNG

Ein Dank geht an meinen Kameraden Denis. Mit seinem Fleiss und Korpsgeist hat er entscheidend zum Erfolg des Projekts beigetragen. Er hat stets gelassen auf Kritik reagiert und nie den Kopf in den Sand gesteckt.

Bei unserem Betreuer, Ivan Bütler, möchte ich mich bedanken. Ich habe seine engagierte, kritische und direkte Art sehr geschätzt. Er hat aktiv in Problemlösungsdiskussionen mitgewirkt und uns die Ressourcen der Compass Security AG zur Verfügung gestellt. Mein Dank geht auch an Cyrill Bannwart. Er hat mir über Wochen stets bei der Lösungsfindung verschiedenster Deploymentprobleme tatkräftig zur Seite gestanden. Danke auch an Christian Spielmann, der uns geholfen hat, die Arbeit zu drucken.



H. PERSÖNLICHER DENIS HODZIC

BERICHT

EINFÜHRUNG

Schon vor Beginn der Bachelorarbeit war ich, als zukünftiger System Engineer sehr erfreut, dass wir ein Thema mit Sicherheitsbezogenen Dienstleistungen bei der Compass Security bearbeiten konnten.

Die Aufgabe einen Chatbot zu entwickeln, selbst die Technologie auszuwählen und vor allem das Themengebiet selbst zu bestimmen war eine sehr spannende und intensive Erfahrung. Dass wir an etwas Handfestem arbeiten, welches eines Tages an der Compass Security eingesetzt werden kann war Motivation genug. Ich konnte nicht nur meine Erfahrungen in Projekten erweitern, sondern dank unserem Betreuer auch Einblick in die Kundenbetreuung und Verkaufsgesprächen erhalten.

ADMINISTRATION UND KOORDINATION

Rückblickend war die Zusammenarbeit im Team sowie die Realisierung des Projektes sehr gut. Giuliano und ich hatten weder Kommunikationsprobleme noch zwischenmenschliche Differenzen.

Die Administration wurde sehr vereinfacht, da Giuliano für uns die Projektverwaltung auf Microsoft DevOps Plattform eingerichtet hat.

In dieser Arbeit habe ich hauptsächlich die Implementierung der Intents auf der Dialogflow Konsole und das Modellieren der Konversation übernommen. Giuliano befasste sich als erfahrener .Net Entwickler mit dem .Net Backend.

ENGINEERING

In dieser Bachelorarbeit ging es darum, in kürzester Zeit sich in die Thematik einzuarbeiten, die theoretischen Grundlagen zu erfassen, Kurzevaluation bestehender Technologien durchzuführen und schliesslich ein Produkt zu entwickeln.

Unter diesen Voraussetzungen wurde für die Evaluation der Technologien wenig Zeit aufgewendet. Wir sind bewusst das Risiko eingegangen, dass im Verlaufe des Projekts sich die Technologie als ungeeignet für unsere Anforderungen erweisen könnte.

Ich hätte gerne mehr Zeit zur Verfügung gehabt, um weitere Dienstleistungen zu implementieren und das Beratungsgespräch zu vertiefen, bin aber mit unserem Endergebnis sehr zufrieden. Ich konnte die Technologie ausreizen und mich mit dem «neuen» Thema Machine Learning auseinandersetzen.

Leider haben wir uns dazu entschieden, kein eigenes User Interface zu entwickeln, den das Integrierte User Interface Web Demo von Dialogflow war sehr limitiert. Deswegen konnten wir einige Funktionen wie z.B. Auswahlboxen nicht implementieren.

LESSONS LEARNED

- Die Ambitionen nicht so hochstecken, wenn man die Technologie nicht kennt.
- Risikomanagement: Grenzen der Technologie stärker berücksichtigen.
- Expertenmeinung früher einholen.
- Mutiger sein, wenn risikoreiche Entscheidungen getroffen werden müssen.



DANKSAGUNG

An erster Stelle möchte ich mich bei meinem Kameraden Giuliano bedanken, welcher mit seiner Erfahrung und seinem unermüdlichen Einsatz entscheidend zum Erfolg des Projektes beigetragen hat.

Auch möchte ich mich bei unserem Betreuer, Ivan Bütler für sein Engagement, seine Motivation und Hilfsbereitschaft bedanken.

Auch meinen Freunden, Arbeitskameraden und Vorgesetzten für die aufgewendete Zeit beim Testen und Bewerten von unserem Chatbot herzlich bedanken.



I.CHARLI API DOCUMENTATION

/swagger/v1/swagger.json

```
{ "swagger": "2.0", "info": { "version": "v1", "title": "Charli Web API" }, "paths": { "/api/Events": { "get": { "tags": [ "Events" ], "operationId": "ApiEventsGet", "consumes": [], "produces": [ "text/plain", "application/json", "text/json" ], "parameters": [], "responses": { "401": { "description": "Unauthorized", "schema": { "$ref": "#/definitions/UnauthorizedResult" } }, "200": { "description": "Success", "schema": { "uniqueItems": false, "type": "array", "items": { "$ref": "#/definitions/EventDTO" } } } } }, "post": { "tags": [ "Events" ], "operationId": "ApiEventsPost", "consumes": [ "application/json-patch+json", "application/json", "text/json", "application/*+json" ], "produces": [ "text/plain", "application/json", "text/json" ], "parameters": [ { "name": "evt", "in": "body", "required": false, "schema": { "$ref": "#/definitions/CreateEventDTO" } } ], "responses": { "401": { "description": "Unauthorized", "schema": { "$ref": "#/definitions/UnauthorizedResult" } }, "201": { "description": "Success", "schema": { "$ref": "#/definitions/EventDTO" } }, "400": { "description": "BadRequest", "schema": { "$ref": "#/definitions/BadRequestResult" } } } }, "/api/Events/id": { "delete": { "tags": [ "Events" ], "operationId": "ApiEventsIdDelete", "consumes": [], "produces": [ "text/plain", "application/json", "text/json" ], "parameters": [ { "name": "id", "in": "query", "required": false, "type": "integer", "format": "int32" }, { "name": "id", "in": "path", "required": true, "type": "string" } ], "responses": { "401": { "description": "Unauthorized", "schema": { "$ref": "#/definitions/UnauthorizedResult" } }, "200": { "description": "Success", "schema": { "$ref": "#/definitions/OkResult" } }, "404": { "description": "NotFound", "schema": { "$ref": "#/definitions/NotFoundResult" } } } } }, "/api/Intents": { "get": { "tags": [ "Intents" ], "operationId": "ApiIntentsGet", "consumes": [], "produces": [ "text/plain", "application/json", "text/json" ], "parameters": [], "responses": { "401": { "description": "Unauthorized", "schema": { "$ref": "#/definitions/UnauthorizedResult" } } } } }, "/api/Intents/{id}": { "get": { "tags": [ "Intents" ], "operationId": "ApiIntentsByIdGet", "consumes": [], "produces": [ "text/plain", "application/json", "text/json" ], "parameters": [ { "name": "id", "in": "path", "required": true, "type": "string" } ], "responses": { "401": { "description": "Unauthorized", "schema": { "$ref": "#/definitions/UnauthorizedResult" } } } } }, "definitions": { "UnauthorizedResult": { "type": "object", "properties": { "statusCode": { "format": "int32", "type": "integer", "readOnly": true } }, "EventDTO": { "type": "object", "properties": { "id": { "format": "int32", "type": "integer" }, "date": { "format": "datetime", "type": "string" }, "title": { "type": "string" }, "location": { "type": "string" }, "description": { "type": "string" } } }, "CreateEventDTO": { "type": "object", "properties": { "date": { "format": "datetime", "type": "string" }, "title": { "type": "string" }, "location": { "type": "string" }, "description": { "type": "string" } } }, "BadRequestResult": { "type": "object", "properties": { "statusCode": { "format": "int32", "type": "integer", "readOnly": true } } }, "OkResult": { "type": "object", "properties": { "statusCode": { "format": "int32", "type": "integer", "readOnly": true } } }, "NotFoundResult": { "type": "object", "properties": { "statusCode": { "format": "int32", "type": "integer", "readOnly": true } } } } }
```



J. RISIKOMANAGEMENT



RISIKOMANAGEMENT

Projekt: Chatbot Charli
 Erstellt am: 27.09.2018
 Autor: gdegani
 Total Gewichteter Schaden: 75.28

LEGENDE

S = MAX. SCHADEN [h]
 EW = Eintrittswahrscheinlichkeit
 GS = Gewichteter Schaden

Änderungsgeschichte		
Datum	Autor	Beschreibung
04.10.2018	gdegani	technische Risiken R8, R9 hinzugefügt, "Krankheit" Risiko entfernt. Projektname aktualisiert
16.10.2018	gdegani	R1,R2,R3,R5 EW angepasst, R10 hinzugefügt
18.10.2018	gdegani	R11 hinzugefügt
22.10.2018	gdegani	R9 EW erhöht von 20% auf 25%, R4 EW reduziert von 20% auf 10%, R5 EW reduziert auf 10%
21.11.2018	gdegani	R12 hinzugefügt

NR	TITEL	BESCHREIBUNG	S	EW	GS	VORBEUGUNG	VERHALTEN BEI EINTRETEN
R1	Komplexität	Unerwartet hohe Komplexität und Unerfahrenheit im Umgang mit der Technologie, welche aus der Aufgabenstellung resultiert	64	40%	25.6	wöchentliche Meetings durchführen um Komplexitäten zu erkennen und Lösungsansätze abzusprechen.	Umfang der Funktionen verringern.
R2	Anforderungs-spezifikation	Wachsende oder neu hinzukommende Anforderungen	20	25%	5	Anforderungen in der Elaborationsphase verabschieden. Projekt agil führen, um besser damit umgehen zu können.	Anforderungen und die resultierenden Arbeitspakete werden bei der Sprintplanung neu priorisiert und eingeplant.
R3	Projekt-management	Koordinationsprobleme bei der Aufgabenaufteilung	20	25%	5	DevOps WorkItems verwenden und pflegen. Wöchentliche Teamsynchronisation durchführen.	Synchronisation durchführen. Workitems bereinigen und das Arbeiten damit forcieren und kontrollieren.



R4	3rd party services	Mögliche Drittanbieter wie LUIS oder Azure services sind möglicherweise schwierig zu integrieren oder bieten keine Testperiode an / Testperiode geht zu Ende oder bremst aus	32	10%	3.2	Frühzeitiger Architekturprototyp aufsetzen mit dem kritischen Pfad abgedeckt. Frühzeitige Evaluation der relevanten services durchführen	Support HSR oder Betreuer kontaktieren, falls Kredite für die Verwendung der services benötigt werden. Auf kostenlose Alternativen umschalten
R5	Konflikte der Entwicklerumgebungen (Win vs Mac)	Unterschiedliche Visual Studio 2017 Versionen für Win und Mac können zu Problemen führen (UNIX CRLF, git VCS, ...)	16	10%	1.6	So früh wie möglich Teamübergreifend die Tools evaluieren und sich auf gemeinsame Tools festlegen.	Zeitreserven nutzen.
R6	Projekt-managemantool	Unklarheiten bzgl des Umgangs mit DevOps (ehemals Teamservices) von Microsoft als Projektmanagement Tool	16	25%	4	Sich auf die bestehenden Prozesse und Funktionalitäten beschränken.	Schulung in Form eines Online Tutorials durchführen.
R7	Datenverlust	Erzeugnisse gehen datentechnisch verloren	64	2%	1.28	sämtliche Dokumentation dezentral mit git verwalten. Remote git Repository regelmässig aktualisieren. Git workflow umsetzen.	dezentrale Kopie zur Wiederherstellung nutzen. Notfallmeeting einberufen und Planung überarbeiten.
R8	Intent Erkennung ist ungenügend	Die Absichtserkennung aus der natürlichen Sprache heraus ist nicht gut genug, um das Ziel einer natürlichen Gesprächsführung erreichen zu können	96	10%	9.6	In Varianten denken, d.h. mehrere Bot Frameworks und NLU Services evaluieren und das Beste nehmen	Die Gesprächsführung starrer machen, mit Formularen arbeiten, die Trainings der NL Modelle verbessern, indem mehr Text Phrasen eintrainiert werden.
R9	Gesprächsführung Modellierung nicht flexibel genug	Die Modellierung des "Flow" / Gesprächsablaufs ist umständlich und schwer zugänglich.	80	25%	20	Früh mit der Modellierung beginnen (auch wenn es nicht final ist), um Hindernisse und Einschränkungen früh zu erkennen. Den Gesprächsablauf einfach halten.	Den Gesprächsablauf vereinfachen. Im Notfall auf ein anderes (zuvor evaluiertes) Bot Framework umsteigen.
R10	Buildzeit Verfügbarkeit	Die CI Umgebung wird bei jedem Commit getriggert. Gefahr besteht, dass die Build Agents nicht verfügbar sind, da die Free Version nur bestimmte Buildzeit beinhaltet.	24	10%	2.4	Repositories Docu und Code aufspalten.	Local Build Agent einrichten, was etwas Aufwand bedeutet
R11	Zeitliches Verhalten von Dialogflow	Zu hohe Latenzen für die Beantwortung machen das Produkt unbrauchbar	80	10%	8	Früh eine Modellierung in die "Breite" anstreben um Limitationen frühzeitig aufzudecken (max. 5 Input Contexts)	Dialogflow Supportanfrage für Vorzugsbehandlung während der BA Phase. Modellierung vereinfachen



R12	Deployment Probleme	Probleme der Konfiguration und Berechtigungen beim Deployment	32	50%	16	Hilfe anfordern	Supportanfragen machen, Betreuer einbeziehen
	SUMME		544		101.7		