Hochschule Wismar
University of Applied Sciences
Technology, Business and Design
Fakultät für Ingenieurwissenschaften, Fachbereich Informatik

Master-Thesis

# Analyse von IT-Sicherheitsaspekten in Spracherkennungssystemen

Abschlussarbeit zur Erlangung des Grades eines

**Master of Engineering (M.Eng.)**

der Hochschule Wismar

eingereicht von: Robin Siebers
geboren am 09. Februar 1981 in Stuttgart
Studiengang IT-Sicherheit und Forensik

Matrikelnummer: 240688

Erstgutachter: Prof. Dr.-Ing. Antje Raab-Düsterhöft
Zweitgutachter: Prof. Dr.-Ing. Andreas Ahrens

Bearbeitungszeitraum: 06. März 2019 bis 27. August 2019

Stuttgart, den 27. August 2019

# Aufgabenstellung

Im Rahmen der Master-Thesis ist zunächst ein Überblick über die Grundbegriffe und Begriffserklärung der künstlichen Intelligenz sowie die Geschichte der einzelnen Sprachassistenten Amazon Alexa, Google Home und Apple Siri zu geben. Des Weiteren sind die technischen Details, d.h. die Architektur und Funktionsweise der einzelnen Sprachassistenten, zu erläutern und zu beschreiben. Ein Vergleich der Systeme bezüglich Sicherheit und Forensik wird in den Mittelpunkt der Master-Thesis gestellt. Darüber hinaus wird der Datenschutz der einzelnen Sprachassistenten analysiert. Die Sprachassistenten sind hinsichtlich ihrer Einsatzmöglichkeiten sowie ihrer Stärken und Schwächen zu beurteilen.

## Abstract

As part of the Master's thesis, first of all an overview of the basic concepts and definitions of artificial intelligence as well as the history of the individual voice assistants Amazon Alexa, Google Home and Apple Siri is to be given. Furthermore, the technical details, i.e. the architecture and functionality of the individual voice assistants, are to be explained and described. A comparison of the systems regarding security and forensics are the focus of the Master's thesis. In addition, the data protection of the individual voice assistants is analyzed. The voice assistants are to be assessed with regard to their possible applications as well as their strengths and weaknesses.

# Inhaltsverzeichnis

**Aufgabenstellung** ..... **II**
**Inhaltsverzeichnis** ..... **III**
**Bilderverzeichnis** ..... **VIII**
**Tabellenverzeichnis** ..... **IX**
**1 Einleitung** ..... **1**
**1.1 Motivation und Zielsetzung** ..... **1**
**1.2 Vorgehen** ..... **2**
**1.3 Abgrenzung** ..... **2**
**1.4 Stand der Forschung** ..... **2**
**2 Grundlagen** ..... **4**
**2.1 Künstliche Intelligenz** ..... **4**
2.1.1 Maschinelles Lernen ..... 5
2.1.2 Deep Learning ..... 7
**2.2 Geschichte der einzelnen Sprachassistenten** ..... **8**
2.2.1 Amazon ..... 8
2.2.2 Amazon Alexa ..... 9
2.2.3 Google ..... 10
2.2.4 Google Home ..... 11
2.2.5 Apple ..... 12
2.2.6 Apple Siri ..... 13
**3 Technik und Funktion der einzelnen Sprachassistenten** ..... **15**
**3.1 Technik der einzelnen Spracherkennungssysteme** ..... **15**
3.1.1 Technische Daten von Amazon Echo (1. Generation) ..... 15
3.1.2 Technische Daten von Google Home ..... 17
3.1.3 Technische Daten von iPhone 6s Plus ..... 19
**3.2 Architektur und Funktion der Spracherkennungssysteme** ..... **20**
3.2.1 Architektur und Funktion von Amazon Echo ..... 20
3.2.2 Architektur und Funktion von Google Home ..... 23
3.2.3 Architektur und Funktion von Apple Siri ..... 26
**3.3 Zusammenfassung** ..... **28**

**4 Sicherheitsrisiken der Spracherkennungssysteme ... 29**
**4.1 IT-Sicherheit und Schutzziele ... 29**
**4.2 Schwachstellen, Bedrohungen, Angriffe, Risiko ... 31**
**4.3 Sicherheitsproblem Stimmenerkennung ... 33**
4.3.1 Amazon Echo (1. Generation) mit Alexa ... 33
4.3.2 Google Home mit Google Assistant ... 35
4.3.3 iPhone 6s Plus mit Siri ... 36
4.3.4 Angriff im nicht hörbaren Bereich („DolphinAttack“) ... 37
4.3.5 Ähnlich klingende Begriffe ... 38
4.3.6 Sicherheitsempfehlungen ... 39
4.3.7 Zusammenfassung und Fazit ... 39
**4.4 Sicherheitsproblem WLAN (Wireless Local Area Network) ... 40**
4.4.1 WLAN Angriffsmöglichkeiten ... 41
4.4.2 WLAN-Standards nach IEEE ... 42
4.4.3 Sicherheitsproblem Fehlkonfiguration ... 43
4.4.4 Sicherheitsproblem WPA / WPA2 ... 45
4.4.5 Sicherheitsproblem Abhören ... 47
4.4.6 Sicherheitsproblem Man-in-the-Middle-Angriff ... 48
4.4.7 Sicherheitsproblem Denial-of-Service (DOS) ... 49
4.4.8 Sicherheitsempfehlungen ... 49
4.4.9 Zusammenfassung und Fazit ... 50
**4.5 Sicherheitsproblem Bluetooth ... 50**
4.5.1 Sicherheitsmodi bei Bluetooth ... 52
4.5.2 Sicherheitsproblem Bluetooth Stack (BlueBorne) ... 53
4.5.3 Sicherheitsproblem Man-in-the-Middle ... 53
4.5.4 Sicherheitsproblem Denial-of-Service (DOS) (BlueSmacking) ... 53
4.5.5 Sicherheitsempfehlungen ... 54
4.5.6 Zusammenfassung und Fazit ... 54
**4.6 Sicherheitsproblem Application-Programming-Interface (API) ... 55**
4.6.1 Sicherheitsproblem API bei Amazon Echo ... 55
4.6.2 Sicherheitsproblem API bei Google Home ... 57
4.6.3 Sicherheitsproblem API bei Apple Siri ... 61
4.6.4 Sicherheitsempfehlungen ... 63
4.6.5 Zusammenfassung und Fazit ... 63
**4.7 Sicherheitsproblem Künstliche Intelligenz ... 64**

**5 Datenschutz bei den Spracherkennungssystemen ... 65**
**5.1 EU-Datenschutzgrundverordnung (EU-DS-GVO) ... 65**
**5.2 Analyse der Sprachaufzeichnungen ... 66**
5.2.1 Sprachaufzeichnung Amazon Echo ... 66
5.2.2 Ergebnis ... 69
5.2.3 Sprachaufzeichnung Google Home ... 70
5.2.4 Ergebnis ... 74
5.2.5 Sprachaufzeichnung Apple Siri ... 74
5.2.6 Ergebnis ... 77
**5.3 Analyse der Kommunikation mithilfe von Wireshark ... 77**
**5.4 Wireshark ... 77**
**5.5 Allgemeiner Versuchsaufbau ... 78**
**5.6 Amazon Alexa ... 79**
5.6.1 Datenverkehr ohne Aktivierungswort ... 79
5.6.2 Ergebnis ... 82
5.6.3 Datenverkehr mit Aktivierungswort ... 82
5.6.4 Ergebnis ... 85
**5.7 Google Home ... 86**
5.7.1 Datenverkehr ohne Aktivierungswort ... 86
5.7.2 Ergebnis ... 88
5.7.3 Datenverkehr mit Aktivierungswort ... 89
5.7.4 Ergebnis ... 90
**5.8 Apple Siri ... 90**
5.8.1 Datenverkehr ohne Aktivierungswort ... 90
5.8.2 Ergebnis ... 92
5.8.3 Datenverkehr mit Aktivierungswort ... 93
5.8.4 Ergebnis ... 95
**6 Bewertung der Spracherkennungssysteme ... 96**
**6.1 Einsatzmöglichkeiten der Spracherkennungssysteme ... 96**
6.1.1 Amazon Alexa ... 96
6.1.2 Google Home ... 99
6.1.3 Apple Siri ... 103
**6.2 Bewertung ausgewählter Spracherkennungssysteme ... 106**
6.2.1 Amazon Alexa ... 106
6.2.2 Google Home ... 107
6.2.3 Apple Siri ... 108

**7 Zusammenfassung und Ausblick** ..... **110**
**Abkürzungsverzeichnis** ..... **113**
**Literaturverzeichnis** ..... **117**
**Online-Quellen** ..... **118**
**Anhang** ..... **125**
**A.1 Technische Details von Amazon Echo (1 Generation)** ..... **125**
**A.2 Technische Details von Google Home** ..... **127**
**A.3 Technische Details vom iPhone 6s Plus mit Apple Siri** ..... **128**
**Erklärung** ..... **129**
**Thesen** ..... **130**

# Bilderverzeichnis

Bild 1: Wichtige Begriffe und Definitionen im Umfeld von KI ..... 5
Bild 2: Aufbau eines Maschinelles Lernen Algorithmus ..... 5
Bild 3: Neuronales Netz ..... 7
Bild 4: Amazons Echo Produktlinie ..... 10
Bild 5: Google Home Produktlinie ..... 12
Bild 6: Apple Siri Produktlinie ..... 14
Bild 7: Aufbau von Amazon Echo (1. Generation) ..... 15
Bild 8: Draufsicht von Amazon Echo (1. Generation) ..... 16
Bild 9: Google Home Aufbau ..... 17
Bild 10: Ansicht von Google Home ..... 18
Bild 11: iPhone 6s Plus Technik Details ..... 19
Bild 12: Architektur von Amazon Echo (1.Generation) ..... 21
Bild 13: Architektur von Google Home ..... 24
Bild 14: Aktivierung von Siri & Konfiguration ..... 26
Bild 17: Zusammenhang zwischen Schwachstellen, Bedrohungen und Risiken ..... 31
Bild 18: Hörflächen-Schaubild ..... 37
Bild 19: IT-Schutzziele WLAN ..... 40
Bild 20: Man-in-the-Middle-Angriff ..... 48
Bild 21: Alexa Developer Console ..... 56
Bild 22: Google Actions Console ..... 58
Bild 23: MAC-Adresse ..... 59
Bild 24: Google Home SSID ..... 60
Bild 25: Google Home Local API GET/POST Befehle ..... 60
Bild 26: Kurzbefehle-APP Galerie ..... 61
Bild 28: Alexa Sprachaufnahmen-Verlauf überprüfen im Browser ..... 67
Bild 29: Sprachaufnahmen-Verlauf überprüfen Alexa-APP ..... 68
Bild 30: Google Assistant Sprach-& Audioaktivitäten Browser ..... 72
Bild 31: Google Home App Google Assistant-Aktivitäten ..... 73
Bild 32: Apple Daten und Datenschutz ..... 76
Bild 33: Versuchsaufbau Analyse der Kommunikation der Sprachassistenten ..... 79
Bild 34: Amazon Alexa Datenverkehr ohne Aktivierung ..... 80
Bild 35: Amazon Alexa I/O Graphen bei nicht Aktivierung ..... 80
Bild 36: Amazon Alexa Mitschnittdatei ohne Aktivierung ..... 81
Bild 37: Amazon Alexa Verbindungen ohne Aktivierung ..... 81
Bild 38: Amazon Alexa Verbindung ohne Aktivierung ..... 82
Bild 39: Amazon Alexa I/O Graphen mit Aktivierung ..... 83
Bild 40: Amazon Alexa Mitschnittdatei mit Aktivierung ..... 83
Bild 41: Amazon Alexa Verbindungen mit Aktivierung ..... 84
Bild 42: Amazon Alexa Verbindung mit Aktivierung ..... 84
Bild 43: Amazon Alexa Verbindung mit Aktivierung ..... 85
Bild 44: Google Home I/O Graphen ohne Aktivierung ..... 86
Bild 45: Google Home Mitschnittdatei ohne Aktivierung ..... 87
Bild 46: Google Home Verbindungen ohne Aktivierung ..... 87
Bild 47: Google Home Verbindung ohne Aktivierung ..... 88
Bild 48: Google Home I/O Graphen mit Aktivierung ..... 89
Bild 49: Google Home Mitschnittdatei mit Aktivierung ..... 89
Bild 50: Google Home Verbindungen mit Aktivierung ..... 90
Bild 51: Apple Siri I/O Graphen ohne Aktivierung ..... 91

Bild 52: Apple Siri Mitschnittdatei ohne Aktivierung ..... 91
Bild 53: Apple Siri Verbindungen ohne Aktivierung ..... 92
Bild 54: Apple Siri I/O Graphen mit Aktivierung ..... 93
Bild 55: Apple Siri Mitschnittdatei mit Aktivierung ..... 94
Bild 56: Apple Siri Verbindungen mit Aktivierung ..... 94

# Tabellenverzeichnis

Tabelle 1: Apple Produktübersicht (Eigene Darstellung) ..... 13
Tabelle 2: Status Lichtring von Amazon Echo (1. Generation) ..... 22
Tabelle 3: Leuchtanzeige von Google Home ..... 24
Tabelle 4: WLAN-Standards IEEE ..... 42
Tabelle 5: Amazon Echo (1. Generation) Alexa Stärken und Schwächen ..... 106
Tabelle 6: Google Home Stärken und Schwächen ..... 107
Tabelle 7: Apple Siri Stärken und Schwächen ..... 108
Tabelle 8: Technische Details von Amazon Echo (1. Generation) ..... 125
Tabelle 9: Technische Details von Google Home ..... 127
Tabelle 10: Technische Details vom iPhone 6s Plus mit Apple Siri ..... 128

# 1 Einleitung

## 1.1 Motivation und Zielsetzung

Spracherkennungssysteme wie zum Beispiel: Amazon Alexa, Google Home sowie Apple Siri sind heutzutage allgegenwärtig. Jeder benutzt sie fast täglich, bewusst oder unbewusst, diese intelligenten Assistenten, die immer benutzerfreundlicher und durch ihre einfache Handhabung den Alltag erheblich erleichtern können. Daher sind gegenwärtig in fast jedem Haushalt, egal ob im Wohnzimmer, Schlafzimmer, Küche oder sogar im Kinderzimmer, solche Spracherkennungssysteme vorhanden. Die Sprachassistenten sollen die Kommunikation zwischen Maschine und Menschen erheblich erleichtern und verbessern. Im privaten Alltagsbereich werden diese Sprachassistenten mithilfe von bestimmten Sprachbefehlen häufig genutzt wie zum Beispiel: „Alexa, wie wird das Wetter morgen? Hey Siri, welche Einkaufsläden gibt es in der Nähe? OK Google, wie weit ist es bis zum nächsten Supermarkt?“

Allerdings werden diese Sprachassistenten von vielen Menschen derzeit sehr sorglos verwendet, ohne sich über deren Sicherheitsrisiken bewusst zu sein.
So kann der Sprachassistent schnell zum hohen Sicherheitsrisiko werden, wenn sensible Daten wie Passwörter oder Kontoinformationen durch einen Hackerangriff abgefangen und für andere kriminelle Zwecke verwendet werden. Zudem ist es vielen Anwendern nicht bewusst, dass die Sprachassistenten nicht nur aktiviert werden, wenn man direkt vor ihnen steht, sondern es ist auch möglich, Sprachbefehle von außen zu geben. Auf diese Art und Weise ist es Einbrechern schon gelungen, in Wohnungen oder Häuser einzudringen, indem sie die Befehle durch Türen oder Fenster gegeben haben. Es kann aber auch passieren, dass der Assistent unbeabsichtigt aktiviert wird und ungewollt mithört. Problematisch ist das bei Spracherkennungssystemen auch deswegen, weil für den Nutzer gar nicht nachvollziehbar ist, was genau mit den Aufnahmen passiert, die häufig personenbezogene Daten enthalten.

Ziel der Master-Thesis ist es, einen Überblick über IT-Sicherheitsrisiken der Sprachsysteme zu geben.

## 1.2 Vorgehen

Die Master-Thesis gliedert sich in sieben Kapitel. Das zweite Kapitel widmet sich der Grundlagen und beinhaltet die Grundbegriffe der Künstlichen Intelligenz sowie die Geschichte der einzelnen Sprachassistenten Amazon Alexa, Google Home und Apple Siri. Als nächstes werden im dritten Kapitel die technischen Details, d.h. die Architektur und Funktionsweise der einzelnen Sprachassistenten erläutert und beschrieben. Im vierten Kapitel werden die Systeme hinsichtlich Sicherheit und Forensik verglichen. Im folgenden fünften Kapital wird der Datenschutz der einzelnen Sprachassistenten analysiert. Schließlich vergleiche ich im sechsten Kapitel die Sprachassistenten in Bezug auf ihre Einsatzmöglichkeiten sowie ihrer Stärken und Schwächen. Zum Schluss, im siebten Kapitel, erfolgt eine kurze Zusammenfassung.

## 1.3 Abgrenzung

Folgende Bereiche können in der Master-Thesis behandelt werden:

- Es werden nur drei Sprachassistenten Amazon Echo (1. Generation) mit Alexa, Google Home mit Google Assistant und Apple iPhone 6s Plus mit Siri analysiert.
- Es erfolgt keine Hardware Forensik.

## 1.4 Stand der Forschung

Die Thematik *Sicherheitsaspekte von Spracherkennungssystemen* mit der sich die Master-Thesis beschäftigt, ist laut Forschungsstand noch nicht ausreichend analysiert. Laut Ergebnisse der Forschungsarbeiten ist eine Analyse der Sicherheitsrisiken in diesem Bereich deshalb sehr angebracht.

Forschungsliteratur oder wissenschaftliche Publikationen zum konkreten Gegenstand *Sicherheitsaspekte von Sprachsystemen,* ist nicht besonders frequentiert zu finden, jedoch sind einzelne Papers zu nennen, die als Basis des Forschungsstandes dienen. Wie in einem Paper von den Autoren Haack (vgl. Haack u.a. https://cources.csail.mit.edu/6.857/2017/project/8.pdf, 2017) im Jahre 2017 beschrieben, ist es zum Beispiel möglich die

Sprachassistenten durch nicht authentisierte Personen zu aktivieren. Somit ist man imstande durch Fenster, Türen oder sogar durch Stimmen von einem Fernsehgerät, eine Aktivierung auszulösen. Aber auch die Feststellung, dass ein Angriff mit einem Sprachkommando, die für den Menschen im nicht hörbaren Bereich liegt möglich ist, wurde untersucht. Des Weiteren sind Netzwerkangriffe wie Man-in-the-Middle bei denen sensible Daten, im schlimmsten Fall die Kontoinformationen abgefangen werden können möglich. Ebenfalls wird in dem Paper erwähnt, dass über Schnittstellen zu Drittanbietern Angriffe ausgeführt werden können.

Auch Wuesst (vgl. Wuesst, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-security-voice-activated-smart-speakers-en.pdf, 2017) kommt im Jahre 2017 zu ähnlichen Erkenntnissen wie Haack. Allerdings werden die Forschungserkenntnisse dahingehend erweitert, dass es wichtig ist, seine WLAN-Umgebung vor Angriffen ausreichend zu schützen. So wird empfohlen mindestens eine WPA2-Verschlüsselung zu wählen und neben einem starken Passwort regelmäßig Updates auszuführen. Des Weiteren wird auch auf bereits erfolgreich ausgeführte Bluetooth-Angriffe hingewiesen, vorausgesetzt, ein Angreifer befindet sich in Reichweite. Im Unterschied zu Haack hat Wuesst in seiner Publikation auch den Datenschutz der Sprachassistenten untersucht. Laut Studie befürchten immer mehr Nutzer, dass ihre private Kommunikation permanent überwacht oder von unbefugten Dritten mitgehört und weiterverwendet wird.

Die Autoren Zhang (vgl. Zhang u.a. https://arxiv.org/pdf/1805.01525.pdf, 2018) widmen sich im Jahre 2018 in einem Paper speziell der Untersuchung von Skills von Drittanbietern die zum Sicherheitsrisiko werden können. In der Studie konnte nachgewiesen werden, dass zwei neue Angriffsarten bei den Skills vorkommen können. Zu einem, dass es möglich ist, böswillige Skills zu veröffentlichen, die dann durch ähnliche Signalwörter unwissentlich ausgeführt werden und zum Beispiel heimlich die private Kommunikation aufzeichnen können. Des Weiteren ist es laut Studie möglich, die Aktionen von Skills so zu manipulieren, dass diese in Wirklichkeit im Hintergrund dann eine andere Funktion ausführen. Da die wissenschaftlichen Publikationen meistens aus dem Jahre 2017 und 2018 sind, sind manche Erkenntnisse möglicherweise heute nicht mehr aktuell. Allerdings zeigen die Forschungsergebnisse auch, dass verschiedene Sicherheitsrisiken vorhanden sind, die näher in dieser Arbeit analysiert werden sollen, um letztendlich neue Erkenntnisse zu gewinnen.

# 2 Grundlagen

In diesem Kapitel wird zunächst definiert, was unter der Künstlichen Intelligenz sowie deren wichtigsten Grundbegriffen verstanden wird. Darüber hinaus wird die Geschichte der einzelnen Sprachassistenten Amazon Alexa, Google Home und Apple Siri erläutert, um ein besseres Verständnis zu erhalten.

## 2.1 Künstliche Intelligenz

Für den Begriff Künstliche Intelligenz oder KI (engl. artificial intelligence oder AI) gibt es eine Vielzahl von Definitionen, daher ist es nicht leicht eine einheitliche Begriffsbestimmung zu finden. Vor allem ist es schwierig, den Ausdruck „Intelligenz“ exakt zu formulieren, da es in verschiedenen Wissenschaften unterschiedlich ausgelegt und bewertet wird. „John McCarthy, einer der Pioniere der KI, definierte 1955 als Erster den Begriff Künstliche Intelligenz etwa so: Ziel der KI ist es, Maschinen zu entwickeln, die sich verhalten, als verfügten sie über Intelligenz.“ (Ertel, 2016, S. 1) Die Künstliche Intelligenz ist ein Teilgebiet der Informatik die sich damit befasst, intelligente Agenten zu entwickeln, die selbständig Funktionen ausführen können wie beispielsweise: Problemlösung, logisches Denken, aus vergangenen Ereignissen zu lernen oder Spracherkennung. Bei der Künstlichen Intelligenz wird unterschieden zwischen einer starken KI und schwachen KI. Bei einer starken Künstlichen Intelligenz wird versucht die Vorgänge im menschlichen Gehirn abzubilden beziehungsweise zu imitieren. Allerdings ist die heutige Forschung noch weit von so einem System entfernt. Anders sieht es bei der schwachen KI aus, die gezielt Algorithmen für bestimmte Problemstellungen entwickelt. Für beide Varianten, die starke als auch die schwache KI, ist die Lernfähigkeit eine Grundanforderung. Die folgende Abbildung zeigt die wichtigsten Begriffe im Umfeld der Künstlichen Intelligenz:

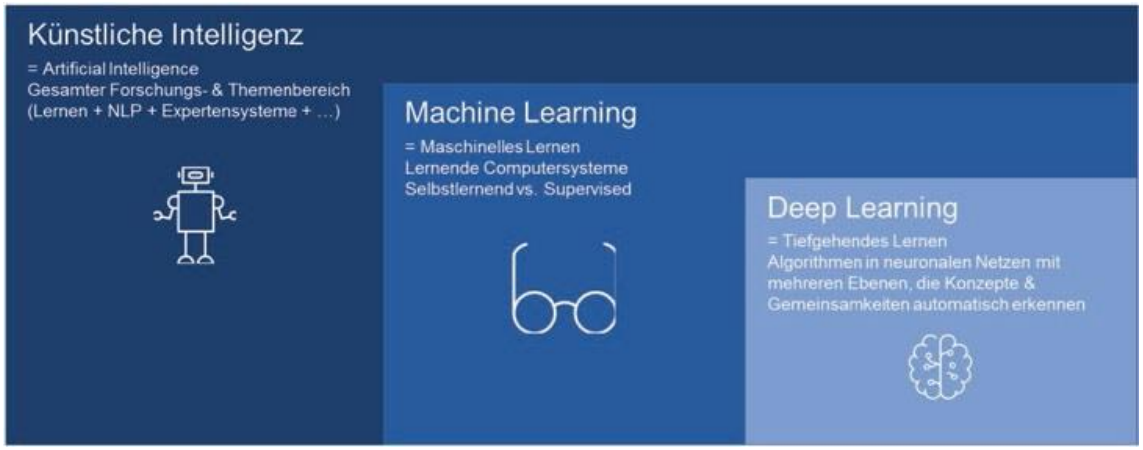



**Bild 1: Wichtige Begriffe und Definitionen im Umfeld von KI (Buxmann, Schmidt, 2019, S. 123)**

### 2.1.1 Maschinelles Lernen

Ein zentraler Baustein von allen Sprachassistenten ist maschinelles Lernen. Maschinelles Lernen (engl. Machine Learning oder ML) ist ein wichtiger Teilbereich der Künstlichen Intelligenz. Im Allgemeinen beschreibt der Begriff maschinelles Lernen „Die Fähigkeit einer Maschine oder Software, bestimmte Aufgaben zu lernen, beruht darauf, dass sie auf der Basis von Erfahrungen (Daten) trainiert wird.“ (Buxmann, Schmidt, 2019, S. 8)

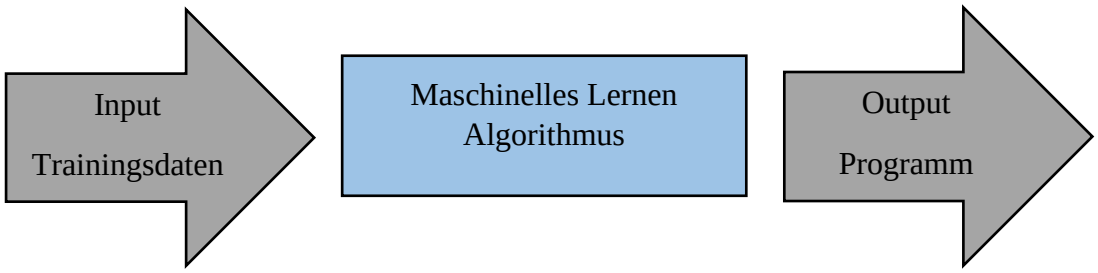



**Bild 2: Aufbau eines Maschinelles Lernen Algorithmus (Eigene Zeichnung)**

Prinzipiell, lässt sich das maschinelle Lernen in folgende Lernmethoden unterteilen:

- **überwachtes Lernen** (Supervised Learning)
- **unüberwachtes Lernen** (Unsupervised Learning)
- **bestärkendes Lernen** (Reinforcement Learning)
- **teilüberwachtes Lernen** (Semisupervised Learning)

Bei der ersten Art, dem **überwachten Lernen**, gibt es Trainingsdaten die eindeutig beschriftet sind. Dadurch kann der Algorithmus selbständig bessere Entscheidungen treffen und Verbindungen herstellen, ähnlich wie Menschen beim Lernen vorgehen. Beschriftet bedeutet hier, dass der Algorithmus jedes Mal die Informationen erhält, um welche Tierart (Hund, Katze usw.) es sich z.B. auf Bildern von Tieren handelt. Nach dem Lernen erfolgt eine Überprüfung mit Testdaten.

Demgegenüber steht das **unüberwachte Lernen**. Bei diesem Ansatz gibt es eine Menge von Daten, allerdings ist hier die Klassenzugehörigkeit der Daten nicht bekannt. Wenn man hier das Beispiel vom ersten Ansatz betrachtet, dann wird hier dem Algorithmus nicht mitgeteilt um welche Tierart es sich auf den Bildern handelt, sondern der Algorithmus muss selbst die Klassenzugehörigkeiten finden.

Bei der dritten Art, **bestärkendes Lernen** sollte der Algorithmus selbstständig eine Strategie erlernen, um Belohnungen zu erhalten. Hier soll der Algorithmus aus der Bestärkung lernen. Ein Beispiel ist hier der Restaurantbesuch. Das Fehlen eines Trinkgeldes an den Kellner gibt dem Algorithmus einen Hinweis darauf, dass sein Verhalten nicht wünschenswert ist.

Eine andere Lernmethode ist das **teilüberwachte Lernen**. Diese Methode wird für die gleichen Zwecke wie das überwachte Lernen eingesetzt. Allerdings werden hier nur wenig Daten mit Beschriftung und viele ohne Beschriftung verwendet. Diese Technik kann zum Beispiel für die Identifikation von Gesichtern benutzt werden.

Maschinelles Lernen hat sich in das heutige Leben etabliert. Waren selbst lernende Programme noch bis vor kurzem nur für bestimmte Institutionen oder moderne Unternehmen vorbehalten, so sind sie nun auch für normale Anwender zugänglich. Diesen Umstand verdankt das maschinelle Lernen auch den verbesserten Rahmenbedingungen. So ist es möglich, auf eine nie gekannte verfügbare Menge von Daten bzw. Big Data zurückzugreifen sowie eine verbesserte Rechenleistung. Anwendungsbeispiele für maschinelles Lernen sind zum Beispiel digitale Sprachassistenten, Spracherkennung auf Mobiltelefonen, medizinische Diagnosen, Spam-Filter oder Gesichtserkennung.

### 2.1.2 Deep Learning

„Deep Learning ist eine spezielle Methode der Informationsverarbeitung und ein Teilbereich von Machine Learning, das neuronale Netze sowie große Datenmengen zur Entscheidungsfindung nutzt“ (Kownatzki, 2018, https://www.empolis.com/blog/kuenstliche-intelligenz/deep-learning/) Durch die Nutzung von bestehenden Informationen und dem neuronalen Netz, ist das System in der Lage, das Erlernte mit neuen Inhalten zu verbinden und so erneut zu lernen. „Die Grundidee der Entwicklung von KNN besteht darin, das (menschliche) Gehirn zu simulieren. Allgemein besteht ein KNN daher aus Knoten (Neuronen) und Kanten (Synapsen).“ (Buxmann, Schmidt, 2019, S. 13) Das neuronale Netz verfügt über eine Eingangsschicht und einer Ausgangsschicht, dazwischen befinden sich mehre Zwischenschichten. Je nach getroffener Entscheidung erhalten dann die Informationsverknüpfungen eine höhere oder niedrigere Gewichtung.

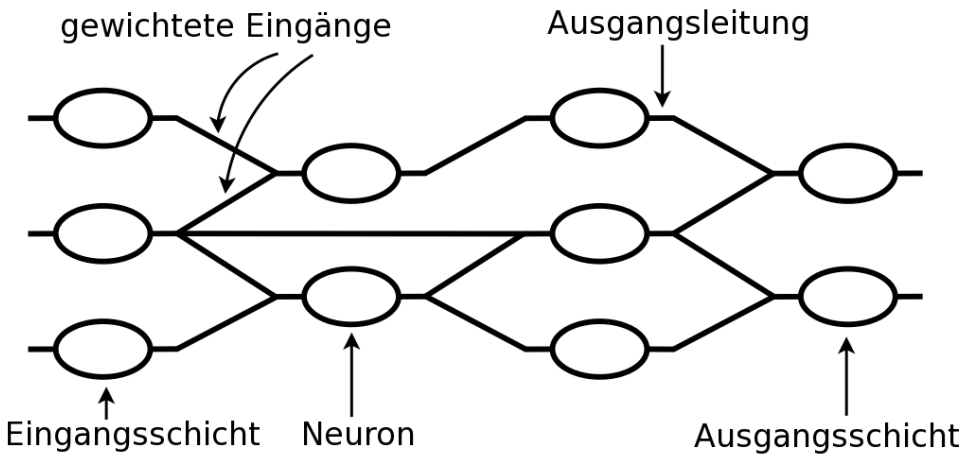



**Bild 3: Neuronales Netz (http://emergenz.hpfsc.de/da_sstein.pdf, S.33)**

Das Ergebnis ist, dass es der Maschine möglich ist, Prognosen oder Entscheidungen zu treffen und diese in Frage zu stellen. Der Mensch überlässt der Maschine den Lernprozess und beeinflusst diesen nicht mehr. Der Hauptunterschied besteht darin, dass sich beim maschinellen Lernen der Mensch in die Analyse der Daten und den Entscheidungsprozess einmischt. Im Gegensatz dazu werden beim Deep Learning von Menschen nur die Informationen für den Lernprozess zur Verfügung gestellt. Die eigentliche Entscheidung und Prognose überlässt er der Maschine. Problem ist hier, dass im Anschluss nicht mehr klar nachvollzogen werden kann, auf welcher Basis die Maschine oder diese Black Box eine Entscheidung getroffen hat. Deep Learning kann für eine Vielzahl von Anwendungsfällen im Bereich der Künstlichen Intelligenz eingesetzt werden. So spielt Deep Learning bei

den Sprachassistenten eine immer wichtigere Rolle. Benutzt man Sprachassistenten im Alltag, merkt man schnell, dass noch nicht alles perfekt ist. So stoßen die digitalen Assistenten bei unterschiedlichen Sprachmustern und verschiedenen Akzenten von Menschen schnell an ihre Grenzen. Hier können Deep-Learning-Algorithmen helfen die menschliche Sprache besser zu verstehen. Bereits das Erkennen des „Aufwachwortes“, basiert auf Deep-Learning-Technologie.

## 2.2 Geschichte der einzelnen Sprachassistenten

Nachfolgend werden nun die einzelnen Geschichten der Sprachassistenten erläutert.

### 2.2.1 Amazon

Die Website Amazon.com ist weltweit einer der größten Online-Versandhändler. Gegründet wurde das Unternehmen Amazon.com im Jahre 1994 von Jeffrey P. Bezos in einer Garage in Seattle. Der Name Amazon soll eine Anspielung auf den Amazonas sein, dem längsten Fluss der Welt und steht für eine große Auswahl. Zudem enthält das Amazon Logo ein Schmunzeln, in Form eines Pfeils, dass den ersten Buchstaben „A“ und den Buchstaben „Z“ verbindet und soll alles von „A“ bis „Z“ interpretieren. Das Lächeln soll die Zufriedenheit der Kunden veranschaulichen, also die Produktvielfalt darstellen. Die Idee von Jeffrey P. Bezos war anfangs ein elektronisches Buchgeschäft. Als dann im Jahre 1995 der Online-Buchhandel online war und das erste Buch verkauft wurde, begann eine unvorstellbare Erfolgsgeschichte. Bereits im ersten Jahr 1996, ein Jahr nach der Gründung, machte das Unternehmen einen Umsatz von 15,7 Millionen US-Dollar, im Folgejahr 1997 bereits 147,8 Millionen US-Dollar. In den darauffolgenden Jahren erweiterte Amazon stets sein Sortiment, Waren und Dienste. Amazon bietet die weltweit größte Auswahl an Elektronik & Foto, Bücher sowie Küche & Haushalt an. Im Prinzip kann bei Amazon alles bestellt werden was in einen Karton passt. Neben dem klassischen Bücherverkauf bietet Amazon zahlreiche weitere Dienste an. Dazu gehören auch Produkte, die von Amazon selbst entwickelt wurden wie zum Beispiel Amazon Kindle zum Lesen, elektronische Bücher, Tabletcomputer Amazon Fire HD, Fire TV Stick und das Spracherkennungssystem Amazon Echo. Zudem ist es möglich mit einer patentierten „1-Click“ Funktion, Bestellungen nur mit einem Klick auszuführen.

Weitere Dienste sind zum Beispiel:

- **Amazon Marketplace**: Ein Dienst der es ermöglicht, Privatpersonen als auch Unternehmen neue und gebrauchte Waren online anzubieten.
- **Amazon Prime**: Nach Abschluss eines jährlichen Abos ist ein schneller Versand möglich.
- **Amazon Music**: Musik-Downloadshop
- **Amazon Pay**: Online-Bezahlfunktion

Amazon zählt heute mit weltweit über 300 Millionen Kunden und ca. 647.500 Mitarbeiter und einem Umsatz von 232 Milliarden US-Dollar zu den reichsten Unternehmen der Welt. Jeffery P. Bezos der Gründer von Amazon ist heute noch dessen Präsident, Vorsitzender und CEO und gehört zu den reichsten Menschen der Welt.

### 2.2.2 Amazon Alexa

Amazon investierte in den vergangenen Jahren viele Millionen US-Dollar, um einen intelligenten Sprachassistenten zu entwickeln. Der Durchbruch kam für Amazon im Jahre 2013, als man das Start-Up Unternehmen Ivona aus Danzig in Polen übernahm. Die Firma Ivona, die auf Sprachaufnahmen spezialisiert ist, lieferte für Amazon die entsprechende Technik, den Amazon Dienst Alexa Voice Service (AVS), die für einen Sprachassistenten ausschlaggebend ist. Aus dieser Kooperation wurde „Alexa“, ein cloudbasierter Sprachdienst, geboren. Der Name „Alexa“ der zugleich auch das Aktivierungswort ist, soll an die weltbekannte Bibliothek von Alexandria erinnern. Alexa ist eine weibliche Frauenstimme, die auf verschiedene Sprachbefehle antworten und reagieren kann. Dank der Anbindung an die Cloud (Amazon Web Services) und die dahinter vorhandene Künstliche Intelligenz (KI) ist Alexa fähig zu lernen und ihre Fähigkeiten stets weiterzuentwickeln. Alexa ist somit die Schaltzentrale eines jeden Amazons Sprachassistenten.

Erstmals wurde Alexa im Amazon Echo ausgewählten Amazon Prime Kunden am 06. Oktober 2014 in den USA zur Verfügung gestellt. Am 26. Oktober 2016 war es dann auch deutschen Kunden möglich, den Amazon Echo zu erwerben.

Amazon bietet seinen Kunden folgende Produkte mit integrierter Alexa an:

- Am 20. Oktober 2016 wurde **Amazon Echo Dot** (2. Generation) veröffentlicht
- Am 31. Oktober 2017 wurde **Amazon Echo** (2. Generation) veröffentlicht
- Am 19. Dezember 2017 wurde **Amazon Echo Spot** veröffentlicht
- Am 31. Oktober 2017 wurde **Amazon Echo Plus** veröffentlicht
- Am 26. April 2017 wurde **Amazon Echo Look** veröffentlicht
- Am 28. Juni 2017 wurde **Amazon Echo Show** veröffentlicht
- Am 13. Dezember 2017 wurde **Echo Connect** veröffentlicht
- Am Juni 2016 wurde **Amazon Tap** veröffentlicht
- Am Juni 2017 wurde **Amazon Dash Wand** veröffentlicht

Die folgende Abbildung zeigt die verschiedenen Amazon Echo Produktvarianten.

**Bild 4: Amazons Echo Produktlinie (https://www.cnet.com/news/heres-every-echo-that-amazon-has-ever-announced/)**

### 2.2.3 Google

Die Internetseite Google.com ist weltweit einer der erfolgreichsten Internetsuchmaschinen der Welt. Gegründet wurde das Unternehmen Google. Inc. am 07. September 1998 von Lary Page und Sergey Brin in einer kleinen Garage in der Stadt Menlo Park in Kalifornien. Lary Page und Sergey Brin kannten sich bereits schon aus ihrem gemeinsamen Studium an der Standardford University. Der Begriff „Google“ sollte eine Ableitung von dem Namen „Googol“ sein. Der Name „Googol“ ist eine Zahl aus der Mathematik und ist die Bezeichnung für eine Zahl mit 100 Nullen. Für die beiden Gründer Lary Page und Sergey Brin sollte der Name „Google“ als Sinnbild stehen, für die unglaubliche Menge an Webseiten, die Google in seinen Suchindex einbinden sollte. Dabei erzielt Google 99 Prozent seines Einkommens durch Werbung. Google ermöglicht die Suchergebnisse in weniger als einer Sekunde. Der Suchdienst ist für die Benutzer kostenlos. Google bearbeitet pro Tag ca. mehr als drei Milliarden Suchanfragen. Im Jahre 2002 war der Umsatz

von Google bei 400 Millionen US-Dollar und bereits im folgenden Jahr 2003 bei 1,5 Milliarden US-Dollar. Neben dem Kerngeschäft der Suchmaschine hat sich Google stets weiterentwickelt und bietet inzwischen mehr als 60 Onlineprodukte an. Auch diese Produkte stehen dem Kunden weitestgehend kostenlos zur Verfügung. Dazu gehören beispielsweise:

- **Gmail**
- **Google Docs**
- **Google Earth**
- **Google Map**
- **Google Assistant**
- **Google Translate**

Im Jahre 2006 kaufte Google das Videoportal YouTube und somit zählt nun auch diese Onlineplattform zum Google Produktportfolio. Mit ca. 98.771 Mitarbeiter weltweit und einem Umsatz im Jahre 2018 von 136,8 Milliarden US-Dollar zählt Google zu den reichsten Firmen der Welt. Larry Page ist Vorstandsmitglied und Sergey Brin ist seit 2015 der Präsident der Tochterfirma von Google Alphabet Inc. Beide gehören heute zu den reichsten Menschen der Welt. Sundar Pichai ist seit 2015 Vorstandsmitglied von Google.

### 2.2.4 Google Home

Der von Google entwickelte Smart-Home-Lautsprecher ist Google Home. Google Home beinhaltet einen intelligenten Sprachassistenten genannt Google Assistant. Google Assistant ist der Nachfolger von Google Now. Der Google Assistant ist eine Software mit einer weiblichen oder männlichen Stimme, die hauptsächlich gesprochene Sprache empfängt und verarbeitet. Google Assistant ist auf immer mehr Geräten verfügbar. So ist der Google Assistant auf Android-Betriebssystemen, Google Home und als APP auf iOS-Smartphones und Tablets verfügbar. Google Home wurde zusammen mit dem dazugehörigen Google Assistant erstmals am 18. Mai 2016 auf der Google Entwicklerkonferenz vorgestellt. Anschließend wurde Google Home am 04. Oktober 2016 zuerst in den USA veröffentlicht. In Deutschland ist Google Home seit dem 08. August 2017 erhältlich.

Google veröffentlichte folgende Google Home Varianten in Kombination mit Google Assistant:

- Am 04. Oktober 2017 wurde **Google Home Mini** veröffentlicht
- Am 11. Dezember 2017 wurde **Google Home Max** veröffentlicht
- Am 09. Oktober 2018 wurde **Google Home Hub** veröffentlich

Im unteren Bild wird ein Überblick der Google Home Produktlinie dargestellt.

**Bild 5: Google Home Produktlinie (https://store.google.com/de/category/connected_home)**

### 2.2.5 Apple

Das Unternehmen Apple Inc. ist ein amerikanisches Technologieunternehmen mit dem Geschäftszweig Hardwareentwicklung und Softwareentwicklung. Die Firma Apple wurde am 01. April 1976 in Palo Alto in Silicon Valley USA als Garagenfirma von Steve Jobs, Stephan Wozniak und Ronald Wayne gegründet. Wobei der Mitbegründer Ronald Wayne bereits nach einer Woche das Unternehmen wieder verlassen hatte. Apple gehört zu den ersten Herstellern von Personal Computern. Bereits im ersten Jahr erzielte Apple einen Umsatz von mehreren hunderttausend US-Dollar. Apple gehörte somit bereits im Jahre 1982 zu den Top 500 führenden amerikanischen Firmen. Der Name Apple war eine Idee von Steve Jobs. Allerdings gibt es verschiedene Theorien warum Steve Jobs gerade diesen Namen ausgewählt hat. Eine Theorie besagt, dass Steve Jobs, als er gerade auf einer Apfelplantage war, auf den Namen Apple kam. Apple entwickelte seine Produkte und Dienste immer weiter, so lieferte Apple mit dem Apple Macintosh den ersten Personal Computer mit einer Computermaus, die die grafische Bedienoberfläche bedienen konnte, aus. Apple bietet heute zahlreiche verschiedene Hardwareprodukte, Dienste und eigen entwickelte Betriebssysteme an.

Anbei ein Überblick über die zahlreichen Produkte:

**Tabelle 1: Apple Produktübersicht (Eigene Darstellung)**

| Hardware | Betriebssysteme | Dienste |
|---|---|---|
| MacBook | Mac OS | iCloud |
| iPhone | iOS | iMessages |
| iWatch | watchOS | FaceTime |
| iPod | iOS | iMovie |
| AppleTV | tvOS | iLife |
| iPad | iPadOS | iTunes |

Leider verstarb der Gründer Steve Jobs im Jahre 2011 an einer Krebserkrankung. Daher wurde im Jahre 2012 Tim Cook als Nachfolger von Steve Jobs gewählt. Apple zählt heute mit weltweit ca. 123.000 Mitarbeiter und mit einem Umsatz von 265,6 Milliarden US-Dollar zu den wertvollsten Unternehmen der Welt. Tim Cook ist bis heute der Vorstandsvorsitzende von Apple.

### 2.2.6 Apple Siri

Apple kaufte im April 2010 die Firma Siri. Die Firma Siri ist ein Unternehmen, dass sich auf mobile, virtuelle, persönliche Assistenten, die auf Spracherkennung basieren, spezialisiert hatte. Siri war nun eine Software von Apple die als ein intelligenter Assistent Sprachbefehle beantworten konnte. Apple präsentierte am 04. Oktober 2011 erstmals ein Smartphone, dass iPhone 4S mit der Sprachsteuerung Siri. Apple veröffentlichte am Anfang die Software Siri als eine Beta-Version. Der Grund war hierfür, dass Siri erst noch viele Daten sammeln musste, damit das System die gesprochene Sprache von verschiedenen Menschen immer besser verstehen konnte. Ganze zwei Jahre dauerte es bis der Beta Status aufgehoben wurde. Die Abkürzung Siri steht für „Speech Interpretation and Recognition Interface“. Apple entwickelte Siri stets weiter und somit befindet sich heute Siri auf allen Geräten mit dem Betriebssystem iOS.

Siri gibt es auf folgenden Geräten:

„**iPhone**: Jedes iPhone ab dem Modell iPhone 4S

- **iPad**: Ab der 3. Generation (also ab dem iPad, das 2012 auf den Markt kam)
- **iPad mini**: Jedes Modell
- **iPad Air**: Jedes Modell
- **iPad Pro**: Jedes Modell
- **iPod Touch**: Ab der 5. Generation (das sind die Geräte, die Ende 2012 auf den Markt kamen)
- **Mac:** Alle Mac-Computer, auf denen MacOS Sierra installiert ist.
- **Apple TV**: Auf dem Apple TV läuft zwar kein iOS, aber Siri gibt es hier auch, nämlich in Form der Fernbedingung „Siri Remote“, die zusammen mit dem Apple TV der 4. Generation im September 2015 eingeführt wurde.
- **Apple Watch**: Auch auf Apples Smartwatch ist Siri verfügbar.“ (Damaschke, 2016, S. 15)
- **Apple Homepod:** Jedes Modell

**Bild 6: Apple Siri Produktlinie (https://voicebot.ai/2018/01/24/apple-siri-devices-total-500-million-not-users-still/)**

# 3 Technik und Funktion der einzelnen Sprachassistenten

Dieses Kapitel soll einen Einblick in die technischen Details, d.h. die Architektur und Funktionsweise der einzelnen Sprachassistenten gewähren.

## 3.1 Technik der einzelnen Spracherkennungssysteme

Anbei werden nun die technischen Details der einzelnen Sprachassistenten erläutert.

### 3.1.1 Technische Daten von Amazon Echo (1. Generation)

**Bild 7: Aufbau von Amazon Echo (1. Generation) (https://i1.wp.com/amz-echo-ratgeber.de/wp-content/uploads/2017/08/echo-technik.jpg)**

Der Amazon Echo (1. Generation) ist ein zylinderförmiger smarter Lautsprecher, mit dem Intelligenten Persönlichen Assistent (IPA) Alexa. Der Amazon Echo ist erhältlich in zwei Farben: schwarz oder weiß. So besitzt dieses Modell einen 50 mm-Hochtonlautsprecher für die höheren Tonlagen und einen 63 mm-Woofer für tiefere Basstöne. Mit einer Höhe von 235 mm und einem Gewicht von 1064 Gramm gehört der Amazon Echo zusammen mit dem Amazon Echo Plus zu den größten Lautsprechern in der Echo Familie. Das Gerät wird über ein WLAN–Netzwerk mit dem Internet verbunden. Hierbei wird das WLAN-Netzwerk mit den Standards 802.11 a/b/g/n unterstützt. Bei der Bluetooth-Verbindung wird das Advanced Audio Distribution Profile (A2DP) verwendet. Mithilfe eines Lautstärkenringes an der Oberseite, können durch eine Drehung von der Stufe 0 (min.) bis zur Stufe 10 (max.) verschiedene Lautstärkenstufen gewählt werden. Zudem befindet sich auf der Oberseite eine Mikrofon-aus-Taste mit der das Mikrofon deaktiviert werden kann. Somit ist es nicht mehr möglich mit Alexa zu kommunizieren. Mit einer Aktionstaste wird Alexa wieder aktiviert. Unterhalb des Lichtringes befinden sich sieben Mikrofone, die über Richtstrahltechnologie und Geräuschunterdrückung verfügen. An der Unterseite befindet sich eine Reset-Taste, die man mithilfe einer Büroklammer 20 Sekunden lang gedrückt hält, so dass der Amazon Echo zurückgesetzt werden kann.

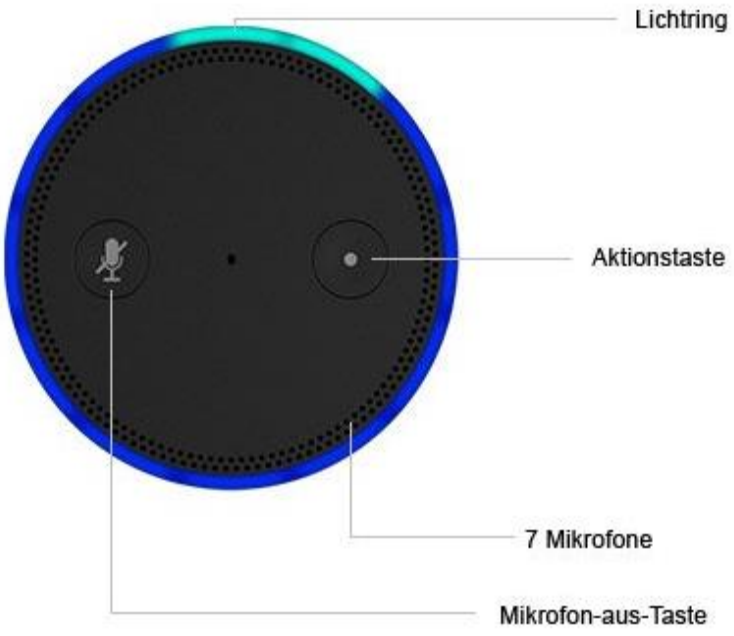



**Bild 8: Draufsicht von Amazon Echo (1. Generation) von oben (https://schleeh.de/2016/11/05/alexa-auf-dem-amazon-echo-einrichten-der-digitale-sprachassistent-im-haus/)**

### 3.1.2 Technische Daten von Google Home

Google Home ist ein smarter Lautsprecher, mit dem Intelligenten Persönlichen Assistent (IPA) Google Assistant. Der Google Home ist in verschiedenen Farben erhältlich: Schiefer (Hellgrau), Karbon (Dunkelgrau, Schwarz), Kupfer, Koralle (Stoffausführung). Google Home verwendet drei Lautsprecher, sogenannte High Excursion-Lautsprecher, 2“-Treiber plus 2“-Passivradiatoren und zwei Mikrofone. Zudem wird eine Fair Field-Technologie verwendet, um die Sprache besser erkennen zu können. Das Gerät hat eine Höhe von 142,8 mm und einen Durchmesser von 96,4 mm. Für eine Internetverbindung wird das WLAN mit 802.11b/g/n/ac (2,4 GHz / 5 GHz) unterstützt. Dabei wird WPA2-Enterprise nicht unterstützt.

**Bild 9: Google Home Aufbau (https://electronics360.globalspec.com/article/7718/all-the-technology-inside-your-google-home)**

Der gesamte obere Teil vom Google Home kann per Touch Oberfläche bedient werden. Auf der Oberseite befinden sich vier LED`s mit denen farblich der aktuelle Status

angezeigt und die Lautstärke geregelt werden kann. Zudem können per Touch-Oberfläche durch einmal Tippen Antworten oder Wiedergaben gestoppt werden. Durch langes Drücken in der Mitte kann der Google Assistant gestartet werden. Außerdem sind auf der Oberseite zwei Mikrofone integriert. Auf der Rückseite befindet sich die Mikrofon Aus-Taste ist diese aktiviert ist das Mikrofon deaktiviert und der Google Home hört nicht mehr zu und kann nicht reagieren. Zudem besitzt Google Home im inneren Bereich bei den Lautsprechern noch einen Micro-USB-Port, der aber nur für den Support-Service vorgesehen ist und nicht für die Anwender. Google Home wird automatisch über das Internet aktualisiert, falls ein neues Update zur Verfügung steht. Damit man Google Home auf die Werkseinstellungen zurücksetzen kann, ist es notwendig auf der Rückseite die Mikrofonstummtaste 12 Sekunden gedrückt zu halten.

**Bild 10: Ansicht von Google Home (http://www.areamobile.de/bilder/211683-original-google-home-c-google)**

### 3.1.3 Technische Daten von iPhone 6s Plus

Das iPhone 6s Plus ist ein Smartphone mit dem Intelligenten Persönlichen Assistent (IPA) Siri. Das iPhone ist in vier verschiedenen Farben erhältlich: Roségold, Gold, Silber und Space Grau. Das Gerät gibt es mit folgenden Speicherkapazitäten: 16 GB, 32 GB, 64 GB und 128 GB.

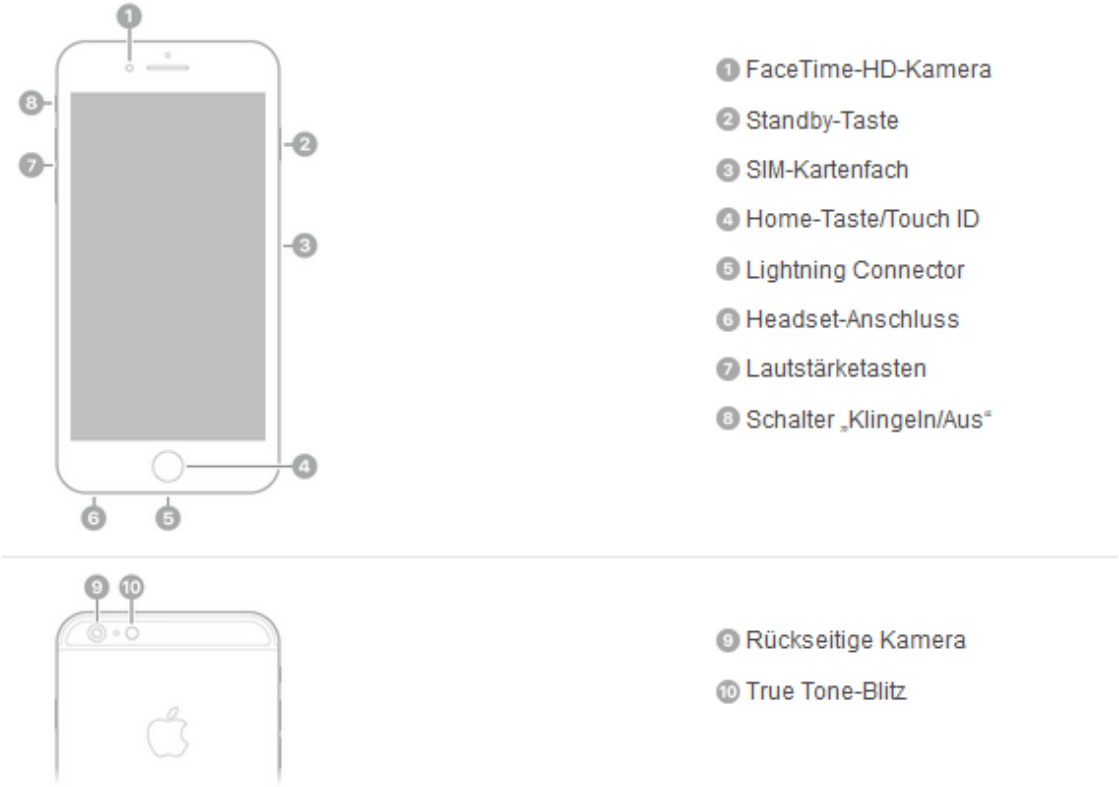



**Bild 11: iPhone 6s Plus Technik Details (https://help.apple.com/iphone/11/?lang=de#iphf8ff0253f)**

Das Smartphone hat folgende Abmessungen: eine Höhe von 158,2 mm, Breite: 77,9 mm, Tiefe: 7,3mm und ein Gewicht von 192 Gramm. Hierbei wird das WLAN-Netzwerk mit 802.11ac mit MIMO unterstützt. Bei der Bluetooth-Verbindung wird die Version 4.2 verwendet. Die Bedienung des iPhones erfolgt hauptsächlich durch einen Touchscreen oder die Home-Taste. Die Konfiguration des iPhones sowie die Eigenschaften der einzelnen Apps erfolgt weitgehend über die App „Einstellungen“.

## 3.2 Architektur und Funktion der Spracherkennungssysteme

Nachfolgend wird die Architektur und Funktion der einzelnen Sprachassistenten beschrieben.

### 3.2.1 Architektur und Funktion von Amazon Echo

Bevor man Amazon Echo benutzen kann, müssen gewisse Voraussetzungen erfüllt sein. So ist für die Einrichtung der Echo-Modelle die Nutzung einer entsprechenden mobilen App notwendig. Bei den Echo-Modellen ist es die Alexa-App, die kostenlos im jeweiligen App Store je nach verwendetem Endgerät, hier Tablet oder Smartphone, heruntergeladen werden kann. Die Alexa-App steht für Android, iOS und Fire OS zur Verfügung. Die Alexa-App führt den Anwender Schritt für Schritt durch die Konfiguration des Amazon Echo. Es gibt aber auch die Möglichkeit über den Web-Browser, also mit dem Computer, über die URL-Adresse: https://alexa.amazon.de den Echo einzurichten. Allerdings ist hier zu beachten, dass über den Web-Browser nicht alle Funktionen zur Verfügung stehen. Daher wird für die Einrichtung des Echos die App empfohlen. Zudem ist es notwendig für die Einrichtung einen Amazon Account zu besitzen. Für den Betrieb des Amazon Echo ist es erforderlich, dass dieser immer am Netzteil aktiv angeschlossen ist. Daher ist der Amazon Echo nicht tragbar, sondern steht meistens in einem Raum an einem bestimmten Ort. Für die Einrichtung wird empfohlen den Amazon Echo an einer zentralen Stelle im Raum mit ca. 20 cm Abstand von Wänden und Fenster zu platzieren. Die Verbindung mit dem Internet erfolgt hier über das WLAN. Erst wenn die oben aufgeführten Optionen erfüllt sind, ist der Amazon Echo einsatzbereit und voll funktions-fähig.

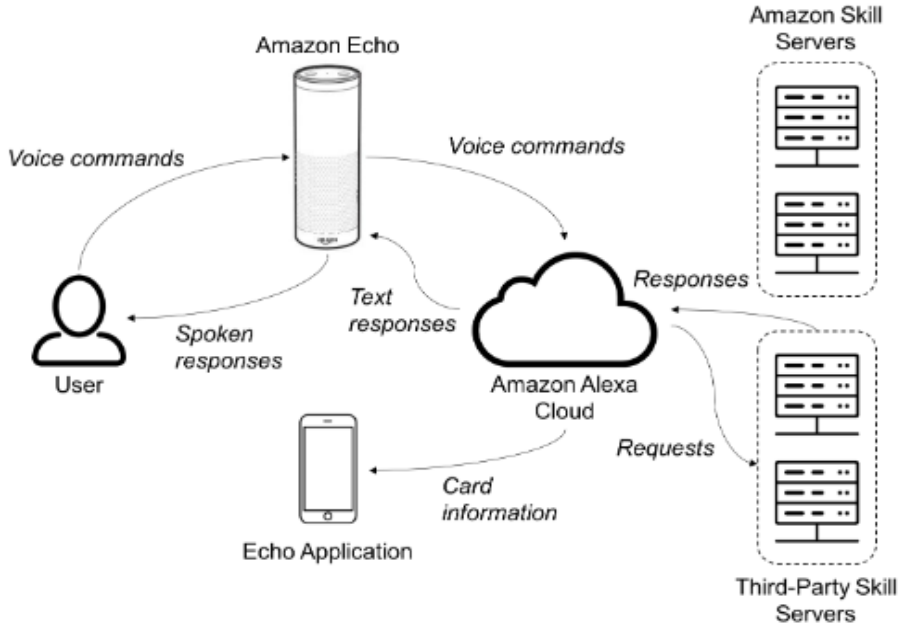



**Bild 12: Architektur von Amazon Echo (1.Generation) (https://courses.csail.mit.edu/6.857/2017/project/8.pdf, S. 2)**

Die Funktionsweise des Amazon Echo wird nun mit folgenden Schritten erläutert:

1. Die Kommunikation mit dem Amazon Echo erfolgt hauptsächlich über gesprochene Sprache. Es gibt keine anderen Eingabequellen wie Tastatur oder Touchscreen. Der Amazon Echo beinhaltet ein Mikrofon-Array, dass permanent aktiv eingeschaltet ist und eine eingehende Nutzeranfrage hier Sprachsignal nach einem Aktivierungswort filtert.

   **„Alexa“** wie wird das Wetter in Stuttgart?“

   Das Aktivierungswort ist hier „Alexa“, nur wenn das Gerät dieses Aktivierungswort wahrnimmt, wird er aktiv und hört zu. Beim Amazon Echo kann man zwischen vier unterschiedlichen Aktivierungswörter wählen:

   - **„Alexa“**
   - **„Amazon“**
   - **„Echo“**
   - **„Computer“**

Die Definition von anderen Aktivierungswörter ist nicht möglich.

War die Spracheingabe erfolgreich, kann man dies an den Farben des Lichtringes an der Oberseite des Amazon Echo erkennen. Folgende Lichtsignale sind möglich:

**Tabelle 2: Status Lichtring von Amazon Echo (1. Generation) (Eigene Darstellung Daten aus: https://www.amazon.de/gp/help/customer/display.html?nodeId=201601790)**

| Status Lichtring | Funktion |
|---|---|
| **Alle Lichter sind aus** | Das Gerät ist eingeschaltet und wartet auf ihre Aufforderung. |
| **Durchgehend blau mit zyanblauen, sich drehenden Lichtern** | Das Gerät wird gestartet. |
| **Durchgehend blau mit zyanblau in Richtung der Person, die spricht** | Alexa ist damit beschäftigt, ihre Anfrage zu verarbeiten. |
| **Abwechselnd einfarbig blau und zyanblau** | Das Gerät reagiert. |
| **Orangefarbenes Licht, das sich im Uhrzeigersinn dreht** | Das Gerät verbindet sich mit dem WLAN-Netzwerk. |
| **Durchgehend rotes Licht** | Sie haben die Mikrofone auf dem Gerät ausgeschaltet. Drücken Sie die **Mikrofontaste**, um die Mikrofone einzuschalten. |
| **Pulsierendes gelbes Licht** | Eine Nachricht oder Benachrichtigung wartet auf sie. Sagen sie „Spiele meine Nachrichten ab“ oder „Was sind meine Benachrichtigungen?“ |
| **Pulsierendes grünes Licht** | Sie erhalten einen Anruf. Oder jemand führt ein Drop In bei ihrem Gerät durch. |
| **Grünes Licht, das sich im Uhrzeigersinn dreht** | Sie befinden sich in einem aktiven Gespräch. Oder es findet gerade ein aktiver Drop In auf ihrem Gerät statt. |
| **Weißes Licht** | Sie passen die Lautstärke auf dem Gerät an. |
| **Kontinuierlich pulsierendes, violettes Licht** | Bei der WLAN-Einrichtung ist ein Fehler aufgetreten. |
| **Ein Aufblitzen des lilafarbenen Lichts nach einer Interaktion mit Alexa** | Bitte nicht stören ist aktiviert. |

2. Anschließend wird der Audio-Mitschnitt zur Sprachanalyse an die Amazon Alexa Cloud gesendet und dort gespeichert.
3. Verläuft die Analyse erfolgreich, wird die Antwort vom entsprechenden Dienst, hier der Wetterdienst, an Amazon Alexa Service Plattform zurück übertragen.
4. Alexa sendet dann die Antwort an den Amazon Echo.
5. Amazon Echo antwortet dann mit gesprochener Ausgabe der Antwort:

„Das Wetter in Stuttgart wird sonnig bei 20 Grad“

### 3.2.2 Architektur und Funktion von Google Home

Damit Google Home voll einsatzbereit und funktionsfähig ist, müssen gewisse Voreinstellungen vorgenommen werden. So ist es für die Inbetriebnahme notwendig, dass das Gerät mit dem Netzteil, also per Stromkabel, und mit dem heimischen Netzwerk über WLAN stetig verbunden ist. Deswegen ist Google Home nicht tragbar und steht fest an einer bestimmten Stelle in einem Raum. Die Einrichtung aller Google Home Geräte erfolgt über die Verwendung einer mobilen App. Die Einrichtungs-App für die Google Home Geräte ist die Google-Home-App, die kostenlos über den App Store heruntergeladen werden kann. Die Google-Home-App steht für Android als auch für iOS, also Smartphones und Tablets, zur Verfügung. Die Möglichkeit der Einrichtung der Home-Geräte über einen Web-Browser gibt es nicht. Zudem ist es notwendig für die Einrichtung ein Google Konto zu besitzen. Erst wenn die oben aufgeführten Punkte erfüllt sind, ist Google Home einsatzbereit.

Die Funktionsweise von Google Home wird nun mit folgenden Schritten erläutert:

1. Die Kommunikation mit Google Home erfolgt hauptsächlich über gesprochene Sprache. Es gibt keine anderen Eingabequellen wie Tastatur oder Touchscreen. Google Home beinhaltet ein Mikrofon, dass permanent eingeschaltet ist und eine eingehende Nutzeranfrage, hier Sprachsignal, nach einem Aktivierungswort filtert.

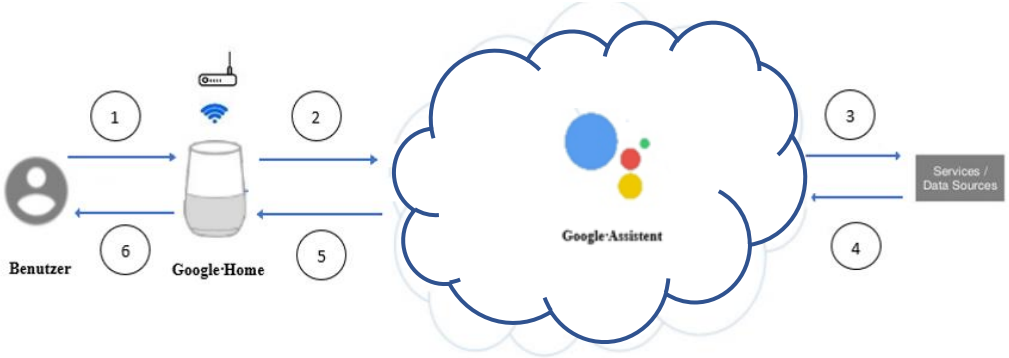



**Bild 13: Architektur von Google Home (Eigene Darstellung Daten aus: https://www.slideshare.net/bretmc/google-home-and-google-assistant-workshop-build-your-own-serverless-action-on-google-app)**

„OK Google, hat Bayern München gewonnen?“

Das Aktivierungswort ist hier „OK Google“, nur wenn das Gerät dieses Aktivierungswort wahrnimmt, wird er aktiv und hört zu. Beim Google Home kann man zwischen zwei unterschiedlichen Aktivierungswörter wählen:

- **„OK Google“**
- **„Hey Google“**

Die Definition von anderen Aktivierungswörter ist nicht möglich.

2. War die Spracheingabe erfolgreich, kann man dies an den Farben der LED`S an der Oberseite des Google Home erkennen. Folgende Lichtsignale sind möglich:

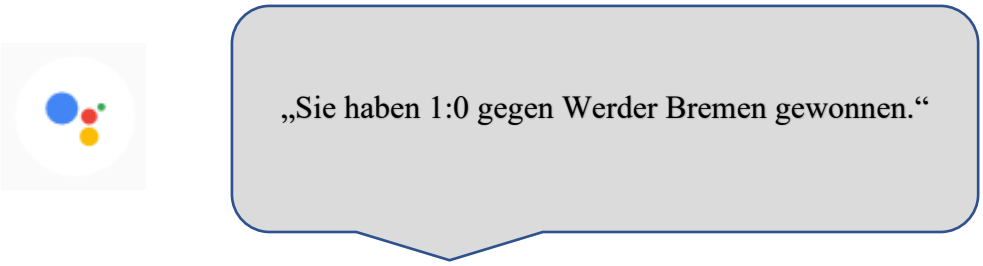
**Tabelle 3: Leuchtanzeige von Google Home (Eigen Darstellung Daten aus: https://support.google.com/googlehome/answer/7073219)**

| Status Leuchtanzeige | Funktion |
|---|---|
| Fortlaufendes Drehen im Uhrzeigersinn (mehrfarbig) | Google Home hat wahrgenommen, dass "Hey Google" oder "OK Google" gesagt wurde und wartet auf ihren Sprachbefehl |

| Status Leuchtanzeige | Funktion |
|---|---|
| Fortlaufendes Drehen im Uhrzeigersinn (mehrfarbig) | Google Home verarbeitet das Gehörte |
| Fortlaufendes Pulsieren (mehrfarbig) | Google Home reagiert |
| Durchgängiges Leuchten (orange) | Mikrofon ist stummgeschaltet (Google Home hört nicht zu und kann nicht reagieren) |
| Langsames Pulsieren (weiß) | Bereit zur Einrichtung |
| Langsames Pulsieren (blau) | Gerät wird geprüft |
| Drehen im Uhrzeigersinn (weiß) | WLAN-Verbindung wird hergestellt |
| Aufleuchten von oben nach unten (weiß) | Download läuft |
| Drehen im Uhrzeigersinn (weiß) | Installation läuft |
| Drehen und Blinken (weiß und mehrfarbig) | Starten |
| Countdown (orange) | Zurücksetzen auf Werkseinstellungen |
| Langsames Pulsieren (weiß) | Wecker klingelt |
| Drehen (weiß) | Timer klingelt |
| 1 weiße LED, die ca. 10 Minuten durchgehend leuchtet, wenn eine Benachrichtigung vorhanden ist. Sagen sie "Hey Google, was gibt es Neues?", um die Benachrichtigung zu hören. | Erinnerung |
| 1 Punkt in der Mitte (weiß) Nur sichtbar, wenn sie die Geste zur Lautstärkeregelung machen | Stummgeschaltet |
| 1 Punkt (weiß)/10 Punkte (weiß) | Lautstärke 1 / Lautstärke 10 |
| Durchgängiges Leuchten von 6 LEDs (orange) | Update dauert länger als erwartet |

Die Spracheingabe wird nun an den Google Server mit dem Google Assistant in der Google Cloud weitergeleitet und gespeichert.

3. Anschließend wird der Audio-Mitschnitt zur Sprachanalyse gesendet. Verläuft die Analyse erfolgreich, wird die Antwort vom entsprechenden Dienst, hier den Sportdienst, an die Google Cloud mit dem Google Assistant zurückübertragen.
4. Google Assistant sendet dann die Antwort an Google Home.
5. Google Home antwortet dann mit gesprochener Ausgabe der Antwort.



### 3.2.3 Architektur und Funktion von Apple Siri

Apple Siri ist ein fester Bestandteil vom iOS-Betriebssystem. Dies bedeutet, steht eine neue iOS-Version zur Verfügung, dann wird auch im Zuge dessen Siri mit aktualisiert. Das iOS-Update erfolgt über eine aktive Internetverbindung automatisch oder manuell, je nach Konfiguration. Für die Nutzung von Apple Siri ist eine Internetverbindung notwendig. Jedoch muss vor der Nutzung von Siri erstmal Siri explizit aktiviert und konfiguriert werden. So ist es zum Beispiel zuerst erforderlich über die App „Einstellungen“ Siri & Suchen → auf „Hey Siri“ achten, aktivieren → oder optional, wenn gewünscht, für Siri Home-Taste drücken, aktivieren.

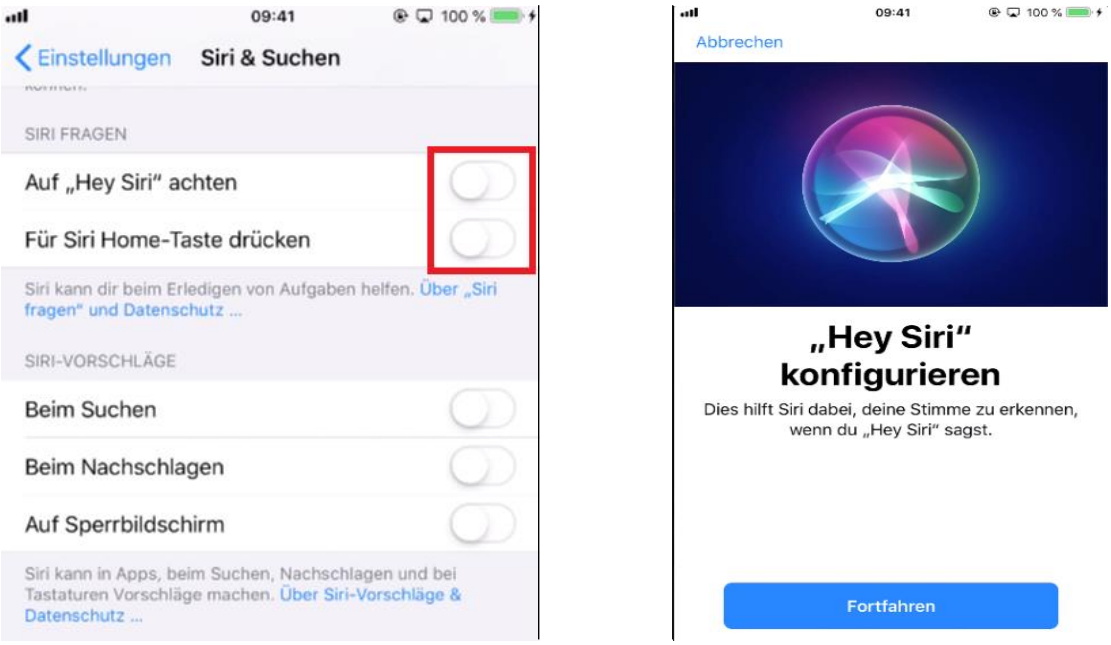



**Bild 14: Aktivierung von Siri & Konfiguration (Eigenes Bild)**

Während der Konfiguration verlangt das iPhone vom Benutzer mehrmals „Hey Siri“ zu sagen, damit die Stimme eindeutig identifiziert wird und Siri nur auf die eigene Stimme reagiert und nicht auf andere. Möchte man Siri deaktivieren, kann man dies über den bereits oben beschriebenen Weg tun, nur eben anstatt Siri zu aktivieren dann entsprechend deaktivieren. Dank integrierter Lagesensoren im iPhone gibt es allerdings auch die Möglichkeit „Hey Siri“ auszuschalten, indem man das iPhone mit dem Display nach unten auf eine flache Oberfläche wie zum Beispiel einen Tisch legt. Erst wenn diese Grundeinstellungen vorgenommen werden ist Siri für den Betrieb bereit.

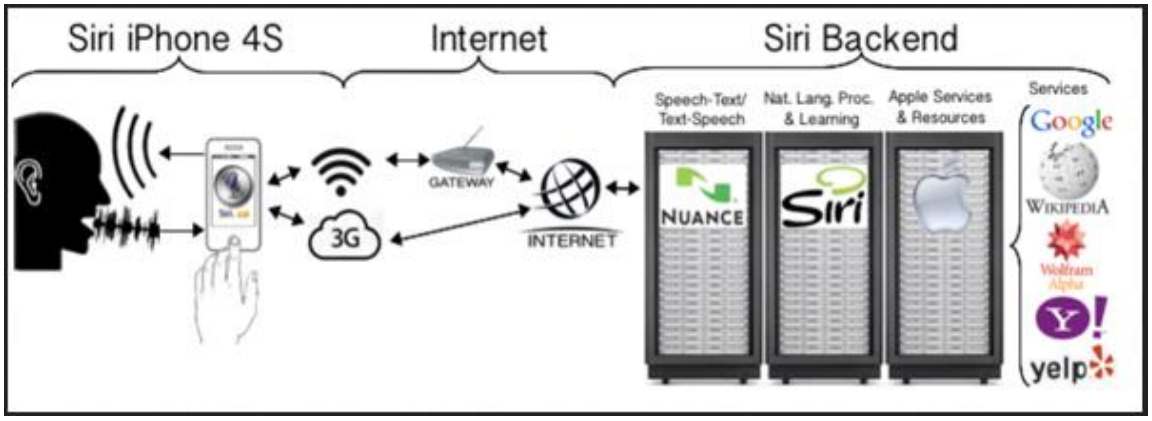



**Bild 15: Architektur von Apple Siri (http://www.howtechnologywork.com/wp-content/uploads/2014/11/How-Siri-Technology-Work1.png)**

Die Funktionsweise von Apple Siri wird nun mit folgenden Schritten erläutert:

1. Die Kommunikation mit Siri erfolgt hauptsächlich über gesprochene Sprache. Das iPhone beinhaltet ein Mikrofon, dass permanent aktiv eingeschaltet ist und eine eingehende Nutzeranfrage, hier Sprachsignal, nach einem Aktivierungswort filtert.

**„Hey Siri“** wie hoch ist die Zugspitze?“

Das Aktivierungswort ist hier „Hey Siri“, nur wenn das Gerät dieses Aktivierungswort wahrnimmt, wird er aktiv und hört zu. Bei Siri gibt es nur ein Aktivierungswort:

- **„Hey Siri“**

Die Definition von andern Aktivierungswörter ist nicht möglich.

2. „Siri zeichnet die Eingabe auf und komprimiert sie.
3. Die komprimierte Audiodatei wird via Internet an die Server von Apple geschickt.

4. Auf den Servern von Apple wird die Anfrage analysiert und das Ergebnis an das iPhone via Internet zurückgeschickt.
5. Im gewählten Beispiel erhält Siri etwa von den Servern die Anweisung, eine Websuche nach „Höhe Zugspitze“ durchzuführen und das Ergebnis anzuzeigen.“ (Damaschke, 2016, S.12)

„Zugspitze liegt 2.962 m über dem Meeresspiegel.“

## 3.3 Zusammenfassung

Alle drei Sprachassistenten setzen für die Funktionsfähigkeit eine ständige WLAN-Internetverbindung voraus. Bis auf den Sprachassistenten Siri im iPhone müssen die beiden anderen Spracherkennungssysteme die ganze Zeit am Strom über ein Netzteil angeschlossen sein. Sicherheitsupdates und Softwareupdates werden bei allen Spracherkennungssystemen über ein Online-Update automatisch eingespielt. Bei allen drei Sprachassistenten ist ein bestimmtes Aktivierungswort notwendig, damit dieser aktiviert werden kann. Alle drei Spracherkennungssysteme setzen ein gültiges Benutzerkonto beim jeweiligen Anbieter voraus. Die Konfiguration der Sprachassistenten erfolgt hauptsächlich über eine mobile App. Dank der Verwendung von Bluetooth und der Möglichkeit der Verbindung mit anderen SmartHome Geräten bei den Sprachassistenten, können andere Geräte eingebunden werden. Für die Verarbeitung und Analyse der gesprochenen Sprache besteht bei allen Sprachassistenten die Notwendigkeit, dies an einen außenstehenden Server, meistens in der Cloud zu senden und dort zu speichern. So können sich die intelligenten Sprachassistenten stets weiterentwickeln und verbessern.

# 4 Sicherheitsrisiken der Spracherkennungssysteme

Im Fokus des vierten Kapitels steht die Sicherheit der hier betrachteten Spracherkennungssysteme. Die einzelnen Spracherkennungssysteme werden miteinander verglichen und hinsichtlich ihrer wichtigsten Sicherheitsrisiken analysiert. Manche Sicherheitsrisiken betreffen alle drei Sprachsysteme gleichermaßen und werden daher zu einem Punkt zusammengefasst, ansonsten erfolgt ein Vergleich der Systeme.

## 4.1 IT-Sicherheit und Schutzziele

Die IT-Sicherheit kann wie folgt definiert werden:

„IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.“ (BSI, 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html?cms_lv2=6658220

Damit Angriffe besser beschrieben werden können verwendet man Schutzziele, die in verschiedene Kriterien eingeteilt sind.

Die drei wichtigsten Schutzziele sind die sogenannten **CIA-Traide**, nimmt man nämlich die englischen Anfangsbuchstaben dieser Schutzziele:

- Vertraulichkeit (**C**onfidendiality)
- Integrität (**I**ntegrity)
- Verfügbarkeit (**A**vailability)

so ergibt sich die Abkürzung **CIA**. Da aber auch das Schutzziel Authentizität (engl. authenticity) immer mehr an Bedeutung gewinnt, kann man die Abkürzung CIA erweitern um das Kriterium CIAA auch genannt **CIAA-Quartett**.

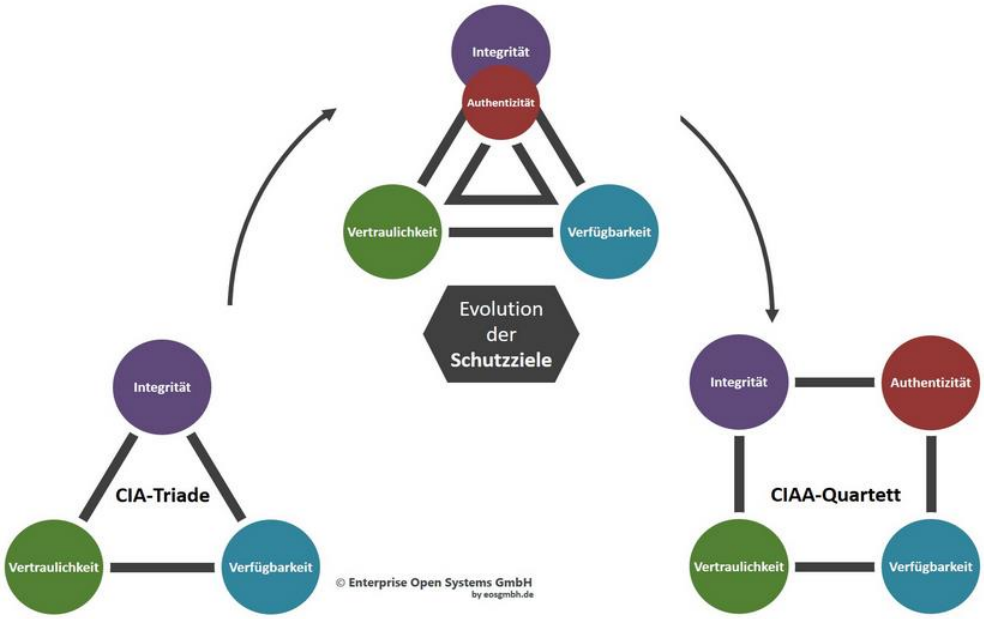



**Bild 16: IT-Schutzziele (https://www.eosgmbh.de/wp-content/uploads/2018/07/Evolution_der_Schutzziele_jpg_2.jpg)**

Die hier verwendeten Schutzziele werden nun wie folgt erläutert:

**Vertraulichkeit:**

„Wir sagen, dass das System die Informationsvertraulichkeit (engl. confidentiality) gewährleistet, wenn es keine unautorisierte Informationsgewinnung ermöglicht. (Eckert, 2014, S. 39)

**Datenintegrität:**

„Wir sagen, dass das System die Datenintegrität (engl. integrity) gewährleistet, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.“ (Eckert, 2014, S. 37)

**Verfügbarkeit:**

„Wir sagen, dass das System die Verfügbarkeit (engl. availability) gewährleistet, wenn authentifizierte und autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisierte beeinträchtigt werden können.“ (Eckert, 2014, S.42)

**Authentizität:**

„Unter der Authentizität eines Objektes bzw. Subjektes (engl. authenticity) verstehen wir die Echtheit und Glaubwürdigkeit des Objektes bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist.“ (Eckert, 2014, S. 36)

**Verbindlichkeit:**

„Wir sagen, dass das System die Verbindlichkeit bzw. Zuordenbarkeit (engl. repudiation) einer Menge von Aktionen gewährleistet, wenn es nicht möglich ist, dass ein Subjekt im Nachhinein die Durchführung einer solchen Aktion abstreiten kann.“ (Eckert, 2014, S.43)

## 4.2 Schwachstellen, Bedrohungen, Angriffe, Risiko

Ein Endgerät wie zum Beispiel die Spracherkennungssysteme, können unterschiedliche Schwachstellen besitzen. Diese Schwachstellen können von Angreifern ausgenutzt werden und stellen somit eine Bedrohung für das Gerät dar. Deshalb gibt es bei Spracherkennungssystemen verschiedene Sicherheitsrisiken.

**Bild 17: Zusammenhang zwischen Schwachstellen, Bedrohungen und Risiken (Eckert, 2014, S. 54)**

Folgende Begriffsdefinitionen werden verwendet, die an dieser Stelle beschrieben werden:

**Schwachstelle: (engl. vulnerability)**

„Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der

Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.“ (BSI, 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html?nn=6597936&cms_lv2=6658240)

**Bedrohungen: (engl. threat)**

„Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung, ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.“ (BSI, 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html?nn=657936&cms_lv2=6658206)

**Angriff:**

„Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.“ (BSI, 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html?nn=657936&cms_lv2=6658204)

**Risiko:**

„Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen

ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.“ (BSI, 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html?nn=6597936&cms_lv2=6658238)

## 4.3 Sicherheitsproblem Stimmenerkennung

Das Aktivierungswort wird genutzt um den Sprachassistenten zu aktivieren. Dabei reagieren die Sprachassistenten nicht auf jeden x-beliebigen Befehl, sondern müssen durch ein sogenanntes „Wake-Word“ oder „Aufwachwort“ durch ein bestimmtes Schlüsselwort aktiviert werden. Je nach Spracherkennungssystem gibt es vordefinierte Schlüsselwörter die genutzt werden können.

Eine Schwachstelle ist hier die Stimmenerkennung, da das Aktivierungswort nicht nur einer bestimmten Person zugeordnet werden kann. Dies bedeutet, dass jede Person die sich im Raum oder in der Nähe befindet, den Sprachassistenten mithilfe des Schlüsselwortes aktivieren und für weitere Aktionen missbrauchen könnte. Somit ist hier eine eindeutige Authentizität nicht gewährleistet. Hier kann nicht sichergestellt werden, dass der Kommunikationspartner auch der ist, für den man ihn hält. Es findet hier also keine Personenidentifikation statt.

### 4.3.1 Amazon Echo (1. Generation) mit Alexa

Es gibt vier verschiedene Schlüsselwörter zur Auswahl:

- „Alexa“
- „Amazon“
- „Echo“
- „Computer“

Die Definition anderer Schlüsselwörter ist nicht möglich, zudem sind diese Schlüsselwörter nicht einer einzigen Personen eindeutig zugewiesen. So ist es für den Angreifer sehr einfach das Schlüsselwort zu ermitteln, da es nur vier Möglichkeiten gibt. Ist das Schlüsselwort dem Angreifer bekannt, könnte er quasi unabhängig von der eigenen Stimme auf sensible Daten wie Kontakte, Kalender zugreifen oder sogar Einkäufe tätigen. Folgende reale Szenarien zeigen was alles möglich ist:

**Sicherheitsvorfall:**

„Die Sprachsteuerung kann etwa durch ein offenes Fenster oder eine hellhörige Tür auch von Unbefugten genutzt werden“, berichtet Michael Veit. Er verweist zudem auf Fälle, bei denen Alexa durch die geschlossene Wohnungstür hindurch das Kommando zum Öffnen eben dieser Tür annahm und das Smart-Home-Türschloss daraufhin den Einbrechern den Zugang gewährte.“ (Schlücker, 2017, https://www.it-zoom.de/mobile-business/e/grosser-lauschangriff-im-wohnzimmer-16881/)

**Sicherheitsvorfall:**

„Der Nachrichtensprecher Jim Patton hat in der US-News-Sendung CW6 in San Diego eine Serie von Bestellungen bei Amazon ausgelöst. Dabei wollte er eigentlich nur über das kleine Mädchen berichten, das mit der Sprachassistentin Alexa in Amazons intelligentem Lautsprecher Echo kommunizierte und dabei versehentlich die Bestellung eines Puppenhauses und kiloweise Keksen auslöste.“ (Kaltschmidt, 2017, https://www.heise.de/newsticker/meldung/Amazon-Echo-Nachrichtensprecher-loest-Massenbestellung-aus-3591039.html)

Allerdings gab es von Amazon im Dezember 2018 ein Update für die Alexa-App mit der neuen Funktion ab sofort, Stimmen von bestimmten Personen erkennen zu können. Die neue Funktion nennt sich „Stimmprofil“. Diese neue Option muss aber explizit vom Anwender in der Alexa-App aktiviert werden. In der Alexa-App ist es nun möglich über die Einstellungen → Alexa Konto → Registrierte Stimmen zu aktivieren. Anschließend wird man aufgefordert zehn Sätze nachzusprechen. Danach kann man über den Sprachbefehl „Alexa, wer bin ich?“ prüfen ob Alexa das richtige Stimmprofil erkennt und den Namen sagt. Soweit die Theorie, in der Praxis zeigt sich die neue Funktion als noch nicht

ausgereift und ist noch nicht zuverlässig. So kann Alexa nicht immer eindeutig das Stimmprofil einer Person zuweisen. Die neue Funktion funktioniert nur von einer kurzen Distanz, noch immer ist es anderen Personen möglich durch das Verwenden der Schlüsselwörter Alexa zu aktivieren. Daher bleibt weiterhin das Aktivierungswort und das Nichtvorhandensein einer eindeutigen Stimmerkennung ein Sicherheitsrisiko.

### 4.3.2 Google Home mit Google Assistant

Im Gegensatz zu Amazon Echo, gibt es bei Google Home nur zwei mögliche Schlüsselwörter zur Auswahl:

- „OK Google“
- „Hey Google“

Andere Definitionen der Schlüsselwörter sind auch hier nicht möglich. Auch diese Signalwörter sind in den Grundeinstellungen keiner eindeutigen Person, also Stimme, zugeordnet. Dies bedeutet, kennt auch hier der Angreifer die Schlüsselwörter, es gibt hier nur zwei Möglichkeiten, kann der Angreifer mit seiner Stimme Befehle an den Sprachassistenten ausführen. So wäre ein Zugriff auf sensible Daten wie Termine, Kalender möglich.

Anbei ein Beispiel, wie der Sprachassistent durch eine fremde Stimme fremd gesteuert werden kann:

**Sicherheitsvorfall:**

„Mit einer überraschenden Aktion hat die Fastfoodkette Burger King Fernsehzuschauer und Google überrumpelt. In einem 15-sekündigen Werbespot, der am Mittwochabend auf verschiedenen Sendern in den USA ausgestrahlt wurde, wendet sich ein Schauspieler an Googles Sprachassistenten: "OK Google, was ist der Whopper Burger?" Geräte wie der vernetzte Lautsprecher Google Home antworteten auf die Frage mit einer aus der Wikipedia entnommenen Definition, die insbesondere die verschiedenen Zutaten des Burgers werblich hervorhob.“ (Kleinz, 2017, https://www.heise.de/newsticker/meldung/Werbespot-Burger-King-kapert-Google-Home-3685167.html)

Ähnlich wie bei der Alexa-App, bietet Google seit dem 03. Oktober 2017 eine neuere Google-Home App mit der Versionsnummer 1.25.81.13 an. Mit der erweiterten Funktion Voice-Match, die nun dem Google Assistant ermöglicht, die Stimme einer bestimmten

Person zu erkennen. Auch diese Funktion muss zuerst manuell aktiviert werden. Voice-Match kann über die Google-Home App über Zuhause → Tippen auf den Lautsprecher → Geräteeinstellungen →Voice-Match hinzufügen aktiviert werden. Erkennt Google ihre Stimme erhalten Sie von ihrem Sprachassistent persönliche Ergebnisse. Sollte Google ihre Stimme nicht erkennen, wird der Sprachbefehl wie eine Gastanfrage behandelt und man erhält keine persönlichen Ergebnisse. Jedoch gibt es auch hier keinen einhundert prozentigen Schutz. So ist es möglich Menschen mit ähnlicher Stimme oder mithilfe einer Stimmaufzeichnung, das Gerät auszutricksen und auf Informationen zuzugreifen.

### 4.3.3 iPhone 6s Plus mit Siri

Siri bietet als einziger Sprachassistent nur ein Signalwort zur Auswahl an:

- „Hey Siri“

Auch dieses Schlüsselwort kann nicht geändert werden. Im Vergleich zu den anderen beiden Sprachassistenten kann Siri nur eingerichtet werden, wenn man sein Stimmenprofil konfiguriert. Dies bedeutet, hier wird es für einen Angreifer schwierig Zugriff auf das System zu bekommen. Das Signalwort kann nur in Verbindung mit der Stimmenerkennung benutzt werden. „Die Stimme gehört zu den biometrischen Parametern eines Menschen, das heißt, genau so wie die Fingerabdrücke oder die DNA ist sie einzigartig bei jedem einzelnen Menschen und kann nicht verwechselt werden.“ (Kubiv, 2015, https://www.macwelt.de/tipps/Voice-ID-Siri-9831918.html) Befinden sich mehrere Personen in einem Raum kann Siri nur von der Person aktiviert werden bei der zuvor das Stimmprofil hinterlegt wurde. Zudem hat man auf die Einstellungen des Sprachassistenten nur Zugriff, wenn das Smartphone entsperrt ist. Allerdings arbeitet Siri nicht immer zuverlässig und auch hier kann es vorkommen, dass durch eine ähnlich klingende Stimme oder eine Sprachaufzeichnung Siri unabsichtlich aktiviert werden kann.

### 4.3.4 Angriff im nicht hörbaren Bereich („DolphinAttack“)

„Unter Laborbedingungen ist es sechs Forschern der Zhejiang Universität gelungen, mehrere Sprachassistenz-Systeme – darunter Siri, Alexa und den Google Assistant – mit Sprachkommandos im nicht-hörbaren Bereich zu aktivieren.“ (Nicolas, 2017, https://www.iphone-ticker.de/lautlos-aktiviert-siri-angriff-im-nicht-hoerbaren-bereich-116331/) Dieser Angriff ist auch bekannt als Delfin-Angriff (engl. „DolphinAttack“). Bei diesem Experiment wurden Standard-Sprachbefehle digital mit speziellen Frequenz-Effekten auf oberhalb von 20.000Hz geändert. Der Grund ist hier, Menschen hören Töne nur zwischen 20Hz und 20.000Hz. Das nachfolgende Bild zeigt den Hörbereich der von einem menschlichen Gehör wahrgenommen werden kann.

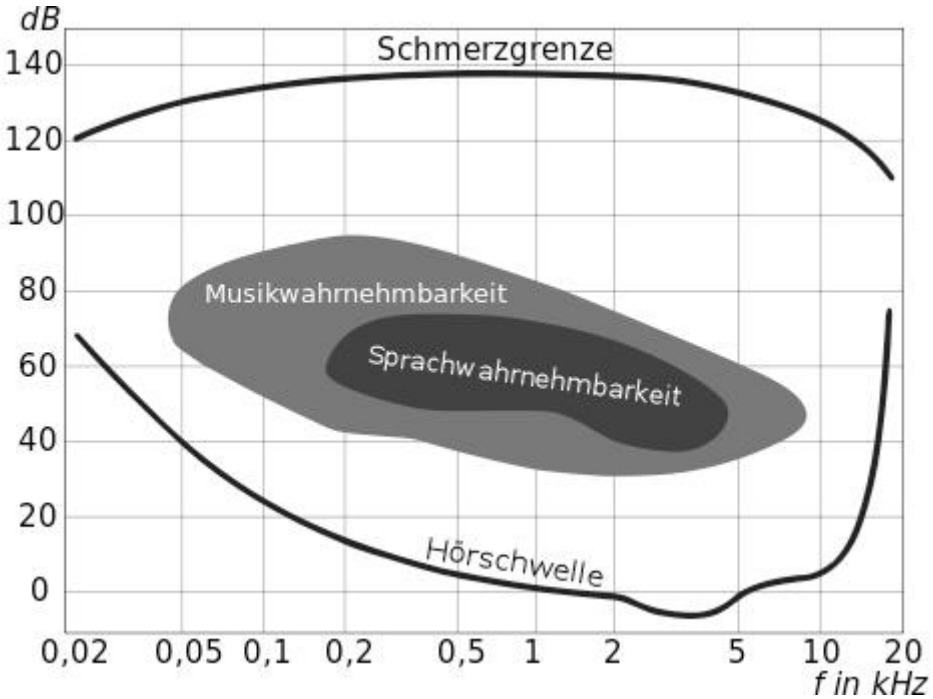



**Bild 18: Hörflächen-Schaubild (https://images.iphone-ticker.de/wp-content/uploads/2017/09/hoer-flaeche.jpg)**

Der Angriff war von einer Distanz zwischen einem Meter bis zu sieben Meter möglich. Jedoch sind die eingebauten Mikrofone der einzelnen Spracherkennungssysteme auch auf Frequenzen ausgelegt, die nicht mehr für den Menschen hörbar sind. Daher war es den Forschern möglich per Ultraschall die Sprachassistenten zu aktivieren, auch wenn es für den Menschen nicht hörbar war. Dieses Experiment verdeutlicht, dass auch für den Menschen nicht hörbare Stimmen ein Sicherheitsrisiko für die Sprachassistenten

darstellen können. Zudem, was noch viel gefährlicher ist, dass diese Angriffe infolgedessen unbemerkt bleiben und erst wahrgenommen werden, wenn es meistens zu spät ist.

### 4.3.5 Ähnlich klingende Begriffe

Die Spracherkennungssysteme Alexa und Google Assistant konnten bereits schon durch ähnlich klingende Begriffe wie das Signalwort unbewusst aktiviert werden. So kann es vorkommen, dass ähnlich klingende Wörter wie das Aktivierungswort den Sprachassistenten ungewollt aktivieren. Hier wird verdeutlicht wie wichtig es ist deutlich zu sprechen. Oder es kann auch vorkommen, dass man im Alltag zu Hause einen Satz spricht indem am Anfang, in der Mitte oder am Ende zufällig ein Begriff vorkommt, der eine Ähnlichkeit mit dem Schlüsselwort hat. So könnte auch eine Aktion aus Versehen ausgelöst werden. Nachfolgend sind ähnlich klingende Begriffe aufgelistet, mit denen es passieren kann, dass der Sprachassistent glaubt, das richtige Aufwachwort zu hören:

**Beispiele für den Google Assistant:**

- „OK Kuchen“ (für „OK Google“)
- „OK Muggel“ (für „OK Google“)
- „OK Kookle“ (für „OK Google“)
- „OK Nudel“ (für „OK Google“)
- „OK Gockel“ (für „OK Google“)

**Beispiele für Alexa:**

- „Alexandra“ (für Alexa)
- „Gecko“ (für Echo)
- „Ham wa schon“ (für Alexa)
- „Alexis“ (für Alexa)
- „Alexander“ (für Alexa)

Etwas wählerischer ist da der Sprachassistent von Apple Siri. Siri kann in Einzelfällen auch plötzlich aktiviert werden, wenn es ein ähnlich klingendes Sprachkommando wie „Hey Siri“ hört. Trotzdem ist Siri aber bei weitem nicht so anfällig wie die anderen beiden Sprachassistenten. Daher gibt es hier wenig gefundene Beispiele für

ähnlich klingende Wörter. Bei Siri äußert es sich dann eher so, dass Siri plötzlich aktiviert wird und antwortet „Ich bin mir nicht sicher, ob ich das richtig verstanden habe“.

### 4.3.6 Sicherheitsempfehlungen

Folgende Sicherheitsempfehlungen sollten hier eingehalten werden:

- Die Sprachassistenten sollten nicht in der Nähe von einem Fernsehgerät, Radio, Wohnungstür oder einem Anrufbeantworter aufgestellt werden. Damit die Sprachassistenten nicht durch eine fremde Stimme zufällig aktiviert werden können.
- Beim Verlassen der Wohnung sollten die Fenster geschlossen werden, damit niemand durch das offene oder gekippte Fenster Sprachbefehle ausführen kann.
- Die Erkennung eines Stimmenprofils sollte explizit aktiviert werden.
- Sprachassistenten sollten unhörbare Frequenzen siehe „DolphinAttack“, wenn möglich, zukünftig ignorieren.
- Wird der Sprachassistent gerade nicht benutzt, dann sollten die Mikrofone über die Mikrofon Stummtaste ausgeschaltet oder das Gerät über den Netzwerkstecker ganz ausgeschaltet werden.

### 4.3.7 Zusammenfassung und Fazit

Bei allen drei Spracherkennungssystemen gibt es noch Verbesserungsbedarf bei der Stimmenerkennung. Bei Amazon Echo als auch Google Home ist das Einrichten eines Stimmenprofils nicht Pflicht und von daher hat im Prinzip jede Person Zugriff auf den Sprachassistenten. Siri ist hier schon weiter und verlangt das Hinterlegen eines Stimmenprofils als Pflichtkonfiguration. Zudem bieten alle drei Spracherkennungssysteme keinen Schutz gegen das Erkennen von aufgezeichneter Sprache und sind anfällig auf ähnlich klingende Stimmen sowie ähnlich klingende Signalwörter.

## 4.4 Sicherheitsproblem WLAN (Wireless Local Area Network)

Die Bezeichnung WLAN steht für „Wireless Local Area Network. „Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.“ (BSI, 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html?nn=6597936&cms_lv2=6658248)

Alle drei Sprachassistenten Amazon Alexa, Google Assistant und Apple Siri sind nur funktionsfähig, wenn Sie mit einem WLAN-Netzwerk verbunden sind. Ohne eine WLAN-Netzwerkverbindung sind die Sprachassistenten ausgeschaltet und quasi für den Gebrauch nutzlos. Daher ist die Kommunikation über das WLAN für die Spracherkennungssysteme ein unausweichlicher fester Bestandteil. Die drahtlose Kommunikation verbirgt allerdings neben der großen Freiheit und Mobilität auch Gefahren, die von einem Angreifer ausgenutzt werden können.

Folgende Schutzziele können bei einem Angriff auf das WLAN verletzt werden:

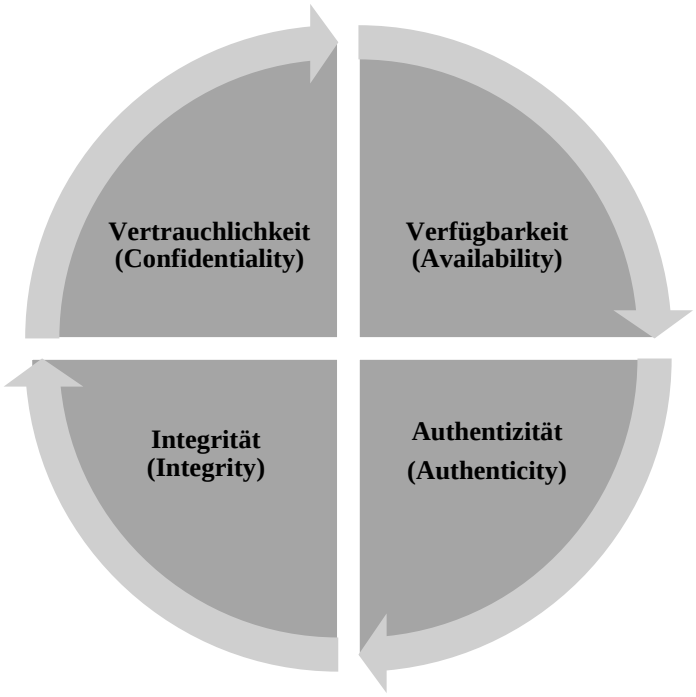



**Bild 19: IT-Schutzziele WLAN (Eigene Darstellung)**

Die im Bild 19 aufgeführten Schutzziele können beim WLAN wie folgt verletzt werden:

- „Eindringen und Übernehmen (sog. Hacking“)
- Täuschen, Fälschen und Betrügen (Angriffe auf die Integrität und Authentizität)
- Ausspähen und Entwenden (Angriffe auf die Vertraulichkeit)
- Verhindern und Zerstören (Angriffe auf die Verfügbarkeit)“ (BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_wlan_leitlinie.pdf?__blob=publicationFile&v=1, S. 10)

### 4.4.1 WLAN Angriffsmöglichkeiten

Anbei werden die wichtigsten Angriffe auf ein drahtloses Netzwerk aufgelistet:

- Angriff durch Fehlkonfiguration Router
- Angriff auf die Verschlüsselung WPA und WPA2
- Abhören
- Man-in-the-Middle
- Denial of Service

Somit sind alle drei Sprachassistenten von den Sicherheitslücken des WLAN betroffen.

### 4.4.2 WLAN-Standards nach IEEE

Damit sich ein Sprachassistent mit dem WLAN-Netzwerk verbinden kann, sendet es auf einem bestimmten WLAN-Standard. Dies ist entweder 802.11 a, b, g, n oder ac. Bei der 802 steht die Zahl **(2)** für den Monat Februar und die Zahl **(80)** für das Jahr 1980, in dem Jahr veröffentlichte das Institute of Electrical and Electronics Engineers (IEEE) den WLAN-Standard. Die **.11** ist eine Norm für das WLAN-Netzwerk. Die Buchstaben a, b, g, n und ac beschreiben die Geschwindigkeit und die Frequenz. Die hier untersuchten Spracherkennungssysteme verwenden folgende WLAN-Standards:

- Der Amazon Echo (1. Generation) verwendet den WLAN-Standard IEEE 802.11a/b/g/n.
- Der Google Home verwendet den WLAN-Standard IEEE 802.11b/g/n/ac.
- Apple Siri verwendet den WLAN-Standard IEEE 802.11a/b/g/n/ac

**Tabelle 4:WLAN-Standards IEEE (vgl. https://www.wlansignalverstaerken.de/wlan-standards)**

| Spezifikation | 802.11 | 802.11b | 802.11g | 802.11n | 802.11ac |
|---|---|---|---|---|---|
| **Veröffentlichung** | 1997 | 1999 | 2003 | 2009 | 2013 |
| **max. Datenrate** | 2 Mbit | 11 Mbit | 54 Mbit | 600 Mbit | 6939 Mbit |
| **Frequenzband** | 2,4 Ghz | 2,4 Ghz | 2,4 Ghz | 2,4 bis 5 Ghz | 5 Ghz |
| **Reichweite** | 20 Meter | 38 Meter | 38 Meter | 70 Meter | 50 Meter |
| **Kompatibel** | Ja | Ja | Ja | Ja | Nur mit 802.11 n |

Der WLAN-Standard IEEE 802.11a wird hier in der oberen Tabelle nicht aufgelistet, da dieser Standard nur in den USA relevant war und nicht in Europa. Der Standard IEEE 802.11ac gilt derzeit als modernster und am meisten verwendete Standard.

### 4.4.3 Sicherheitsproblem Fehlkonfiguration

Damit sich die Sprachassistenten und die mobile App der Assistenten mit dem drahtlosen Netzwerk verbinden können, wird ein WLAN-Router benötigt. Über den Router kann eine Funkverbindung zu den digitalen Assistenten aufgebaut werden. Allerdings kann eine Fehlkonfiguration des Routers zu einem Sicherheitsrisiko führen.

**Admin-Passwort**

So werden die Router vom Hersteller mit einem **Standardpasswort** auch genannt Admin-Passwort ausgeliefert. Dieses Passwort ist bei allen Routern des gleichen Herstellers identisch und in den Werkseinstellungen hinterlegt und ist daher für die Angreifer ein beliebtes Angriffsziel. Meistens ist dieses Passwort einfach definiert wie zum Beispiel „Passwort“. Daher ist es dringend notwendig das voreingestellte Passwort durch ein sicheres Passwort, dass die Sicherheitsstandards erfüllt zu ändern.

**Fernkonfiguration**

Eine weitere Schwachstelle, ist die Option „**Fernkonfiguration**“. Diese Option sollte deaktiviert werden, da ansonsten ein Zugriff einer dritten Person auf das Gerät möglich ist.

**SSID: Service Set Identifier**

Zudem sollte der **SSID** (Service Set Identifier) in der Konfiguration geändert werden. Der SSID kann auch als WLAN-Name des Routers bezeichnet werden und dient als eindeutige WLAN-Identifikation. Sucht ein Sprachassistent nach einer verfügbaren WLAN-Verbindung in der Nähe, so werden dem Gerät die SSID-Namen angezeigt. Es gibt auch die Möglichkeit über eine Option den SSID-Namen zu verbergen. Hier ist es wichtig den SSID-Namen so zu ändern, dass keine Rückschlüsse für den Angreifer auf die verwendete Hardware getroffen werden kann. Oft ist als SSID-Name die Gerätebezeichnung des Routers standardmäßig hinterlegt wie zum Beispiel: „ FritzBox-7490“. Dank dieser Bezeichnung könnte dann der Angreifer gezielt Schwachstellen dieses Gerätetyps suchen.

**WLAN-Passwort**

Anschließend sollte das **WLAN-Passwort** entsprechend der Sicherheitsrichtlinien angepasst werden. Leider wird auch dieser Schlüssel am Router oft durch ein Etikett oder

Schild, meistens an der Unterseite des Gerätes, vom Hersteller hinterlegt. Damit ist das Passwort für jeden sichtbar und stellt ein Risiko dar.

**WPS: Wi-Fi Protected Setup**

Die Abkürzung WPS steht für Wi-Fi Protected Setup. Mit WPS besteht die Möglichkeit per Knopfdruck oder durch die Eingabe einer PIN, sich mit anderen Geräten ohne die Eingabe der Zugangsdaten schnell zu verbinden. Eine Schwachstelle ist hier der PIN. Der PIN besteht aus acht Zeichen und kann von einem Angreifer leicht entschlüsselt werden. Zudem wird der PIN häufig nicht zufällig erstellt, sondern leitet sich von der eigenen MAC-Adresse ab. „Die MAC-Adresse (Media Access Control) stellt die physikalische Adresse einer Netzwerkschnittstelle dar. Sie ist eindeutig und besitzt eine Länge von 48 Bit. MAC-Adressen kommen beispielsweise im Ethernet und Token Ring aber auch bei Bluetooth und WLAN zum Einsatz. Bestandteil jeder Adresse ist eine Herstellerkennung.“ (Luber, 2018, https://www.ip-insider.de/was-ist-eine-mac-adresse-a-665074/) Ist dem Angreifer die MAC-Adresse bekannt, dann kann er auch den PIN davon ableiten. Aufgrund dieses Sicherheitsrisikos wird empfohlen diese Option zu deaktivieren.

**Verschlüsselung WPA und WPA2**

Des Weiteren sollte bei der Konfiguration darauf geachtet werden eine sichere **Verschlüsselung** zu wählen. Hier besteht die Auswahl zwischen den Verschlüsselungsverfahren **WPA** (Wi-Fi Protected Access) oder **WPA2** (Wi-Fi Protected Access 2). Hier sollte das sichere WPA2 Verfahren gegenüber dem WPA Verfahren bevorzugt werden. Die Verschlüsselungsart muss manuell aktiviert werden, da diese Option oft in der Standardkonfiguration deaktiviert ist. Dies wird häufig vergessen. Nähere Informationen zur Verschlüsselung WPA und WPA 2 werden in einem weiteren Unterpunkt näher erläutert.

**Updates und Patches**

Zuletzt sollte darauf geachtet werden ob für die Software des Routers gewisse **Updates** oder **Patches** vorliegen. Werden hier nicht regelmäßige Updates durchgeführt, besteht die Gefahr nicht genügend vor Schwachstellen oder Angriffe geschützt zu sein.

### 4.4.4 Sicherheitsproblem WPA / WPA2

Eines der wichtigsten Schritte beim Konfigurieren des Routers ist die Auswahl der Verschlüsselungsart. Denn die Verschlüsselungsart ist entscheidend ob ein definiertes Passwort am Ende ein hohes Sicherheitsniveau hat oder ein niedriges. Jedoch gibt es auch hier, je nach Auswahl der Verschlüsselung gewisse Sicherheitslücken bei den einzelnen Verfahren, die zu beachten sind.

**WPA: Wi-Fi Protected Access**

„WPA steht für Wi-Fi Protected Access und bezeichnet den 2003 verabschiedeten Nachfolgestandard von WEP zur Verschlüsselung und Authentifizierung im WLAN. WPA sollte die bekannt gewordenen Sicherheitslücken und Schwachstellen von WEP beseitigen und wieder für Sicherheit in Funknetzwerken sorgen.“ (Luber, 2018, https://www.security-insider.de/was-ist-wpa-a-742206/) WPA wurde von Anfang an nur als Zwischenlösung angesehen.

**Funktionsweise WPA:**

WPA verwendet ein TKIP Verfahren. „TKIP (Temporal Key Integrity Protocol) wurde nachträglich für den Standard 802.11i definiert. Es kam allerdings vorher bereits für WPA zum Einsatz. Statt eines stationären Schlüssels wird mit einem temporären gearbeitet. Die RC4-Prozedur wurde allerdings beibehalten, um Kompatibilität zu erreichen. Insofern ist TKIP eine Verbesserung von WEP mit

- einem erweiterten Initialisierungsvektor
- einer dynamischen Schlüsselgenerierung
- dem kryptografischen Message Integrity Check (MIC).“ (Osterhage, 2018, S. 42)

Zudem verwendet WPA für die Authentifizierung einen Pre-shared Key (PSK). Auch bekannt unter der Bezeichnung WPA-PSK. Mit einem PSK Schlüssel ist es möglich Daten zu verschlüsseln und entschlüsseln. Alle Personen die im Besitz eines PSK Schlüssels sind können Daten verschlüsseln und entschlüsseln. Der PSK-Schlüssel wird in der Regel zwischen den Teilnehmern vor einer verschlüsselten Kommunikation ausgetauscht. Man spricht hier auch von symmetrischer Verschlüsselung. Der PSK kann hier als WLAN-Passwort verwendet werden.

Für den Integritätsschutz wird der Michael-Hash verwendet. „Bei dem Michael-Hash handelt es sich um einen extra für WLANs entwickelten Hash-Algorithmus, der einen vertretbaren Overhead mit sich bringt. Er wird abgeleitet vom Pairwise Transient Key (PTK) oder vom Group Transient Key (GTK). Der Hashwert, in den der Michael-Schlüssel eingeht, kann ohne Kenntnis des Michael-Schlüssels nicht berechnet werden und Modifikationen an Datenpaketen werden somit erkannt.“ (ITWissen., 2019, https://www.it-wissen.info/Michael-Hash-Michael-hash.html)

**Schwachstellen WPA**

- Bei WPA ist ein Brute Force oder Wörterbuchangriff (engl. dictionary attack) möglich. Diese Angriffe haben das Ziel Passwörter zu knacken. Bei einem Brute Force Angriff werden viele verschiedene Buchstaben und Zeichenkombinationen ausprobiert, während bei einem Wörterbuchangriff jedes Wort mit einer Wörterliste durchgeführt wird. Dies gelingt häufig nur bei zu schwachen Passwörtern, also die zu kurz, zu einfach oder zu wenig verschiedene Buchstaben enthalten.

**WPA2: Wi-Fi Protected Access 2**

„Bei WPA2 handelt es sich um einen Sicherheitsstandard für drahtlose Funknetzwerke, der auf der Advanced-Encryption-Standard-Technologie (AES) basiert. Er kommt für die IEEE 802.11a, b, g, n und ac WLAN-Standards zum Einsatz und sorgt für die Verschlüsselung der Daten und die Verhinderung des unbefugten Zugriffs. WPA2 ist der Nachfolger von WPA und hat die zu Beginn in WLAN-Netzen genutzte WEP-Verschlüsselung, die heute als unsicher und angreifbar eingestuft wird, abgelöst.“ (NFON, 2019, https://www.nfon.com/at/service/knowledge-base/knowledgebase-detail/wpa2/)

**Funktionsweise WPA2:**

Im Gegensatz zu WEP und WPA die das Stromchiffreverfahren RC4 verwenden, wird bei WPA2 die Verschlüsselungsmethode AES (Advanced Encryption Standard) benutzt. AES ist ein symmetrisches Verschlüsselungsverfahren, dass ein 8 bis 63 Zeichen langes Passwort für die Ermittlung eines 128 Bit langen einzigartigen Schlüssels benutzt. Der Schlüssel wird zwischen Client und Access Point (AP) ausgehandelt. Die Berechnung des Schlüssels erfolgt mithilfe eines 48 Bit langen Initialisierungsvektor (IV). Damit es nicht

zu Wiederholungen des Schlüssels kommt, wird zwischen dem Access Point (AP) und dem Client nach gewissen Zeitabständen ein neuer Schlüssel generiert. Zudem wird bei WPA 2 anstatt dem TKIP-Protokoll (Temporal Key Integrity Protocol) das CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) angewandt. Die Authentifizierung erfolgt wie bei WPA über einen Pre-shared Key (PSK).

**Schwachstellen WPA2:**

- Wie bei WPA sind bei schwachen Passwörtern Brute Force Angriffe oder Wörterbuchangriffe möglich.
- Allerdings wurde durch einen Hackerangriff, im Jahre 2017 von Mathy Vanhoef eine neue Schwachstelle von WPA2 bekannt. Dieser Angriff wird bezeichnet als **„KRACK“**. Krack steht hier für Key Reinstallation Attack. „Der Angriff erfolgt über den Handshake, mit dem Client und Access Point beim Verbindungsaufbau durch den Client den Schlüssel austauschen. Durch eine Manipulation und erneutes Einspielen von Handshake-Nachrichten ist es möglich, den Client zur erneuten Installation eines bereits verwendeten Schlüssels zu bringen. Eigentlich sollte ein Schlüssel nur einmal installiert und verwendet werden, das wird vom WPA2-Protokoll aber nicht garantiert. Bei der Re-Installation werden zugehörige Werte wie z.B. der Nonce und der Replay Counter auf ihre Ausgangswerte zurückgesetzt.
  Die erneute Verwendung des Nonce-Werts erlaubt Angriffe auf die Verschlüsselung, sodass Pakete erneut gesendet („Replay“), entschlüsselt und/oder gefälscht werden können“ (Eilers, 2017, https://entwickler.de/online/security/krack-ueberblick-579816756.html)

### 4.4.5 Sicherheitsproblem Abhören

Da die Spracherkennungssysteme und die hierfür benötigten mobilen Apps auf den Smartphones und Tablets sich mit dem WLAN für die Datenübertragung und Kommunikation verbinden müssen und quasi über Funkwellen miteinander verbunden sind, gibt es hier Schwachstellen, die die Angreifer bei der Funkübertragung ausnutzen können. Da das WLAN übertragene Daten über Funk sendet, ist es möglich, dass diese Daten mitgehört oder aufgezeichnet werden. So können die Funkwellen die eigenen Räumlichkeiten

ohne Probleme überschreiten und sind somit auch über weite Entfernungen abgreifbar. Der Angreifer muss also nicht in unmittelbarer Nähe sein, sondern kann auch von einem anderen Ort außerhalb das System angreifen und abhören. Dabei kann der Angreifer von der mobilen App des Smartphones zum Beispiel übertragene Daten mitlesen oder überwachen, welche Webseiten aufgerufen wurden. Um Daten abhören zu können benötigt man einen Punkt im Netzwerk, der die Daten mitschneiden kann. Hier bietet sich der Router an. Viele Router bieten eine Funktion an, den Netzwerkverkehr mitzuschneiden. Anschließend ist es möglich über die kostenlose Software „Wireshark“ den Datenmitschnitt auszuwerten.

### 4.4.6 Sicherheitsproblem Man-in-the-Middle-Angriff

„Bei diesem Angriff täuscht ein böswilliger Dritter "in der Leitung" zwei Kommunikationspartner, indem er ihnen jeweils die Identität des anderen vorspiegelt. Typischerweise geschieht das, um eine an sich sichere Verschlüsselung auszuhebeln. Beide Kommunikationspartner verschlüsseln zwar ihre Daten, aber so, dass sie der in der Mitte sitzende Angreifer entschlüsseln und wie ein Proxy an den anderen weiterleiten kann. Voraussetzung dafür ist, dass er eine Verbindungsanfrage auf sich umleiten kann und die Kommunikationspartner die Identität des Gegenübers nicht überprüfen.“ (Heise, 2019, https://www.heise.de/glossar/entry/Man-in-the-Middle-Angriff-399039.html)

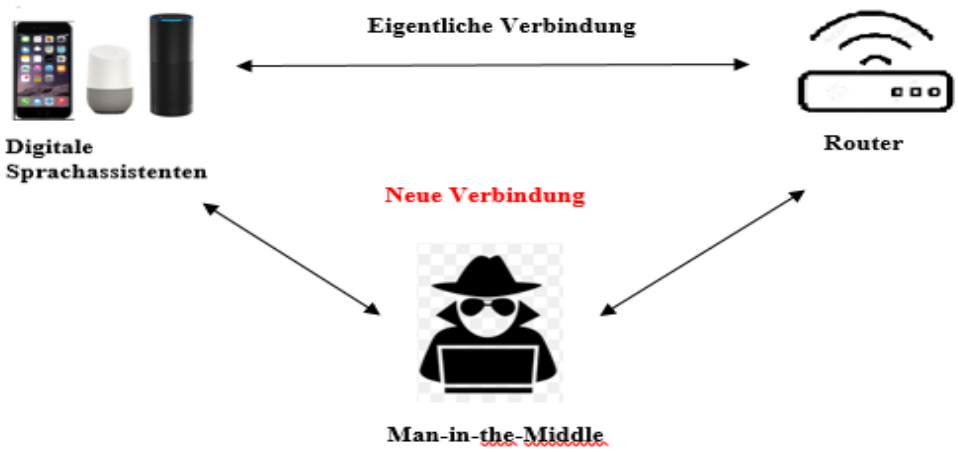



**Bild 20: Man-in-the-Middle-Angriff (Eigene Darstellung)**

Meistens verbinden sich die WLAN-Endgeräte mit dem stärksten Signal und stellen eine Verbindung zu dem Access Point (AP) her. Daher ist es für den Angreifer leicht einen gefälschten Access Point (AP) zu integrieren. Verbinden sich nun die WLAN-Endgeräte mit dem vorgetäuschten Access Point (AP) so hat der Angreifer vollen Zugriff auf die Kommunikation und es ist ihm möglich, Daten abzuhören, zu manipulieren oder einzuschleusen.

### 4.4.7 Sicherheitsproblem Denial-of-Service (DOS)

"Denial of Service – oder kurz DoS – bedeutet so viel wie etwas unzugänglich machen oder **außer Betrieb setzen**. Technisch passiert dabei folgendes: Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht." (BSI, 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/DoS/dos_node.html) Bei den Spracherkennungssystemen könnte ein DOS-Angriff auf den Router erfolgen. Gelingt es dem Angreifer den Dienst des Routers mit vielen Anfragen zum Absturz zu bringen, dann wäre die Verfügbarkeit der drahtlosen Kommunikation also WLAN nicht mehr gewährleistet. Somit wären die Spracherkennungssysteme nicht mehr einsatzbereit.

### 4.4.8 Sicherheitsempfehlungen

Folgende Sicherheitsempfehlungen sollten beim Verwenden von einem WLAN bei den Spracherkennungssystemen beachtet werden:

- Das standardmäßige ausgelieferte Standardpasswort beim Router sollte schnellst möglich durch ein sicheres Passwort ersetzt werden. Das sichere Passwort sollte mindestens Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten und mindestens 20 Zeichen lang sein. Allgemein gilt, je länger das Passwort desto sicherer ist es.
- Beim Router sollte die Option „Fernkonfiguration" deaktiviert werden, um den Zugriff Dritter zu unterbinden.
- Der SSID-Name, der Name des WLAN-Netzwerkes, sollte so gewählt werden, dass es keine Rückschlüsse auf sensiblen Daten wie zum Beispiel Gerätetyp, Straße oder Nachname gibt.

- Das WLAN-Passwort sollte durch ein sicheres Passwort sofort geändert werden.
- Die Option WPS (Wi-Fi Protected Setup) sollte beim Router deaktiviert werden.
- Es sollte stets die neueste Verschlüsselungsmethode mindestens WPA2 verwendet werden.
- Das automatische Verbinden mit voreingestellten WLAN-Geräten sollte deaktiviert werden.
- Der WLAN-Router sollte so eingestellt sein, dass regelmäßig automatische Updates durchgeführt werden.

### 4.4.9 Zusammenfassung und Fazit

Mithilfe von WLAN können die Sprachassistenten bequem kabellos mit dem Internet verbunden werden. Dies hat den Vorteil, dass dadurch die digitalen Assistenten in einem Raum besser verteilt und flexibel eingesetzt werden können. Zudem benötigen die Geräte eine Internetverbindung, um die Sprachbefehle für die weitere Bearbeitung an die Cloud weiterleiten zu können. Die Voraussetzung einer ständig bestehenden drahtlosen Verbindung kann aber zugleich auch ein Sicherheitsrisiko sein. So besteht immer die Gefahr, dass die bei der Funkübertragung übertragenen sensible Daten wie zum Beispiel das Passwort eines Online-Banking Kontos ggf. abgefangen und woanders verwendet werden. Zudem ist die WLAN-Sicherheit sehr abhängig von der Konfiguration der Geräte. Somit sind die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit sowie Authentizität bei der drahtlosen Kommunikation sehr abhängig vom Faktor Mensch. Denn vergisst der Anwender die entsprechenden Sicherheitsvorkehrungen auszuführen, wie zum Beispiel die entsprechenden Passwörter sicherheitstechnisch anzupassen oder die richtige Verschlüsselung auszuwählen, ist es für den Angreifer ein leichtes Spiel in eine WLAN-Verbindung einzudringen, zu übernehmen, zu täuschen, zu fälschen, zu betrügen, auszuspähen, zu entwenden, zu verhindern oder zu zerstören.

## 4.5 Sicherheitsproblem Bluetooth

„Bluetooth ist ein Industriestandard gemäß IEEE 802.15.1 für die drahtlose (Funk-)Vernetzung von Geräten über kurze Distanz.“ (BSI; 2019, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html;jsessionid=4CAEF2A65

8AD0720316D82A543E16018.1_cid351?nn=6597936&cms_lv2=6658206). Seit 1998 gibt es eine spezielle Gruppe, ein Zusammenschluss aus ca. 2.500 Firmen wie IBM, Intel, Nokia auch genannt die Bluetooth Special Interest Group (SIG) mit dem Ziel, eine Bluetooth-Spezifikation zu entwickeln. Der Name „Bluetooth“ kommt von einem dänischen König genannt Harald Blauzahn (übersetzt Harald Bluetooth). Bluetooth dient der Datenübertragung zwischen Geräten über kurze Distanz, meistens zwischen einem und zehn Meter per Funktechnik. Neuere Geräte erreichen sogar schon eine Reichweite von einhundert Meter. Bluetooth kann weltweit eingesetzt werden und hat einen geringen Stromverbrauch. Bei den Sprachassistenten kann Bluetooth zum Beispiel dazu verwendet werden, um das Smartphone mit dem Lautsprecher zu koppeln um anschließend Musik abzuspielen zu können.

Allerdings gibt es auch bei der Bluetooth-Technologie im Zusammenhang mit den Spracherkennungssystemen einige Schwächen und Angriffspunkte. „Die Bluetooth-Spezifikation selbst ist im Vergleich zu anderen Protokollen massiv und komplex. Nur als Referenz, die Bluetooth-Spezifikation ist mehr als 5 mal so groß wie die Wi-Fi-Spezifikation. Es gibt mehrere Gründe, die zur Größe beitragen, aber einer der wichtigsten ist, dass Bluetooth in vielerlei Hinsicht eine eigene Version des TCP/IP-Stacks erstellt. Infolgedessen ist der Bluetooth-Stapel ziemlich groß und komplex. Und im Allgemeinen ist groß und komplex ein Nährboden für Verwundbarkeiten.“ (Armis, 2017, http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf, S. 3)

So haben Forscher des IT-Sicherheitsunternehmen Armis bei den digitalen Assistenten verschiedene Bluetooth Schwachstellen entdeckt und diese zu dem Sammelbegriff „BlueBorne“ zusammengefasst. Unter anderem nutzen die Angreifer Sicherheitslücken der einzelnen Betriebssysteme aus hier der Amazon Echo mit Linux-Kernel, Google Home mit Android und Apple Siri mit iOS.

So wurden bei Amazon Echo folgende zwei Schwachstellen entdeckt:

- Sicherheitslücke bei der Ausführung von Remote-Code im Linux-Kernel (CVE-2017-1000251)
- Schwachstelle bei Informationslecks im SDP-Server (CVE-2017-1000250)

Google Home Geräte sind von einer Schwachstelle betroffen:

- Sicherheitslücke durch Informationslecks im Bluetooth-Stapel von Android (CVE-2017-0785)

Durch die oben aufgeführten Schwachstellen können Geräte vollständig übernommen, Dateien abgefangen oder Denial-of-Service Angriffe ausgeführt werden.

### 4.5.1 Sicherheitsmodi bei Bluetooth

„Bei Bluetooth unterscheidet man vier Modi. Bei einer Anfrage zur Etablierung einer Bluetooth-Verbindung wird überprüft, in welchem Modus sich die Geräte befinden und abhängig davon werden unterschiedliche Sicherheitsdienste angestoßen.“ (Eckert, 2014, S. 934)

**Modus 1**

Der Modus 1 wird auch als „unsicherer Modus“ bezeichnet, da es hier keine Sicherheitsfunktionen gibt. Jedoch gibt es eine Reaktion auf eine Authentifizierungsanforderung eines anderen Gerätes.

**Modus 2**

Beim Modus 2 werden Sicherheitsdienste auf der Dienstebene angeboten, sodass unterschiedliche Anwendungen mit verschiedenen Sicherheitsfunktionen bestückt werden können. Voraussetzung ist hier eine L2CAP-Verbindung, damit ein Sicherheitsdienst genutzt werden kann.

**Modus 3**

Der Modus 3 liegt auf einer tieferen Ebene, der Link-Ebene, und liefert einen Grundschutz. Eine höhere Modusnummer bedeutet nämlich hier nicht automatisch auch einen höheren Sicherheitsschutz. Er sorgt für Authentifizierung und Verschlüsselung der Kommunikation. Wird erstmalig zwischen zwei Geräten kommuniziert, muss ein gemeinsames Geheimnis, ein Verbindungsschlüssel, vereinbart werden. Für die Schlüsselerzeugung wird eine PIN benötigt. Der Modus 3 ist der am häufigsten verwendete Modus.

**Modus 4**

Der Modus 4 erweitert den Modus 2. Hier erfolgt die Autorisierung auf Dienstebene. Beim Modus 4 wird das Secure Simple Pairing (SSP) verwendet.

### 4.5.2 Sicherheitsproblem Bluetooth Stack (BlueBorne)

Forscher vom IT-Sicherheitsunternehmen Armis fanden heraus, dass zum Beispiel der Amazon Echo von einer Entfernung bis zu zehn Meter via Bluetooth das Ausführen beliebiger Codes erlaubt. Hier nutzten die Angreifer eine Sicherheitslücke bei der Ausführung von Remote-Code im Linux-Kernel aus. Das Opfer muss hier nichts aktivieren oder klicken. Bei diesem Angriff muss das Opfer nur Bluetooth aktiviert haben. Hier besteht sogar die Gefahr der Übernahme des kompletten Gerätes. Da gerade Amazon Echo sowie Google Home Bluetooth nicht deaktiviert werden kann, sind diese Geräte sehr anfällig auf diese Angriffe. Das Opfer selbst merkt vom Angriff nichts, während der Angreifer in Ruhe seinen Schadcode ausführen kann. Der Angriff dauert nicht länger als zehn Sekunden. Diese Sicherheitslücke ist auch bekannt unter dem Namen „BlueBorne“ (CVE-2017-1000251)

### 4.5.3 Sicherheitsproblem Man-in-the-Middle

Eine weitere Schwachstelle ist der Verbindungsschlüssel. Ist ein Angreifer in der Lage den Verbindungsschlüssel zwischen zwei Geräten auszuspähen, so gibt es die Möglichkeit ein Man-in-the-Middle-Angriff auszuführen. Hierfür nimmt der Angreifer Kontakt zu den beiden Geräten auf und täuscht zuerst dem Gerät A vor er sei Gerät B. Dann führt er umgekehrt diesen Schritt bei Gerät B durch. Beide Geräte werden in dem Glauben gelassen sie würden miteinander kommunizieren. Somit ergibt sich für den Angreifer die Chance, an den Verbindungsschlüssel zu kommen.

### 4.5.4 Sicherheitsproblem Denial-of-Service (DOS) (BlueSmacking)

Bei Denial-of-Service Angriffen im Bereich Bluetooth wird versucht ein Endgerät nicht nutzbar zu machen, indem man zum Beispiel das Endgerät mit zahlreichen Pairing-Anfragen überflutet. BlueSmacking ist ein bekannter Bluetooth Angriff bei dem die L2CAP-Anfragen genutzt werden, um andere Bluetooth Geräte in Reichweite gleichzeitig zu stören.

### 4.5.5 Sicherheitsempfehlungen

Folgende Sicherheitsempfehlungen sollten bei den digitalen Assistenten bei der Verwendung von Bluetooth eingehalten werden:

- Es sollte unbedingt darauf geachtet werden regelmäßig die neuesten Updates einzuspielen.
- Es sollte nur mit anderen Bluetooth Geräten eine Verbindung aufgebaut werden, die als vertrauenswürdig gelten.

### 4.5.6 Zusammenfassung und Fazit

Bluetooth bietet verschiedene Sicherheitsmodi an. Zugute kommt dem Bluetooth-Prinzip dass unterschiedliche Schlüssel für unterschiedliche Aufgaben verwendet werden und eine wechselseitige Authentifizierung möglich ist. Das Bluetooth-Protokoll wurde nicht dafür entwickelt sensible Daten über eine große Entfernung zu übertragen. Sondern es wurde entwickelt, um Daten zwischen Geräten innerhalb einer kurzen Reichweite, meistens von ein bis zehn Meter, zu transportieren. Daher muss sich der Angreifer in der Nähe von etwa zehn Meter befinden, um die Schwachstellen ausnutzen zu können. Daher könnte das Risiko bestehen, dass der Angreifer die digitalen Assistenten vor der Wohnungstür oder in der Nähe eines Fensters übernehmen könnte. Eine weitere Gefahr besteht darin, dass sich bei den Sprachassistenten Amazon Alexa und Google Home im Gegensatz zu Apples Siri auf dem Smartphone keine Möglichkeit gibt, Bluetooth zu deaktivieren. Somit sind die Sprachassistenten Amazon Alexa und Google Home permanent mit Bluetooth auf der Suche nach Kommunikationspartnern. Des Weiteren sind die Geräte, wenn Sicherheitslücken entdeckt werden sehr abhängig von den automatischen Updates der Hersteller. Zwar wurden die meisten Sicherheitslücken bereits durch Updates und Patches geschlossen, allerdings nimmt die Zahl der Bluetooth-fähigen Geräte rasant zu. Es ist nur eine Frage der Zeit, bis die Angreifer weitere Sicherheitslücken in der komplexen Bluetooth-Spezifikation finden werden.

## 4.6 Sicherheitsproblem Application-Programming-Interface (API)

Der Begriff API ist die Kurzform von „Application-Programming-Interface“. Umgangssprachlich wird die Abkürzung API meistens als „Programmierschnittstelle“ bezeichnet. Die Sprachassistenten sind von Haus aus mit Grundfunktionen ausgestattet wie zum Beispiel Setzen eines Weckers, Begriffe erklären, Kalender verwalten oder das Abspielen von Musik. Möchte man die Grundfunktionen der Sprachassistenten erweitern, kann dies mithilfe der Schnittstelle erfolgen. APIs ermöglichen es Drittanbietern die Fähigkeiten der digitalen Assistenten zu erweitern. So ist es möglich SmartHome Geräte anzubinden um zum Beispiel Lichter einzuschalten, das Heizungssystem zu verwalten oder die Überwachungskameras zu aktivieren.

Allerdings verbirgt das Öffnen der Schnittstelle an Dritte auch Gefahren. So besteht das Sicherheitsrisiko Malware-verseuchte Programme über die Assistenten heimlich aufzurufen oder die Geräte zum Abhören zu missbrauchen.

### 4.6.1 Sicherheitsproblem API bei Amazon Echo

Bei Amazon Echo werden die erweiterten Fähigkeiten „Alexa-Skills“ genannt. Derzeit gibt es Zehntausende von „Alexa-Skills“, die in verschiedenen Sprachen und Kategorien wie Essen & Trinken, Nachrichten, Sport oder Lifestyle eingeteilt sind. Über die Amazon-Website www.amazon.de oder der Alexa-App ist es dann möglich, die passende „Alexa-Skill“ auszuwählen und auf einem Echo-Gerät zu installieren. Die meisten „Alexa-Skills“ werden kostenlos angeboten. Um einen Alexa-Skill entwickeln zu können, benötigt man einen kostenlosen Amazon Developer Account. Hierüber erhält man Zugriff auf die „Alexa Developer Console“, die momentan nur in englisch verfügbar ist. Alexa-Skills können leicht ohne weitere Programmierkenntnisse entwickelt werden, da es schon vorgefertigte Bausteine und Bibliotheken gibt. Bei der Neuanlage einer Skill kann der Entwickler wählen zwischen „Alexa Skills Kit“ (ASK) für die Erstellung von Skills oder „Alexa Voice Service“ (AVS), um Fähigkeiten an andere Alexa Geräte zu verleihen. Über die „Alexa Developer Console“ können alle wichtigen Punkte Schritt

für Schritt über eine leicht verständliche Oberfläche für die Entwicklung und Konfiguration einer Skill durchgeführt werden.

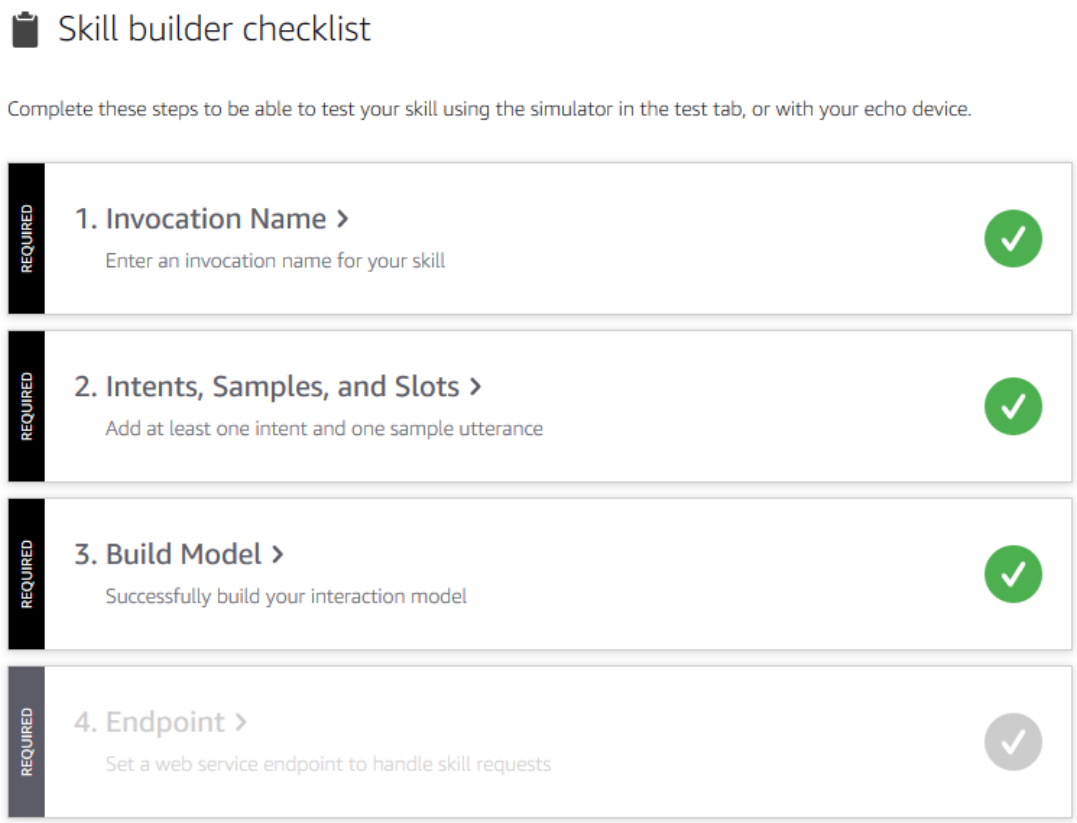



**Bild 21: Alexa Developer Console (Eigene Darstellung)**

So ist es möglich neben dem Skill-Namen, Skill-Typ auch zu definieren, mit welchem Satztyp bzw. Intents Alexa zukünftig die eigene Skill aufrufen soll. Für die Kommunikation mit Alexa stellt Amazon Java und Node.jS Frameworks bereit. Für die Hosting-Plattform kann der AWS Lambda als Backend mit der Programmiersprache Java verwendet werden. Skills können jederzeit zum Beispiel über die Alexa-App aktiviert oder deaktiviert werden, wobei hier der Begriff Aktivierung quasi für eine Installation steht und die Deaktivierung für eine Deinstallation.

Allerdings ist es Sicherheitsforscher von „Checkmarx“ in einem Experiment gelungen, dass man eine selbst entwickelte Alexa-Skill so konfigurieren kann, dass Amazon Echo auch zum Abhören genutzt werden kann. So haben die Forscher extra eine Skill so

entwickelt, dass auch nach einem abgeschlossenen Sprachbefehl weiter gelauscht und aufgenommen wird.

**Sicherheitsvorfall:**

„Die Checkmarx-Forscher haben eine Schwachstelle in einer Java-Script Bibliothek ausgenutzt. Dabei griffen sie auf die Funktion der erneuten Nachfrage zurück. Echo tat also so, als hätte es einen Nutzer-Wunsch nicht verstanden und daher eine erneute Nachfrage senden müsse. Allerdings wurde anstatt einer Nachfrage nur Stille gesendet - die Aufnahme des Nutzers wurde fortgeführt.“ (Osswald, 2018, https://www.chip.de/news/Amazon-Echo-gehackt-Skill-macht-Lautsprecher-zur-Wanze_138594450.html)

### 4.6.2 Sicherheitsproblem API bei Google Home

Google Home bietet für die Verwendung von Diensten von Drittanbietern sogenannte „Google Actions“ an. Die „Google Actions“ werden in unterschiedlichen Kategorien wie Spiel & Spaß, Sport, Shopping oder Kinder & Familie angeboten. Eine Actions-Übersichtsseite findet man auf der Website unter https://assistant.google.com/explore?hl=de oder über die Google Home App. „Google Actions“ müssen nicht installiert oder aktiviert werden. Stattdessen kennt der Google Assistant bereits alle verfügbaren Dienste. Möchte man eine Actions nutzen, so kann dies über den Sprachbefehl „OK Google“ und den Aufruf des gewünschten Dienstes erfolgen. Erfolgt über einen längeren Zeitraum keine Kommunikation mehr, erfolgt ein Signalton als Zeichen dafür, dass der Dienst nicht mehr aktiv ist. Die meisten „Google Actions“ stehen kostenlos zur Verfügung. Für die Entwicklung von „Google Actions“ wird ein kostenloser Google Account benötigt. Mithilfe des Google Accounts kann man sich bei der „Actions Console“ anmelden. Die „Actions Console“ Oberfläche gibt es nur in der Sprache englisch. Die „Actions Console“ dient als zentraler Ort für die Konfiguration, Einstellungen und Veröffentlichung von Actions.

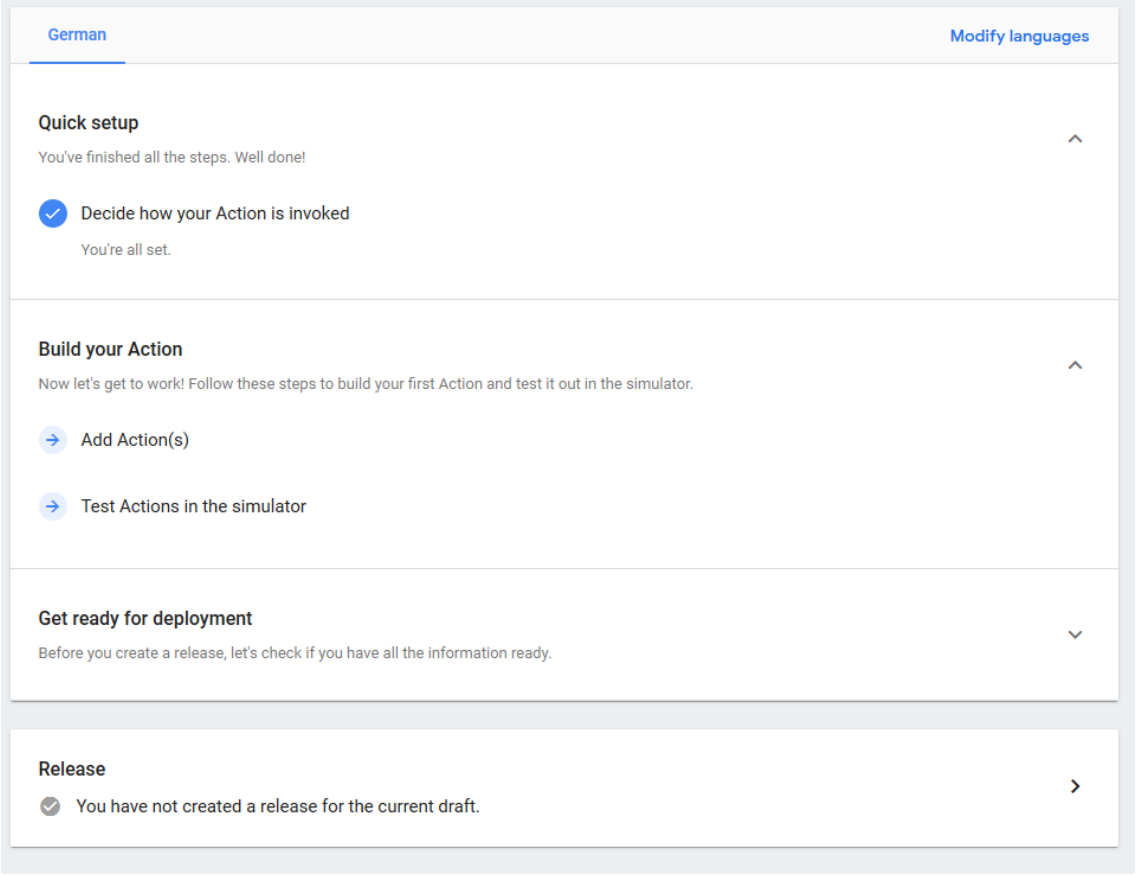



**Bild 22: Google Actions Console (Eigene Darstellung)**

Für die Entwicklung von Actions, kann entweder API.AI oder Actions SDK verwendet werden. Mit API.AI können Entwickler direkt über eine grafische Oberfläche Actions entwickeln. Bei Actions SDK besteht die Möglichkeit, Actions von Grund auf mit Node.jS Frameworks und JSON aufzubauen. Bei der Neuanlage von Actions, können deren Aufrufname und verschiedene Beispielsätze mit entsprechender Aktion hinterlegt werden. Als Hosting-Plattform kann die Cloud Functions for Firebase als Backend verwendet werden.

Ein Sicherheitsforscher mit dem Namen „Rithvik Vibhu“ hat herausgefunden, dass Google Home eine inoffizielle API besitzt, auch bekannt unter dem Namen „Google Home Local API“. Über diese API besteht die Möglichkeit von extern ohne weitere Authentifizierung auf das Gerät zuzugreifen und GET- und POST-Befehle auszuführen, und diese Daten in einem JSON-Format auszugeben. Diese Befehle können von jedem Gerät im gleichen Netzwerk ausgeführt werden. Für den Zugriff wird die IP-Adresse des

Google Home Gerätes und der Port 8008 benötigt. Die IP-Adresse erhält man einfach über die Google Home App unter den Geräteeinstellungen.

Diese Methode könnte es einem Angreifer ermöglichen, sensible Informationen zu erhalten und kleinere Manipulationen durchzuführen.

**Beispielszenario:**

Mit der Eingabe der hier verwendeten URL-Adresse: http://192.168.1.14:8008/setup/eureka_info ist es möglich, folgende Geräteinformationen auszulesen:

- MAC-Adresse
- Google Home Gerätenamen
- SSID

**MAC-Adresse:**

**Bild 23: MAC-Adresse (Eigene Darstellung)**

**SSID (Service Set Identifier):**


```
ssdp_udn:        "9e36f4a9-5bdd-55c2-41cd-0f0c5914af34"
ssid:            "O2-WLAN33"
time_format:     2
```


**Bild 24: Google Home SSID (Eigene Darstellung)**

Beispielsweise sind folgende Änderungen oder Abrufe möglich:

- Timer und Alarm auslesen
- Benachrichtigungen abrufen oder einstellen
- Abruf alle Geräte im WLAN
- Abruf aller Bluetooth-Geräte
- Ausführen eines Reboots

Eine Liste aller möglichen GET- und POST-Befehle können über die Website https://rithvikvibhu.github.io/GHLocalApi/ aufgerufen werden.

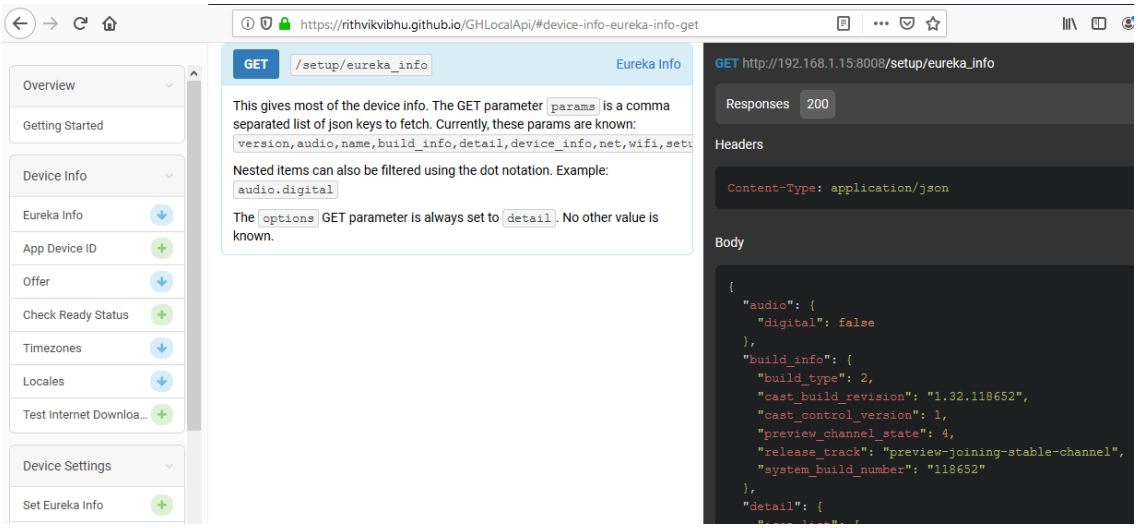



**Bild 25: Google Home Local API GET/POST Befehle (https://rithvikvibhu.github.io/GHLocalApi/)**

Eine Funktionsfähigkeit aller Befehle, kann nicht gewährleistet werden, da Google manche Lücken bereits verändert oder geschlossen hat.

### 4.6.3 Sicherheitsproblem API bei Apple Siri

Das Apple iPhone bietet für die Nutzung von Diensten von Drittanbietern sogenannte „Kurzbefehle“ (engl. shortcuts) an.

„Zusätzlich zum Ausführen der einfachen Kurzbefehle, die du von Siri vorgeschlagen bekommst, kannst du die App „Kurzbefehle“ verwenden, um bereits vordefinierte oder eigene Kurzbefehle zu deinem iOS-Gerät hinzuzufügen.“ (Apple, 2019, https://support.apple.com/de-de/guide/shortcuts/apdf22b0444c/2.2/ios/12.0) Eine Übersicht von vordefinierten Kurzbefehlen können über die App „Kurzbefehle“ unter „Galerie“ aufgerufen werden. Diese sind in verschiedenen Rubriken eingeteilt wie zum Beispiel Highlights, Bleib gesund, Im Haushalt oder Fotografie.

**Bild 26: Kurzbefehle-APP Galerie (Eigene Darstellung)**

Die Entwicklung eines eigenen Kurzbefehls kann über die App „Kurzbefehle“ unter Bibliothek erfolgen. Jeder Kurzbefehl besteht aus mehreren verschiedenen Aktionen, die eine bestimmte Funktion ausführen. Es gibt über 300 Aktionen die miteinander verkettet werden können. Damit bilden die Aktionen das Kernstück eines Kurzbefehls.

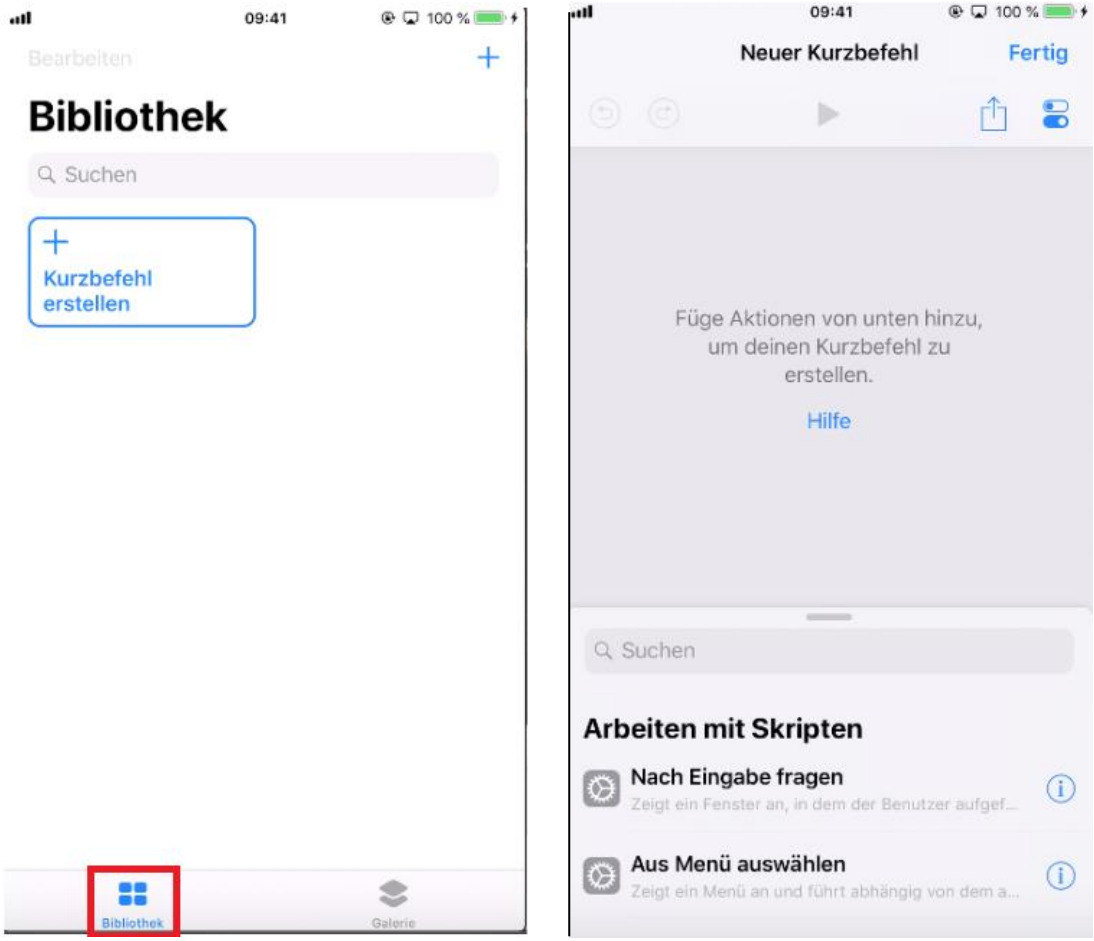



**Bild 27:Kurzbefehle-App Bibliothek (Eigene Darstellung)**

Selbst erstellte Kurzbefehle können über die App „Kurzbefehle“ unter der Bibliothek abgerufen werden. Um einen Kurzbefehl ausführen zu können spricht man einfach „Hey Siri“ und anschließend den persönlichen Satz, den man zuvor bei Anlegen seines Kurzbefehls aufgenommen hat.

Allerdings kann auch Apples Kurzbefehle-App ein Sicherheitsrisiko darstellen. Denn so konnte der Sicherheitsforscher @userlandkernel nachweisen, dass Kurzbefehle auf geschützte iPhone-Dateien zugreifen können.

**Sicherheitsvorfall:**

Beim Download von manipulierten Kurzbefehlen besteht die Gefahr, dass diese durch eine Verzeichnislücke auf normalerweise geschützte Systemdateien zugreifen.

„Die in Apples Kurzbefehle-App hinterlegte Aktion "Ordner erstellen" lässt sich einsetzen, um aus der Sandbox auszubrechen, erklärt der Sicherheitsforscher @userlandkernel. Dafür reiche es, durch eine Reihe von "../"-Befehlen sich in der Verzeichnisstruktur weiter nach oben zu bewegen, um dann ein gewünschtes Verzeichnis zu öffnen – dabei versagt offenbar die Sandbox.“ (Becker, 2019, https://www.heise.de/mac-and-i/meldung/Apples-Kurzbefehle-App-Shortcuts-koennen-geschuetzte-iPhone-Dateien-abgreifen-4283745.html) Durch diese Sicherheitslücke ist es Angreifern möglich in geschützte Bereiche wie die SMS-Datenbank, Notizen oder die Konfiguration von Apples Heimvernetzungsprotokoll HomeKit zuzugreifen.

### 4.6.4 Sicherheitsempfehlungen

Folgende Sicherheitsempfehlungen sollten beim Erstellen oder Verwenden von Diensten von Drittanbietern beachtet werden:

- Nur vertrauenswürdige Amazon Skills, Google Actions oder Siri-Kurzbefehle herunterladen und nutzen.
- So viele Informationen wie möglich über einen Dienst eines Drittanbieters sammeln: Kundenbewertung, Hersteller, Beschreibung, Update-Historie, Versionsnummer, Veröffentlichungsdatum.
- Prüfen welche Freigaben man den Amazon Skills, Google Actions oder Siri-Kurzbefehle erteilt.
- Regelmäßige Updates ausführen, wenn vorhanden.

### 4.6.5 Zusammenfassung und Fazit

Alle drei Sprachassistenten, Amazon Alexa, Google Assistant oder Siri, verfügen über ein gewisses Grundwissen. So können die Sprachassistenten Basisfunktionen durch Zuruf eines Kommandos zum Beispiel Musik spielen, den Wetterbericht abrufen oder einen Freund anrufen. So dient dies zur Unterhaltung oder als Alltagshelfer. Ist dies einem nicht

genug, können diese Fähigkeiten erweitert werden. Durch Schnittstellen von Drittanbietern können nun Smart Home Geräte angebunden oder eigene Apps entwickelt werden. Durch diese Erweiterungen können die digitalen Assistenten noch klüger konfiguriert werden. Jedoch ergeben sich durch die Verwendung von Schnittstellen auch Risiken. Angreifer können Erweiterungen ausnutzen, um durch versteckte Aktionen und Funktionen Gespräche abzuhören, auf geschützte Dateien zuzugreifen. Auch über einen Webbrowser ist es möglich, direkt auf ein Gerät zuzugreifen und sensible Konfigurationseinstellungen auszulesen oder zu ändern.

## 4.7 Sicherheitsproblem Künstliche Intelligenz

Allerdings können die gelernten Muster im Bereich der Künstlichen Intelligenz (KI) bei den Sprachassistenten auch ein Sicherheitsproblem darstellen. So kann es hierbei zu folgendem Angriff kommen.

**Angriff während des Lernens**

Für das Anlernen der KI-Systeme werden umfangreiche Trainingsdaten benötigt. Jedoch kann die Integrität dieser Trainingsdaten nicht immer eindeutig sichergestellt werden. So kann es vorkommen, dass manipulierte Eingaben in den Trainingsdaten das System täuschen und die Funktionsweise des Gerätes beeinflussen. So ein Angriff könnte für eine reduzierte Vorhersagegenauigkeit genutzt werden oder zu gezielten Fehlentscheidungen führen.

Die Algorithmen des maschinellen Lernens sind für eine unsichere Umgebung nicht ausgelegt und können durch falsche Eingaben während des Lernens oder der Vorhersage gestört werden.

# 5 Datenschutz bei den Spracherkennungssystemen

Im Fokus dieses Kapitels steht die Analyse des Datenschutzes der einzelnen Sprachassistenten. Im ersten Schritt wird zuerst analysiert, wo die Sprachaufzeichnungen beziehungsweise die Daten abgelegt und abgerufen werden können. Anschließend erfolgt im zweiten Schritt eine Analyse der Kommunikation mithilfe von Wireshark. Hier wird mit der Unterstützung eines Versuchsaufbaus analysiert, ob bei den einzelnen Sprachassistenten eine Aufzeichnung der Sprache bereits mit und ohne das Aktivierungswort erfolgt.

## 5.1 EU-Datenschutzgrundverordnung (EU-DS-GVO)

„Ab dem 25. Mai 2018 gilt in ganz Europa die EU-Datenschutz-Grundverordnung (kurz: EU-DS-GVO bzw. DS-GVO). Die Verordnung wird wesentliche Teile des Datenschutzrechts in Europa vereinheitlichen.“ (Kranig, Sachs, Gierschmann, 2017, S.21) Die Datenschutzgrundverordnung ersetzt im Wesentlichen, das Bundesdatenschutzgesetz (BDSG).

Gerade bei den Sprachassistenten spielt der Datenschutz eine zentrale Rolle. Denn für die digitalen Assistenten ist das Sammeln und Verarbeiten von Nutzerdaten für die stetige Weiterentwicklung unverzichtbar.

So enthält die Verordnung Vorschriften zum Schutz von natürlichen Personen und den Schutz personenbezogener Daten.

- „Nur nach Einwilligung der betroffenen Person dürfen überhaupt Daten erhoben werden.
- Die Datenverarbeitung ist stets zweckgebunden.
- Die Datenerfassung muss so minimal wie möglich gehalten werden.
- Daten, die eine Person identifizieren, dürfen nur beschränkt gespeichert werden.
- Daten müssen vor Verlust, Zerstörung und unbefugter Verarbeitung geschützt werden.“ (Pfeifer, 2018, https://www.homeandsmart.de/datenschutz-apple-siri)

Der Begriff „personenbezogene Daten“ kann wie folgt definiert werden kann:

„personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“ (intersoft consulting, 2018, https://dsgvo-gesetz.de/art-4-dsgvo/)

## 5.2 Analyse der Sprachaufzeichnungen

### 5.2.1 Sprachaufzeichnung Amazon Echo

Nach Erkennung des Aktivierungswortes wird die Sprachaufzeichnung an die Amazon Cloud weitergeleitet, dort wird Alexa`s Antwort analysiert und generiert. Die Sprachbefehle werden mit dem jeweiligen Amazon-Konto verknüpft. Um den Alexa Voice Service (AVS) nutzen zu können, muss der Nutzer die Nutzungsbedingungen und die Datenschutzerklärung von Amazon anerkennen. Damit sichert sich Amazon die Rechte für die übertragenden Daten. Laut Datenschutzbestimmungen von Amazon werden die Sprachaufzeichnungen unbefristet in der Cloud gespeichert. Ein genauer Standort der Amazon Cloud, wo die Daten gespeichert werden, konnte leider nicht festgestellt werden. Laut Amazon können dies auch Server außerhalb Europas, also auch Server im Ausland z.B. USA sein. Die Speicherung der Daten dient laut Amazon zum Trainieren und der stetigen Verbesserung der Systeme, um natürliche Sprache besser verstehen zu können.

„Wir speichern Ihre Informationen solange, wie dies erforderlich ist, um die in dieser Datenschutzerklärung beschriebenen Zwecke zu erfüllen oder wie dies gesetzlich vorgeschrieben wird, z.B. für Steuer- und Buchhaltungszwecke. Andere Speicherdauern werden wir Ihnen mitteilen.“ (Amazon, 2019, https://www.amazon.de/gp/help/customer/display.html?nodeId=3312401)

Laut Datenschutzerklärung nimmt sich Amazon auch das Recht nicht nur Sprachaufzeichnungen zu speichern, sondern auch folgende Informationen wie:

- Passwörter
- E-Mail-Adressen
- IP-Adresse
- Zahlungsverhalten
- Informationen über eingesetzte Hardware und Software
- Gesuchte Produkte
- Besuchte Internetseiten
- Die Weitergabe von Daten an Dritte (Partner von Amazon)

Jedoch ist es jedem Amazon-Kunde möglich, jederzeit seine Sprachaufzeichnungen zu überprüfen und zu verwalten. So gibt es folgende zwei Möglichkeiten um seine Sprachdateien zu verwalten:

1. Mit dem Webbrowser unter: www.amazon.de/alexaprivacy über die Option „Sprachaufnahmen-Verlauf überprüfen oder
2. über die Alexa-App hier unter „Einstellungen“ → „Alexa Datenschutz“ → „Sprachaufnahmen-Verlauf überprüfen

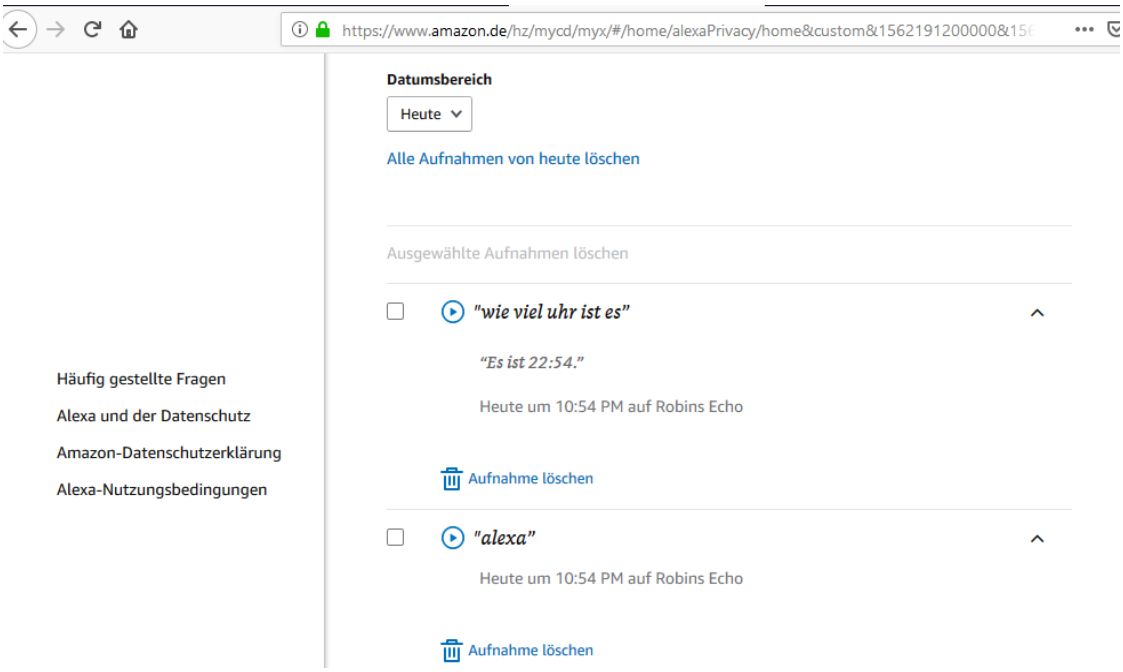



**Bild 28: Alexa Sprachaufnahmen-Verlauf überprüfen im Browser (Eigene Darstellung)**

Über den Browser können die einzelnen Sprachaufzeichnungen angezeigt werden. Je nach gewähltem Datumsbereich: „Heute“, „Gestern“, „Diese Woche“, „Dieser Monat“, „Gesamter Verlauf“ oder „Benutzerdefiniert“ (Startdatum, Enddatum). Die Sprachaufzeichnungen können entweder als Audiodatei angehört oder als Text gelesen werden. Zudem wird zur jeder Sprachaufzeichnung das Datum, die Uhrzeit, die Antwort von Alexa sowie der Gerätenamen von Amazon Echo angezeigt. Durch einen Klick lassen sich einzelne Sprachaufzeichnungen löschen oder gleich alle. Zudem kann man die Option „Löschen per Sprachbefehl“ aktivieren. Ist diese Option aktiviert, gibt es eine weitere Möglichkeit mit einem Sprachbefehl „Alexa, lösche, was ich gerade gesagt habe“, Sprachaufzeichnungen zu löschen. Auf der Seite Alexa Datenschutz ist es zudem Nutzern möglich einzustellen, dass die Sprachaufnahmen zur Entwicklung neuer Funktionen verwendet werden dürfen.

Die zweite Methode Sprachaufzeichnungen zu überprüfen und zu verwalten ist über die-Alexa-App. Hier werden die gleichen Optionen wie über den Browser angeboten.

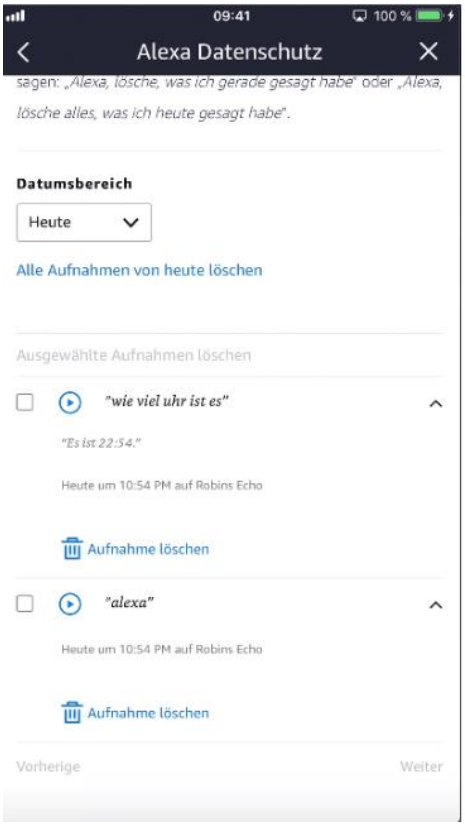



**Bild 29:Sprachaufnahmen-Verlauf überprüfen Alexa-APP (Eigene Darstellung)**

Leider gab es in Bezug auf Alexa schon mindestens zwei gemeldete Datenschutz Zwischenfälle.

**Datenschutzvorfall**

„Amazon lässt zum Teil Mitarbeiter aufgezeichnete Befehle von Nutzern an seine Assistenzsoftware Alexa anhören, abtippen und prüfen, um die Spracherkennung zu verbessern. Der Konzern bestätigte die Vorgehensweise am Donnerstag dem Finanznachrichtendienst *Bloomberg*. "Wir versehen nur eine sehr geringe Auswahl an Alexa-Sprachaufnahmen mit Kommentaren, um das Kundenerlebnis zu verbessern." (Kannenberg, 2019, https://www.heise.de/newsticker/meldung/Amazon-Mitarbeiter-tippen-zum-Teil-Alexa-Sprachbefehle-ab-4374871.html)

**Datenschutzvorfall**

**„**Ein Amazon.de-Kunde hatte die deutsche Niederlassung des Konzerns um Auskunft der zu ihm gespeicherten Daten nach DSGVO gebeten. Amazon stellte ihm zwei Monate später ein ZIP-Archiv bereit. Rund 50 der darin enthaltenen Dateien enthielten auf seine Person bezogene Daten. Allerdings fand er auch rund 1700 WAV-Dateien sowie eine PDF-Datei vor, die offensichtlich chronologisch unsortierte Transskripte darüber enthielt, was Amazons Sprachassistent Alexa aus Spracheingaben verstanden hat.

Das Problem: Der Kunde hat noch nie Alexa genutzt. Er teilte Amazon.de mit, dass die ZIP-Datei offensichtlich Alexa-Sprachaufzeichnungen eines ihm fremden Amazon-Kontos enthielt und bat um Auskunft dazu.“ (Bleich, 2018, https://www.heise.de/newsticker/meldung/Amazon-gibt-intime-Sprachdateien-preis-4254716.html)

### 5.2.2 Ergebnis

Seien sie sich bewusst, mit der Anerkennung der Nutzungsbedingungen von „Amazon Voice Service“ (AVS) geben sie Amazon das Recht, ihre eigenen personenbezogen Daten zu verarbeiten. Dies bedeutet, Amazon kann über sie genaue Nutzerprofile erstellen, Gewohnheitsmuster oder gezielt Werbung versenden. Außerdem nimmt Amazon sich das Recht die Nutzerdaten jederzeit an Dritte weiterzuleiten. Zudem ist es bedenklich, dass Amazon die Sprachaufzeichnungen unbefristet in der Cloud speichert. Zwar gibt es

die Möglichkeit die Sprachaufzeichnungen zu löschen, allerdings ist vielen Nutzern nicht bewusst, dass die Sprachdaten überhaupt archiviert werden. Die Option der Löschung ist vielen auch nicht bekannt. Des Weiteren verweist Amazon beim Löschen der Daten, darauf, dass sich dadurch ihre Erfahrung bei der Verwendung mit dem Gerät verschlechtern kann. Da die Daten auch auf Servern außerhalb Deutschlands gespeichert werden können, besteht die Gefahr, da es im Ausland andere Datenschutzbestimmungen gibt, dass z.B. ein Geheimdienst auf die Daten zugreifen darf. Allerdings kann es auch vorkommen, dass ungewollte Sprachaufzeichnungen bei denen Alexa irrtümlich das Aktivierungswort hört, in der Cloud gespeichert werden. Da die Sprachaufzeichnungen auch in Form einer Audiodatei vorliegen, muss einem bewusst sein, dass auch alle Hintergrundgeräusche oder Gespräche von anderen Personen mit aufgezeichnet werden. Oft ist es auch nicht ersichtlich, wie lange ein Gespräch aufgezeichnet wird. Ein mulmiges Gefühl bekommt man, wenn man erfährt, dass Amazon Mitarbeiter oder vielleicht auch andere Zugriff auf die Sprachaufnahmen haben. Man weiß nie genau, was mit den eigenen biometrischen Daten passiert. So ist es schon vorgekommen, dass Amazon Mitarbeiter Sprachaufzeichnungen auswerten sollten, in denen es um sensible Daten wie Kontoinformationen ging. Darüber hinaus nimmt sich Amazon auch das Recht, Alexa jederzeit zu ändern oder den Zugang zu sperren.

### 5.2.3 Sprachaufzeichnung Google Home

Ab dem Moment, wenn Google Home das Aufwachwort hört, erfolgt eine Sprachaufzeichnung. Diese Audiodatei wird dann an einen Server in der Cloud gesendet, der dann die Antwort kreiert. Die Audiodatei ist mit einem Google-Konto verknüpft. Die Sprachaufzeichnungen werden laut Google so lange gespeichert, bis man selbst entscheidet diese zu löschen, also unbefristet. Die übertragene Daten werden weltweit auf verschiedenen Servern in Rechenzentren gespeichert. Den genauen Standort, wo sich die eigenen Daten befinden, verrät Google nicht. Mit der am Anfang zugestimmten Nutzungsbedingung und Datenschutzerklärung erlaubt man quasi Google, seine personenbezogenen Daten zu sammeln und auszuwerten. Daher kann es auch vorkommen, dass Google gewisse Informationen an Dritte weitergibt. In der Google Datenschutzerklärung steht dazu folgendes:

„Wir geben personenbezogene Daten an Unternehmen, Organisationen oder Personen außerhalb von Google weiter, wenn wir hierfür Ihre Einwilligung erhalten haben.“ (Wendel,

2018, https://www.homeandsmart.de/google-datenschutz) Mit der Zustimmung der Nutzungsbedingungen hat man bereits schon Google die Einwilligung erteilt. Google betont stets, dass das Sammeln von Daten und Informationen der Verbesserung der Dienste dient.

Laut Datenschutzerklärung erhebt Google zahlreiche Informationen, hier ein paar Beispiele:

- Kaufaktivitäten
- Standortdaten
- Zahlungsinformationen
- Namen
- Telefonnummer
- Passwort
- Geräteinformationen
- IP-Adresse
- E-Mails die erfasst oder erstellt werden
- Fotos, Videos die erstellt werden
- Youtube-Videos, Kommentare
- Browseraktivitäten
- Welche Apps benutzt werden

Die von Google gespeicherten Sprachdateien können wie folgt abgerufen oder gelöscht werden:

1. Unter https://myaccount.google.com/ mit dem Google-Konto anmelden → Daten & Personalisierung → Sprach- & Audioaktivitäten → Aktivitäten verwalten oder
2. über die Google Home App → Mein Google-Konto anmelden → unter Google Assistant → Meine Aktivitäten auswählen

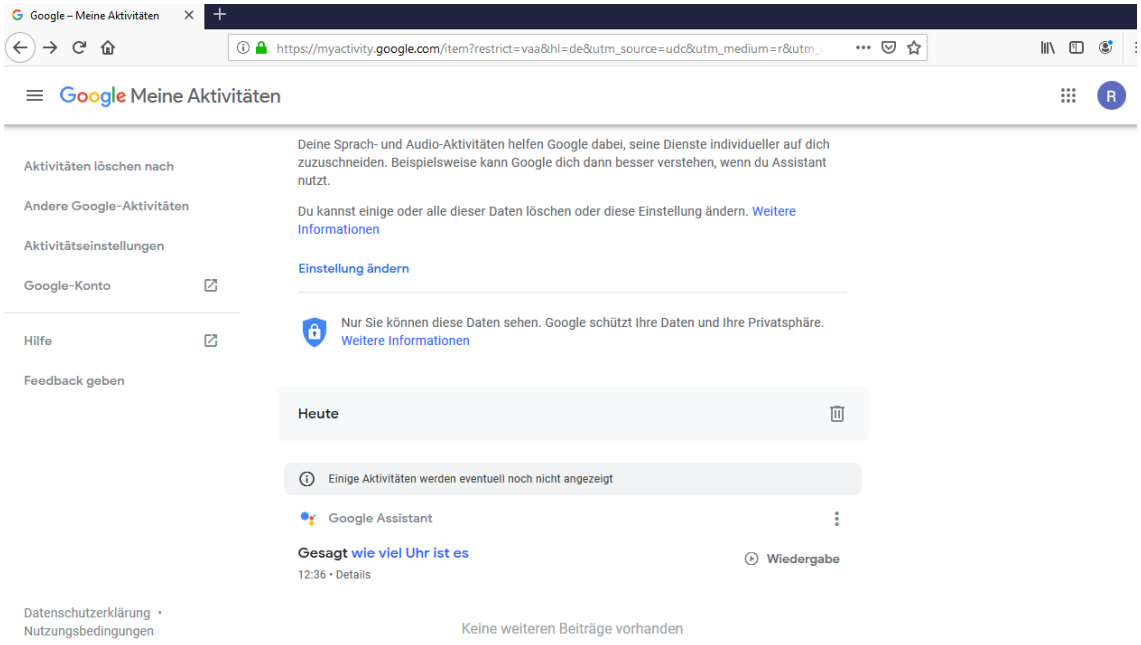



**Bild 30: Google Assistant Sprach-& Audioaktivitäten Browser (Eigene Darstellung)**

Über die Website können die Sprachaufzeichnungen chronologisch angezeigt werden. Mit einem Filter „Heute“, „Letzte 7 Tage“, „Letzte 30 Tage“, „Gesamte Zeit“, „Benutzerdefiniert“ (Nach dem, Vor dem) oder nach Produkten „Google Assistant“, „Voice und Audio“ kann gezielt nach den Audiodateien gesucht werden. Die Audiodateien können direkt wiedergegeben oder per Text gelesen werden. Die Sprachaufnahmen werden mit folgenden Metadaten hinterlegt: Datum, Uhrzeit, Sprachbefehl und welcher Dienst, hier Google Assistant, genutzt hat. Die Datensätze können entweder einzeln oder gesamt gelöscht werden. Interessant sind die Aufnahmen die mit „kein Transkript“ dargestellt werden. Hier handelt es sich oft um Aufnahmen die unbemerkt oder aus Versehen aufgenommen wurden.

Wer seine Privatsphäre schützen möchte, kann untern den Aktivitätseinstellungen die Option „Sprach- & Audioaktivitäten“ deaktivieren. Ist diese Funktion aktiviert werden die Stimme sowie Audiodaten nicht aufgezeichnet. Möchte man diese Funktion deaktivieren warnt Google davor, dass bei einer Deaktivierung die Google Dienste nur noch eingeschränkt arbeiten können und es sein kann, wenn man „OK, Google“ sagt, der Google Assistant einen nicht mehr versteht.

Über die Google Home App stehen die gleichen Optionen wie im Browser zur Verfügung.

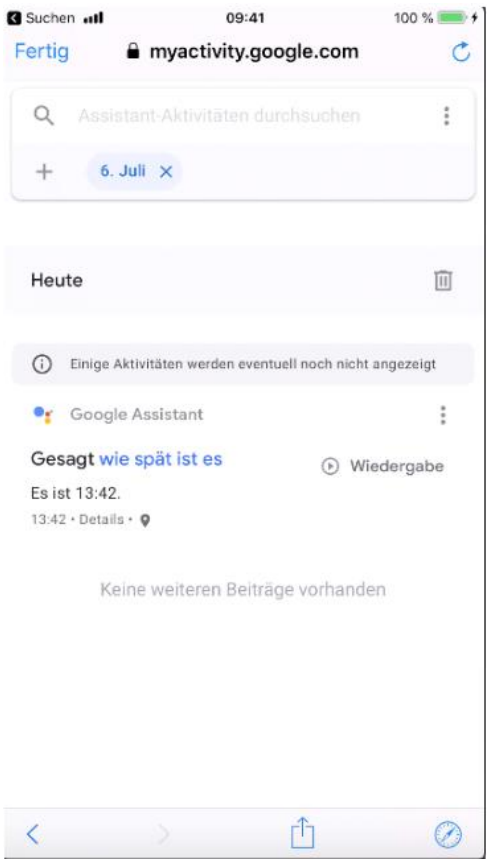



**Bild 31:Google Home App Google Assistant-Aktivitäten (Eigene Darstellung)**

Jedoch sind auch bei Google Home Datenschutzvorfälle bekannt.

**<u>Datenschutzvorfall</u>**

„In Frankreich wurde Google wegen DSGVO-Verstößen verklagt

Im Januar hatte die die französische Datenschutzbehörde CNIL gegen Google eine Strafzahlung in Höhe von 50 Millionen Euro verhängt. Dabei ging es um Verstöße gegen die seit Mai 2018 geltende Datenschutzgrundverordnung (DSGVO). Außerdem wurde kritisiert, dass Nutzerinnen bezüglich der Anzeige personalisierter Werbung nicht ausreichend informiert würden.“ (Zeit Online, 2019, https://www.zeit.de/digital/datenschutz/2019-05/google-daten-automatisches-loeschen-datensicherheit)

### 5.2.4 Ergebnis

Auch Google sammelt viele personenbezogene Daten und gilt weltweit als größter Datensammler. Möchte man einen Dienst von Google nutzen, wie hier das Google-Konto oder den Google Assistant, stimmt man der Datenschutzerklärung von Google zu. Google nennt die persönlich erfassten Informationen „Aktivitäten“. Das Problem ist hier, dass der Nutzer wenig Möglichkeiten hat zu entscheiden, welche persönlichen Daten erfasst werden sollen und welche nicht. Denn anschließend lassen sich nur wenige „Aktivitäten“ nachträglich deaktivieren. Findet man eine „Aktivität“ die sich deaktivieren lässt kann es passieren, dass der Dienst nur noch eingeschränkt genutzt werden kann oder gar nicht mehr funktioniert. Häufig kommt dann bei „OK, Google“ die Sprachausgabe „Bitte gib mir die Berechtigung, um dir zu helfen“. Man ist hier mehr oder weniger den Bedingungen von Google ausgeliefert. Zudem ist vielen Nutzern gar nicht bewusst, was alles erfasst wird, da Google die Anwender nicht ausreichend informiert. Die Datensammlung erfolgt im Prinzip unbemerkt im Hintergrund. Ansonsten ist auch bei Google die Datenhaltung von personenbezogenen Daten auf ausländische Server bedenklich, da hier eine andere Rechtslage gelten kann.

### 5.2.5 Sprachaufzeichnung Apple Siri

Sobald Siri das entsprechende Signalwort wahrnimmt, erfolgt eine Sprachaufzeichnung. Anders als bei Amazon Echo oder Google Home, werden bei Siri die meisten Befehle direkt auf dem Gerät analysiert und verarbeitet. Manche Daten vor allem Sprachaufnahmen erfordern jedoch den Zugriff auf den Apple-Servern in der Cloud. Die Apple-Server sind jedoch weltweit verteilt, und für den Nutzer ist es völlig unklar in welchem Land die eigenen Daten verarbeitet werden, und ob in diesen Ländern die Vorgaben der DSGVO wirklich eingehalten werden. Der Zugriff erfolgt hier anonymisiert und die Kennung der Daten wird dann nach sechs Monaten gelöscht, wobei die Sprachaufzeichnungen selbst bis zu zwei Jahren gespeichert werden. Apple benötigt vor allem diese Daten, um den Nutzer immer besser verstehen zu können. Zudem erstellt Siri auf dem betroffenen Gerät ein lokales Profil des Nutzers, um sich ständig verbessern zu können. Bei Siri werden die Daten nicht mit der Apple-ID verknüpft, sondern über eine zufällig generierte Kennung

mit dem Gerät. Die generierte Kennung kann aber jederzeit wieder zurückgesetzt werden, indem man Siri deaktiviert und anschließend wieder Siri aktiviert. Beim Deaktivieren von Siri löscht Apple die mit der Siri Kennung verknüpften Daten und der Lernprozess beginnt neu.

„Wir versuchen, alle deine Daten auf deinem Gerät zu lassen, wo es am sinnvollsten ist, und dir Optionen zu geben, mit denen du bestimmen kannst, wie sie geteilt werden. Suchst du mit Siri zum Beispiel ein Foto anhand von Standort oder Albumname, dann müssen wir das Foto für ein Ergebnis nicht an einen Server senden. Albumtitel werden nur an Siri gesendet, um dir bessere Ergebnisse zu liefern. QuickType Tastaturfeatures werden durch einen von Apple entwickelten lernfähigen Sprachprozess ermöglicht, der direkt auf deinem Gerät läuft. Apps können mit Siri auf deine Fragen antworten oder Audio an Apple senden, um es in Text umzuwandeln – natürlich nur mit deiner Zustimmung.“ (Apple, 2019, https://www.apple.com/de/privacy/approach-to-privacy/)

Apple sendet aber auch Benutzerdaten über verschlüsselte Protokolle an den Apple-Server. Folgende Daten werden beispielsweise an den Server gesendet:

- Name
- Kontakte
- Standort
- Suchaktivitäten
- Musikaktivitäten
- Beziehungen

Welche Daten Apple bisher über einen gesammelt hat, kann der Nutzer wie folgt abfragen:

1. Über die Seite https://privacy.apple.com → Mit der Apple-ID anmelden → Eingeben der Zwei-Faktor-Authentifizierung

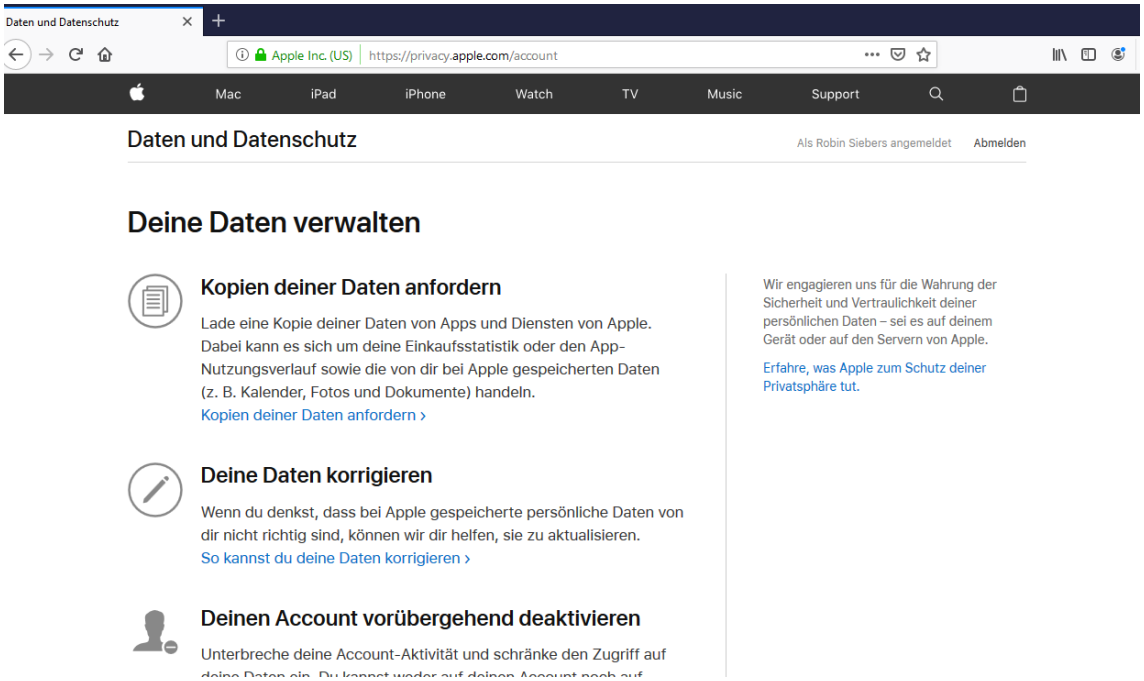



**Bild 32: Apple Daten und Datenschutz (Eigene Darstellung)**

Im Gegensatz zu Amazon Echo und Google Home kann der Nutzer sich bei Apple Siri nicht die einzelnen Sprachaufzeichnungen ansehen und gezielt löschen. Stattdessen erhält der Nutzer bei Apple über die Website https://privacy.apple.com folgende Auskunft: „Um Ihnen Kontrolle über Ihre Daten und Ihre Privatsphäre zu geben, bietet Apple Ihnen die Möglichkeit, eine Kopie der mit Ihrer Apple-ID verknüpften Daten anzufordern. Der Zugriff auf diese Funktion variiert je nach Land und Region.“ (Apple, 2019, https://support.apple.com/de-de/HT208502) Folgende Funktionen stehen dem Nutzer hier zur Verfügung: „Kopien deiner Daten anfordern“, „Deine Daten korrigieren“ „Deinen Account vorübergehend deaktivieren“ oder „Deinen Account löschen“. Der Vorgang „Kopien deiner Daten anfordern“ kann bis zu sieben Tagen dauern.

Allerdings kam es bei Apple Siri auch schon zu Datenschutzverstößen wie dieses Beispiel zeigt.

## Datenschutzvorfall

„Wie die brasilianische Apple-Seite MacMagazine herausgefunden hat, liest Siri auf Befehl allerdings alle Mitteilungen auf dem Sperrbildschirm vor - inklusive der ausgeblendeten. Insbesondere bei Messaging-Apps wie WhatsApp oder dem Facebook Messenger ist dies unter Umständen ein ärgerlicher Datenschutzfehler.“ (MacTechNews, 2018,

https://www.mactechnews.de/news/article/Privatsphaere-Fehler-Siri-liest-im-Sperrbildschirm-auch-versteckte-Mitteilungen-laut-vor-169167.html)

### 5.2.6 Ergebnis

Apple verspricht seinen Anwendern sehr auf den Datenschutz zu achten, allerdings ist auch hier vieles für den Nutzer nicht einfach nachzuvollziehen. Denn welche Daten genau wo und wann gesammelt werden, ist für den Nutzer nicht klar ersichtlich. Außerdem fehlt dem Kunden bei Apple wie bei Amazon Echo oder Google Home eine klare Übersicht, über die bereits erfassten Sprachaufzeichnungen zu verwalten und ggf. gezielt zu löschen. Ein weiteres Manko ist die fehlende Transparenz des Standortes der gesendeten Daten an die weltweit verteilten Apple-Server. Denn für den Endkunden ist völlig unklar, ob nun für seine gesendeten und gespeicherten Daten auf den Apple-Server die Datenschutzbestimmungen seines oder eines anderen Landes gelten. Zudem ist auch bekannt, dass bei Apple wie auch bei den anderen Spracherkennungssystemen Mitarbeiter oder sogar vielleicht andere Firmen Zugriff auf die Sprachaufzeichnungen haben. Anscheinend werden diese Daten genutzt, um kontinuierlich den Sprachassistenten zu verbessern und weiterzuentwickeln.

## 5.3 Analyse der Kommunikation mithilfe von Wireshark

## 5.4 Wireshark

Wireshark ist einer der beliebtesten Sicherheitswerkzeuge und ist ein kostenloses Programm zur Analyse von Netzwerkkommunikationsverbindungen. Solche Programme werden oft auch als Sniffer bezeichnet. Wireshark hat die Besonderheit, dass es für alle Plattformen Linux, Mac OS und Windows zur Verfügung steht. Die Hauptaufgabe von Wireshark ist die Fehlererkennung und Fehlerbehebung im Netzwerk sowie die Sicherheitsanalyse im Bereich Netzwerkforensik. Das Programm kann über verschiedene Schnittstellen wie USB, Ethernet oder WLAN den Datenverkehr mitschneiden und anschließend analysieren. Die Aufzeichnungen können in verschiedenen Formaten gespeichert werden. „Wireshark erkennt viele verschiedene Protokolle und stellt die wichtigsten Informationen der Protokollheader übersichtlich und leicht lesbar dar.

Das Dekodierungsverfahren von Wireshark nutzt sogenannte Dissektoren welche einzelne Werte in Frames identifizieren und anzeigen kann. Diese sind über Jahre gewachsen und können mit allen gängigen Protokollen und Applikationen umgehen.“ (Lemche, Fritsche, 2019, Fritsche-Lemche.pdf, S.4)

Für die Analyse der Aufzeichnungen bietet das Programm zahlreiche Filtermöglichkeiten z. B. Netzwerkpakete, Protokolle oder Netzwerkschichten.

## 5.5 Allgemeiner Versuchsaufbau

Bei diesem Versuch soll der Datenverkehr der verschiedenen Spracherkennungssysteme mithilfe von Wireshark aufgezeichnet werden. Folgende Datenströme sollten aufgezeichnet werden:

- Datenverkehr ohne Aktivierungswort: Hier soll untersucht werden ob bei den Sprachassistenten auch wirklich keine Kommunikation stattfindet, wenn der Anwender kein „Aktivierungswort“ spricht.
- Datenverkehr mit Aktivierungswort: Hier soll untersucht werden welche Kommunikation stattfindet, wenn der Anwender das „Aktivierungswort“ spricht.

Folgende Hardwarekomponenten und Softwarekomponenten werden hierfür benötigt:

- Spracherkennungssysteme:
  - Amazon Echo (1. Generation)
  - Google Home
  - Apple iPhone mit Siri
- WLAN-Router
- Notebook 64-bit Windows 10 (1809), build 17763
- Wireshark Version 3.0.2

Aufgrund der hier benötigten Hardwarekomponenten und Softwarekomponenten hat sich hier folgender Aufbau ergeben.

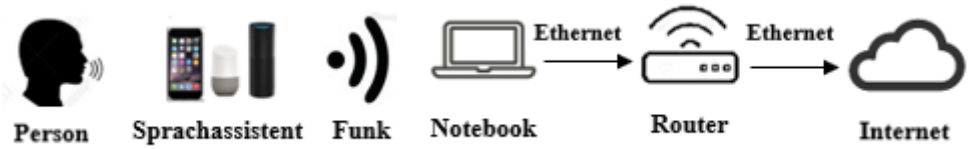



**Bild 33: Versuchsaufbau Analyse der Kommunikation der Sprachassistenten (vgl. Lemche, Fritsche, 2019, Fritsche-Lemche.pdf, S.5)**

Der Nutzer überträgt per Sprache einen Sprachbefehl an den Sprachassistenten. Der digitale Assistent leitet per WLAN (Funk) dann das Signal an den mobilen Hotspot an das Notebook. Dieser Datenverkehr kann dann mit dem auf dem Notebook installierten Analysetool Wireshark aufgezeichnet und analysiert werden. Anschließend leitet dann das Notebook die Anfrage über ein LAN-Kabel an den WLAN-Router und dieser wieder an das Internet.

## 5.6 Amazon Alexa

### 5.6.1 Datenverkehr ohne Aktivierungswort

Untersucht wird welcher Datenverkehr stattfindet, wenn der Anwender kein Aktivierungswort sagt. Alexa befindet sich quasi im Lauschmodus und wartet permanent auf das Aktivierungswort.

Zuerst erfolgt in Wireshark eine Aufzeichnung des Datenverkehrs. Der Mitschnitt wird nach einem selbst festgelegten Zeitintervall von 120 Sekunden gestoppt, um diesen besser auswerten zu können.

Anschließend erfolgt mithilfe eines Filters eine Analyse des Datenverkehrs:

**ip.src = = 192.168.137.6 || ip.dst = = 192.168.137.6 && (frame.time_relative <=120)**

Der Filter bedeutet, nur Pakete anzeigen, die von der IP-Adresse 192.168.137.6 zu einer bestimmten IP-Adresse 192.168.137.6 in einem bestimmten Zeitraum von 120 Sekunden empfangen oder gesendet werden.

Auffällig ist, dass Alexa, trotz Nichtaktivierung die ganze Zeit Daten austauscht. Immer wieder werden kleinere Pakete versendet. Wie man sehen kann, erfolgt ständig eine Kommunikation zwischen Alexa hier „Source“ mit der IP-Adresse 192.168.137.6 zu einem anderen Ort „Destination“ mit der zum Beispiel der IP-Adresse 52.95.112.20 und umgekehrt.

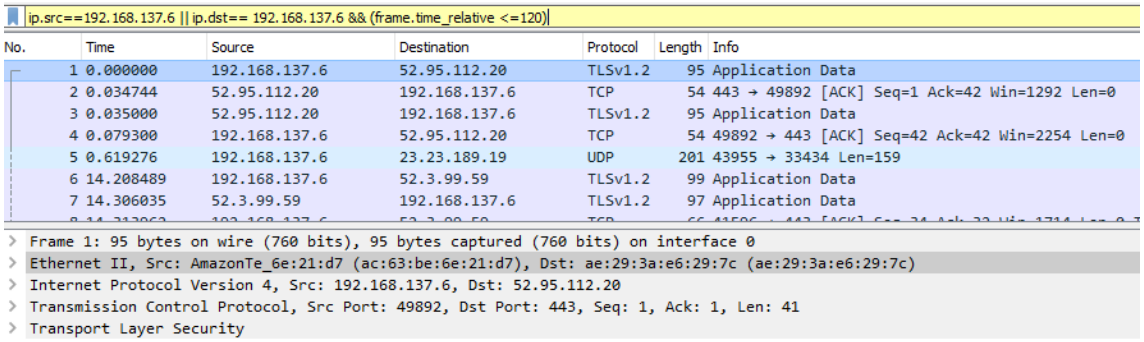



**Bild 34:Amazon Alexa Datenverkehr ohne Aktivierung (Eigenes Bild)**

Dass immer wieder Pakete versendet werden, kann man am besten mit Hilfe des I/O Graphen in Wireshark darstellen.

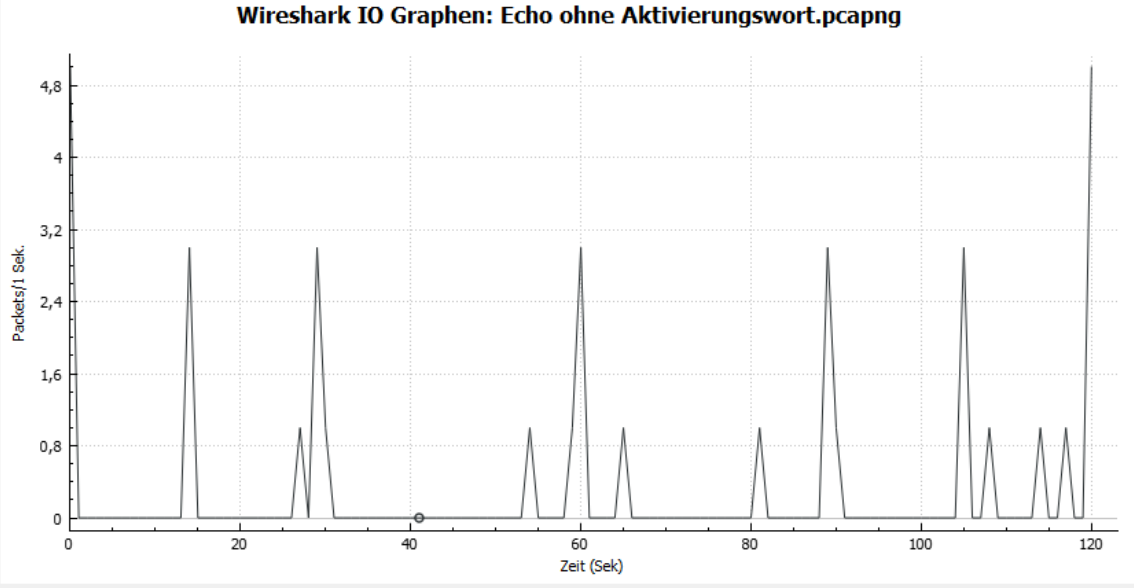



**Bild 35: Amazon Alexa I/O Graphen bei nicht Aktivierung (Eigene Darstellung)**

Der I/O Graph ist eine Übersicht über die Pakete pro Sekunde (Y-Achse) und zur Zeitmessung in Sekunden (X-Achse).

In der Mitschnittdatei kann man erkennen, dass in dem kurzen Zeitraum von 120 Sekunden 35 Pakete versendet wurden. Die durchschnittliche Paketgröße beträgt 109 Bytes und insgesamt wurden 3799 Byte versendet.

**Statistik**

| Messwerte | Aufgezeichnet | Angezeigt | Markiert |
|---|---|---|---|
| Pakete | 35 | 35 (100.0%) | — |
| Zeitspanne, s | 120.369 | 120.369 | — |
| Durchschnittliche pps | 0.3 | 0.3 | — |
| Durschnittliche Paketgröße, B | 109 | 109 | — |
| Byte | 3799 | 3799 (100.0%) | 0 |
| Durschnittliche Byte/s | 31 | 31 | — |
| Durschnittliche Bit/s | 252 | 252 | — |

**Bild 36: Amazon Alexa Mitschnittdatei ohne Aktivierung (Eigene Darstellung)**

Dabei sind die 35 Pakete wie folgt aufgeteilt:

- 9 Pakete als User Datagram Protocol (UDP)
- 26 Pakete als Transmission Control Protocol (TCP) und diese beinhalten
- 12 Pakete zur verschlüsselten Kommunikation Transport Layer Security (TLS)

Wobei die Kommunikation hauptsächlich über IPv4 erfolgt.

Ethernet · 3 | IPv4 · 5 | IPv6 | TCP · 2 | UDP · 3

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A |
|---|---|---|---|---|---|---|---|
| 192.168.137.1 | 192.168.137.255 | 1 | 243 | 1 | 243 | 0 | 0 |
| 192.168.137.1 | 239.255.255.250 | 3 | 537 | 3 | 537 | 0 | 0 |
| 23.23.189.19 | 192.168.137.6 | 5 | 1005 | 0 | 0 | 5 | 1005 |
| 52.3.99.59 | 192.168.137.6 | 6 | 524 | 2 | 194 | 4 | 330 |
| 52.95.112.20 | 192.168.137.6 | 20 | 1490 | 10 | 745 | 10 | 745 |

**Bild 37: Amazon Alexa Verbindungen ohne Aktivierung (Eigene Darstellung)**

Betrachtet man nun die Verbindungen an die Adressen, an die die Pakete versendet wurden, fällt auf, dass an die **Adresse „52.95.112.20“** die meisten Pakete, hier 20, versendet wurden. Prüft man diese Adresse zum Beispiel über die Website IP Location Finder unter https://tools.keycdn.com/geo stellt man fest, dass die meisten Pakete an einen Amazon Server nach Irland mit dem Standort Dublin versendet wurden. Aber auch die Spur der anderen Verbindungen „**23.23.189.19**“ und „ **52.3.99.59**“ führen alle zu einem Amazon Server allerdings hier der Standort USA.

| LOCATION | |
|---|---|
| City | Dublin |
| Region | Leinster (L) |
| Postal code | D02 |
| Country | Ireland (IE) |
| Continent | Europe (EU) |
| Coordinates | 53.3338 (lat) / -6.2488 (long) |
| Time | 2019-07-11 22:29:41 (Europe/Dublin) |
| NETWORK | |
| IP address | 52.95.112.20 |
| Hostname | 52.95.112.20 |
| Provider | Amazon.com, Inc. |
| ASN | 16509 |

**Bild 38: Amazon Alexa Verbindung ohne Aktivierung (Eigenes Bild)**

### 5.6.2 Ergebnis

Amazon Alexa kommuniziert auch im Lauschmodus ständig mit den weltweit verteilten Amazon Servern. Die Übertragung der Pakete findet hauptsächlich verschlüsselt über Transport Layer Security (TLS) und Secure Sockets Layer (SSL) statt. Daher war es leider nicht möglich festzustellen, welche genaue Daten übertragen werden. Aufgrund der kleinen Paketgrößen und der geringen Anzahl versendeter Pakete wird vermutlich nur laufend überprüft, wie spät es ist oder ob noch die Verbindung steht. Damit konnte nicht festgestellt werden, dass viele Daten und ungewollter Datenverkehr vorkommen. Es konnte nicht festgestellt werden, dass Gespräche, die in dieser Zeit stattfinden, an Amazon oder an andere Anbieter gesendet werden.

### 5.6.3 Datenverkehr mit Aktivierungswort

Jetzt erfolgt nun die Analyse des Datenverkehrs mit einem Aktivierungswort. Für die Analyse der Kommunikation erfolgt wieder eine Aufzeichnung des Datenverkehrs. Dieses Mal wird die Aufzeichnung kurz nach der Aktivierung nach ca. 40 Sekunden gestoppt. Für die Analyse wird die Aktivierung mit folgendem Befehl ausgeführt:

**„Alexa, berechne die Route von Stuttgart nach München“.**

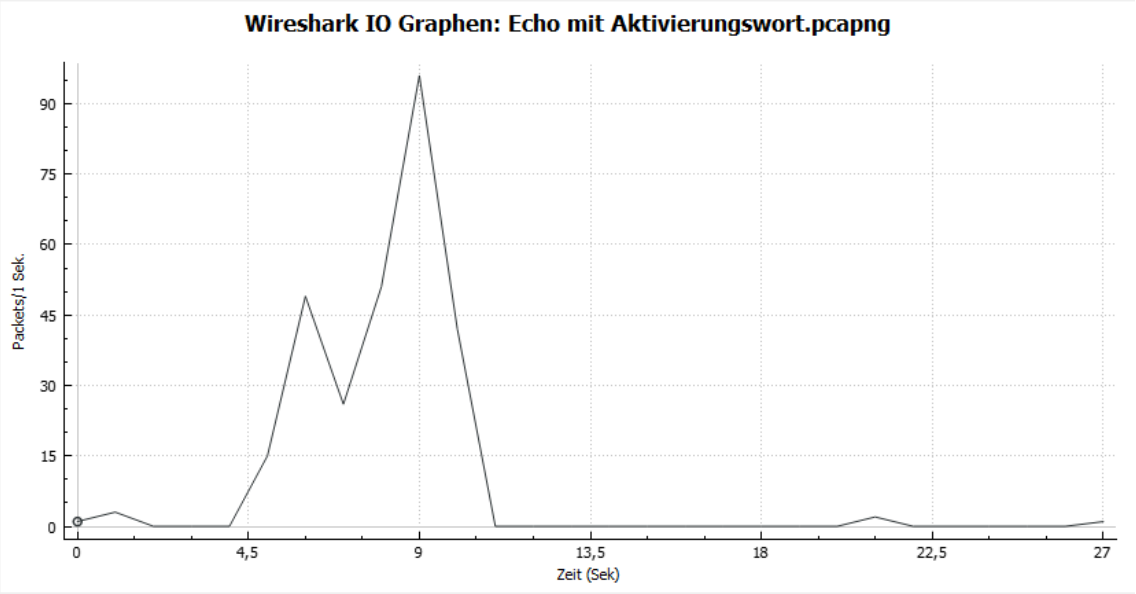



**Bild 39: Amazon Alexa I/O Graphen mit Aktivierung (Eigene Darstellung)**

Anhand des I/O Graphen kann man nun deutlich erkennen, dass bei der 4. Sekunde ein erheblicher Datenverkehr stattfindet. Dies ist der Moment, indem die Aktivierung mit dem Befehl „**Alexa, berechne die Route von Stuttgart nach München“** erfolgt und anschließend eine gesprochene Antwort generiert wird.

Interessant ist es nun zu analysieren, wieviele Pakete mit welcher Größe nun versendet wurden. Diese Werte können nun über die Mitschnittdatei ermittelt werden:

**Statistik**

| Messwerte | Aufgezeichnet | Angezeigt |
|---|---|---|
| Pakete | 286 | 286 (100.0%) |
| Zeitspanne, s | 27.027 | 27.027 |
| Durchschnittliche pps | 10.6 | 10.6 |
| Durschnittliche Paketgröße, B | 535 | 535 |
| Byte | 152893 | 152893 (100.0%) |
| Durschnittliche Byte/s | 5657 | 5657 |
| Durschnittliche Bit/s | 45 k | 45 k |

**Bild 40: Amazon Alexa Mitschnittdatei mit Aktivierung (Eigenes Darstellung)**

Im Vergleich zur Paketanzahl bei Nichtaktivierung ist die Anzahl der Pakete erheblich gestiegen. Waren es zuvor bei der Nichtaktivierung noch 35 Pakete innerhalb von 120 Sekunden, wurden hier bereits innerhalb von 27 Sekunden 286 Pakete übertragen. Die durchschnittliche Paketgröße liegt nun bei 535 Bytes und insgesamt wurden in 27 Sekunden bereits 152839 Byte versendet. Die Kommunikation erfolgt weiterhin über IPv4

und wird mit TLS verschlüsselt. Aufgrund der Verschlüsselung erfolgt hier keine weitere Analyse des Inhalts der übertragenen Daten.

Anschließend erfolgt nun eine Analyse der Verbindungen, die bei der Kommunikation hergestellt werden. Hierfür kann die Übersicht der Verbindungen betrachtet werden:

Ethernet · 1 | IPv4 · 3 | IPv6 | TCP · 2 | UDP · 1

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A |
|---|---|---|---|---|---|---|---|
| 23.23.189.19 | 192.168.137.127 | 2 | 402 | 0 | 0 | 2 | 402 |
| 34.236.103.70 | 192.168.137.127 | 3 | 262 | 1 | 97 | 2 | 165 |
| 52.95.121.236 | 192.168.137.127 | 281 | 152 k | 151 | 89 k | 130 | 62 k |

**Bild 41:Amazon Alexa Verbindungen mit Aktivierung (Eigene Darstellung)**

Die meisten Pakete, hier 281, werden an folgende IP-Adresse „52.95.121.236“ gesendet. Prüft man diese Adresse über die Website IP Location Finder unter https://tools.keycdn.com/geo, erhält man folgendes Ergebnis:

LOCATION

| | |
|---|---|
| **City** | Dublin |
| **Region** | Leinster (L) |
| **Postal code** | D02 |
| **Country** | Ireland (IE) |
| **Continent** | Europe (EU) |
| **Coordinates** | 53.3338 (lat) / -6.2488 (long) |
| **Time** | 2019-07-12 09:52:11 (Europe/Dublin) |

NETWORK

| | |
|---|---|
| **IP address** | 52.95.121.236 |
| **Hostname** | 52.95.121.236 |
| **Provider** | Amazon.com, Inc. |
| **ASN** | 16509 |

**Bild 42: Amazon Alexa Verbindung mit Aktivierung (Eigene Darstellung)**

Per Zufall werden auch hier die meisten Pakete an einen Amazon-Server in Irland gesendet. Bei den anderen zwei IP-Adressen ergaben sich folgende Ergebnisse:

Die IP-Adresse „34.236.103.70“ befindet sich in Virginia in den USA. Hier wurden anscheinend einzelne Pakete an den Amazon Web Services (AWS) versendet.

| LOCATION | |
|---|---|
| **City** | Ashburn |
| **Region** | Virginia (VA) |
| **Postal code** | 20149 |
| **Country** | United States (US) |
| **Continent** | North America (NA) |
| **Metro code** | 511 |
| **Coordinates** | 39.0481 (lat) / -77.4728 (long) |
| **Time** | 2019-07-12 04:56:19 (America/New_York) |
| NETWORK | |
| **IP address** | 34.236.103.70 |
| **Hostname** | ec2-34-236-103-70.compute-1.amazonaws.com |
| **Provider** | Amazon.com, Inc. |
| **ASN** | 14618 |

**Bild 43: Amazon Alexa Verbindung mit Aktivierung (Eigene Darstellung)**

Die IP-Adresse „23.23.189.19“ wurde bereits schon bei der Nichtaktivierung verwendet. Auch dieser ist ein Amazon Web Service (AWS) in den USA.

### 5.6.4 Ergebnis

Wie zu erwarten werden bei einer Aktivierung erheblich mehr Daten übertragen. Dies kann man an der Größe und der Anzahl der Pakete deutlich erkennen. Erneut wurden für die Kommunikation Amazon-Server in den USA und Europa verwendet. Andere Dienste von Drittanbietern mussten wohl bei dieser Anfrage nicht von Amazon in Anspruch genommen werden.

## 5.7 Google Home

### 5.7.1 Datenverkehr ohne Aktivierungswort

Für den Versuch wird der Datenverkehr ohne Aktivierungswort mit einer Zeitspanne von 120 Sekunden aufgezeichnet. Damit nur die Verbindungen von und zu Google Home besser ausgewertet werden können, wird folgender Filter in Wireshark definiert:

**ip.src = = 192.168.137.253 || ip.dst = = 192.168.137.253 && (frame.time_relative <=120)**

Man kann beobachten, dass Google Home ständig kommuniziert und kleinere Pakete an verschiedene Verbindungen auch ohne Aktivierung versendet. Eine Übersicht der versendeten Pakete in einem Zeitintervall von 120 Sekunden erhält man über den I/O Graphen.

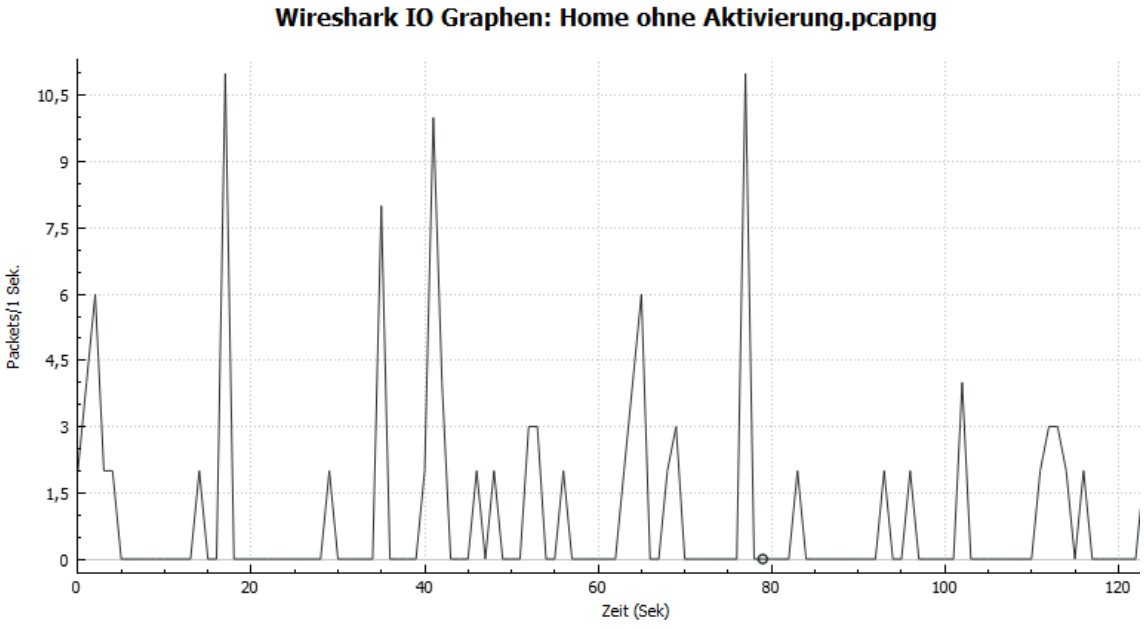



**Bild 44: Google Home I/O Graphen ohne Aktivierung (Eigene Darstellung)**

In der Mitschnittdatei ist zu sehen, dass in der kurzen Zeit von 120 Sekunden 125 Pakete versendet wurden. Die durchschnittliche Paketgröße beträgt 195 Bytes und insgesamt wurden 23046 Byte versendet.

**Statistik**

| Messwerte | Aufgezeichnet | Angezeigt | Markiert |
|---|---|---|---|
| Pakete | 125 | 113 (90.4%) | — |
| Zeitspanne, s | 126.866 | 114.939 | — |
| Durchschnittliche pps | 1.0 | 1.0 | — |
| Durschnittliche Paketgröße, B | 184 | 196 | — |
| Byte | 23046 | 22139 (96.1%) | 0 |
| Durschnittliche Byte/s | 181 | 192 | — |
| Durschnittliche Bit/s | 1453 | 1540 | — |

**Bild 45: Google Home Mitschnittdatei ohne Aktivierung (Eigene Darstellung)**

Dabei enthalten die 125 Pakete folgende Protokolle:

User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), Multicast Domain Name System (mDNS), Google Quick UDP Internet Connections (GQUIC), Domain Name System (DNS), Data und zur Verschlüsselung wird Transport Layer Security (TLS) verwendet.

Google Home kommuniziert ausschließlich im IPv4 Bereich. Anschließend können nun die einzelnen Verbindungen analysiert werden.

Ethernet · 2 | IPv4 · 7 | IPv6 | TCP · 2 | UDP · 8

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A |
|---|---|---|---|---|---|---|---|
| 192.168.137.1 | 192.168.137.253 | 12 | 1176 | 6 | 588 | 6 | 588 |
| 66.102.1.188 | 192.168.137.253 | 13 | 910 | 6 | 422 | 7 | 488 |
| 172.217.21.227 | 192.168.137.253 | 13 | 4046 | 6 | 1829 | 7 | 2217 |
| 172.217.23.163 | 192.168.137.253 | 13 | 4046 | 6 | 1829 | 7 | 2217 |
| 192.168.137.253 | 224.0.0.251 | 20 | 4879 | 20 | 4879 | 0 | 0 |
| 8.8.8.8 | 192.168.137.253 | 22 | 2048 | 11 | 1084 | 11 | 964 |
| 172.217.23.174 | 192.168.137.253 | 28 | 5773 | 14 | 1018 | 14 | 4755 |

**Bild 46: Google Home Verbindungen ohne Aktivierung (Eigene Darstellung)**

Man kann erkennen, dass an die **Adresse „172.217.23.174“** die meisten Pakete, hier 28, versendet wurden. Prüft man diese Adresse über die Website IP Location Finder unter https://tools.keycdn.com/geo, erhält man folgendes Ergebnis:

Hinter der IP-Adresse 172.217.23.174 steckt ein Google Server in den USA.

**Bild 47: Google Home Verbindung ohne Aktivierung (Eigene Darstellung)**

Die anderen relevanten IP-Adressen ergeben folgende Ergebnisse:

**Adresse „8.8.8.8“**: Hinter dieser IP-Adresse steckt ein dns.google Server in den USA.

**Adresse „172.217.23.163“**: Hinter dieser IP-Adresse steckt ein fra15s22-in-f3.1e100.net Google-Server in den USA.

**Adresse „66.102.1.188“:** Hinter dieser IP-Adresse steckt ein wb-in-f188.1e100.ne Google-Server in den USA.

### 5.7.2 Ergebnis

Die Analyse zeigt, Google Home kommuniziert auch im Ruhemodus ohne Aktivierung stetig mit anderen Google-Servern. Auffallend ist hier, dass nur mit Google-Servern in den USA kommuniziert wurde. Es wurden nur kleine Pakete versendet. Die Übertragung findet hauptsächlich verschlüsselt mit Transport Layer Security (TLS) statt. Daher war eine Analyse des Inhalts der gesendeten Daten leider nicht möglich. Aber aufgrund der Größe der Pakete nehme ich an, dass nur Grunddaten wie die Verbindung oder der Ping ständig gegengeprüft werden. Schließlich lässt sich festhalten, dass Gespräche, die ohne Aktivierung nicht an Google weiter versendet werden. Auffälliger oder ungewollter Datenverkehr konnte hiermit nicht festgestellt werden.

### 5.7.3 Datenverkehr mit Aktivierungswort

Nun wird für die Analyse Google Home mit dem Sprachbefehl **„OK Google, berechne die Route von Stuttgart nach München“** aktiviert.

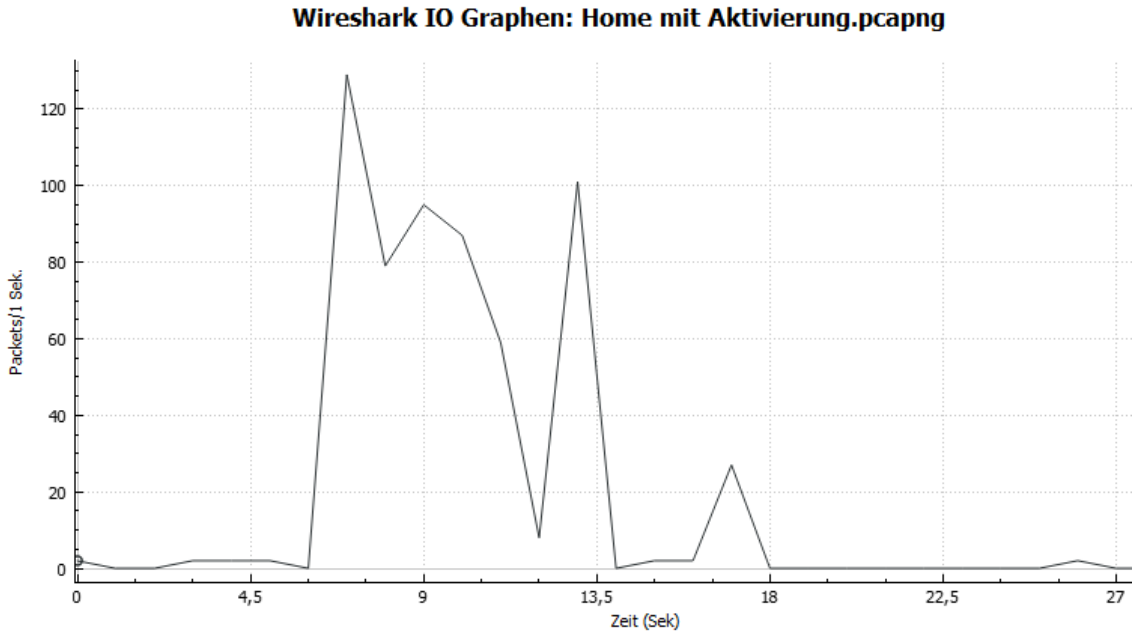



**Bild 48:Google Home I/O Graphen mit Aktivierung (Eigene Darstellung)**

Wie man beim I/O Graph nun erkennen kann, beginnt bei der 6. Sekunde die Aktivierung und somit die Aufzeichnung des Sprachbefehls. Die Anzahl der Pakete wird nun erheblich mehr. Dieser Dialog geht bis zur 14. Sekunde.

Vergleicht man nun die Anzahl der Pakete „ohne Aktivierung“ mit „Aktivierung“, ist die Anzahl der Pakete erheblich gestiegen. So wurden bei der Aktivierung bereits nach 29 Sekunden 642 Pakete übertragen, bei der Nichtaktivierung waren es zum Vergleich nach 120 Sekunden nur 125 Pakete. Die durchschnittliche Paketgröße beträgt nun 519 Byte und insgesamt wurden 332878 Byte versendet.

**Statistik**

| Messwerte | Aufgezeichnet | Angezeigt | Markiert |
|---|---|---|---|
| Pakete | 642 | 642 (100.0%) | — |
| Zeitspanne, s | 29.376 | 29.376 | — |
| Durchschnittliche pps | 21.9 | 21.9 | — |
| Durschnittliche Paketgröße, B | 519 | 519 | — |
| Byte | 332878 | 332878 (100.0%) | 0 |
| Durschnittliche Byte/s | 11 k | 11 k | — |
| Durschnittliche Bit/s | 90 k | 90 k | — |

**Bild 49: Google Home Mitschnittdatei mit Aktivierung (Eigene Darstellung)**

Die Kommunikation erfolgt hauptsächlich über IPv4 und wird mit Transport Layer Security (TLS) verschlüsselt. Daher können auch hier keine Inhalte analysiert werden. Die Verbindungen mit „Aktivierung“ haben folgendes ergeben:

Ethernet · 1 | IPv4 · 8 | IPv6 | TCP · 5 | UDP · 7

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A |
|---|---|---|---|---|---|---|---|
| 66.102.1.188 | 192.168.137.253 | 4 | 264 | 2 | 132 | 2 | 132 |
| 172.217.22.67 | 192.168.137.253 | 4 | 348 | 2 | 162 | 2 | 186 |
| 192.168.137.1 | 192.168.137.253 | 4 | 392 | 2 | 196 | 2 | 196 |
| 172.217.23.174 | 192.168.137.253 | 6 | 434 | 3 | 227 | 3 | 207 |
| 8.8.8.8 | 192.168.137.253 | 18 | 1874 | 9 | 1145 | 9 | 729 |
| 172.217.18.14 | 192.168.137.253 | 24 | 11 k | 11 | 5765 | 13 | 5255 |
| 172.217.22.74 | 192.168.137.253 | 40 | 9176 | 21 | 3424 | 19 | 5752 |
| 192.168.137.253 | 216.58.205.228 | 540 | 309 k | 285 | 217 k | 255 | 92 k |

**Bild 50:Google Home Verbindungen mit Aktivierung (Eigene Darstellung)**

Die meisten Pakete 540 wurden an die **IP-Adresse „192.168.137.253“** gesendet. Prüft man diese Adresse stößt man wieder auf einen Google-Server in den USA. Auch die Überprüfung der anderen IP-Adressen hat ergeben, dass alle Adressen zu einem Google-Server in den USA führen.

### 5.7.4 Ergebnis

Ab dem Zeitpunkt der Aktivierung werden erheblich mehr Daten wie im I/O Graph dargestellt übertragen. Bei der Übertragung der Daten konnten keine Auffälligkeiten festgestellt werden. Die Kommunikation erfolgte bei diesem Versuch hauptsächlich über Google Server in den USA. Andere Dienste mussten bei dieser Anfrage von Google nicht mit einbezogen werden. Die Kommunikation erfolgt hauptsächlich über IPv4 und ist über Transport Layer Security (TLS) verschlüsselt. Daher können die genauen Inhalte der gesendeten Daten nicht eingesehen werden.

## 5.8 Apple Siri

### 5.8.1 Datenverkehr ohne Aktivierungswort

Für diese Analyse wird der Datenverkehr ohne Aktivierungswort mit einer Zeitspanne von 120 Sekunden mitgeschnitten. Damit nur der Verkehr von und zu Siri besser ausgewertet werden kann, wird folgender Filter eingestellt:

**ip.src = =192.168.137.25 || ip.dst = = 192.168.137.25 && (frame.time_relative <=120)**

Auch bei Siri werden immer wieder kleinere Pakete auch ohne das Aktivierungswort versendet. Eine Übersicht über die Anzahl der Pakete pro Sekunde erhält man über den I/O Graphen.

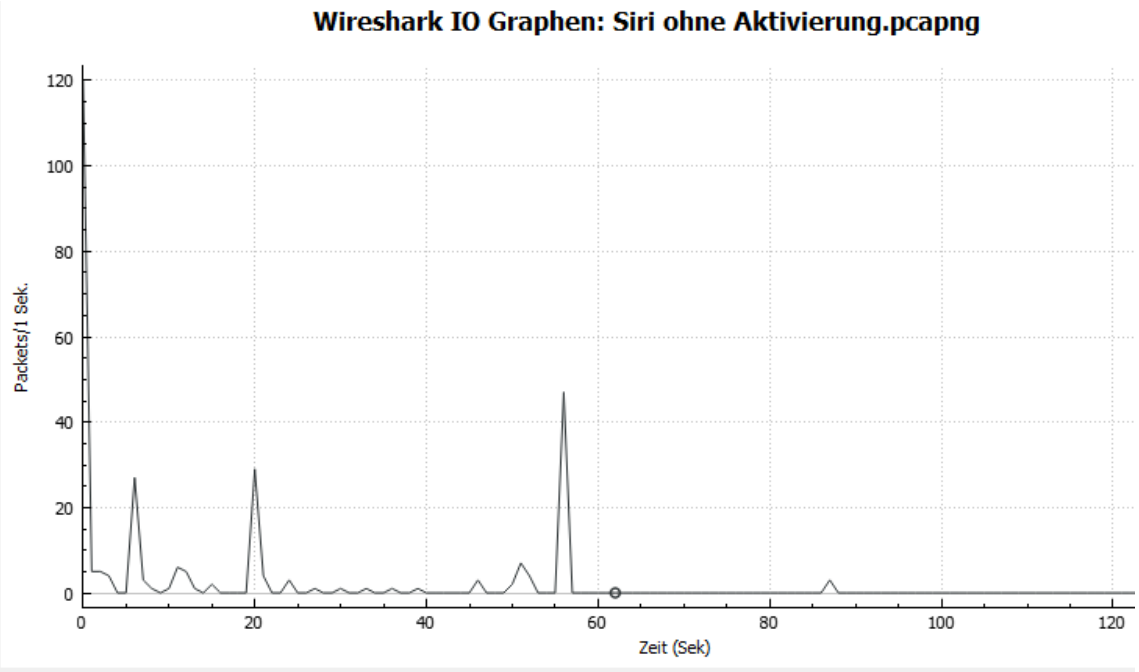



**Bild 51: Apple Siri I/O Graphen ohne Aktivierung (Eigene Darstellung)**

Die Anzahl der Pakete ist pro Sekunde sehr überschaubar. So gibt es auch Abschnitte, die keine Pakete senden. In der Mitschnittdatei ist zu erkennen, dass in der Zeit von ca. 120 Sekunden 294 Pakete versendet wurden.

**Statistik**

| Messwerte | Aufgezeichnet | Angezeigt | Markiert |
|---|---|---|---|
| Pakete | 294 | 30 (10.2%) | — |
| Zeitspanne, s | 135.313 | 78.641 | — |
| Durchschnittliche pps | 2.2 | 0.4 | — |
| Durschnittliche Paketgröße, B | 253 | 370 | — |
| Byte | 74383 | 11088 (14.9%) | 0 |
| Durschnittliche Byte/s | 549 | 140 | — |
| Durschnittliche Bit/s | 4397 | 1127 | — |

**Bild 52: Apple Siri Mitschnittdatei ohne Aktivierung (Eigene Darstellung)**

Die durchschnittliche Paketgröße ist 235 Bytes und insgesamt wurden 74383 Byte versendet. Für die Kommunikation wird hauptsächlich IPv4 verwendet. Bei den 294 Paketen wurden folgende Protokolle verwendet: User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Multicast Domain Name System (mDNS), Domain Name

System (DNS), Online Certificate Status Protocol (OCSP), Internet Group Management Protocol (IGMP), Data und zur Verschlüsselung wird Transport Layer Security (TLSv1.2 /TLSv1.3) verwendet. Um zu prüfen ob mit Adressen kommuniziert wird, die vielleicht verdächtig sind, analysiere ich nun die relevanten Verbindungen.

Ethernet · 6 | IPv4 · 13 | IPv6 · 2 | TCP · 11 | UDP · 21

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A |
|---|---|---|---|---|---|---|---|
| 192.168.137.25 | 224.0.0.2 | 1 | 46 | 1 | 46 | 0 | 0 |
| 17.164.1.38 | 192.168.137.25 | 3 | 198 | 1 | 66 | 2 | 132 |
| 17.252.28.14 | 192.168.137.25 | 5 | 359 | 2 | 185 | 3 | 174 |
| 192.168.137.1 | 239.255.255.250 | 6 | 1074 | 6 | 1074 | 0 | 0 |
| 192.168.137.25 | 224.0.0.251 | 7 | 941 | 7 | 941 | 0 | 0 |
| 93.184.220.29 | 192.168.137.25 | 10 | 1763 | 4 | 1059 | 6 | 704 |
| 185.93.236.24 | 192.168.137.25 | 19 | 9801 | 9 | 8939 | 10 | 862 |
| 17.242.57.246 | 192.168.137.25 | 28 | 8383 | 12 | 5320 | 16 | 3063 |
| 17.164.1.41 | 192.168.137.25 | 29 | 7812 | 13 | 5553 | 16 | 2259 |
| 74.125.71.109 | 192.168.137.25 | 36 | 3236 | 21 | 2137 | 15 | 1099 |
| 192.168.137.1 | 192.168.137.25 | 36 | 4224 | 18 | 2688 | 18 | 1536 |
| 17.248.146.137 | 192.168.137.25 | 37 | 12 k | 16 | 8719 | 21 | 3930 |
| 17.252.28.85 | 192.168.137.25 | 65 | 22 k | 26 | 9160 | 39 | 13 k |

**Bild 53: Apple Siri Verbindungen ohne Aktivierung (Eigene Darstellung)**

Prüft man diese Adressen über die Website IP Location Finder unter https://tools.keycdn.com/geo, erhält man folgende Ergebnisse**:**

**Adresse „17.252.28.85“**: An diese Adresse wurden die meisten Pakete, hier 65, gesendet. Prüft man diese Adresse erfährt man, dass dies eine Verbindung zu Apple in den USA ist.

**Adresse „17.248.146.137“:** Hinter dieser IP-Adresse steckt ein Apple-Server in Deutschland in Frankfurt am Main.

**Adresse „17.242.57.246“:** Es handelt sich hierbei um eine Verbindung zu Google in den USA.

### 5.8.2 Ergebnis

Bei Nichtaktivierung von Siri erfolgt trotzdem eine geringe Kommunikation mit verschiedenen Verbindungen. Die meiste Kommunikation findet mit Apple-Servern in den USA oder Deutschland statt. Es konnte aufgrund der Paketgrößen und Anzahl der Pakete

kein unerwünschter Datenverkehr festgestellt werden. Der meiste Datenverkehr beruht wahrscheinlich darauf, Zertifikate oder die bestehende Verbindung zu prüfen. Die übertragenen Pakete sind mit Transport Layer Security (TLS) verschlüsselt und können daher nicht näher ausgewertet werden. Es konnte nicht festgestellt werden, dass Audiomitschnitte, bevor Siri aktiviert wird, an Apple-Server übertragen werden.

### 5.8.3 Datenverkehr mit Aktivierungswort

Als nächstes erfolgt die Analyse des Datenverkehrs mit folgender Aktivierung:

**„Hey Siri, berechne die Route von Stuttgart nach München“**

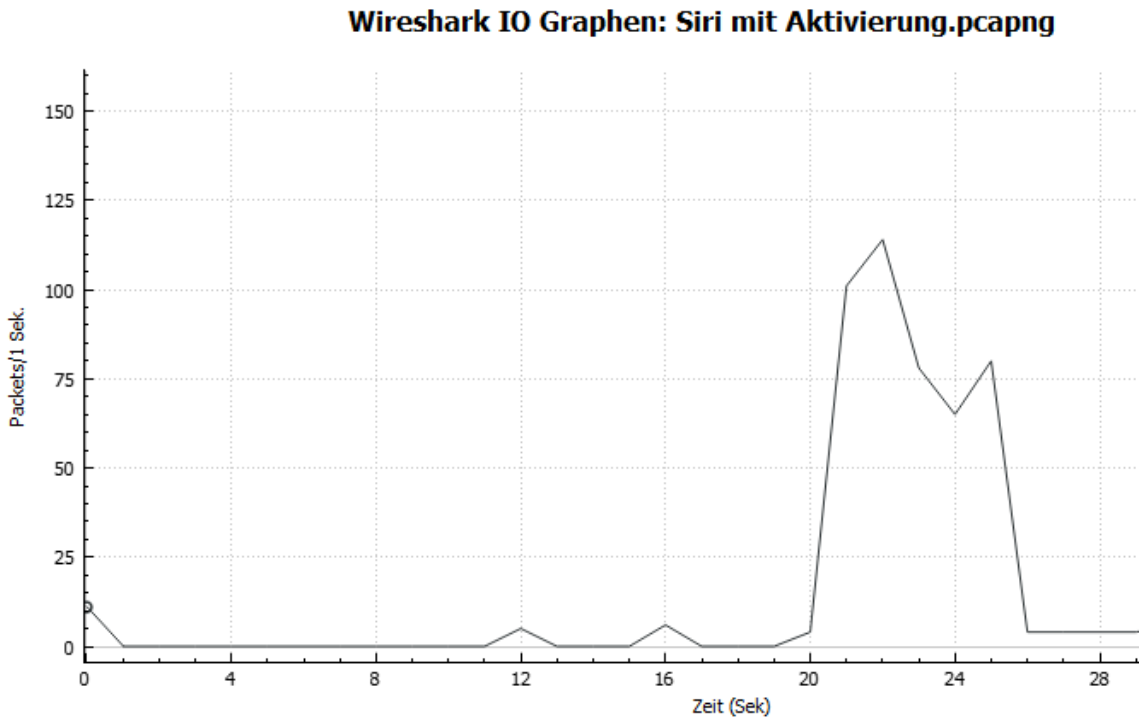



**Bild 54: Apple Siri I/O Graphen mit Aktivierung (Eigene Darstellung)**

Beim I/O Graphen kann man nun gut erkennen, dass ab der 20. Sekunde der Datenverkehr zunimmt. Dies hängt damit zusammen, dass ab der 20. Sekunde bis zu 26. Sekunde der Sprachbefehl verarbeitet und an den entsprechenden Apple-Server zur Bearbeitung versendet wird. Zudem resultiert daraus wie man bei der Mitschnittdatei gut erkennen kann, ein Anstieg der Pakete von 294 Pakete bei der Nichtaktivierung auf 872 Pakete bei der Aktivierung.

Die durchschnittliche Paketgröße hat sich nun auf 323 Bytes geändert und insgesamt wurden 281652 Byte versendet.

**Statistik**

| Messwerte | Aufgezeichnet | Angezeigt | Markiert |
|---|---|---|---|
| Pakete | 872 | 872 (100.0%) | — |
| Zeitspanne, s | 35.022 | 35.022 | — |
| Durchschnittliche pps | 24.9 | 24.9 | — |
| Durschnittliche Paketgröße, B | 323 | 323 | — |
| Byte | 281652 | 281652 (100.0%) | 0 |
| Durschnittliche Byte/s | 8042 | 8042 | — |
| Durschnittliche Bit/s | 64 k | 64 k | — |

**Bild 55: Apple Siri Mitschnittdatei mit Aktivierung (Eigene Darstellung)**

Die Kommunikation erfolgt hauptsächlich über IPv4 und wird mit Transport Layer Security (TLS) verschlüsselt.

Ethernet · 1 | IPv4 · 8 | IPv6 | TCP · 13 | UDP · 4

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | F |
|---|---|---|---|---|---|---|---|---|
| 192.168.137.1 | 192.168.137.252 | 8 | 877 | 4 | 540 | 4 | 337 | 2 |
| 104.102.19.241 | 192.168.137.252 | 11 | 795 | 6 | 422 | 5 | 373 | ( |
| 17.167.194.230 | 192.168.137.252 | 12 | 741 | 5 | 301 | 7 | 440 | 1 |
| 17.253.57.205 | 192.168.137.252 | 16 | 2807 | 6 | 1046 | 10 | 1761 | 2 |
| 104.102.19.87 | 192.168.137.252 | 29 | 10 k | 13 | 8361 | 16 | 2110 | 3 |
| 104.102.18.41 | 192.168.137.252 | 38 | 22 k | 19 | 19 k | 19 | 2604 | 3 |
| 17.252.82.47 | 192.168.137.252 | 320 | 154 k | 166 | 103 k | 154 | 50 k | 2 |
| 17.130.74.5 | 192.168.137.252 | 438 | 89 k | 219 | 36 k | 219 | 52 k | 1 |

**Bild 56: Apple Siri Verbindungen mit Aktivierung (Eigene Darstellung)**

Prüft man nun die wichtigsten Verbindungen ergeben sich folgende Ergebnisse:

**Adresse „17.130.74.5“:** An diese Adresse werden die meisten Pakete 438 gesendet. Hierbei handelt es sich um einen Apple-Server in den USA.

**Adresse „104.102.18.41“:** Es handelt sich hierbei um eine Verbindung zu der Firma Akamai Technologies, Inc. Hostname: a104-102-18-41.deploy.static.akamaitechnologies.com in Holland. Akamai ist ein Dienst für eine bessere Lastverteilung von Web-Inhalten.

Bei den anderen IP-Adressen ergaben sich keine Auffälligkeiten, meistens sind dies Verbindungen zu Apple-Servern in den USA oder Europa.

### 5.8.4 Ergebnis

Auffallend ist bei dieser Aktivierung, dass es neben den neuen Verbindungen, die alle auf Apple-Servern in den USA oder Europa verarbeitet werden, drei neue Verbindungen gibt. Die neuen Verbindungen weisen auf eine Kommunikation mit der Firma Akamai Technologies in Holland hin. Welche Informationen und Daten hier genau und zu welchem Zweck an diese Firma gesendet werden, konnte aufgrund der Verschlüsselung nicht herausgefunden werden. Allerdings benötigt die Firma laut Recherche für ihre Dienste personenbezogene Daten von den Anwendern wie IP-Adresse und Zeitpunkt.

.

# 6 Bewertung der Spracherkennungssysteme

Das folgende Kapitel enthält einen Überblick der wichtigsten Einsatzmöglichkeiten der Sprachassistenten. Darüber hinaus werden für die Spracherkennungssysteme Stärken und Schwächen formuliert.

## 6.1 Einsatzmöglichkeiten der Spracherkennungssysteme

### 6.1.1 Amazon Alexa

**Musik und Radio**

Amazon Echo unterstützt folgende Musik-Streaming-Dienste: TuneIn, Amazon Music Unlimited, Amazon Prime Music, Spotify, und Deezer. Da Amazon Echo mit dem Amazon-Konto verknüpft ist, besteht die Möglichkeit auf die eigene Amazon Music-Bibliothek zuzugreifen. Amazon-Prime Kunden können zudem auf über 2 Millionen Songs, Radiosender und ausgewählte Playlists zugreifen.

- „Alexa, spiel Musik von [Interpret]“
- „Alexa, spiele [Sendername] auf TuneIn.“

Zudem ist eine Bluetooth-Verbindung mit Boxen oder mobilen Geräten möglich.

**Kalender**

Alexa kann mit folgenden Kalendern verknüpft werden: Apple iCloud, Google-Kalender, Microsoft Office 365, Microsoft Outlook.com oder Microsoft Exchange. Es können per Sprache Termine eingetragen oder Erinnerungen hinzugefügt werden. Das Verknüpfen von mehreren Kalendern ist ebenfalls möglich.

- „Alexa, füge einen Termin zu meinem Kalender hinzu.“
- „Alexa, erinnere mich daran, am [Wochentag] um [Uhrzeit] [geplante Tätigkeit]“

**Übersetzung**

Übersetzungen von Wörtern und kurzen Sätzen sind in mehr als 50 Sprachen möglich.

- „Alexa, frage PONS was heißt [Wort] auf englisch?“

**Wecker und Timer**

Per Sprachbefehl oder Alexa-App lassen sich Wecker oder Timer einstellen.

- „Alexa, welche Wecker sind für morgen eingestellt?“
- „Alexa, welche Timer sind eingestellt?“

**Anrufe und Nachrichten oder Drop In**

Mit Alexa ist es möglich, Anrufe zu tätigen oder Sprachnachrichten an Freunde oder Familienangehörige zu senden. Voraussetzung für das Tätigen von Anrufen und Nachrichten ist, dass die Kontakte die Alexa-App oder ein unterstützendes Echo-Gerät besitzen. Drop In ist eine Funktion, um sich mit anderen Echo-Geräten zuhause zu verbinden.

- „Alexa, ruf Peter an.“
- „Alexa, sende eine Nachricht an Papa.“
- „Alexa, Drop In in der Küche.“

**Wetter**

Dank Alexa ist es möglich, per Sprachbefehl jederzeit das momentane Wetter, Vorhersagen, Informationen über einen bestimmten Ort abzufragen.

- „Alexa, wie ist das Wetter?“
- „Alexa, wird es morgen regnen?“

**Hörbücher**

Verknüpft man Alexa mit Audible hat man Zugriff auf mehr als 200.000 Hörspiele und Hörbücher.

- „Alexa, spiele das Hörbuch [Titel] ab.“
- „Alexa, mein Hörbuch fortsetzen.“

**Smart-Home**

Alexa bietet die Möglichkeit, Smart Home Geräte wie: Glühbirnen, Kameras, Thermostate, Stecker, Schalter, Türschlösser zu steuern. Es können auch Routinen erstellt werden. Routinen erlauben es, eine Abfolge bestimmter Aktionen mit nur einem Befehl zu steuern, z.B. das Türschloss öffnen oder das Licht anmachen.

- „Alexa, schalte das Licht im Flur an."
- „Alexa, schalte die Kaffeemaschine ein."

**Nachrichten und Informationen**

Jederzeit können aktuelle Top-Nachrichten von Nachrichtenanbietern abgerufen werden.

- „Alexa, was ist in den Nachrichten?"
- „Alexa, was gibt es Neues?"

**Einkaufen oder Einkaufslisten erstellen**

Alexa kann mittels Sprachbefehl im Amazon Online-Shop einkaufen oder auf Wunsch Einkauflisten erstellen. Zudem können To-do-Listen angelegt und abgefragt werden.

- „Alexa, füge „Butter" zur Einkaufsliste hinzu."
- „Alexa, bestelle [Artikel]."

**Fragen und Antworten und Unterhaltung**

Alexa kann aber auch auf eine Vielzahl von verschiedenen Fragen beantworten. So kann Alexa für das Allgemeinwissen genutzt werden oder für Spiele, Spaß und für Rezepte.

- „Alexa, schlag mir ein Rezept vor."
- „Alexa, erzähle mir einen Witz."

### 6.1.2 Google Home

**Alltags-Infos**

Google Home kann auch Fragen beantworten, die für den Alltag nützlich sind. So kann er behilflich sein beim: Rechnen, Übersetzen oder bei Wissensfragen.

- „OK Google, was ist die Hauptstadt von Kanada?“
- "OK Google, was sind 12 % von 86?“

**Einkaufsliste**

Die Einkaufslisten-Funktion von Google Home bzw. Google Assistant kann genutzt werden, um Einkaufslisten zu erstellen. Per Sprachbefehl können so Artikel hinzugefügt oder es erfolgt eine Abfrage was auf der Liste steht.

- „OK Google, was steht auf meiner Einkaufsliste?“
- „OK Google, füge Brot auf meine Einkaufsliste hinzu.“

**Anruf-Funktion**

Mit Google Home können Anrufe über das WLAN gestartet werden. Damit dies funktioniert, muss der Google Assistant auf die im Google-Account gesicherten Kontakte zugreifen können.

- „OK Google, Peter Müller anrufen.“
- „OK Google, rufe Restaurant [Name] an.“

**Erinnerungen**

Per Sprachkommando können Erinnerungen erstellt werden.

- „OK Google, erinnere mich um (Uhrzeit) an (Termin).“
- „OK Google, erinnere mich daran, im Supermarkt Wasser zu kaufen.“

**Nachrichten hören**

Mit der Nachrichten-Funktion von Google Home kann man die wichtigsten Schlagzeilen oder Nachrichten abfragen. Über die Google-Home App können verschiedene Nachrichtenquellen definiert werden.

- „OK Google, ich möchte die Nachrichten hören."
- „OK Google, lies mir die Nachrichten vor.“

**Wetter**

Bei Google Home erhält man per Sprachbefehl Wettervorhersagen.

- „OK Google, welche Temperatur ist draußen?“
- „OK Google, wie ist das Wetter in Bremen?“

**Timer und Wecker**

Google-Home bietet eine Weck- und eine Timer-Funktion. Die Timer-Funktion kann vor allem beim Kochen hilfreich sein.

- „OK Google, wecke mich um 09.30 Uhr.“
- „OK Google, setze einen Timer von 15 Minuten.“

**Kalender**

Die Kalender-Funktion von Google Home setzt einen Zugriff auf persönliche Ergebnisse voraus. Es können Kalendereinträge vom Google Kalender, importierte und iCal-Kalender abgerufen werden. Termine können auch per Sprachbefehl eingetragen werden.

- „OK Google, trage einen neuen Termin ein.“
- „OK Google, mein nächster Termin.“

**Route und Reiseinformationen**

Die Route-Funktion von Google Home kann genutzt werden, um den Weg zur Arbeit berechnen zu lassen oder die Verkehrslage zu prüfen. Es können aber auch Infos zu einer anstehenden Reise abgerufen werden. So ist es möglich, Infos zu Flügen, Buchungen oder Flugpreise zu erhalten.

- „OK Google, wie weit ist Prag entfernt?“
- „OK Google, wann landet FR1708?“

**Infos zu lokalen Geschäften**

Über diese Funktion können die Öffnungszeiten lokaler Geschäfte abgerufen werden.

- „OK Google, welche Apotheke hat geöffnet?“
- „OK Google, hat der Zoo geöffnet?“

**Abläufe/Routinen**

Abläufe oder Routinen ermöglichen es, mehrere Befehle zu kombinieren und per Sprachbefehl auszuführen.

- „OK Google, wenn es Wochentag X um Y Uhr ist, dann führe die Routine Z aus.“

**Musik-Streaming**

Mit Google Home kann man Musik hören. Google Home unterstützt folgende Musik-Streamingdienste: Spotify, Google Play Musik und Deezer.

- „OK Google, spiele Musik.“
- „OK Google, was läuft gerade?“

Zudem ist es möglich, Google Home als Bluetooth Lautsprecher zu nutzen.

**Sprachnachrichten versenden**

Sprachnachrichten können bei Google Home von einem Google-Lautsprecher zu einem anderen innerhalb desselben WLAN-Netzwerkes versendet werden.

- „OK Google, Nachricht an alle: Es gibt Kuchen."
- „OK Google, Nachricht an alle: Könnt ihr bitte ins Kinderzimmer kommen."

**Serien, Filme und Videos abspielen**

Über Google Home ist die Wiedergabe von Serien und Filmen per Sprachbefehle sowie das Starten und Steuern möglich. Dies gilt für alle TV-Geräte mit Chromecast.

- „OK Google, spiele [Filmtitel] auf dem Fernseher ab."
- „OK Google, nächste Folge."

**Smart-Home-Geräte bedienen**

Smart-Home-Geräte können über die App mit Google Home verbunden und per Sprachbefehl gesteuert werden.

- „OK Google, ändere die Farbe von [Lichtname] zu gelb."
- „OK Google, schalte [Lichtname] ein."

**Entspannen mit Google Home**

Man kann zwischen verschiedenen Geräuschen wie Meeresrauschen oder Waldgeräuschen wählen, um abzuschalten.

- „OK Google, spiele Regengeräusche."
- „OK Google, spiele Feuergeräusche."

**Unterhaltung**

Google-Home bietet auch Spaßfunktionen mit der man verschiedene Spiele spielen kann.

- „OK Google, spiele ein Quiz."
- „OK Google, singe ein Lied."

### 6.1.3 Apple Siri

**Anrufe und Nachrichten**

Mit Siri können Anrufe getätigt oder Nachrichten versendet werden.

- „Hey Siri, rufe Thomas an."
- „Hey Siri, sende eine Nachricht an Petra."

**Aufgaben und Erinnerungen**

Per Sprachbefehl können Aufgaben oder Erinnerungen festgelegt werden.

- „Hey Siri, zeige mir Aufgaben an, die für heute anstehen."
- „Hey Siri, erinnere mich: Büro anrufen."

**Wecker und Timer**

Siri bietet eine Weck-Funktion und eine Timer-Funktion.

- „Hey. Siri, wecke mich um 10 Uhr."
- „Hey Siri, stelle den Timer auf 10 Minuten."

**Kalender und Termine**

Siri kann dazu benutzt werden, Kalenderdaten abzurufen oder Termine einzutragen.

- „Hey Siri, wann ist mein nächster Termin?"
- „Hey Siri, zeige mir den Kalender."

**Musik**

Mit Siri ist es möglich, Musik zu hören oder eine Playlist zu erstellen. Dazu wird ein Apple-Music-Abonnement benötigt. Besitzt man kein Apple-Music-Abonnement kann Siri Musik aus der eigenen Mediathek abspielen.

- „Hey Siri, spiele meine Musik."
- „Hey Siri, spiele die Top-10-Songs von Deutschland."

**Smart-Home**

Dank Siri können Smart-Home Geräte gesteuert werden.

- „Hey Siri, schalte das Licht an."
- „Hey Siri, stelle die Temperatur auf 16 °C ein."

**Fragen und Antworten**

Siri kann auch genutzt werden, um allgemeine Fragen zu stellen.

- „Hey Siri, rechne 10 plus 10."
- „Hey Siri, werfe eine Münze."

**System**

Siri kann aber auch verwendet werden, um gewisse Systemeinstellungen auf dem Smartphone zu konfigurieren.

- „Hey Siri, schalte WLAN an."
- „Hey Siri, maximale Display-Helligkeit."

**Suchfunktion**

Siri kann helfen bestimmte Sachen, Personen oder Kontakte zu finden.

- „Hey Siri, zeig mir meine Fotos aus Italien.“
- „Hey Siri, wo ist Tom?“

**Börse**

Mit Siri können Aktienkurse und Börseninformationen einfach abgerufen werden.

- „Hey Siri, wie steht der DAX?“
- „Hey Siri, Aktienkurs von Google.“

**Karten und Navigation**

Siri kann für die Routenberechnung oder Navigation genutzt werden.

- „Hey Siri, wo ist das nächste Freibad?“
- „Hey Siri, zeige mir eine Route von Hamburg nach Hannover.“

**Wetter**

Siri kann Wetterinformationen abfragen.

- „Hey Siri, wie wird das Wetter am Freitag?“
- „Hey Siri, ist es heute windig?“

## 6.2 Bewertung ausgewählter Spracherkennungssysteme

### 6.2.1 Amazon Alexa

**Tabelle 5: Amazon Echo (1. Generation) Alexa Stärken und Schwächen (Eigene Darstellung)**

| Stärken | Schwächen |
|---|---|
| **Datenschutz:** Die Sprachaufzeichnungen können abgerufen und gelöscht werden. | **Abhängigkeit:** Sprachassistent ist abhängig von WLAN-Verbindung und Netzteil. |
| **Konfiguration:** Der Amazon Echo kann per Alexa-APP oder Browser leicht eingerichtet werden.. | **Bluetooth:** Kann nicht deaktiviert werden. |
| **Multimedia Bluetooth-Fähigkeit:** Bluetooth-Verbindung mit Boxen oder mobilen Geräten möglich. | **Datenschutz:** Amazon nimmt sich das Recht jederzeit Alexa zu ändern oder den Dienst abzuschalten. |
| **Multimedia-Dienste**: Amazon Music, Prime Music, TuneIn, Audible, Spotify, Amazon Fire-TV, Deezer, YouTube, Netflix. | **Datenschutz:** Personenbezogene Daten werden gesammelt und auf weltweiten Servern gespeichert und ggf. an Dritte weitergegeben. |
| **Shopping:** Einkaufen per Sprachbefehl | **Datenschutz:** Sprachaufzeichnungen werden unbefristet gespeichert. |
| **Sicherheit:** Die Kommunikation findet hauptsächlich verschlüsselt über SSL oder TLS statt. | **Sicherheit:** Der Einkauf ist mit PIN geschützt, dieser kann aber von jedem in der Nähe mitgehört werden. |
| **Sicherheit:** Über die Mikrofon-Aus-Taste kann der Sprachassistent deaktiviert werden. | **Sicherheit:** Schwierigkeit mit eindeutiger Stimmerkennung und ähnlich klingende Aktivierungswörter. |
| **Skills**: In Deutschland stehen über 9.400 Skills von Drittanbietern zur Verfügung. Weltweit sind es 50.000. | **Sicherheit:** Gefahr von Aktivierung von unsicheren Skills die Gespräche abhören können. |
| **Smart-Home-Kooperationen:** Samsung SmartThings, Insteon, Ecobee, Phillips Hue, August Smart Lock | **Skills:** Konfiguration nur in englischer Sprache möglich. |
| **Status**: Der Status einer Anfrage wird mithilfe eines Lichtringes in verschiedenen Farben dargestellt. | **Sprachassistent:** Derzeit gibt es keine Möglichkeit die Alexa Stimme in eine männliche Stimme zu ändern. |
| **Updates:** Per Online-Update automatisch. | **Sprachassistent:** Nicht transportabel also mobil einsetzbar. |
| **Sprachassistent:** Alexa steht in mehreren Sprachen zur Verfügung**.** | **Sicherheit:** Das Aufwachwort ist nicht frei definierbar. |

| Stärken | Schwächen |
|---|---|
| **Reichweite:** Die 7 integrierten Mikrofone erlauben auch Sprachbefehle aus großer Entfernung wie z.B. Nebenzimmer. | **Sprachassistent:** Folgefragen noch nicht möglich. |
| **Smart-Home:** Automatisierungsdienst „ If this then that “ (IFTTT) möglich. | **Smart-Home:** Leider ist beim Amazon Echo (1. Generation) keine Bridge vorhanden. Bei diesem Model ist man auf externe Bridge angewiesen. (Beim Amazon Echo Plus ist eine Bridge integriert) |

### 6.2.2 Google Home

**Tabelle 6: Google Home Stärken und Schwächen (Eigene Darstellung)**

| Stärken | Schwächen |
|---|---|
| **Actions:** Die meisten Actions werden kostenlos angeboten. | **Actions:** Konfiguration nur in englischer Sprache möglich |
| **Actions:** Können leicht selber entwickelt werden. | **Actions:** Geringe Auswahl von Google-Actions weltweit nur ca. 4.000. |
| **Actions:** Können über Sprachbefehl aktiviert werden. | **Bluetooth:** Kann nicht deaktiviert werden |
| **Basis:** Auswechselbare Basis in verschiedenen Farben. | **Datenschutz:** Sprachaufzeichnungen werden unbefristet gespeichert. |
| **Datenschutz:** Die Sprachaufzeichnungen können abgerufen und gelöscht werden. | **Datenschutz:** Personenbezogene Daten werden erfasst und gespeichert und ggf. an Dritte weitergegeben. |
| **Google Assistant:** Erkennt Folgefragen | **Dienste:** Es können keine Apple Dienste wie Apple Musik integriert werden. |
| **Konfiguration**: Google Home kann per Google-Home App sehr leicht eingerichtet werden. | **Einkaufen:** Momentan ist das Einkaufen per Sprachbefehl nur in den USA möglich |
| **Multimedia-Dienste**: Google Play Musik, TuneIn, Spotify, Deezer, YouTube Musik, Netflix. | **Konfiguration:** Leider besteht keine Möglichkeit den Google Home per Browser am PC einzurichten. |
| **Sicherheit:** Die Kommunikation findet hauptsächlich verschlüsselt über SSL oder TLS statt. | **Mobilität:** Der Google-Home ist nicht mobil tragbar sondern muss immer per Netzteil angeschlossen sein. |
| **Smart-Home:** Automatisierungsdienst „ If this then that “ (IFTTT) möglich. | **Sicherheit:** Anfällig auf ähnlich klingende Aufwachwörter und keine eindeutige Stimmerkennung. |
| **Smart-Home-Kooperationen:** Bis zu 10.000 verschiedene Geräte sind kompatibel. (Belkin, Nest, Philips Hue etc.) | **Sicherheit:** Abhängigkeit von einer WLAN-Verbindung und Netzteil. |
| **Status**: Der Status einer Anfrage wird mithilfe einer Leuchtanzeige in verschiedenen Farben dargestellt. | **Sicherheit:** Das Aufwachwort kann nicht frei definiert werden. |

| Stärken | Schwächen |
|---|---|
| **Multimedia Bluetooth-Fähigkeit**: Bluetooth-Verbindung mit Boxen oder mobilen Geräten möglich. | **Dienste:** Für viele Dienste ist ein kostenpflichtiger Account notwendig. |
| **Sprachassistent:** Ausführliche Antworten, da hier auf die Google Suche zugegriffen wird. | **Reichweite:** Sprachbefehle aus einer weiteren Entfernung werden manchmal gar nicht verstanden. |
| **Sprachassistent:** Auswahl männliche oder weibliche Stimme. | **Sicherheit:** Actions können heimlich für andere Zwecke verwendet werden. |
| **Sprachassistent:** Google Assistant steht in mehreren Sprachen zur Verfügung**.** | **Sicherheit:** Zugriff auf inoffizielle Schnittstelle möglich. |
| **Sicherheit:** Google Assistant kann per Stummschalttaste für Mikrofon deaktiviert werden. | **Smart-Home:** Keine integrierte Bridge vorhanden. Man ist auf externe Bridge angewiesen. |
| **Updates:** Per Online-Update automatisch. | **Übersicht Actions:** Es gibt keine Filterfunktion auf der Website welche Actions für den Google-Home eingesetzt werden können. |

### 6.2.3 Apple Siri

**Tabelle 7: Apple Siri Stärken und Schwächen (Eigene Darstellung)**

| Stärken | Schwächen |
|---|---|
| **Konfiguration**: Siri kann über das Smartphone sehr leicht eingerichtet werden. | **Dienste:** Für viele Dienste ist ein kostenpflichtiger Account notwendig. |
| **Multimedia Bluetooth-Fähigkeit**: Bluetooth-Verbindung mit Boxen oder mobilen Geräten möglich. | **Datenschutz:** Die Sprachaufzeichnungen können nicht einzeln abgerufen und gelöscht werden. |
| **Sicherheit:** Bluetooth kann über die Einstellungen manuell deaktiviert werden. | **Datenschutz:** Sprachaufzeichnungen werden bis zu 2 Jahre gespeichert |
| **Sicherheit:** Die Kommunikation findet hauptsächlich verschlüsselt über SSL / TLS statt. | **Datenschutz:** Sprachaufzeichnungen werden teilweise von Mitarbeitern abgehört und ausgewertet. |
| **Sicherheit:** Siri kann nur in Bezug mit einer Stimmerkennung aktiviert werden**.** | **Datenschutz:** Siri könnte ungewollt über den Sperrbildschirm versteckte Mitteilungen laut vorlesen. |
| **Sicherheit:** Siri nicht mit Apple-ID verknüpft, sondern mit zufälliger Kennung. | **Datenschutz:** Personenbezogene Daten werden erfasst und gespeichert und ggf. an Dritte weitergegeben. |
| **Smart-Home-Kooperationen:** Über HomeKit können zahlreiche Apple zertifizierte Geräte angebunden werden. | **Multimedia-Dienste**: Apple erlaubt nur eigene Dienste wie Apple Music. Fremde Anbieter können nicht genutzt werden. |
| **Sprachassistent:** Siri erkennt Folgefragen | **Smart-Home:** Keine integrierte Bridge vorhanden. Man ist auf externe Bridge angewiesen. |

| Stärken | Schwächen |
|---|---|
| **Sprachassistent:** Siri ist mobil einsetzbar | **Sicherheit:** Gefahr von Aktivierung von Siri mit ähnlich klingendem Aufwachwort. |
| **Sprachassistent:** Siri kann jederzeit über die Einstellungen deaktiviert werden. | **Sicherheit:** Probleme mit ähnlich klingenden Stimmen. |
| **Sprachassistent:** Siri steht in mehreren Sprachen zur Verfügung**.** | **Sicherheit:** Das Aufwachwort kann nicht frei definiert werden. |
| **Smart-Home:** Automatisierungsdienst „ If this then that " (IFTTT) möglich | **Status**: Der Status einer Anfrage wird nicht klar mit einem Leuchtring angezeigt. |
| **Sprachassistent: D**ie Siri-Stimme kann nach Geschlecht. (männlich oder weiblich) eingestellt werden. | **Sicherheit:** Abhängigkeit von einer WLAN-Verbindung |
| **Updates:** Online-Update können manuell oder automatisch ausgeführt werden. | **Sicherheit:** Manipulierter Kurzbefehl könnte Zugriff auf sensible Daten vom iPhone erhalten. |

# 7 Zusammenfassung und Ausblick

In fast allen Science-Fiction-Filmen ist es ein fester Bestandteil, dass sich Maschinen mit Menschen unterhalten können. Was noch als unvorstellbar galt, ist heute schon Realität. Dank neu entwickelter Technologien gibt es heutzutage verschiedene Anwendungen die benutzt werden können. Gerade im Bereich des automatischen Verstehens von gesprochener Sprache, hat es in den vergangenen Jahren eine erhebliche Weiterentwicklung gegeben. So gibt es inzwischen Smartphones mit Sprachsteuerung wie Siri oder Smart Speaker mit Intelligenten Persönlichen Assistenten (IPA) wie Alexa oder Google Assistant. Die Kommunikation mit den Maschinen findet nicht mehr über die Tastatur oder Maus statt, sondern über die Sprache. Alle Sprachassistenten basieren im Prinzip darauf, nach einem bestimmten Signalwort die gesprochene Sprache aufzunehmen und in einen Text umzuwandeln. Dies geschieht mithilfe von Künstlicher Intelligenz (KI) beziehungsweise maschinelles Lernen und Deep-Learning-Technologien. Vor allem beim Erkennen des Signalwortes spielen Deep-Learning-Algorithmen eine große Rolle. Daher ist in Bezug auf Sprachassistenten die Künstliche Intelligenz (KI) von großer Bedeutung. Denn die Verarbeitung der Audiomitschnitte erfolgt meist nicht mehr auf dem Gerät selbst, sondern in der Cloud mit Unterstützung der Künstlichen Intelligenz (KI). Zudem können sich die intelligenten Sprachassistenten stetig weiterentwickeln je mehr Trainingsdaten zur Verfügung stehen.

Gleichzeitig steigen aber auch bei der Verwendung von Sprachassistenten die Risiken für die **Informationssicherheit** und den **Datenschutz** deutlich. So sind sich viele Anwender von Sprachassistenten über deren Sicherheitsrisiken nicht bewusst. Die einfache Konfiguration und Bedienung verleiten zum Irrglauben, dass es nichts zu beachten oder zu befürchten gibt.

Jedoch weit gefehlt, alleine schon die **falsche Platzierung** der Sprachassistenten in den eigenen vier Wänden kann ein Sicherheitsrisiko darstellen. So können Angreifer durch Fenster oder Türen Sprachbefehle geben, und **SmartHome Geräte** dazu zwingen zum Beispiel Türen zu öffnen oder Alarmanlagen auszuschalten. Hier zeigt sich auch schon die nächste Gefahr. Die intelligenten Sprachassistenten können aufgrund der nicht frei wählbaren **Aktivierungswörter** und ohne konfigurierte **Stimmprofile** problemlos von

jeder x-beliebigen Person allein durch die Stimme aktiviert und für andere Zwecke missbraucht werden. Aber auch bei der ständigen Verbindung mit dem **WLAN** gibt es Schwachstellen für Angreifer. So können Angreifer eine falsche Konfiguration, eine schwache Verschlüsselung oder unsichere Passwörter für ihre WLAN-Angriffe ausnutzen. Mögliche WLAN-Angriffe können **Man-in-the-Middle** oder **Denial-of-Service** sein. Dies könnte Angreifer in die Lage versetzen einzudringen, zu übernehmen, zu täuschen, zu fälschen, zu betrügen, auszuspähen, zu entwenden, zu verhindern oder zu zerstören. Des Weiteren kann die von vielen Benutzern hilfreiche Funktion **Bluetooth,** um sich mit anderen Smartphones oder Lautsprecher zu verbinden, zum Sicherheitsproblem werden. Gelingt es einem Angreifer in unmittelbarer Nähe eine Bluetooth Schwachstelle auszunutzen, so ist die Übernahme eines Gerätes, Abfangen von Verbindungsschlüsseln oder die Störung anderer Geräte möglich. Der Angriff auf diese Bluetooth-Sicherheitslücke ist erst recht möglich, da sich bei den Sprachassistenten wie Alexa und Google Home die Bluetooth Funktion nicht deaktivieren lässt. Außerdem nutzen viele Anwender die Möglichkeit, die Grundfunktionen der Sprachassistenten durch **Schnittstellen** zu anderen Drittanbietern zu erweitern. Allerdings besteht hier das Risiko Dienste anderer Anbieter zu aktivieren, die nicht vertrauenswürdig sind und ggf. heimlich Funktionen ausführen, die dem Benutzer nicht bewusst sind. Aber auch die Trainingsdaten im Bereich **maschinelles Lernen** die dem Sprachassistenten für die stetige Weiterentwicklung dienen, können von Angreifern so manipuliert werden, dass andere Ergebnisse oder Aktionen das Resultat sind.

Beim **Datenschutz** muss wiederum einem bewusst sein, dass die Hersteller von Sprachassistenten erhebliche **personenbezogene Daten** gesammelt, ausgewertet und ggf. an andere weitergeleitet werden. Wie die Analyse bewiesen hat, beginnt die Aufzeichnung der gesprochenen Sprache erst mit dem Signalwort, zuvor erfolgt keine heimliche Aufzeichnung. Ab dem Signalwort wird alles Gesprochene, auch Hintergrundgeräusche oder Stimmen aufgezeichnet und an eine Cloud meistens nicht im eigenen Land weitergeleitet und analysiert. Da die Sprachassistenten oft in den eigenen vier Wänden platziert sind, muss einem bewusst sein, dass hier auch teilweise sehr **private Gespräche** mitgeschnitten werden. Leider erfolgt die Auswertung der Audiomitschnitte zur Verbesserung der Sprachassistenten ohne Wissen der Nutzer meistens noch von **Mitarbeitern** der einzelnen

Hersteller. So könnten sehr intime Gespräche usw. von wildfremden Menschen mitgehört werden. Zudem konnte eindeutig nachgewiesen werden, dass die Tonaufnahmen zur Analyse **weltweit** auf verschiedenen Cloud-Servern abgespeichert werden. Die Gefahr ist hier, dass in jedem Land andere **Datenschutzbestimmungen** gelten, und der Anwender nicht eindeutig weiß, wer Zugriff auf seine Gesprächsaufzeichnungen hat. Zwar besteht die Möglichkeit bei den meisten Herstellern die Sprachaufzeichnungen abzurufen und ggf. zu löschen, jedoch ist vielen diese Funktion gar nicht bekannt. Leider erfolgt die Auswertung der Audiomitschnitte sowie die ggf. Weiterleitung der Daten an Dritte meistens im Verborgenen. Der Benutzer bekommt von diesen Ereignissen nichts mit und wird darüber auch nicht immer informiert. Zudem lassen die Hersteller den Nutzern bei der **Datenschutzerklärung** und **Nutzungsbedingungen** wenig Handlungsfreiheit. Im Prinzip wird man nahezu gezwungen diese bedingungslos zu akzeptieren, tut man dies nicht, ist der Sprachassistent entweder nicht verwendbar oder nur eingeschränkte Funktionen stehen zur Verfügung.

Allerdings sind diese Systeme von der Robustheit und Flexibilität der menschlichen Sprachwahrnehmung noch weit entfernt. So gibt es Probleme mit Hintergrundgeräuschen, Akzenten und Dialekten sowie spontan gesprochener Sprache. Derzeit findet die Kommunikation mit den Sprachassistenten eher in Befehlsform statt, anstelle mit richtigen Dialogen. Zudem hat man derzeit immer noch das Gefühl man spricht nicht mit einem Menschen, sondern mit einer Maschine. Dennoch ist jetzt schon zu erkennen, dass spracherkennende und sprachverstehende Systeme den Alltag in der Zukunft immer mehr bestimmen werden. Der Trend geht ganz klar zu intelligenten Spracherkennungssystemen trotz Sicherheitsrisken oder Datenschutzbedenken. Momentan überwiegen noch die zahlreichen Funktionen wie Musik abspielen oder die Steuerung der SmartHome Geräte sowie die einfache Bedienung. Wie so oft muss immer dem Nutzer selbst etwas passieren, bevor er die Sicherheit und den Datenschutz ernst nimmt.

# Abkürzungsverzeichnis

## A

**A2DP** Advanced Audio Distribution Profile

**AES** Advanced Encryption Standard

**AI** Artificial Intelligence

**AP** Access Point

**API** Application Programming Interface

**ASK** Alexa Skill Kit

**AVS** Alexa Voice Service

**AWS** Amazon Web Services

## B

**BDSG** Bundesdatenschutzgesetz

**BSI** Bundesamt für Sicherheit in der Informationstechnik

## C

**CCMP** Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

**CEO** Chief Executive Officer

**CIA** Confidendiality, Integrity, Availbiliy

## D

**DOS** Denial-of-Service

## E

**EU-DS-VGO** EU-Datenschutz-Grundverordnung

## G

**GQUIC** Google Quick UDP Internet Connections

**GTK** Group Transient Key

## H

**HTTP** Hypertext Transport Protocol

**HTTPS** Hypertext Transport Protocol Secure

## I

**I/O** Input/Output

**ICMP** Internet Control Message Protocol

**ID** Identification Number

**IEEE** Institute of Electricial and Electronics Engineers

**IFTTT** If This Than That

**IGMP** Internet Group Management Protocol

**iOS** Internetwork Operating System

**IP** Internet Protocol

**IPA** Intelligenten Persönlichen Assistent

**IPv4** Internet Protocol version 4

**IT** Informationstechnik

**IV** Initialisierungsvektor

## K

**KI** Künstliche Intelligenz

**KRACK** Key Reinstallation Attack

## L

**L2CAP** Logical Link Control and Adaption Protocol

**LAN** Local Area Network

## M

| | |
|---|---|
| **MAC** | Media Access Control |
| **mDNS** | multicast Domain Name System |
| **MIC** | Message Integrity Code |
| **MIMO** | Multiple Input Multiple Output |
| **MITM** | Man-in-the-Middle |
| **ML** | Machine Learning |

## O

| | |
|---|---|
| **OCSP** | Online Certificate Status Protocol |

## P

| | |
|---|---|
| **PIN** | Personal Identification Number |
| **PSK** | Pre-Shared-Key |
| **PTK** | Pairwise Transient Key |

## S

| | |
|---|---|
| **SDK** | Software Development Kit |
| **SIG** | Special Interest Group |
| **Siri** | Speech Interpretation and Recognition Interface |
| **SSID** | Service Set Identifier |
| **SSL** | Secure Socket Layer |
| **SSP** | Service Discovery Protocol |

## T

| | |
|---|---|
| **TCP** | Transport Control Protocol |
| **TKIP** | Temporal Key Integrity Protocol |
| **TLS** | Transport Layer Security |

## U

| | |
|---|---|
| **UDP** | User Datagram Protocol |
| **URL** | Uniform Resource Locator |
| **USB** | Universal Serial Bus |

## W

| | |
|---|---|
| **WEP** | Wide Area Network |
| **WLAN** | Wireless Local Area Network |
| **WPA** | Wi-Fi Protected Access |
| **WPS** | Wi-Fi Protected Setup |
| **WWW** | World Wide Web |

# Literaturverzeichnis


[1] Brandt, R: Mr. Amazon Jeff Bezos und der Aufstieg von amazon.com. Ambition, 2012.

[2] Buxmann, P; Schmidt H: Künstliche Intelligenz: Mit Algorithmen zum wirtschaftlichen Erfolg. Springer Gabler, 2019.

[3] Damaschke G: Siri Handbuch. Amac-Buch, 2016.

[4] Eckert, C: IT-Sicherheit: Konzepte – Verfahren – Protokolle. Oldenburg Wissenschaftsverlag, 2014.

[5] Ertel, W: Grundkurs Künstliche Intelligenz. Springer Vieweg, 2016.

[6] Galloway S: the four: Die geheime DNA von Amazon, Apple, Facebook und Google. Plassen Verlag, 2018.

[7] Gerdes H: Amazon Echo & Alexa: Der Ratgeber für Ihr smartes Zuhause. Vierfarben, 2019.

[8] Gläß, R: Künstliche Intelligenz im Handel 1 – Überblick. Springer Vieweg, 2018.

[9] Jacobsen N: Das Apple-Imperium. Springer Spektrum, 2014.

[10] Kranig, T; Sachs, A; Gierschmann, M: Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden. Bundesanzeiger Verlag, 2017.

[11] Mainzer, K: Künstliche Intelligenz – Wann übernehmen die Maschinen? Springer, 2019.

[12] Osterhage, W: Sicherheitskonzepte in der mobilen Kommunikation: Drahtlose Kommunikation – Protokolle und Gefahren. Springer Vieweg, 2018.

# Online-Quellen


[1] Amazon.: „Alexa Skills – Glossar“, Unter: https://developer.amazon.com/de/designing-for-voice/glossary/, (abgerufen am 15.05.2019)

[2] Amazon.: „Amazon.de: Datenschutzerklärung.“ Unter: https://www.amazon.de/gp/help/customer/display.html?nodeId=3312401, (abgerufen am 04.06.2019)

[3] Amazon.: „Informationen zum Lichtring.“ Unter: https://www.amazon.de/gp/help/customer/display.html?nodeId=201601790, (abgerufen am 09.03.2019)

[4] Apple.: „Kurzbefehle – Benutzerhandbuch“, Unter: https://support.apple.com/de-de/guide/shortcuts/apdf22b0444c/2.2/ios/12.0, (abgerufen am 23.06.2019)

[5] Apple.: „Eine Kopie der mit dem Apple-ID-Account verknüpften Daten erhalten.“ Unter: https://support.apple.com/de-de/HT208502, (abgerufen am 20.06.2019)

[6] Apple.: „iPhone 6s Plus - Technische Daten.“ Unter: https://support.apple.com/kb/SP727?locale=de_DE&viewlocale=de_DE, (abgerufen am 03.04.2019)

[7] Apple.: „iPhone-Benutzerhandbuch.“ Unter: https://help.apple.com/iphone/11/?lang=de#/iphf8ff0253f), (abgerufen am 05.04.2019)

[8] Apple.: „Kurzbefehle im Überblick.“ Unter: https://support.apple.com/de-de/guide/shortcuts/apdf22b0444c/2.2/ios/12.0, (abgerufen am 25.06.2019)

[9] Apple.: „So schützen wir deine Privatsphäre.“ Unter: https://www.apple.com/de/privacy/approach-to-privacy/, (abgerufen am 27.06.2019)

[10] Areamobile.: „original-google-home.“ Unter: http://www.areamobile.de/bilder/211683-original-google-home-c-google, (abgerufen am 12.04.2019)

[11] Armis.: „BlueBorne: PROTECTING THE ENTERPRISE FROM BLUEBORNE.“ Unter: https://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf, S. 3, (aufgerufen am 21.05.2019)

[12] Armis.com.: „BlueBorne Cyber Threat Impacts Amazon Echo and Google Home“, Unter: https://armis.com/blueborne-cyber-threat-impacts-amazon-echo-google-home/, (abgerufen am 22.05.2019)

[13] Arnold, A.: „WLAN-Verschlüsselung.“ Unter: https://www.heise.de/ct/artikel/WLAN-Verschluesselung-221639.html?seite=all, (abgerufen am 14.05.2019)

[14] Arnold, M.: „Datenkraken im Wohnzimmer – Ist die Privatsphäre noch zu retten?“ Unter: https://www.heise.de/newsticker/meldung/Datenkraken-im-Wohnzimmer-Ist-die-Privatsphaere-noch-zu-retten-4270545.html, (abgerufen am 19.03.2019)

[15] Aschermann, T.: „Bluetooth - Einfach erklärt.“, Unter: https://praxistipps.chip.de/bluetooth-einfach-erklaert_100370, (abgerufen am 20.05.2019)

[16] Becker, L.: „Apples Kurzbefehle-App: Shortcuts können geschützte iPhone-Dateien abgreifen.“ Unter: https://www.heise.de/mac-and-i/meldung/Apples-Kurzbefehle-App-Shortcuts-koennen-geschuetzte-iPhone-Dateien-abgreifen-4283745.html, (abgerufen am 09.05.2019)

[17] Bergmann, P.: SmartHome Vol. 2: „Spannende Hintergründe zu Alexa, Google Assistant und Siri.“ Unter: https://www.apfelpage.de/news/smart-home-vol-2-spannende-hintergruende-zu-alexa-google-assistant-und-siri/, (abgerufen am 06.03.2019)

[18] Bleich, H.: „Amazon gibt intime Alexa-Sprachdateien preis.“ Unter: https://www.heise.de/newsticker/meldung/Amazon-gibt-intime-Sprachdateien-preis-4254716.html, (abgerufen am 08.06.2019)

[19] Blumenstein, S.: „Modernes WLAN-Hacking.“, Unter: https://www.computerwoche.de/a/modernes-wlan-hacking,2521564, (abgerufen am 22.05.2019)

[20] Brown, P.: „All the Technology Inside Your Google Home.“ Unter: https://electronics360.globalspec.com/article/7718/all-the-technology-inside-your-google-home, (abgerufen am 13.04.2019)

[21] BSI.: „B 4.8 Bluetooth.“, Unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b04/b04008.html?nn=6604914, (abgerufen am 26.05.2019)

[22] BSI.: „G 4.79 Schwachstellen in der Bluetooth-Implementierung.“, Unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04079.html, (abgerufen am 27.05.2019)

[23] BSI.: „M 4.362 Sichere Konfiguration von Bluetooth.“, Unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04362.html, (abgerufen am 28.05.2019)

[24] BSI.: „Glossar.“ Unter: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/Functions/glossar.html?cms_lv2=6658220, (abgerufen am 10.05.2019)

[25] BSI.: „Denial-of-Service-Attacken.“ Unter: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/DoS/dos_node.html, (abgerufen am 13.05.2019)

[26] BSI.: „Sichere Nutzung von WLAN (ISi-WLAN).“ Unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_wlan_leitlinie.pdf?__blob=publicationFile&v=1, (abgerufen am 12.05.2019)

[27] Dornbach, R.; Schmitz, Peter.: „Nutzen und Risiko von Sprachassistenten.“ Unter: https://www.security-insider.de/nutzen-und-risiko-von-sprachassistenten-a-744746/. (abgerufen am 02.07.2019)

[28] ECHO Lautsprecher.: „Technische Daten der Amazon Echo Familie.“ Unter: https://www.echolautsprecher.de/technische-daten-der-amazon-echo-familie/, (abgerufen am 16.03.2019)

[29] Echo-Ratgeber.: „Was Du noch nicht über Echo & Alexa wusstest:“ Unter: https://i1.wp.com/amz-echo-ratgeber.de/wp-content/uploads/2017/08/echo-technik.jpg, (abgerufen am 07.03.2019)

[30] Eilers, C.: „KRACK – Angriff auf WPA2.“ unter: https://entwickler.de/online/security/krack-ueberblick-579816756.html, (abgerufen am 17.05.2019)

[31] Elkenberg, R.: „Bluetooth-Lücke in Millionen Geräten entdeckt.“ Unter: https://www.heise.de/security/meldung/Bluetooth-Luecke-in-Millionen-Geraeten-entdeckt-4118968.html, (abgerufen am 18.05.2019)

[32] Emmer, W.: „Alexa Smart Home: Die besten Geräte für Amazon Echo.“ Unter: https://www.pcwelt.de/a/alexa-smart-home-die-besten-geraete-fuer-amazon-echo,3391001, (abgerufen am 10.03.2019)

[33] Eos.: „Schutzziele: CIA und CIAA.“ Unter: https://www.eosgmbh.de/wp-content/uploads/2018/07/Evolution_der_Schutzziele_jpg_2.jpg, (abgerufen am 01.05.2019)

[34] Feldmann, M.: „Google öffnet Google Home für Entwickler.“ Unter: https://jaxenter.de/conversational-actions-google-home-50536, (abgerufen am 02.06.2019)

[35] Fischer, J.: „How Does a Virtual Assistant Work?“ Unter: https://gearpatrol.com/2017/07/19/how-does-a-virtual-assistant-work/, (abgerufen am 14.03.2019)

[36] Gallwitz, F.; Niemann, H.; Nöth, E.: „Spracherkennung – Stand der Technik, Einsatzmöglichkeiten und Perspektiven.“ Unter: https://link.springer.com/article/10.1007/bf03250681, (abgerufen am 08.03.2019

[37] Google.: „Connected Home.“ Unter: https://store.google.com/de/category/connected_home, (abgerufen am 17.03.2019)

[38] Google.: „Google Home LED lights.“ Unter: https://support.google.com/googlenest/answer/7073219, (abgerufen am 18.03.2019)

[39] Google.: „Google Home Produktlinie.“ Unter: https://store.google.com/de/category/connected_home, (abgerufen am 19.03.2019)

[40] Google.: „Google Home Technische Daten.“ Unter: https://store.google.com/de/product/google_home_specs, (abgerufen am 20.03.2019)

[41] Haack, W.; Severance, M.; Wallace, M.; Wohlwend, J.: „Security Analysis of he Amazon Echo.“ Unter: https://courses.csail.mit.edu/6.857/2017/project/8.pdf, (abgerufen am 10.03.2019)

[42] Heise.: „Man-in-the-Middle-Angriff.“ Unter: https://www.heise.de/glossar/entry/Man-in-the-Middle-Angriff-399039.html, (abgerufen am 15.05.2019)

[43] Hifitest.: „Ausstattungsliste: Amazon Echo (2. Generation).“ Unter: https://www.hifitest.de/test/ausstattungsliste/bluetooth-lautsprecher/amazon-echo_2_generation_50520, (abgerufen am 11.03.2019)

[44] Hifitest.: „Ausstattungsliste: Google Home.“ Unter: https://www.hifitest.de/test/ausstattungsliste/bluetooth-lautsprecher/google-home_46052, (abgerufen am 20.03.2019)

[45] Intersoft Consulting.: „Art. 4 DSGVO Begriffsbestimmungen.“ Unter: https://dsgvo-gesetz.de/art-4-dsgvo/, (abgerufen am 04.06.2019)

[46] IT-Wissen.: „Michael-Hash.“ Unter: https://www.itwissen.info/Michael-Hash-Michael-hash.html, (abgerufen am 27.05.2019)

[47] Jackob, C.: „Actions on Google Tutorial: Apps für Google Assistant selbst schreiben.“ Unter: https://www.inovex.de/blog/actions-on-google-tutorial/, (abgerufen am 24.05.2019)

[48] Jaffe, J.: „Here’s every Amazon Echo device you can buy right now.“ Unter: https://www.cnet.com/news/heres-every-echo-that-amazon-has-ever-announced/, (abgerufen am 12.03.2019)

[49] Jurren, N.: „Was Alexa & Co. aufzeichnen und wie diese Daten verarbeitet werden.“ Unter: https://www.heise.de/select/ct/2018/23/1541817688628620, (abgerufen am 02.07.2019)

[50] Kaltschmidt, T.: „Amazon Echo: Nachrichtensprecher löst Massenbestellung aus.“ Unter: https://www.heise.de/newsticker/meldung/Amazon-Echo-Nachrichtensprecher-loest-Massenbestellung-aus-3591039.html, (abgerufen am 04.05.2019)

[51] Kannenberg, A.: „Amazon-Mitarbeiter tippen zum Teil Alexa-Sprachbefehle ab.“ Unter: https://www.heise.de/newsticker/meldung/Amazon-Mitarbeiter-tippen-zum-Teil-Alexa-Sprachbefehle-ab-4374871.html, (abgerufen am 14.06.2019)

[52] Kekeisen, T.: „Mein erster eigener Amazon Echo Skill: Der Nörgelgenerator.“ Unter: https://thomaskekeisen.de/de/blog/amazon-echo-dot-alexa-skill-noergelgenerator-entwickelt/, (abgerufen am 13.05.2019)

[53] Kinsella, B.: „Apple Siri Devices Total 500 Million. This is Not Users. But Still.“ Unter: https://voicebot.ai/2018/01/24/apple-siri-devices-total-500-million-not-users-still/, (abgerufen am 11.04.2019)

[54] Kleinz, T.: „Werbespot: Burger King kapert Google Home.“ Unter: https://www.heise.de/newsticker/meldung/Werbespot-Burger-King-kapert-Google-Home-3685167.html, (abgerufen am 16.07.2019)

[55] Kownatzki, B.: „Deep Learning: Was ist das eigentlich?.“ Unter: https://www.empolis.com/blog/kuenstliche-intelligenz/deep-learning/, (abgerufen am 23.03.2019)

[56] Kubiv, H.: „Siri ist zurück: Alexa und Google müssen weichen.“ Unter: https://www.macwelt.de/a/siri-ist-zurueck-alexa-und-google-muessen-weichen,3439136, (geboren am 30.03.2019)

[57] Kubiv, H.: „Apple schaltet Stimmerkennung bei Siri für alle frei.“ Unter: https://www.macwelt.de/tipps/Voice-ID-Siri-9831918.html, (abgerufen am )

[58] Kühl, E.: „Drittanbieter sollen Skills entwickeln.“ Unter: https://www.zeit.de/digital/mobil/2016-10/amazon-echo-alexa-test-deutschland/seite-3, (abgerufen am )

[59] Lemche, F; Fritsche, C.: „Analyse und Vergleich zwischen Amazon Alexa und Google Home in Bezug auf (un)gewollte externe Netzwerk Kommunikation.pdf.“ (abgerufen am 11.07.2019)

[60] Luber, S.: „Was ist Deep Learning.“ Unter: https://www.bigdata-insider.de/was-ist-deep-learning-a-603129/, (abgerufen am 29.03.2019)

[61] Luber, S.: „Was ist eine MAC-Adresse?“ Unter: https://www.ip-insider.de/was-ist-eine-mac-adresse-a-665074/, (abgerufen am 10.06.2019)

[62] Luber, S.: „Was ist WPA?“ Unter: https://www.security-insider.de/was-ist-wpa-a-742206/, abgerufen am 26.05.2019)

[63] MacTechNews.: „Privatsphäre-Fehler: Siri liest im Sperrbildschirm auch versteckte Mitteilungen laut vor.“ Unter: https://www.mactechnews.de/news/article/Privatsphaere-Fehler-Siri-liest-im-Sperrbildschirm-auch-versteckte-Mitteilungen-laut-vor-169167.html, (abgerufen am 29.07.2019)

[64] McGowen, B.: „Google Home and Google Assistant.“ Unter: https://www.slideshare.net/bretmc/google-home-and-google-assistant-workshop-build-your-own-serverless-action-on-google-app, (abgerufen am 06.06.2019)

[65] Nicolas.: „Lautlos aktiviert: Siri-Angriff im nicht hörbaren Bereich.“ Unter: https://www.iphone-ticker.de/lautlos-aktiviert-siri-angriff-im-nicht-hoerbaren-bereich-116331/, (abgerufen am 08.05.2019)

[66] NFON: „WPA2.“ Unter: https://www.nfon.com/at/service/knowledge-base/knowledgebase-detail/wpa2/, (abgerufen am 27.05.2019)

[67] o. V.: „WLAN-Sicherheit: So machen Sie Ihr kabelloses Netzwerk zur Festung.“ Unter: https://www.ionos.de/digitalguide/server/sicherheit/wlan-sicherheit-so-machen-sie-ihr-kabelloses-netzwerk-zur-festung/, (abgerufen am 01.06.2019)

[68] o. V.: „Man-in-the-Middle.“ Unter: https://www.elektronik-kompendium.de/sites/net/1710251.htm, (abgerufen am 22.05.2019)

[69] o. V.: „Schutz für Wi-Fi-Netzwerke.“ Unter: https://www.kaspersky.de/resource-center/preemptive-safety/protecting-wireless-networks, (abgerufen am 30.05.2019)

[70] o. V.: „WLAN sichern.“ Unter: https://www.botfrei.de/de/anleitungen/sicheres-wlan.html, (abgerufen am 01.06.2019)

[71] o. V.: „WPA2 - WiFi Protected Access 2 / IEEE 802.11i.“ Unter: https://www.elektronik-kompendium.de/sites/net/0907111.htm, (abgerufen am 07.05.2019)

[72] o. V.: „Ausstattungsliste-Bluetooth-Lautsprecher-Amazon-Echo.“ Unter: https://www.hifitest.de/test/ausstattungsliste/bluetooth-lautsprecher/amazon-echo_2_generation_50520, (abgerufen am 15.03.2019)

[73] o. V.: „How-Siri-Technology-Work.“ Unter: http://www.howtechnologywork.com/wp-content/uploads/2014/11/How-Siri-Technology-Work1.png, (abgerufen am 17.03.2019)

[74] o. V.: „Technische Daten der Amazon Echo Familie.“ Unter: https://www.echolautsprecher.de/technische-daten-der-amazon-echo-familie/, (abgerufen am 06.04.2019)

[75] o.V.: „Echo-Technik.“ Unter: https://i1.wp.com/amz-echo-ratgeber.de/wp-content/uploads/2017/08/echo-technik.jpg“, (abgerufen am 09.03.2019)

[76] Osswald, V.: „Amazon Echo gehackt: Skill macht Lautsprecher zur Wanze.“ Unter: https://www.chip.de/news/Amazon-Echo-gehackt-Skill-macht-Lautsprecher-zur-Wanze_138594450.html, (abgerufen am 19.07.2019)

[77] Reinwarth, M.: „Von Schnittstellen zu geplanten Schwachstellen.“ Unter: https://digitaleweltmagazin.de/2017/12/14/von-schnittstellen-zu-geplanten-schwachstellen/, (abgerufen am 12.06.2019)

[78] Schierhorn, T.: „Google Actions: Das kann der Google Home Speaker.“ Unter: https://www.otto.de/updated/ratgeber/google-actions-das-kann-der-google-home-speaker-53851/, (abgerufen am 20.06.2019)

[79] Schleeh, H.: „Alexa auf dem Amazon Echo einrichten – Der Digitale Sprachassistent im Haus.“ Unter: https://schleeh.de/2016/11/05/alexa-auf-dem-amazon-echo-einrichten-der-digitale-sprachassistent-im-haus/, (abgerufen am 11.03.2019)

[80] Schlücker, I.: „Großer Lauschangriff im Wohnzimmer.“ Unter: https://www.it-zoom.de/mobile-business/e/grosser-lauschangriff-im-wohnzimmer-16881/, (abgerufen am 09.07.2019)

[81] Schöne, B.; Schmitz, P.: „Spracherkennungssoftware als Angriffsziel.“ Unter: https://www.security-insider.de/spracherkennungssoftware-als-angriffsziel-a-588514/, (abgerufen am 23.06.2019)

[82] Srocke, D.: „Alexa, hör mal bitte weg!“, Unter: https://www.security-insider.de/alexa-hoer-mal-bitte-weg-a-821728/, (abgerufen am 25.07.2019)

[83] Stahl, M.: „Alexa abhören? So sicher ist der Amazon Echo wirklich.“ Unter: https://praxistipps.chip.de/alexa-abhoeren-so-sicher-ist-der-amazon-echo-wirklich_98035, (abgerufen am 10.07.2019)

[84] Stein, S.: „Neuronales Netze.“ Unter: http://emergenz.hpfsc.de/da_sstein.pdf, (abgerufen am 16.03.2019).

[85] Tißler, J.: „Alexa, Siri & Co: Sprachsuche, digitale Assistenten und Smart Speaker verändern das Marketing“.Unter: https://upload-magazin.de/blog/16055-alexa-sprachassistenten/, (abgerufen am 08.04.2019)

[86] Tjkrajewski, T.: „Wie programmiert man Google Home Assistent Skill?“ Unter: https://thecattle-crew.net/2018/08/16/wie-programmiert-man-google-home-assistent-skill-node-js-express-app-und-dialogflow/, (angerufen am 07.06.2019)

[87] Vibhu, R.: „Google Home Local API.“ Unter: https://rithvikvibhu.github.io/GHLocalApi/, (abgerufen am 08.07.2019)

[88] Wendel, M.: „Google Home Datenschutz - Was weiß der Sprachassistent von mir?“, Unter: https://www.homeandsmart.de/google-datenschutz, (abgerufen am 07.07.2019)

[89] Wendel, M.: „Google Home Datenschutz - Was weiß der Sprachassistent von mir?.“ Unter: https://www.homeandsmart.de/google-datenschutz, (abgerufen am 15.07.2019)

[90] Westerhagen, O.: „BlueBorne: Bluetooth-Schwachstellen auch in Amazon Echo und Google Home“ Unter: https://www.heise.de/security/meldung/BlueBorne-Bluetooth-Schwachstellen-auch-in-Amazon-Echo-und-Google-Home-3891500.html, (abgerufen am 28.05.2019)

[91] Wlansignalverstaerken.: „WLAN-Standards: Alle wichtigen Infos zu IEEE 802.11a/b/g/n/ac.“ Unter, https://www.wlansignalverstaerken.de/wlan-standards, (abgerufen am 11.05.2019)

[92] Wuesst, C.: „A guide tot he security of voice-activated smart speakers.“ Unter: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-security-voice-activated-smart-speakers-en.pdf, (abgerufen am 13.03.2019)

[93] Zeit.: „Google ermöglicht automatisches Löschen von Web- und Ortsdaten.“ Unter: https://www.zeit.de/digital/datenschutz/2019-05/google-daten-automatisches-loeschen-datensicherheit, (abgerufen am 02.06.2019)

[94] Zhang, N.; Mi, X.; Feng, X.; Wang, X,: Tian, Y.; Qian, F.: „Understanding and Mitigating the Security Risks of Voice-ControlledThird-Party Skills on Amazon Alexa and Google Home.“ Unter: https://arxiv.org/pdf/1805.01525.pdf,%202018.pdf, (abgerufen am 12.03.2019)

# Anhang

## A.1 Technische Details von Amazon Echo (1 Generation)

**Tabelle 8: Technische Details von Amazon Echo (1. Generation) (Eigene Darstellung Daten aus: vgl. https://www.echolautsprecher.de/technische-daten-der-amazon-echo-familie/; https://www.hifitest.de/test/ausstattungsliste/bluetooth-lautsprecher/amazon-echo_2_generation_50520 )**

| Technische Daten | Antwort |
|---|---|
| **Produkttyp** | WLAN Lautsprecher, Bluetooth Lautsprecher, Smart Speaker |
| **Maße** | 235 mm x 83,5 mm x 83,5 mm |
| **Gewicht** | 1064 Gramm |
| **Audio** | 63 mm-Woofer und 50 mm Hochtonlautsprecher |
| **Gehäuseeigenschaft** | Bassreflex |
| **Stromversorgung** | Netzteil |
| **Systemanforderungen** | Amazon Echo muss nur mit ihrem WLAN verbunden werden |
| **Integrierte Geräte** | Mikrofon |
| **Intelligenter Persönlicher Assistent (IPA):** | Alexa |
| **Alexa Sprache** | Deutsch, Englisch, Französisch, Italienisch, Spanisch, Chinesisch |
| **Steuerung über** | Fernbedingung, App, Sprache |
| **Steuerungseigenschaft** | Stumm (Mute), Lautstärke, Ein/Aus, Rufannahme, Bluetooth Pairing, Beleuchtung |
| **Smartphone Steuerung-App** | App: Amazon Alexa |
| **Funktion** | Internetradio, Streaming, Freisprechfunktion, Smartphone-Steuerung, Sprachassistent |
| **Aktivierung von Alexa** | Aktions-Button, Spracherkennung und Steuerung über Codewort „Alexa“; „Computer“, „Echo“, „Amazon“ |
| **WLAN-Verbindung** | WLAN-Verbindung: Dualband-WLAN mit zwei Antennen (MIMO) Unterstützt WLAN-Netzwerke mit den Standards 802.11a/b/g/n. Unterstützt nicht die Verbindung zu ad-hoc oder Peer-to-Peer WLAN-Netzwerken. Dual Band (2,4 GHz und 5 GHz) |
| **Bluetooth Verbindung** | Unterstützt Advanced Audio Distribution Profile (A2DP) für Audiostreaming von Mobilgeräten auf Amazon Echo und Audio/Video Remote Control Profile |
| **Kompatibilität** | Notebook, sonstige Geräte mit Bluetooth, Tablet, Smartphone |
| **APP verfügbar für** | Android, iOS, Fire OS |

| Technische Daten | Antwort |
|---|---|
| **Soundfunktion** | 360° Klangfeld, Rauschunterdrückung |
| **Verfügbarer Musikdienst** | Spotify, Amazon Music, iHeartRadio, Pandora, TuneIn AllPlay |
| **Empfangsbereich:** | Webradio |
| **Einsatzgebiet** | Wohnzimmer, Multiroom |
| **Bemerkung** | 7 integrierte Mikrofone |
| **Lieferumfang** | Amazon Echo, Netzteil/Kabel und Kurzanleitung |

## A.2 Technische Details von Google Home

**Tabelle 9:Technische Details von Google Home (Eigene Darstellung Daten aus: (https://store.google.com/de/product/google_home_specs; (https://www.hifitest.de/test/ausstattungsliste/bluetooth-lautsprecher/google-home_46052)**

| Technische Daten | Antwort |
|---|---|
| **Produkttyp** | WLAN Lautsprecher, Smart Speaker, Bluetooth Lautsprecher |
| **Maße** | Tiefe: 96,4 mm<br>Höhe: 142,8 mm<br>Breite: 96,4 mm |
| **Gewicht** | 477 Gramm |
| **Audio** | High Excursion-Lautsprecher und 2“-Treiber und zwei 2“-Passivradiatoren |
| **Soundfunktion** | 360° Klangfeld |
| **Stromversorgung** | Netzteil |
| **Systemanforderungen** | Google Home muss nur mit ihrem WLAN verbunden werden |
| **Integrierte Geräte** | Mikrofon |
| **Intelligenter Persönlicher Assistent (IPA):** | Google Assistant |
| **Google Assistant Sprache** | Deutsch, Englisch (Australien, Großbritannien, Indien, Kanada, Singapur, USA), Französisch, Italienisch, Japanisch und Spanisch (Spanien) verfügbar. |
| **Steuerung über** | Sensortasten, App, Sprache |
| **Steuerungseigenschaft** | Stumm (Mute), Lautstärke, Wecker |
| **Smartphone Steuerung-App** | App: Google Home |
| **Funktion** | Kalender, Internetradio, Streaming, Freisprechfunktion, Smarthome-Steuerung, Sprachassistent |
| **Aktivierung von Google Assistant** | Spracherkennung und Steuerung über Codewort „OK Google“; „Hey Google“ |
| **WLAN-Verbindung** | 802.11b/g/n/ac (2,4 GHz/5 GHz) WLAN |
| **Bluetooth Verbindung** | Unterstützt Advanced Audio Distribution Profile (A2DP) |
| **Kompatibilität** | Tablet, Smartphone |
| **APP verfügbar für** | Android 5.0 und höher, iOS 9.1 und höher |
| **Soundfunktion** | Far Field-Spracherkennung |
| **Verfügbarer Musikdienst** | Google Play, iHeartRadio, Pandora, Spotify, TuneIn AllPlay, Youtube, Google Cast |
| **Empfangsbereich:** | Webradio, FM |
| **Einsatzgebiet** | Wohnzimmer, Multiroom |
| **Bemerkung** | 2 integrierte Mikrofone |
| **Ports und Anschlüsse** | Stromanschluss, Micro-USB-Port (nur für Support-Service) |
| **Lieferumfang** | Google Home, Netzteil/Kabel und Kurzanleitung |

## A.3 Technische Details vom iPhone 6s Plus mit Apple Siri

**Tabelle 10: Technische Details vom iPhone 6s Plus mit Apple Siri (Eigene Darstellung Daten aus: https://support.apple.com/kb/SP727?locale=de_DE&viewlocale=de_DE)**

| Technische Daten | Antwort |
|---|---|
| **Produkttyp** | Smartphone |
| **Maße** | Tiefe: 7,3 mm<br>Höhe: 158,2 mm<br>Breite: 77,9 mm |
| **Gewicht** | 192 Gramm |
| **Stromversorgung** | Akku oder Netzteil |
| **Systemanforderungen** | Apple Siri muss nur mit ihrem WLAN verbunden werden |
| **Integrierte Geräte** | Mikrofon |
| **Intelligenter Persönlicher Assistent (IPA):** | Apple Siri |
| **Siri Sprachen** | Englisch (Australien, Kanada, Indien, Irland, Neuseeland, Singapur, Südafrika, Großbritannien, USA), Spanisch (Chile, Mexiko, Spanien, USA), Französisch (Belgien, Kanada, Frankreich, Schweiz), Deutsch (Österreich, Deutschland, Schweiz), Italienisch (Italien, Schweiz), Japanisch, Koreanisch, Mandarin (Festlandchina, Taiwan), Kantonesisch (Festlandchina, Hongkong, Macau), Arabisch (Saudi-Arabien, Vereinigte Arabische Emirate), Dänisch (Dänemark), Niederländisch (Belgien, Niederlande), Finnisch (Finnland), Hebräisch (Israel), Malaysisch (Malaysia), Norwegisch (Norwegen), Portugiesisch (Brasilien), Russisch (Russland), Schwedisch (Schweden), Thai (Thailand), Türkisch (Türkei) |
| **Smartphone Steuerung-Apple Siri** | Einstellungen – Siri & Suchen |
| **Funktion** | Kalender, Aufgaben, Nachrichten, Internetradio, Streaming, Freisprechfunktion, Smarthome-Steuerung, Sprachassistent |
| **Aktivierung von Apple Siri** | Home-Taste, Spracherkennung und Steuerung über Codewort „Hey Siri“ |
| **WLAN-Verbindung** | 802.11ac WLAN mit MIMO |
| **Bluetooth Verbindung** | Bluetooth 4.2 |
| **Kompatibilität** | Tablet, Smartphone, Apple TV, Mac Book, Apple Watch, HomePod |
| **Verfügbarer Musikdienst** | Apple Music |
| **Empfangsbereich:** | Webradio, FM |
| **Einsatzgebiet** | überall |
| **Ports und Anschlüsse** | Lightning Connector |

# Erklärung

Hiermit erkläre ich, dass ich die hier vorliegende Arbeit selbstständig, ohne unerlaubte fremde Hilfe und nur unter Verwendung der in der Arbeit aufgeführten Hilfsmittel angefertigt habe.

--- ---

Ort, Datum Unterschrift

# Thesen

- Die Popularität der Spracherkennungssysteme nimmt an Bedeutung stetig zu. Je mehr intelligente Lautsprecher eingesetzt werden, desto attraktiver wird es auch als Angriffsziel.
- Die Künstliche Intelligenz (KI) basierend auf maschinelles Lernen und Deep Learning spielt bei den Sprachassistenten eine zentrale Rolle. Hierfür werden eine Vielzahl von Trainingsdaten benötigt.
- Die Spracherkennung ist noch nicht perfekt ausgereift und bietet somit eine Angriffsfläche.
- Die Grundvoraussetzung einer ständigen WLAN Verbindung ist ein Schwachpunkt.
- Die Anzahl von Bluetooth-fähigen Geräten nimmt drastisch zu, daher suchen Angreifer gezielt nach Schwachstellen in diesem Bereich.
- Offene Schnittstellen (API) zu Drittanbietern können vielseitig genutzt aber auch für andere Zwecke missbraucht werden.
- Der Datenschutz der Spracherkennungssysteme erfordert mehr Transparenz gegenüber den Anwendern.