MASTERARBEIT

Sicherheitsrisiken beim Betrieb kritischer Geräte und Anwendungen im Smart Home Umfeld

ausgeführt am

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Tobias Pichler

Personenkennzeichen: 1910320012

Graz, am 22. März 2021 Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

Unterschrift

DANKSAGUNG

Ich möchte mich an dieser Stelle bei all denjenigen bedanken, die mich während der Anfertigung dieser Masterarbeit unterstützt und motiviert haben. Speziell möchte ich mich bei meinem Betreuer DI (FH) Christian Schmid, MSc für die gute Betreuung bedanken.

Meiner Freundin Pauline danke ich besonders für den emotionalen Rückhalt über die Dauer meines gesamten Studiums. Abschließend möchte ich bei meiner Familie und allen Freunden für das stets offene Ohr sowie die moralische Unterstützung bedanken.

KURZFASSUNG

Das Smart Home hat sich als Anwendungsgebiet innerhalb des IoT große Beliebtheit verschafft. Mithilfe von verschiedenartigen, miteinander vernetzten Geräten werden Komfort und Sicherheit im Wohnbereich gesteigert. Aufgrund der einfachen Bedienung und der Interoperabilität zwischen unterschiedlichen Plattformen ist diese Art von Geräten besonders in Privathaushalten verbreitet. Durch ständige Konnektivität zum Internet bestehen jedoch Risiken hinsichtlich der Informationssicherheit sowie des Schutzes von Daten der BenutzerInnen. Die untersuchte Architektur im Rahmen dieser Arbeit behandelt ein generisches, Cloud-basiertes System. Dieses wird mithilfe des Risikoanalysemodells OCTAVE Allegro und dem Fokus auf kritische Informationsassets systematisch auf Sicherheitsrisiken überprüft. Für eine bessere Übersicht wird das Gesamtsystem in drei Subsysteme aufgeteilt. Ziel der Risikoanalyse ist es, die unterschiedlichen Sicherheitsrisiken, welche mit der Nutzung von Cloud-basierten Smart Home Systemen verbunden sind, aufzuzeigen. Für die Reduzierung von Risiken werden Gegenmaßnahmen sowie ein Katalog über Handlungsempfehlungen für NutzerInnen erarbeitet. Die Ergebnisse zeigen, dass NutzerInnen innerhalb ihres Einflussbereiches gezielt Maßnahmen zur Reduzierung der Risiken setzen können. Besonders beim Betrieb von kritischen Geräten sind eine stabile Energieversorgung und Internetverbindung essenziell. Der restliche Anteil der Sicherheitsrisiken geht bei einem Cloud-basierten System auf die Systemanbieter sowie Service Provider über. Durch die Entwicklung von Systemen innerhalb aktueller Security-Frameworks können Systemanbieter bereits in der Konzeptphase spätere Risiken vermeiden und Security und Privacy by Design Prinzipien einhalten. Für eine nachhaltige Durchsetzung von Smart Home Systemen ist dies ein essenzieller Faktor. Mithilfe neuer Technologien wie Blockchain könnten traditionelle Sicherheitsprobleme im IoT obsolet werden, konkrete Anwendungsfälle dafür befinden sich noch im Forschungsstadium.

ABSTRACT

The smart home is a key field within the IoT. Connected devices boost comfort and security in the home. Thanks to their ease-of-use and interoperability, these devices are common in private households. However, their permanent internet connection poses risk regarding information security and the protection of user data. This thesis investigates a generic, cloud-based architecture. It is systematically checked for security risks using the OCTAVE Allegro risk-analysis model and focusses on critical-information assets. The overall system is divided into three subsystems. The risk analysis identifies the different security risks associated with the use of cloud-based smart-home systems. Countermeasures and a catalogue of recommended actions for users to reduce risks are given. The results show that users can take some targeted measures to reduce risks. A stable energy supply and internet connection are essential, especially for critical devices. The remaining security risks in a cloud-based system are transferred to the system and service providers. By developing systems within state-of-the-art security frameworks, system providers can avoid later risks in the concept phase and comply with security and privacy-by-design principles. This is an essential factor for a sutsainable implementation of smart-home systems. With the help of new technologies such as blockchain, traditional security issues in the IoT could become obsolete; specific use cases for this are still at research stage.

INHALTSVERZEICHNIS

1 EINLEITUNG

Aufgrund der technologischen Entwicklungen im Umfeld der Informationstechnologien erfreut sich das Internet der Dinge (IoT) seit Jahren großer Beliebtheit. Es handelt sich im Allgemeinen um ein offenes System, in dem verschiedenste Geräte autonom miteinander kommunizieren, um Nutzen oder eine Effizienzsteigerung für die BetreiberInnen zu generieren (Jeyanthi et al., 2019). Man kann das IoT auch als eine Vernetzung von physischen Objekten mit dem Internet beschreiben, wodurch eine kontinuierliche Verarbeitung von Daten die Folge ist. Im Unternehmensumfeld, speziell in der Logistik, im Gesundheitswesen und in der Automotive-Industrie existieren etablierte Lösungen und Hersteller, weiters unterliegt der Betrieb dieser Geräte üblicherweise einer Aufsicht durch professionelle Systemadministratoren.

Die steigende Anzahl an Geräten und Anwendungen im privaten Umfeld birgt durch das Fehlen dessen jedoch Risiken im Bereich Datenschutz, Datensicherheit und Privatsphäre. Der Begriff „Smart Home“ hat sich für diese Art von IoT-Systemen durchgesetzt. NutzerInnen verwandeln ihr Zuhause mittels elektronischer Sensoren, Schlössern, Beleuchtung und Überwachungskameras in ein intelligentes Zuhause, das mithilfe von Apps und Sprachsteuerung zum Leben erweckt wird. Für ältere als auch körperlich beeinträchtigte Menschen birgt ein Smart Home System Erleichterungen im täglichen Leben. Durch die einfache Bedienung der smarten Geräte entsteht jedoch ein Kompromiss zwischen Komfort und Datensicherheit. Angreifer können potenziell die Privatsphäre von NutzerInnen verletzen oder sensible Daten stehlen, falls Lücken im Sicherheitskonzept des Systems bestehen. Durch die permanente Internetanbindung und Geräten mit fehlerhaften Sicherheitsimplementierungen werden Angriffe weiter erleichtert. Darüber hinaus können viele Sicherheitsmechanismen wie Authentifizierung und aktuelle Verschlüsselungsmethoden in IoT-Geräten nicht oder nur eingeschränkt genutzt werden, da diese Technologien große Rechenkapazitäten erfordern. Daraus folgt, dass ausschließlich schlanke und leichtgewichtige Algorithmen verwendet werden können, um ein Gleichgewicht zwischen Sicherheit und geringem Ressourcenverbrauch erzielen zu können. Traditionellen PCs sowie Serverumgebungen in der Cloud stehen demgegenüber genug Rechenleistung für komplexe Algorithmen zur Maximierung der Sicherheit zur Verfügung.

Aufgrund von Angriffen auf sicherheitskritische Geräte wie Überwachungskameras und Türschlösser kann erheblicher Schaden für NutzerInnen entstehen. Mögliche Abhilfen dagegen möchte ich in dieser Arbeit aufzeigen, da die Bewahrung von Informationssicherheit und Datenschutz für die Akzeptanz neuartiger Technologien zwingend notwendig ist (Lin & Bergmann, 2016).

1.1 Ziele der Arbeit

Das Ziel dieser Masterarbeit ist die Identifikation und Bewertung von Sicherheitsrisiken beim Betrieb von Geräten und Anwendungen in einem Smart Home System. Das Ergebnis soll eine Sammlung an Kriterien für die Auswahl und Konfiguration solcher Systeme sein, um NutzerInnen Empfehlungen zu Kaufentscheidungen zu geben, bei der richtigen, sicheren Konfiguration der Geräte zu unterstützen und allgemein ein Bewusstsein für das Thema Informationssicherheit zu entwickeln.

Die zu beantwortende Forschungsfrage der Arbeit lautet:

- Welche Sicherheitsrisiken entstehen durch die Nutzung von Cloud-basierten Geräten im Smart Home Umfeld?

Zusätzlich sollen die zwei folgenden Subforschungsfragen beantwortet werden:

- Welche Folgen bergen diese Sicherheitsrisiken bei einem Eintritt?
- Welche Gegenmaßnahmen können NutzerInnen zur Risikominimierung empfohlen werden?

Die von der Forschungsfrage abgeleiteten Hypothese und die dazugehörige Alternativhypothese werden wie folgt formuliert:

H_0: Die Nutzung von Smart Home Geräten stellt kein Risiko für die Privatsphäre der NutzerInnen dar, wenn diese keine oder fehlerhaft implementierte Sicherheitsfunktionen aufweisen.

H_1: Die Nutzung von Smart Home Geräten stellt ein Risiko für die Privatsphäre der NutzerInnen dar, wenn diese keine oder fehlerhaft implementierte Sicherheitsfunktionen aufweisen.

Basierend auf den Erkenntnissen des theoretischen Teils, der der Behandlung der ersten Forschungsfrage dient, sollen die zwei weiteren Forschungsfragen mittels einer anerkannten Risikoanalysemethode beantwortet werden. Das Vorgehen wird im nächsten Kapitel beschrieben.

1.2 Aufbau und Methodik

In der Einleitung wurde zum Thema der Arbeit hingeführt. Der anschließende Hauptteil besteht aus zwei Teilen. Folgend werden der Inhalt und die Methodik dieser erläutert.

1.2.1 Theoretischer Teil

Im ersten Teil werden die technischen Grundlagen und die Elemente eines Smart Home Systems sowie die essenziellen Technologien der Informationssicherheit erläutert. Hier handelt es sich um das Ergebnis einer Literaturrecherche auf Basis des aktuellen Forschungsstandes. Mithilfe der Erkenntnisse wird die Antwort auf die erste Forschungsfrage erarbeitet: Welche Sicherheitsrisiken entstehen durch die Nutzung von Cloud-gestützten Geräten im Smart Home Umfeld?

Als Referenzen dienen ausschließlich wissenschaftlich anerkannte Artikel und Bücher, die in Bibliotheken und Online-Portalen verfügbar sind. Die Referenzen können dem Literaturverzeichnis entnommen werden.

1.2.2 Praktischer Teil

Im zweiten, praktischen Teil wird anhand der Methodik des Risikobewertungsmodells OCTAVE Allegro (Caralli et al., 2007) eine Risiko-Analyse eines generischen Smart Home Systems durchgeführt. Im Rahmen meiner Recherche über Risiko-Bewertungsmodelle hat sich diese als geeignet herausgestellt. Für die im Microsoft Secure Development Lifecycle enthaltene Methodik STRIDE (Howard & Lipner, 2006) existieren Tools für die Erstellung von Datenflussmodellen für untersuchte Systeme, auf die ebenfalls zurückgegriffen wird. Das verwendete System ist ein fiktives, welches die Kernkomponenten beinhaltet. Generell sollen in der Analyse die Elemente im internen System vorranging untersucht werden. Die externe Webapplikation, auch als „Cloud-Service“ bezeichnet, wird als Blackbox angesehen und nur die wesentlichen Sicherheitsrisiken davon werden erläutert.

Die durchzuführenden Schritte der Analyse umfassen:

1. Definition des Systems und der Systemgrenzen
2. Definition der Stakeholder
3. Definition der Informationsassets und physischen Assets
4. Erstellung eines Datenflussdiagramms
5. Identifikation von potenziellen Bedrohungen und Risiken für jedes Asset
6. Analyse und Bewertung eines jeden Risikos
7. Ausarbeitung von Abhilfen gegen die Risiken

Falls es sich notwendig und sinnvoll erweist, werden Subsysteme definiert. Es wird vertieft auf die Domäne des privaten Umfeldes und den sicherheitskritischen Geräten und Anwendungen eingegangen und deren Charakteristika berücksichtigt.

1.3 Abgrenzung und Begründung der Themenwahl

Der Rahmen der Arbeit umfasst ausschließlich Smart Home Systeme mit Cloud-Funktionalitäten. Es wird versucht, speziell auf sicherheitskritische Anwendungen einzugehen. Weiters werden keine praktischen Implementierungen oder Experimente durchgeführt sowie auf keine am Markt erhältlichen Lösungen eingegangen.

Aufgrund von persönlichem Interesse sowie der bedrohlichen Situation auf diesem Gebiet wählte ich dieses Thema. Daneben ist die Datenschutzgrundverordnung, die 2018 in Kraft trat (EU-DSGVO, 2016) ein ernstzunehmender, rechtlicher Rahmen für die Anbieter von Smart Home Systemen.

2 THEORETISCHE GRUNDLAGEN UND BEGRIFFSDEFINITIONEN

Im Rahmen dieses Hauptkapitels werden für den weiteren Inhalt der Arbeit relevante Begriffe erläutert. Es wird ein Überblick über die behandelten Umgebungen gegeben sowie eine Abgrenzung zu verwandten Gebieten durchgeführt. Zuerst wird das *Internet of Things* im Allgemeinen beschrieben, weiters Smart Home als ein Anwendungsfall davon sowie die dabei verwendete Technologien.

2.1 IoT

"The Internet of Things is not a concept; it is a network, the true technology-enabled Network of all networks." (Oriwoh, 2018)

Um zum konkret untersuchten Anwendungsfall des Smart Home hinzuführen, muss zuerst der Überbegriff für ein System vernetzter physischen Geräte beschrieben werden: das sogenannte „IoT". Die Zunahme der Internetnutzer und die Fortschritte im *Ubiquitous Computing* ermöglichen eine umfassende Vernetzung alltäglicher Dinge über das Internet. In den letzten Jahren hat sich das Akronym „IoT", welches für *Internet of Things* steht, zu einem der populärsten Begriffe innerhalb der Informations- und Kommunikationstechnologie entwickelt (Atzori et al., 2017). Kein anderer Begriff auf diesem Gebiet wird heute in so vielen verschiedenen Kontexten genannt. Beispiele, die von der Identifizierung von Artikeln in einem Lagersystem bis zu intelligenten Stromzählern reichen, deuten darauf hin, dass es bereits heute keine Grenzen mehr gibt. Dies ist womöglich ein Grund dafür, warum es keine einzig gültige Definition gibt. In der Literatur werden häufig einzelne Anwendungen des IoT damit in Verbindung gebracht, jedoch kann mithilfe einer ganzheitlichen Betrachtung der weite Sinn leichter erfasst werden. Verschiedene Personen haben nach der weltweiten Etablierung des Internets erkannt, dass die erste Version des Internets den menschengenerierten Daten galt. Primär entstand die erste Form von IoT-Anwendungen im Industrieumfeld, wodurch sich der mit IoT verwandte Begriff „Machine-to-Machine-Kommunikation" (M2M) entwickelte. Die logische Entwicklung bewegte sich in die Richtung von maschinengenerierten Daten, womit das Akronym IoT begründet werden kann. Im Jahr 2020 übersteigt die Anzahl der Geräte im IoT bereits 20 Milliarden (Dahmen-Lhuissier, 2020).

2.1.1 Begriffsdefinitionen

Eingangs muss erwähnt werden, dass es keine allgemeingültige Definition gibt. Weder öffentliche Institutionen noch die Privatwirtschaft kann heute wissen, welche Szenarien in Zukunft durch das IoT möglich gemacht werden. Häufig spricht man erst vom Anfang des IoT-Zeitalters. Als Erfinder der Phrase gilt Kevin Ashton, der diese 1999 erstmals öffentlich verwendete (Ashton, 2009). Er beschrieb damit die Verschmelzung und Interaktion zwischen der physischen und digitalen Welt, damals bezogen auf die Nutzung von RFID-Tags zur Identifizierung von Waren im

Produktionsumfeld. Mehrere Personen und Personengruppen haben den Begriff seitdem unterschiedlich definiert. An dieser Stelle werden einige Beispiele genannt.

Die IETF (Internet Engineering Task Force) beschreibt das IoT wie folgt:

> *"The Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, actuators, and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices." (Internet Engineering Task Force [IETF], 2020)*

Es kann herausgelesen werden, dass die Vernetzung aller Geräte eine zentrale Rolle spielt. Voraussetzung dafür ist die eindeutige Identifikation eines jeden Objekts sowie die Interoperabilität und Kompatibilität beim Datenaustausch. Dies wird von der IEEE (Institute of Electrical and Electronics Engineers) in einer Definition von 2015 betont:

> *"An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything." (Institute of Electrical and Electronics Engineers, 2015)*

Zusätzlich wird die Bedeutung des zeitlich und örtlich unabhängigen Zugriffs und die Veränderbarkeit der Objekte und Gerätekonfiguration hervorgehoben. Weltweit existiert eine Vielzahl an Gremien und Arbeitsgruppen, die an der der Definition von Standards arbeiten, um eine geräte- und plattformübergreifende Interoperabilität sicherzustellen. Bei diesen beiden Definitionen wird das IoT vorwiegend aus dem technologischen Standpunkt aus betrachtet. Eine einfachere und abstrakte Definition kommt von Vermesan et al. (2009). Hier wird es als eine Interaktion zwischen der physischen und der digitalen Welt mithilfe von Sensoren und Aktoren bezeichnet.

2.1.2 Architektur und Bestandteile

Nachdem es sich beim Begriff IoT um eine Sammlung an Konzepten, Technologien und standardisierten Datenaustauschmethoden handelt, kann im Allgemeinen nur eine abstrakte Veranschaulichung einer Architektur passieren. Dennoch sind Referenzarchitekturen essenziell für die Etablierung von Standards und die korrekte und nachhaltige Implementierung von IoT-Systemen (Weyrich & Ebert, 2016). Mit ihnen soll ein in der Industrie gemeinsames Verständnis eines abstrakten Konzeptes dargestellt werden. Eine weitere Herausforderung ist die Fragmentierung über Plattformen und Ökosysteme hinweg, dieser können gemeinsame Architekturen Abhilfe entgegenwirken.

Das IoT beruht allgemein auf einer offenen Architektur, um die Interoperabilität zwischen heterogenen Systemen und verteilten Ressourcen zu ermöglichen. Dies schließt die Anbieter und Konsumenten der Daten und Informationen ein, seien es die NutzerInnen, Services, oder andere Geräte im System. Die Architektur muss weiters auf eng definierten Standards wie abstrakten

Datenmodellen, Schnittstellen und Protokollen zusammen mit plattformneutralen Technologien wie Web-Services basieren, um eine Vielfalt an Betriebssystemen und Programmierumgebungen und -sprachen zu unterstützen. Wie das Konzept des Internets selbst muss eine IoT-Architektur so konzipiert sein, dass es sich robust gegenüber Unterbrechungen von Netzwerkverbindungen von mobilen Geräten verhält, die nur zeitweise eine Verbindung zum System haben (Vermesan et al., 2009).

Nachdem nun einige theoretische Ideen in textueller Form vorgestellt wurden, versuchen Autoren in den folgenden Darstellungen diese in schematischen Grafiken darzustellen. Am einfachsten können die oben genannten Anforderungen mithilfe eines Schichtenmodells abgedeckt werden, deshalb basieren auch die IoT-Architekturen darauf. Die Architekturen gelten übergeordnet und unabhängig von der Applikationsdomäne.

Die allgemeine, schematische Darstellung eines Schichtenmodells des IoT gestaltet sich wie folgt:

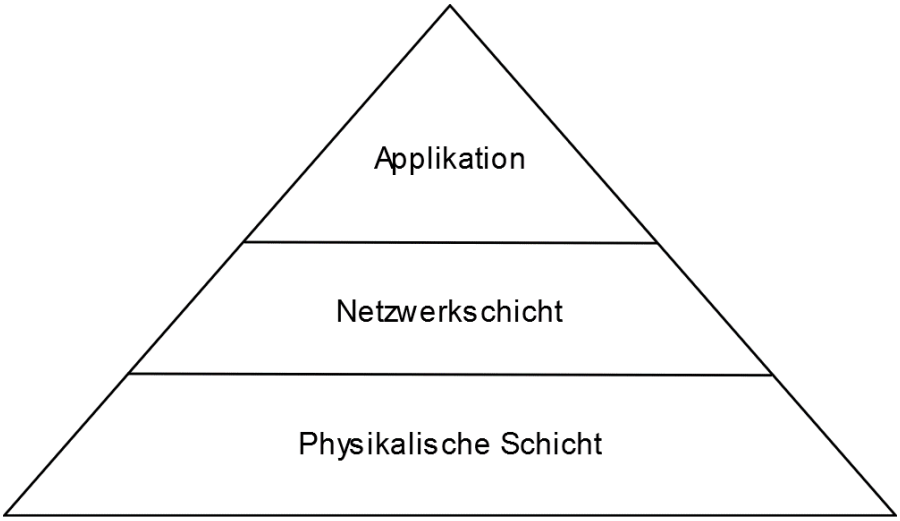

Abbildung 1: Allgemeine IoT-Architektur nach Yaqoob et al. (2017)

Bereits zu Beginn der Forschung auf diesem Gebiet etablierte sich diese abstrakte Architektur zu einem Defacto-Standard. Die unterste Schicht *„Physikalische Schicht“* beinhaltet Sensoren, um Daten aus der Umwelt zu sammeln sowie Aktoren, um eine Aktion auszulösen und die Umwelt zu verändern. Die *Netzwerkschicht* ist für die Kommunikation zwischen allen Geräten innerhalb der physikalischen Schicht zuständig sowie für die Datenübertragung zwischen Datenbanken und den physikalischen Geräten. Üblich ist auch das Hinzuzählen der Datenspeicher, die die Daten und Informationen verarbeiten, zu dieser Schicht. Die oberste Schicht ist die eigentliche Anwendung, das Ergebnis des Zusammenspiels der unteren Schichten sowie die Schnittstelle zu den NutzerInnen der IoT-Anwendung. In ihr findet sich die konkrete Anwendung wieder; in Kapitel 2.1.3 „Anwendungen und Ziele“ werden einige Stellvertreter dafür genannt.

Eine in der Literatur verwendete Architektur ist die „Reference IoT Layered Architecture“ (RILA) von Karzel et al. (2016). Diese wird üblicherweise zu den konkreten Architekturen gezählt. Das Referenzmodell besteht insgesamt aus sechs Schichten, wie in Abbildung 2 ersichtlich. Parallel dazu gibt es die beiden Schichten „Security“ und „Management“, welche allgegenwärtig sind und von jeder Schicht miteinbezogen werden.

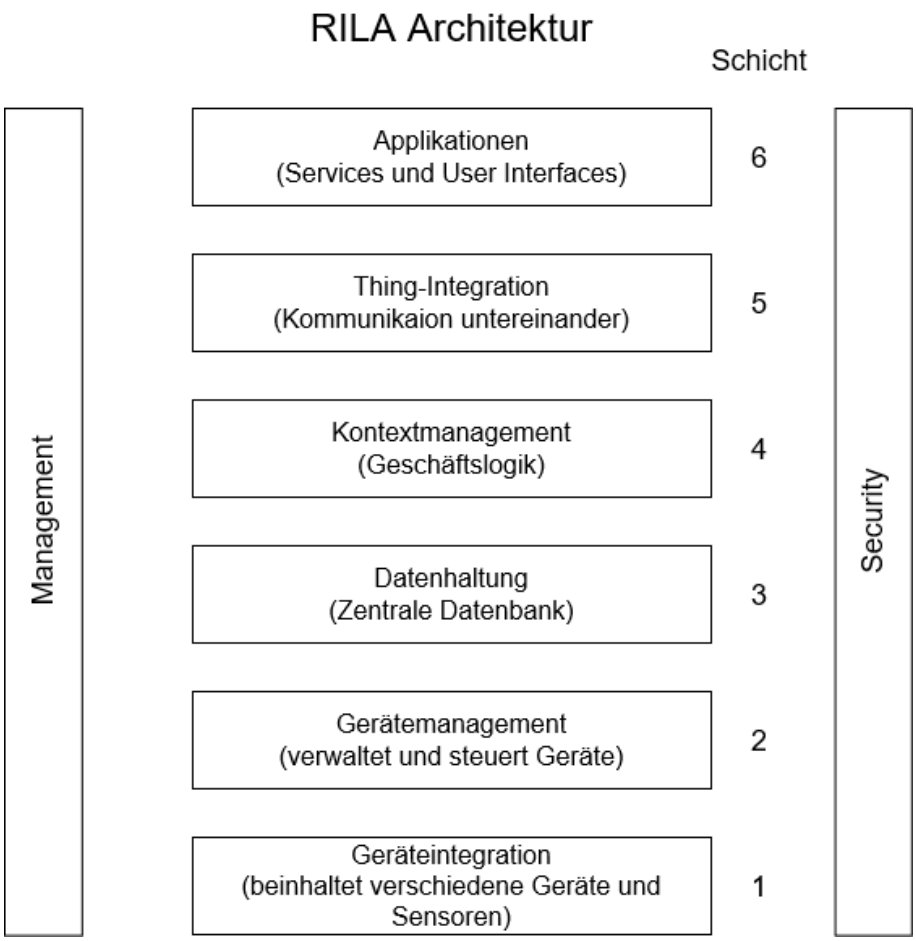

Abbildung 2: Reference IoT Layered Architecture nach Karzel et al. (2016)

Im gesamten Modell wird jede Schicht beschrieben sowie der Übergang in die nächste Schicht beschrieben. An dieser Stelle werden diese Beschreibungen zusammengefasst.

Die erste Schicht *Geräteintegration* umfasst alle Geräte inklusive dem Empfang ihrer Messwerte (Sensoren) und deren Steuerung (Aktoren). Es muss somit eine Reihe an unterschiedlichen Gerätetypen unterstützt werden und zwischen ihnen übersetzt werden.

Die zweite Schicht *Gerätemanagement* ist verantwortlich für den Datenaustausch mit der Schicht *Geräteintegration* und neuen Registrierungen von Dingen in dieser. Bei einer Änderung der Konfiguration oder des Status eines Geräts in der Integrationsschicht wird vom *Gerätemanagement* überprüft, ob diese tatsächlich vom Aktor durchgeführt wurde. Zentraler Punkt dieser Schicht ist die Kommunikation aller Daten der Sensoren und Aktoren zur Schicht *Geräteintegration*, damit diese Informationen gespeichert werden können.

Bei der Schicht *Datenhaltung* handelt es sich üblicherweise um eine zentrale Datenspeicher, der alle Daten der zwei untergeordneten Schichten speichert. Die Implementierung dieser Schicht hängt stark vom Anwendungsfall ab (Karzel et al., 2016).

Die Schicht *Kontextmanagement* umfasst die Geschäftslogik und stellt das Hirn der Anwendung dar. Sie ist verantwortlich für das Erreichen von gewünschten Zuständen der verbundenen Geräte

und Dinge, in dem kontextuell der aktuelle Zustand erfasst wird und intelligent die erforderlichen Schritte für den gewünschten Zustand ausgeführt werden.

In der Schicht *Kontextintegration* werden weitere Geräte automatisch erkannt und geprüft, ob eine Kommunikation mit diesen stattfinden kann. Falls diese Prüfung erfolgreich ist, wird direkt ein Registrierungsprozess ausgelöst.

Die oberste Schicht *Applikationen* stellt die Interaktionsschicht zwischen den UserInnen und den Geräten dar. Dieses ist speziell auf den Anwendungsfall zugeschnitten und bietet das notwendige Benutzerinterface, um die gewünschten Prozesse auszulösen.

Die beiden übergeordneten Schichten *Management* und *Security* sind ein Hinweis auf die Relevanz dieser beiden Gebiete, welche ganzheitlich über die gesamte Anwendung aufgespannt werden soll. Zusammengefasst ist dieses Modell eine Architektur, mithilfe jener robuste und integrierbare IoT-Systeme gebaut werden können.

2.1.3 Anwendungen und Ziele des IoT

Das übergeordnete Ziel von IoT-Systemen besteht darin, eine Synergie zwischen verschiedenen Systemen zu erreichen, sie sollten also interagieren und automatisch miteinander kommunizieren können, um für NutzerInnen wertsteigernde Dienste bereitzustellen. Daher ist eine Standardisierung erforderlich, um eine zuverlässige Interoperabilität verschiedener IoT-Systeme und -Plattformen sicherzustellen. Es besteht ein allgemeiner Konsens, dass das IoT verschiedene Bereiche der Gesellschaft positiv verändern wird, gleichzeitig wird dabei jedoch eine riesige Menge an Daten generiert. Dies bringt nicht nur neue Herausforderungen hinsichtlich der Verwaltung, Verarbeitung und Übertragung dieser Daten mit sich, sondern vor allem Bedenken hinsichtlich der Datensicherheit und des Datenschutzes. Neben der Standardisierung für die Interoperabilität sind also auch Sicherheitsstandards erforderlich, um die Personen, Unternehmen und Regierungen zu schützen, die die IoT-Systeme nutzen werden (Hassan et al., 2017). Diese potenziellen Risiken werden in Kapitel 3 „Informationssicherheit im “ behandelt.

Bereits heute existiert eine Reihe an Anwendungsgebieten im IoT-Umfeld (Dahmen-Lhuissier, 2020):

- Smart Homes
- Smart Metering
- Smart Cities
- Smart Grids
- eHealth

Aufgrund der flexiblen Gestaltungsmöglichkeiten werden in Zukunft weitere Anwendungsgebiete erschlossen werden können. Die Entwicklung wird einerseits durch Wirtschaft und Industrie, andererseits im privaten Bereich durch Konsumenten, die häufig als TesterInnen von neuen Technologien herangezogen werden, vorangetrieben.

Zusammenfassend können folgende Eigenschaften für die Beschreibung aller gültigen Definitionen genannt werden, da sie sich in diesen wiederfinden (i-SCOOP, 2020):

- Things (Geräte, Aktoren, Sensoren)
- Vernetzung der Things
- Daten und Informationen sind zentrales Gut
- Intelligente Services („Smart Services“)
- Kommunikation (über standardisierte Protokolle)
- Aktionen (auf Basis von Daten)
- Ökosystem (Partnerschaften und Interoperabilität zwischen Plattformen)

Sensoren oder ähnliche Geräte sammeln Daten, welche in einem Speicher abgelegt werden oder direkt von anderen Geräten abgefragt und weiterverarbeitet werden. Die Kommunikation erfolgt über standardisierte Methoden und Protokolle. Auf Basis dieser darunterliegenden Schichten können intelligente Services aufgebaut werden, welche Entscheidungen auf Basis von Daten und Informationen treffen. Die Aktionen durch das System werden schlussendlich von einem Aktor ausgeführt, dabei kann es sich beispielsweise um eine Temperaturregelung einer Heizung handeln. Ein einzelnes System kann sich in einem größeren Ökosystem wiederfinden und mit anderen Systemen kombiniert genutzt werden.

2.2 Smart Home

In Zukunft werden sich durch das Konzept des IoT, wie im vorigen Kapitel beschrieben, noch viele weitere Anwendungen im privaten sowie geschäftlichen Bereich etablieren, die die Lebensqualität und die Wirtschaft im Allgemeinen verbessern (Suryadevara & Mukhopadhyay, 2015). Nachdem nun der Ursprung des Konzeptes eines Smart Home erläutert wurden, handelt dieses Kapitel nun von dem konkreten Anwendungsspektrum des Smart Home. Mithilfe der Technologien ist es möglich, überall und jederzeit auf die im Wohnraum installierten, elektronischen Geräte zuzugreifen und diese über die Ferne zu steuern. Smart Homes ermöglichen es den Bewohnern, automatisch die Garage zu öffnen, wenn sie nach Hause kommen, Kaffee zu kochen sowie Klimaanlagen, intelligente Fernseher (Smart TVs) und andere Geräte im Haus zu steuern. Alle diese Geräte können mit Hilfe des Internets miteinander jederzeit kommunizieren. Einfachere Anwendungsbeispiele von Hausautomation schließend die Verwendung von Timern und Uhrzeiten ein, um gewünschte Prozesse und Abfolgen durchzuführen, jedoch können durch Smart Home Technologien komplexere Szenarien abgebildet werden und Geräte auf der Basis von Inputdaten anderer Geräte wiederum Prozesse auslösen.

Mithilfe dieser Kapitelstruktur soll die Abgrenzung zwischen IoT und Smart Home geschafft werden. Das Smart Home ist einer der potenziellen Anwendungsfälle des IoT, der bereits umgesetzt und in verschiedenen Weisen implementiert wurde.

Auch für das Smart Home gibt es, analog zum IoT, verschiedene Definitionen. Die erste wurde bereits 2003 von Nicola King formuliert:

> *"A dwelling incorporating a communications network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed." (King, 2003, S. 2)*

Eine weitere Definition lautet:

> *A smart home is a residence equipped with a communications network, linking sensors, domestic appliances, and devices, that can be remotely monitored, accessed or controlled and which provides services that respond to the needs of its inhabitants. (Balta-Ozkan et al., 2014, S. 66)*

Die Aussagen dieser einfachen Definition treffen auch heute noch auf Smart Home Systeme zu. Was die beiden Definitionen gemeinsam haben ist, dass die einzelnen Geräte miteinander kommunizieren und über die Ferne mithilfe von intelligenten Services gesteuert werden können. Die Art und Weise der Konnektivität geht jedoch weit über die von bei Smart Metering verwendeten Informations- und Kommunikationstechnologien (IKT) oder die Fernsteuerung eines Smart-TVs hinaus (Darby, 2018). Durch die Entwicklungen in der Zeit bis heute erweitern die Systeme jedoch zu intelligenten Wohnräumen, welche die Aspekte der Datensicherheit und des Energiemanagements miteinbeziehen sowie proaktive Services auf Basis von Künstlicher Intelligenz und Machine Learning anbieten.

2.2.1 Geschichte

Die Entstehung der Basis für Smart Home reicht viele Jahre zurück. Der Begriff „Smart Home" wurde bereits 1984 von der *American Association of House Builders* genannt (Bhatia et al., 2016). Obwohl das Konzept eines Smart Home schon länger bestand, erlebte es erst im letzten Jahrzehnt einen Aufschwung. Der wichtigste Grundstein war die Versorgung der Haushalte mit Elektrizität, was Anfang des 20. Jahrhunderts geschah (Harper, 2003). Durch das Vorhandensein von Strom in den Haushalten wurde die Entwicklung von Haushaltsgeräten stark vorangetrieben.

Ein weiterer Meilenstein war das Einziehen von Informationstechnologie in Form von Rechnern und dem Internet im letzten Viertel des 20. Jahrhunderts. Somit konnte Information ausgetauscht werden und Rechenoperationen effizient durchgeführt werden (Harper, 2003). Dies trieb erstmals konkret die Entwicklung von Smart Home an.

In den letzten Jahren gibt es speziell im Bereich der Mikroelektronik und den Sensoren neue Innovationen. Diese werden im Kapitel 3 „Technologien und Komponenten eines Smart Home" genauer erläutert.

Die ersten Geräte, die man als Smart Home Geräte bezeichnen kann, entstanden in den 1960er Jahren, wobei der „Electronic Computing Home Operator" dabei das erste darstellte (Hendricks, 2014). Dieser Rechner wurde verwendet um monetäre Ausgaben aufzeichnen, ein Inventar des Haushalts zu führen sowie für eine Klimaregelung. In den 1970er Jahren wurde es durch die

Erfindung des „Personal Computers“ erstmals für Hobby-Elektroniker möglich, eigene Anwendungen in kleinem Rahmen selbst zu entwickeln. Durch die Anbindung an das Telefonnetz konnte bereits eine Steuerung über die Ferne umgesetzt werden (T. K. Hui et al., 2017).

Mit dem Einzug des Internets in private Wohnräume in den 1990er Jahren wurde die Entwicklung des Smart Homes stark angetrieben und die Potenziale davon wurden erstmals erkannt (Katre & Rojatkar, 2017). Zur gleichen Zeit konnten aufgrund verbesserter Halbleitertechnik bereits kleine Geräte zur Steuerung und Sensorik entwickelt werden.

In den 2000er Jahren und bis heute schritt die Weiterentwicklung konstant voran. Mittlerweile stellen die Rechenleistung von CPUs und die Größe von Sensoren keine Hürde mehr da. Heutzutage handelt es sich bei Smart Home um ein Konglomerat an Technologien, welche erschwinglich sind und keine Vorkenntnisse auf diesem Gebiet voraussetzen.

2.2.2 Ziele eines Smart Home

Die Ziele eines Smart Home von unterschiedlichen UserInnen kann in folgende Kategorien eingeteilt werden:

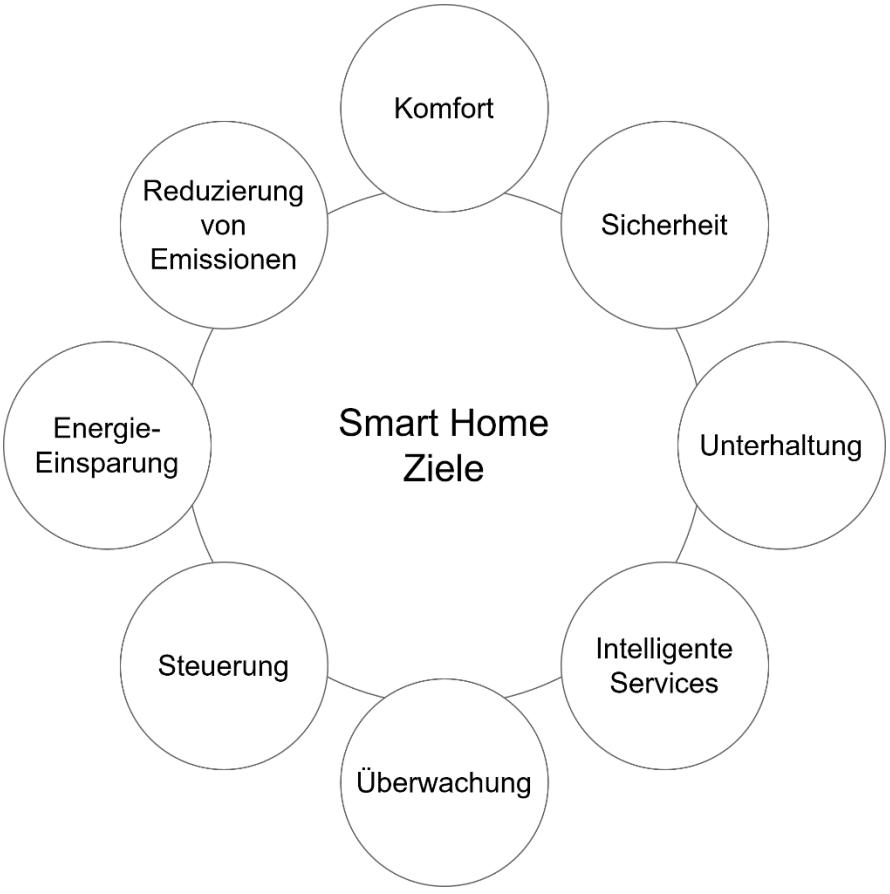

Abbildung 3: Ziele eines Smart Home aus Sicht der UserInnen

Aus Sicht der UserInnen sind diese acht Kategorien von Ziele die am häufigsten angestrebten. Sie sollen die Gründe dafür nennen, warum die Technologien von Smart Home überhaupt eingesetzt werden. Für ältere oder beeinträchtigte Menschen steht häufig der Komfort und die Steuerung im Vordergrund. Umweltbewusste Personen setzen Smart Home Technologien ein,

um Energie zu sparen – etwa durch die automatische Temperaturregelung – und dadurch Emissionen zu reduzieren. Möglich wird die Energieeinsparung durch drei notwendige Methoden (Marikyan et al., 2019): Die Überwachung des Energieverbrauchs stellt die Basis dar. Darauf aufbauend muss der Energieverbrauch von Geräten von anderen Geräten gesteuert werden können. Durch den Einsatz von intelligenten Services, die die Geräte kontrollieren, wird der Energieverbrauch optimiert. In einem größer gedachten Kontext kann mittels flächendeckend eingesetzter Technologien der Energieverbrauch über eine Stadt hinweg gesenkt werden.

Eine dritte Rolle können technologieinteressierte UserInnen darstellen, die mittels intelligenten Services und Unterhaltung neue Innovationen ausprobieren wollen. Diese Einteilung stellt bloß eine mögliche dar; in der Praxis entstehen Mischformen daraus.

2.2.3 Smart Home Architektur

Aufbauend auf generischen Architekturen des IoT, die in vorigen Kapiteln untersucht wurden, findet sich in Smart Home Systemen ebenfalls ein Muster von etablierten Architekturen wieder. Es werden in dieser Arbeit rein moderne, auf Konzepten des IoT basierende Smart Home Systeme untersucht, da traditionelle Modelle in der Praxis und in der Verbreitung in der Masse keine Bedeutung mehr haben. Auf Basis des Modells von Chong et al. (2011) wurde folgendes Schichtenmodell entworfen:

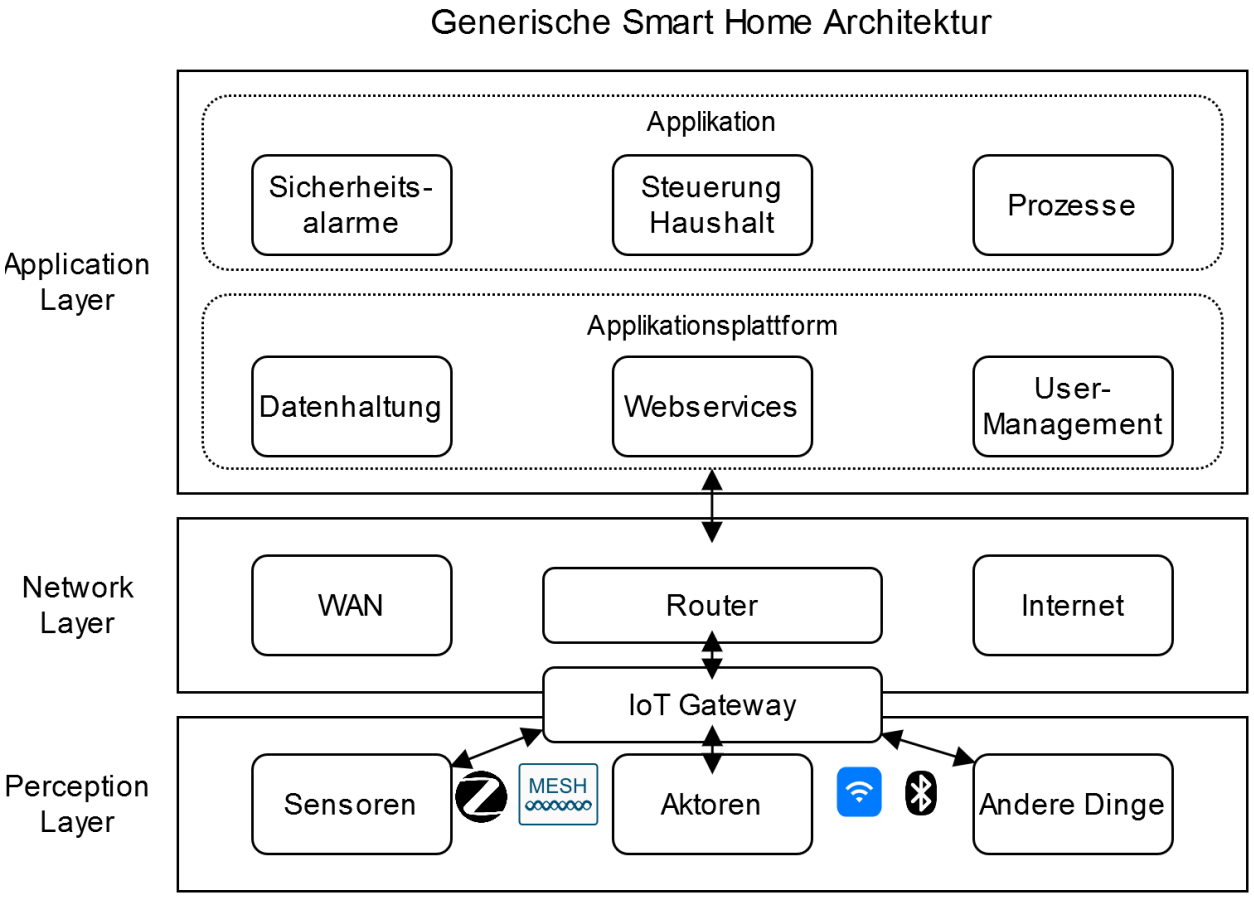

Abbildung 4: Generische Smart Home Architektur nach Chong et al. (2011)

Dieses vom Konzept des Schichtenmodells in Kapitel 2.1.2 „Architektur und Bestandteile“ eines IoT abgeleitete stellt nun eine konkrete Version gängiger Implementierungen dar. Folgend werden die einzelnen Bestandteile erläutert.

Der *Perception Layer* ist wie auch im Grundmodell die Basis der gesamten Architektur. Durch die Verwendung verschiedenster physischer und logischer Sensoren kann der Zustand diverser Parameter im Haushalt in Echtzeit überwacht werden. Diese umfassen Sensoren für die Messung von Umwelt-Parametern wie Temperatur und Luftfeuchtigkeit, Überwachungskameras, Türschlösser, Fensteröffner und ähnliches (Chong et al., 2011). Gleichzeitig umfasst diese Schicht Aktoren, dessen Zustand mithilfe eines Steuersignals geschalten werden kann. Eine intelligente Glühbirne oder eine elektrische Jalousie stellt so einen Aktor dar. Diese Geräte kommunizieren meist über schlanke, einfache Protokolle mit dem IoT Gateway oder direkt miteinander, welche im Kapitel 3 „Technologien“ beschrieben werden.

Das IoT Gateway stellt grundsätzlich die Verbindung zwischen dem *Perception* und dem *Network Layer* her. Es handelt sich dabei um einen Mikrocontroller, welcher Netzwerksignale aus dem LAN in das dementsprechende Kommunikationsprotokoll für die IoT-Geräte transformiert. Gleichzeitig kann somit eine gewisse Resilienz gegen Verbindungsabbrüche mit dem Internet hergestellt werden, falls dieser Mikrocontroller über Funktionen zum manuellen Umschalten von Aktoren verfügt. So kann innerhalb des Heimnetzwerkes bei Internetproblemen weiterhin agiert werden.

Der *Network Layer* umfasst die zentrale Kommunikation zwischen dem Heimnetzwerk und der Cloud-Umgebung der Smart Home Lösung. Diese Verbindung wird meist über den Heimrouter mithilfe des Internets oder Wide Area Networks (WAN) hergestellt. Diese Schicht basiert auf IP-Protokollen, welche weit verbreitet sind; somit kann bereits in dieser Schicht eine Interoperabilität zu Drittsystemen hergestellt werden, falls gewünscht und von der Smart Home Lösung unterstützt.

Der *Application Layer* stellt wie auch in der generischen IoT-Architektur die Schnittstelle zu UserInnen dar. Dieser *wurde* im obigen Modell in zwei Teile getrennt. Die unterliegende Komponente *Applikationsplattform* ist die Infrastruktur der Cloud-Lösung, in welcher alle notwendigen Daten gespeichert sind und diese zur Verfügung gestellt werden. In der darüberliegenden Schicht *Applikation* befindet sich die Geschäftslogik der Anwendung, hiermit können UserInnen die gewünschten Funktionen zur Verfügung gestellt werden. Näher wird im Rahmen dieser Arbeit jedoch auch nicht auf die von Herstellern implementierten Cloud-Lösungen eingegangen.

Wie in Abbildung 4 ersichtlich, handelt es sich bei der Kommunikation um bidirektionale Kommunikation zwischen den Teilnehmern im gesamten Netzwerk. Lediglich im verwendeten Übertragungsprotokoll unterscheiden sie sich. Welche hier verwendet werden, wird im folgenden Kapitel erläutert. Diese Illustration ist die Basis für alle weiteren Untersuchungen.

3 TECHNOLOGIEN UND KOMPONENTEN EINES SMART HOME

Das Smart Home als eine Anwendungsfall des IoT verwendet verschiedene Technologien, um ein Zusammenspiel der einzelnen Geräte und Komponenten im Gesamten zu ermöglichen. Eine Standardisierung ist hierbei unerlässlich (Atzori et al., 2017). In diesem Kapitel sollen die meistverwendeten Technologien und ihre Funktionsweise erläutert werden. Die Auswahl dafür basiert auf der Umfrage von Lin und Bergmann (2016).

3.1 Physische Endgeräte

Diese Geräte sind nach der aufgezeigten Architektur im Kapitel 2.2.3 „Smart Home Architektur“ dem *Perception Layer* sowie teilweise, im Falle eines IoT-Gateway, dem *Network Layer* zuzuordnen.

Sensoren können das Heimnetzwerk „sehen“ und „hören“. Es gibt Sensoren für eine Vielzahl von Anwendungen, z. B. zur Messung von Temperatur, Feuchtigkeit, Licht, Flüssigkeiten und Gasen sowie zur Erkennung von Bewegungen oder Geräuschen, wie sie in Überwachungskameras zu finden sind. Aktoren stellen jenen Teil dar, der die gewünschte Aktion in der realen Welt durchführt. Es gibt mechanische Aktoren wie Pumpen und Elektromotoren sowie elektronische Aktoren wie elektrische Schalter oder smarte Glühbirnen. Die mit Sensoren ausgestatteten Smart Home Geräte fungieren als *Datensammler* und die mit Aktoren als *Durchführende*. Es gibt weiters Geräte, die sowohl über Sensoren als auch über Aktoren verfügen.

Aufgrund der einfachen und günstigen Konzeption von Endgeräten in Smart Home Lösungen bringen diese im Vergleich zu traditionellen Rechnern wenig Leistungsressourcen auf. Die meisten Geräte sind energiesparsam, verwenden einen einfachen Mikrocontroller und haben begrenzte Speicherresourcen (Hahm et al., 2016). Hierbei unterscheiden sich klassische IoT-Geräte im industriellen Umfeld und Smart Home Geräte dennoch, da im Smart Home Bereich üblicherweise mehr Ressourcen zur Verfügung stehen und die Geräte meist über eine ununterbrochene Stromversorgung verfügen (Küchemann, 2014). Die ursprünglich entwickelten Protokolle des Internets wurden nicht für Architekturen der heutigen Smart Home Geräte entwickelt. Die spezifischen Anforderungen an ein Betriebssystem für Smart Home Geräte, seien es Sensoren, Bedienmodule oder smarte Lautsprecher, führten zur Entwicklung einer Vielzahl von unterschiedlichen Betriebssystemen (Silva et al., 2019). Die grundsätzliche Wahl der Kernelarchitektur hat einen signifikanten Einfluss auf Energieverbrauch, Leistung und das allgemeine Systemverhalten.

Bei den Anforderungen an ein Betriebssystem für Smart Home Endgeräte handelt es sich um folgende (Silva et al., 2019):

- Niedriger Energieverbrauch
- Speichereffizienz
- Konnektivität
- Sicherheitsfunktionen

Diese vier Bedürfnisse werden besonders von auf dem Linux-Kernel basierenden Betriebssystemen abgedeckt. Ein weiterer, alternativer Vertreter dieser Gruppe ist Windows 10 IoT von Microsoft. Hersteller verwenden meist eigens angepasste Varianten davon, welche nach außen hin und ohne Kenntnisse über den möglichen Zugang zum System isoliert sind.

Bei den IoT-Gateways, welche im Kontext auch Smart Home Hubs genannt werden, handelt es sich um Geräte, welche die Rohdaten der Sensoren sammeln und über etablierte Protokolle über das Internet an das Cloud-Service übertragen. Es stellt somit die Schnittstelle zwischen der Smart Home Welt und den webbasierten Anwendungen dar (Risteska Stojkoska & Trivodaliev, 2017). Um die Menge an übertragenen Daten zu reduzieren, sollen maximal viele Daten auf den Hubs selbst verarbeitet werden. In Smart Home Anwendungen kann das Gateway selbst die Rolle eines Load Balancers oder Schedulers einnehmen, ohne dass zuerst Daten vom Cloud-Service übertragen werden müssen. Hubs treten in die Rolle des Übersetzers zwischen Protokollen und sind in aktuellen Implementierungen notwendig. Durch eine erweiterte Interoperabilität können diese in Zukunft obsolet werden (Gubbi et al., 2013).

3.2 Datenübertragung

Die Datenübertragung spielt durch die Anwendung des Smart Home eine große Rolle. Aufgrund des Datenaustauschs sind Aktionen aufgrund von Änderungen der gelieferten Daten möglich. Vor allem drahtlose Technologien und Netzwerke spielen eine wichtige Rolle als eine der Schlüsselfaktoren für „Ubiqitous Computing“ und „Persuasive Computing“. Die starke Verbreitung von Drahtlos-Technologien wird durch Kommunikationsstandards wie Bluetooth und Bluetooth Low Energy, ZigBee und WiFi ermöglicht (Mahmoud & Jeedella, 2010). Die Auswahl der Technologien in diesem Kapitel ist an die Auswahl von Mahmoud und Jeedella (2010) angelehnt.

Als Übersicht über die einzelnen Technologien und Protokolle dient diese Veranschaulichung des auf das IoT angepasste ISO/OSI-Schichtenmodell:

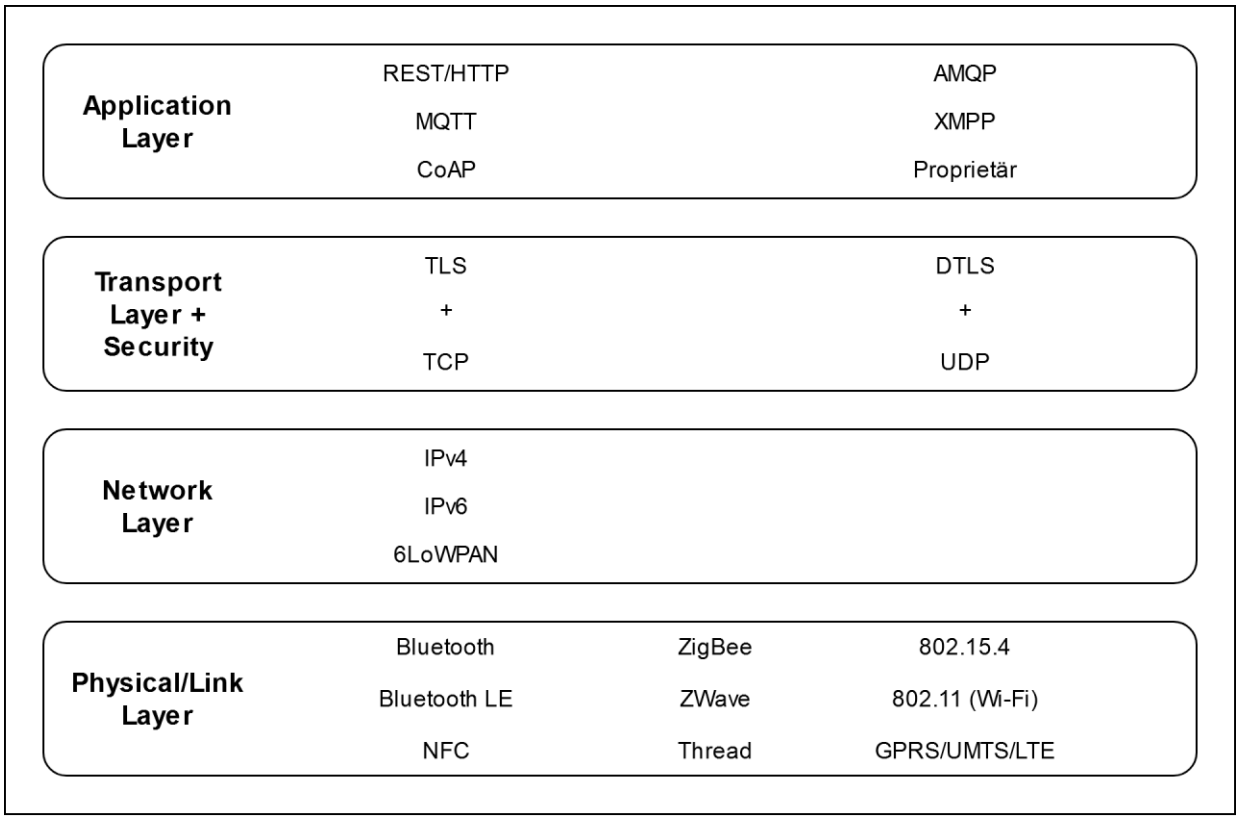

Abbildung 5: IoT-Protokolle und Standards (Russell, 2016)

In den nächsten Kapiteln werden insbesondere die speziellen Protokolle des IoT vorgestellt. Auf die Beschreibung etablierter und universeller Protokolle wie TCP, UDP und IP wird explizit verzichtet.

3.2.1 Drahtlose Technologien des Data Link und Physical Layer

Drahtlose Kommunikationsstandards sind heute in vielen Bereichen weit verbreitet. In einem Smart Home werden üblicherweise mehrere dieser Standards verwendet, abhängig von der Anwendung und dem Hersteller. In diesem Kapitel werden die wichtigsten Vertreter erläutert. Die Reihenfolge der Aufzählung richtet sich nach der steigenden Datenübertragungsrate der Technologie, die jedoch mit steigendem Energieverbrauch einhergeht.

3.2.1.1 RFID

Radio-Frequency Identification (RFID) bezeichnet ein System, das die Identität eines Geräts oder Objekts mittels Funkwellen überträgt (Want, 2006). Es umfasst einen RFID-Tag, welcher Information über das Objekt enthält, und ein dazugehöriges RFID-Lesegerät. Der Tag sendet ein Signal aus, sobald der Inhalt vom Lesegerät angefragt, also gelesen wird. Ein RFID-Tag kann aktiv oder passiv sein, wobei ein aktiver Tag einen Akku besitzt und der passive nicht. Ein passiver Tag nutzt das Magnetfeld des Lesegeräts und wandelt dieses in Gleichspannung um.

Folglich besitzen passive Tags eine geringere Reichweite, diese sind jedoch günstiger in der Beschaffung.

RFID-Systeme können auf Grundlage des verwendeten Frequenzbereichs kategorisiert werden. Niederfrequenzsysteme (LF) verwenden Signale mit einer Frequenz zwischen 124-135 kHz. Die Hochfrequenzsysteme (HF) verwenden eine Frequenz von 13,56 MHz, Ultrahochfrequenzsysteme (UHF) eine Frequenz zwischen 860-960 MHz. Im Allgemeinen haben LF-RFID-Systeme kurze Lesereichweiten und geringere Systemkosten. Falls eine größere Lesereichweite erforderlich ist, können HF-RFID-Systeme eingesetzt werden, deren Kosten jedoch höher sind.

Systeme basierend auf RFID können in Smart Homes eingesetzt werden, in denen jedes einzelne Objekt über eine virtuelle Adresse und eine eindeutige Kennung mit dem Heimnetzwerk verbunden wird (Darianian & Michael, 2008). Dies kann dazu verwendet werden, eine Datenbank mit der Information über den aktuellen Ort von Objekten zu führen. Eine Abfrage beim Smart Home System kann den Ort des Autoschlüssels oder der TV-Fernbedienung zeigen. Studien zeigten, dass der Aufenthaltsort von Bewohnern in einem Wohngebäude mittels an den Bewohnern angebrachten RFID-Tags sowie verstreuten RFID-Lesegeräten verfolgt werden kann (Yamazaki et al., 2007). Ein Problem bei der Verwendung von RFID ist die schwierige Lesbarkeit von Tags in der Nähe von Wasser sowie metallischen Gegenständen, wodurch ein Lesen von einem Tag an einem Menschen erschwert wird (Samuel, 2016). Daher wird laufend an Methoden geforscht, um die Lesbarkeit in diesen Umgebungen zu verbessern.

3.2.1.2 NFC

Near Field Communication (NFC) ist eine Funktechnologie mit kurzer Reichweite für die Kommunikation zwischen zwei Geräten in unmittelbarer Nähe. Das NFC-Forum standardisiert diese Technologie als offene Plattform für mobile Geräte und Systeme (NFC Forum, 2020). NFC-Systeme basieren auf der Hochfrequenz-RFID-Technologie (HF), die mit 13,56 MHz arbeitet. Der typische Kommunikationsbereich für NFC kann bis zu 8 cm betragen und hängt vom verwendeten Protokoll und dem Antennendesign ab. Derzeit unterstützt der NFC-Standard verschiedene Datenübertragungsraten mit Geschwindigkeiten bis zu 424 kbit/s (Proehl, 2013). Die prinzipielle Funktionsweise von NFC-Kommunikation zwischen zwei Geräten ist dieselbe wie bei herkömmlichem 13,56 MHz-RFID, bei der es sowohl einen Master als auch einen Slave gibt. Der Master wird als Emitter oder Lese-/Schreibgerät bezeichnet, während der Slave ein Tag oder eine Karte ist. Der Unterschied zur RFID-Technologie besteht darin, dass ein NFC-Gerät nicht nur die Rolle eines Lesegeräts, sondern ebenfalls eines Tags (Card Emulation Mode). Mittels Peer-to-Peer Modus können Daten zwischen zwei Geräten ausgetauscht werden, was von RFID nicht unterstützt wird (Märtens, 2017).

Das NFC-Forum definiert verschiedene Arten von Tags, um eine Interoperabilität zu gewährleisten. Diese Tags unterscheiden sich im verwendeten Speicher: dieser kann nur lesbar, einmal beschreibbar oder wiederbeschreibbar sein. Die gespeicherten Daten können beliebiger Natur sein, werden in einer standardisierten Form gespeichert und können vom verwendeten Betriebssystem direkt abgerufen werden (Proehl, 2013). Verwendet wird diese Technologie im

Smart Home üblicherweise als Trigger für ein Smartphone, welches an das entsprechende Gerät gehalten wird und somit eine Aktion auslöst – etwa das Öffnen der Haustüre.

3.2.1.3 ZigBee

ZigBee bezeichnet eine drahtlose Übertragungstechnik, die auf dem IEEE Standard 802.15.4 aufsetzt und für die Kommunikation innerhalb kurzer Entfernungen in IoT-Anwendungen verwendet wird (ITWissen.info, 2015a). Der Standard IEEE 802.15.4 ist ein kostengünstiger und ressourcenschonender Standard für *Personal Area Networks* (PAN). Ein weiterer Standard, der auf IEEE 802.15.4 aufsetzt, ist 6LoWPAN, welcher häufig Einsatz im industriellen IoT-Umfeld findet. Aufgrund der energiesparsamen Anwendung können Endgeräte, die mittels ZigBee kommunizieren, sinnvoll mit Batterien betrieben werden. Der ressourcenschonende Betrieb geht auf Kosten der Datenrate; diese ist im Vergleich zu anderen etablierten Standards wie Bluetooth oder WiFi gering (Mahmoud & Jeedella, 2010). Die Spezifikationen des Standards definieren nur die zwei untersten Schichten des OSI-Referenzmodells: den *Physical Layer* sowie den *Media Access Control Layer (MAC)*. 2002 wurde der ZigBee Standard von der ZigBee Allianz ins Leben gerufen (Gislason, 2008).

Die Datenübertragungsrate, die Übertragungsfrequenz und die maximale Anzahl der Netzwerkteilnehmer sind spezifiziert. Die erzielten Datenraten reichen von 250 kbit/s bis zu 20 kB/s, abhängig von der Entfernung zwischen den Geräten sowie der verwendeten Übertragungsleistung. Die maximale Übertragungsreichweite beträgt in Innenräumen 100 Meter (Zigbee Alliance, 2020). Die Endgeräte arbeiten auf Basis folgender Funkfrequenzen: 868 MHz in Europa, 915 MHz in den Vereinigten Staaten und 2,4 GHz weltweit, da dieses Frequenzband frei und unlizenziert verwendet werden darf (Zigbee Alliance, 2020). Die maximale Anzahl der Netzwerkteilnehmer ist nicht limitiert, jedoch werden die Netzwerkadressen der Teilnehmer in 64-bit Zahlen gespeichert. Somit ergibt sich eine theoretische Höchstanzahl von 2^{64} Endgeräten.

IEEE 802.15.4 definiert drei mögliche Schemas im Netzwerk: das Sternschema, den Cluster Tree sowie das Mesh-Netzwerk.

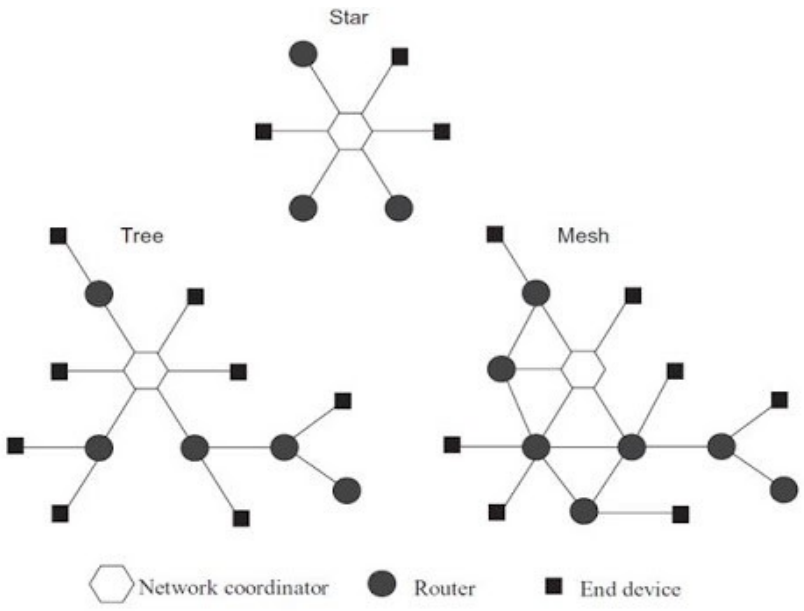

Abbildung 6: ZigBee Netzwerktopologien (Gislason, 2008)

Ein Mesh-Netzwerk, wie in Abbildung 6 veranschaulicht, ermöglicht eine hohe Stabilität sowie Reichweite, da es mehrere Pfade durch das Netzwerk bereitstellt. Dies macht das Mesh-Netzwerk zur bevorzugten Topologie. In einem Sternschema existiert immer ein einzelner Punkt, von dem das gesamte Netzwerk abhängig ist. In einem ZigBee-Netzwerk gibt es drei verschiedene Arten von Netzwerkteilnehmern (Gislason, 2008):

- *PAN Coordinator*: Dieses Gerät stellt den Eintrittspunkt im Netzwerk dar, ist nur einmal vertreten und ist für die Verbindung unter den Geräten zuständig. Gleichzeitig fungiert es als Router zwischen den anderen Netzwerkteilnehmern. Es gehört zur Gruppe der *Full Function Devices* (FFD) und stellt üblicherweise den dauerhaft mit Strom versorgten sowie mit einer IP-Schnittstelle ausgestatteten Gateway dar.
- *Router*: Ein Router kann das ZigBee-Netzwerk nicht initiieren, jedoch sucht er nach Netzwerken, um einem beitreten zu können. Sobald es einem Netzwerk angehört, kann dieser Daten zwischen *Reduced Function Devices* (RFD) routen.
- *Endgerät*: Diese Geräte versuchen, einem bestehenden Netzwerk beizutreten. Es handelt sich dabei entweder um ein RFD oder FFD und es ist üblicherweise akku- oder batteriebetrieben.

Übliche ZigBee-Endgeräte sind Lichtschalter, Rauchmelder, Bewegungsmelder und Tür- und Fensteröffnungssensoren.

3.2.1.4 Z-Wave

Z-Wave versteht sich analog zu ZigBee als energiesparsame und kostengünstige, drahtlose Übertragungstechnik, die eine geringe Bandbreite aufweist. Sie basiert auf dem Standard G.9959 der International Telecommunications Union (ITU) (International Telecommunications Union [ITU], 2015). Es wird in Smart Home Anwendungen für Beleuchtung, Temperaturregelung, Sensoren und Sicherheitstechnik verwendet (ITWissen.info, 2015b). Der Z-Wave Standard umfasst die vier Schichten *Physical Layer*, *MAC Layer*, *Network Layer* und einen Teil des *Application Layer*. Wie ZigBee stellt ein Z-Wave Netzwerk ein selbst konfigurierendes Personal Area Network dar, das als Mesh-Netzwerk aufgebaut werden kann. Somit muss jeder Netzwerkteilnehmer Daten senden, empfangen und weiterleiten können. Unterstützt wird ein Schlafmodus für Netzwerkknoten, damit diese nur bei Bedarf aufgeweckt werden; dadurch entsteht eine lange Akkulaufzeit. Der Frequenzbereich beträgt 868 MHz und es werden Datenraten zwischen 9,6 und 100 kbit/s erreicht (ITU, 2015). Die maximale Übertragungsreichweite beträgt auf freiem Sichtfeld 40 bis 150 Meter.

3.2.1.5 Bluetooth (Low Energy)

Bluetooth ist eine universelle, drahtlose Kommunikationstechnologie, die es verschiedenen Geräten ermöglicht, auf kurze Distanz Daten auszutauschen. Dieser wurde 1989 von der Bluetooth Special Interest Group (BSIG) zur Abschaffung von Kabelverbindungen zwischen mobilen Geräten und Peripheriegeräten entwickelt (Bluetooth Special Interest Group, 2020) und vom Institute of Electrical and Electronics Engineers (IEEE) unter dem Standard 802.15.1 zusammengefasst. Im Gegensatz zu den vorhin beschriebenen Technologien stellt Bluetooth eine Technologie mit hoher Datenübertragungsrate dar, welche auf Kosten des

Energieverbrauchs geht. Es wird daher bei Geräten mit ununterbrochener Stromversorgung sowie mobilen Geräten mit größeren Akkus verwendet (ITWissen.info, 2017).

Im Vergleich zu den oben beschriebenen Standards kann Bluetooth nicht innerhalb eines Mesh-Netzwerks betrieben werden, es handelt sich zwingend um eine Master-Slave Topologie. Es kann somit immer nur ein Hop im Netzwerk zurückgelegt werden, was eine Einschränkung im Vergleich zu den anderen Technologien darstellt (Gomez et al., 2012).

Bluetooth-Geräte verwenden die lizenzfreie Frequenz von 2,45 GHz, welche sich im Bereich des Industrial-Scientific-Medical (ISM) Frequenzbandes, das von 2,4 bis 2,4835 GHz reicht, befindet (Labiod et al., 2007). Da dieser Frequenzbereich ebenfalls von anderen Applikationen verwendet wird, bedient sich Bluetooth dem Frequenzsprungverfahren, um Interferenzen zu vermeiden. Die drei verschiedenen Klassen 1, 2 und 3 besitzen unterschiedliche Reichweiten und Übertragungsraten: Klasse 1 unterstützt Reichweiten bis 100 Meter, Klasse 2 bis 10 Meter und Klasse 3 bis 1 Meter. Diese ergeben sich durch die unterschiedliche emittierte Leistung. Die maximale Datenrate liegt bei 1 Mbit/s. Beim Verbindungsaufbau wird mittels Diffie-Hellman-Verfahren ein 128-Bit Schlüssel ausgetauscht, womit die Daten während der Übertragung synchron mittels dem Advanced Encryption Standard (AES) verschlüsselt werden.

Für stromsparende IoT- und weitergehend Smart-Home Anwendungen wurde von der Bluetooth Special Interest Group innerhalb der Version 4.0 im Jahre 2009 der neue Protokollstapel „Bluetooth Low Energy“ (BLE) entwickelt (ITWissen.info, 2018). Diese Variante weist keine Abwärtskompatibilität zum herkömmlichen Bluetooth-Protokollstapel auf, es werden Endgeräte mit hybrider Unterstützung angeboten. Der Vorteil von BLE liegt im reduzierten Stromverbrauch, welcher durch einen schnelleren Übertragungsaufbau sowie längeren Schlafphasen zwischen den Übertragungen erreicht wird. Der Nachteil liegt in der reduzierten Datenübertragungsrate und erhöhten Latenz, womit keine Echtzeitdaten wie Audiodaten übertragen werden können.

3.2.1.6 Wi-Fi

Wi-Fi bezeichnet eine Gruppe von verschiedenen drahtlosen Netzwerkstandards, welche unter der Bezeichnung IEEE 802.11 von der IEEE zusammengefasst werden (ITWissen.info, 2019). *Wi-Fi* ist ein von der Wi-Fi Alliance genutzte Marke, um kompatible Geräte zu kennzeichnen. In diesem Überblick stellt Wi-Fi die Technologie mit der höchsten Datenübertragungsrate dar. Aufgrund des hohen Energiebedarfs wird es nur in Endgeräten mit Stromversorgung oder großem Akku verwendet. Weltweit ist Wi-Fi die am häufigsten genutzte drahtlose Kommunikationstechnologie (Wi-Fi Alliance, 2020). Oberstes Ziel ist es, die Kompatibilität mit dem kabelgebundenen Pendant „Ethernet“ beizubehalten.

Der Basisstandard 802.11 ist 1997 mit einer maximalen Übertragungsrate von 2 Mbit/s verabschiedet worden, mittlerweile existieren Standards mit Übertragungsraten im Gigabit-Bereich (ITWissen.info, 2019). Die verwendeten Frequenzbereiche sind 2,4 sowie 5 GHz und die Bandbreite liegt bei 20, 40, 80 oder 160 MHz. Zum aktuellen Stand (2020) ist der aktuellste Standard 802.11ax (Wi-Fi Alliance, 2020). Für eigene Anwendungszwecke speziell entwickelte Standards weisen gänzlich andere Frequenzen, Bandbreiten und Übertragungsraten auf. Diese werden im Smart Home Kontext nicht näher erläutert.

Innerhalb der 802.11-Standards wird die Übertragung auf der physikalischen Schicht definiert. Ein Netzwerk besteht aus mindestens einem Access Point, welcher den Standard unterstützt und mit dem ebenfalls kompatiblen Endgerät kommuniziert (Wi-Fi Alliance, 2020), nachdem sich diese mit dem drahtlosen Netzwerk auf Basis des Service Set Identifier (SSID) verbunden hat. Es besteht die Möglichkeit, mittels der Verwendung mehrerer Access Points die Funkabdeckung eines Bereiches zu verbessern sowie eine Redundanz zu schaffen.

3.2.1.7 Zusammenfassung

Drahtlose Übertragungstechnologien stellen die Basis für ein modernes Smart Home Netzwerk dar und sind aufgrund dem Wunsch der Konsumenten nach drahtlosen Lösungen essenziell für den Markt. In den letzten 20 Jahren entstanden mehrere Standards, die für unterschiedliche Einsatzzwecke verwendet werden können. Damit einhergehende Sicherheitsrisiken werden im anschließenden Kapitel beschrieben. In dieser Tabelle werden die in diesem Kapitel beschriebenen Technologien und deren technischen Eigenschaften zusammengefasst:

	NFC	**Z-Wave**	**ZigBee**	**Bluetooth LE**	**Wi-Fi**
IEEE Standard	-	-	802.15.4	802.15.1	802.11
Frequenzband	13,56 MHz	900 MHz	2,4 GHz	2,4 GHz	2,4 GHz 5 GHz
Max. Reichweite	20 cm	30 m	100 m	10 m	150 m
Max. Stromverbrauch	15 mA	17 mA	30 mA	12,5 mA	116 mA
Stromverbrauch pro Bit	0,03 µW	0,71 µW	186 µW	0,15 µW	0,0053 µW
Max. Datenrate	424 kbit/s	100 kbit/s	250 kbit/s	1 Mbit/s	>1Gbit/s
Netzwerktopologie	Punkt-zu-Punkt	Mesh	Stern, Cluster, Mesh	Stern-Bus	Stern, Mesh
Max. Anzahl der Netzwerkteilnehmer	2	232	65000	One-to-many	250 pro Access Point

Tabelle 1: Übersicht drahtloser Übertragungstechnologien

Die Anordnung der Technologien wurde von links nach rechts entsprechend des steigenden Energiebedarfs, Komplexität aber auch der maximalen Datenrate vorgenommen. Auf Mobilfunktechnologien wurde an dieser Stelle verzichtet.

3.2.2 Kabelgebundene Technologien des Data Link und Physical Layer

Analog zu den drahtlosen Technologien werden in einem Smart Home kabelgebundene Technologien eingesetzt. In einem Consumer-orientierten Smart Home spielen diese auf den ersten Blick eine untergeordnete Rolle, da die Endgeräte primär kabellos an das System angebunden werden. Spätestens bei der Umsetzung von speziellen Drahtlostechnologien auf IP-Basis durch Hubs werden Kabel verwendet. Bei Anwendungen, die hohe Datenraten benötigen (Video- oder Audioübertragung) oder eine stabile Verbindung unerlässlich ist, wird üblicherweise eine verkabelte Verbindung genutzt.

Im vorherigen Kapitel wurden verschiedene Standards beschrieben, die bereits auf der physikalischen Schicht eine unterschiedliche Implementierungen aufweisen. Bei kabelgebundenen Netzwerken hingegen spielt einzig Ethernet als Übertragungstechnik eine Rolle, da alle weiteren Technologien der höheren Schichten des OSI-Modells diese verwenden (Samuel, 2016). Darauf aufbauend wird der TCP/IP-Protokollstapel mit diversen Applikationsprotokollen in der Praxis angewandt. Auf Ethernet wird an dieser Stelle nicht genauer eingegangen, da diese Technologie an sich keine relevanten Sicherheitsrisiken hervorbringt, solange kein physikalischer Zugriff erlangt wurde.

Neben Ethernet und dem dabei verwendeten TCP/IP-Protokollstapel sind im Smart Home Bereich die zwei Alternativen „KNX“ (KNX Association, 2020) und „Powerline Communication“ (IEEE Standards Association, 2020) nennenswert. Bei beiden handelt es sich um ein Bussystem, wobei KNX eigene Kabelleitungen und Powerline die vorhandenen, elektrischen Leitungen der Stromversorgung nutzt. KNX ist im Bereich der Gebäude- und Objektautomatisierung beliebt, während Powerline vor allem in Privathäusern ohne zusätzliche Verkabelung gängig ist.

Diese beiden Technologien werden von dem in dieser Arbeit behandelten, generischen Smart Home System, nicht verwendet und daher nicht näher erläutert.

3.3 Netzwerkprotokolle

Innerhalb der Netzwerkschicht des ISO/OSI-Modells spielen die bekannten Protokolle IPv4 (Internet Protocol, Version 4) und IPv6 (Internet Protocol, Version 6) eine große Rolle. Analog zu den vorherigen Kapiteln sollen hier nur speziell für IoT-Anwendungen konzeptionierte Protokolle beschrieben werden.

Ein Vertreter in dieser Schicht ist 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks), welches genau genommen dem Adaption Layer zwischen dem Data Link Layer sowie dem Netzwerkprotokoll IPv6 zuzuordnen ist (Russell, 2016). Dabei soll die Brücke zwischen den vorhin beschriebenen Technologien des 802.15.4 Standards und IPv6 geschlagen werden. Es ermöglicht die Nutzung von IPv6 und komprimierten UDP-Headern in drahtlosen Anwendungen mit unstabilen Netzwerkverbindungen (J. Hui & Thubert, 2011). Gleichzeitig bietet es die Möglichkeit, die Verschlüsselung von 802.15.4 sowie des darüberliegenden UDP (DTLS) zu nutzen.

3.4 Applikationsprotokolle

Eine Interoperabilität zwischen verschiedenen Endgeräten kann nur geschaffen werden, wenn die einzelnen Netzwerkteilnehmer auf dieselben Protokolle beim Datenaustausch zurückgreifen (Atzori et al., 2017). Vor allem im industriellen IoT-Sektor greifen Hersteller und EntwicklerInnen auf spezielle Anwendungsprotokolle zurück, um geräteübergreifend eine horizontale Kompatibilität zu schaffen. Hierbei können AnwenderInnen auf dokumentierte APIs (Application Programming Interface) zurückgreifen und eigene Lösungen schaffen.

Im Smart Home Bereich versuchen Hersteller für AnwenderInnen fertig einsetzbare Lösungen auf den Markt zu bringen, welche in sich an erster Stelle als geschlossene Systeme erscheint. Um trotzdem ein untereinander funktionierendes Ökosystem anzubieten, stellen Smart Home Plattformen in der Cloud Konnektoren bereit. Mittels Authentifizierung und Verknüpfung durch die NutzerInnen können unterschiedliche Endgeräte von einer Plattform aus gesteuert werden. Zusätzlich werden teils Schnittstellen angeboten, um versierten AnwenderInnen erweiterte Möglichkeiten zu bieten.

Obwohl die in dieser Arbeit behandelten Smart Home Geräte aus dem Consumer-Bereich meist als geschlossene Systeme nach außen auftreten, werden an dieser Stelle die meistverwendeten Protokolle in einer Abbildung gezeigt. Diese werden von den Herstellern in den Endgeräten zur Kommunikation untereinander verwendet.

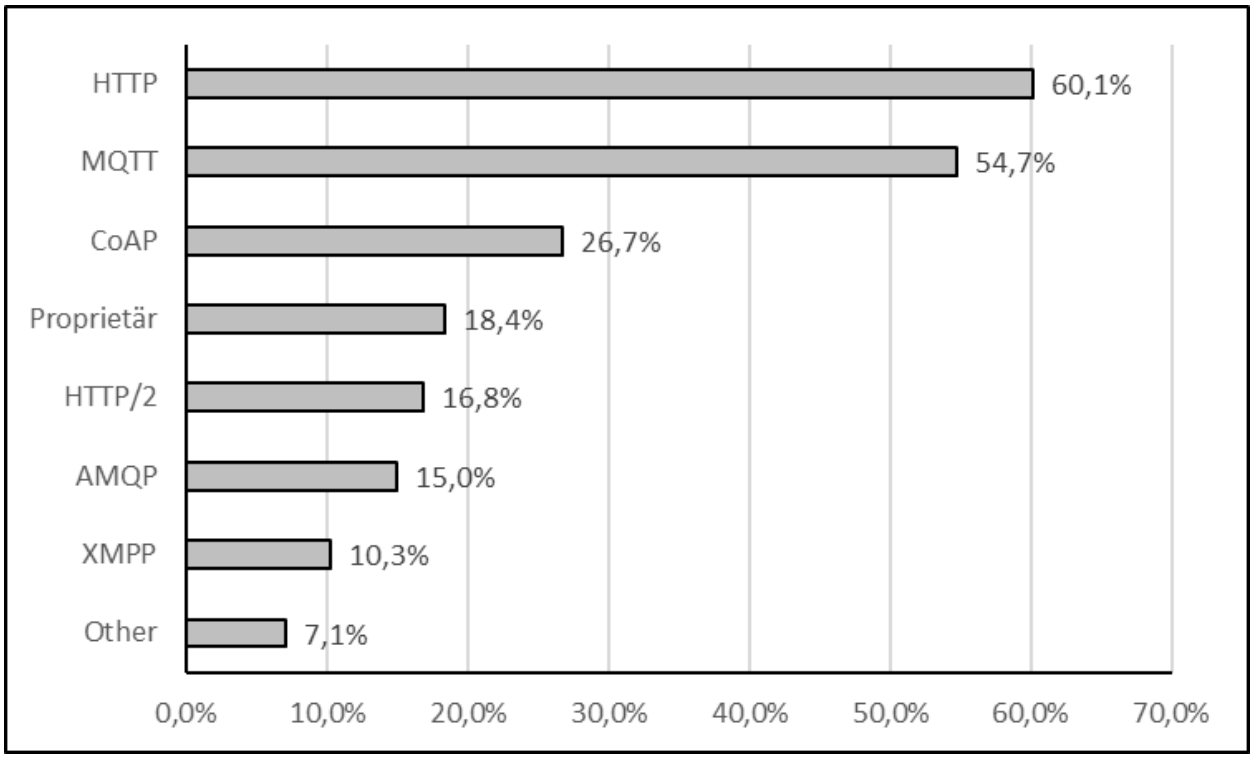

Abbildung 7: Meistverwendete IoT-Applikationsprotokolle (Skerrett, 2017)

Nach den Ergebnissen der Umfrage von Skerrett (2017) wird HTTP (Hypertext Transfer Protocol) mit 60,1 % am häufigsten verwendet. Durch das beliebte Programmierparadigma REST (Representational State Transfer), welches mit HTTP umgesetzt wird, landet dieses auf dem 1. Platz. Mit 54,7 % kommt MQTT (Message Queue Telemetry Transport) danach, gefolgt von CoAP

(Constrained Application Protocol) mit 26,7 % und proprietären Entwicklungen mit 18,4 %. Das neuere Protokoll HTTP/2 nutzen 16,8 %, danach kommt das AMQP (Advanced Message Queuing Protocol), gefolgt von dem auf XML basierenden XMPP (Extensible Messaging and Presence Protocol) mit 10,3 %.

Alle Protokolle bis auf HTTP nutzen grundsätzlich eine dem Publisher/Subscriber-Modell ähnliches Konzept, und lassen sich dadurch besonders effektiv in IoT-Anwendungen einsetzen. Die Sicherheitsmechanismen in darunterliegenden Schichten im ISO/OSI-Modell werden nächsten Hauptkapitel 4 „Informationssicherheit im Smart Home Umfeld“ beschrieben.

3.5 Cloud-Service und Wide Area Network

Das Cloud-Service der Smart Home Lösung und das Wide Area Network (WAN), welches zur Datenübertragung zwischen dem Eigenheim und dem Datenspeicher des Lösungsanbieters dient, sind von den NutzerInnen nicht beeinflussbar. Bei der Nutzung dieser Komponenten des Smart Home Systems muss den jeweiligen Anbietern für einen sicheren und stabilen Betrieb vertraut werden. Die Datenmengen verdoppeln sich durch die steigende Nutzung von Sensorik in physischen Geräten jedes Jahr , was große Anforderungen an die darunterliegenden Cloud-Services stellt (Sivarajah et al., 2017).

Der Grund für die Etablierung der Cloud-Services vor allem im Smart Home Bereich ist die Interoperabilität zwischen den Geräten. Diese fordert Rechenleistung, welche in einem typischen Endgerät nicht vorhanden ist (Lin & Bergmann, 2016). Ein Cloud-Service stellt die notwendigen Ressourcen bereit, um die Daten der Geräte zu sammeln, zu speichern und zu verarbeiten sowie diese zu überwachen. Durch Vorliegen aller Daten kann so eine Interoperabilität geschaffen sowie durch Analyse des Geräteverhaltens intelligente, automatisierte Abläufe erkannt werden. Für die Implementierung eines solchen Backend-Systems gibt es heute etablierte Architekturen und Konzepte, welche jedoch nicht Teil dieser Arbeit sind. Das Cloud-Service wird in diesem Rahmen als Black-Box angesehen. Als besonders wichtig sind die Aspekte des Datenschutzes und der Datensicherheit anzusehen, da die Daten einer Drittpartei anvertraut werden.

4 INFORMATIONSSICHERHEIT IM SMART HOME UMFELD

Sicherheitsrisiken in einem Smart Home stellen die potenzielle Gefahr für AnwenderInnen dar, durch Handlungen von Dritten unerwünschten Schaden davonzutragen. Insbesondere bei sicherheitskritischen Systemen wie Alarmanlagen und Überwachungskameras kann dadurch ein massiver Eingriff in die Privatsphäre des Anwenders passieren. Deshalb müssen in einer vernetzten Welt Vorkehrungen getroffen werden, um dies zu unterbinden. Auch für Systemhersteller kann eine öffentlich bekannt gewordene Sicherheitslücke zu einem Reputationsschaden führen. Allgemein kann niemals ein vollkommen sicheres System in der Natur existieren, sondern es werden immer Maßnahmen entsprechend der Situation vorgenommen. Auch gibt es keine einzig richtige Art und Weise, die Sicherheit eines IT-Systems in allen Dimensionen zu untersuchen und zu bewerten.

In diesem Kapitel werden die Begriffe der Informationssicherheit und des Datenschutzes sowie deren gesetzliche Grundlagen beschrieben, welche Systemanbieter einzuhalten haben. Abschließend werden konkrete Sicherheitsrisiken erläutert, welche im anschließenden praktischen Teil untersucht werden.

4.1 Informationssicherheit

Informationssicherheit ist ein wesentlicher Aspekt für Personen wie auch Unternehmen bei der Verwendung von IT-Systemen. Der Begriff Informationssicherheit ist weitreichend und lässt sich als Zusammenspiel aus mehreren Disziplinen definieren. Eine Definition der International Organisation for Standardisation (ISO) beinhaltet folgende Begriffe:

> *“Preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.” (International Organisation for Standardisation, 2018)*

Innerhalb der Informationssicherheit sollen alle vorliegenden Informationen und Daten geschützt werden, während der Verwendung und Übertragung wie auch beim Speichern. Diese Definition greift bereits auf die Aspekte der Informationssicherheit vor, welche in Kapitel 4.1.1 „Aspekte der Informationssicherheit“ beschrieben werden. Dabei werden explizit die technischen Voraussetzungen und Ziele beschrieben. Um Informationssicherheit innerhalb eines Gesamtsystems zu bewahren, welches von AnwenderInnen verwendet wird, gehören weitere Themen miteinbezogen. Die folgende Abbildung soll diese Gebiete veranschaulichen:

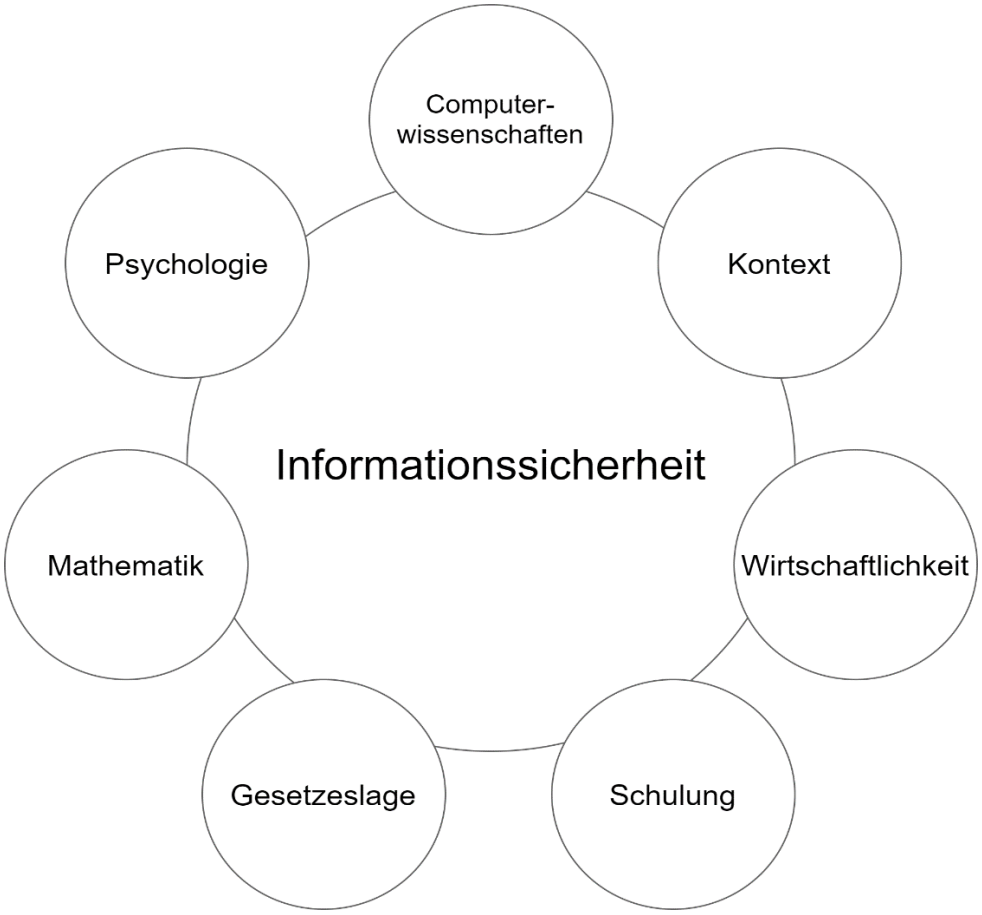

Abbildung 8: Bestandteile der Informationssicherheit (Awad et al., 2018, S. 27)

- Computerwissenschaften: Diese Wissenschaft beinhaltet die Technologien wie Datenbanken, Netzwerktechnik und Software Engineering und ist notwendig, um verwendbare Applikationen für AnwenderInnen bereitzustellen.
- Kontext: Der Kontext, in welchem Informationssicherheit bewahrt werden soll, spielt im Smart Home Umfeld aus Sicht der AnwenderInnen eine große Rolle, da es sich um persönliche, sensible Daten handelt. Unternehmen verfolgen andere Ziele, beispielsweise die Bewahrung des Rufes sowie die Geheimhaltung von internen Informationen.
- Wirtschaftlichkeit: Hierbei geht es um die Gegenüberstellung des Schadens bei einer Veröffentlichung von Information und den dagegen durchgeführten Maßnahmen.
- Schulung: Nicht nur im Unternehmensumfeld, sondern auch im privaten Umfeld kann durch Schulung und Awareness bei den AnwenderInnen die Relevanz von Informationssicherheit verstanden werden.
- Gesetzeslage: Die von Systemherstellern angebotenen Lösungen müssen den entsprechenden, gültigen Gesetzen unterliegen.
- Mathematik: Diese Naturwissenschaft stellt die Basis für eine Reihe von Sicherheitstechnologien bereit, allen voran die Verschlüsselungsmethoden.
- Psychologie: Sie hilft zu verstehen, wie NutzerInnen Sicherheit und Vertrauen wahrnehmen, wie sie sich in Risikoszenarien verhalten und welche Faktoren ein Verhalten beeinflussen.

In allgemeinen Definitionen ist oft nicht festgehalten, ob es sich um digitale oder analoge Information handelt, somit wäre niedergeschriebene Information auf Papier oder ähnlichem ebenfalls miteingeschlossen. Im Rahmen dieser Arbeit wird rein auf digitale Information Bezug genommen.

4.1.1 Aspekte der Informationssicherheit

Seit dem Entstehen des Themas gibt es die Grundprinzipien der Informationssicherheit. Diese werden auch „Schutzziele“ genannt und beschreiben die Basisanforderungen an valide Informationssicherheit. Folgend werden die Aspekte sowie der konkrete Zusammenhang zu Smart Home Systemen beschrieben.

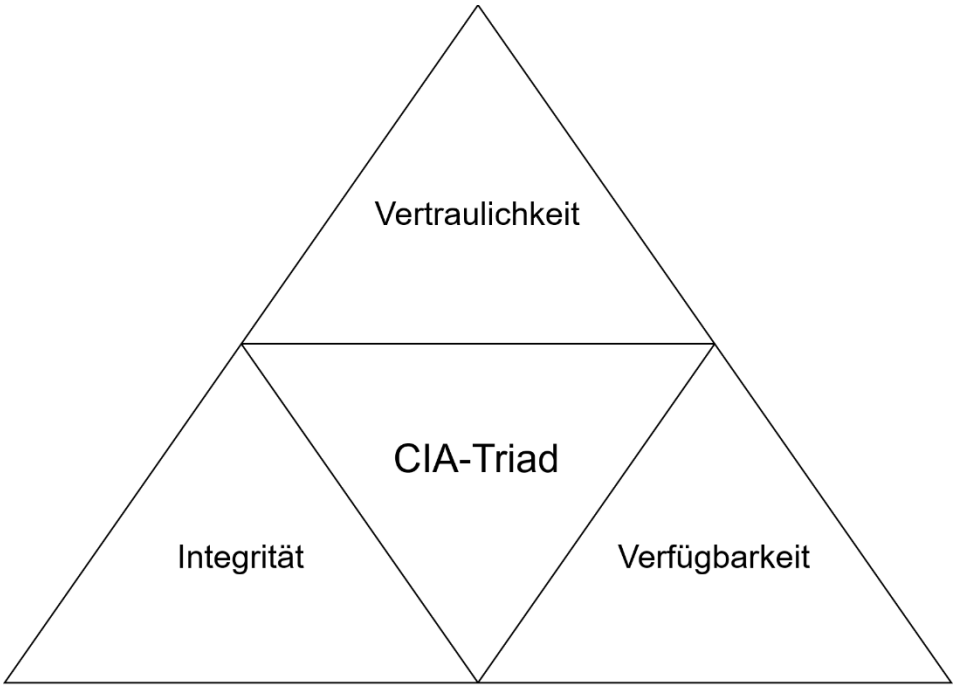

Abbildung 9: Dreieck der Informationssicherheit ("CIA-Triad")

Das 1998 ins Leben gerufene, allgemeine „Dreieck der Informationssicherheit“ („CIA-Triad“) besteht aus folgenden drei Eigenschaften (Whitman & Mattord, 2018):

Vertraulichkeit (engl. *Confidentiality*) besitzt eine Information, wenn sie vor unautorisiertem Zugriff durch Personen oder andere IT-Systeme geschützt ist. Bei Einsehen der Information durch Personen oder andere IT-Systeme ohne das Recht darauf wird diese Vertraulichkeit verletzt. Dieser Aspekt von Information ist, wie die meisten anderen, von anderen Aspekten abhängig und steht in enger Beziehung zu den Begriffen „Datenschutz“ und „Privatsphäre“. Als Beispiel hierfür kann die Wichtigkeit von Vertraulichkeit für personenbezogene Informationen genannt werden.

Um die Vertraulichkeit der Informationen in einem Smart Home Systems zu bewahren, müssen konkrete Notwendigkeiten vom System abgedeckt werden (Han et al., 2015). Die Nutzdaten der Geräte sowie die Schlüsselinformationen, die für die Verschlüsselung genutzt werden, müssen sicher über den Transportweg übertragen und gespeichert werden. Die Informationen zur Identifizierung bei einem Smart Home Gerät müssen ebenfalls kryptografisch sicher gespeichert

sein. Um ein Brute-Forcing der Informationen zur Identifizierung nutzlos zu machen, sollte das System bei NutzerInnen ein sicheres Passwort erzwingen. Dies gilt nicht nur für die Smart Home Geräte, sondern auch für die dazugehörigen Netzwerkgeräte wie Firewall und Router.

Integrität (engl. *Integrity*) weist Information vor, wenn sie nachweislich vollständig und unverfälscht ist. Dieses Ziel wird nicht erreicht, wenn Information einer unbewussten Beschädigung, Zerstörung unterliegt oder ihr authentischer Zustand auf andere Weise verändert wird (Whitman & Mattord, 2018). Eine Beschädigung von Information kann auf dem Transportweg und während des permanenten Speicherns erfolgen. Die kryptografische Methodik dagegen ist *Hashing*, welches mittels eines definierten Algorithmus ein eindeutiges Ergebnis (Wert) für eine Datei errechnet. Hiermit kann nach dem Vergleich der beiden Werte vor und nach dem Transport die Unversehrtheit einer Datei oder Information sichergestellt werden.

Um Integrität innerhalb der Informationen in einem Smart Home System sicherzustellen, soll grundsätzlich unerlaubter Zugriff auf das System unterbunden werden. Die übertragenen Daten auf ihrem Transportweg und im permanenten Speicher müssen gegen „unsichtbare" Veränderung geschützt sein.

Verfügbarkeit (engl. Availability) ermöglicht autorisierten NutzerInnen oder anderen IT-Systemen den Zugriff auf Informationen in der gewünschten Art und Weise ohne Behinderungen. Der Verlust von Information unterbindet ebenfalls die Verfügbarkeit. Für diesen Aspekt der Informationssicherheit existiert im Vergleich zu den anderen Aspekten kein direkt zuordenbares, kryptografisches Element. Es handelt sich mehr um ein Set an technischen und organisatorischen Maßnahmen innerhalb eines Systems, das eine hohe Verfügbarkeit sicherstellt.

In Smart Home Systemen kann durch automatische, intelligente Abwehrmechanismen gegen Hacker-Angriffe vorgegangen werden und so die oft zwingend notwendige Verfügbarkeit sichergestellt werden (Han et al., 2015). Weiters müssen die Methoden für eine schnelle Aktualisierung von Software bei Bekanntwerden einer Sicherheitslücke durch den Anbieter bereitstehen. Eine Überwachung des physikalischen Status eines Geräts wie Entfernung oder Hinzufügen zum System kann durch ein Geräte-Management erzielt werden. Bei ungewollten Statusänderungen, sollte beispielsweise ein Gerät offline sein, müssen entsprechende Benachrichtigungen versendet werden können. Daten und Informationen sollen bei unbeabsichtigtem Verlust immer wiederherstellbar sein.

In der Literatur wird dieses Dreieck häufig um weitere Aspekte ergänzt, um den heutigen Anforderungen an Informationssicherheit gerecht zu werden. Das *Parkerian Hexad* ergänzt das Dreieck um drei weitere Eigenschaften (Parker, 1998): **Authentizität** (engl. Authenticity) einer Information bezeichnet die Echtheit dieser, und, dass es sich dabei um keine Kopie oder Fälschung handelt, sie also in der ursprünglichen Form vorliegt. Wenn sich Absender einer E-Mail als jemand anders ausgeben, liegt keine Authentizität der Nachricht vor. Im **Besitz** (engl. *Possession or Control*) einer Information sollen nur berechtigte NutzerInnen oder andere IT-Systeme sein. Dabei wird nicht berücksichtigt, ob diese Information verschlüsselt oder im Klartext vorliegt. Die letzte Ergänzung ist die **Nützlichkeit** (engl. *Utility*) von Information, welche den Wert von Information beschreibt. Wenn beispielsweise Information verfügbar ist, jedoch nur in verschlüsselter Form, ist diese nicht nützlich.

Für die Risikoanalyse im empirischen Teil der Arbeit werden die vier Aspekte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität in Betracht gezogen. Diese stellen einen Kompromiss zwischen der Relevanz für Smart Home Systeme sowie einem entsprechendem Umfang der anschließenden Risikoanalyse dar.

4.1.2 Sicherheitstechnologien

Um die Aspekte der Informationssicherheit in der Praxis abdecken zu können, werden kryptografische Primitive eingesetzt. Sie verstehen sich als Bausteine für kryptografisch sichere Anwendungen. Die Nachfrage für sicherere Datenübertragung und -haltung steigt sowohl im öffentlichen, als auch privaten Bereich (Russell, 2016). Aufgrund der Notwendigkeit von Datensicherheit bei der wachsenden Anzahl von IoT-Geräten wird Kryptografie in Zukunft weiterhin unerlässlich sein. Diese Grundelemente kommen zum Einsatz bei der Absicherung drahtloser Netzwerke, Verschlüsselungen von Datenbanken, Datenübertragung über das Internet sowie der Integritätsprüfung von Firmware-Updates für Endgeräte.

Durch diese kryptografischen Elemente können Daten nachweislich folgende Aspekte der Informationssicherheit abdecken:

Sicherheitsaspekt	**Kryptografisches Element**
Vertraulichkeit	Verschlüsselung
Integrität	Digitale Signatur, Message Authentication Code (MAC)
Authentizität	Digitale Signatur, Hashfunktion, Message Authentication Code (MAC)

Tabelle 2: Aspekte der Informationssicherheit und dazugehöriges kryptografisches Element

Moderne Varianten dieser kryptografischen Elemente sind öffentlich nachprüfbar und gelten allgemein als kryptografisch sicher. Sicherheitslücken entstehen in der Praxis häufig durch die Verwendung mehrerer Elemente in Kombination, veralteter Version dieser oder der falschen Implementierung. Abhilfe dagegen schafft der Einsatz von öffentlich geprüften Algorithmen und Implementierungen.

4.1.2.1 Vertraulichkeit

Für die Ver- und die dazugehörige Entschlüsselung von Daten kommen verschiedene Methoden und Algorithmen zum Einsatz. Zweck ist die Verschlüsselung von Daten während der Übertragung über unsichere Netzwerke Dritter sowie während dem Speichern in einem persistenten Datenspeicher. Damit kann eine Vertraulichkeit erreicht werden, da nur berechtigte Personen mithilfe eines Schlüssels die Daten in Klartext umwandeln können. Es existieren symmetrische sowie asymmetrische Verschlüsselungsverfahren. Der Unterschied liegt in der Anzahl der verwendeten Schlüssel zum Ver- und anschließendem Entschlüsseln. Bei

symmetrischen Verschlüsselungsverfahren werden zum Ver- und Entschlüsseln derselbe Schlüssel genutzt. Der bekannteste Algorithmus dieser Gruppe ist der Advanced Encryption Standard (AES), der seit 2000 den Nachfolger des Data Encryption Standards (DES) darstellt (Daemen & Rijmen, 2002). Durch symmetrische Verschlüsselung können Datenströme schnell und ressourcensparsam verarbeitet werden.

Bei asymmetrischen Verschlüsselungsverfahren wird zum Ver- und Entschlüsseln ein unterschiedlicher Schlüssel verwendet. Diese öffentlichen und privaten Schlüssel existieren immer als zusammengehöriges Paar. Mithilfe des öffentlichen Schlüssels des Empfängers wird die Nachricht für diesen verschlüsselt und ist anschließend nur mehr mithilfe des dazugehörigen privaten Schlüssels lesbar. Diese Verfahren werden für Digitale Signaturen, zur Verwaltung von Schlüssel und zum initialen Austausch von Schlüssel für eine anschließende symmetrische Verschlüsselung genutzt. Der bekannteste Vertreter dieser Gruppe ist der RSA-Algorithmus (Rivest et al., 1978).

4.1.2.2 Integrität

Integrität bezeichnet die Verhinderung von unautorisierter Modifikation von Daten, anders ausgedrückt als die verlässliche Unversehrtheit von Daten. Dies kann bei Datenübertragung in üblichen Computernetzwerken aufgrund des technischen Prinzips nicht verhindert werden. In der Praxis kann durch eine von einer Hashfunktion generierten Prüfsumme sichergestellt werden, ob die Nachricht am Übertragungsweg zwischen Sender und Empfänger manipuliert wurde. Die Prüfsummen werden durch verschiedene Hashfunktionen berechnet, die verbreitetste Gruppe ist die Familie der Secure Hash Algorithmen (SHA) (Eastlake & Jones, 2001).

Hashfunktionen allein haben einen begrenzten Nutzungsumfang. In der Praxis sind sie notwendiger Bestandteil von Message Authentication Codes wie HMAC (Hash Message Authentication Code) und Digitalen Signaturen, um zusätzlich zur Integrität der Daten den Ursprung von Nachrichten sicherzustellen (Authentizität).

4.1.2.3 Authentizität

Wenn der Ursprung einer Nachricht nachgewiesen werden kann, spricht man von Authentizität der Nachricht des Senders. Mithilfe von digitalen Signaturen wird dies in der Praxis bewerkstelligt. Sie kann neben der Authentizität auch die Integrität und Verbindlichkeit einer Nachricht sicherstellen. Durch die eIDAS-Verordnung ist sie innerhalb der Europäischen Union einer analogen Unterschrift durch Personen gleichgestellt (eIDAS-Verordnung, 2014).

Asymmetrische Signaturverfahren wie RSA oder der Elliptic Curve Digital Signature Algorithm (ECDSA) werden für digitale Signaturen unter anderem eingesetzt, um Netzwerkteilnehmer zu authentisieren und Software, Firmware und PKI-Zertifikate zu signieren. Aufgrund der Annahme, dass digitale Signaturen auf Basis eines privaten, unbekannten Schlüssels generiert werden, kann ein einzelner Netzwerkteilnehmer die Signatur durch ihn nicht abstreiten. Verwendet wird diese Technologie weiters in Verbindung mit Zertifikaten bei TLS, IPSec und ZigBee in Smart Home Systemen.

4.2 Datenschutz und gesetzliche Grundlagen

Unter Datenschutz versteht man allgemein den Schutz personenbezogener Daten vor Missbrauch und unsachgemäßer Verarbeitung (Kuhrau, 2020). Im Vordergrund steht dabei die Wahrung des Grundrechts auf informationelle Selbstbestimmung jeder Person. Der Datenschutz und die Informationssicherheit gehen einher, da die Informationssicherheit die technischen und organisatorischen Maßnahmen für die Einhaltung des Datenschutzes darstellen.

Nachdem in Verbindung mit Smart Home Systemen meist personenbezogene Daten verarbeitet werden, wird dieses Themengebiet im Rahmen der Arbeit in diesem Kapitel erläutert. Eine zentrale Rolle spielt seit deren Inkrafttreten im Jahr 2018 die EU-Datenschutzgrundverordnung (DSGVO). Sie erklärt ihren Umfang mithilfe der Definition von personenbezogenen Daten in Art. 4 Abs. 1 wie folgt:

> *„Personenbezogene Daten“ sind 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“* (EU-DSGVO, 2016)

Die in dieser Arbeit behandelte Architektur für Smart Home Systeme schließt die Verwendung von Services eines Drittanbieters mit ein, wodurch der Datenschutz durch Dritte erst Relevanz bekommt. In einer Smart Home Architektur, welche keine Drittanbieter oder dessen Infrastruktur miteinbezieht, können der Datenschutz und dessen gesetzliche Grundlagen ignoriert werden. Die EU-DSGVO behandelt in ihrem Umfang die Verarbeitung und Speicherung personenbezogener Daten, welche nicht pseudonymisiert oder unkenntlich gemacht wurden. Im Falle eines Smart Homes können dies Standortdaten und persönliche Daten der NutzerInnen sein. Mithilfe hoher Strafen von bis zu 20 Millionen Euro oder anteilig 4% des Jahresumsatzes für datenverarbeitende Organisationen soll ein adäquater Umgang mit personenbezogenen Daten durchgesetzt werden (Bussche & Voigt, 2018) . Es werden innerhalb des Gesetzestexts keine konkreten Umsetzungsmaßnahmen vorgeschlagen, sondern die Wahrung der Aspekte Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Daten mithilfe dem aktuellen „Stand der Technik“ erzwungen.

Eine weitere wichtige gesetzliche Grundlage bildet die NIS-Richtlinie (*Richtlinie über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*), welche für Netzbetreiber, Internetanbieter, Verkehr, Energiebetreiber sowie für weitere öffentliche Verwaltungen von Diensten gilt und in Österreich seit 2018 in Kraft ist (Schallbruch, 2016). Unternehmen und Organisationen werden unter anderem zur öffentlichen Meldung von Datenschutzvorfällen gezwungen, was das Vertrauen in das gesamte Wirtschaftssystem stärken soll.

Datenschutz als solches wird im Rahmen dieser Arbeit nicht tiefergehend behandelt, da es sich nicht um das Kernthema der Arbeit handelt. Themengebiete wie Informationssicherheitsmanagement und die Normenreihe der ISO 27000-Gruppe werden ebenfalls nicht behandelt, da diese für Unternehmen relevant sind und im privaten Bereich für NutzerInnen keine Relevanz haben.

4.3 Potenzielle Sicherheitsbedrohungen im Smart Home

Analog zu allgemeinen Computernetzwerken sind Smart Home Netzwerke auf einem Schichtenmodell aufgebaut. Es existiert kein internationaler Standard für eine genormte Architektur, somit wird die in Kapitel 2.2.3 „Smart Home Architektur“ definierte 3-Schichten-Architektur für die Unterteilung der Bedrohungen wiederverwendet.

Die Forschung im Bereich Informationssicherheit im IoT-Umfeld wird durch hohes Interesse an sicheren Protokollen und Modellen getrieben, was sich zum traditionellen Modell des Internets unterscheidet. Die Sicherheitsmaßnahmen im Smart Home müssen sowohl mit den üblichen Attacken wie auch mit einer sicheren Kommunikation zwischen Mensch und Maschine sowie zwischen Maschine und Maschine umgehen können. Damit diese Anforderungen erfüllt werden können, müssen verschiedene Maßnahmen erfüllt werden, welche später beschrieben werden. Zuerst werden in diesem Kapitel die möglichen Sicherheitsbedrohungen innerhalb der drei Schichten erläutert. Diese Ausarbeitung dient als Vorbereitung für die in Kapitel 6 durchgeführte Risikoanalyse. Dadurch kann diese übersichtlicher beschrieben werden.

4.3.1 Perception Layer

Die Absicherung des Perception Layer verfolgt den physikalischen Schutz der Smart Home Geräte und Sensoren. Diese sammeln Daten und speichern Informationen, welche als sensibel angesehen werden können. Einerseits spielt die Vermeidung von physikalischen Schäden eine Rolle, andererseits geht es um den Schutz der Geräte vor missbräuchlicher Verwendung durch Menschen (Radoglou et al., 2019). Dazu kann Diebstahl sowie weitere, durch physikalischen Zugang zu den Geräten ermöglichte Schäden, zählen.

4.3.1.1 Bedrohungen durch Menschen

Hierzu zählen Diebstahl, Vandalismus, die Manipulierung von Sensoren und Geräten sowie dadurch möglich gemachte Eavesdropping-Angriffe. Speziell bei Geräten im Außenbereich, wie Überwachungskameras, muss diese Bedrohung hoch priorisiert werden. Im weiteren Sinn können zu den bedrohten Sensoren und Geräten auch Geräte zur Bedienung des Smart Home Systems gezählt werden. Die Auswirkungen können bei dieser Art von Vorfall verheerend sein, die Eintrittswahrscheinlichkeit kann allgemein als gering angenommen werden. Die Verfügbarkeit des Systems wird bei Eintritt jedenfalls in entsprechender Form beeinträchtigt.

4.3.1.2 Bedrohungen durch die Natur

Zu dieser Gruppe zählen alle bekannten Gefahren wie Stürme, Gewitter, Erdbeben und weitere Naturkatastrophen, welche zur physikalischen Zerstörung von Geräten und Sensoren führen können. Hierbei müssen die geografischen Gegebenheiten berücksichtigt werden, welche sich naturgemäß unterscheiden und sich auf die Eintrittswahrscheinlichkeit auswirken. Schwankungen und Extrema von Temperatur und Luftfeuchtigkeit können Geräten nachhaltigen Schaden zufügen und somit den Sicherheitsaspekt „Verfügbarkeit“ stören. Die Auswirkungen eines solchen Vorfalls kann ebenfalls verheerend sein, die Eintrittswahrscheinlichkeit ist als selten anzunehmen.

4.3.2 Network Layer

Forschung sowie Wirtschaft und Industrie haben durch Authentifizierungs- und Verschlüsselungstechnologien frühzeitig Abhilfe gegen Angriffe im Network Layer geschaffen. Dennoch zählt die Absicherung gegen diese Art von Angriffen zu den größten Herausforderungen, da verschiedene Systeme und die dazugehörigen Geräte nicht immer auf übliche Technologien Rücksicht nehmen und diese unsachgemäß implementieren. Folgend werden die in der Praxis laut Radoglou et al. (2019) relevantesten Bedrohungen erläutert. Einige davon stellen speziell in Drahtlos-Netzwerken eine Gefahr dar.

4.3.2.1 Jamming-Angriffe

Drahtlos-Netzwerken können aufgrund der offenen Architektur grundsätzlich jederzeit Teilnehmer beitreten. Dadurch entstehen Sicherheitslücken wie beispielsweise Jamming-Attacken. Dabei werden vom Angreifer bewusst schadhafte Netzwerkteilnehmer eingespeist, welche durch das Verwerfen von Paketen das Netzwerk und dessen Übertragungen stören können. Dies kann bei Erfolg zu einem Denial-of-Service (DoS) führen, wodurch der Sicherheitsaspekt der Verfügbarkeit nicht mehr gegeben wäre. Mittels Intrusion Detection Systemen (IDS) können solche böshaften Netzwerkteilnehmer aufgespürt werden und so aus dem Netzwerk ausgeschlossen werden. Durch kryptografische Technologien kann die Integrität der Datenpakete sichergestellt und somit ebenfalls gegen diese Art von Angriffen vorgegangen werden (Dorus & Vinoth, 2013).

4.3.2.2 Sniffing- und Traffic-Analysis-Angriffe

Netzwerk-Sniffing und die Analyse des Traffics in einem Netzwerk werden von Angreifern dazu verwendet, Informationen über das Netzwerk und dessen Teilnehmer zu gewinnen sowie die übertragenen Daten selbst auszulesen. Diese Angriffe spielen ebenfalls bei Drahtlos-Netzwerken eine große Rolle, da hierbei kein direkter, physikalischer Zugang zum Netzwerk vorliegen muss. Gegenmaßnahmen stellen sichere Verschlüsselungsverfahren dar, welche den Aspekt der Vertraulichkeit bewahren. In der Praxis sind fehlende, kryptografisch sichere Passwörter zur Verschlüsselung ein Grund für den häufigen Erfolg bei dieser Art von Angriffen (Lee et al., 2014).

4.3.2.3 Man-in-the-Middle (MITM) Attacken

Bei dieser Art des Angriffs kann sich ein Angreifer unbemerkt in die Netzwerkübertragung einschleichen und so den Verkehr mitlauschen. Hierfür existiert eine Vielzahl von

unterschiedlichen Angriffen wie Address Resolution Protocol (ARP) Poisoning, Session Hijacking, Replay Attacken und schadhafte Proxy Server (Radoglou et al., 2019). Aufgrund der großen Anzahl an unterschiedlichen Angriffen in dieser Gruppe ist die Wahrscheinlichkeit für ein Eintreten vergleichsweise hoch. Mittels kryptografisch sicheren Verschlüsselungsmethoden sowie Intrusion Detection und Prevention Systemen kann gegen diese Angriffe vorgegangen werden. Bei Vorliegen eines solchen Angriffs werden die Sicherheitsaspekte der Vertraulichkeit sowie der Authentizität verletzt.

4.3.3 Application Layer

Die in dieser Arbeit behandelte Architektur von Smart Home Systemen behandelt Cloud-basierte Anwendungen. Aufgrund dessen behandelt der Application Layer ausschließlich Elemente einer webbasierten Lösung zur Bedienung der Smart Home Geräte. Eine zentrale Rolle hinsichtlich der Datensicherheit spielen die für die Datenhaltung verwendeten Datenbanksysteme und dazugehörige Authentifizierungssysteme der Anwendungen sowie die gesamte verwendete Infrastruktur. Die aufgezeigten Bedrohungen in dieser Gruppe wurden nach der Wahrscheinlichkeit des Auftretens in der Praxis ausgewählt (Radoglou et al., 2019).

4.3.3.1 Unautorisierter Zugriff

Ein Zugriff auf geschützte Ressourcen durch eine unautorisierte Person ist im allgemeinen Kontext der Informationssicherheit ein mit allen Mitteln zu vermeidbarer Vorfall. Aufgrund dessen existieren sämtliche Technologien, um dessen entgegenzuwirken. Hierbei muss erwähnt werden, dass für die Prävention gegen diese Art des Vorfalls sowohl der Lösungsanbieter, dessen Lieferanten oder Infrastrukturbetreiber sowie die Benutzer des Smart Home Systems zur Verantwortung gezogen werden können. Beide Parteien müssen geeignete Mechanismen der Zugriffskontrolle beachten und implementieren. Bei den BenutzerInnen kann dies Verwendung von sicheren und zufälligen Passwörtern sein. Der Anbieter ist dazu aufgrund der DSGVO in ihrem Geltungsbereich sogar gesetzlich verpflichtet, wenn es um personenbezogene Daten geht. Bei diesem Vorfall wird der Aspekt der Authentizität sowie die Vertraulichkeit aufgrund des Zugriffs auf geschützte Daten verletzt. Die Wahrscheinlichkeit für ein Eintreten ist relativ gesehen mittelmäßig hoch, die Auswirkungen jedoch potenziell signifikant.

4.3.3.2 Unsichere Software

Aufgrund der Nutzung von Drittsoftware und Webservices durch alle verbreiteten Smart Home Lösungen innerhalb der Cloud-Umgebung besteht ein Risiko von bestehenden Sicherheitslücken, die bemerkt oder unbemerkt existieren und potenziell von Angreifern ausgenutzt werden kann. Trotz hoher Sicherheitsanforderungen kommt es regelmäßig zu Vorfällen dieser Art (Lee et al., 2014). Durch konsequentes Aktualisieren und Patching von betroffener Software können Lösungsanbieter Lücken schnell schließen, jedoch muss dies im Vorfeld organisatorisch und technisch möglich gemacht werden. Bei dieser Art von Vorfall können theoretisch alle Aspekte der Informationssicherheit betroffen sein. In der Praxis wird die Wahrscheinlichkeit für solche Vorfälle als gering eingestuft.

4.3.3.3 Backdoors (Hintertüren)

Eine bewusste Umgehung von Sicherheitsmechanismen durch einen geheimen Weg wird als „Backdoor“ bezeichnet. Diese wird von Herstellern in Software eingebaut und ist grundsätzlich nur Personen und Organisationen bekannt, welche darüber informiert werden. In seltenen Fällen werden Hintertüren zufällig entdeckt, naturgemäß werden diese jedoch so versteckt wie möglich implementiert. Zusätzlich muss erwähnt werden, dass gewisse Hintertüren für die Administration in Systemen bewusst implementiert werden, um langwierigere Prozeduren abzukürzen. Dabei handelt es sich genau genommen nicht um klassische Hintertüren. Ein bekanntes Beispiel einer Hintertür wurde 2016 in Samsungs SmartThings Türschloss entdeckt (Greenberg, 2016), woraufhin viele Systeme von Dritten übernommen wurden. Ein weiterer, großflächiger Angriff wurde 2021 von einem internationalen Hackerkollektiv durchgeführt, welches sich Zugang zu etwa 150.000 Überwachungskameras des US-amerikanischen Herstellers Verkada über ein internes Administrationskonto verschaffte (Donath, 2021). Oftmals funktionieren Hintertüren auf Basis eines Services unter einem unbekannten Netzwerkport, worüber schadhafter Code ausgeführt werden. Ziele der Nutzung von Hintertüren sind die Verletzung der Aspekte der Vertraulichkeit, Integrität sowie Authentizität. Mittels Nutzung von Open-Source-Software können Lösungsanbieter beweisen, auf Hintertüren verzichtet zu haben.

4.3.4 Multi-Layer-Angriffe

Neben den vorhin beschriebenen Angriffen, welche eindeutig einem Layer im Schichtenmodell zugeordnet werden können, existieren übergeordnete Angriffe. Diese beziehen mehrere Ebenen mit ein oder können auf mehreren, unterschiedlichen Ebenen durchgeführt werden. Die Auswahl basiert auf den in der Praxis am häufigsten vorgefallenen Arten (Radoglou et al., 2019).

4.3.4.1 DoS-Angriffe

Bei Denial-of-Service-Angriffen kommt es zu einer vorübergehenden Nicht-Verfügbarkeit eines Services aufgrund einer Überlastung der vorhandenen Rechenkapazitäten. Da in jedem Layer des in dieser Arbeit genutzten Schichtenmodells Rechner eingesetzt werden, kann diese Art von Angriff auf allen Layern vorfallen. Beispiele dafür sind die Überlastung der Central Processing Unit (CPU) eines Sensors sowie die Überbeanspruchung von Speicher eines Webservers der Smart Home Lösung. Zu den verschiedenen Arten zählen die in Kapitel 4.3.2.1 „Jamming-“ beschrieben Angriffe, wie auch Flooding Angriffe. Abhilfe dagegen schaffen IDPS, welche jedoch keinen absoluten Schutz gegen diese Art von Angriffen darstellt (Apthorpe et al., 2017). In der Praxis treten solche Angriffe häufig auf und stellen eine ernstzunehmende Gefahr für Betreiber von Cloud-basierten Smart Home Lösungen dar.

4.3.4.2 Botnetze

Als Botnetze werden Zusammenschlüsse von vielen Rechnern und Geräten genannt, welche von Personen oder Organisationen gezielt für Angriffe auf die Infrastruktur oder Server anderer genutzt werden. Bei bereits vorgefallenen Angriffen durch Botnetze, allen voran dem Botnetz „Mirai“, wurden IoT-basierte Geräte wie Überwachungskameras, Router und andere, mit dem Internet verbundene Haushaltsgeräte böswillig verwendet (Johnson, 2016). Durch DoS-Angriffe

in dieser Größe, wie er 2016 auf den DNS-Provider „Dyn“ vorfiel, kann ein Dienst vollkommen ausgeschalten werden. Das Ziel solcher Angriffe ist vorrangig die Verletzung der Aspekte der Verfügbarkeit und Authentizität (Apthorpe et al., 2017). Einmal mehr können solche Angriffe durch IDPS bei Infrastruktur- und Service-Betreibern frühzeitig erkannt werden.

4.3.4.3 Kryptoanalytische Angriffe

Eine weitere Art von Angriff umfasst den gezielten Versuch, verschlüsselte Daten in Klartext zu entschlüsseln (Surendran et al., 2018). Diese können auf allen Layern des Schichtenmodells auftreten, da überall kryptografische Technologien verwendet werden, um die Aspekte der Vertraulichkeit, Integrität und Authentizität der zu schützenden Information zu bewahren. Ebendiese werden bei einem erfolgreichen Angriff verletzt. Besonders in ressourcenschwachen Rechnern, Sensoren und Geräten werden von Herstellern leichtgewichtige, kryptografische Algorithmen verwendet, die ein erhöhtes Sicherheitsrisiko darstellen. Es existieren verschiedene Arten von kryptoanalytischen Angriffen, wie „ciphertext- only“-Angriffe, „chosen-plaintext“-Angriffe und „side-channel“-Angriffe.

5 METHODIK DER RISIKOANALYSE

Der Bereich des Smart Home ist eines der in der Zukunft wichtigsten Bereiche des Internets (Ricquebourg et al., 2006). Generell ist ein sicheres Design der Systeme deshalb von Nöten. Aus diesem Grund sind systematische Methodiken zur Bewertung von theoretischen Risiken aus der Sicherheitsperspektive anzuwenden. Einerseits dienen dessen Ergebnisse den Herstellern von Smart Home Geräten und Systemen, andererseits können sich BenutzerInnen dieser ein Bild von relevanten Gefahren und Risiken machen.

In diesem Kapitel werden folgend Risikoanalysen an sich sowie das konkret verwendete Risikobewertungsmodell beschrieben.

5.1 Begriffsdefinitionen

Es gibt mehrere Erläuterungen und Definitionen für den Begriff der Risikoanalyse oder Risikobewertung. Nach dem National Institute of Technology (NIST) behandelt diese den Prozess der Identifikation von Gefahren, deren Wahrscheinlichkeit des Eintretens, deren Auswirkungen beim Eintreten sowie geeignete Methoden zur Verhinderung des Eintretens (NIST, 2012).

Allgemein handelt es sich bei Risikobewertungen um eine elementare Praktik im Bereich der Informationssicherheit und untersteht einem laufenden Prozess. Erst durch eine Untersuchung der bestehenden Gefahren kann ein Smart Home System überhaupt den gewünschten Ansprüchen an die Informationssicherheit gerecht werden. Gleichzeitig kann BenutzerInnen bei der Kaufentscheidung geholfen werden sowie Hilfestellungen bei der Verbesserung der Sicherheit des eigenen Systems gegeben werden. Da im nachfolgend verwendeten Risikobewertungsmodell die englische Sprache verwendet wird, werden die wichtigen Begriffe in deutscher und englischer Sprache erläutert.

Asset (dt. Asset oder Anlage): Dabei handelt es sich allgemein um eine Sache mit Wertbestand oder eine Person. Beispiele sind eine Festplatte ein Mitarbeiter in einer Firma.

Information Asset (dt. Informationsasset): Ein Informationsasset bezeichnet ein Stück Information in Form von Daten auf analogen oder digitalen Medien. Ein Beispiel dafür sind Daten auf einem Server, welche digital verarbeitet werden können.

Threat (dt. Gefahr oder Bedrohung): Ein Threat umfasst jeden Umstand oder jedes Ereignis mit dem Potenzial, ein Informationssystem durch unautorisierten Zugriff, Zerstörung, Offenlegung oder Änderung von Daten oder Denial-of-Service zu schädigen (NIST, 2006). Gefahren entstehen durch menschliche Handlungen sowie natürliche Ereignisse. Wenn ein Angreifer eine Schwachstelle ausnutzt, entsteht so eine Bedrohung oder Gefahr.

Impact (dt. Auswirkungen): Die Auswirkungen bezeichnen die Schwere der Folgen nach Ausnutzung einer Gefahr an einem Asset. Dies wiederum kann die Veröffentlichung von sensiblen Informationen, die Nichtverfügbarkeit nach einem DDoS-Angriff oder das Abhandenkommen von Daten sein. Diese Kennzahl wirkt sich in der Ermittlung des vorliegenden Risikos aus.

Risk (dt. Risiko): Das Risiko beschreibt das Ausmaß an Folgen, welches durch das Eintreten einer theoretischen Gefahr oder Bedrohung vorliegen würde. Es wird üblich aus der Eintrittswahrscheinlichkeit einer Gefahr und dessen potenziellen Auswirkungen berechnet.

Mitigation (dt. Maßnahmen): Bei Maßnahmen handelt es sich um konkrete Aktionen zur Risikominimierung. Diese werden im Rahmen einer Risikoanalyse nach Vorliegen der einzelnen Risiken erarbeitet, um das in der Analyse behandelte System gegenüber den Gefahren abzusichern.

Die aufgezählten Begriffe finden sich in allen Risikobewertungsmethoden und -modellen wieder, zumindest innerhalb verwandter Synonyme.

5.2 Verwendetes Risikobewertungsmodell

Für die Analyse des generischen Smart Home Systems mit den enthaltenen kritischen Geräten wird eine Methode herangezogen, um an die vorangestellte Forschungsfrage systematisch heranzugehen und diese beantworten zu können. Dafür muss im Vorhinein ein geeignetes Modell begründet ausgewählt werden.

5.2.1 Begründung der Auswahl

Nach der Recherche fiel die Auswahl dafür auf das OCTAVE Allegro Modell (Caralli et al., 2007). Es handelt sich dabei um eine Weiterentwicklung aus 2007 des allgemeinen OCTAVE Modells. OCTAVE ist ein Akronym für *Operationally Critical Threat, Asset and Vulnerability Evaluation* und wurde vom US-amerikanischen Software Engineering Institute (SEI) in seiner ersten Version 1999 veröffentlicht (Caralli et al., 2007). Vorrangig im englischsprachigen Raum hat sich dieses Framework als „de facto“ Standard etabliert (Pecb, 2015). Der Vorteil von OCTAVE Allegro liegt im reduzierten Umfang des Prozesses verglichen mit dem normalen OCTAVE Modells oder anderen, standardisierten Methodiken. Für das im Rahmen dieser Arbeit untersuchte System eignet es sich aus diesem Grund besser als andere Modelle.

Bei der Durchführung einer Risikoanalyse ist es wichtig zu wissen, welche Assets warum geschützt werden. Die logische Konsequenz daraus ist im Falle eines funktionierenden Smart Home Systems der Schutz von Informationsassets. Aus diesem Grund wird im Rahmen dieser Arbeit der Fokus auf diese Art von Assets gelegt. Als Folge daraus können weitere relevante Assets aus dem Speicherort der jeweiligen Informationen abgeleitet werden.

Durch die Nutzung des Modells soll die Robustheit von Ergebnissen sichergestellt werden. Besonders genau betrachtet das OCTAVE Allegro Modell Informationsassets und untersucht

dabei die Art und Weise, wie diese Information genutzt wird und wie sie aufgrund ihres Orts der Speicherung gewissen Risiken ausgesetzt ist. Es stellt die Technologien dafür in den Hintergrund, was sich für diese Arbeit – verglichen mit einer Risikoanalyse der Systeme eines großen Unternehmens – besser eignet. Ein weiterer Vorteil im Rahmen der Arbeit ist die Strukturierung der Phasen innerhalb des Modells, welche sich einfach auf die Beantwortung der Forschungsfragen umlegen lassen. Mit vorgegeben Arbeitsblättern können die Ergebnisse einer jeden Phase festgehalten werden und als Input für die nächste Phase dienen. So kann entlang eines roten Fadens jedes Risiko untersucht werden und immer im Fokus behalten werden.

5.2.2 Phasen des OCTAVE Allegro Modells

Es existieren acht Einzelschritte im Gesamtprozess, welche in vier Phasen eingeteilt sind. Sie sind in der Originalfassung in englischer Sprache verfasst und werden deshalb auch hier in dieser Form vorgestellt. Diese sehen wie folgt aus:

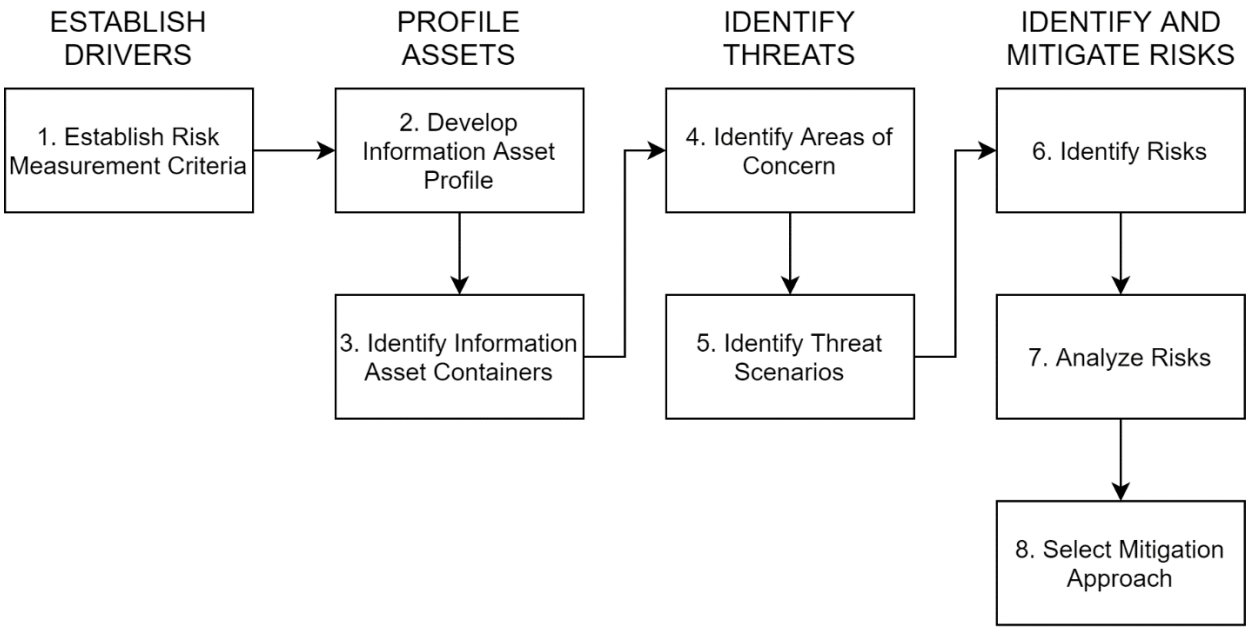

Abbildung 10: OCTAVE Allegro Prozess (Caralli et al., 2007, S. 4)

Der gesamte Prozess besteht aus vier Hauptphasen, welchen acht einzelne Schritte zugeordnet sind. Die in Abbildung 9 veranschaulichten Phasen werden folgend erläutert.

5.2.2.1 Phase 1 – „Establish Drivers“

In der ersten Phase werden die grundlegenden Kriterien definiert, nach dem im weiteren Prozess vorgegangen wird („1. Establish Risk Measurement Criteria“). Dabei geht es um die entscheidenden und kritischen Kategorien, nach dem das System untersucht werden soll. Das Ergebnis der Phase ist ein Set an Risikokriterien für das Smart Home System. Mithilfe dieser können die einzelnen Risiken bewertet werden und sind dadurch vergleichbar. Beispiele für Kriterien, die für Stakeholdern relevant sind, umfassen die Sicherheit und Gesundheit von NutzerInnen sowie die Reputation des Systems für Hersteller. Weiters wird den einzelnen Kriterien eine Bedeutung zugewiesen, welche auf einer Skala von 1(niedrigste Priorität) bis 5 (höchste Priorität) eingeschätzt wird (Caralli et al., 2007).

5.2.2.2 Phase 2 – „Profile Assets“

Ziel der zweiten Phase ist die Identifizierung von Assets und die Erstellung von Profilen dieser („2. Develop Information Asset Profile“ und „3. Identify Information Asset Containers“). Das Profil eines Assets bezeichnet dessen systematische Beschreibung innerhalb eines Worksheets in Bezug auf dessen besondere Eigenschaften, der Charakteristik sowie dessen Wert für die Stakeholder des Smart Home Systems. Während der Erstellung des Profils wird auf die Begrenzung des Einflussbereichs eines Assets und dessen Sicherheitsanforderungen Acht gegeben. Zusätzlich werden alle Orte identifiziert, an denen die Assets gespeichert, übertragen, verarbeitet und von den BenutzerInnen genutzt werden. Ein Teil des Profils ist die Verantwortung über ein Asset und wer diese besitzt. Es werden die technischen, physikalischen, logischen und personellen Assets miteinbezogen. Auf diese Weise können Lücken in der Einhaltung der Aspekte der Informationssicherheit ausfindig gemacht werden (Caralli et al., 2007).

5.2.2.3 Phase 3 – „Identify Threats“

Diese Phase beinhaltet die Schritte 4 („Identify Areas of Concern“) und 5 („Identify Threat Scenarios“), in denen die Gefahren in Bezug auf die Informationsassets mithilfe einer strukturierten Weise identifiziert und dokumentiert werden (Pecb, 2015). Die zu beachtenden Bereiche („Areas of Concern“) stellen die Schwachstellen („Vulnerabilities“) im untersuchten Smart Home System dar, aus welchen sich potenziell mögliche Bedrohungen ableiten lassen.

5.2.2.4 Phase 4 – „Identify and mitigate Risks”

In der letzten Phase, die die Schritte 6, 7 und 8 beinhaltet, werden letztlich die Risiken zu den Informationsassets auf Basis der dazugehörigen Gefahren und der Eintrittswahrscheinlichkeit definiert. Davon werden geeignete Maßnahmen zur Eindämmung jedes Risikos auf Basis der Höhe des Risikos erarbeitet. Die Risiken stellen ein Abbild der Schwere der Folgen bei Ausnutzen einer Gefahr durch einen Angreifer dar. Diese werden qualitativ bewertet, um den Stakeholdern eine Einschätzung zu geben. Allgemein gilt für die Ermittlung des Risikos folgende Berechnungsformel:

$$Risiko = Eintrittswahrscheinlichkeit * Auswirkungen\ bei\ Eintritt$$

6 DURCHFÜHRUNG DER RISIKOANALYSE

Innerhalb dieses Hauptkapitels wird das generische Smart Home System auf Basis des im vorhergehenden Kapitels beschriebenen Modells OCTAVE Allegro durchgeführt. Das Ziel dieser Analyse ist das ganzheitliche Verständnis über das System und seine Abhängigkeiten zur Umwelt, die Identifizierung von Risiken. Ein weiteres, anschließendes Ziel ist die Erarbeitung von Maßnahmen zur Eindämmung dieser Risiken und zur möglichst weitgehenden Bewahrung der Aspekte der Informationssicherheit während der gesamten Nutzungsdauer des Systems. Durch diese dürfen jedoch weder eine zeitgemäße und einfache Usability noch die Funktionalität des Systems beeinträchtigt werden. Es geht dabei um den Kompromiss zwischen Informationssicherheit und Usability (B. Ali & Awad, 2018).

6.1 Abgrenzung des analysierten Systems (Scope)

Zu einer IT-Leitung in einem Unternehmen gehört immer ein der Organisation entsprechendes Risikomanagement in Bezug auf die gesamte, eingesetzte Infrastruktur und dem Applikationsportfolio. Im kontinuierlichen Prozess des Risikomanagements sollen bestmöglich alle zu schützenden Assets berücksichtigt werden. In einem Smart Home System ist die Ausgangslage dieselbe, jedoch handelt es sich meist um kleinere, homogenere Systeme. Das übergeordnete Ziel, alle schützenswerten Assets vor Angriffen durch Dritte zu bewahren, ist jedoch dasselbe.

Wie in Kapitel 2.2 „Smart Home“ beschrieben, gibt es heute verschiedene Ziele bei der Nutzung von Smart Home Systemen. Besondere Bereiche sind die der Alten- und Krankenpflege sowie für die effiziente Energienutzung. Im Rahmen dieser Arbeit können nicht alle Aspekte dieser speziellen Ausprägungen abgedeckt werden, deshalb deckt sich das analysierte System weitgehend mit den Eigenschaften eines Smart Home System für komfortables, sicheres Wohnen und Unterhaltungsanwendungen. Es wird versucht, die aktuelle Architektur eines generischen, Cloud-basierten Smart Home Systems abzubilden. Der Fokus liegt primär auf den von BenutzerInnen beeinflussbaren Bereichen und den dazugehörigen Informationsassets. Die Infrastrukturen der Internetanbieter, das Cloud-Service des Systemherstellers sowie die genutzte Software müssen in separaten Arbeiten untersucht werden. Diese Komponenten werden im Detail im Rahmen dieser Arbeit nicht behandelt.

Die untersuchte Architektur wurde auf Basis von Abbildung 4: Generische Smart Home Architektur nach Chong et al. (2011)“ für eine Gliederung wie folgt in drei Subsysteme aufgeteilt:

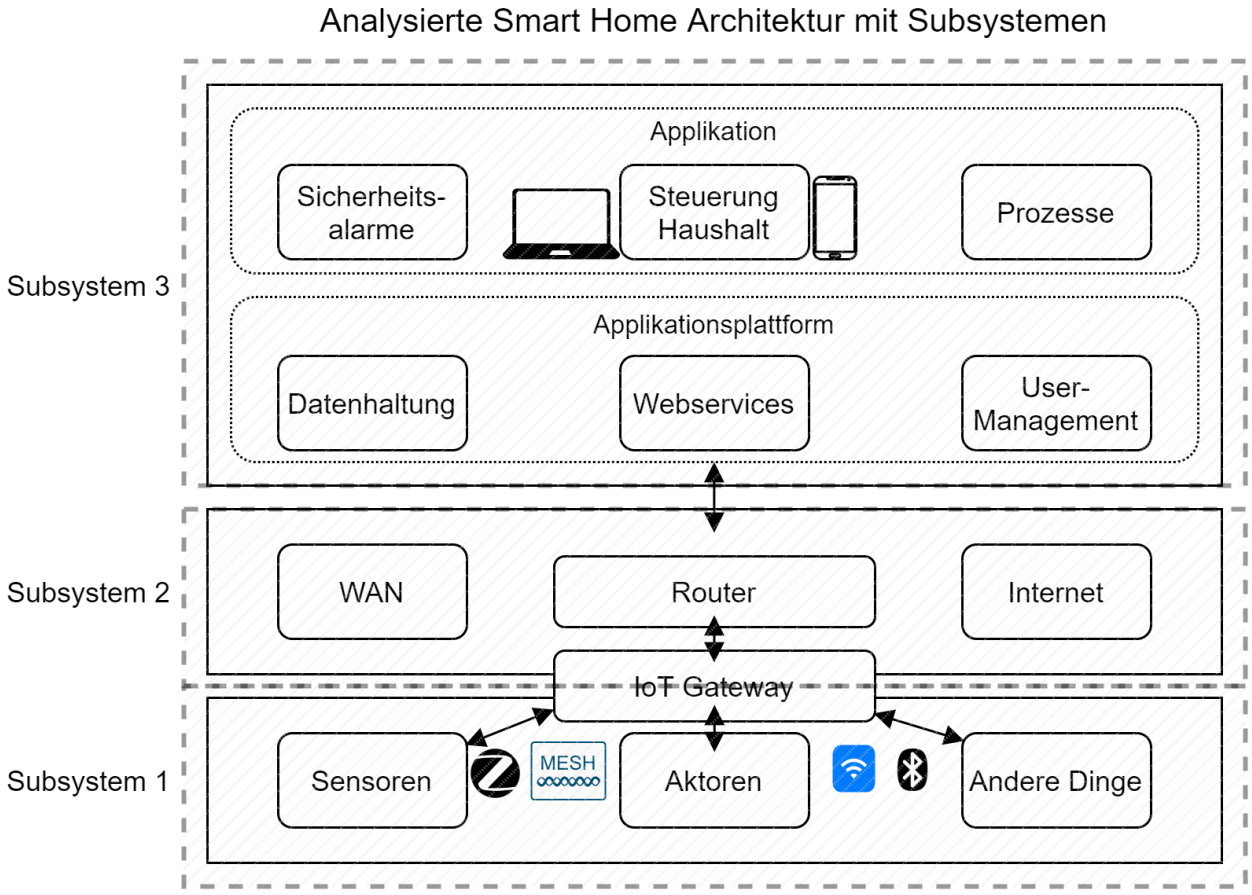

Abbildung 11: Analysierte Smart Home Architektur mit Subsystemen

Die in der obigen Abbildung gezeigten drei Subsysteme enthalten folgende physikalische Geräte:

1. **Subsystem 1**: Zu diesem System werden alle Smart Home Geräte gezählt, welche zur Datensammlung (Sensoren) sowie zur Ausübung einer Aktion (Aktoren) im Wohnbereich genutzt werden. Beispiele sind smarte Glühbirnen, Überwachungskameras und smarte Waschmaschinen. Einige dieser sind sowohl Sensoren als auch Aktoren. Zusätzlich wird die protokollspezifische Anbindung des Smart Home Gateways und in Folge dieser als Ganzes zu diesem Subsystem gezählt. Dabei spielen besonders Informationsassets eine große Rolle. Die Anbindung der Geräte erfolgt über Kabel sowie kabellos.
2. **Subsystem 2**: Dieses System umfasst alle beteiligten Netzwerkgeräte, die auf dem Transportweg von Sensoren und Aktoren bis zum Datenspeicher des Cloud-Services genutzt werden. Es existieren dabei Geräte, die im Eigentum der BenutzerInnen des Smart Home System sind, sowie Infrastruktur, die Drittanbietern wie Internetanbietern gehören. Beispiele für Geräte in diesem Subsystem sind der lokale Router, Modem, Wireless Access Points und andere, für den Betrieb eines Local Area Networks (LAN) notwendigen Geräte.

Die im Rahmen der Risikoanalyse zu betrachtenden Daten innerhalb dieses Subsystems betreffen weniger Daten, welche auf den Geräten selbst gespeichert oder dort generiert worden sind, sondern mehr die von ihnen übertragenen und verarbeiteten Daten.

3. **Subsystem 3**: Im dritten Subsystem werden das Cloud-Service des Systemanbieters inklusive zugehöriger Infrastruktur sowie die Endgeräte für die Benutzung des Smart Home Systems, wie Smartphone oder PC, bearbeitet. Ein Webinterface und/oder eine Smartphone-Applikation stehen zur Bedienung der Geräte bereit. Besonders im Vordergrund dieses Subsystems steht der Schutz vor unautorisiertem Zugriff auf das System, da alle Informationen und Daten hier gespeichert sind.

Angreifer versuchen grundsätzlich, das schwächste Glied in einem System anzugreifen. Dadurch kann potenziell der Zugriff auf den Rest des Systems möglich gemacht werden. Deshalb wird versucht, über die ganze Kette des Transports und der Speicherung von Daten eine durchgängige Sicherheit zu gewährleisten. Wie in Kapitel 5.2.1 „Begründung der Auswahl“ beschrieben, wurde das OCTAVE Allegro Modell verwendet, da es einen Fokus auf die Informationsassets legt. Die physikalische Sicherheit der beteiligten Geräte im Smart Home System werden nachrangig behandelt, besitzen jedoch in gesamter Hinsicht dieselbe Relevanz. Der Schutz vor Manipulation oder Beschädigung einer Überwachungskamera als Beispiel veranschaulicht dies, da hier die Sicherheitsaspekte der Verfügbarkeit und Integrität verletzt werden.

6.2 Identifikation kritischer Informationsassets

Aufbauend auf die in Kapitel 5.1 „Begriffsdefinitionen“ erläuterten Begriff des Informationsassets werden in diesem Schritt die relevanten und kritischen Informationsassets ermittelt. Allgemein gibt es Methoden, welche bei der Findung dieser unterstützen, wie der mit OCTAVE Allegro kombinierbare „Genre-Based Approach“ (Padyab et al., 2014). Mithilfe dieser Methodik kann ein System strukturiert auf alle potenziellen und schützenswerten Assets geprüft werden. Um diese Arbeit in einem überschaubaren Rahmen zu halten, werden insgesamt 6 kritische Informationsassets aus allen Subsystemen auf Basis der Literaturrecherche ausgewählt und als wichtig eingestuft. Wenn ein Angreifer in das System eindringen möchte, werden diese Assets als die zuerst angegriffenen angenommen.

6.2.1 Subsystem 1

Die in Subsystem 1 ausgewählten, kritischen Informationsassets umfassen folgende Assets:

- Nutzdaten der Smart Home Geräte
    - Hierzu zählen unter anderem das Videobild der Überwachungskameras, der Status des smarten Türschlosses (offen oder geschlossen) sowie eines Bewegungsmelders (Person erkannt oder nicht erkannt). Sie stellen den zentralen Datenbestand eines Smart Home Systems dar.
- Metadaten über das interne Smart Home Netzwerk (inklusive IoT-Gateway)
    - Hierzu zählen Informationen über die Struktur der Geräte im geschlossenen Smart Home Netzwerk, welche physikalisch auf dem Smart Home Gateway gespeichert sein können. Diese können die Anzahl und Art der Sensoren und Aktoren umfassen sowie zugeordnete Konfigurationen.

6.2.2 Subsystem 2

In Subsystem 2 werden folgende kritische Informationsassets definiert:

- Übertragene Daten über das Internet
    - Die Gerätedaten verlassen über den lokalen Router oder Modem das Local Area Network der BenutzerInnen. Sie beinhalten alle für die Kommunikation notwendigen Daten und müssen für die Bewahrung des Sicherheitsaspekts der Vertraulichkeit verschlüsselt sein. Im Rahmen dieser Arbeit wird angenommen, dass das Internet sicher ist, da BenutzerInnen keinen Einfluss darauf haben.
- Konfiguration des lokalen Netzwerks und Informationen darüber
    - Die sichere Konfiguration des Local Area Networks gegen Angreifer, besonders des Wireless Local Area Networks, sind unerlässlich. Wenn diese nicht vorliegt, entsteht aufgrund der niedrigen Eintrittsbarriere eine große Schwachstelle gegenüber Angreifern.

6.2.3 Subsystem 3

Innerhalb des dritten Subsystems werden folgende kritische Informationsassets analysiert:

- Client-Applikation
    - Dieses Asset umfasst alle Geräte, mit denen BenutzerInnen die Smart Home Geräte bedienen. Typischerweise handelt es sich beim physikalischen Gerät um ein Smartphone oder einen Computer, mit denen über applikations- oder webbasierte Benutzeroberflächen das Smart Home System gesteuert und konfiguriert wird.

- Cloud-Service (API)
    - Das grundsätzlich als Blackbox betrachtete Cloud-System des Herstellers der Smart Home Lösung ist maßgeblich für die Sicherheit des Gesamtsystems verantwortlich. Es liegt außerhalb des Einflussbereichs der BenutzerInnen. Es umfasst eine API für bereitgestellte Funktionen, die gespeicherten Daten und verwaltet den autorisierten Zugriff auf diese.

6.3 Risikobewertungsprozess

Nachdem alle Rahmenbedingungen für die Risikoanalyse definiert sind, wird in diesem Kapitel der Prozess mit seinen acht Einzelschritten, welche in vier Phasen eingeteilt sind, nach Vorgabe durchlaufen (Caralli et al., 2007). Alle verwendeten Arbeitsblätter werden offiziell in englischer Sprache zur Verfügung gestellt. Im Rahmen der Vorbereitungen für die Risikoanalyse wurden diese in die deutsche Sprache übersetzt.

6.3.1 Schritt 1 – „Definition der Risikobewertungskriterien"

Der Ziel dieses Schrittes ist die Definition der Kriterien, nach welchen die negativen Folgen für kommerzielle Stakeholder (Systemanbieter) sowie für nichtkommerzielle Stakeholder (BenutzerInnen des Smart Home Systems) eingeteilt werden können. Nach Vorlage des Modells sind Auswirkungen auf diese sechs Kriterien zu berücksichtigen (Caralli et al., 2007):

1. Reputation und Kundenzufriedenheit
2. Finanzielles Vermögen
3. Produktivität
4. Sicherheit und Gesundheit
5. Rechtliche Konsequenzen (Nichteinhaltung gesetzlicher Vorlagen)
6. Eventuelle eigens definierte Kriterien

Die Kriterien können innerhalb Punktes Nr. 6 individuell erweitert werden. Als kommerzielle Stakeholder werden im Rahmen der Risikoanalyse Systemanbieter, Internetanbieter, Hardwarehersteller, Software von Drittanbietern sowie jeweils deren Lieferanten angesehen. Zur Gruppe der nichtkommerziellen Stakeholdern werden BenutzerInnen des Smart Home Systems und öffentliche Behörden und Einrichtungen gezählt (B. Ali, 2016).

In Worksheet 1 (Tabelle 3) werden die drei Schweregrade des Risikobewertungskriteriums der Reputation und Kundenzufriedenheit qualitativ definiert. Wie alle weiteren Kriterien werden diese vom Ausmaß in *Niedrig*, *Mittel* und *Hoch* eingeteilt. Dieses Kriterium betrifft nur die kommerziellen Stakeholder.

Allegro Worksheet 1	***Risikobewertungskriterium – Reputation und Kundenzufriedenheit***		
Auswirkung	**Niedrig**	**Mittel**	**Hoch**
Reputation der kommerziellen Stakeholder	Die Reputation ist minimal beschädigt und es sind keine bis niedrige Einbußen im Ruf des Unternehmens hinzunehmen.	Die Reputation ist in gewissem Ausmaß beschädigt und es sind bis zu € 500.000 für einen Ausgleich dessen zu investieren.	Die Reputation ist nachhaltig beschädigt und es ist über € 500.000 für einen Ausgleich dessen zu investieren.
Kundenverlust der kommerziellen Stakeholder	Verlust von weniger als 10% der Kunden	Verlust von 10 bis 20% der Kunden	Verlust von mehr als 20% der Kunden

Tabelle 3: Allegro Risikobewertungskriterium "Reputation"

In Worksheet 2 (Tabelle 4) werden die drei Schweregrade des Risikobewertungskriteriums der des finanziellen Vermögens definiert. Dieses betrifft sowohl die kommerziellen als auch nichtkommerziellen Stakeholder, vorrangig hier die BenutzerInnen.

Allegro Worksheet 2	***Risikobewertungskriterium – Finanzielles Vermögen***		
Auswirkung	**Niedrig**	**Mittel**	**Hoch**
Einmaliger finanzieller Verlust für kommerzielle Stakeholder	Die Reputation ist minimal beschädigt und es sind keine bis niedrige Einbußen im Ruf des Unternehmens hinzunehmen.	Die Reputation ist in gewissem Ausmaß beschädigt und es sind bis zu € 500.000 für einen Ausgleich dessen zu investieren.	Die Reputation ist nachhaltig beschädigt und es ist über € 500.000 für einen Ausgleich dessen zu investieren.
Kundenverlust bei kommerziellen Stakeholdern	Verlust von weniger als 10% der Kunden	Verlust von 10 bis 20% der Kunden	Verlust von mehr als 20% der Kunden
Einmaliger finanzieller Verlust für nichtkommerzielle Stakeholder	Einmaliger Verlust bis zu € 500	Einmaliger Verlust bis zu € 1000	Einmaliger Verlust über € 1000

Tabelle 4: Allegro Risikobewertungskriterium "Finanzielles Vermögen"

Der einmalige, finanzielle Verlust für nichtkommerzielle Stakeholder bezieht sich auf die BenutzerInnen des Systems und umfasst ein ausgebautes Smart Home System mit mehreren Geräten.

Beim nächsten Kriterium handelt es sich um die Produktivität. Dabei werden den drei Auswirkungsgraden jeweils entsprechende Werte zugewiesen. Die Ergebnisse sind folgend in Worksheet 3 (Tabelle 5) dokumentiert:

Allegro Worksheet 3	***Risikobewertungskriterium – Produktivität***		
Auswirkung	**Niedrig**	**Mittel**	**Hoch**
Erhöhter Arbeitsaufwand bei kommerziellen Stakeholdern	Erhöhung des Personalaufwandes bis 10%	Erhöhung des Personalaufwandes von 10 bis 20%	Erhöhung des Personalaufwandes über 20%
Beeinträchtigte Usability bei nichtkommerziellen Stakeholdern	Erhöhter zeitlicher Aufwand bis 10%	Erhöhter zeitlicher Aufwand von 10 bis 20%	Erhöhter zeitlicher Aufwand über 20%

Tabelle 5: Allegro Risikobewertungskriterium "Produktivität"

Die beeinträchtigte Usability für BenutzerInnen kommt beispielsweise bei komplexeren Authentifizierungsmethoden zum Tragen, welche die Sicherheit erhöhen.

Beim Allegro Worksheet 4 (Tabelle 6) werden die Eigenschaften des Kriteriums Sicherheit und Gesundheit definiert. Dieses ist besonders wichtig für die BenutzerInnen des Smart Home Systems, welche nichtkommerzielle Stakeholder darstellen.

Allegro Worksheet 4	***Risikobewertungskriterium – Sicherheit und Gesundheit***		
Auswirkung	**Niedrig**	**Mittel**	**Hoch**
Gesundheit von nichtkommerziellen Stakeholdern	Geringe gesundheitliche Auswirkungen auf die BenutzerInnen	Gesundheitliche Auswirkungen, welche mindestens sieben Tage zur Heilung benötigen	Gesundheitliche Auswirkungen, welche permanente Schäden an BenutzerInnen verursacht.
Sicherheit von nichtkommerziellen Stakeholdern	Die Sicherheit der BenutzerInnen wird in Frage gestellt, jedoch liegt keine tatsächliche Gefährdung vor.	Die Sicherheit der BenutzerInnen wird gering gefährdet, ohne gesetzliche Verstöße.	Die Sicherheit der BenutzerInnen wird gering gefährdet, mit Vorliegen gesetzlicher Verstöße.

Tabelle 6: Allegro Risikobewertungskriterium "Sicherheit und Gesundheit"

Im Risikobewertungskriterium „Sicherheit und Gesundheit“ geht es aus Sicht der BenutzerInnen um die Bewahrung deren Sicherheit und Gesundheit. Diese darf durch die Nutzung des Smart Home Systems nicht bedroht werden.

Im nächsten Risikobewertungskriterium werden die Auswirkungen von Strafen definiert, welche sich im Allegro Worksheet 5 (Tabelle 6) wiederfinden. Diese können aufgrund von gesetzlichen Verstößen durch die Systemanbieter anfallen und sind deshalb nur für kommerzielle Stakeholder relevant.

Allegro Worksheet 5	***Risikobewertungskriterium – Strafen***		
Auswirkung	**Niedrig**	**Mittel**	**Hoch**
Kosten von Gerichtsverfahren für kommerzielle Stakeholder	Kosten bis € 100.000	Kosten von € 100.000 bis € 500.000	Kosten über € 500.000
Finanzielle Strafen für kommerzielle Stakeholder	Strafen bis € 100.000	Strafen von € 100.000 bis € 500.000	Strafen über € 500.000

Tabelle 7: Allegro Risikobewertungskriterium "Strafen"

Dieses Kriterium betrifft nur die kommerziellen Stakeholder und sind für die BenutzerInnen nicht relevant.

Im Rahmen der Risikoanalyse mittels Allegro OCTAVE können im Allegro Worksheet 6 eigenständig Kriterien definiert werden. Im Rahmen dieser Arbeit sind die bereits definierten Kriterien ausreichend, deshalb werden keine weiteren Kriterien definiert. Die obig definierten Kriterien wurden nun für nichtkommerzielle und kommerzielle Stakeholder definiert. Im nächsten Schritt der Risikoanalyse werden im Allegro Worksheet 7 die Priorität der Kriterien festgelegt. Im Falle des Smart Home Systems ist allgemein die Sicherheit der BenutzerInnen das wichtigste Kriterium. Folgend die Definition der Prioritäten (Tabelle 8):

Allegro Worksheet 7	***Definition der Prioritäten der Risikobewertungskriterien***
Prioritätsstufe	**Risikobewertungskriterium**
4	Reputation und Kundenzufriedenheit
3	Finanzielles Vermögen
3	Produktivität
5	Sicherheit und Gesundheit
1	Strafen

Tabelle 8: Prioritäten der einzelnen Risikobewertungskriterien

Neben dem wichtigsten Kriterium „Sicherheit und Gesundheit“ für BenutzerInnen ist das Kriterium der „Reputation und Kundenzufriedenheit“ mit der Prioritätsstufe 4 ein wichtiges, da davon der Erfolg von Smart Home Systemen abhängt. Es muss dafür Vertrauen in das System und die Hersteller vorliegen. Den Kriterien „Produktivität“ und „Finanzielles Vermögen“ wird eine mittlere Prioritätsstufe (3) zugewiesen. Als letztes Kriterium wird „Strafen“, das ausschließlich die kommerziellen Stakeholder betrifft, mit der niedrigsten Priorität (1) definiert.

6.3.2 Schritt 2 – „Entwicklung von Profilen der Informationsassets“

Nach der Definition der Risikobewertungskriterien im vorhergehenden Kapitel werden anschließend die Eigenschaften der kritischen Informationsassets, welche in Kapitel 6.2 „Identifikation kritischer Informationsassets“ aufgestellt wurden, mittels Profilen erarbeitet. Ziel dabei ist es, das Asset so genau und abgegrenzt wie möglich zu definieren, inklusive der Speicherorte, der Verantwortlichen sowie der notwendigen Sicherheitsanforderungen. Die weiteren Schritte werden anhand des Beispiels dieses Informationsassets veranschaulicht. Alle weiteren Informationsassets werden im Anschluss gesammelt den Arbeitsschritten unterzogen.

Folgend wird für einen einfachen Überblick nach der Einteilung der drei Subsysteme vorgegangen. Im ersten Subsystem befinden sich die zwei kritischen Informationsassets „Nutzdaten der Smart Home Geräte“ und „Metadaten über das interne Smart Home Netzwerk (inklusive IoT-Gateway)“. Als Beispiel für Nutzdaten, welche alle gesammelten Daten von Sensoren umfassen, kann das Videobild einer Überwachungskamera sowie der Status einer Alarmanlage genannt werden.

Hier werden die Profile der kritischen Informationsassets des Subsystems 1 erarbeitet. Zuerst ist dies das Informationsasset der „Nutzdaten der Smart Home Geräte“:

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Kritisches Asset *Was ist das kritische Informationsasset?*	**(2) Begründung für Auswahl** *Warum ist dieses Asset wichtig für die Organisation?*	**(3) Beschreibung** *Wie wird das Asset beschrieben?*
Nutzdaten des Smart Home Systems (Beispiele: Videoaufnahme der Überwachungskamera, Status der Alarmanlage)	Der Inhalt der Informationen umfasst die gesamten Daten, die für die Nutzung des Smart Home Systems notwendig sind. Eine Offenlegung würde die Privatsphäre der NutzerInnen verletzen.	Daten, welche von allen im Smart Home System von Sensoren gesammelt oder von Überwachungskameras erstellt werden.
(4) Verantwortliche und BesitzerInnen *Wer besitzt dieses Informationsasset?*		
BenutzerInnen und EigentümerInnen des Smart Home Systems		
(5) Sicherheitsanforderungen *Welche Sicherheitsanforderungen sind für dieses Informationsasset notwendig?*		
✓ **Vertraulichkeit**	Nur autorisierte Personen dürfen auf die Daten zugreifen können:	BenutzerInnen des Smart Home Systems
✓ **Integrität**	Alle Änderungen an den Daten müssen nachvollzogen werden können und dürfen nur von autorisierten Personen durchgeführt werden:	BenutzerInnen des Smart Home Systems
✓ **Verfügbarkeit**	Dieses Asset muss zur Verfügung stehen, um die Nutzung des Smart Home Systems und die Bewahrung der Privatsphäre sicherstellen zu können.	BenutzerInnen und Anbieter des Smart Home Systems
	Dieses Asset muss 24 Stunden am Tag und 7 Tage in der Woche zur Verfügung stehen.	BenutzerInnen und Anbieter des Smart Home Systems
✓ **Authentizität**	Dieses Asset darf nur für autorisierten Personen zugänglich sein:	BenutzerInnen des Smart Home Systems
(6) Wichtigster Sicherheitsaspekt *Welcher ist der wichtigste Aspekt der Informationssicherheit dieses Informationsassets?*		
✓ Vertraulichkeit	✓ Integrität	✓ Verfügbarkeit ✓ Authentizität

Tabelle 9: Profil kritisches Informationsasset "Nutzdaten des Smart Home Systems"

Bei diesem Informationsasset handelt es sich um die Daten, von dem das Smart Home System abhängig ist. Sie müssen neben dem autorisierten Zugriff zu jeder Zeit richtig und verfügbar sein, um Automatismen durchführen und die Sicherheit der BewohnerInnen bewahren zu können. Damit ist der zweite Schritt der Risikoanalyse für dieses Informationsasset abgeschlossen.

6.3.3 Schritt 3 – „Identify Information Asset Containers"

Unter einem Container für ein Informationsasset werden Orte bezeichnet, an dem die Information erstellt, übertragen, verarbeitet oder gespeichert wird. Technisch umfassen diese Festplatten, Cloud-Server und Netzwerkkomponenten. Zusätzlich sind noch der physikalische Ort und involvierte Personen relevant (Caralli et al., 2007). Es werden drei Worksheets für jeweils die technische, physikalische und personelle Umgebung erarbeitet. Folgend die Beschreibung der drei Container für das Asset „Nutzdaten der Smart Home Geräte":

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Intern	
Beschreibung des Containers	**BesitzerInnen**
1. Smart Home Geräte: Auf den Geräten selbst sind Nutzdaten gespeichert. Aus diesem Grund muss ein physischer Schutz vor Diebstahl gewährleistet sein.	BenutzerInnen
2. Netzwerkgeräte im Heimnetz (LAN)	BenutzerInnen
Extern	
Beschreibung des Containers	**BesitzerInnen**
1. Bediengeräte (PC, Smartphone, Tablet)	BenutzerInnen
2. Cloud-Server und Datenbanken	Systemanbieter und Service Provider
3. Netzwerkgeräte im Internet	Internet Service Provider

Tabelle 10: Container (Technical) "Nutzdaten der Smart Home Geräte"

Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Intern	
Beschreibung des Containers	**BesitzerInnen**
1. Backup-Medien: Festplatten, Disks	BenutzerInnen
Extern	
Beschreibung des Containers	**BesitzerInnen**
-	-

Tabelle 11: Container (Physical) "Nutzdaten der Smart Home Geräte"

Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Intern	
Beschreibung des Containers	**Personen**
1. BenutzerInnen des Smart Home Systems	BenutzerInnen
Extern	
Beschreibung des Containers	**Personen**
1. Gäste im Wohnbereich	Gäste
2. Arbeitende im Wohnbereich (HandwerkerInnen, etc.)	Arbeitende

Tabelle 12: Container (People) "Nutzdaten der Smart Home Geräte"

6.3.4 Schritt 4 – „Identify Areas of Concern"

Im vierten Schritt der OCTAVE Allegro Risikoanalyse werden Szenarien beschrieben, in denen ein Informationsasset Schaden annehmen kann (Caralli et al., 2007). Dieser umfasst den Verlust, die Offenlegung, die Unterbrechung der Verfügbarkeit oder geheime Manipulation von Informationen. Alle Bereiche, die Gefahren darstellen können, werden auf Basis des Wissens aus der Literaturrecherche abgeleitet. Aufgrund der erhobenen Daten aus Schritt 3 sind die Speicherorte der Informationsassets bereits bekannt.

6.3.5 Schritt 5 – „Identify Threat Scenarios"

Unter Threat wird eine potenzielle Bedrohung bezeichnet, welche zu jeder Zeit bewusst böswillig oder unbewusst ausgenutzt werden kann. Beispiele sind der Angriff eines Hackers, der zu einem DoS des Smart Home Systems führt und ein Naturereignis, welche Geräte physisch zerstört. Ein Bedrohungsszenario ist eine konkrete Situation, in der ein Actor mit einem bestimmten Motiv eine dieser Bedrohungen ausnützt. Es handelt sich dabei um einen einfach Weg, über den ein Risiko untersucht werden kann (Caralli et al., 2007).

Die in diesem Schritt verwendeten Begriffe werden aus praktischen Gründen nicht ins Deutsche übersetzt, jedoch hier erläutert (Caralli et al., 2007):

- Actor – die Person oder Sache, welche potenziell die Sicherheit eines Informationsassets gefährden kann
- Means – die Art und Weise, wie ein Sicherheitsaspekt des Informationsassets verletzt werden kann
- Motive – die Absicht des Actors bei der Ausnutzung eines Bedrohungsszenarios (bezogen auf Personen), bewusst oder unbewusst

- Outcome – das resultierende Ergebnis des Assets aus dem Eintreten der Bedrohung (Offenlegung, Verlust, Modifizierung, Unterbrechung der Verfügbarkeit des Informationsassets)

6.3.6 Schritt 6 – „Identify Risks“

In diesem Schritt spielen die Auswirkungen beim Eintreten einer Gefahr sowie das damit zusammenhängende Risiko eine Rolle. In einer Beschreibung der Auswirkung wird festgehalten, was die konkreten Auswirkungen auf die BenutzerInnen des Smart Home Systems sind. Ein Risiko beschreibt die Kombination aus der Wahrscheinlichkeit, zu der ein unerwünschtes Ereignis eintritt, und dessen Schweregrad der Konsequenzen des Eintretens. Kein System kann ohne Risiken betrieben werden (W. Ali et al., 2017).

6.3.7 Schritt 7 – „Analyze Risks“

Es wird in jedem Worksheet 10 für jedes Risiko der Informationsassets dieses Risiko untersucht. Dabei wird auf Basis der Konsequenzen eine qualitative Bewertung mittels den drei Möglichkeiten „Low“, „Medium“ und „High“ definiert. Im Anschluss erfolgt die Bewertung durch Multiplikation der definierten Impact Areas aus Worksheet 7 mit der vorangegangenen, qualitativen Bewertung. Daraus leiten sich Werte ab, welche aufsummiert werden und damit das relative Risiko für dieses Risiko eines Informationsassets abbilden.

6.3.8 Schritt 8 – „Select Mitigation Approach“

Im abschließenden Schritt werden die Maßnahmen gegenüber jedem Risiko definiert. Diese werden nach OCTAVE Allegro in drei Arten kategorisiert (Caralli et al., 2007):

- Accept: Das Risiko wird in seinem Ausmaß akzeptiert und keine Gegenmaßnahmen definiert. Diese Strategie wird ausschließlich bei niedrigen Risiken verfolgt.
- Mitigate: Bei dieser Herangehensweise wird für das Risiko eine entsprechende Gegenmaßnahme definiert. Diese Strategie wird bei mittleren und hohen Risiken angewandt.
- Defer: Bei diesem Umgang mit einem Risiko wird direkt keine Maßnahme getroffen, das Risiko jedoch nicht akzeptiert. Es dient zur Klassifizierung eines Risikos, welches zu einem späteren Zeitpunkt untersucht wird, da es aktuell kein Risiko darstellt.

Bei Einhaltung der Gegenmaßnahmen besteht weiterhin bei jedem Risiko ein Restrisiko, welches akzeptiert werden muss. Ziel dieses Schrittes ist es, geeignete Abhilfen für die höchsten Risiken zu finden und gegenzusteuern.

6.3.9 Erarbeitung der Risiken

In den folgenden Unterkapiteln werden die einzelnen Risiken entsprechend den Subsystemen erarbeitet. Es werden ausgewählte „Areas of Concern“ erläutert, welche nicht alle in der Praxis vorkommenden Gefahren abbilden. Dies würde über den Rahmen dieser Arbeit hinausgehen und ist allgemein nicht möglich (Surendran et al., 2018).

6.3.9.1 Subsystem 1

Die Ergebnisse des ersten Szenarios werden in Allegro Worksheet 10 festgehalten. Es folgt das erarbeitete Risk Worksheet für das Informationsasset „Nutzdaten der Smart Home Geräte“ und der Area of Concern „Unautorisierter Zugriff auf Nutzdaten der Smart Home Geräte“ in Tabelle 13:

Allegro - Worksheet 10		**Informationsasset - Risk Worksheet**			
Information Asset Risk	**Threat**	Informations-Asset	Nutzdaten der Smart Home Geräte		
		Area of Concern	Unautorisierter Zugriff auf Nutzdaten der Smart Home Geräte		
		(1) Actor *Who would exploit the area of concern or threat?*	Hacker		
		(2) Means *How would the actor do it? What would they do?*	Eine Schwachstelle bewusst ausnutzen, um Zugriff auf private Informationen zu erhalten		
		(3) Motive *What is the actor's reason for doing it?*	Versuch des Abgreifens von persönlichen Informationen und möglicher Verkauf dieser		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Offenlegung** ✓ **Modifizierung**	✓ **Verlust** ✓ **Unterbrechung der Verfügbarkeit**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Bei Bekanntwerden des Passworts des Smart Home Accounts oder Eindringen in das lokale Netzwerk oder Smart Home Geräte. Das Passwort muss sicher verwahrt werden.		
		(6) Likelihood *What is the likelihood that this threat scenario could occur?*	**High**	✓ **Medium**	**Low**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Wert**	**Score**
	Diese „Area of Concern“ ist potenziell gefährlich und kann den Smart Home BenutzerInnen großen Schaden zufügen. Die Ressourcen können für die BenutzerInnen nicht mehr verfügbar sein und dadurch eine Gefährdung		Reputation und Kundenzufriedenheit - 4	3	12 (=4*3)
			Finanzielles Vermögen – 3	2	6

	der Sicherheit entstehen. Eine Verletzung der Privatsphäre bei Abgreifen des Videobilds einer Überwachungskamera liegt vor. Durch damit möglicher Spionage ist ein Einbruch in den Wohnbereich möglich.	Produktivität – 3	3	9
		Sicherheit und Gesundheit – 5	3	15
		Strafen - 1	1	1
			Relativer Risiko-Score	**43**

(9) Umgang mit Risiken *Based on the total score for this risk, what action will you take?*			
Accept	**Defer**	✓ **Mitigate**	**Transfer**
Gewählte Maßnahmen als Abhilfe gegen das Risiko:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Physical	Die Smart Home Geräte müssen physisch unzugänglich oder schwer demontierbar sein. Eine Überwachungskamera muss dafür an den richtigen Orten installiert sein. Etwaige Backup-Medien werden für Besucher unzugänglich aufbewahrt.		
People	Alle BenutzerInnen des Smart Home Systems wird das Bewusstsein für Informationssicherheit in Kombination mit Smart Home Systemen durch Aufklärung geschult. Allen BenutzerInnen des Smart Home Systems wird die Bedeutung von kryptografisch sicheren Passwörtern mitgeteilt.		
Technical	Verwendung von kryptografisch sicheren Transportprotokollen mit TLS. Nutzung von kryptografisch sicheren Algorithmen bei der notwendigen Verschlüsselung von Nutzdaten durch die Software des Anbieters. Nutzung von kryptografisch sicheren Passwörtern. Aktivierung von 2-Faktor-Authentifizierung. Einsatz von Ende-zu-Ende Verschlüsselung durch den Systemanbieter.		

Tabelle 13: Risk Worksheet 10 "Nutzdaten der Smart Home Geräte" 1

Innerhalb kritischer Smart Home Infrastruktur spielt die Verfügbarkeit eine große Rolle. Die Area of Concern „Permanente Energieversorgung“ ist für Geräte in diesem Bereich relevant, daher folgt das Risk Worksheet für diese Area of Concern in Tabelle 14 als zweites Risiko für das wichtige Informationsasset „Nutzdaten der Smart Home Geräte“:

Allegro - Worksheet 10		**Informationsasset - Risk Worksheet**	
Information Asset Risk	**Threat**	Informations-Asset	Nutzdaten der Smart Home Geräte
		Area of Concern	Unterbrechung der Energieversorgung (Stromversorgung, Batterien)
		(1) Actor *Who would exploit the area of concern or threat?*	Stromausfälle Leere Akkus und Batterien
		(2) Means *How would the actor do it? What would they do?*	Keine Personen beteiligt

		(3) Motive *What is the actor's reason for doing it?*	Keine Personen beteiligt		
		(4) Outcome *What would be the resulting effect on the information asset?*	**Offenlegung** **Modifizierung**	✓ **Verlust** ✓ **Unterbrechung der Verfügbarkeit**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Bei Fehlen einer stabilen Stromversorgung und regelmäßigen Tausches von Batterien		
		(6) Likelihood *What is the likelihood that this threat scenario could occur?*	**High**	**Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Wert**	**Score**
Die Verfügbarkeit des Systems oder des Geräts wäre unterbrochen und kritische Vorgänge können nicht durchgeführt werden. Die Überwachung der Wohneinheit mittels Überwachungskameras oder Alarmanlage ist unterbrochen. Es kann zu Datenverlust durch Beschädigung von Geräten kommen. Smarte Türschlösser können nicht mehr betätigt werden.	Reputation und Kundenzufriedenheit - 4	2	8
	Finanzielles Vermögen – 3	1	3
	Produktivität – 3	2	6
	Sicherheit und Gesundheit – 5	3	15
	Strafen - 1	1	1
		Relativer Risiko-Score	**33**

(9) Umgang mit Risiken *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	**Defer**	✓ **Mitigate**	**Transfer**

Gewählte Maßnahmen als Abhilfe gegen das Risiko:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Physical (Mitigate)	Die Smart Home Geräte müssen physisch gegen Vandalismus abgesichert sein.
Technical (Mitigate und Accept)	Für kritische Geräte kann eine redundante Stromversorgung angedacht werden, wenn baulich möglich.

Tabelle 14: Risk Worksheet 10 "Nutzdaten der Smart Home Geräte" 2

6.3.9.2 Subsystem 2

In Subsystem 2 werden die beiden kritischen Informationsassets „Übertragene Daten über das Internet“ sowie „Konfiguration des lokalen Netzwerks und Informationen darüber“. Zuerst wird das Asset in Worksheet 8 definiert und abgegrenzt (Tabelle 15) und danach die drei Container definiert (Tabellen 16-18):

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Kritisches Asset *Was ist das kritische Informationsasset?*	**(2) Begründung für Auswahl** *Warum ist dieses Asset wichtig für die Organisation?*	**(3) Beschreibung** *Wie wird das Asset beschrieben?*
Übertragene Daten über das Internet (Beispiele: Videoaufnahme der Überwachungskamera, Status der Alarmanlage)	Der Inhalt der Informationen umfasst die gesamten Daten, die für die Nutzung des Smart Home Systems notwendig sind. Eine Offenlegung würde die Privatsphäre der NutzerInnen verletzen.	Daten, welche von allen im Smart Home System von Sensoren gesammelt oder von Überwachungskameras erstellt werden. Daten zur Steuerung der Smart Home Geräte.
(4) Verantwortliche und BesitzerInnen *Wer besitzt dieses Informationsasset?*		
BenutzerInnen und EigentümerInnen des Smart Home Systems Systemanbieter und Service Provider		
(5) Sicherheitsanforderungen *Welche Sicherheitsanforderungen sind für dieses Informationsasset notwendig?*		
✓ **Vertraulichkeit**	Nur autorisierte Personen dürfen auf die Daten zugreifen können:	BenutzerInnen des Smart Home Systems
✓ **Integrität**	Alle Änderungen an den Daten müssen nachvollzogen werden können und dürfen nur von autorisierten Personen durchgeführt werden:	BenutzerInnen des Smart Home Systems
✓ **Verfügbarkeit**	Dieses Asset muss zur Verfügung stehen, um die Nutzung des Smart Home Systems und die Bewahrung der Privatsphäre sicherstellen zu können. Das Asset muss 24 Stunden am Tag und 7 Tage in der Woche zur Verfügung stehen.	BenutzerInnen des Smart Home Systems Anbieter des Smart Home Systems
✓ **Authentizität**	Dieses Asset darf nur für autorisierte Personen zugänglich sein:	BenutzerInnen des Smart Home Systems
(6) Wichtigster Sicherheitsaspekt *Welcher ist der wichtigste Aspekt der Informationssicherheit dieses Informationsassets?*		
✓ Vertraulichkeit	✓ Integrität	✓ Verfügbarkeit ✓ Authentizität

Tabelle 15: Profil kritisches Informationsasset "Übertragene Daten über das Internet"

Allegro Worksheet 9a	Information Asset Risk Environment Map (Technical)
Intern	
Beschreibung des Containers	**BesitzerInnen**
1. Internetmodem	BenutzerInnen
Extern	
Beschreibung des Containers	**BesitzerInnen**
1. Bediengeräte (PC, Smartphone, Tablet)	BenutzerInnen
2. Cloud-Service und Datenbanken	Systemanbieter und Service Provider
3. Netzwerkgeräte im Internet	Internet Service Provider

Tabelle 16: Container (Technical) "Übertragene Daten über das Internet"

Allegro Worksheet 9b	Information Asset Risk Environment Map (Physical)
Intern	
Beschreibung des Containers	**BesitzerInnen**
-	-
Extern	
Beschreibung des Containers	**BesitzerInnen**
1. Rechenzentrum	Systemanbieter und/oder Service Provider

Tabelle 17: Container (Physical) "Übertragene Daten über das Internet"

Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Intern	
Beschreibung des Containers	**Personen**
-	-
Extern	
Beschreibung des Containers	**Personen**
1. Mitarbeiter der Systemanbieter und Service Provider	Systemanbieter und Service Provider

Tabelle 18: Container (People) "Übertragene Daten über das Internet"

Nach der Definition der Container folgt in Worksheet 10 die Erarbeitung der Risiken des Informationsasset (Tabelle 19):

Allegro - Worksheet 10		**Informationsasset - Risk Worksheet**			
Information Asset Risk	**Threat**	Informations-Asset	Übertragene Daten über das Internet		
		Area of Concern	Unautorisierter Zugriff auf übertragene Daten im Internet Nicht-Verfügbarkeit von über das Internet übertragenen Daten		
		(1) Actor *Who would exploit the area of concern or threat?*	Hacker		
		(2) Means *How would the actor do it? What would they do?*	Eine Schwachstelle bewusst ausnutzen, um Zugriff auf übertragene Daten zu erhalten		
		(3) Motive *What is the actor's reason for doing it?*	Versuch des Abgreifens von persönlichen Informationen und möglicher Verkauf dieser		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Offenlegung** ✓ **Modifizierung**	✓ **Verlust** ✓ **Unterbrechung der Verfügbarkeit**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Bei Aufbrechen einer der Sicherheitsmechanismen während der Übertragung über das Internet.		
		(6) Likelihood *What is the likelihood that this threat scenario could occur?*	**High**	✓ **Medium**	**Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Wert**	**Score**
Diese „Area of Concern" ist potenziell gefährlich und kann den Smart Home BenutzerInnen großen Schaden zufügen. Die Ressourcen können für die BenutzerInnen nicht mehr verfügbar sein und dadurch eine Gefährdung der Sicherheit entstehen. Eine Verletzung der Privatsphäre bei Abgreifen des Videobilds einer Überwachungskamera liegt vor. Durch damit möglicher Spionage ist ein Einbruch in den Wohnbereich möglich.	Reputation und Kundenzufriedenheit - 4	3	12
	Finanzielles Vermögen – 3	1	3
	Produktivität – 3	3	9
	Sicherheit und Gesundheit – 5	3	15
	Strafen - 1	1	1
		Relativer Risiko-Score	**40**

(9) Umgang mit Risiken *Based on the total score for this risk, what action will you take?*			
✓ **Accept (BenutzerInnen)**	**Defer**	✓ **Mitigate (Service Provider)**	**Transfer**

Gewählte Maßnahmen als Abhilfe gegen das Risiko:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Physical	Die involvierten Netzwerkgeräte müssen unautorisierten Personen unzugänglich sein.
People	Intaktes Informationssicherheitsmanagement bei allen involvierten Service Providern und dem Anbieter des Smart Home Systems und vorhandenes Bewusstsein über die Relevanz von Informationssicherheit.
Technical	Verwendung von kryptografisch sicheren Transportprotokollen mit TLS. Nutzung von kryptografisch sicheren Algorithmen bei der notwendigen Verschlüsselung von Nutzdaten durch die Software des Anbieters. Nutzung von kryptografisch sicheren Passwörtern bei allen involvierten Netzwerkgeräten. Stabile Internetanbindung zum Smart Home System. Einsatz von Ende-zu-Ende Verschlüsselung für den Transport durch den Systemanbieter.

Tabelle 19: Risk Worksheet "Übertragene Daten über das Internet"

Das zweite, kritische Informationsasset in Subsystem 2 lautet „Konfiguration des lokalen Netzwerks und Informationen darüber“. Dazu wird die Konfiguration des LAN der BenutzerInnen inklusive den getroffenen Sicherheitseinstellungen auf den Netzwerkgeräten gezählt. Es folgt die Definition des Informationsassets in Tabelle 20:

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Kritisches Asset *Was ist das kritische Informationsasset?*	**(2) Begründung für Auswahl** *Warum ist dieses Asset wichtig für die Organisation?*	**(3) Beschreibung** *Wie wird das Asset beschrieben?*
Konfiguration des lokalen Netzwerks und Informationen darüber	Bei fehlenden oder inkorrekt konfigurierten Netzwerkgeräten entstehen Schwachstellen, die von AngreiferInnen ausgenützt werden können und diesen Zugang zum LAN verschaffen kann.	Der Inhalt dieser Informationen umfasst die physikalische und logische Zusammenstellung und Konfiguration des LAN der BenutzerInnen.
(4) Verantwortliche und BesitzerInnen *Wer besitzt dieses Informationsasset?*		
BenutzerInnen und EigentümerInnen des Smart Home Systems		
(5) Sicherheitsanforderungen *Welche Sicherheitsanforderungen sind für dieses Informationsasset notwendig?*		
✓ **Vertraulichkeit**	Nur autorisierte Personen dürfen auf die Konfiguration zugreifen können:	BenutzerInnen des Smart Home Systems

✓ **Integrität**	Alle Änderungen an der Konfiguration müssen nachvollzogen werden können und dürfen nur von autorisierten Personen durchgeführt werden:	BenutzerInnen des Smart Home Systems
✓ **Verfügbarkeit**	Dieses Asset muss zur Verfügung stehen, wenn Änderungen an der Konfiguration des LAN durchgeführt werden.	BenutzerInnen des Smart Home Systems
✓ **Authentizität**	Dieses Asset darf nur für autorisierte Personen zugänglich sein:	BenutzerInnen des Smart Home Systems

(6) Wichtigster Sicherheitsaspekt *Welcher ist der wichtigste Aspekt der Informationssicherheit dieses Informationsassets?*			
✓ Vertraulichkeit	✓ Integrität	Verfügbarkeit	✓ Authentizität

Tabelle 20: Profil kritisches Informationsasset "Konfiguration des lokalen Netzwerks und Informationen darüber"

Anschließend werden die drei Container des Assets erläutert (Tabellen 21-23):

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Intern	
Beschreibung des Containers	**BesitzerInnen**
1. Internetrouter (Firewall)	BenutzerInnen
2. Netzwerkswitch	BenutzerInnen
3. Wireless Access Points	BenutzerInnen
Extern	
Beschreibung des Containers	**BesitzerInnen**
-	-

Tabelle 21: Container (Technical) "Konfiguration des lokalen Netzwerks und Informationen darüber"

Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Intern	
Beschreibung des Containers	**BesitzerInnen**
1. Digital gespeichert (Passwörter, Zugangsdaten)	BenutzerInnen
2. Analog niedergeschrieben (Passwörter, Zugangsdaten)	BenutzerInnen
Extern	
Beschreibung des Containers	**BesitzerInnen**
-	-

Tabelle 22: Container (Physical) "Konfiguration des lokalen Netzwerks und Informationen darüber"

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Intern	
Beschreibung des Containers	**Personen**
1. BenutzerInnen und EigentümerInnen des LAN	BenutzerInnen
Extern	
Beschreibung des Containers	**Personen**
-	-

Tabelle 23: Container (People) "Konfiguration des lokalen Netzwerks und Informationen darüber"

Abschließend wird das bestehende Risiko über das Informationsasset erarbeitet (Tabelle 24):

Allegro - Worksheet 10		**Informationsasset - Risk Worksheet**	
Information Asset Risk	**Threat**	Informations-Asset	Konfiguration des lokalen Netzwerks und Informationen darüber
		Area of Concern	Unautorisierter Zugriff auf Konfiguration des LAN
		(1) Actor *Who would exploit the area of concern or threat?*	Hacker
		(2) Means *How would the actor do it? What would they do?*	Eine Schwachstelle oder falsche Konfiguration bewusst ausnutzen, um Zugriff auf das LAN und darin enthaltene Geräte zu erhalten
		(3) Motive *What is the actor's reason for doing it?*	Versuch des Abgreifens von persönlichen Informationen und möglicher Verkauf dieser
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Offenlegung** ✓ **Modifizierung** ✓ **Verlust** ✓ **Unterbrechung der Verfügbarkeit**

		(5) Security Requirements *How would the information asset's security requirements be breached?*	Bei erfolgreicher Verbindung in das LAN der BenutzerInnen.		
		(6) Likelihood *What is the likelihood that this threat scenario could occur?*	**High**	**Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Wert**	**Score**
Diese „Area of Concern" ist potenziell gefährlich und kann den Smart Home BenutzerInnen großen Schaden zufügen. Bei Zugang zum Netzwerk über den WLAN-Accesspoint können unbemerkt Informationen über das Netzwerk und dessen Teilnehmer abgegriffen werden. Frei zugängliche LAN-Ports müssen mittels Port-Security abgesichert werden.	Reputation und Kundenzufriedenheit - 4	1	4
	Finanzielles Vermögen – 3	1	3
	Produktivität – 3	2	6
	Sicherheit und Gesundheit – 5	2	10
	Strafen - 1	1	1
		Relativer Risiko-Score	**24**

(9) Umgang mit Risiken
Based on the total score for this risk, what action will you take?

Accept	**Defer**	✓ **Mitigate**	**Transfer**

Gewählte Maßnahmen als Abhilfe gegen das Risiko:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Physical	Die Netzwerkgeräte müssen unautorisierten Personen unzugänglich sein.
People	Vorhandenes Bewusstsein für Informationssicherheit bei BenutzerInnen des Smart Home Systems durch bereitgestellte Informationen und Schulungen.
Technical	Nutzung von kryptografisch sicheren Passwörtern bei Zugang zu allen involvierten Netzwerkgeräten sowie beim WLAN-Accesspoint. Ausschließliche Nutzung von WPA2 oder WPA3 innerhalb des WLAN mit kryptografisch sicheren Passwörtern. Daten müssen auf den Geräten physisch verschlüsselt gespeichert sein. Nutzung von Port Security Methoden bei frei zugänglichen LAN-Ports.

Tabelle 24: Risk Worksheet "Konfiguration des lokalen Netzwerks und Informationen darüber"

6.3.9.3 Subsystem 3

Im dritten Subsystem sind die aus der Sicht des Smart Home Systems bei BenutzerInnen vor Ort externen Informationsassets „Client-Applikation“ und „Cloud-Service“. Genau genommen handelt es sich bei diesen beiden Assets nicht um reine Informationsassets, da damit verknüpft physische Geräte eingesetzt werden. Deshalb wird dies in den Profilen spezifisch erläutert. Es werden aus diesem Subsystem beide Informationsassets beschrieben, da diese in einem Cloud-basierten Smart Home System zentrale Bestandteile und somit Angriffsflächen darstellen.

Folgend das Profil des ersten Informationsassets „Bediengeräte“ (Tabelle 25):

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Kritisches Asset *Was ist das kritische Informationsasset?*	**(2) Begründung für Auswahl** *Warum ist dieses Asset wichtig für die Organisation?*	**(3) Beschreibung** *Wie wird das Asset beschrieben?*
Client-Applikation zur Steuerung des Smart Home Systems (Smartphone, PC)	Mit einem Bediengerät wird das gesamte Smart Home Gerät gesteuert und der Zugriff auf das System erlangt. Ein unautorisierter Zugriff hat informationssicherheitstechnisch potenziell schwere Folgen.	Es handelt sich um eine mobile Applikation oder Web-Applikation, welche zur Steuerung und Verwaltung des Smart Home Systems verwendet wird.
(4) Verantwortliche und BesitzerInnen *Wer besitzt dieses Informationsasset?*		
BenutzerInnen des Smart Home Systems		
(5) Sicherheitsanforderungen *Welche Sicherheitsanforderungen sind für dieses Informationsasset notwendig?*		
✓ **Vertraulichkeit**	Nur autorisierte Personen dürfen auf die Applikation zugreifen können:	BenutzerInnen des Smart Home Systems
✓ **Integrität**	Alle Änderungen an den Daten müssen nachvollzogen werden können und dürfen nur von autorisierten Personen durchgeführt werden:	BenutzerInnen des Smart Home Systems
✓ **Verfügbarkeit**	Dieses Asset muss zur Verfügung stehen, um die Nutzung des Smart Home Systems und die Bewahrung der Privatsphäre sicherstellen zu können. Das Asset muss zu jeder gewünschten Änderung des Smart Home Systems zur Verfügung stehen.	BenutzerInnen des Smart Home Systems Anbieter des Smart Home Systems

✓ **Authentizität**	Dieses Asset darf nur für autorisierten Personen zugänglich sein:	BenutzerInnen des Smart Home Systems

(6) Wichtigster Sicherheitsaspekt *Welcher ist der wichtigste Aspekt der Informationssicherheit dieses Informationsassets?*			
✓ Vertraulichkeit	✓ Integrität	Verfügbarkeit	✓ Authentizität

Tabelle 25: Profil kritisches Informationsasset "Bediengeräte mit Client-Applikation"

Anschließend werden die drei Arten der Container erarbeitet (Tabellen 26-28):

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Intern	
Beschreibung des Containers	**BesitzerInnen**
1. Bediengeräte (Smartphone, PC)	BenutzerInnen
Extern	
Beschreibung des Containers	**BesitzerInnen**
-	-

Tabelle 26: Container (Technical) "Client-Applikation"

Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Intern	
Beschreibung des Containers	**BesitzerInnen**
1. Zugangsdaten: Passwortmanager (Digital)	BenutzerInnen
2. Zugangsdaten: Zettel, Dokument (Analog)	BenutzerInnen
Extern	
Beschreibung des Containers	**BesitzerInnen**
-	-

Tabelle 27: Container (Physical) "Client-Applikation"

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Intern	
Beschreibung des Containers	**Personen**
-	-
Extern	

Beschreibung des Containers	Personen
1. MitarbeiterInnen der Systemanbieter und Service Provider	Systemanbieter und Service Provider

Tabelle 28: Container (People) "Client-Applikation"

Nach der Definition der Container folgt in Worksheet 10 die Erarbeitung der Risiken des Informationsasset (Tabelle 29):

Allegro - Worksheet 10		**Informationsasset - Risk Worksheet**			
Information Asset Risk		Informations-Asset	Client-Applikation zur Steuerung des Smart Home Systems (Smartphone, PC)		
		Area of Concern	Unautorisierter Zugriff auf Applikationsinhalte		
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Hacker		
		(2) Means *How would the actor do it? What would they do?*	Erlangung von Zugriff auf die Smart Home Applikation durch Diebstahl des Bediengeräts oder Kenntnis von Zugangsdaten		
		(3) Motive *What is the actor's reason for doing it?*	Versuch des Abgreifens von persönlichen Informationen und möglicher Verkauf dieser		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Offenlegung** ✓ **Modifizierung**	✓ **Verlust** ✓ **Unterbrechung der Verfügbarkeit**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Bei Entwendung eines Bediengeräts oder Bekanntwerden von Zugangsdaten der BenutzerInnen der Smart Home Plattform		
		(6) Likelihood *What is the likelihood that this threat scenario could occur?*	**High**	✓ **Medium**	**Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Wert**	**Score**
Diese „Area of Concern" ist potenziell gefährlich und kann den Smart Home BenutzerInnen großen Schaden zufügen. Die Ressourcen können für die BenutzerInnen nicht mehr verfügbar sein und dadurch eine Gefährdung der Sicherheit entstehen. Eine Verletzung der Privatsphäre bei Abgreifen des Videobilds einer Überwachungskamera liegt vor. Durch damit möglicher Spionage ist ein Einbruch in den Wohnbereich möglich.	Reputation und Kundenzufriedenheit - 4	1	4
	Finanzielles Vermögen – 3	1	3
	Produktivität – 3	3	9
	Sicherheit und Gesundheit – 5	3	15
	Strafen - 1	1	1

		Relativer Risiko-Score	**32**

(9) Umgang mit Risiken *Based on the total score for this risk, what action will you take?*			
Accept	**Defer**	✓ **Mitigate**	**Transfer**
Gewählte Maßnahmen als Abhilfe gegen das Risiko:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Physical	Die Client-Applikation auf den Bediengeräten muss unautorisierten Personen unzugänglich und durch Authentifizierung der BenutzerInnen am Gerät selbst oder bei Start der Client-Applikation geschützt sein. Eine Multi-Faktor-Authentifizierung ist, wenn beim Smart Home System möglich, zu aktivieren.		
People	Bei allen BenutzerInnen muss ein Sicherheitsbewusstsein geschaffen werden.		
Technical	Die Client-Applikation auf den Bediengeräten muss unautorisierten Personen unzugänglich und durch Authentifizierung der BenutzerInnen am Gerät selbst oder bei Start der Client-Applikation geschützt sein. Eine Multi-Faktor-Authentifizierung ist, wenn beim Smart Home System möglich, zu aktivieren. Die Bediengeräte müssen regelmäßig aktualisiert werden. Die Authentifizierung muss durch die Cloud-Service API kryptografisch implementiert sein.		

Tabelle 29: Risk Worksheet "Client-Applikation"

Das weitere Informationsasset in Subsystem 3 lautet „Cloud-Service (API)“. Dabei wird die gesamte Service-Landschaft des Systemanbieters inklusive den Datenspeichern eingeschlossen. In einem Cloud-basierten Smart Home System spielt dieses naturgemäß eine wichtige Rolle.

Folgend werden laut dem OCTAVE Allegro Prozess die Risiken des Informationsassets erarbeitet. Zuerst wird das Profil definiert (Tabelle 30) und danach die drei Container (Tabellen 31-33):

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Kritisches Asset *Was ist das kritische Informationsasset?*	**(2) Begründung für Auswahl** *Warum ist dieses Asset wichtig für die Organisation?*	**(3) Beschreibung** *Wie wird das Asset beschrieben?*
Cloud-Service und dabei verarbeitete und gespeicherte Daten (API)	Die mit diesem Asset gespeicherten Daten enthalten private Informationen und bilden den zentralen Datenbestand des Smart Home Systems.	Dieses externe Asset bildet die Grundlage der im Smart Home System verarbeiteten Daten und deren Verarbeitung und Speicherung.
(4) Verantwortliche und BesitzerInnen *Wer besitzt dieses Informationsasset?*		

Besitz: BenutzerInnen des Smart Home Systems Verantwortlichkeit: Systemanbieter und/oder Service Provider des Smart Home Systems		
(5) Sicherheitsanforderungen *Welche Sicherheitsanforderungen sind für dieses Informationsasset notwendig?*		
✓ **Vertraulichkeit**	Nur autorisierte Personen dürfen auf die Daten zugreifen können:	BenutzerInnen des Smart Home Systems
✓ **Integrität**	Alle Änderungen an den Daten müssen nachvollzogen werden können und dürfen nur von autorisierten Personen durchgeführt werden:	BenutzerInnen des Smart Home Systems
✓ **Verfügbarkeit**	Dieses Asset muss zur Verfügung stehen, um die Nutzung des Smart Home Systems und die Bewahrung der Privatsphäre sicherstellen zu können. Das Asset muss zu jeder gewünschten Änderung des Smart Home Systems zur Verfügung stehen.	BenutzerInnen des Smart Home Systems Anbieter des Smart Home Systems
✓ **Authentizität**	Dieses Asset darf nur für autorisierten Personen zugänglich sein:	BenutzerInnen des Smart Home Systems
(6) Wichtigster Sicherheitsaspekt *Welcher ist der wichtigste Aspekt der Informationssicherheit dieses Informationsassets?*		
✓ Vertraulichkeit	✓ Integrität	✓ Verfügbarkeit ✓ Authentizität

Tabelle 30: Profil kritisches Informationsasset "Cloud-Service (API)"

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Intern	
Beschreibung des Containers	**BesitzerInnen**
-	-
Extern	
Beschreibung des Containers	**BesitzerInnen**
1. Datenverarbeitung (Cloud-Service)	Systemanbieter
2. Datenspeicherung (Cloud-Service)	Systemanbieter und/oder Service Provider

Tabelle 31: Container (Technical) "Cloud-Service (API)"

Allegro Worksheet 9b	Information Asset Risk Environment Map (Physical)
Intern	
Beschreibung des Containers	**BesitzerInnen**
	-
Extern	
Beschreibung des Containers	**BesitzerInnen**
1. Serverstandort(e) für Datenverarbeitung	Systemanbieter und/oder Service Provider
2. Serverstandort(e) für Datenspeicherung	Systemanbieter und/oder Service Provider

Tabelle 32: Container (Physical) "Cloud-Service (API)"

Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Intern	
Beschreibung des Containers	**Personen**
-	-
Extern	
Beschreibung des Containers	**Personen**
1. MitarbeiterInnen der Systemanbieter und Service Provider	Systemanbieter und Service Provider

Tabelle 33: Container (People) "Cloud-Service (API)"

Abschließend wird das Risk Worksheet10 (Tabelle 34) für das kritische Informationsasset „Cloud-Service (API)“ erarbeitet:

Allegro - Worksheet 10			Informationsasset - Risk Worksheet
Information Asset Risk	**Threat**	Informations-Asset	Cloud-Service (API) und darin gespeicherte Daten
		Areas of Concern	Unautorisierter Zugriff auf Informationen Nicht-Verfügbarkeit des Cloud-Services
		(1) Actor *Who would exploit the area of concern or threat?*	Hacker Umwelteinflüsse und Stromausfälle

		(2) Means *How would the actor do it? What would they do?*	Erlangung von Zugriff auf die Smart Home Applikationsserver durch Kompromittierung des Services oder Kenntnis von Zugangsdaten Versuch eines DDoS-Angriffes für Erreichung von Nicht-Verfügbarkeit des Cloud-Services		
		(3) Motive *What is the actor's reason for doing it?*	Versuch des Abgreifens von persönlichen Informationen und möglicher Verkauf dieser Veranschaulichung von Vulnerabilität des Services		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Offenlegung** **Modifizierung**	**Verlust** ✓ **Unterbrechung der Verfügbarkeit**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Bei erfolgreicher Kompromittierung des Cloud-Services Bei erfolgreicher Durchführung eines DDoS-Angriffs		
		(6) Likelihood *What is the likelihood that this threat scenario could occur?*	**High**	✓ **Medium**	**Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Wert**	**Score**
Diese „Area of Concern" ist potenziell gefährlich und kann den Smart Home BenutzerInnen großen Schaden zufügen. Die Ressourcen können für die BenutzerInnen nicht mehr verfügbar sein und dadurch eine Gefährdung der Sicherheit entstehen. Bei Nicht-Verfügbarkeit des Services ist die Funktion des Smart Homes eingeschränkt.	Reputation und Kundenzufriedenheit - 4	3	12
	Finanzielles Vermögen – 3	2	6
	Produktivität – 3	3	9
	Sicherheit und Gesundheit – 5	3	15
	Strafen - 1	3	3
		Relativer Risiko-Score	**45**

(9) Umgang mit Risiken *Based on the total score for this risk, what action will you take?*			
Accept	**Defer**	✓ **Mitigate**	**Transfer**

Gewählte Maßnahmen als Abhilfe gegen das Risiko (betrifft Systemanbieter):	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Physical	Alle Serverstandorte müssen gegen unautorisierten Zugriff geschützt sein. Bei Verwendung von Service Providern und Auftragsverarbeitern müssen diese alle gesetzlichen Vorgaben einhalten. Nutzung hochverfügbarer Infrastrukturen.

People	Vertragliche Vereinbarungen für die gesetzlich vorgegebene Datenverarbeitung durch Auftragsverarbeiter müssen abgeschlossen werden. Alle MitarbeiterInnen müssen nach den Sicherheitsvorgaben geschult sein. Ein Informationssicherheitsmanagement-System muss eingeführt sein und regelmäßig verbessert werden.
Technical	Die vom Informationssicherheitsmanagement abgeleiteten, technischen Maßnahmen müssen von Systemanbietern durchgeführt werden. Einhaltung von grundlegenden Sicherheitsvorgaben in der Softwareentwicklung (Open Web Application Security Project [OWASP], 2019). Transparenz gegenüber BenutzerInnen hinsichtlich der verarbeiteten Daten. Erzwingung der Nutzung von kryptografisch sicheren Passwörtern durch die BenutzerInnen. Leben von Privacy und Security by Design Prinzipien durch die Systemanbieter. Sämtliche weitere Maßnahmen, welche zu einem sicheren Betrieb von Cloud-Applikationen nach den Aspekten der Informationssicherheit zählen, werden im Rahmen dieser Arbeit nicht näher erläutert.

Tabelle 34: Risk Worksheet "Cloud-Service (API)"

Mit der Analyse der insgesamt sechs „Areas of Concern“ ist der Risikoanalyseprozess im Rahmen dieser Arbeit abgeschlossen. Die Zusammenfassung wird im anschließenden Kapitel erläutert.

7 CONCLUSIO UND AUSBLICK

Mithilfe der gesammelten Informationen aus dem theoretischen sowie praktischen Teil der Arbeit werden in diesem letzten Kapitel die Ergebnisse zusammengefasst und auf die gestellten Forschungsfragen angewandt. Das Ziel dieses Kapitels ist es, alle gewonnen Informationen aus der Risikoanalyse des Cloud-basierten Smart Home Systems für die Beantwortung der Forschungsfrage sowie für Handlungsempfehlungen für NutzerInnen sowie Anbieter dieser Systeme zu verarbeiten.

Cloud-basierte Smart Home Geräte gewinnen aufgrund einfacher Bedienbarkeit und der Interoperabilität unter verschiedenen Anbietern immer mehr an Beliebtheit (Yaqoob et al., 2017). Dies kann nachvollzogen werden, die dabei entstehenden Risiken sollten jedoch nicht außer Acht gelassen und BenutzerInnen bewusst gemacht werden.

7.1 Beantwortung der Forschungsfragen

Um die Ergebnisse der Risikoanalyse mit OCTAVE Allegro übersichtlich darstellen zu können, werden auf der folgenden Seite die acht untersuchten Risiken („Areas of Concern“) der sechs kritischen Assets zusammengefasst und tabellarisch aufgelistet. Die Sortierung erfolgt absteigend nach Höhe des Risiko-Scores. Der Risiko-Score innerhalb der Risikoanalyse stellt keinen allgemein vergleichbaren Wert dar, sondern nur das relative Risiko unter den aufgestellten Risiken.

Die in der Einleitung definierte Nullhypothese H_0 lautet:

„Die Nutzung von Smart Home Geräten stellt kein Risiko für die Privatsphäre der NutzerInnen dar, wenn diese keine oder fehlerhaft implementierte Sicherheitsfunktionen aufweisen.“

Diese Hypothese kann aufgrund der vorliegenden Ergebnisse der Risikoanalyse, welche auf den folgenden Seiten tabellarisch dargestellt sind, verworfen werden.

Die zu beantwortende Forschungsfrage der Arbeit lautet:

„Welche Sicherheitsrisiken entstehen durch die Nutzung von Cloud-basierten Geräten im Smart Home Umfeld?“

Mithilfe der folgenden Tabelle 35, die eine Aufstellung aller Risiken mit deren Gefahren, Auswirkungen und Gegenmaßnahmen darstellt, wird diese Fragestellung beantwortet. Im Rahmen der Arbeit wurden die acht als größte Risikogruppen eingestuften analysiert. In der Praxis existieren weitere Risiken, welche nicht alle ganzheitlich erfasst werden können.

Zusätzlich sollen die zwei folgenden Subforschungsfragen beantwortet werden:

1. *„Welche Folgen bergen diese Sicherheitsrisiken bei einem Eintritt?“*
2. *„Welche Gegenmaßnahmen können NutzerInnen zur Risikominimierung empfohlen werden?“*

Die Antwort auf die 1. Subforschungsfrage wird in Tabelle 35 in der Spalte „Auswirkungen“ zu jedem Risiko aufgeführt. Die Antwort auf die 2. Subforschungsfrage wird in Tabelle 35 in der Spalte „Gegenmaßnahmen“ zu jedem Risiko aufgeführt. In den Kapiteln 7.2 „Handlungsempfehlungen für BenutzerInnen“ werden diese Gegenmaßnahmen aus der Tabelle extrahiert, um einen Empfehlungskatalog für NutzerInnen anzubieten.

Nr.	Asset	Gefahr	Risiko-Score	Auswirkungen	Gegenmaßnahmen
1	Cloud-Service (API)	Unautorisierter Zugriff durch Dritte	45	Offenlegung von Daten Manipulation von Daten Verletzung der Privatsphäre von BenutzerInnen	Informationssicherheitsmanagement seitens der Systemanbieter und Service Provider Softwareentwicklungsprozess nach fundierten Praktiken mit Sicherheit im Vordergrund (OWASP, 2019) Security und Privacy by Design innerhalb der Applikationslandschaft der Systemanbieter und Service Provider Verschlüsselung der Daten mit sicheren Algorithmen (AES) und Zulassung der Verwaltung der Schlüssel durch die BenutzerInnen
2	Cloud-Service (API)	Nicht-Verfügbarkeit des Services durch: DDoS-Angriffe Betriebsfehler des Systemanbieters	45	Einschränkung der Funktion des Smart Home Systems Verlust von Daten	Nutzung hochverfügbarer Infrastrukturen durch Systemanbieter und Service Provider Resistenz gegen DDoS-Angriffe durch geeignete technische Maßnahmen (außerhalb des Rahmens dieser Arbeit)
3	Nutzdaten des Smart Home Systems	Unautorisierter Zugriff	43	Offenlegung von Daten Manipulation von Daten Verletzung der Privatsphäre von BenutzerInnen	Implementierung von Ende-zu-Ende Verschlüsselung der übertragenen Daten zwischen Cloud-Service und Smart Home Geräten

					Integritätsüberprüfung von Firmware-Updates durch die Smart Home Geräte Erzwingung der Nutzung von kryptografisch sicheren Passwörtern von BenutzerInnen durch Systemanbieter Sichere Verwahrung der Zugangsdaten Physischer Schutz gegen Diebstahl der Geräte
4	Übertragene Daten über das Internet	Unautorisierter Zugriff	40	Offenlegung von Daten Manipulation von Daten Verletzung der Privatsphäre von BenutzerInnen	Implementierung von Ende-zu-Ende Verschlüsselung der übertragenen Daten zwischen Cloud-Service und Smart Home Geräten (Nutzung von TLS ab Version 1.2, besser 1.3)
5	Übertragene Daten über das Internet	Nicht-Verfügbarkeit durch Internetausfall	40	Einschränkung der Funktion des Smart Home Systems Nicht-Verfügbarkeit des Smart Home Systems	Sicherstellung einer stabilen Internetanbindung durch BenutzerInnen Implementierung einer Backup-Internetanbindung beim Betrieb kritischer Smart Home Geräte
6	Nutzdaten des Smart Home Systems	Nichtverfügbarkeit durch Unterbrechung der Energieversorgung von Geräten	33	Einschränkung der Funktion des Smart Home Systems Nicht-Verfügbarkeit des Smart Home Systems	Sicherstellung einer stabilen Energieversorgung aller Smart Home Geräte (Stromnetz, Batterien) Sicherstellung einer stabilen Internetverbindung

7	Client-Applikation	Unautorisierter Zugriff	32	Offenlegung von Daten Manipulation von Daten Verletzung der Privatsphäre von BenutzerInnen	Keine Nutzung von öffentlichen, ungesicherten WLAN-Hotspots Regelmäßige Updates der Bediengeräte Nutzung einer sicheren Sperrmethode des Bediengeräts Aktivierung einer Zwei-Faktor-Authentifizierung in der Smart Home Applikation Schutz des Bediengeräts vor Diebstahl
8	Konfiguration des LAN der BenutzerInnen	Unautorisierter Zugriff	24	Offenlegung von Daten Manipulation von Daten Verletzung der Privatsphäre von BenutzerInnen	Nutzung des WLAN mit sicherer WPA2/WPA3-Verschlüsselung Nutzung eines IDPS innerhalb des LAN Nutzung von Port Security Mechanismen bei frei zugängliche LAN-Ports außerhalb des geschützten Wohnbereichs

Tabelle 35: Zusammenfassung einzelner Risiken eines generischen, Cloud-basierten Smart Home Systems

Zu den Risiken des Assets „Cloud-Services (API)“ kann zusätzlich die Gefahr der Einstellung des Services seitens des Systemanbieters genannt werden, wodurch Smart Home Geräte nicht mehr benutzbar sein können. Die Transparenz innerhalb der Datenschutzvereinbarung des Systemanbieters kann ein weiteres Kriterium für eine Entscheidung der gewählten Geräte sein.

Übergeordnet spielt das Verhalten und Wissen der BenutzerInnen gegenüber Informationssicherheit eine Rolle, weshalb die Maßnahme „Bildung von Bewusstsein gegenüber Informationssicherheit“ in jedem von den BenutzerInnen beeinflussbaren Risiken angeführt ist.

7.2 Handlungsempfehlungen für BenutzerInnen

Nach der Aufstellung der untersuchten Risiken im vorigen Kapitel soll zusätzlich ein Maßnahmenkatalog für BenutzerInnen einen vereinfachten Überblick über risikomindernde Maßnahmen darstellen. Dieser ist in folgender Tabelle 36 zu finden:

Einholen von Informationen über die Verarbeitung der gespeicherten Daten durch den Systemanbieter (Datenschutzvereinbarung) vor Kauf von Smart Home Geräten
Korrekte Einrichtung der lokalen Netzwerkgeräte im LAN, welche umfassende Sicherheitsfunktionen bereitstellen müssen (Firewall, Router, Switches)
Nutzung eines IDPS für das LAN, wenn vorhanden
Nutzung von kryptografisch sicheren Passwörtern in allen Systemen sowie Netzwerkgeräten und Smart Home Geräten
Verwahrung der genutzten Zugangsdaten und Passwörter an einem sicheren Ort (auditierte Passwortmanager)
Einspielen von verfügbaren Updates auf allen genutzten Geräten
Verzicht auf die Nutzung von nicht mehr unterstützten Software-Plattformen und Betriebssystem-Versionen der mobilen Bediengeräte
Nutzung des WLAN mit WPA2/WPA3 und AES-Verschlüsselung mit kryptografisch sicherem Passwort
Nutzung von Port Security Mechanismen für LAN-Ports in öffentlich zugänglichen Bereichen, wenn diese durch die genutzte Infrastruktur zur Verfügung stehen
Nutzung von separiertem, isoliertem Netzwerk für Smart Home Geräte, falls Methoden und Wissen dafür zur Verfügung stehen
Nutzung von Zwei-Faktor-Authentifizierung für das Cloud-basierte Smart Home System, falls diese vom System unterstützt wird
Nutzung einer kryptografisch sicheren Sperrmethode auf den Bediengeräten (bevorzugt Passwortphrasen)

Tabelle 36: Handlungsempfehlungen für NutzerInnen

Um den Begriff der kryptografisch sicheren Passwörter zu definieren, soll einer aktuellen Empfehlung von Kävrestad et al. (2020) gefolgt werden. Diese aus seiner sozio-technologischen Perspektive betrachteten Arbeit schlägt vor, die Länge der Passwörter durch Aneinanderreihung von mehreren, leicht zu merkenden Worten zu erhöhen. Die Länge von Passwörtern ist demnach von größerer Bedeutung als der Umfang des verwendeten Zeichensatzes (Kävrestad et al., 2020). Übergeordnet über alle Risiken stellt der Faktor Mensch aufgrund von Unwissenheit oder die Gefahr von Social Engineering ein unberechenbares Risiko dar.

7.3 Zusammenfassung

Der Einzug von Smart Home Geräten in immer mehr Haushalte sowie kommerzielle Gebäude ist eine seit Jahren voranschreitende und logische Entwicklung. Durch die Vernetzung von heterogenen Systemen sowie Cloud-basierten Geräten über Plattformen schaffen für BenutzerInnen einfach zu bedienende Lösungen. Dadurch werden Datenstände miteinander vereint, welche von außen betrachtet intransparent sind und möglicherweise an Dritte verkauft werden. Dies kann vorbehaltlich bei kostenlosen Angeboten vermutet werden (Darby, 2018). Bei kritischen Smart Home Geräten wie Überwachungskameras, Rauchmeldern und Türschlössern treten Anforderungen in den Vordergrund, welche besonders berücksichtigt werden müssen. Um das zu erreichen, müssen diese Risiken den NutzerInnen jedoch bewusst sein.

Durch Berücksichtigung von Empfehlungen können die Risiken, auf die NutzerInnen Einfluss haben, reduziert werden. Risiken, die auf Seite der Anbieter von Smart Home Geräten und Service Providern aufliegen, müssen von BenutzerInnen akzeptiert werden. Dabei kann durch eine gezielte Auswahl von Geräten von Herstellern mit anerkannten Datenschutzpraktiken durch BenutzerInnen zumindest teilweise Einfluss genommen werden. Die Entwicklung innerhalb der Gesellschaft Richtung mehr Transparenz über die Art und Weise der Verarbeitung von persönlichen Daten durch Anbieter wird erfordern, dass NutzerInnen ein umfassender und verständlicher Überblick über alle gesammelten und verarbeiteten Daten gegeben wird (Jacobsson et al., 2016). Dazu gehören die Anonymisierung und Minimierung von Daten sowie die Kontrolle darüber. Die Erarbeitung der EU-Verordnung zum Schutz von persönlichen Daten, welche 2016 in Kraft trat, verstärkt diese Entwicklung von Seite der Gesetzgeber (EU-DSGVO, 2016).

Ein entscheidender Faktor für eine flächendeckende Verbreitung und Akzeptanz von Systemen und Geräten ist die Durchsetzung von Security by Design sowie Privacy by Design Prinzipien beim Entwurf von Cloud-basierten Smart Home Systemen durch die Anbieter. Dafür existieren bereits mehrere Entwürfe, ausschlaggebend ist dabei eine von außen prüfbare Architektur. Die Nutzung von etablierten und offenen Standards durch Systemanbieter ist essenziell für eine nachhaltige Entwicklung von Ökosystemen, welche miteinander funktionieren. Ein Vertreter für ein derartiges Framework ist der Internet of Things Security Verification Standard (ISVS) des Open Web Application Security Projects (OWASP, 2020). Gleichzeitig können NutzerInnen, welche die Kunden der Systemanbieter darstellen, durch stärkere Nachfrage nach sicheren Smart Home Lösungen diese Entwicklung forcieren. Bei Cloud-basierten Smart Home Systemen

werden, wie die Ergebnisse der Risikoanalyse zeigen, ein Teil der größten Risiken auf den Anbieter übergeführt. Dies ist für BenutzerInnen als positiv zu sehen, da sich somit das benötigte Wissen über Netzwerk- und IT-Sicherheitstechnologien verringert. Jedoch müssen sich die Anbieter umso mehr um ganzheitliche Informationssicherheit innerhalb ihres Produktportfolios kümmern.

7.4 Weiterführende Forschung und Ausblick

Weitergehende Forschungen als Anknüpfung an diese Arbeit kann eine tiefergehende Erarbeitung eines Smart Home Gerätes oder spezifischen Art von Systems, wie Systeme für ältere und beeinträchtigte Menschen oder im Gesundheitsbereich, sein. In dieser Arbeit wurde eine generische Architektur untersucht.

Das Feld der Informationstechnologie unterliegt erfahrungsgemäß einem stetigen und schnelllebigen Wandel. Als Alternative zu traditionellen Konzepten der Informationssicherheit für IoT-Geräte werden in den letzten Jahren vermehrt Blockchain-Technologien in unterschiedlichen Anwendungen erforscht. Diese Ideen umfassen die integritätsüberprüfende Firmware-Verteilung über eine dezentrale Blockchain (S. Dhakal et al., 2019) bis zu vollständigen IoT-Architekturen, welche vollumfänglich Blockchain-Technologien einsetzen (Yu et al., 2018). Die Forschungen auf diesem Gebiet werden zukünftig zu in der Praxis anwendbaren und intrinsisch sicheren Systemarchitekturen führen.

ABKÜRZUNGSVERZEICHNIS

6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
CIoT	Consumer Internet of Things
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
DNS	Domain Name System
DoS	Denial-of-Service
dt.	deutsch
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification, Authentication, and trust Services
engl.	englisch
HTTP	Hypertext Transfer Protocol
IDPS	Intrusion Detection and Prevention System
IKT	Informations- und Kommunikationstechnologien
IoT	Internet of Things
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
kB	Kilobyte
kBit	Kilobit
kHz	Kilohertz
LAN	Local Area Network
mA	Milli-Ampere
M2M	Machine-to-Machine (Kommunikation)
MITM	Man-in-the-Middle
MHz	Megahertz

MQTT	Message Queue Telemetry Transport
NFC	Near Field Communication
Nr.	Nummer
OSI	Open Systems Interconnection
PAN	Personal Area Network
REST	Representational State Transfer
RFID	Radio-Frequency Identification
RILA	Reference IoT Layered Architecture
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TV	Television
WAN	Wide Area Network
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

8 LITERATURVERZEICHNIS

Ali, B. (2016). *Internet of Things based Smart Homes: Security Risk Assessment and Recommendations.* Luleå University of Technology, Lulea. https://ltu.diva-portal.org/smash/record.jsf?pid=diva2%3A1032194&dswid=8050

Ali, B. & Awad, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors (Basel, Switzerland)*, *18*(3). https://doi.org/10.3390/s18030817

Ali, W., Dustgeer, G., Awais, M. & Ali Shah, M. (2017). IoT based smart home: Security challenges, security requirements and solutions. *Proceedings of the 23rd International Conference on Automation & Computing, University of Huddersfield.* Vorab-Onlinepublikation. https://doi.org/10.23919/iconac.2017.8082057

Apthorpe, N., Reisman, D. & Feamster, N. (2017). *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic*. http://arxiv.org/pdf/1705.06805v1

Ashton, K. (2009). That ‘internet of things’ thing. *RFID journal*, *22*(7), 97–114. http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

Atzori, L., Iera, A. & Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, *56*, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Awad, A. I., Yen, N. & Fairhurst, M. (2018). *Information Security: Foundations, technologies and applications*. *IET Security Series: Bd. 01*. The Institution of Engineering and Technology. https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=5400685

Balta-Ozkan, N., Amerighi, O. & Boteler, B. (2014). A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: reflections for policy and future research. *Technology Analysis & Strategic Management*, *26*(10), 1176–1195. https://doi.org/10.1080/09537325.2014.975788

Bhatia, J., Evans, M. C., Wadkar, S. & Breaux, T. D. (2016). Automated Extraction of Regulated Information Types Using Hyponymy Relations. In *2016 IEEE 24th International Requirements Engineering Conference workshops: Proceedings : 12-16 September 2016, Beijing, China* (S. 19–25). IEEE. https://doi.org/10.1109/REW.2016.018

Bluetooth Special Interest Group. (2020). *Bluetooth Technology - Spezifikation*. https://www.bluetooth.com/

Bussche, A. von dem & Voigt, P. (2018). *EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch*. Springer. https://doi.org/10.1007/978-3-662-56187-4

Caralli, R. A., Stevens, J. F., Young, L. R. & Wilson, W. R. (2007). *Introducing octave allegro: Improving the information security risk assessment process*. Pittsburgh. Carnegie-Mellon

Univ Pittsburgh PA Software Engineering Inst. https://apps.dtic.mil/dtic/tr/fulltext/u2/a470450.pdf

Chong, G., Zhihao, L. & Yifeng, Y. (2011). The research and implement of smart home system based on Internet of Things. In *International Conference on Electronics, Communications and Control (ICECC), 2011: 9 - 11 Sept. 2011, Ningbo, China ; proceedings* (S. 2944–2947). IEEE. https://doi.org/10.1109/ICECC.2011.6066672

Daemen, J. & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. *Information Security and Cryptography, Texts and Monographs*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-04722-4

Dahmen-Lhuissier, S. (2020). *ETSI - Internet of Things - IoT Standards | Machine to Machine Solutions (M2M)*. https://www.etsi.org/technologies/internet-of-things

Darby, S. J. (2018). Smart technology in the home: time for more clarity. *Building Research & Information*, *46*(1), 140–147. https://doi.org/10.1080/09613218.2017.1301707

Darianian, M. & Michael, M. P. (2008). Smart Home Mobile RFID-Based Internet-of-Things Systems and Services. In *International Conference on Advanced Computer Theory and Engineering, 2008: ICACTE '08 ; 20 - 22 Dec. 2008, Phuket, Thailand* (S. 116–120). IEEE. https://doi.org/10.1109/ICACTE.2008.180

Donath, A. (3. Oktober 2021). Tesla, Gefängnisse, Ärzte: Tausende Livevideos aus Verkada-Überwachungskameras erbeutet - Golem.de. *Golem.de*. https://www.golem.de/news/tesla-gefaengnisse-aerzte-tausende-livevideos-aus-verkada-ueberwachungskameras-erbeutet-2103-154803.html

Dorus, R. & Vinoth, P. (2013). Mitigation of jamming attacks in wireless networks. In *2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN 2013): Tirunelveli, India, 25-26 March 2013* (S. 168–171). IEEE. https://doi.org/10.1109/ICE-CCN.2013.6528486

Eastlake, D. & Jones, P. (2001). *US Secure Hash Algorithm 1 (SHA1).* https://doi.org/10.17487/rfc3174

Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (2014). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE

Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (2016). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Gislason, D. (2008). *Zigbee wireless networking: Includes ZigBee Pro specifications, contains several coding examples, details how to plan and develop ZigBee networks*. Elsevier; Newnes. http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10254625

Gomez, C., Oller, J. & Paradells, J. (2012). Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *Sensors*, *12*(9), 11734–11753. https://doi.org/10.3390/s120911734

Greenberg, A. (5. Februar 2016). Flaws in Samsung's 'Smart' Home Let Hackers Unlock Doors and Set Off Fire Alarms. *WIRED*. https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Hahm, O., Baccelli, E., Petersen, H. & Tsiftes, N. (2016). Operating Systems for Low-End Devices in the Internet of Things: A Survey. *IEEE Internet of Things Journal*, *3*(5), 720–734. https://doi.org/10.1109/JIOT.2015.2505901

Han, J.-H., Jeon, Y. & Kim, J. (2015). Security considerations for secure and trustworthy smart home system in the IoT environment. In *Information and Communication Technology Convergence (ICTC), 2015 International Conference on* (S. 1116–1118). IEEE. https://doi.org/10.1109/ICTC.2015.7354752

Harper, R. (2003). *Inside the Smart Home*. Springer-Verlag London Limited. http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10130034 https://doi.org/10.1007/b97527

Hassan, Q. F., Khan, A. u. R. & Madani, S. A. (Hg.). (2017). *Chapman & Hall / CRC Computer and Information Science Series*. *Internet of Things: Challenges, Advances, and Applications* (1. Aufl.). CRC Press.

Hendricks, D. (2014). *The History of Smart Homes*. https://www.iotevolutionworld.com/m2m/articles/376816-history-smart-homes.htm

Howard, M. & Lipner, S. (2006). *The security development lifecycle: SDL, a process for developing demonstrably more secure software*. *Microsoft secure software development series*. Microsoft Press. http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10762138

Hui, J. & Thubert, P. (2011). *RFC 6282 - Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*. https://tools.ietf.org/html/rfc6282

Hui, T. K., Sherratt, R. S. & Sánchez, D. D. (2017). Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Future Generation Computer Systems*, *76*, 358–369. https://doi.org/10.1016/j.future.2016.10.026

IEEE Standards Association. (2020). *1901-2010 - IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications*. https://standards.ieee.org/standard/1901-2010.html

Institute of Electrical and Electronics Engineers. (2015). *Towards a definition of the Internet of things (IoT)*. http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

International Organisation for Standardisation. (2018). *ISO/IEC 27000:2018: Information Technology—Security Techniques—Information Security Management Systems—Overviewand Vocabulary.* https://www.iso.org/standard/73906.html

International Telecommunications Union. (2015). *G.9959 : Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications*. https://www.itu.int/rec/T-REC-G.9959-201501-I/en

Internet Engineering Task Force. (2020). *The Internet of Things*. https://ietf.org/topics/iot/

i-SCOOP. (19. Mai 2020). *What is IoT? The Internet of Things - definitions and facts*. https://www.i-scoop.eu/internet-of-things/

ITWissen.info. (2015a). *ZigBee - ITWissen.info*. https://www.itwissen.info/ZigBee-ZigBee.html

ITWissen.info. (2015b). *Z-Wave - ITWissen.info*. https://www.itwissen.info/Z-Wave-Z-wave.html

ITWissen.info. (2017). *Bluetooth - ITWissen.info*. https://www.itwissen.info/Bluetooth-Bluetooth.html

ITWissen.info. (2018). *BLE (Bluetooth low energy) - ITWissen.info*. https://www.itwissen.info/BLE-Bluetooth-low-energy-Bluetooth-Low-Energy.html

ITWissen.info. (2019). *IEEE 802.11 - ITWissen.info*. https://www.itwissen.info/IEEE-802DOT-11-802DOT-11.html

Jacobsson, A., Boldt, M. & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733. https://doi.org/10.1016/j.future.2015.09.003

Jeyanthi, N., Abraham, A. & Mcheick, H. (2019). *Ubiquitous computing and computing security of IoT*. *Studies in Big Data*. Springer.

Johnson, A. L. (2016). *Botnet "Mirai"*. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=48e65595-ef3d-4653-bc6f-4c04d2667c36&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Karzel, D., Marginean, H. & Tran, T.-S. (2016). *A Reference Architecture for the Internet of Things*. https://www.infoq.com/articles/internet-of-things-reference-architecture/

Katre, S. R. & Rojatkar, D. V. (2017). Home automation: past, present and future. *International Research Journal of Engineering and Technology (4: 10)*, 343–346.

Kävrestad, J., Lennartsson, M., Birath, M. & Nohlberg, M. (2020). Constructing secure and memorable passwords. *Information & Computer Security*, *28*(5), 701–717. https://doi.org/10.1108/ICS-07-2019-0077

King, N. (2003). Smart home – a definition (2003). https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf

KNX Association. (2020). *knx.org - Website*. https://www.knx.org/knx-en/for-professionals/What-is-KNX/A-brief-introduction/

Küchemann, D. (2014). Betriebssysteme für IoT-Geräte. https://dekue.de/literature/IoT.pdf

Kuhrau, S. (2020). Was ist Datenschutz? *a.s.k. Datenschutz e.K.,* 2020. https://bdsg-externer-datenschutzbeauftragter.de/datenschutz/was-ist-datenschutz/

Labiod, H., Afifi, H. & Santis, C. de. (2007). *WI-FI TM, BLUETOOTH TM, ZIGBEE TM AND WIMAX TM*. Springer. http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10192164 https://doi.org/10.1007/978-1-4020-5397-9

Lee, C., Zappaterra, L., Choi, K. & Choi, H.-A. (2014). Securing smart home: Technologies, security challenges, and security requirements. In *2014 IEEE Conference on Communications and Network Security (CNS 2014): San Francisco, California, USA, 29-31 October 2014 ; [including workshop papers]* (S. 67–72). IEEE. https://doi.org/10.1109/CNS.2014.6997467

Lin, H. & Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information (Switzerland)*, *7*(3), 44–59. https://doi.org/10.3390/info7030044

Mahmoud, A. & Jeedella, S. (2010). Integrated Wireless Technologies for Smart Homes Applications. In M. A. Al-Qutayri (Hg.), *Smart home systems.* InTech. https://doi.org/10.5772/8412

Marikyan, D., Papagiannidis, S. & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, *138*, 139–154. https://doi.org/10.1016/j.techfore.2018.08.015

Märtens, A. (2017). *RFID vs. NFC - Was ist der Unterschied?* https://www.ecom-ex.com/de/blog/post/rfid-vs-nfc-was-ist-der-unterschied/

NFC Forum (Hg.). (2020). *NFC Forum*. https://nfc-forum.org/

NIST. (2006). *NIST Glossary*. https://csrc.nist.gov/glossary/term/threat

NIST. (2012). *Guide for conducting risk assessments*. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-30r1

Open Web Application Security Project. (2019). *OWASP SAMM Model*. https://owaspsamm.org/about

Open Web Application Security Project. (2020). *OWASP IoT Security Verification Standard*. https://owasp.org/www-project-iot-security-verification-standard/

Oriwoh, E. (2018). *19 Astonishing Quotes About The Internet Of Things Everyone Should Read*. https://www.forbes.com/sites/bernardmarr/2018/09/12/19-astonishing-quotes-about-the-internet-of-things-everyone-should-read/

Padyab, A. M., Päivärinta, T. & Harnesk, D. (2014). Genre-Based Approach to Assessing Information and Knowledge Security Risks. *International Journal of Knowledge Management*, *10*(2), 13–27. https://doi.org/10.4018/ijkm.2014040102

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. *Wiley computer publishing*. John Wiley & Sons, Inc.

Pecb. (2015). *Risk Assessment with OCTAVE*. https://pecb.com/whitepaper/risk-assessment-with-octave

Proehl, G. (2013). An Introduction to Near Field Communications. *ST-Microelectronics*. http://www. st. com/content/st_com/en/applications/connectivit y/near-field-communication-nfc. html

Radoglou, G., Panagiotis I., Sarigiannidis, P. G. & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, *5*, 41–70. https://doi.org/10.1016/j.iot.2018.11.003

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L. & Loge, C. (2006). The Smart Home Concept : our immediate future. In *2006 1ST IEEE International Conference on E-Learning in Industrial Electronics* (S. 23–28). IEEE / Institute of Electrical and Electronics Engineers Incorporated. https://doi.org/10.1109/ICELIE.2006.347206

Risteska Stojkoska, B. L. & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006

Rivest, R. L., Shamir, A. & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Russell, B. (2016). *Practical Internet of Things security: A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world*. *Community experience distilled*. Packt Publishing. http://proquest.tech.safaribooksonline.de/9781785889639

S. Dhakal, F. Jaafar & P. Zavarsky (2019). Private Blockchain Network for IoT Device Firmware Integrity Verification and Update. In *2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE)*.

Samuel, S. S. I. (2016). A review of connectivity challenges in IoT-smart home. In *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC): Muscat, Oman 15-16 March 2016* (S. 1–4). IEEE. https://doi.org/10.1109/ICBDSC.2016.7460395

Schallbruch, M. (2016). Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste. *Computer und Recht*, *32*(10). https://doi.org/10.9785/cr-2016-1011

Silva, M., Cerdeira, D., Pinto, S. & Gomes, T. (2019). Operating Systems for Internet of Things Low-End Devices: Analysis and Benchmarking. *IEEE Internet of Things Journal*, *6*(6), 10375–10383. https://doi.org/10.1109/JIOT.2019.2939008

Sivarajah, U., Kamal, M. M., Irani, Z. & Weerakkody, V. (2017). Critical analysis of Big Data challenges and analytical methods. *Journal of Business Research*, *70*, 263–286. https://doi.org/10.1016/j.jbusres.2016.08.001

Skerrett, I. (2017). *IoT Developer Survey 2017*. https://www.slideshare.net/IanSkerrett/iot-developer-survey-2017

Surendran, S., Nassef, A. & Beheshti, B. D. (2018). A survey of cryptographic algorithms for IoT devices. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT 2018): Farmingdale, New York, USA, 4 May 2018* (S. 1–8). IEEE. https://doi.org/10.1109/LISAT.2018.8378034

Suryadevara, N. K. & Mukhopadhyay, S. C. (2015). *Smart homes: Design, implementation and issues*. *Smart Sensors, Measurement and Instrumentation: Bd. 14*. Springer Science and Business Media. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=935781 https://doi.org/10.1007/978-3-319-13557-1

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I. S., Mazura, M., Harrison, M. & Eisenhauer, M. (2009). Internet of things strategic research roadmap. *Internet of things-global technological and societal trends*, *1*, 9–52. https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2430372/SINTEF%2BS13363.pdf?sequence=2

Want, R. (2006). An Introduction to RFID Technology. *IEEE Pervasive Computing*, *5*(1), 25–33. https://doi.org/10.1109/MPRV.2006.2

Weyrich, M. & Ebert, C. (2016). Reference Architectures for the Internet of Things. *IEEE Software*, *33*(1), 112–116. https://doi.org/10.1109/MS.2016.20

Whitman, M. E. & Mattord, H. J. (2018). *Principles of information security* (Sixth edition). Cengage Learning.

Wi-Fi Alliance. (2020). *Discover Wi-Fi | Wi-Fi Alliance*. https://www.wi-fi.org/discover-wi-fi

Yamazaki, D., Radecki, A. & Gotoh, K. (2007). RFID tag device, RFID reader/writer device, and distance measuring system.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M. & Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications*, *24*(3), 10–16. https://doi.org/10.1109/MWC.2017.1600421

Yu, Y., Li, Y., Tian, J. & Liu, J. (2018). Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wireless Communications*, *25*(6), 12–18. https://doi.org/10.1109/MWC.2017.1800116

Zigbee Alliance. (2020). *Zigbee - Spezifikation*. https://zigbeealliance.org/solution/zigbee/