Bachelorarbeit

Sicherheitsaspekte beim Connected Living.

Betrachtung der Risiken in Bezug auf die Datenübertragung und Sicherheitsmaßnahmen der Kommunikationsstandards.

Fachbereich Informatik und Kommunikationssysteme

Studiengang: Technische Redaktion (BTREL10)

Sommersemester 2016

HOME
HOCHSCHULE
MERSEBURG FH
University of
Applied Sciences

vorgelegt von:	Manuel Klausing Weingärten 48 06110 Halle
Matrikelnummer:	18273
Email:	manuel.klausing@stud.hs-merseburg.de
Erstgutachter:	Herr Prof. Dr.-Ing. Rüdiger Klein
Zweitgutachter:	Herr Prof. Dr. phil. Dr. rer. nat. habil. Michael Schenke
Abgabetermin:	04.05.2016

Inhalt

1 Einleitung

Wir leben im Multimediazeitalter. Der Fortschritt moderner Technologien schreitet schneller voran als je zuvor. Das Internet ist zum alltäglichen Gebrauchsgegenstand geworden und längst nicht mehr ausschließlich auf den Computer beschränkt. Mobiltelefone und Tablets, mit denen man unterwegs im World Wide Web surfen kann, sind zum Standard unserer modernen Gesellschaft geworden. Nach und nach folgen immer mehr Elektrogeräte und Maschinen mit eigener Internetschnittstelle. Das Internet der Dinge vernetzt viele milliarden Geräte weltweit miteinander. Die Vision des Connected Living, also das vernetzte Leben, wird sich in der Zukunft auf das normale Leben auswirken, und ein Teil davon werden. Es wird sich auf die Arbeit, auf Dienstleistungen, auf Konsumgüter und deren Produktionsprozesse, ebenso wie auf Politik und Wirtschaft auswirken. Ebenso, wie es das Internet einige Jahre zuvor getan hat. Die Anwendungsmöglichkeiten sind unzählig, denn fast jedes Gerät könnte vernetzt werden. Von der Armbanduhr, über die Lampe bis hin zu Kraftfahrzeugen.
Viele Anwendungsbeispiele sind bereits weitreichend bekannt, wie das Konzept des Smart Homes, das durch mediale Präsenz die meiste Bekanntheit erlangt hat. Weitere Bereiche des IoT sind unter anderem Wearables, Smart Cars und die Industrie 4.0.

Die Datensicherheit ist einer der wichtigsten Punkte dieser Technologien. Wie sicher ist die Datenübertragung? Können Dritte an die Daten gelangen oder gar die Steuerung der Geräte übernehmen? Das sind Fragen, die es zu klären gilt.
In dieser Arbeit beginne ich damit die Unterschiede in den Begriffen Connected Living, Smart Home, Industrie 4.0 und Internet der Dinge zu erläutern (Kapitel 1.1). Danach zeige ich auf, wie sich diese Technologien am Markt entwickeln (Kapitel 1.2). Im zweiten Kapitel werden verschiedene Kommunikationsstandards und deren Sicherheitsmaßnahmen aufgezeigt. Dabei werden als erstes, Hardwarenahe, beim Smart Home Konzept genutzte, Funkprotokolle (Kapitel 2.1.1 - 2.1.5) betrachtet. Als Nächstes wird die Kommunikationsarchitektur Universal Plug and Play (Kapitel 2.1.6) begutachtet. Anschließend folgt eine Gegenüberstellung von offenen und proprietären Standards (Kapitel 2.1.7). Das nächste Kapitel zeigt Kommunikationsarchitekturen aus dem Bereich der Industrie 4.0. Dabei handelt es sich um OPC UA und MTConnect, gefolgt von ihrem gemeinsamen Projekt und der Gegenüberstellung beider (Kapitel 2.2.1 - 2.2.4). Das dritte Kapitel befasst sich mit den Sicherheitsrisiken und bietet Beispiele bekannter Sicherheitslücken (3.1 – 3.6). Im abschließenden Fazit (Kapitel 4) folgt eine Zusammenfassung und Auswertung der Arbeit.

1.1 Begriffsabgrenzung

1.1.1 Connected Living[1]

Connected Living bedeutet, die Vernetzung der unterschiedlichsten Geräte miteinander. So wird es ermöglicht, dass diese untereinander kommunizieren, sich koordinieren und aus der Ferne steuern lassen. Dies betrifft neben PCs, Smartphones und Tablets auch Haushaltsgeräte, Autos, Produktionsmaschinen bis hin zu sogenannten Wearables wie Uhren, Hörgeräte oder Brillen. Begriffe wie "Smart Home, "Industrie 4.0" oder "Internet der Dinge" sind in Multimedia und Literatur häufig verwendet und somit geläufig. "Connected Living" ist der Oberbegriff für diese Konzepte (siehe Abb 1), da es sich überall um die sogenannte Maschine-zu-Maschine-Kommunikation (M2M), also den Datentransfer zwischen zwei Endgeräten handelt. So folgen alle dem Prinzip des "Vernetzten Lebens".

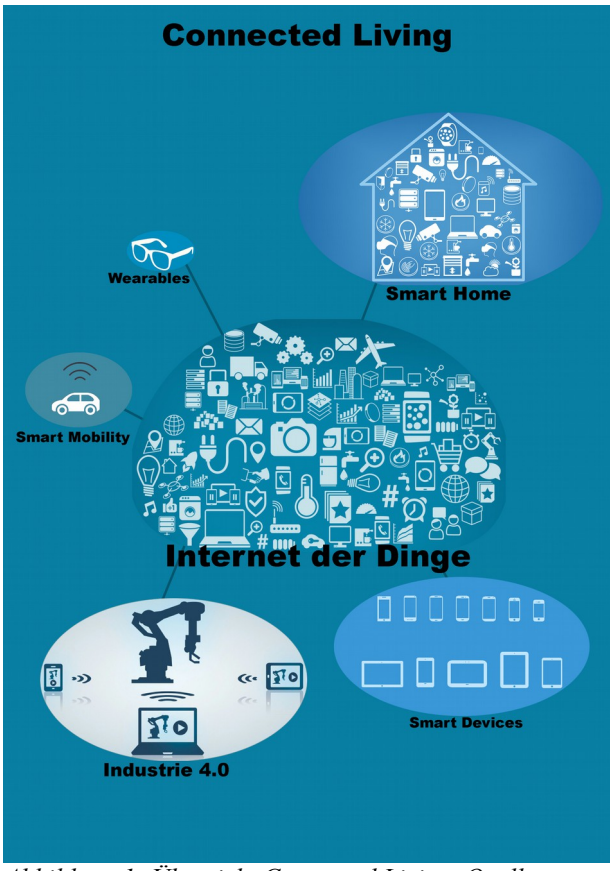

Abbildung 1: Übersicht Connected Living, Quelle: eigene Darstellung

1 Vgl. Connected Living e.V. [Online]

1.1.2 Smart Home[2]

Beim Konzept des Smart Homes oder Gebäudeautomation geht es darum, eine Vielzahl von Haushaltsgeräten und Unterhaltungselektronik in einem Netzwerk zu vereinen. Über dieses Netzwerk können die Geräte miteinander kommunizieren und gesteuert werden. Diese Kommunikation kann über Funk oder eine Datenleitung erfolgen. Wobei die Methode, alle Endgeräte mit Kabeln zu versehen wenig komfortabel und sehr viel kostenintensiver ist, als bei einer drahtlosen Datenübertragung. Aus diesem Grund werden bevorzugt Techniken der Drahtloskommunikation, abseits des heimischen Computernetzwerks, genutzt, welche eigenständige Funknetze etablieren und eigenständig administrieren. Die Vernetzung der Heimelektronik soll das Leben der Bewohner zum einen sicherer machen. So können beispielsweise intelligente Rauchmelder eigenständig die Feuerwehr alarmieren oder die Alarmanlage die Polizei rufen. Ebenso kann eine Smart Home Lösung die physische Sicherheit der Bewohner erhöhen und das Eigentum schützen. So können beispielsweise automatische Rolläden vortäuschen, ein Haus sei während des Urlaubs bewohnt. Sollte dennoch etwas passieren, können Überwachungskameras durch Sensoren in Türen und Fenstern aktiviert werden. Es wird ein Alarm ausgelöst, die Bewohner werden per SMS informiert und die Bilder der Überwachungskameras werden zur Beweissicherung in einer privaten Cloud gespeichert. Zum anderen sollen Smart Homes energieeffizient und ressourcenorientiert sein. So kann, wenn niemand zu Hause ist, ein intelligentes Türschloss melden, wenn es abgeschlossen ist. und die aufgedrehte Heizung, die vergessen wurde, dreht sich selbstständig ab.

1.1.3 Industrie 4.0[3]

Die Industrie 4.0 wird als sogenannte vierte industrielle Revolution bezeichnet. Nach der Dampfmaschine, dem Fließband und der Digitalisierung kommen nun, mit den Smart Factories, die intelligenten Fabriken. Durch sie sollen Produktionsprozesse flexibler und effizienter werden. Wie bei einem Smart Home die Sensoren und Aktoren, kommunizieren hier Maschinen, Anlagen und Menschen mittels einer Schnittstelle miteinander. Auch hier befinden sich alle Teilnehmer in einem Netzwerk, das größer ist als zu Hause. Anders als bei einem Smart Home, bei dem ein PC nicht zwingend notwendig ist, übernehmen bei einer smarten Produktionsstätte der Industrie 4.0, Computer oder Server die Steuerung einzelner Maschinen und Anlagen. Es könnten somit, beispielsweise Produktionszeiten verkürzt werden, da eine Anlage selbstständig neue Produktionsrohstoffe nachbestellen kann, wenn diese zur Neige gehen.

2 Vgl. Smart Home Guide [Online]
3 Vgl. Plattform Industrie 4.0 2015, [Online]

1.1.4 Internet der Dinge/ Internet of Things (IoT)[4]

Das Internet der Dinge schließt die Konzepte Smart Home und Industrie 4.0 mit ein. Im IoT beschränkt sich die Kommunikation der Geräte nicht auf ein Netzwerk innerhalb eines Gebäudes, sondern ermöglicht sie theoretisch weltweit. Anders als bei Smart Home- und Industrie 4.0 Netzen, welche nicht zwangsläufig eine Verbindung zum Internet haben, senden IoT-Devices ihre Daten durch IP-basierte Netzwerke zu anderen Endgeräten. Das bedeutet jedoch nicht, dass jedes IoT Gerät direkt an das Internet angeschlossen ist. Viele Geräte nutzen beispielsweise das Smartphone als Gateway. Das heißt, dass die Daten, etwa eines Fitnessarmbandes, an das Mobiltelefon gesendet werden, und dieses leitet sie über das Mobilfunknetz an eine Cloud oder ein anderes Endgerät weiter.

1.2 Trend

Das Interesse von Kundenseite an den neuen Technologien besteht, zeigen diverse Befragungen. So soll die Zahl der Smart Homes bis zum Jahr 2020 von derzeit etwa einer halben Million auf circa 2,4 Millionen ansteigen (siehe Abb. 2).

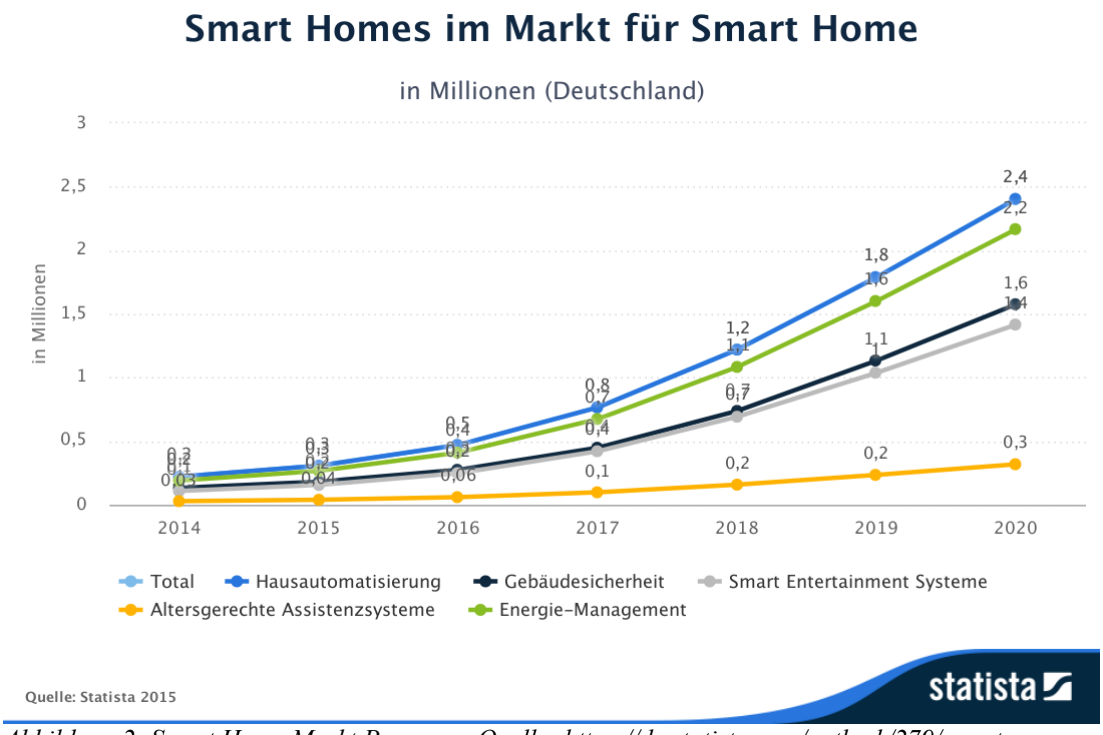

Abbildung 2: Smart Home Markt Prognose, Quelle: https://de.statista.com/outlook/279/smart-home#market-revenue

Wie eine Studie aus dem Jahr 2014 zum Thema Sicherheit bei Smart

4 Vgl. ITWissen 2015, [Online]

Metering Produkten ergab, spielt diese eine große Rolle. Die Studie wurde von GMI, einer Abteilung von Lightspeed Research, im Auftrag des Sicherheitsanbieters Fortinet geführt. Die Umfrageteilnehmer waren Hauseigentümer zwischen 20 bis 50 Jahren mit Technikerfahrung. Die Befragten stammten aus Deutschland, den USA, Frankreich, Großbritannien, Italien, Australien, China, Indien, Malaysia und Südafrika. Etwa 61 Prozent der über 1800 befragten, technisch versierten Hausbesitzer sicher, dass sich das vernetzte Eigenheim mit an das Internet angeschlossenen Haushaltsgeräten und Unterhaltungselektronik in den nächsten vier bis fünf Jahren vermehrt durchsetzen wird. Zum Thema Sicherheitsbedenken äußerten sich 69 Prozent der weltweit befragten Teilnehmer mit mäßiger bis sehr großer Sorge. Nur 55 Prozent der Befragten, haben bedenken, wenn es um die Bedrohung der eigenen Privatsphäre geht. Sollte sich jedoch herausstellen, dass ein Smart Device heimlich Daten über die Besitzer sammelt und weitergibt, würden 61 Prozent der Befragten sofort Konsequenzen ziehen. Auf der anderen Seite wären 35 Prozent der Teilnehmer bereit, es den Herstellern zu erlauben, die gesammelten Daten zu nutzen. Der Industrie wird dieser Anteil vermutlich zu niedrig sein, da beispielsweise Energieversorger hoffen, ihre Kapazitäten und Netzsteuerungen durch diese Daten zu optimieren. Dies dürfte nicht vollends gelingen, sollte nur ein Drittel aller smarten Haushalte ihre Informationen freigeben. Hersteller und Internetdienste, die ebenso ihre Arbeit in diesem Feld ausweiten wollen, müssen noch vermehrt Überzeugungsarbeit leisten um den Absatz zu erhöhen. Denn laut der Umfrage würden in Deutschland momentan nur 17 Prozent der Teilnehmer den Zugriff auf ihre intelligenten Haushaltsgeräte erlauben. Im weltweiten Durchschnitt forderten sogar 41 Prozent, dass die Datenerhebung gänzlich vom Staat geregelt werden sollte, in Deutschland waren nur 26 Prozent dieser Ansicht. Ein wenig paradox wird es beim Thema Gewährleistung der Systemsicherheit, denn 54 Prozent der Befragten sehen die Hersteller in der Sicherheitsverantwortung und nur 25 Prozent sehen diese bei sich selbst. Dabei stellt sich unweigerlich die Frage, wie die Gerätehersteller die Sicherheit gewährleisten, Firmwareupdates einspielen und Sicherheitslücken schließen soll, ohne auf die Geräte zugreifen zu dürfen. Möglicherweise ist aber genau diese Frage der Ansatz um die Nutzer davon zu überzeugen, den Zugriff auf die Smartobjekte zu gestatten und auf diesem Weg nicht nur Sicherheitslücken ausmerzen, sondern auch, die auf Kapazitäts- und Energieeffizienz gerichtete Datenerhebung zu gewährleisten.[5]

5 Vgl. Fortinet - 2014 Fortinet Reveals “Internet of Things: Connected Home” Survey Results S.1ff

2 Kommunikationsstandards und ihre Sicherheitsmaßnahmen

2.1 Smart Home Standards

Wie bei einem Netzwerk, wo der Router entweder über WLAN oder via Ethernet-Kabel mit einem PC kommuniziert, kann bei Smartobjekten die Kommunikation ebenfalls kabelgebunden oder kabellos erfolgen. Der Vorteil von sogenannten Feldbussen liegt darin, dass sie kabelgebunden sind und einem Angreifer somit nicht die Möglichkeit bieten, sie per Fernzugriff zu manipulieren. Andererseits bieten Feldbusse weniger Komfort und haben höhere Anschaffungskosten. Können Geräte in einem Funksystem ohne Weiteres integriert werden, muss es in einem kabelgebundenen Netz mindestens mit einer zusätzlichen Leitung und eventuell noch mithilfe weiterer Hardware hinzugefügt werden. Das limitiert die Anzahl der Endgeräte oftmals stärker als bei Funkbussen. Im Umkehrschluss bedeutet das, dass ein Funksystem einfacher erweiterbar und komfortabler ist.[6] Da kabelgebundene Systeme wie KNX[7] meist nur bei Neubau oder Kernsanierungen installiert, und somit eher selten genutzt werden, und weil sie, wie eingangs erwähnt, einen physischen Zugang benötigen, um attackiert werden zu können, werden sie an dieser Stelle nur kurz erwähnt.

2.1.1 WLAN und Bluetooth

Standards, wie WLAN und Bluetooth bringen zwar die Voraussetzungen für das Connected Living mit, und haben zudem den Vorteil, dass sie in den meisten Haushalten bereits existieren. Jedoch wurden sie nicht für diesen Zweck entwickelt und eignen sich, besonders im Hinblick auf die Energieeffizienz, nur wenig für die Gebäudeautomation. WLAN bietet zwar den Vorteil, die kleinen Datenpakete der Smartobjekte problemlos mitzuübertragen, da es für hohe Datenaufkommen konzipiert wurde. Doch steht dem ein sehr hoher Energiebedarf gegenüber. Der Energieverbrauch eines handelsüblichen Controllers mit WLAN Schnittstelle, welcher in einem Sensor verbaut sein könnte, beträgt bis zu 500 mA. Bei einem ständigen Betrieb wäre eine Batterie innerhalb weniger Stunden aufgebraucht. Bei einem Smart Home ist ein langer Dauerbetrieb jedoch der entscheidende Faktor. Deshalb sollte die Datenübertragung so selten wie möglich geschehen und kurz gehalten werden. Das ist sowohl bei WLAN als auch bei Bluetooth etwas schwierig, da der Verbindungsaufbau unter den Geräten selbst schon einige Sekunden dauern kann. Kommt dann noch eine SSH-Verschlüsselung zum Einsatz, kann sich der zeitliche Rahmen weiter in die Länge ziehen. Zudem ist die Frequenz von 2,4 GHz, auf der WLAN funkt, viel genutzt. Andere WLAN-Netzwerke und Geräte auf dieser Frequenz können zu Störsignalen führen. Aufgrund dieser Tatsachen, berücksichtigen die

6 Vgl. KNX Impuls 2015, S.1f

7 KNX: Feldbussystem zur Gebäudeautomation. Siehe auch: https://www.knx.org

meisten Hersteller WLAN nicht als Smart Home Standard und die Smartobjekte auf WLAN-Basis sind nicht kompatibel mit denen anderer Funkstandards.[8]
Ähnlich nachteilig verhält es sich bei Bluetooth. Auch hier ist der Energiebedarf der Geräte zu hoch, um für ein Smart Home infrage zu kommen. Zumindest war das bei älteren Versionen der Fall. Mit einer neuen Protokollarchitektur namens Bluetooth Low Energy (BLE) wurde eine energieeffizientere Arbeitsweise für Bluetoothgeräte entwickelt. Die Übertragungsrate liegt bei maximal 1MBit/s, was für die geringen Datenmengen bei Smartobjekten genügt. Doch aufgrund der Nutzung unterschiedlicher Protokolle, ist die Interoperabilität zu anderen Standards ebenso selten, wie auch bei WLAN gegeben. Dazu kommt, die geringe Reichweite, von nur etwa zehn Metern, welche in einer durchschnittlichen Haushaltsgröße als zu wenig beschrieben werden kann.[9]
Trotz der Möglichkeit, sich ein Smart Home mit auf WLAN oder Bluetooth basierenden Geräten einzurichten, ist ihre Verbreitung vergleichsweise gering, da sie nicht die geeignetsten Smart Home Netze bieten. Dennoch werden sie fester Bestandteil jedes automatisierten Eigenheims sein. Denn egal welcher Übertragungsstandard unter den Smart Devices genutzt wird, mindestens zur Steuerung einzelner Geräte per Smartphone oder Tablet wird WLAN als Schnittstelle unumgänglich sein.

2.1.2 ZigBee

ZigBee ist ein hardwarenahes Protokoll und für die Übertragung geringer Datenmengen auf kurzen Distanzen ausgelegt ist. Entwickelt wurde es von der ZigBee Alliance, der unter anderem bekannte Konzerne wie Samsung, Philips und LG angehören. Im Dezember 2004 verabschiedete die Alliance die erste ZigBee Spezifikation. Es wurde für das Connected Living, genauer für Smart Homes konzipiert. Aufgrund des geringen Datendurchsatzes ist ZigBee Hardware sehr energieeffizient und wird oftmals nur mit einer Batterie betrieben. ZigBee sendet auf Frequenzen um 868 MHz, 915 MHz und 2,4 GHz und ist für Entfernungen zwischen zehn und 100 Metern ausgelegt.[10]
Beim Sicherheitskonzept von ZigBee setzt auf dem Sicherheitsmodell von IEEE 802.15.4, einem Übertragungsprotokoll das auf den beiden untersten Schichten, dem „Physical Layer“ und dem „Medium Access Control Layer“, arbeitet. Dieses wurde hierfür um zwei zusätzliche Schichten erweitert, den „Network Layer“ (NWK) und den „Application Support Sublayer“ (APS). Außerdem setzt dort auch, für Softwareentwickler, das „Application Programming Interface“ kurz API an (siehe Abb. 3).[11]

8 Vgl. Andelfinger 2015 S.21
9 Vgl. Bluetooth SIG 2016 [Online]
10 Vgl. ZigBee Alliance S.591
11 Vgl. ebd. S. 2

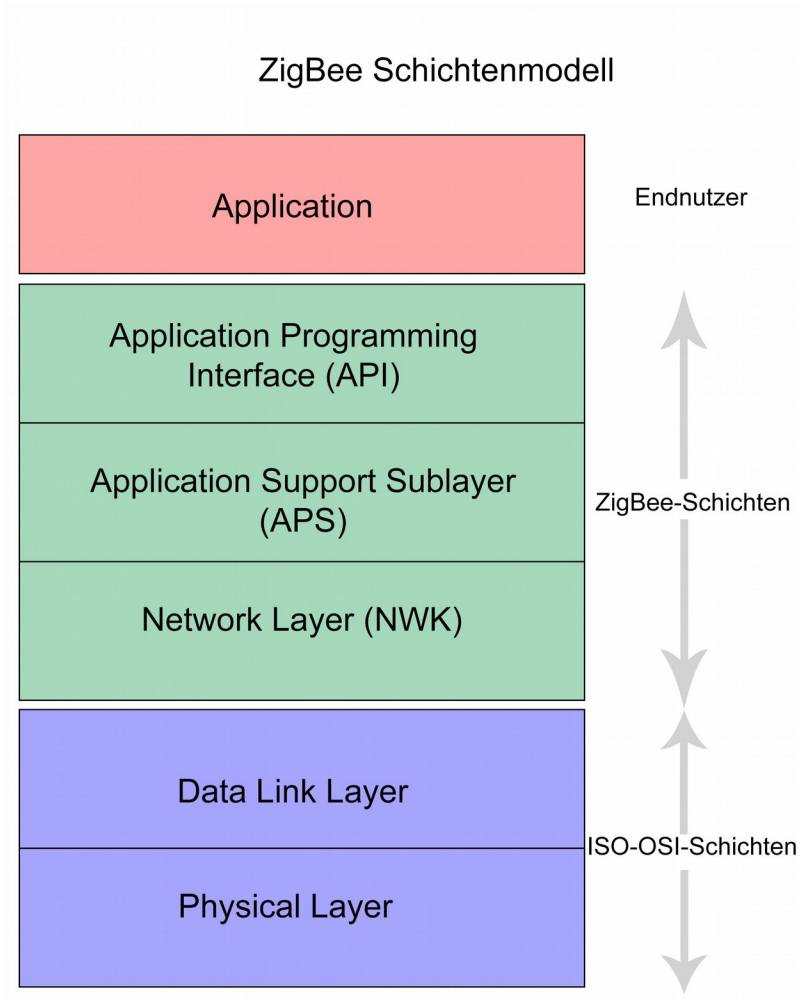

Abbildung 3: ZigBee Schichtenmodell, Quelle: eigene Darstellung

Bei ZigBee werden Mesh-Netzwerke, also vermaschte Netze, unterstützt. Das bedeutet, dass jedes Gerät in einem Netz als Knotenpunkt dient und mit einem oder mehreren anderen Endgeräten verbunden ist. Dadurch dehnt sich die Reichweite des Netzes aus, denn kommunizieren zwei Geräte, die eigentlich zu weit voneinander entfernt sind, leiten die anderen Geräte die Datenpakete weiter. Dabei arbeitet ZigBee nach dem Open Trust Prinzip. Das sogenannte Trust Center baut Instanzen auf, bei denen sich die Schichten und Anwendungen der Geräte gegenseitig vertrauen.[12] Das spart Ressourcen bei der Verschlüsselung, da nicht in jeder Schicht neu verschlüsselt werden muss. Ab der Sicherungsschicht kann jede Instanz eine sichere Verbindung zu der gleichen Schicht anderer ZigBee Geräte herstellen. Dabei findet nur ein Schlüsselaustausch zwischen dem Sende- und dem Empfangsgerät statt, egal von welcher Schicht die Verbindung ausgeht und über wie viele Geräteknoten sie führt. Auf den Schlüsselcode können ausschließlich die in Verbindung stehenden Partner zugreifen,

12 Vgl. Zillner 2015 S.6

wodurch sie nicht in jedem Gateway ent- und verschlüsselt werden müssen. Grundsätzlich gibt es drei Arten von Schlüsseln bei ZigBee, den Master Key, den Link Key und den Network Key. Dabei ist der Master Key ein in jedem ZigBee-Gateway vorinstallierter Schlüssel der für den vertraulichen Austausch des Link Keys unterhalb der Knoten verantwortlich ist. Der Link Key ist ein 128 Bit langer, einzigartiger Key, welcher mithilfe des AES-Verfahrens[13] generiert und zwischen zwei Partnern vor der eigentlichen Kommunikation zu deren Absicherung ausgetauscht wird. Der Network Key ist ebenfalls ein 128 Bit langer, im AES-Verfahren generierter Schlüssel, welchen sich die ZigBee-Geräte teilen beziehungsweise, der unter allen Geräten im Netz bekannt ist.[14]

2.1.3 Z-Wave

Z-Wave wurde von dem dänischen Unternehmen Zensys in Zusammenarbeit mit der Z-Wave Alliance direkt für die drahtlose Kommunikation in Smart Homes konzipiert. Der Z-Wave Alliance gehören derzeit 350 Konzerne an, darunter Technikgrößen wie LG, Bosch, Panasonic und D-Link. Er wurde im Jahr 2012 von der ITU-T als Standard G.9959 definiert. Einen großen Vorteil im Gegensatz zu anderen Standards ist, dass es bei Z-Wave aktuell mehr als 1500 lizenzierte Geräte gibt, welche alle interoperabel sind.[15] Der Standard sendet in Europa auf dem freien ISM-Band um 868 MHz und auf dem vom WLAN genutzten 2400 MHz-Band. Es wird ein vermaschtes Netz aufgebaut, in dem alle Geräte als Knoten fungieren. Ebenso wie es bei ZigBee der Fall ist.[16] Z-Wave kommuniziert zwar verschlüsselt, ebenfalls mittels des 128-Bit AES Verfahrens, jedoch sind bei offenen Standards die technischen Details für jeden einsehbar und somit können Dritte Schwachstellen leichter ausfindig machen. Aufgrund dessen, ist das nicht die einzige Sicherheitsmaßnahme im Z-Wave Standard. Ebenso ist die Kommunikation innerhalb eines Z-Wave Netzes nur unter miteinander bekannten Geräten möglich. Endgeräte, die dem Netz hinzugefügt werden, müssen vom Nutzer mithilfe einer Passwortabfrage autorisiert werden. Noch einen Schritt weiter geht der Standard mit seiner Securityklasse, welche auf Einmalpasswörtern basiert. Es wird ein verschlüsselter Kommunikationskanal geöffnet und der Empfänger übermittelt dem Sender ein zufällig generiertes und nur kurzzeitig gültiges Passwort. Erst danach findet die eigentliche Datenübertragung statt (siehe Abb.4). Die Securityklasse ist nicht bei allen Z-Wave Geräten zu finden. Sie ist aber beispielsweise bei Türschlössern und Fenstersensoren Pflicht und kann bei einigen Geräten extra aktiviert werden.[17]

---

13 AES: Advanced Encryption Standard - Algorithmus für die symmetrische Blockverschlüsselung (Blockchiffre). Weltweit in Hard- und Software implementiert, um sensible Daten zu verschlüsseln. Als äußerst sicher eingestuft.

14 Vgl. Gascón 2009, [Online]

15 Vgl. Z-Wave Alliance 2016, [Online]

16 Vgl. Z-Wave 2016, [Online]

17 Vgl. Pätz 2014, S. 196

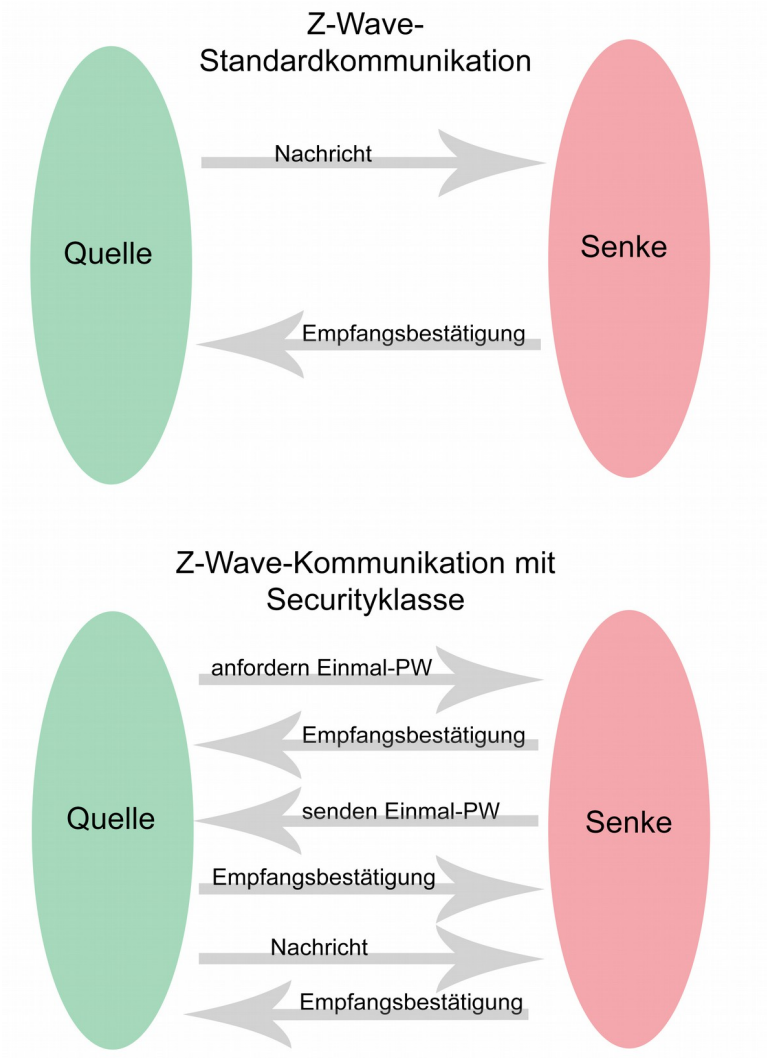

Abbildung 4: Kommunikationswege Z-Wave, Quelle: eigene Darstellung

Die Securityklasse bietet zwar ein enormes Maß an Sicherheit, vervielfacht andererseits aber das Datenaufkommen und somit die benötigte Zeit. Bei einer Kommunikation ohne Securityklasse wird ein wenige Byte langer Befehl gesendet und dieser wird vom Empfänger, aufgrund der bei Z-Wave üblichen Zweiwegekommunikation, bestätigt. Ist die Securityklasse aktiv, fordert der Sender ein Einmalpasswort an, das wird vom Empfänger bestätigt. Nun sendet der Empfänger das Einmalpasswort zum Sender und auch dieser bestätigt dessen Empfang. Dann erst sendet die Quelle das eigentliche Datenpaket mithilfe des Einmalpasswortes. Und auch dieses wird von der Senke mit einer Empfangsbestätigung quittiert. Durch diese Schutzmaßnahmen und die begrenzte Reichweite solcher Netze ist Z-Wave gegen Lauschangriffe auf den Funkverkehr gut abgesichert. Jedoch obliegt sowohl bei ZigBee als auch bei Z-Wave die Absicherung der Geräte vor

Cyberattacken aus dem World Wide Web den Herstellern der jeweiligen Smart Home Basisstationen.[18]

2.1.4 EnOcean

Der Übertragungsstandard EnOcean wurde in Deutschland, von der EnOcean GmbH entwickelt. Seit dem Jahr 2012 ist EnOcean ein international anerkannter Funkstandard und unter der Kennung ISO/IEC 14453-3-10 bekannt. Das bedeutet, dass es sich, wie bei Zigbee und Z-Wave, um einen offenen Standard handelt. Energieeffizienz soll ein Aushängeschild der Smart Home Technologie sein. Mit EnOcean wurde dieses Credo sehr erfolgreich umgesetzt. Während die meisten Smart Home Geräte so sparsam sind, dass die Batterien nur selten ausgetauscht werden müssen, funktionieren EnOcean Produkte meist komplett ohne Batterie. Die geringen Energiemengen, die zum Senden von Datenpaketen notwendig sind, werden mithilfe von Solarzellen, Peltierelementen oder elektrodynamischen Energiewandlern erzeugt. Durch dieses Konzept können die Geräte wartungsfrei betrieben werden (siehe Abb. 5).

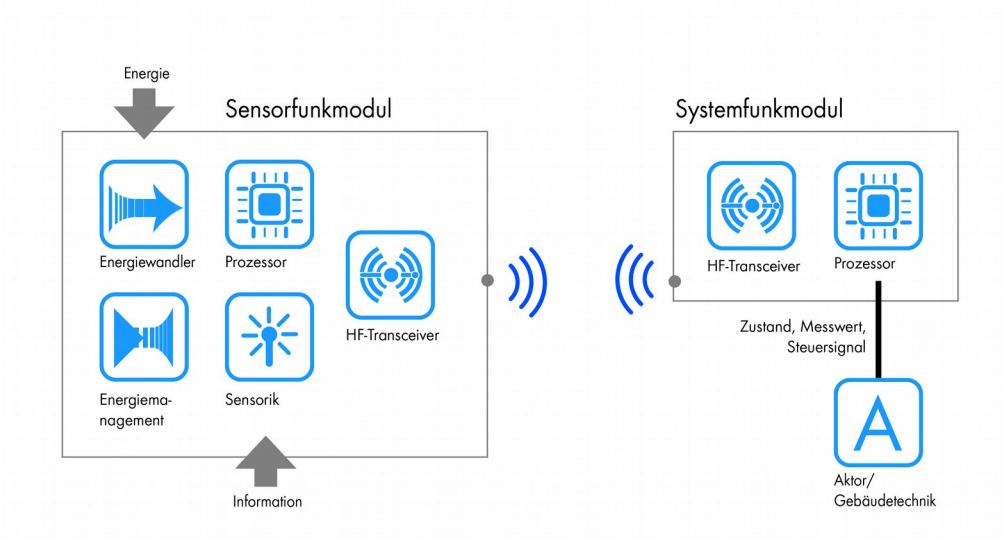

Abbildung 5: EnOcean Systemgrafik, Quelle: http://www.wago.de/loesungen/gebaeudetechnik/gebaeudeautomation/systembeschreibung/enocean/index.jsp

EnOcean sendet in Europa auf dem freien ISM-Frequenzband von 868,42 MHz. Eine Basisstation auf EnOcean-Grundlage kann an ein kabelgebundenes KNX-System angeschlossen werden und kann dieses somit erweitern. Derzeit bieten über 100 Firmen, Produkte auf EnOcean Basis an, darunter beispielsweise Siemens, Honeywell und Osram[19].
Das Sicherheitsmodell von EnOcean setzt sich aus mehreren Komponenten

18 Vgl. König 2016, [Online]
19 Vgl. EnOcean 2016, [Online]

zusammen. Angefangen bei der Integrität, wobei dem Datenpaket eine eine Prüfsumme, die sogenannte Checksum, angehängt wird. Mit dieser soll sichergestellt werden, dass die Daten auf dem Weg nicht manipuliert werden. Des Weiteren verfügen EnOcean Geräte über eine individuelle, vom Hersteller vergebene ID. Diese ist 32 Bit lang und kann weder entfernt noch verändert werden. Mithilfe dieser ID wird die Authentifizierung der Geräte gewährleistet. Hinzu kommt, das mit jedem Datenpaket ein sogenannter Rolling-Code generiert und mitgesendet wird. Dieses Verfahren ist beispielsweise bei Autoschlüsseln oder Garagentoröffnern gängige Praxis. Als Verschlüsselungsverfahren kommt bei EnOcean die 128-Bit AES Verschlüsselung zum Einsatz. Da sich die Sicherheit immer negativ auf den Energieverbrauch auswirkt, können die Sicherheitseinstellung flexibel angepasst werden. Das bedeutet, dass EnOcean-Produkte proportional zu ihrer steigenden Energieeffizienz unsicherer arbeiten.[20]

2.1.5 HomeMatic/RWE Smart Home

HomeMatic wurde von der deutschen Firma eQ-3 entwickelt und direkt für die Gebäudeautomation konzipiert. Das Übertragungsprotokoll ist unter dem Namen BidCos bekannt, was für „Bidirectional Communication System“ steht. Im Gegensatz zu bisher genannten Varianten handelt es sich bei HomeMatic nicht um einen offenen Standard. Folglich gibt es keine Geräte anderer Unternehmen, die mit diesem Protokoll arbeiten. Geräte der HomeMatic Reihe gibt es sowohl batterie- als auch netzbetrieben. Es wurde auf die Kommunikation zwischen batteriebetriebenen Endgeräten ausgelegt und arbeitet somit sehr energieeffizient. Gleichwie die offenen Standards, nutzt HomeMatic das freie Frequenzband um 868 MHz. Eine Besonderheit bei der HomeMatic Lösung ist, dass es nicht zwingend ein Gateway benötigt, und nicht mit dem Internet verbunden sein muss. Beim Thema Sicherheit ähnelt es den offenen Standards. Bei der Authentisierung der Geräte, der Webzugriff und bei der Verschlüsselung der Kommunikation werden das 128-Bit AES Verfahren und CCM/RFC3610 verwendet, der dazu verwendete Systemsicherheitsschlüssel ist standardmäßig in der Firmware der Basisstation hinterlegt und wurde laut Angabe von eQ-3 „bisher nicht „gehackt““[21]. Wie der Name „Bidirectional Communication System“ suggeriert, läuft die Kommunikation im Zweiwegesystem ab. Wie bei Z-Wave bestätigt das Empfangsgerät den Eingang des Datenpakets beim Sender. Die übertragenen Daten werden mit einer XOR Operation codiert (siehe Abb. 6).[22]

20 Vgl. Ohland 2012, [Online]
21 eQ-3 2016a, [Online]
22 Vgl. eQ-3 2016b, [Online]

```
1  dec [0] = enc [0]; // Laengenbyte
2  dec [1] = ~ enc [1]) ^ 0 x89;
3
4  for ( 1 =2; 1 < n -3; 1 ++)
5      dec [ 1 ] = ( enc [1 -1] + 0 xdc ) ^ enc [ 1 ];
6  dec [ 1 ] = enc [ 1 ] ^ dec [2];
```

Abbildung 6: Beispiel einer XOR-Codierung, Quelle: eigene Darstellung

Die Smart Home Lösung der Firma RWE ähnelt stark HomeMatic. Der Grund dafür ist, dass die Firma eQ-3, die Entwickler von HomeMatic, ebenfalls für RWE die Endgeräte und das Übertragungsprotokoll entwickelt haben. Dafür hat RWE mehr Wert auf Datensicherheit Schutz gegen Angreifer gelegt. Zudem sind bereits alle Geräte auf IPv6 Standard. Genau wie HomeMatic, ist auch die RWE-Lösung vorwiegend auf Batteriebetrieb ausgelegt. Im Unterschied zu den offenen Systemen, bei denen die technischen Spezifikationen meist frei verfügbar sind, bleiben diese bei proprietären Lösungen meist Firmengeheimnis. Bekannt ist, dass RWE Smart Home, da es auf dem HomeMatic Protokoll „BidCos“ basiert, ebenfalls die Datenpakete per 128 Bit AES-Encryption, verschlüsselt überträgt. Und durch die bidirektionale Kommunikation wird der Empfang einer Nachricht vom Empfangsgerät quittiert. Zudem können optionale Sicherheitsfeatures aktiviert werden. Mit der Berechtigungsüberprüfung sendet der Empfänger nicht nur eine Empfangsbestätigung, sondern eine verschlüsselte Rückfrage, welche vom Sender bestätigt werden muss. Zur Authentifizierung wird ein AES-Schlüssel genutzt, der auf einem Systemsicherheitsschlüssel basiert, der vom Hersteller standardmäßig hinterlegt ist, aber vom Nutzer geändert werden kann.[23]

2.1.6 Universal Plug and Play (UPnP)

Zum Connected Living gehören neben der Steuerung der Haushaltselektronik auch die Steuerung der Unterhaltungselektronik. Dabei können verschiedene Medien wie beispielsweise Filme, Musik, Fotos oder Spiele auf einem zentralen Server gespeichert, und von dort aus abgerufen werden. Ebendies wird durch Universal Plug and Play möglich. Deshalb ist UPnP auch ein wesentlicher Bestandteil der Smart Home Unterhaltungselektronik. Außerdem beinhaltet UPnP die Option, dank Internet Gateway Device Protocol (IGD) den Router anzuweisen, ausgewählte Ports zu öffnen und Internetanfragen an einen Rechner, welcher per NAT[24] an das Netzwerk gekoppelt ist, weiterzugeben. Dies ist

23 Vgl. eQ-3 2016a [Online]

24 NAT: Network Address Translation (dt. Netzwerkadressübersetzung) Verfahren die automatisiert Adressinformationen in Datenpaketen ersetzen, um verschiedene Netze zu verbinden.

beispielsweise für Datenaustausch oder Videotelefonie über Instantmessenger notwendig. Universal Plug and Play ist kein Smart Home Verbindungsstandard wie die bisher genannten, da er weder für das Smart Metering konzipiert wurde, noch gibt es die für das Smart Home typischen Sensoren und Aktoren mit dieser Technologie. UPnP wurde ursprünglich von Microsoft eingeführt, um in einem IP basiertem Netzwerk verschiedene Geräte wie zum Beispiel Router, Drucker, Audio- und Videogeräten oder Haussteuerungen herstellerübergreifend und -unabhängig anzusteuern. UPnP wird zur universellen Vernetzung sowohl gewerblicher als auch privater Netzwerke besonders im Feld der Smart Homes verwendet. Standardisierte Netzwerkprotokolle und Datenformate wie IP, UDP, HTML, TCP und XML bilden die Basis dieser Architektur[25]. Mit UPnP ist es nicht möglich, ein eigenes Netz wie bei den vorhergehend genannten Standards aufzubauen. UPnP Geräte können aber beispielsweise über Bluetooth, LAN oder WLAN in das bestehende Heimnetz integriert werden. Bedauerlicherweise sind im Universal Plug and Play Konzept keine eigenen Sicherheitsfunktionen vorhanden. Deshalb sind UPnP Geräte auf Übertragungsarten und Protokolle angewiesen, die eigene Sicherheitsvorkehrungen besitzen.[26]

2.1.7 Offene vs. Proprietäre Standards

Sowohl offene Standards wie auch proprietäre Lösungen, bringen jeweils Vor- und Nachteile mit sich. Es sollte gut überlegt sein, welche Technik den eigenen Anforderungen und Wünschen an ein Smart Home gerecht wird. Zweifellos sind offene Systeme, da sie herstellerübergreifend sind, einfacher erweiterbar. Die Zahl der Produkte auf dem Markt ist um ein Vielfaches höher, da Produkte der unterschiedlichen Anbieter interoperabel agieren. Dadurch ist es möglich, ein Smart Home mit noch mehr Funktionen auszustatten. Anders bei den proprietären Varianten, wo die Zahl der in einem Netzwerk möglichen Endgeräte meist stärker limitiert ist, da nicht so viele Produkte zur Erweiterung zur Verfügung stehen. Betrachtet man die IT-Sicherheit, sind die proprietären Lösungen schon von Hause aus etwas besser aufgestellt. Haben die offenen Standards zwar mehr oder weniger solide Sicherheitskonzepte, kann sie jedoch jeder einsehen. Außerdem versuchen sich Hacker eher an offenen Standards, da diese verbreiteter sind und mehr Ziele bieten. Des Weiteren werden komplette Smart Home Kits von proprietären Systemen häufiger Expertentests unterzogen. Und die dabei gefundenen Sicherheitsmängel werden meist rasch behoben. Es steht also Flexibilität und Erweiterbarkeit gegen höhere Sicherheit. Bei vielen Käufern wird im Endeffekt sicherlich der Preis der Smartobjekte ausschlaggebend sein, welcher bei den offenen Systemen meist etwas niedriger ist.

25 Vgl. Universal Plug and Play 2008, S. 1
26 Vgl. ebd. S. 71

2.2 Industrie 4.0 Standards

Anders als bei den Standards zur Haussteuerung, bei denen die Module aus kleineren Geräten wie Rauchwarnmelder, Fenstersensoren, Heizungsthermostaten oder Türschlössern bestehen, sind es auf Unternehmensebene große Maschinen und Anlagen, die selbstständig Arbeiten verrichten, wie Fertigungsroboter in einer Autofabrik. Diese Maschinen und Anlagen sind miteinander vernetzt und werden zentral von Computern gesteuert. Durch die langlebige Industrietechnik werden die typischen industriellen Kommunikationsprotokolle wie Modbus TCP und Profinet, welche auf TCP/IP basieren, noch einige Zeit bestehen bleiben. Nebenher gibt es eine Menge neuer Standards, welche sich beim Vernetzen intelligenter Geräte zum Internet der Dinge etablieren wollen. Am Vielversprechendsten sind dabei, die im Folgenden erklärten, OPC UA und MTConnect.[27]

2.2.1 Open Platform Communications Unified Architecture (OPC UA)

Bei OPC UA geht es ausschließlich um Standardisierung und Interoperabilität. Es beschreibt zum einen die Vernetzung der Maschinen untereinander, die sogenannte M2M-Kommunikation, und zum anderen die Anbindung von Automatisierungstechnik an Anwendungen. Der typische OPC-Standard baut auf dem von Microsoft definiertem „Distributed Component Object Model“, kurz DCOM, auf, welches der COM-Technologie ermöglicht in Rechnernetzen zu kommunizieren. Jedoch ist DCOM, da es bereits in den Neunzigerjahren entwickelt wurde, heutzutage angreifbar. Weshalb die OPC-Fondation eine einheitliche Datenaustauschmethode für einige Teile der existierenden OPC-Spezifikationen entwickelte. Diese sollte für Einfachheit, höchste Interoperabilität und Sicherheit sorgen. Die Foundation, zu der inzwischen mehr als 450 Unternehmen, darunter über 100 aus Deutschland, Österreich und der Schweiz gehören [28], veröffentlichte im Herbst 2006, nach drei Jahren Entwicklungsarbeit die OPC Unified Architecture. Das veraltete DCOM-Fundament wurde zugunsten einer offeneren und modularen Struktur, auf der Basis von XML-Webservices, ersetzt. Dies hat den enormen Vorteil, dass OPC UA plattformunabhängig arbeitet (siehe Abb. 7).[29]

27 Vgl. Jasperneite,Neumann, Pethig 2015, S.1f
28 Vgl. OPC Foundation 2015a, [Online]
29 Vgl. Schäfer 2015 [Online]

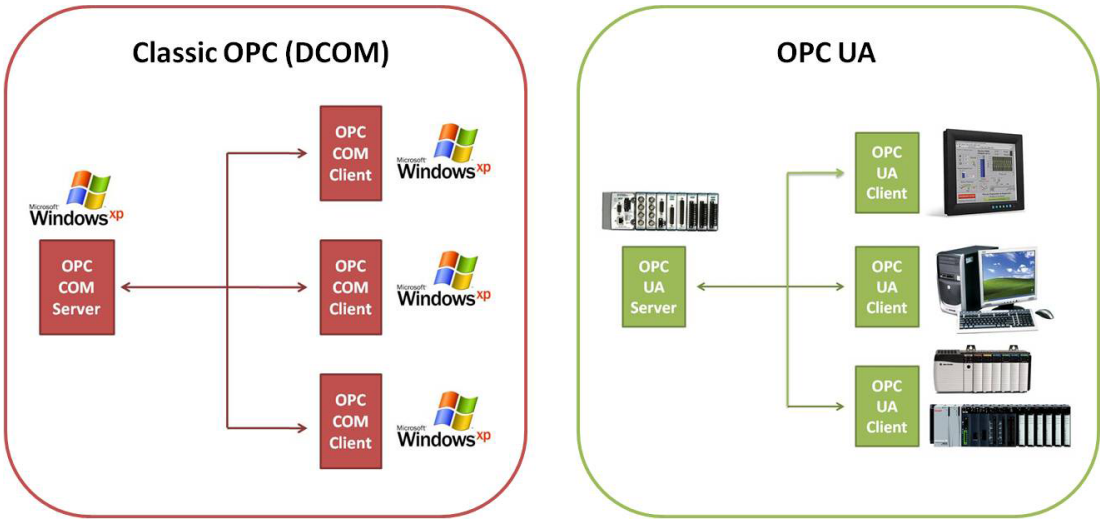

Abbildung 7: Klassisches OPC vs. plattformunabhängiges OPC UA, Quelle: http://www.ni.com/white-paper/13843/en/#

Seit der 2015 erschienenen und aktuellsten Version 1.03 sind die OPC-Standarddokumente nun freigegeben und somit nicht mehr ausschließlich den Mitgliedern der OPC-Foundation vorbehalten. Insgesamt umfasst die Spezifikation von OPC UA etwa eintausend Seiten. Dabei ist sie in dreizehn Teile untergliedert. In den Abschnitten eins bis sieben werden Übersicht und Konzept, Sicherheitsmodell, Adressraummodell, Dienste, Informationsmodell, Protokollabbildungen und Profile definiert. In den Kapiteln acht bis elf sind die Arten der Datenzugriffe definiert. Die letzten beiden Teile, zwölf und dreizehn, definieren seit der aktuellen Version 1.03 Querschnittsfunktionen, wie Discovery sowie das Zusammenfassen von historischen und gepufferten Daten mittels Aggregatfunktionen wie Mittelwert, Minimum und Maximum oder dem sogenannten „Number of Translations“. Primär basiert OPC UA auf einer Serviceorientierten Architektur, sowohl Anfragen wie auch Antworten sind in SOAP XML beschrieben. Durch die Kommunikation via TCP-Port 80 und 443, also HTTP und HTTPS, sind im Normalfall keine Änderungen an der Firewall nötig. Allerdings besteht hier die Gefahr, dass auf eine Risikoanalyse verzichtet wird. Für die Authentifizierung sind bei OPC UA grundsätzlich X-509-Zertifikate[30] vorgesehen. Abgesehen von einigen kleineren „Embeddedprofilen“, besitzen alle Zertifikate Integritäts- und Vertraulichkeitsschutz, außer ein Hersteller oder Administrator setzt den SecurityMode auf „none“ und verzichtet somit bewusst darauf. Dies wird jedoch höchstens dann vom Standard empfohlen, wenn das Netz in dem die Anwendung läuft, physisch sicher ist oder es durch ein sogenanntes „Low-

30 X.509-Zertifikat: Digitales Zertifikat auf Basis einer Public-Key-Infrastruktur.. Damit verifiziert man, dass ein öffentlicher Schlüssel zur Identität eines Anwenders, Computers oder Service gehört, die im Zertifikat hinterlegt ist.

Level-Protokoll“ wie beispielsweise IPsec[31] gesichert wird.[32] Die Foundation möchte mit OPC UA die Informationssicherheit von Anfang an integrieren, und ein sogenanntes „Security by Standard“ Prinzip schaffen. Im zweiten Teil, dem „Security Model“ liefert OPC UA ein 31-seitiges Sicherheitskonzept mit. Zudem sind neben Verfügbarkeit ebenso Integrität, Vertraulichkeit und Authentizität in den meisten Fällen die Standardeinstellung[33]. Auf der anderen Seite verlangt dieses umfangreiche Sicherheitskonzept ein hohes Maß an Arbeit seitens der Hersteller und der Betreiber sowie deren Administratoren. Die große Anzahl an Betriebsmodi erfordern jeweils unterschiedliche Anstrengungen, um die Authentisierung und die Ende-zu-Ende-Verschlüsselung zu gewährleisten. Des Weiteren nutzt OPC UA einige weitere technische Standards wie TLS, „WS-SecureConversation“ mit dessen Abhängigkeiten, insbesondere „WS-Security“, XML-Verschlüsselung und XML-Signaturen. Da ist es kaum verwunderlich, dass einige Schwachstellen im Standard auftauchen. Denn, die schon seit einigen Jahren bekannten Sicherheitsmängel dieser Verfahren, bestehen noch immer.[34] Zudem ist es nachteilig, dass die OPC Foundation ihren Standard nur etwa alle drei Jahre Updated, obwohl beispielsweise bei TLS eine ganze Reihe Sicherheitslücken bekannt sind. In der letzten Version 1.03 wurden aus diesem Grund die besonders komplexen und dadurch enorm fehleranfälligen Webservice Standards entfernt, und es wird nur noch die TLS-Version 1.2 unterstützt, wodurch die bekannten Sicherheitslecks behoben wurden.[35]

Die OPC Foundation wird, besonders mit ihrer aktuellen Version OPC UA 1.03, wegweisend für die Industrie 4.0 und somit auch für das Internet der Dinge sein. Durch die Nutzung von SOAP/XML über HTTP ist es plattformunabhängig, wodurch das Betriebssystem keine Rolle mehr spielt und es auf Windows genauso, wie auf MacOS oder Linux gleichermaßen eingesetzt werden kann. Da OPC UA imstande ist mit bereits vorhandenen Protokollen zu interagieren, ist es problemlos in bestehende Systeme zu integrieren. Der HTTP und HTTPS basierte Transport macht die Konfiguration einfach, da in der Regel große Änderungen an der Firewall ausbleiben. Zudem ist es durch die umfassende Dokumentation und eine transparente API sehr entwicklerfreundlich und durch eigene Binärprotokolle bietet es eine deutlich höhere Performance. Auch wenn die OPC Foundation nur etwa alle drei Jahre eine neue Version herausbringt, schreitet die Entwicklung doch stetig voran. Die erst im Dezember 2015 veröffentlichte Version 1.03 bringt besonders sicherheitstechnisch entscheidende Verbesserungen mit sich. Durch den Webservicestack verringert sich die

31 IPSec: Erweiterung des Internet-Protokolls (IP) um Verschlüsselungs- und Authentifizierungsmechanismen. Zum Transport von kryptografisch gesichert IP-Paketen über öffentliche unsichere Netze.

32 Vgl. OPC Foundation 2015c, S.9

33 Vgl. ebd. S.22

34 Vgl. Böck 2015, [Online]

35 Vgl. Schäfer 2015, [Online]

Komplexität deutlich, was auch die Zahl der Sicherheitslücken mindert. Zudem wurden die TLS-Versionen 1.0 und 1.1 aus dem Standard entfernt, so bleibt im HTTPS-Modus nur TLS 1.2, diese Kombination bietet ein so hohes Sicherheitsniveau, das im Vergleich dazu nur wenige Browser und Websites bieten können. Weiterhin kommen Profile mit Cipher-Suites hinzu, die „Perfect Forward Secrecy“ (PFS) mitbringen.[36] Das birgt vor allem für Internet der Dinge-Anwendungen Vorteile, bei denen auch das nachträgliche Entschlüsseln von abgefangenen Daten, Schäden verursachen könnte. Auf der funktionalen Ebene ist der OPC UA-Transportlayer von einer reinen Client-Server-Architektur mit 1:1 Verbindungen um Publisher/Subscriber-Mechanismen mit 1:n und m:n- Beziehungen ausgeweitet worden.[37] So könnten beispielsweise mit RFID-Devices, Informationen schnell an viele Empfänger verteilt werden, was in großen, dezentralen System für erhebliche Geschwindigkeitsgewinne sorgen kann. Außerdem evaluiert eine neue Task Force eine mögliche Echtzeitfähigkeit von OPC UA, diese stützt sich auf Basis der in Entwicklung befindlichen Standards der IEEE 802.1, der sogenannten TSN-TG, der Time-Sensitive Networking Task Group.[38]

2.2.2 MTConnect

Im Jahr 2006 veranstaltete die Association For Manufacturing Technology (AMT) eine Tagung verschiedener Automatisierungs- und Softwarehersteller zum Thema „Manufacturing in the Internet Age“. Dort wurde gemeinsam von der Firma Sun Microsystems und der Universität von Kalifornien in Berkeley (UCB) der erste Entwurf einer Verbindung des Maschinen- und Anlagenbaus mit dem Internet, für die moderne Produktion im einundzwanzigsten Jahrhundert, vorgestellt. Dies wurde von der AMT aufgegriffen und an einem konkreten Beispiel weitergeführt, und zwar die Überwachung von CNC-Maschinen verschiedener Hersteller über eine gemeinsame Schnittstelle.[39] Im Jahr 2008, nach der Arbeit der UCB und des Georgia Institute of Technology sowie einigem Einfluss aus der Industrie, wurde die erste Version von MTConnect released. Das gemeinnützige Tochterunternehmen der Association namens MTConnect Institute entwickelt den Standard seit 2009 stetig weiter. Über 130 Mitglieder zählt das MTConnect Institute aktuell. Darunter Großkonzerne wie General Electric, Bosch Rexroth Corporation, welches das amerikanische Bosch Tochterunternehmen ist, Cisco und sogar Unternehmen aus der Rüstungsindustrie wie Boeing, Lockheed Martin und die US Army.[40] Zwar gilt die aktuelle Version von MTConnect als „Open Source“, doch das ist nur bedingt richtig. Der Standard ist kostenlos einsehbar und nutzbar, sofern man sich registriert hat. Modifikation und Weitergabe sind jedoch nicht möglich. Ein Vorteil besteht jedoch darin, dass

36 Vgl. OPC Foundation – 2015d, S. 89
37 Vgl. OPC Foundation 2015b S.14
38 Vgl. Schäfer 2015, [Online]
39 Vgl. MTConnect Institute 2015a, S.11
40 Vgl. MTConnect Institute 2015b, [Online]

im Gegensatz zur OPC Foundation, die Mitgliedschaft im MTConnect Institute kostenlos ist. Aktuell umfasst der Standard vier Abschnitte, wobei die Teile drei und vier noch jeweils ein Unterkapitel haben. Der erste Teil „Overview and Protocol“ bietet einen Überblick über die Architektur und legt die technische Infrastruktur dar, beispielsweise die verwendeten Protokolle und Standards, die sich vorwiegend auf HTTP, XML, XML Schema und XPath belaufen.[41] Bei der Kommunikation nutzt MTConnect ein „ReSTful“[42] Webinterface mit HTTP für den Transport, speichernden URIs und zustandslosen Verbindungen. Der Standard nutzt somit das derzeit erfolgreichste moderne Interface. Bei dieser Schnittstelle sind die ausführbaren Operationen sehr begrenzt. Alle Anfragen sind ausschließlich HTTP-Requests mit einem leeren Body, denn sämtliche signifikanten Informationen werden bereits mit der URL ausgeliefert. Die Antworten sind grundsätzlich in XML-Dokumenten formuliert. Essenziell für MTConnect ist, dass ausschließlich lesende Zugriffe vorgesehen sind. Alle anderen Steuerfunktionen sind herstellerspezifisch und nicht standardisiert. Dennoch kann nicht ausgeschlossen werden, dass Anwendungen anhand erhaltener Daten, Entscheidungen treffen. Diese könnten Zustandsänderungen einer Datenbank oder der Anwendung selbst zur Folge haben. Aus diesem Grund ist die Integrität bei MTConnect weiterhin ein heikles Thema. Bei zukunftsorientierten Kommunikationsstandards sollte die Informationssicherheit oberste Priorität haben. Bei MTConnect verwundert daher, dass kein Sicherheitsmodell existiert. Grundlegende Begriffe wie Sicherheit, Integrität oder Vertraulichkeit kommen in der Spezifikation nicht vor. Ebenso die Möglichkeit auf HTTPS umzuschalten findet keinerlei Erwähnung im Standard. Konsequenterweise werden die Gefahren, welche die Verwendung von XML mit sich bringen, nicht erwähnt. In einer Roadmap, welche das Institut 2015 veröffentlichte, wird ihre Logik dahin gehend deutlicher. Denn laut MTConnect erlaube der Standard erstens nur Lesezugriffe und zweitens bedeute „Cyber Security“ für sie Netzwerksicherheit. Ergo, ist das Netz sicher in dem sich die MTConnect-Daten befinden, seien diese auch sicher.[43] Das ist für einen modernen Standard nicht zeitgemäß. Das komplette Isolieren von Netzwerken ist heutzutage sowohl in der Industrie als auch privat völlig undenkbar. Wenn MTConnect als Standard für das Internet Of Things oder das Internet Of Everything in Betracht gezogen werden möchte, sollte sein Sicherheitskonzept nicht ausschließlich auf vorhandene Netzwerksicherheit aufbauen.

Das MTConnect Institute entwickelt ihren Standard stetig weiter, jedoch wird die Sicherheit wohl auch in Zukunft keine tragende Rolle bekommen. Hauptsächlich setzt man auf Expansion. Nicht mehr nur auf Werkzeugmaschinen soll abgezielt werden, sondern auch auf diskrete

41 Vgl. MTConnect Institute – 2014, S.3-5

42 ReST: Representational State Transfer – Programmierparadigma für verteilte Systeme. Zustandslose Architektur, läuft idr. über HTTP. Zum Lesen von Web-XML-Documenten.

43 Vgl. MTConnect Institute 2015a, S.11

Fertigung im Ganzen, und einige andere Produktionsprozesse. Auch wenn es MTConnect an einem Sicherheitsmodell mangelt, so könnte der industrielle Rückhalt, den es erfährt, eine Zukunft als Standard des IoT sichern. Denn Konzerne wie AT&T, Cisco, IBM, Intel und andere, die hinter MTConnect stehen, haben im März 2014 ein Konsortium namens IIC, Industrial Internet Consortium, um eben dies voranzutreiben.[44]

2.2.3 MTConnect-OPC UA Companion Specification

Im Jahr 2010 begannen die OPC Foundation, und das MTConnect Institute zusammenzuarbeiten. Dies sollte die Interoperabilität beider Standards zum Ziel haben. Das Ergebnis dieser Zusammenarbeit war die „MTConnect-OPC UA Companion Specification“ Die erste Version erschien im November 2012, die zweite und bisher letzte Version erschien ein Jahr später, im November 2013. Bedauerlicherweise ist es hierbei bei einem „Release Candidate“ geblieben, welcher auch nicht mehr auf die aktuellsten Versionen beider Standards verweist. Bei dieser Zusammenarbeit ging es nicht darum, die Standards anzugleichen. Die Spezifikation beschreibt lediglich Datentypen und Übergabepunkte und soll so eine Koexistens beider vereinfachen.[45]

2.2.4 OPC UA vs. MTConnect

Zwar ist OPC UA technisch deutlich solider und in punkto Sicherheit klarer Spitzenreiter. Nichtsdestotrotz ist es möglich das sich der Standard durchsetzt, welcher auf Machbarkeit anstatt auf Genauigkeit und Qualität setzt. Treibende Kraft hierbei sind die großen Konzerne der Automatisierungstechnik, welche das Potenzial beider Standards erkannt haben und sicherheitshalber auf beide setzen. Dabei könnten beide Kandidaten voneinander profitieren. MTConnect kann momentan definitiv keinen Standard stellen, mit welchem sich Connected Living-Anwendungen mit sensiblen Daten sicher betreiben oder Überwachen lassen. Auf der anderen Seite ist die Komplexität von OPC UA noch viel zu enorm, was im Endeffekt nicht nur der Verbreitung im Weg steht, sondern auch der Sicherheit schadet, da zu viel beachtet werden muss. Wünschenswert wäre es, wenn OPC UA, durch seine Gründlichkeit, dass Maß der Sicherheitsanforderungen für andere Standards höher legt.

44 Vgl. IIC - INDUSTRIAL INTERNET CONSORTIUM 2015, [Online]
45 Vgl. MTConnect OPC UA Companion Specification 2013, S.13

3 Sicherheitsrisiken

So hilfreich und praktisch die genannten Technologien sind, wird gleichzeitig immer ihre IT-Sicherheit infrage gestellt. Der Datenschutz, sowie die Privatsphäre der Menschen sind ständige Themen in den Medien. Diese sollten oberste Priorität bei den Herstellern haben. Das dies aber nicht so ist, bezeugen ständig neue publik werdende Sicherheitsmängel. Einerseits entstehen diese, weil die Unternehmen oft an der Sicherheit der eigenen Produkte sparen. In die Entwicklung der Software wird zu wenig Zeit und Geld investiert oder diese werden gar gänzlich von Drittanbietern eingekauft. Da die IT-Sicherheit keinen offensichtlichen Gewinn bringt, wird sie häufig vernachlässigt, und entstandene Schäden werden erst dann und oft nur notdürftig behoben. Die „European Union Agency for Network and Information Security“[46], kurz ENISA genannt, veröffentlichte im Februar 2015 eine Studie mit dem Namen *“Threat Landscape and Good Practice Guide for Smart Home and Converged Media”*[47]. In dieser Studie wurden Sicherheitsrisiken und Probleme bei Smart Homes untersucht und erforderliche Gegenmaßnahmen vorgestellt. Als größtes Sicherheitsrisiko werden dabei Cyberkriminelle beziehungsweise „Hacker“, welche sich die Sicherheitslücken der Smart-Objekte zu nutze machen, eingestuft. Ebenso wird angenommen, dass der Missbrauch der intelligenten Geräte, aufgrund ihrer stetig steigenden Zahl, proportional zunehmen wird.[48] Eine der Hauptbedrohungen für die Nutzer ist laut ENISA das Abgreifen und Weitergeben persönlicher Informationen, da Smart-Home-Geräte einen Großteil dieser Daten verarbeiten. Hauptsächlich die enorme Anzahl an smarter Unterhaltungselektronik und intelligenten Haushaltsgeräten ist laut der Studie ein Problem. Diese sind beispielsweise in der Lage die Gewohnheiten, Gesundheit, das Konsumverhalten oder die An- beziehungsweise Abwesenheit der Nutzer nachzuverfolgen. Die sogenannten integrierten Medien, zu denen hauptsächlich Smart TVs, der Google Chromecast- und der Amazon Fire-Stick, Spielkonsolen und Settopboxen wie Receiver oder DVD- und BluRay-Player gehören, erhöhen im Hinblick auf Datenschutz und Privatsphäre das Sicherheitsrisiko, da es sich um sogenannte „undurchsichtige Systeme“ handelt, welche beispielsweise Fernsehgewohnheiten aufzeichnen und an den Hersteller weiterleiten könnten. Diese Art der Datenweitergabe kam bereits vor. Der Technikhersteller Samsung machte Anfang 2015 auf seiner Website bekannt, dass bei seinen Smart-TVs die Fernseh- und Nutzungsgewohnheiten, Hardware- und Browserdaten und wenn die Sprachsteuerung nicht deaktiviert ist, sogar Sprachdaten übermittelt werden.[49]
Schon im Jahr 2013 kam es beim Technikkonzern LG zum Skandal, da seine

46 dt. Europäische Agentur für Netz-und Informationssicherheit
47 dt. Bedrohungslandschaft und Anleitung zum richtigen Umgang mit Smart Homes und integrierten Medien
48 Vgl. European Union Agency for Network and Information Security 2015, S.36
49 Vgl. ebd. S.20

smarten Fernsehgeräte die Sehgewohnheiten der Nutzer an den Hersteller sendeten. In Deutschland wurden unter anderem der gewählte Fernsehsender, die TV-Plattform und die Sendequelle mitgeteilt. Die Geräte besaßen zwar eine Funktion, die ungewollte Datenerhebung zu deaktivieren, diese war allerdings wirkungslos. LG konnte den Fehler erst mit einem Firmwareupdate beheben, mit dem dann bei deaktivierter Funktion auch tatsächlich keine Daten der Besitzer mehr an den Hersteller übermittelt wurden.[50]
Laut der Studie ist die meist zentrale Lage der Geräte in den Räumen ein verstärkender Faktor, denn diese erlaube es die im Zimmer stattfindenden Aktivitäten zu überwachen und aufzuzeichnen und diese dann letztendlich an Dritte zu übermitteln. Da diese Art der Geräte in der Regel als erste Smart-Objekte in einen Haushalt integriert wird, sind sie laut ENISA die Hauptursache der meisten identifizieren Sicherheitslücken.[51]

3.1 Sicherheitslücken in der Firmware

Die Kosten der intelligenten Geräte soll möglichst gering sein. So werden sie millionenfach in Serie produziert und müssen mit einer Firmware versehen werden. Ist diese bereits fehlerhaft, sind schon ab Werk Millionen Geräte fehlerhaft. Ein Beispiel dafür brachte Anfang 2014 die Firma Belkin hervor.
In der Firmware der Geräteserie Wemo war ein Schlüssel implementiert worden, welcher über eine serielle Schnittstelle ausgelesen werden konnte. Da derlei Keys nicht für jedes Gerät individuell vergeben, sondern meist für eine ganze Gerätereihe genutzt werden, hätte der Key nur auf einem Gerät ausgelesen werden müssen, um die ganze Reihe angreifen zu können. Das Unternehmen behob das Problem mit einem Firmwareupdate, welches SSL-Verschlüsselung und Verifizierung hinzufügte. Damit machte Belkin den vorhandenen Schlüssel überflüssig. Zudem wurde die serielle Schnittstelle mit einer Passwortabfrage gesichert.[52] Leider handeln nicht alle Hersteller so zügig auf derartige Probleme und solche Sicherheitslücken bleiben eine lange Zeit bestehen.
Ein herstellerunabhängiges Problem stellen Router dar. Da sie das Bindeglied zwischen dem heimischen Netzwerk und dem World Wide Web, und ebenso die Tür in das Smart Home sind. Gerade deshalb sollte bei einem Router die Sicherheit an erster Stelle stehen. Doch wie, die bereits erwähnte, Studie der Firma Fortinet aus dem Jahr 2014 hervorbrachte, sind bei Routern eine fehlerhafte Firmware oder versteckte Passwörter keine Seltenheit. Bei einigen 2013 und 2014 entdeckten Sicherheitslecks in Routern, unterschiedlicher Hersteller, wurde festgestellt, dass es für derlei Geräte nicht genügend oder gar keinen Sicherheitssupport mehr gibt oder die User sich wenigstens im Router einloggen müssten, um diesen zu aktualisieren. Der Großteil der Nutzer wartet den Router nach der Einrichtung

50 Vgl. ebd. S.7
51 Vgl. ebd. S.1
52 Vgl. Burns 2014, [Online]

nicht mehr, da sie entweder der Meinung sind, dass dies nicht notwendig ist oder da sie mangels technischem Know-how nicht wissen wie oder angst haben ihr funktionierendes System zu schädigen. Hinzu kommt, dass einige Hersteller beim Entwickeln von Firmwareupdates, um die Sicherheitslücken zu schließen, sehr viel Zeit benötigen.[53] Des Weiteren wurden in einigen Geräten versteckte Root-Zugänge gefunden, und durch die Manipulation der Router-URL konnte Zugang Provider-Support-Seite bekommen und sehen, was ein Supportmitarbeiter im Netzwerk sehen kann[54]. Im Rahmen der Studie fand eine Umfrage zum Thema Sicherheit statt. Von den, in Deutschland befragten, waren 43 Prozent der Meinung, dass Router gegen Attacken immun oder wenigstens eine eigene Art von Schutz besitzen sollten. Demgegenüber sind circa ebenso viele der Befragten der Ansicht, der Internetanbieter habe die Sicherheit zu gewährleisten. Womit hier die Frage bleibt, wie dies, ohne Zugriff auf die Geräte möglich sein soll. Laut der Umfrage sind 40 Prozent der Befragten bereit für neue WLAN-Router, welche für das Verbinden mit smarten Geräten ausgelegt sind, extra zu bezahlen. Sogar 49 Prozent der Befragten sind bereit mehr Geld für Internetdienste zu bezahlen, um sicherzustellen, dass die intelligenten Haushaltsgeräte und das Netzwerk ordnungsgemäß und sicher funktionieren.[55]

3.2 Unzureichende Passwörter

Ein ähnliches Problem, wie mit dem Schlüssel der in der Firmware abgelegt ist, verhält es sich wenn Standardpasswörter auf den Geräten hinterlegt sind. Diese können meist auch ohne größere Mühe ausfindig gemacht werden. Einem Forscherteam der Universität Institut Eurécom ist es gelungen, auf mehr als 100.000 Geräten SSH-Schlüssel und Zugangsdaten für die Administration zu finden. Auf mehr als 2000 Geräten wurden im Code hinterlegte Telnet-Zugänge gefunden. In über 600 weiteren wurden in Verzeichnissen abgelegte Passwort-Hashes[56] ausfindig gemacht, von denen sie circa 10 Prozent der Passwörter auslesen konnten. Teilweise waren die Passwörter solche einfachen wie „pass“, „admin“, „12345“ oder sie waren gar nicht erst vorhanden. Die Forscher kamen zu der Erkenntnis, dass ein Großteil der Lecks von einer gemeinsamen Ursache stammt. So könnten Softwarehersteller, die ihre Software an mehrere Hardwareproduzenten lizenzieren, die Lecks selbst, durch eine fehlerhafte SDK oder Ähnliches, einbringen. Denn das Forscherteam entdeckte häufig die gleichen Sicherheitslücken bei Geräten unterschiedlicher Hersteller.[57] Dadurch würden durch einen einzigen bekannten Bug Gerätereihen mehrerer Hersteller

53 Vgl. Fortinet – 2014, S.1
54 Vgl. Jacoby 2014, [Online]
55 Vgl. Fortinet 2014, S.2
56 Hashfunktion: kryptografische Prüfsumme für eine Nachricht, um deren Integrität sicherzustellen. Dient der Reduzierung des Rechenaufwands bei der Verschlüsselung von Daten im Public-Key-Verfahren
57 Vgl. Pauli 2014, [Online]

angreifbar.
Es beginnt jedoch bereits bei viel einfacheren Dingen, wie der Passwortvergabe durch den Nutzer. Bei einer Studie der Firma HP aus dem Jahr 2014 fand man heraus, dass achtzig Prozent der getesteten Geräte den Benutzer nicht auffordern einen komplexen Zugriffscode zu wählen.[58] Ist das Passwort zu einfach oder gar nicht vorhanden, nützen die besten Sicherheitsmaßnahmen nichts.

3.3 Sicherheitslücken bei Protokollen

Jeder Übertragungsstandard nutzt zur Kommunikation Protokolle. Die Daten stehen in den Protokollen und diese werden bestenfalls vom Sender verschlüsselt und vom Empfänger entschlüsselt.
Bei Bluetoothgeräten ist zwar die 128 Bit AES-Verschlüsselung vorgesehen, diese wird aber nicht immer angewendet, denn Verschlüsselung wirkt sich immer auf den Akku der Geräte und damit auf die Arbeitszeit aus. Zudem ist die Verschlüsselung abhängig davon, wie lang der verwendete PIN ist. Ein PIN kann bis zu 16-stellig sein, dies kommt aus Komfortgründen jedoch selten vor. Mit geeigneten Tools und unter Anwendung von Bruteforce[59] lassen sich PINs mit bis zu acht Stellen relativ problemlos herausfinden. Des weiteren ist ein 128 Bit langer Schlüssel bei Bluetooth, nur bei der Authentisierung bindend. Bei der Codierung der Datenpakete kann die Schlüssellänge zwischen acht und 128 Bit variieren.[60]
Eine weitere Schwachstelle in den Protokollen tut sich bei der Authentifizierung auf. Bei ZigBee ist ein Masterkey notwendig um Geräte im Netz zu authentifizieren, dieser ist ebenfalls häufig in der Firmware abgelegt. Zudem ist Tracking möglich, da bei der Kommunikation der ZigBee Geräte die Mac-Adressen übertragen werden. Ein Weiterer Sicherheitsmängel beim ZigBee-Protokoll wird durch den sogenannten Fallback Key hervorgerufen. Ein asymmetrisches Schlüsselpaar, welches öffentlich bekannt ist und von den Geräten erkannt und akzeptiert werden muss. Normalerweise kommt im ZigBee Home Automation Netz der symmetrische Network Key zum Einsatz, welchen sich die Geräte teilen. Wird ein neues Gerät angeschlossen, fragt dieses nach dem Network Key, den es daraufhin erhält. Zwar wird die Schlüsselübergabe codiert, jedoch mit dem öffentlichen Fallback Key. Das bedeutet, wenn die Schlüsselübergabe von Angreifern mitgelesen wird, können diese sie entschlüsseln und den Network Key bekommen. Hat ein Angreifer den Network Key, kann er die ganze Kommunikation im gesamten ZigBee Netz sehen oder eigene Befehle einspeisen.[61] Die Energieeffizienz wird den ZigBee-Geräten hierbei zum Verhängnis, da man keine Einstellungen an ihnen vornehmen kann. Ebenso fehlt es ihnen an einer

58 Vgl. Hewlett Packard Enterprise 2015, S. 4
59 Gewaltsamer Angriff auf Kryptografischen Algorithmus. Verfahren probiert systematisch alle möglichen Kombinationen durch um Krypto-Algorithus zu knacken. Sehr Zeitaufwendig.
60 Vgl. Bundesamt für Sicherheit in der Informationstechnik 2011, [Online]
61 Vgl. Zillner 2015, S. 3

Benutzeroberfläche, weshalb Firmwareupdates meist nicht möglich sind. Allerdings wäre ein Firmwareupdate auch nur Sinnvoll, wenn die Authentifizierung und die Verschlüsselung verbessert würden.
Dazu kommt, dass ein gezielter Angriff jederzeit erfolgen kann. So kann dem ZigBee Netz vorgegaukelt werden, dass sich ein Gerät, nach einer Abwesenheit, neu verbinden möchte. Oder der Funk auf den ZigBee Frequenzen wird gestört, sodass sich alle Geräte neu einwählen müssen. Die ZigBee Alliance arbeitet derzeit an einer neuen Version der Home Automation. In dieser sollen die Sicherheitslücken behoben werden. Das ist für bereits gekaufte und installierte Hardware aber keine Lösung, da es eben nicht möglich ist Firmwareupdates einzuspielen. Das bedeutet, die einzige Alternative um ein ZigBee-Netz in Zukunft abzusichern, ist die vorhandenen Geräte zu ersetzen.
Ein weiterer Nachteil ist, dass es in der Smart Home Technologie eine Vielzahl an Geräten mit unterschiedlichen Protokollen und Technologien gibt, welche zu den älteren und herkömmlichen Sicherheitssystemen in den Haushalten nicht kompatibel sind.[62] Des Weiteren besitzen viele Smartobjekte noch nicht die notwendige Rechenleistung, um eine Endpunktauthentifizierung oder Verschlüsselungsalgorithmen zu unterstützen. Deshalb sind diese äußerst anfällig für Sniffing-[63] oder Man-in-the-Middle-Angriffe[64] (siehe Abb. 8), welche bei ZigBee und Z-Wave-Protokollen bereits erfolgreich nachgewiesen worden. Ebenfalls kann ein Hacker sich mithilfe des sogenannten Wardriving[65] in Reichweite des Smart Homes bringen, und sich dadurch in die Funkkommunikation der Geräte belauschen. Gemäß der Studie der ENISA genüge die Reichweite der Smartobjekte und Protokolle für derlei Attacken[66]. Mit dieser Vorgehensweise könnten Angreifer in der Lage sein beispielsweise das Licht oder den Kühlschrank im Smart Home ein- und auszuschalten, das Drahtlosnetzwerk oder gar eine unsichere Gebäudeautomation ausfindig zu machen.

62 Vgl. European Union Agency for Network and Information Security 2015, S. 15
63 dt. schnüffeln – Mittels Software den Datenverkehr von Netzwerken auf Schwachstellen überprüfen.
64 dt. Mittelsmannangriff: Angriffsform bei Rechnernetzen. Angreifer befindet sich physikalisch oder logisch zwischen Kommunikationspartnern. Hat dabei vollständige Kontrolle über Datenverkehr zwischen Netzwerkteilnehmern.
65 Systematische Suche nach Funknetzwerken mithilfe eines Fahrzeugs.
66 Vgl. European Union Agency for Network and Information Security 2015, S. 22

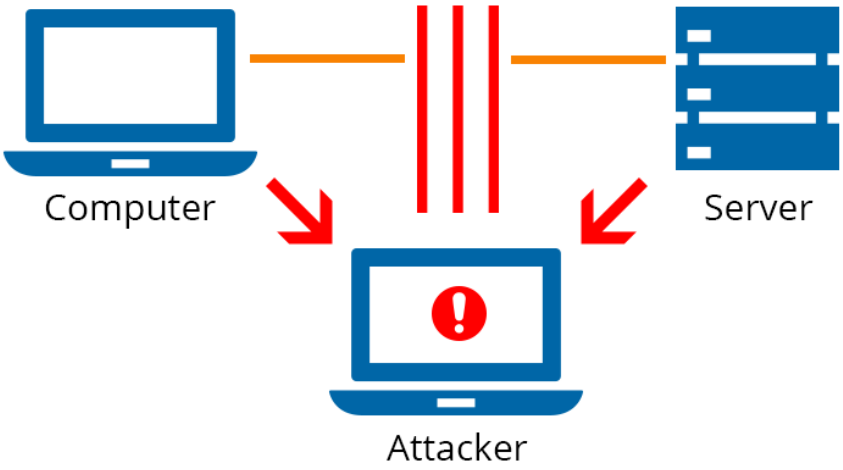

Abbildung 8: Darstellung eines Man-in-the-Middle-Angriffs, Quelle:https://sfletter.com/?_lng=en&_action=blog-08-12-2014

Weitere Probleme bringt Universal Plug and Play mit sich. Da es schon seit einigen Jahren ein wichtiger Bestandteil von Netzwerken weltweit ist und nicht für das Connected Living neu entwickelt wurde, sind bereits eine ganze Reihe Sicherheitslecks bekannt geworden. Diese, sofern sie noch existieren, können bei einem Smart Home große Risiken darstellen, und es leichter angreifbar machen. Im Jahr 2013 haben Sicherheitsexperten der Firma Rapid7 etliche Lücken in UPnP Geräten aufgespürt. Über diese sind mittels Netzwerk verbundene Geräte, wie PCs, Netzwerkspeicher, Drucker etc. verwundbar. Betroffen sollen zu diesem Zeitpunkt, global, circa 40 bis 50 Millionen Geräte gewesen sein. Da es sich bei Universal Plug and Play um eine Auswahl unterschiedlicher Netzwerkprotokolle handelt, welche es ermöglichen, das netzwerkfähige Geräte und Accesspoints sich gegenseitig identifizieren, untereinander verständigen und sogar auf das Internet zugreifen können, macht es das dementsprechend anfällig für Angriffe von außerhalb. Angreifbar macht es zum einen das SSDP, welches es ermöglicht Geräte im Netzwerk zu lokalisieren. Dieses kann dazu zweckentfremdet werden, einen Dienst abstürzen zu lassen oder Schadcode einzuschmuggeln und auszuführen.[67] Weiterhin wurden Schwachstellen beim SOAP und UPnP HTTP ausgemacht. Aufgrund einer fehlerhaften Konfiguration des SSDP wurden weltweit über 81 Millionen eindeutige IP-Adressen gefunden, welche via Internet, über eine UPnP-Anfrage erreichbar waren.[68] Zudem gelang es mittels des SOAP in ein paar Fällen auf Funktionen zuzugreifen, die das Öffnen von Ports in der Firewall ermöglichten. Dazu sind die zwei meistgenutzten Universal Plug and Play Softwarebibliotheken unsicher. Bei der Portable UPnP SDK sind durch ein einzelnes UDP-Paket über 23

67 Vgl. Moore 2013, S.13f
68 Vgl. ebd. S.8

Millionen IP-Adressen empfänglich für eine Remote-Code-Ausführung[69]. Dieses Problem wurde zwar erfolgreich mit einem Patch behoben, doch obliegt es hier dem Besitzer, ein Update durchzuführen. Dies hat zur Folge, dass viele der gefährdeten UPnP-Geräte weiterhin vulnerabel bleiben. Außerdem ist davon auszugehen, dass jene Geräte die nicht mehr auf dem Markt sind, keine Updates mehr erhalten. In diesem Fall ist der einzige Weg um die Sicherheit zu gewährleisten, UPnP am betreffenden Gerät zu deaktivieren. Es wurden noch über 330 Gerätetypen gefunden, welche eine veraltete Version der MiniUPnP-Software nutzten[70]. Es wird davon ausgegangen, dass mehr als 6900 Geräte von etwa 1500 Herstellern mindestens eine dieser Schwachstellen aufweisen. Angreifer können sich mithilfe dieser Sicherheitslücken Zugriff auf das System verschaffen und so beispielsweise Passwörter ausspähen oder Netzwerkdrucker und Webcams kontrollieren.[71]
Möchte der Nutzer Unterhaltungselektronik in sein heimisches Netzwerk einbinden, kommt man um Universal Plug and Play kaum herum. Zwar ist es möglich UPnP in einem Gerät zu deaktivieren, doch geht dann der Komfort und die Idee des Internet der Dinge verloren. De facto wird es bei UPnP wohl immer Sicherheitslücken geben, da die Geräte kaum eigene Schutzmaßnahmen mitbringen. Doch durch permanente Aufdeckung von Sicherheitslecks und die, zumindest bei neueren Geräten relativ häufigen Updates, werden ständig Sicherheitslücken behoben. Sollten die Endnutzer ihre Geräte jedoch nicht updaten, ist ein akkurater Schutz, gegen Angriffe von außen, keinesfalls gegeben.

3.4 Angriffe aus dem World Wide Web

Früher war nur der PC das Angriffsziel von Hackern. Doch im Internet der Dinge, wo viel mehr Geräte eine Schnittstelle zum Internet bieten, ist die Angriffsfläche dementsprechend größer. Deshalb ist es Angreifern unter Umständen möglich, über das Web, in das intelligente Heim einzudringen. Eine Kernfunktionalität der Smart Homes ist der externe Zugriff und die Steuerung über das Internet via Smartphone oder per Webbrowser vom Computer aus. Das bedeutet, dass nicht nur die Kommunikation innerhalb eines Smart Home Netzes sicher, das heißt verschlüsselt und mit Authentifizierung, ablaufen sollte, sondern auch nach außerhalb, wenn über das Web mit dem Smart Home kommuniziert wird. Sicherheitsexperten der Firma AV-Test, testeten 2014, sieben Smart Home Kits der Firmen eSaver, EUROiSTYLE, Gigaset, REV Ritter, Hama, RWE und der Telekom. Den Sicherheitsanforderungen hielten nur die drei Smart Home Lösungen von Gigaset, RWE und der Telekom stand. Es wurde unter anderem die Sicherheit der Fernsteuerung und dementsprechend der Schutz gegen Fernmanipulation getestet. Wobei die Kandidaten von eSaver und Hama

69 Vgl. Moore 2013, S.1, 9
70 Vgl. ebd. S. 9
71 Vgl. ebd. S. 1

durchfielen, da sie unverschlüsselt kommunizierten. Die Lösung von eSaver verlangte keine Authentifizierung beim Webzugriff. Verbindet sich ein solches Smartobjekt mit dem Web, kann das private Netzwerk ohne Weiteres gehackt und belauscht werden. Haben Angreifer einmal einen Zugang zum Heimnetz gefunden, kann dieser genutzt werden, um Viren und Trojaner einzuschleusen. Und diese können sich nicht mehr nur auf dem Computer verstecken, wo sie mit einer geeigneten Software noch gefunden und beseitigt werden könnten, sondern in jedem anderen Smart Device im Netzwerk.[72]
Weitere Beispiele für die Angreifbarkeit von Smart Homes aus dem Internet wurden bei der Sicherheitskonferenz Black Hat in Las Vegas gezeigt. So wurden bei einer Vorführung Smart TVs gehackt, wobei auf die integrierte Kamera und die gespeicherten Nutzerdaten zugegriffen wurde[73].
Einer Journalistin ist es gelungen mithilfe einer Suchmaschine, acht Smart Homes zu identifizieren und Daten abzugreifen[74]. Das bedeutet, dass es teilweise so einfach ist einen Cyberangriff durchzuführen, dass dies auch ein Laie tun kann.
Wie zahlreich und gefährlich die Bedrohungen aus dem World Wide Web sind, zeigt eine interaktive Weltkarte von Kaspersky Lab. Diese registriert in Echtzeit alle Bedrohungen weltweit (siehe Abb. 9).

Abbildung 9: Kaspersky Echtzeitkarte der Cyberbedrohungen, Quelle: https://cybermap.kaspersky.com/

Die unterschiedlichen Bedrohungen sind in verschiedenen Farben dargestellt. Diese sind in acht Kategorien eingeteilt. Grün zeigt die bei einem

72 Vgl. Schiefer, Lösche, Morgenstern 2014, S.2-4
73 Vgl. Lee 2013, [Online]
74 Vgl. ebd. [Online]

System Scan „on-access“, also der Echtzeitfund des Anti-Virus-Programms, gefundenen Bedrohungen. Rot den „on-demand“, also den Virenfund bei einem vom Nutzer manuell ausgeführtem Virenscan. Blau zeigt bösartige Websites und Webobjekte, Orange sind mit Malware behaftete E-Mails. Pink zeigt Netzwerke die durch versteckte Bedrohungen in IP-, TCP- und UDP-Paketen attackiert worden. Gelb stellt Funde einer Schwachstellenanalyse dar. Lila werden Spammails und türkis Botnetze angezeigt. Außerdem zeigen die Statistiken die meist-attackierten Länder, bei denen Deutschland häufig unter den Top fünf ist, mit täglich über 700000 bis 800000 identifizierten Infektionen, Tendenz steigend.[75] Der Nutzer muss sich daher bewusst sein, dass jeder Computer der am Internet angeschlossen ist, angegriffen werden kann und das gilt ebenso für jedes andere internetfähige Gerät. Da diese Art der Angriffe das größte Risiko für Smart Homes Netze und IoT-Geräte darstellen, sollte dieses Thema höchste Priorität bei den Herstellern haben.[76]

75 Vgl. Kaspersky Cybermap 2016, [Online]
76 Vgl. European Union Agency for Network and Information Security 2015, S.36

4 Fazit

Die bei Smart Home Geräten in der Vergangenheit aufgedeckten Schwachstellen zeigen, dass Hersteller häufig auf derartige Probleme zu langsam reagieren und diese in zu geringem Maße ernst nehmen. Lösen lassen sich diese Probleme durch offene Standards und durch die Arbeit unabhängiger Sicherheitsexperten. Die Zeiten, in denen einzig der Computer einen Angriffspunkt für Hacker bot, sind vorbei. Potenzielle Schwachstellen bieten nun allerhand Geräte in einem Haushalt. Insbesondere die Hersteller dieser Geräte dürfen das nicht außer Acht lassen und Sicherheitseinstellungen ab Werk aktivieren. Denn viele Endnutzer sind sich nicht im Klaren, wie es um die Sicherheit im eigenen Netzwerk steht.
Ein Punkt, unter dem zwar nicht unbedingt die Sicherheit aber definitiv der Komfort und die Nerven der Kunden leiden müssen, sind die große Zahl an unterschiedlichen Übertragungsstandards. Egal ob offener Standard oder proprietäres System, sie sind nicht interoperabel. Das bedeutet, dass Geräte die auf unterschiedlichen Standards basieren, nicht untereinander Kommunizieren können. Soll ein Smart Home möglichst viele Geräte und unterschiedliche Funktionen haben, sind die offenen Standards besser geeignet, da an diesen, bis zu mehreren Hundert Hersteller beteiligt sind, und Geräte dafür vermarkten. Doch auch wenn die Geräte auf denselben Standards aufbauen, so gibt es herstellerspezifische Eigenheiten. So kam es beispielsweise vor das ein auf ZigBee Basierendes Smart Home-Kit, andere auf ZigBee basierende Geräte anderer Hersteller nicht ins Netz integrieren konnte.[77] Oder nur sehr umständlich, ohne letztendlich korrekt zu funktionieren. Ähnlich wie bei einer Universalfernbedienung, die funktioniert, aber nicht so gut wie die zum Gerät zugehörige Fernbedienung. Proprietäre Systeme sind nicht in dem Maße erweiterbar, wie es bei offenen der Fall ist, doch bietet ein Hersteller alle gewünschten Komponenten, kann sich der Nutzer bedenkenlos dafür entscheiden. Denn sie bieten den Vorteil, dass die Geräte bereits aufeinander abgestimmt sind und die Einrichtung in der Regel leichter fällt, als bei einem offenen System mit mehreren Herstellern. Dazu können potenzielle Angreifer keine Schwachstellen aus der technischen Spezifikation herauslesen, da diese nicht öffentlich zugänglich sind. Zudem werden viel verkaufte Smart Home Geräte ständigen Tests von fachkundigen Stellen unterzogen. Wird eine Sicherheitslücke entdeckt, sind die Anbieter der Hardware meist recht schnell mit einem Firmwareupdate zur Stelle, welches die Lücke schließt. Dieser ständige Prozess erhöht stetig und dauerhaft die Sicherheit der Smart Home Lösungen. Außerdem empfiehlt auch die ENISA, für einen sicheren und erfolgreichen Umgang im Bereich der protokollgesteuerten und drahtlos kommunizierenden Smart Home Geräte, ein vollständiges und zusammengehöriges Smart Home System und eine genaue Überwachung der Sicherheit bei Cloud basierten

77 Vgl. qivicon 2014, [Online]

Smartobjekten.[78] Da die verschiedenen Standards wohl niemals vollständige Interoperabilität bieten und immer nur nebeneinander existieren werden, sollten sich Endverbraucher vor dem Kauf bewusst sein, was das eigene Smart Home können muss.
In Bezug auf die Sicherheit, die ein Smart Home in Sachen Einbruchschutz leisten soll, kann festhalten, dass die meisten Einbrecher nicht das technische Know-how besitzen, um aus der Ferne die Eingangstür zu öffnen. Außerdem muss sich der Angreifer in Nähe des Smart Home-Netzes befinden, da die Reichweite der Netze begrenzt ist. Auf den Frequenzen der Smartobjekte arbeiten noch allerhand andere Geräte wie Autofernbedienungen, Mikrowellen oder Ampelanlagen. Die entsprechenden Geräte müssen somit erst heraus gefiltert werden. Hat man es dann auch noch auf ein Bestimmtes abgesehen, wie zum Beispiel das Türschloss, muss man auch noch abwarten, bis dieses ein Signal sendet. Diese Faktoren bewirken das ein gezielter Angriff auf ein Smart Home, mehrere Stunden der Vorarbeit in unmittelbarer Nähe zum Objekt erfordern. Das dürfte wohl im Großteil der Fälle zu auffällig und Aufwendig sein. Die größte Bedrohung für die neuen Technologien stellen auch weiterhin Cyberangriffe dar. Hacker, Viren und Trojaner sind sind so Zahlreich wie nie zuvor[79]. Die Gerätehersteller und Anbieter von Sicherheitssoftware arbeiten stetig daran, die Vorkehrungen gegen derlei Attacken zu verbessern. Jedoch beweisen die Zahlen der identifizierten Bedrohungen, dass es keinen 100-prozentigen Schutz gibt und wohl auch nie geben wird. Jedoch ist das die gleiche Art der Bedrohungen die schon seit Jahren existiert und Hand in Hand mit dem Internet und der Computertechnologie geht. Und da die Computerbranche die erfolgreichste und am schnellsten Wachsende ist, kann davon ausgegangen werden, dass die Endverbraucher gewisse Risiken in Kauf nehmen. Außerdem wird es nicht möglich sein, dem Internet der Dinge völlig aus dem Weg zu gehen. Auf die Vorteile und den Komfort, den diese Technologien bieten werden viele gar nicht verzichten wollen. Es sollte sich jeder über die Risiken bewusst sein und es liegt beim Nutzer wie sicher das eigene Smart Home ist. Wie die zuvor angeführte Umfrage des Sicherheitsanbieters Fortinet ergab, sind einem Großteil der Nutzer diese Risiken bekannt. So sind Hausbesitzer an der Technologie interessiert und erwarten eine rasche Entwicklung in den nächsten Jahren, dennoch sind sie was Datenschutz, Sicherheit und Preis angeht, eher skeptisch.[80]
Um diese Sicherheitsrisiken in Zukunft auszumerzen, arbeitet in Deutschland eine Allianz verschiedener Unternehmen und Vereine, an dem "Smart Home Ready"-Siegel, welches jene sicheren und zuverlässigen Lösungen kennzeichnen soll.[81] Ebenso arbeitet ein Normungsausschuss, des Verbands der Elektrotechnik, Elektrik und Informationstechnik, kurz VDE, an den technischen Grundlagen. Dabei liegt das Hauptaugenmerk auf sicheren

78 Vgl. European Union Agency for Network and Information Security 2015, S. 46
79 Vgl. Kaspersky Cybermap 2016, [Online]
80 Vgl. Fortinet 2014, S.1
81 Vgl. Smart Home Zertifizierungsprogramm [Online]

Übertragungsbrücken, den Gateways. Denn in einem Smart Home, ist ein grundlegendes Problem, dass verschiedene Technologien, verschiedener Anbieter zum Einsatz kommen. Deshalb ist eine gemeinsame Plattform, welche mit Open-Source-Protokollen arbeitet, sinnvoll.
Die weitere Entwicklung bleibt für Experten und Laien ebenso spannend wie bedeutend für das zukünftige vernetzte Leben zwischen Mensch und Technik.

5 Literaturverzeichnis

Andelfinger, Volker P.: Internet der Dinge - Technik, Trends und Geschäftsmodelle. Springer Gabler: Wiesbasen, 2015. S. 21

Bluetooth SIG: www.bluetooth.com - Bluetooth Low Energy. 2016. URL: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy (11.02.2016)

Bundesamt für Sicherheit in der Informationstechnik: www.bsi.bund.de – G 4.80 Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen. 2011. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04080.html (16.02.2016)

Burns, Matt: www.techcrunch.com - Belkin Fixes WeMo Vulnerabilities With Firmware Update. 2014. URL: http://techcrunch.com/2014/02/19/belkin-fixes-wemo-vulnerabilities-with-firmware-update/ (18.12.2015)

Böck, Hanno: www.golem.de - XML- Verschlüsselung mit vielen Fallstricken. 2015. URL: http://wwConnected Livingw.golem.de/news/sicherheitsluecken-xml-verschluesselung-mit-vielen-fallstricken-1511-117471.html (19.12.2015)

Connected Living e.V.: www.connected-living.org – Vision Vernetztes Leben. 2015. URL: http://www.connected-living.org/mission (14.12.2015)

EnOcean: www.enocean.com – Funktechnologie. 2016 URL: https://www.enocean.com/de/technology/radio-technology/ (12.02.2016)

eQ-3: www.eq-3.de - Stimmt es, dass die Verschlüsselung des HomeMatic Systems nicht sicher ist bzw. das System gehackt wurde? Wie kann ich mein HomeMatic System vor Angriffen schützen?. 2016a. URL: http://www.eq-3.de/service/faq.html?id=156 (11.02.2016)

eQ-3: www.eq-3.de - Wie sicher ist Homematic IP? Kann es von außen gehackt werden?. 2016b URL: http://www.eq-3.de/service/faq.html?id=189 (11.02.2016)

European Union Agency for Network and Information Security: www.enisa.europa.eu - Threat Landscape for Smart Home and Media Convergence. 2015. URL: https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence (Download 15.12.2015) S. 1, 7,15, 20, 22, 36, 46

Fortinet: www.fortinet.com - Fortinet Reveals “Internet of Things: Connected Home” Survey Results. 2014. URL: http://www.fortinet.com/press_releases/2014/internet-of-things.html (download 18.12.2015) S. 1-3

Gascón, David: www.libelium.com - Security in 802.15.4 and ZigBee networks. 2009. URL: http://www.libelium.com/security-802-15-4-zigbee/ (11.02.2016)

Hewlett Packard Enterprise: www.hp.com - Internet of things research study. 2015. URL: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf (16.12.2015) S.4

INDUSTRIAL INTERNET CONSORTIUM: www.iiconsortium.org - About Us. 2015. URL: http://www.iiconsortium.org/about-us.htm (21.12.2015)

ITWissen: www.itwissen.info – IoT Internet der Dinge. 2015. URL: http://www.itwissen.info/definition/lexikon/Internet-of-things-IoT-Internet-der-Dinge.html (14.12.2015)

Jacoby, David: www.securelist.com - IoT: How I hacked my home. 2014. URL: https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/ (18.12.2015)

Jasperneite, Jürgen; Neumann, Arne; Pethig, Florian: OPC UA versus MTConnect. Hochschule Ostwestfalen-Lippe. 2015. URL: https://www.hs-owl.de/init/uploads/tx_initdb/204_gh_Jasperneite_CA_SH_2015-02_lowres_pdf_01.pdf (19.12.2015) S.1-2

Kaspersky Cybermap: www.cybermap.kaspersky.com – Statistics. 2016. URL: https://cybermap.kaspersky.com/stats/ (12.03.2016)

KNX Impuls: www.knx.de - KNX-Installation: Sicherheit optimieren. 2015 URL: http://www.knx.de/knx-de/medien-service/newsletter/archiv-pdf/KNX_Impuls_Ausgabe_25.pdf (13.02.2016) S. 1-2

König, Rudolf: www.fhemwiki.de – Z-Wave. 2016. URL: http://www.fhemwiki.de/wiki/Z-Wave (16.02.2016)

Lee, SeungJin: www.blackhat.com - Hacking, Survelling, and Deceiving Victims on Smart TV. 2013. URL: https://www.blackhat.com/us-13/archives.html#Lee (12.03.2016)

Moore, HD: www.community.rapid7.com - Security Flaws in Universal Plug and Play Unplug. Don’t Play. 2013. URL: https://community.rapid7.com/docs/DOC-2150 (Download 20.02.2016) S. 1, 8, 9, 13, 14

MTConnect Institute: www.mtconnect.org - Key Findings from the MTConnect Strategic Roadmap. 2015a. URL: http://static1.squarespace.com/static/54011775e4b0bc1fe0fb8494/t/555508cbe4b0a3ac76e50aba/1431636171434/KeyFindings_MTConnectRoadmap20150514.pdf (20.12.2015) S. 11

MTConnect Institute: www.mtconnect.org – Members. 2015b. URL: http://www.mtconnect.org/roster/ (20.12.2015)

MTConnect Institute: www.mtconnect.org - MTConnect Standard Part 1: Overviel and Protocol. 2014. URL: http://static1.squarespace.com/static/54011775e4b0bc1fe0fb8494/t/557f2897e4b04b2acdba80b5/1434396823825/mtc_part_1_overview_v1.3.pdf (20.12.2015) S. 3-5

MTConnect OPC UA Companion Specification: http://www.mtconnect.org - Companion Specification Release Candidate Version 1.02. 2013. URL: http://static1.squarespace.com/static/54011775e4b0bc1fe0fb8494/t/5581baf6e4b09b87d6d781d5/1434565366350/mtconnect-opc-ua-companion-specification-v12-release-candidate.pdf (20.12.2015) S. 13

Ohland, Günther: www.pc-magazin.de - Der EnOcean-Funkstandard auf dem Prüfstand. 2012. URL: http://www.pc-magazin.de/vergleich/geheimfunker-1479624.html (15.02.2016)

OPC Foundation: www. opcfoundation.org – Members. 2015a. URL: https://opcfoundation.org/members (19.12.2015)

OPC Foundation: www. opcfoundation.org - OPC Unified Architecture Specification Part 1: Overview and Concepts Release 1.03. 2015b. URL: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts/ (Download 19.12.2015) S. 14

OPC Foundation: www. opcfoundation.org - OPC Unified Architecture Specification Part 2: Security Model Release 1.03. 2015c. URL: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-2-security-model/ (Download 19.12.2015) S. 9, 22

OPC Foundation: www. opcfoundation.org - OPC Unified Architecture Specification Part 7: Profiles Release 1.03. 2015d. URL: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-7-profiles/ (Download 19.12.2015) S. 89

Pauli, Darren: www.theregister.co.uk - Boffins find hundreds of thousands of woefully insecure IoT devices. 2014. URL: http://www.theregister.co.uk/2014/08/17/boffins_find_ihundreds_of_thousandsi_of_woefully_insecure_iot_devices/ (18.12.2015)

Plattform Industrie 4.0: www.plattform-i40.de - Was ist Industrie 4.0?. 2015. URL: http://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html (14.12.2015)

Pätz, Christian: Z-Wave: Die Funktechnologie für das Smart Home. 2014. S. 196

qivicon: www.qivicon.de - Bitron Geräte lassen sich nicht hinzufügen. 2014. URL: https://community.qivicon.de/questions/bitron-gerate-lassen-sich-nicht-hinzufugen (29.02.2016)

Schiefer, Michael; Lösche, Ulf; Morgenstern, Maik: www.av-test.org - AV-TEST-Studie - 7 Smart-Home-Starter-Kits im Sicherheits-Test. 2014. URL: https://www.av-test.org/fileadmin/pdf/avtest_2014-04_smart_home_deutsch.pdf (23.02.2016) S.2-4

Schäfer, Reinhold: www.maschinenmarkt.vogel.de - Erweiterung des Industrie 4.0 Standards. 2015. URL: http://www.maschinenmarkt.vogel.de/erweiterung-des-industrie-40-standards-a-486313/
Aufgerufen am 19.12.2015

Smart Home Guide: www.smarthome-guide.de – Was ist SmartHome. 2015. URL: http://www.smarthome-guide.de/was-ist-smart-home-und-wozu-gibt-es-den-smarthome-guide/ (14.12.2015)

Smart Home Zertifizierungsprogramm: www.zertifizierungsprogramm-smarthome.de - Smart Home Ready Siegel. 2016. URL: http://www.zertifizierungsprogramm-smarthome.de/smarthome/markt/seiten/siegelzertifikat.aspx (04.01.2016)

Universal Plug and Play: www. upnp.org - UPnP Device Architecture 1.1. 2008. URL: http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf (20.02.2016) S.1, 71

ZigBee Alliance: www.zigbee.org - ZigBee Specification. 2012. URL: http://www.zigbee.org/download/standards-zigbee-specification/ (Download 11.02.2016) S. 2, 591

Zillner, Tobias: www.blackhat.com - ZigBee Exploited - The Good the Bad and the Ugly. 2015.URL: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf (09.02.2016) S.3, 6

Z-Wave Allience: http://z-wavealliance.org - About Z-Wave technology. 2016. URL: http://z-wavealliance.org/about_z-wave_technology/ (11.02.2016)

Z-Wave: www.zwave.de - Was ist Z-Wave. 2016. URL: http://www.zwave.de/about-us/ (11.02.2016)

6 Abkürzungsverzeichnis

AES - Advanced Encryption Standard
AMT - Association For Manufacturing Technology
API - Application Programming interface
BLE - Bluetooth Low Energy
CBC-MAC - Cipher Block Chaining - Message Authentication Code
CCM - Counter with CBC-MAC
CNC - Computerized Numerical Control
DSL - Digital Subscriber Line
ENISA - European Union Agency for Network and Information Security
HTML - Hypertext Markup Language
HTTP - Hypertext Transfer Protocol
IEC - International Electrotechnical Commission
IEEE - Institute of Electrical and Electronics Engineers
IoE – Internet of Everything
IoT – Internet of Things
IP - Internet Protocol
IPSec - Internet Protocol Security
ISM - Industrial, Scientific and Medical
ISO - International Organization for Standardization
KNX - Konnex
M2M – Machine to Machine
mA - mili-Ampere
MacOS - Macintosh Operating System
NAT - Network Address Translation
OPC UA - Open Platform Communications Unified Architecture
PIN - Persönliche Identifikationsnummer
PFS - Perfect Forward Secrecy
Profinet - Process Field Network
ReST - Representational State Transfer
RFC - Request for Comments
SDK - Software Development Kit
SOAP - Simple Object Access Protocol
SSDP - Simple Service Discovery Protocol
SSH - Secure Shell
SSL - Secure Sockets Layer
TCP - Transmission Control Protocol
Telnet - Teletype Network
TLS - Transport Layer Security
TSN TG - Time-Sensitive Networking Task Group
UCB - University of California, Berkeley
UDP - User Datagram Protocol
UPnP – Universal Plug & Play
URI - Uniform Resource Identifier
URL - Uniform Resource Locator

WS - Web Service
XML - Extensible Markup Language

7 Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken (dazu zählen auch Internetquellen) entnommen sind, wurden unter Angabe der Quelle kenntlich gemacht.

04.05.2016, Halle Manuel Klausing