MASTERARBEIT

ENTWICKLUNG EINES SECURITY FRAMEWORKS ZUR BEWERTUNG DER RISIKEN VON IOT-PRODUKTEN FÜR BESTEHENDE IT-INFRASTRUKTUREN

ausgeführt am

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Christopher Gartner, BSc.

Personenkennzeichen: 1610320031

Graz, am 25. November 2017 .....

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

KURZFASSUNG

Die Verbreitung von Geräten, die mit dem Internet kommunizieren und Teile des Alltags vieler Menschen sind, nimmt immer mehr zu. Das Internet of Things (IoT) kombiniert bestehende Technologien mit dem Internet, wodurch neue Einsatzgebiete erschlossen werden. IP-Kameras, Verkehrssteuerungssysteme und kritische Infrastrukturen wandern zunehmend in das Internet und werden dadurch für Personen erreichbar, die keinen Zugriff auf diese Systeme haben sollten. Dies führt dazu, dass neue Angriffsvektoren, die von Hackern und Kriminellen genutzt werden, entstehen und sowohl die IT-Sicherheit der IoT-Objekte selbst, als auch jene von bestehenden IT-Infrastruktur gefährdet werden.

Viele IoT-Produkte, die für die Endkundin und den Endkunden konzipiert wurden, verfügen nicht über die notwendigen Sicherheitsmechanismen, die einen ordnungsgemäßen und sicheren IT-Betrieb gewährleisten sollen. Die Produktentwicklung der Hersteller setzt den Fokus auf Bedienungskomfort und einfacher Konfiguration, vergisst jedoch die Gefahren, welche von ungesicherten IoT-Objekten ausgehen. Diese Gefahren reichen von Funktionsstörungen, dem Versenden von Spam-E-Mails, bis zur Nutzung von IoT-Objekten für großangelegte Hacker-Angriffe auf kritische Infrastrukturen.

In dieser Arbeit wird ein IoT-Security Framework entwickelt, das auf Basis von Analysen bestehender IoT-Sicherheitsproblematiken, Sicherheitsanforderungen definiert und diese in einem Integrationsprozess zusammenfasst. Die Sicherheitsanforderungen wurden aus bereits publizierten Angriffsszenarien abgeleitet und werden sich direkt an das IoT-Objekt richten, der sicheren Kommunikation zwischen den einzelnen Objekten, sowie an die Cloudplattformen, die im Umfeld von IoT häufig zum Einsatz kommen. Das IoT-Security Framework soll es Endkonsumentinnen und Endkonsumenten ermöglichen, die IT-Sicherheit von IoT-Produkten zu bewerten und deren Risiko für sich selbst, als auch für bestehende IT-Infrastrukturen zu beurteilen.

ABSTRACT

The distribution of electronic devices, which communicate with the internet and are part of the daily routine for many people, is constantly increasing. The Internet of Things combines existing technologies and knowledge with the internet and thus opens up new areas of use. IP-cameras, traffic control systems and critical infrastructure are shifting towards the internet. This allows people to use these tools even without access to the systems in the traditional way. However, this development leads to new attack vectors for hackers and criminals and thus endangers the IT-security of IoT-objects as well as those of already existing IT-infrastructure.

Unfortunately, various IoT-products designed for clients do not have the necessary security measures which would guarantee a safe and secure IT-operation. Since the main focus of manufacturers concerning product development is set on the users' comfort and the simple configuration, the hazards of unsecure IoT-objects are neglected. These risks can include malfunction, spamming as well as the misuse of IoT-objects for hacker attacks on critical infrastructure.

This paper presents an IoT-Security Framework which, based on analyses of security issues, specifies safety requirements and condenses the information into an integration process. The security requirements are derived from already published attack scenarios and directly address the IoT-object, the secure communication between individual objects as well as cloud platforms frequently used for IoT. The IoT-Security Framework should allow the end consumer to evaluate IT-security of IoT-products and determine their risks as well as those of the IT-infrastructure.

INHALTSVERZEICHNIS

1 EINLEITUNG

Immer mehr Endgeräte des täglichen Lebens sind mit dem Internet verbunden. Forscherinnen und Forscher zeigen auf, dass zwischen dem Jahr 2017 und 2025, die Anzahl der internet-fähigen Endgeräten um 60 Millionen zunehmen wird. (Statista, 2017) Dies führt unweigerlich dazu, dass die Zahl an potentiellen Angriffsszenarien durch Bedrohungen aus dem Internet steigen wird. Kühlschränke, Fernseher und Heizungssteuerungen, um nur einige Beispiele von vielen zu nennen, besitzen immer öfter Schnittstellen und Funktionalitäten, um mit dem Internet Verbindung aufnehmen zu können. Diese Möglichkeit bietet Endkundinnen und Endkunden den Komfort, von überall aus, auf die eigene Infrastruktur zugreifen zu können und damit unabhängiger zu agieren.

Dieses Tor bietet nicht nur der eigentlichen Endkundin und dem eigentlichen Endkunden, die Möglichkeit des Fernzugriffs, sondern auch Hackern und kriminellen Organisationen, Sicherheitslücken in den einzelnen Systemen zu verwenden, um ebenfalls Zugang zu erlangen. Dadurch ergeben sich neue Arten von Bedrohungen für bestehende IT-Infrastrukturen, die der Endkundin und dem Endkunden aktuell nicht bekannt sind.

Fehlende und nicht installierte Updates von IoT-Produkten führen dazu, dass bestehende und als sicher geltende Infrastrukturen, angegriffen und gekapert werden können. Durch die Vielzahl an unterschiedlichen Herstellern und Produkten wird es der Endkundin und dem Endkunden zudem erschwert, den Überblick über ihr und sein IT-Ecosystem zu wahren und entsprechende Sicherheitsmaßnahmen zu setzen.

Täglich erscheinen Meldungen von neuen Bedrohungen im IT-Sektor, wobei im speziellen jene der IoT-Gefahren kontinuierlich sich erhöhen. (Gartner, 2016) Das Bewusstsein der Endkundinnen und Endkunden, dass IT-Systeme ständig gewartet und aktualisiert werden müssen, hat sich insoweit entwickelt, dass Desktopsysteme, wie PCs (Personal Computer) und Notebooks, einem entsprechenden Updateverhalten unterworfen werden.

Dieses Verhalten hat sich jedoch noch nicht durchgesetzt, sodass IoT-Produkte, als gleichwertige Systeme betrachtet werden sollten und aus diesem Grund ähnlichen Updatezyklen unterliegen müssen. Fehlende Kenntnis über die Gefahren, die IoT-Produkte auslösen können und Hersteller, welche bei der Entwicklung dieser Produkte wesentliche Sicherheitseigenschaften ignorieren, werden zu einem globalen Problem, dessen Ausmaße heute noch nicht abzuschätzen sind, falls diese nicht behoben werden. (Barcena & Wuesst, 2015)

Die vorliegende Arbeit befasst sich mit der Entwicklung eines Security Frameworks für IoT-Produkte, das IoT-Objekte anhand von Sicherheitskriterien bewertet und diese entsprechenden Risikoklassen zuordnet.

1.1 Motivation der Arbeit

IoT-Produkte erfreuen sich aktuell immer steigender Beliebtheit (Forbes, 2014). Die Risiken die davon ausgehen sind aber den wenigsten bekannt. Unterschiedliche Hersteller bieten ihre Produkte am Markt an, ohne darauf hinzuweisen, welche Gefahren bei falscher Konfiguration und Wartung entstehen. Die potentielle Käuferin und der potentielle Käufer solcher Produkte verliert, aufgrund der Vielzahl, die Übersicht und kann dadurch nicht entsprechende Vergleiche auf Basis von implementierten Sicherheitseigenschaften durchführen.

Das Security Framework, welches in dieser Arbeit für den Bereich von IoT entwickelt wird, beinhaltet neben Sicherheitsmerkmalen von Produkten, auch Risikoklassen, die bei der Beurteilung von Risiken unterstützen. Des Weiteren sind zu verwendende Standards, Prozesse und Architekturen enthalten, die zur Sicherheit der IT-Infrastruktur beitragen. (ITPG, 2014) Ein Framework ist essentiell für die Sicherheit dieser Infrastrukturen und schafft einen Überblick über aktuelle Technologien und wie diese eingeschätzt werden sollten.

Die Motivation dieser Arbeit besteht darin, die im nachfolgenden Abschnitt ausgeführte Forschungsfrage zu beantworten und basierend aus den erarbeitenden Erkenntnissen, ein Security Framework zu entwickeln.

1.2 Ziel der Arbeit

Ziel dieser Arbeit ist, folgende Forschungsfrage zu beantworten:

Welche Sicherheitsmerkmale muss ein IoT-Produkt aufweisen, um in bestehende IT-Infrastrukturen eingebunden werden zu können, ohne die Sicherheitsrichtlinien und damit verbundene Maßnahmen zu kompromittieren und die IT-Sicherheit dadurch zu gefährden?

Hierzu sollen im Zuge dieser Arbeit entscheidende Sicherheitsmerkmale von IoT-Produkten analysiert werden. Dabei sollen grundlegende Technologien und Sicherheitsstandards recherchiert und dargestellt werden. Die fundierte Auswahl entscheidender Sicherheitseigenschaften, soll gewährleisten, dass eine entsprechende Sicherheit für IT-Infrastrukturen gegeben ist und durch die Integration neuer IoT-Produkte, nicht gefährdet wird.

Außerdem wird durch die Erarbeitung von grundlegendem Basiswissen, das Verständnis für potentielle Gefahren, welche von IoT-Produkte ausgehen, geschaffen. Dies sollen die Voraussetzungen für das Security Framework darstellen, das im Rahmen des Praxisteils entwickelt wird.

Die ausgewählten Sicherheitsmerkmale sollen mit aktuellen IoT-Technologien kombiniert und im Security Framework zusammengeführt werden.

1.3 Nicht-Ziele der Arbeit

Diese Arbeit bezieht sich im speziellen auf den Einsatz und den Betrieb von IoT-Produkten in IPv4 (Internet Protokoll Version 4) Netzwerken. Netzwerke, die auf dem IPv6 Standard basieren, sind von dieser Arbeit ausgenommen, weil noch weitere Aspekte separat betrachtet werden müssen. Des Weiteren bezieht sich diese Arbeit nur auf den Gebrauch von IoT-Produkten im privaten Umfeld und nicht im unternehmerischen. Diese erfordern spezielle Sicherheitsvorkehrungen und Richtlinien, die nicht mit denen von Heimanwenderinnen und Heimanwendern vergleichbar sind. Darüber hinaus ist nicht möglich, alle am Markt verfügbaren IoT-Produkte zu identifizieren und für diese Sicherheitskonzepte zu entwickeln. Deshalb werden in dieser Masterarbeit einzelne ausgewählte Kategorien von IoT-Produkten analysiert.

Im folgenden Abschnitt wird die Vorgangsweise beschrieben, mit der die genannten Ziele in dieser Arbeit erreicht werden sollen.

1.4 Methodik und Vorgangsweise

Um die angeführten Ziele erreichen zu können, ist es wichtig, Wissen, das zum Verständnis von IoT und den damit verbundenen Risiken notwendig ist, zu erarbeiten. Dazu wird zu Beginn der Arbeit, der Begriff IoT beleuchtet, welche Charakteristiken diese Technologie beschreibt und wo Unterschiede zu bereits bestehenden vernetzten Systemen bestehen. Daran knüpft ein Abschnitt der Arbeit an, welcher essentielle Technologien von IoT-Produkten beschreibt. Dabei werden Funktechnologien, Softwaresysteme und Cloud-Dienste beschrieben.

Diese Auswahl dient als Basis für die Analyse und Entwicklung eines Kriterienkatalogs, in dem die Sicherheitsmerkmale in Klassen unterteilt und entsprechende Konfigurationsmöglichkeiten bereitgestellt werden. Als Grundlage für die Einteilung der IoT-Produkte anhand von Sicherheitseigenschaften sollen anerkannte Literatur und IT-Sicherheitsrichtlinien, wie dem BSI (Bundesamt für Informationssicherheit) und Best-Practice Ansätzen verwendet werden. (Security, 2016) und (Corporation, 2016)

Diese Arbeit basiert auf der folgenden Arbeitshypothese und soll im weiteren Verlauf über eine Literaturrecherche bestätigt und angepasst werden.

H1: IoT-Produkte gefährden die Sicherheit von bestehenden IT-Infrastrukturen, wenn diese nicht auf entsprechende Sicherheitsaspekte geprüft werden.

H0: IoT-Produkte gefährden die Sicherheit von bestehenden IT-Infrastrukturen nicht.

Diese Hypothesen beschreiben die aktuelle Situation, in der es vielen Endkundinnen und Endkunden nicht bekannt ist, dass die gekauften IoT-Produkte, ihre IT-Sicherheit und die damit verbundene Infrastruktur gefährden. Die notwendigen Sicherheitsmerkmale werden zudem kaum oder gar nicht von den einzelnen Herstellern aufgeführt, wodurch eine Guideline, in diesem Fall, ein Security Framework, essentiell für den Kauf von IoT-Produkten ist.

Im letzten Kapitel dieser Arbeit werden die Ergebnisse des IoT-Security Frameworks diskutiert und Anknüpfungspunkte für weitere Entwicklungen bereitgestellt Des Weiteren wird ein Ausblick

gegeben, wie zukünftig mit dem Thema der Sicherheit von IoT-Produkten umgegangen werden kann.

1.5 Struktur der Arbeit

Diese Arbeit gliedert sich in fünf Kapitel (vergleiche Abbildung 1). Das erste Kapitel beschreibt die Motivation, das Ziel und die Nicht-Ziele, sowie die zugrundeliegende Methodik dieser Arbeit. Außerdem werden die Ausgangssituation, die Forschungsfrage und die Arbeitshypothese präsentiert.

Die Grundlagen zu IoT, den damit verbundenen Grundlagentechnologien und die Abgrenzung zu bestehenden IT-Systemen sind im zweiten Abschnitt beinhaltet. Wichtige Technologiemerkmale, wie Betriebssysteme, Funktechnologien und Datenspeicherung werden erläutert.

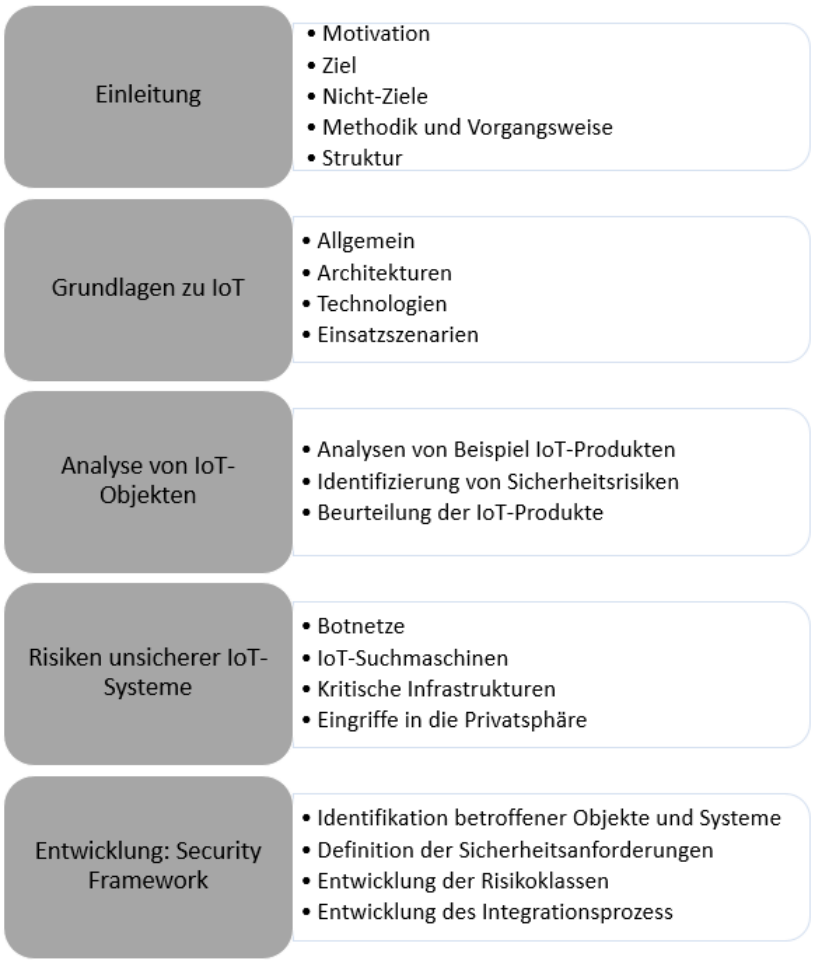


Abbildung 1 Struktur der Arbeit

Das dritte Kapitel beschäftigt sich mit der Analyse von IoT-Objekten und ihren Merkmalen. Dies wird die Grundlage für das Security Framework darstellen, weil die IoT-Produkte in einzelne Klassen unterteilt werden, welche sich durch unterschiedliche Sicherheitseigenschaften charakterisieren.

Aktuelle Risiken und Angriffsvektoren, die im speziellen IoT-Objekte als Angriffsziele nutzen, werden im vierten Kapitel analysiert. Dazu zählen neben Botnetzen, Angriffe auf kritische Infrastrukturen, sowie Eingriffe in die Privatsphäre.

Im Rahmen des fünften Kapitels wird die Entwicklung des Security Frameworks dokumentiert. Zu diesem Zweck werden die im dritten Kapitel erarbeiteten Sicherheitseigenschaften in einzelne Klassen unterteilt, anhand deren anschließend die Risikoklassen definiert werden. Abschließend werden in der Conclusio alle Ergebnisse zusammengefasst und die Forschungsfrage beantwortet, sowie die Arbeitshypothese dieser Arbeit bestätigt oder widerlegt.

2 GRUNDLAGEN ZU IOT

Das IoT ist eine Entwicklung, die sich in den letzten fünf Jahren zu einem globalen Wandel in der Wirtschaft formiert und in Privathaushalten vieler Menschen Einzug gehalten hat. (Brand, Hülser, Grimm, & Zweck, 2009)

Es besteht kein Zweifel, dass durch die Vorteile, die aus der zunehmende Vernetzung entstehen, neue Wirtschaftszweige etabliert werden, an welche heute noch nicht zu denken ist. Die neuen Möglichkeiten der digitalen Kommunikation jeglicher Endgeräte miteinander, die Verfügbarkeit von Sensoren und Kombination aus den Daten, die diese bereitstellen, können sowohl die Effektivität, als auch die Effizienz auf ein neues Level heben. (Gronau, Thim, & Fohrholz, 2017)

Aufgrund des weiten Spektrums, welches IoT abdeckt, gibt es im Moment (Stand: Juli 2017) keine einheitlich standardisierte Definition, was IoT ist. Wichtig ist einen Unterschied zu bereits bestehenden Technologien, welche mit dem Internet kommunizieren, zu treffen, um hier eine klare Abgrenzung zu gewährleisten.

Die Internationale Fernmeldeunion, ITU (International Telecommunication Union), beschreibt IoT als, eine globale Infrastruktur für die Informationsgesellschaft, welche die Vorteile der Zusammenarbeit unterschiedlicher Services (physikalische, als auch virtuelle) nutzt. Dies erfolgt durch existierende und in der Entwicklung stehende interoperable Standards und Kommunikationstechnologien. (International Telecommunation Union, 2012)

Das IEEE (Institute of Electrical and Electronics Engineers) fasst in ihrer Definition, IoT als ein Netzwerk auf, das eindeutig identifizierbare Dinge mit dem Internet verbindet, zusammen. Diese Dinge besitzen sensorische oder aktive Komponenten, die programmierbar sind. Wegen der Möglichkeit der eindeutigen Identifizierung können Daten des Dings gespeichert und zugeordnet werden. Den Datenabruf und die Programmierung des Dings kann von überall, zu jeder Zeit, von jedem abgerufen oder geändert werden. (Minerva, Biru, & Rotondi, 2015)

Des Weiteren beschreibt das IEEE, ein globales Szenario von IoT, als selbstkonfigurierendes, adaptives und komplexes Netzwerk, das die Verbindung zwischen den einzelnen Dingen gewährleistet. Zudem nutzt es Standardkommunikationsprotokolle zum Datenaustausch über das bestehende Internet. Die miteinanderverbundenen Dinge repräsentieren die digitale Welt mit Sensorik, Aktoren und der Möglichkeit, diese zu programmieren oder konfigurieren. Essentiell ist die eindeutige Identifizierbarkeit jedes dieser Dinge über das gesamte Internet. Die Repräsentation beinhaltet Informationen über die Identität des Dings, Status, Örtlichkeit, an dem es sich befindet oder andere entscheidende Informationen für einen Business-Prozess. Die Dinge selbst bieten Services an, welche mit oder ohne menschlicher Interaktion, betrieben werden. Dies können das Auslesen von Datenaufzeichnungen von Sensoren sein oder Aktoren, welche gesteuert werden können. Diese Services können über intelligente Schnittstellen genutzt werden, die von überall aus, zu jedem Zeitpunkt und für jeden erreichbar sind. (Minerva, Biru, & Rotondi, 2015)

Beide Definitionen ergänzen und überlappen sich zum Teil stark, was auch das breite Spektrum von IoT wiederspiegelt. Feststellen lässt sich jedoch, dass IoT auf bereits bestehenden Strukturen

und Systemen aufbaut und diese mit einer feineren Granularität, an unterschiedlichen Systemen und Möglichkeiten anreichert. (vergleiche Abbildung 2)

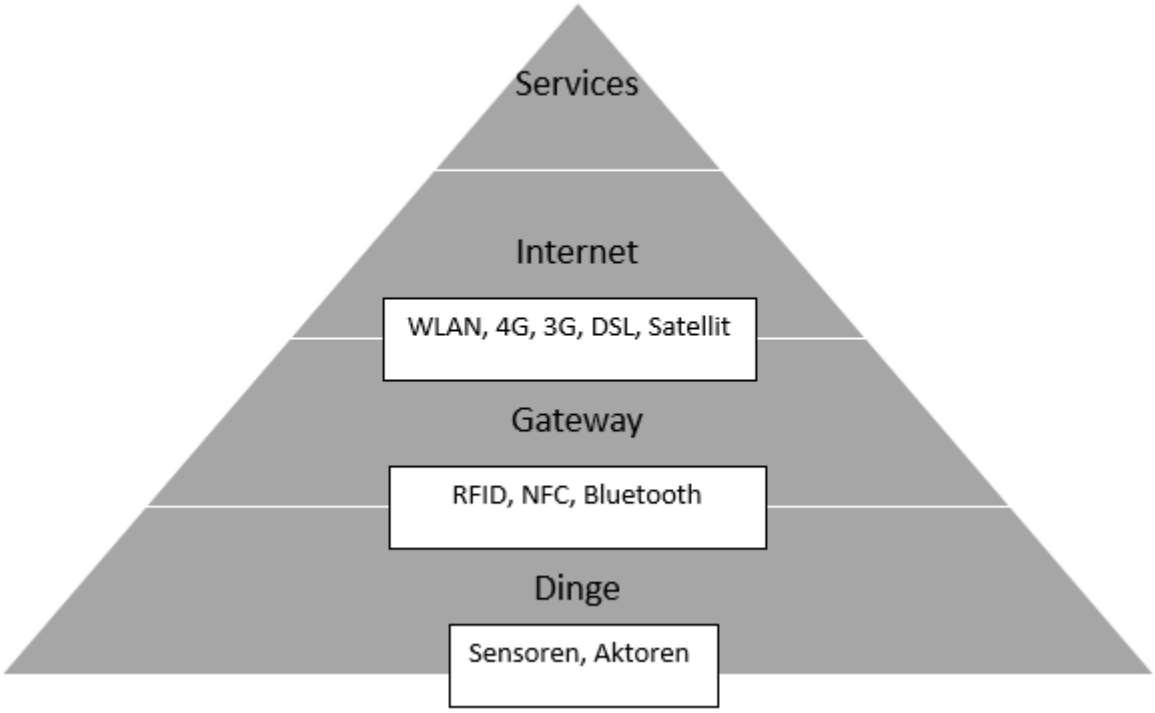


Abbildung 2 Internet of Things Struktur (RF Wireless World, 2015)

2.1 Geschichte

Erste Entwicklungen, Geräte aus dem Alltag, mit dem Internet zu verbinden, gab es bereits Mitte der 1980er. An einer Universität in Pennsylvania (USA) wurde ein Getränkeautomat mit dem Internet verbunden. Ziel war es, die aktuelle Anzahl an verfügbaren Getränke, sowie die Temperatur von neu hinzugegebenen, zu messen. (University, 2014)

Mark Weiser, ein ehemaliger Forscher am XEROX PARC (Palo Alto Research Center Incorporated), prägte Anfang der 90er den Begriff des ubiquitous computing, also den omnipräsenten Computer. Diese Vorphase von IoT beschreibt die allgegenwärtige Verfügbarkeit von Rechenleistung. Voraussetzung dafür ist eine hohe Durchdringung der Rechnerdichte, die mit IoT mehr als gegeben erscheint. Ubiquitous computing fasst zusätzlich die Verknüpfung von Rechnern mit sensorischen und aktiven Elemente auf. In seinem Paper „The Computer for the 21st Century“ beschreibt Mark Weiser, dass die Anzahl an sichtbaren Rechnern, immer mehr verschwinden wird und diese durch intelligente Gegenstände abgelöst werden. (Weiser, 1988)

Im Jahr 1994 beschrieb der US-Amerikaner Reza Raji in einer Publikation der IEEE ein Konzept, welches aktuelle Ansätze in der Datenübertragung in Frage stellte. Dabei erarbeitete er eine neue Herangehensweise, bei welcher kleine Datenpakete zu größeren Datenknoten übertragen werden. Urheber dieser Daten sollen Kleinstrechner sein, wodurch sich alles automatisieren ließe, vom Einfamilienhaus bis hin zu gesamten Produktionsstätten. (Raji, 1994)

Entscheidend für die Etablierung und das schnelle Voranschreiten in der Entwicklung von IoT war jedoch die Markteinführung von RFID (Radio Frequency Identification) (Magrassi, 2002). Forscherinnen und Forscher des Auto-ID Centers am MIT (Massachusetts Institute of Technoloy) veröffentlichten in einer ihrer Publikationen das Statement, dass RFID die Grundvorrausetzung für IoT ist. Nur wenn man Objekte des täglichen Lebens eindeutig identifizieren kann, können Computer und Algorithmen damit arbeiten und diese verwalten. (Wood, 2015)

Die Identifizierung von Objekten wurde zuerst in Produktionsstätten der Automobilindustrie und später im Gesundheitsbereich, eingesetzt, um den aktuellen Status zu ermitteln und die Effizienz steigern zu können. Zukünftig werden Personen mit NFC-Technologien identifiziert, was im Moment noch über Karten und Tags geschieht. Die Miniaturisierung, sowie eine Verbesserung des Energieverbrauchs der IoT-Produkte werden zu einer Verschmelzung von digitalem Web und der physikalischen Welt führen. (vergleiche Abbildung 3) (SRI Consulting Business Intelligence, 2014)

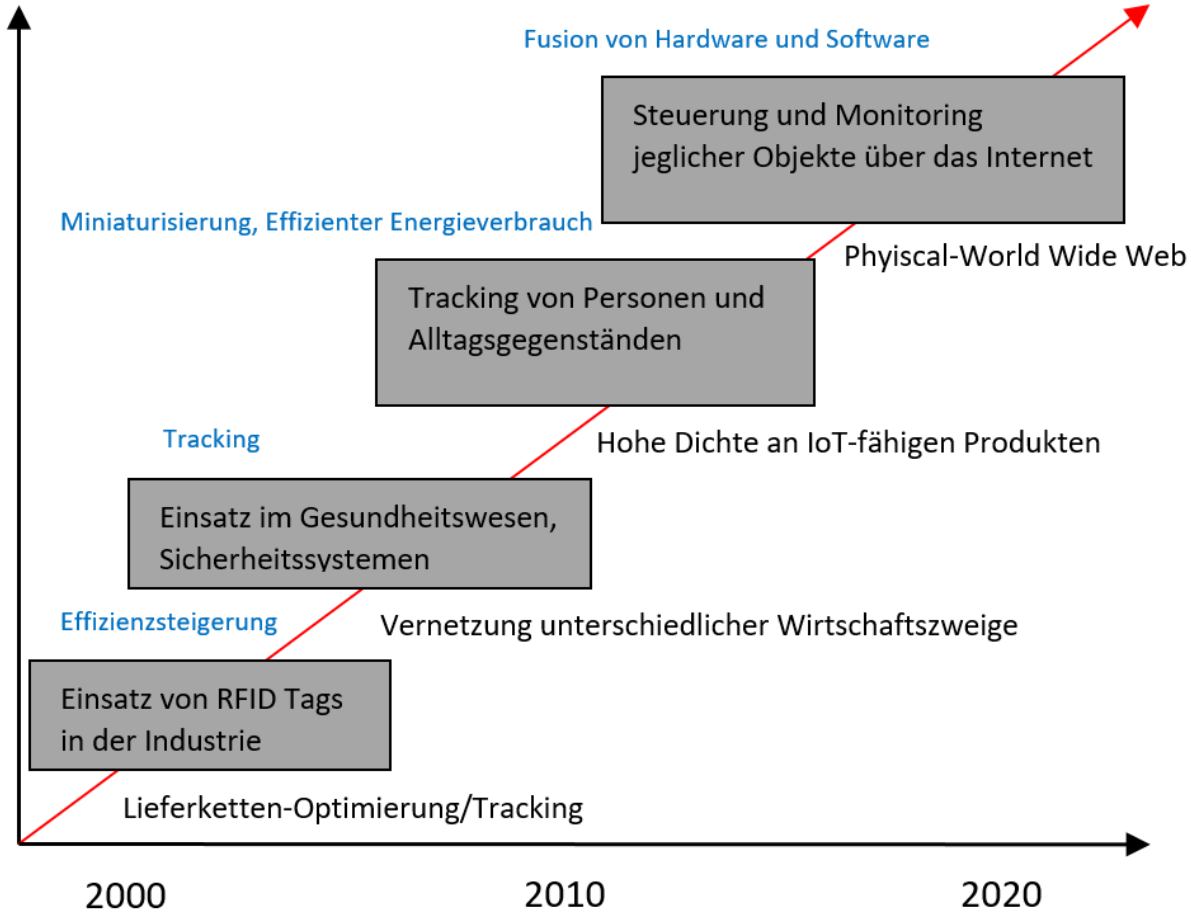


Abbildung 3 Historischer Verlauf des Einsatzes von IoT in der Wirtschaft (SRI Consulting Business Intelligence, 2014)

2.2 Abgrenzung zu M2M (Machine to Machine)

IoT, M2M (Machine 2 Machine) und andere Begriffe prägen aktuell die Medienlandschaft. Beide Begriffe lassen sich nur schwer voneinander trennen. Es finden sich Synergien und

Überlappungen in beiden Technologien, wodurch sich beide nur anhand ihres Fokus abgrenzen lassen.

Die RTR (Rundfunk und Telekom Regulierung) definiert M2M, als generisches Konzept, welches den Informationsaustausch zwischen einzelnen Maschinen über unterschiedliche Übertragungsmedien ohne aktiven Einfluss des Menschen beschreibt. IoT dagegen beschreibe ein viel umfangreicheres Themengebiet, das den Ansatz verfolgt, Informationen so breit wie möglich zu generieren und zu verteilen, damit das daraus gewonnene Wissen, auch für themenfremde Lösungen genutzt werden kann. (Rundfunk und Telekom Regulierung, 2016) Die Abgrenzung und Synergien von IoT und M2M werden in Abbildung 4 dargestellt.

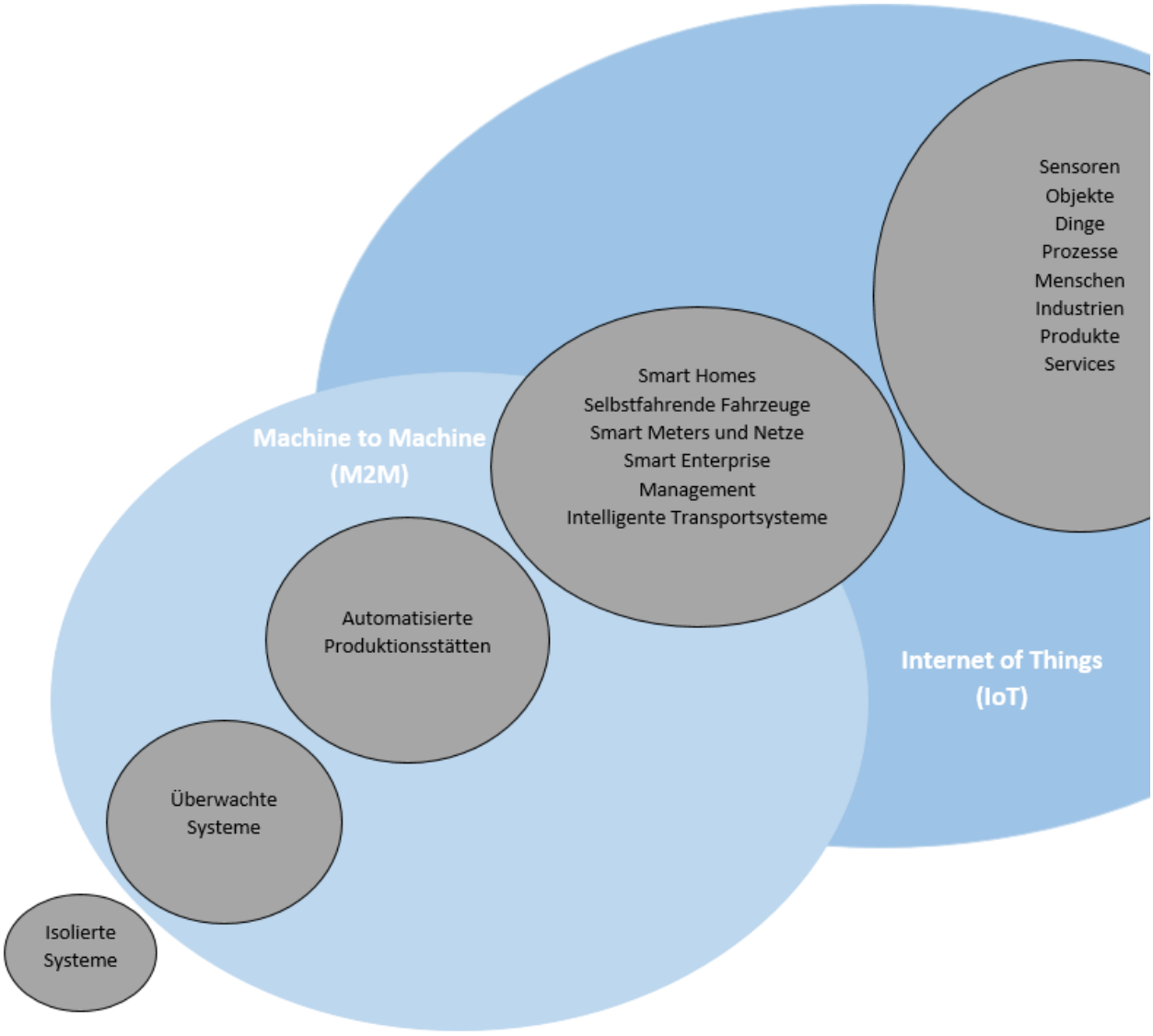


Abbildung 4 Synergien M2M zu IoT (Berthelsen & Morrish, 2014)

Aus Abbildung 4 lässt sich IoT als eine Weiterentwicklung von M2M ableiten. In den Anfangszeiten von M2M standen dezidiert voneinander abgeschlossene Systeme im Vordergrund. Als Beispiel kann hier ein Gebäude genannt werden, das für die einzelnen unterschiedlichen Systeme (beispielsweise Klima- und Sicherheitstechnik) jeweils separate

Sensoren nutzt. Die daraus ausgelesenen Daten werden in eigenen, proprietären, Protokollen und Datenformaten ausgetauscht, sodass eine Interoperabilität nicht gewährleistet ist. Dadurch ergibt sich das Problem, dass Sensoren und andere Komponenten eines intelligenten Systems nicht mit fremden Systemen anderer Hersteller kommunizieren können.

Der Vorteil in M2M Systemen besteht darin, dass jedes System für sich selbst arbeitet und deswegen keine Standards verwendet werden müssen. Eine Implementierung ist deshalb einfacher umzusetzen, als im Bereich von IoT. Des Weiteren sind M2M-Lösungen auf ein Problemgebiet spezialisiert, wodurch die Kommunikation mit anderen (Fremd-)Systemen ausgeschlossen ist.

Im Unterschied zu M2M ist IoT als ein offenes Konzept zu sehen, das ermöglicht über mehrere unterschiedliche Systeme, Sensoren und Kontrolleinheiten hinweg Daten zu erfassen und diese allen im System verbundenen Endgeräten zur Verfügung zu stellen. Somit ist IoT nicht auf einen Geschäftsprozess selbst fokussiert, es beschreibt vielmehr ein Ecosystem, in dem unterschiedlichste Komponenten interagieren. IoT-Netzwerke basieren auf standardisierten und offen-dokumentierten Austauschformaten und nutzen darüber hinaus häufig Cloudanwendungen zur Speicherung und Analyse der Daten. Somit ist im Bereich von IoT meist eine aktive Internetverbindung Voraussetzung, wogegen bei M2M Technologien lokale Netzwerke vielfach ausreichen. (vergleiche Tabelle 1)

Internet of Things (IoT)	**Machine to Machine (M2M)**
Kommunikation über standardisierte, interoperable Protokolle (IP, etc.)	Punkt-zu-Punkt Verbindung zwischen einzelnen Systemen und Endpunkten
Daten werden oft in einer Zwischenschicht für Endkunden bereitgestellt (Cloud)	Endgeräte nutzen mobile und drahtgebundene Netzwerke (3G oder LAN)
Aktive Internetverbindung als Voraussetzung	Internetverbindung nicht unbedingt notwendig (autonom)
Unbegrenzte Anzahl an Integrations- und Kommunikationsmöglichkeiten, aufgrund der genutzten Datenaustauschformate/Protokolle	Begrenzte Anzahl an Integrations- und Kommunikationsmöglichkeiten, weil jedes System autonom agiert

Tabelle 1 Vergleich: IoT und M2M (Hassel, 2015)

Zusammenfassend ist festzuhalten, dass sich IoT und M2M sehr stark überschneiden. Betrachtet man jedoch die Trends wie Cloud-Computing, globale Vernetzung und Digitalisierung, so ist IoT, als eine umfassende Weiterentwicklung von M2M zu sehen. IoT verknüpft offene Standards, welche bereits in unterschiedlichsten Anwendungsgebieten genutzt werden, mit Technologien von M2M. Dadurch ergeben sich neue übergreifende Produkte und Services, die sowohl vernetzte Hardware als auch Cloud-Services beinhalten.

2.3 Technologien

Das IoT ist eine Kombination aus diversen Technologien, die durch die Vernetzung der einzelnen Komponenten neue Möglichkeiten bietet. Laut Samulat ist IoT die Verknüpfung einer Vielzahl von Technologieformen, bestehend aus Sensorik, Cloud und Big Data. Die IoT-Produkte seien ständig mit dem Internet verbunden. Sie sammeln über Sensoren eine große Menge an Daten, die in die Cloud übertragen und entsprechenden Big Data Analyseverfahren unterzogen werden. (Samulat, 2015)

2.3.1 Architektur

Aufgrund der Vielzahl der Anwendungsgebiete, sowie der Vielfalt an verschiedenen IoT-Produkten, lässt sich nur eine abstrakte verallgemeinernde Architektur feststellen. Diese ist in vielen Fällen mit zusätzlichen Funktionen und Möglichkeiten ausgestattet. Von Grund auf basieren IoT-Systeme immer auf Dingen, also Produkten, die in jeglicher Form smart und verbunden mit anderen Produkten interagieren können.

Diese Dinge können einerseits Daten generieren und erfassen, anderseits auch empfangen und dadurch Aktionen setzen. Die Kombination aus beidem ist ebenso möglich. Ein Beispiel wäre ein smartes Heizthermostat, das kontinuierlich die Temperatur erfasst und diese entsprechend der Konfiguration anpasst.

Die Kommunikation mit der Nutzerin und dem Nutzer, kann über das Internet direkt erfolgen, beispielsweise via WLAN und mobilem Internetzugang (3G), oder über ein dazwischengeschaltetes System, einem Gateway. Solche Gateways können handelsübliche WLAN-Router sein, die nur den Zugang zum Internet ermöglichen, aber auch smarte Gateways, die zudem Sicherheitsfunktionalitäten beinhalten.

Nachdem die Daten der Dinge, durch einen Übertragungskanal in die Cloud gelangt sind, stehen sie für Analyse- und Steuerungsmöglichkeiten bereit. Angemerkt sei, dass nicht alle Dinge einen Cloud-Service voraussetzen. Er wird jedoch immer häufiger Teil eines umfassenden Serviceangebots, welches die Hersteller, ihren Kundinnen und Kunden mit dem Produkt zur Verfügung stellen.

In der Cloud selbst, stehen unterschiedlichste Funktionen bereit, die je nach IoT-Produkt und Hersteller vom einfachen Speichern, also dem Monitoring von Parametern, bis hin zu automatisierten Workflows und Event-Handling reichen, wodurch beispielsweise das smarte Zuhause, je nach Tageszeit unterschiedlichste Aktivitäten setzt. (vergleiche Abbildung 5) (Müller, 2016)

Für die bloße Identifikation und das Tracking von verschiedenen Dingen, welches jedoch viel mehr ein Thema des M2M Themengebiets ist, reicht der Einsatz von RFID und NFC (Near Field Communication) Technologien aus. Diese werden von einzelnen Kontrollpunkten aktiviert und erfasst. Ein Beispiel wäre die Erfassung von Materialgütern in der Logistikbranche. (Dominikus & Schmidt, 2011) Diese Art von IoT-Technik und das dazugehörige Einsatzgebiet stehen nicht im Fokus dieser Arbeit.

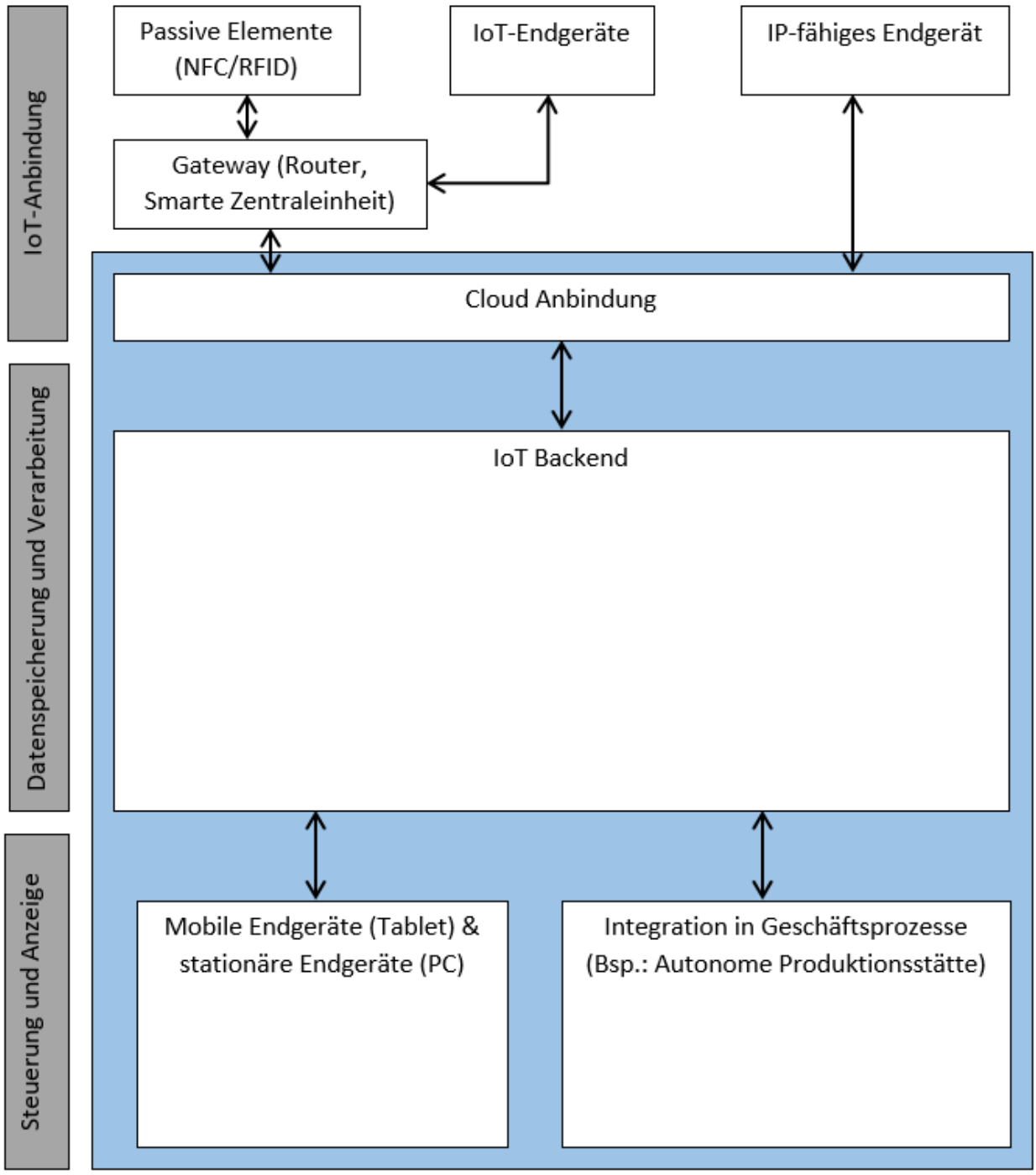


Abbildung 5 Architektur IOT-Systeme (Müller, 2016)

Wie in Abbildung 5 ersichtlich ist, handelt es sich um eine bidirektionale Kommunikation zwischen den Dingen und der Nutzerin und dem Nutzer, welche und welcher mit diesem interagiert. Die immer weiter verbreitete direkte Anbindung an Cloudanwendungen der einzelnen Hersteller wird im Abschnitt 2.3.3 näher beleuchtet, weil es potentielle Sicherheitsprobleme geben kann, die durch Hacker ausgenutzt werden können. Der nächste Abschnitt wird sich mit den zu Grunde liegenden Systemkomponenten, den Betriebssystemen und der Firmware von IoT-Produkten beschäftigen.

2.3.2 Betriebssysteme und Firmwares

Moderne IoT Produkte bieten neben Identifizierungsmerkmalen, auch immer mehr Funktionen zum Austausch von Informationen und der Interaktion mit anderen Objekten, sowie mit den eigentlichen Nutzerinnen und Nutzern, an. Aus diesem Grund sind Betriebssysteme, welche diese Möglichkeiten, ressourcenschonend und kostengünstig, bieten, essentiell für diese Art von IoT-Endgeräten. (Hahm, Baccelli, & Tsiftes, 2015)

Diese Betriebssysteme müssen mit Funknetzwerken kommunizieren können, ein effektives Energiemanagement besitzen, sowie kostengünstig in der Produktion und Entwicklung sein. Darüber hinaus sind Protokolle zu implementieren, über die das IoT-Endgerät mit anderen kommunizieren kann (IPv4, IPv6). Wegen der meist niedrigen Preisspanne, in welcher die IoT-Produkte am Markt erhältlich sind, wird auf möglichst geringe Hardwareanforderungen, auf einen möglichst kleinen Arbeitsspeicher und leistungsschwache CPUs geachtet (Central Processing Unit). (Küchemann, 2014)

Desktop-Betriebssysteme, wie Microsoft Windows oder Apple MacOS lassen sich, aufgrund des enormen Leistungsumfangs und dem einhergehenden Ressourcenbedarf, nicht für IoT-Endgeräte einsetzen. Allerdings gibt es Bemühungen seitens Microsoft hier in den Markt vorzudringen, indem Microsoft Windows IoT eingeführt wurde. Die Plattform führt jedoch im Moment (Stand: Juli 2017) ein Nischendasein. (Liming & Malin, 2015)

Der Fokus dieser und anderer Betriebssysteme für Consumer-Geräte liegt viel mehr in der hohen Anzahl an unterschiedlichen Services, die bereitgestellt werden, der Benutzerfreundlichkeit und der Kompatibilität zu Software von Drittherstellern. Des Weiteren setzen diese Systeme leistungsstarke Ressourcen voraus, die im Gegensatz zu IoT-Lösungen, vorhanden sind. Anzumerken ist der hohe Energieverbrauch, welcher bei IoT-Produkten problematisch ist, weil oft Geräte zum Einsatz kommen, die eine bestimmte Zeitperiode ohne externe Stromversorgung arbeiten müssen.

Offene und modulare Betriebssysteme, wie Linux, bieten den Vorteil, dass man nur jene Module nutzen kann, die für den Anwendungsbereich notwendig sind, um dadurch Ressourcen und Energie zu sparen. (Küchemann, 2014)

Entscheidend ist dabei, dass die Minimalkonfiguration von Linux einen Memory-Footprint von mindestens 1 Megabyte verlangt. (Micrium Embedded Software, 2013) Dies führt unweigerlich dazu, dass nicht jedes kostengünstige IoT-Endgerät mit einem vollwertigen Linux-Betriebssystem ausgestattet werden kann. Eine weitere notwendige Eigenschaft ist, Echtzeitinteraktionen mittels des Betriebssystems durchführen zu können. Da dies aber ressourcenintensiv ist, wird meist auf Hardwarebausteine gesetzt, die diese Funktionen hardwarenahe bereitstellen. (Hahm, Baccelli, & Tsiftes, 2015)

Abbildung 6 illustriert die Eingliederung des Betriebssystems eines IoT-Produkts in die restliche Architektur. Dazu gehören neben der eigentlichen Applikation auch Cloud-Applikationen, Treiber und Steuerungssoftware für Sensoren und Aktoren, Kommunikationsschnittstellen, Sicherheitsimplementierungen auf Hardwarebasis und ein Power-Management.

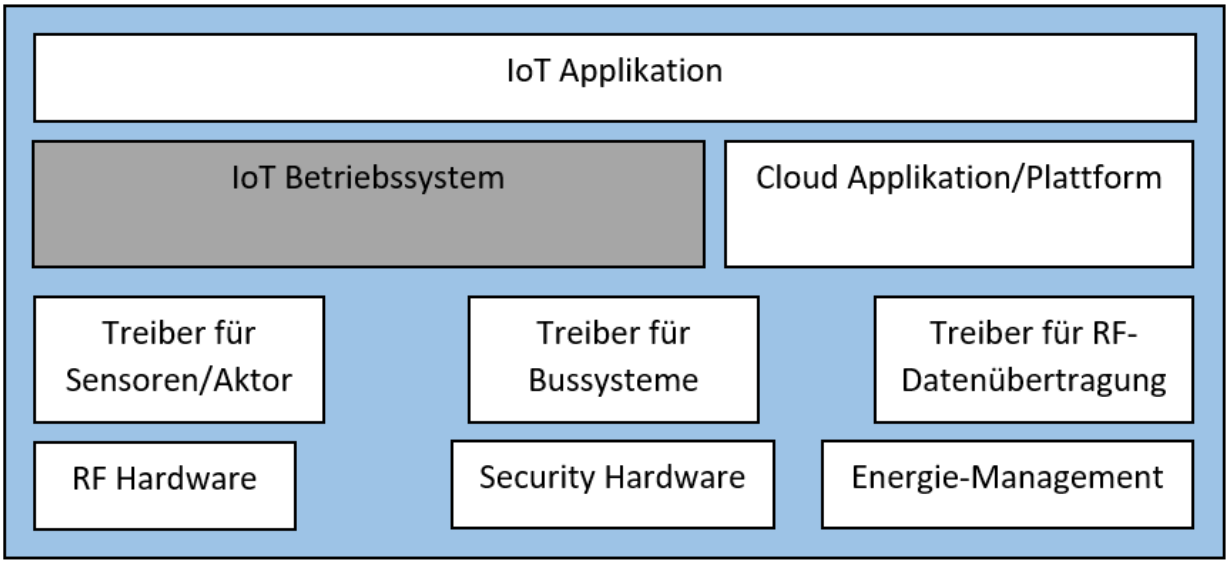


Abbildung 6 Eingliederung IoT-Betriebssystem in ein IoT-System (Jordan, 2015)

Eine Umfrage aus dem Jahr 2017, durchgeführt durch die Eclipse IoT Working Group, ergab, dass von 713 Personen, die im Bereich IoT tätig sind, über 80% Linux als Basis für ihre IoT-Produkte und Lösungen nutzen. Auf Rang zwei sind direkt auf dem Flash-Speicher geschriebene Programme, die in keiner Art und Weise über ein dezidiertes Betriebssystem verfügen. Die nächsten Plätze teilen sich Windows, und einige Linux Derivate. (Skerrett, 2017) (vergleiche Abbildung 7)

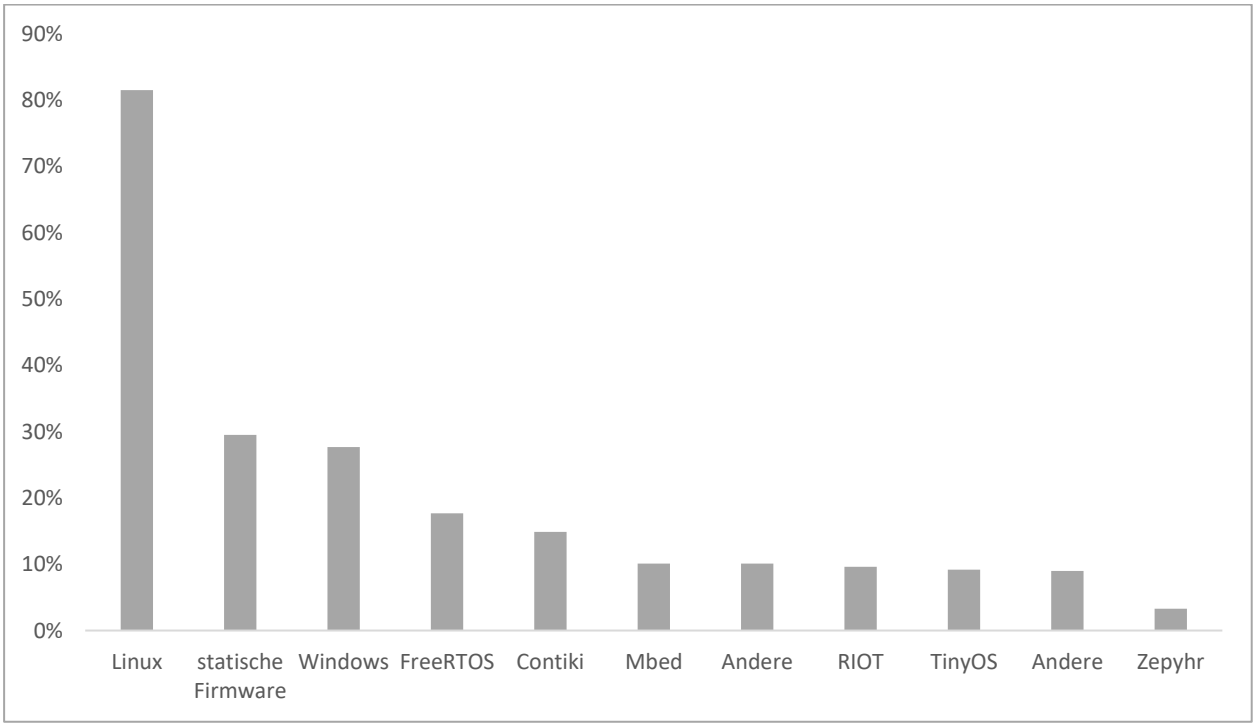


Abbildung 7 Verteilung IoT Betriebssysteme (Skerrett, 2017)

Die Verteilung zeigt, dass immer mehr Entwicklerinnen und Entwickler auf Betriebssysteme setzen, die einen größeren Funktionsumfang besitzen, als Betriebssysteme für eingebettete Systeme. Zu den eingebetteten Systemen zählen FreeRTOS (Free Real Time Operating System)

(FreeRTOS, 2016), Contiki (Contiki-Os, 2017), Mbed (ARM mbed OS, 2017), RIOT (Robuts Internet of Things) (RIOT-OS, 2017) oder TinyOS (GitHub, 2017).

All diese Betriebssysteme für eingebettete Systeme verfügen über die Grundfunktionalitäten, um IoT Aufgabengebiete abdecken zu können. So besitzen sie Implementierungen der notwendigen Protokolle, wie IPv4, TCP (Transmisson Control Protocol) und HTTP (Hyper Text Transfer Protocol). Aufgrund der Kompaktheit und Ressourcenknappheit, die bei diesen Systemen herrscht, fehlen häufig essentielle Sicherheitsmechanismen. (Küchemann, 2014)

2.3.3 Cloudkomponenten und Plattformen

Neben dem eigentlichen Betriebssystem bieten immer mehr IT-Unternehmen, Cloudkomponenten und Plattformen für IoT an. Eine Umfrage aus dem Jahr 2016, durchgeführt durch ein Konsortium von IoT Eclipse, IEEE und Agile, ergab folgende Verteilung der genutzten IoT Plattformen. (Skerret, 2016)

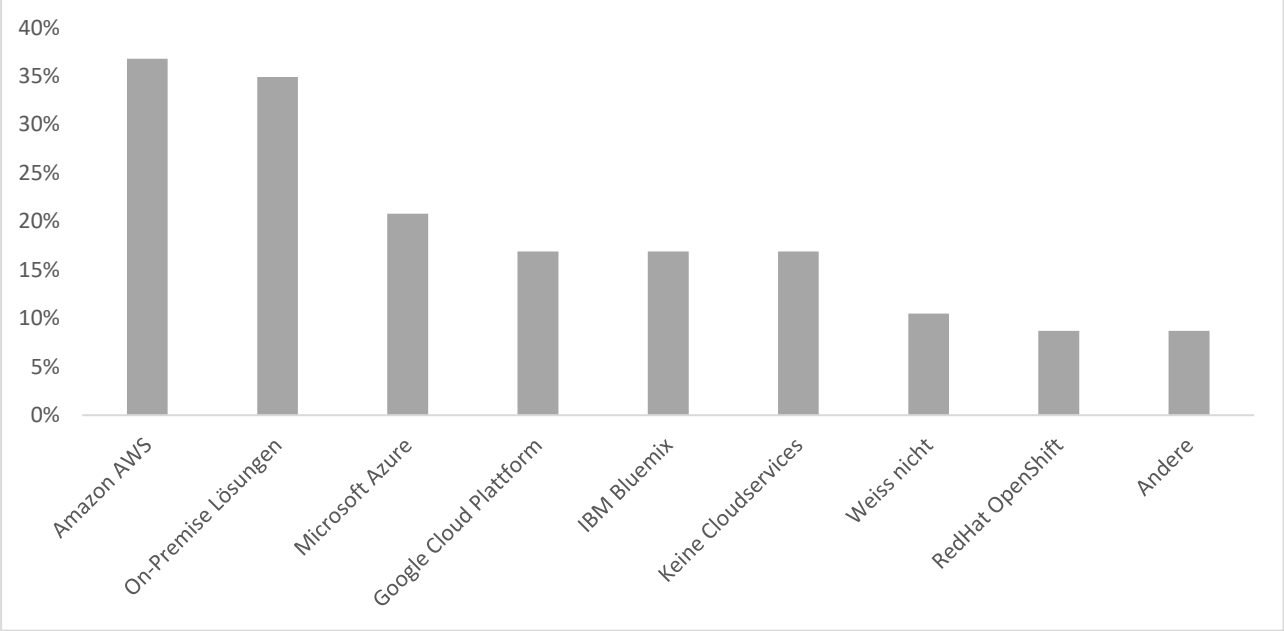


Abbildung 8 Verteilung: IoT Cloudplattformen (Skerret, 2016)

Ersichtlich ist der Trend hin zu Cloudplattformen, die wie Amazon AWS (Amazon Web Services) oder Microsoft Azure bereits unterschiedlichste Funktionalitäten mit sich bringen und dadurch einen wesentlichen Beitrag zur schnellen Implementierung neuer IoT-Lösungen bereitstellen.

Plattformen wie Amazon AWS bieten neben der reinen Implementierung von IoT-Applikationen auch eine sichere Kommunikation zwischen den einzelnen Endgeräten und der Cloud an. (Walker, 2015)

Amazon AWS bietet zwei Möglichkeiten zur Integration von IoT-Produkten in die Cloud-Services. Zum einen besteht die Möglichkeit, mittels Rule-Engines mit den verknüpften Web-Services zu kommunizieren. Ein Beispiel wäre ein smartes Trafficmanagement, bei welchem Sensoren, Fahrzeuge in einem bestimmten Umkreis, über bestimmte Ereignisse informieren. (Amazon AWS, 2017)

Zum anderen wären Device Shadows möglich, bei dem in von Amazon bereitgestellten Web-Services, virtuelle Abbilder von IoT-Produkten erzeugt werden. Diese Abbilder oder virtuellen Stellvertreter speichern jegliche Informationen, welche das reale Produkt erfasst. Dadurch wird eine dauerhafte Kommunikation zwischen der Anwendung und dem Gerät gewährleistet, weil ein ständiger Synchronisierungsprozess dies überwacht. (Amazon AWS, 2017)

An zweiter Stelle der referenzierten Umfrage sind On-Premise Lösungen, also jene, die von Unternehmen und Privatpersonen selbst entwickelt und gewartet werden. Da es hier keine einheitlichen Standards in der Verarbeitung, Speicherung und Kommunikation der Daten gibt, kann auf diese Form der IoT-Plattform nicht näher eingegangen werden.

Die Microsoft Azure Cloud, also jene Cloud-Komponente, die im Zusammenhang mit IoT verwendet wird, ist laut Umfrage auf Platz drei. Diese Cloudplattform basiert auf einer, von Microsoft, entwickelten IoT-Referenzarchitektur. (Microsoft, 2016) Die Komponenten der Plattform sind in Abbildung 9 symbolhaft dargestellt.

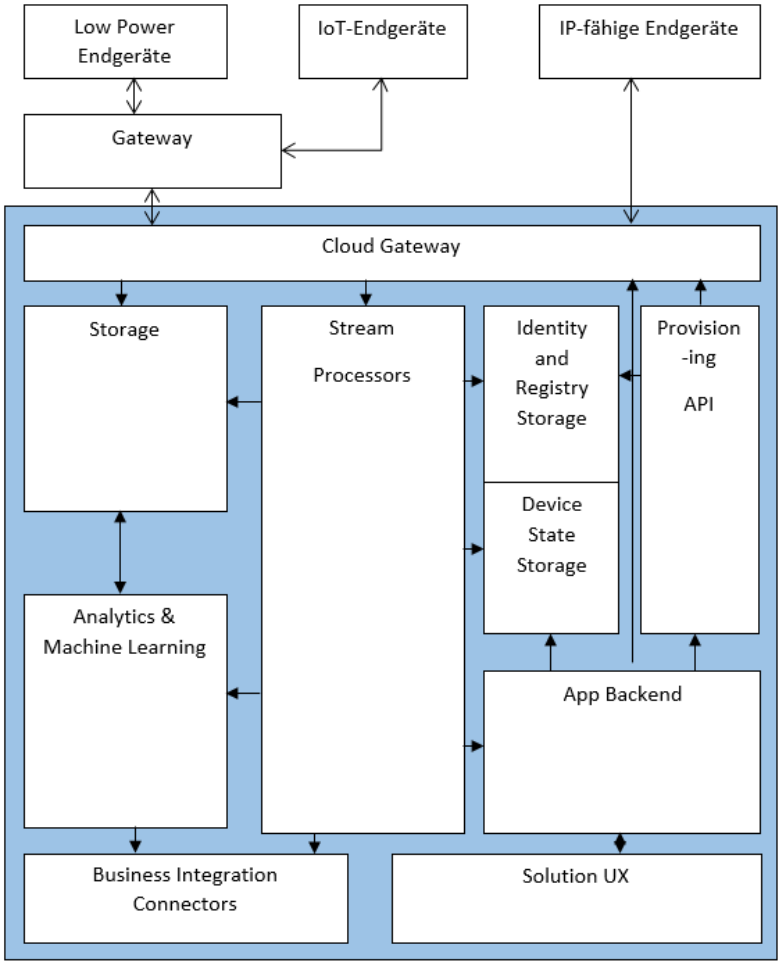


Abbildung 9 Microsoft Azure Cloud Architektur (Microsoft, 2016)

Die wichtigsten Komponenten der Microsoft Azure Cloud werden nach (Microsoft, 2016) in den folgenden Punkten erläutert.

- Cloud Gateway
    - Das Cloud Gateway stellt die Anbindung der IoT Endgeräte bereit und übernimmt, wenn notwendig, Anpassungen und Konvertierungsschritte von verschiedenen Übertragungsprotokollen. Des Weiteren regelt es die Authentifizierung und Autorisierung. Die Abfolge, sowie die Anzahl der Konvertierungsschritte können, je nach Einsatzszenario, variieren.
- Device Provisioning API (Application Programming Interface)
    - Die Hauptaufgabe der Device Provisioning API liegt darin, den Zugriff auf das Device Identity and Registry Store zentral zu regeln. Zudem bietet es die Möglichkeit, neue IoT-Endgeräte, den in der Cloud gehosteten Applikationen zur Verfügung zu stellen.
- Device Identity & Registry Store
    - Im Device Identity & Registry Store werden zentrale Informationen über die Identitäten der einzelnen IoT-Anwendungen abgelegt. Hier werden die notwendigen Informationen gespeichert, die für die Autorisierung und Authentifizierung benötigt werden.
- Data Flow & Stream Processing
    - Im Modul Data Flow & Stream Processing werden alle Datenströme, die für die IoT-Anwendungen benötigt werden, koordiniert und gesteuert. Des Weiteren werden unterschiedliche Kommunikations- und Datenaustauschprotokolle zwischen den Applikationen orchestriert und überwacht.
- Solution UX (User Experience)
    - Das Solution UX Modul beschreibt all jene Funktionen, welche mit der direkten Interaktion mit der eigentlichen Nutzerin und dem eigentlichen Nutzer in Verbindung stehen. Dies kann im einfachsten Fall, eine Website, aber auch eine multifunktionale Applikation für mobile Endgeräte sein.
- App Backend
    - Im App Backend findet sich die gesamte Business-Logik der IoT-Anwendungen. Hier wird auch die Kommunikation unter den einzelnen Applikationen abgebildet.
- Data Analytics
    - Da im IoT-Bereich eine große Menge an unterschiedlichen Daten generiert wird, wurde das Modul Data Analytics geschaffen, das die Daten für Big Data-Algorithmen aufbereitet und bereitstellt.

  (Microsoft, 2016)

Diese Architekturbeschreibung kann als allgemein gültig angenommen werden, da die anderen Plattformen eine ähnliche Struktur aufweisen. (International Electrotechnical Comission, 2015) Die Plattformen unterscheiden sich ansonsten nur in der Aufteilung und Bezeichnung der einzelnen Module, die Kernfunktionalitäten selbst, sind jedoch ähnlich.

2.3.4 Datenübertagung

Laut IOT Developer Survey (Skerret, 2016) sieht die Verteilung der eingesetzten Übertragungsmedien und Schnittstellen wie folgt aus: (vergleiche Abbildung 10)

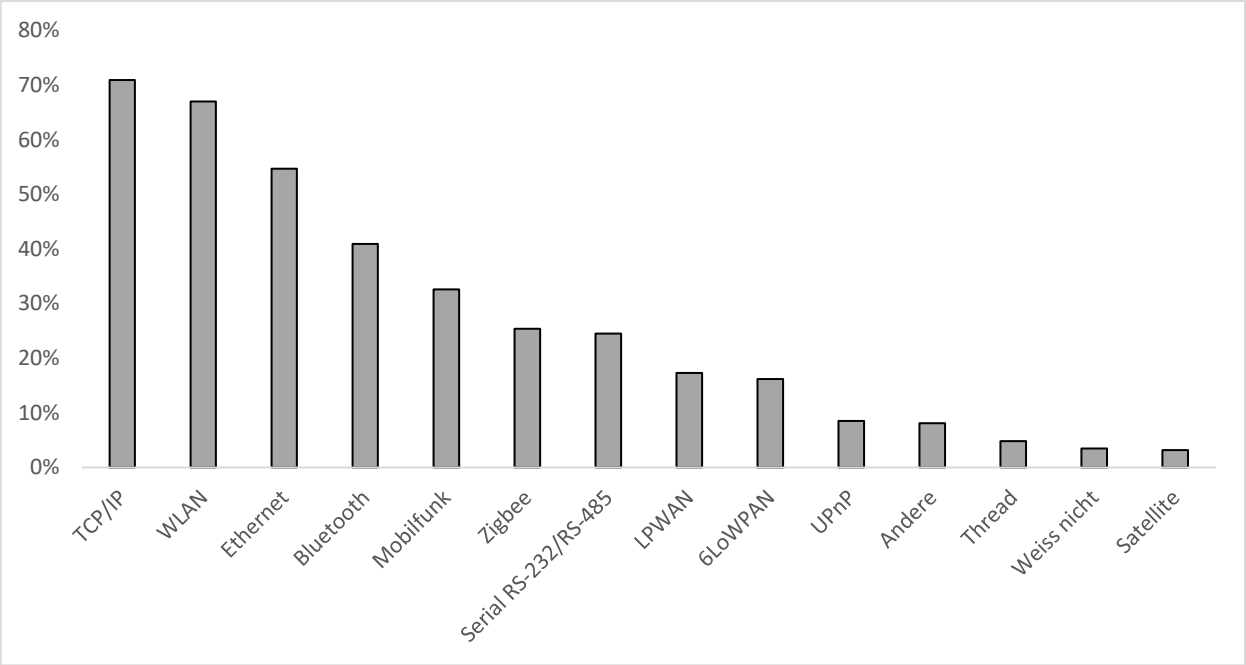


Abbildung 10 Verteilung: Übertragungsmedien und Schnittstellen (Skerret, 2016)

Diese Verteilung zeigt, dass mehr als die Hälfte der Befragten auf Standardprotokolle und Übertragungsmedien setzt. Dazu gehören neben TCP/IP (Kale, 1991), WLAN (Wireless Area Network) mit den dazugehörigen Übertragungsstandards, Ethernet (IEEE, 2017), Bluetooth und Mobilfunk-Technologien. Diese Technologien sind im Fachwissen bekannt und bedürfen keiner näheren Beschreibung. Sie werden jedoch im Kapitel IoT-Security Framework nochmals aufgegriffen, weil hier entscheidende Voraussetzungen gegeben sein müssen, um über diese Technologien eine sicherere Kommunikation gewährleisten zu können.

ZigBee, welches an sechster Stelle der Umfrage (Skerret, 2016) rangiert, ist eine Spezifikation für kleinräumige, drahtlose Netzwerke, das für geringe Datenmengen gedacht ist. Die Reichweite liegt im Bereich von 10 bis 100 Metern. (Zigbee, 2012)

Die wesentlichen Einsatzszenarien von ZigBee liegen in der Automatisierung von Häusern, im Aufbau von Sensornetzwerken und in Steuerungsanlagen im industriellen Umfeld. ZigBee selbst hat in seiner Spezifikation drei unterschiedliche Rollen vorgesehen, welche ein ZigBee-Produkt darstellen kann.

- ZigBee Coordinator
    - Diese Rolle übernimmt die Konfiguration eines ZigBee Netzwerkes mit vorab definierten Parametern. Ist dies erfolgt, wechselt das ZigBee-Endgerät in die Rolle eines ZigBee-Routers.
- ZigBee Router
    - Ein ZigBee Router oder die Rolle des ZigBee Routers übernimmt das Routing der Pakete durch das ZigBee Netzwerk. Existiert bereits ein Router in einem Netzwerk, meldet sich der neue Router bei diesem an.
- ZigBee End Devices
    - Diese Rolle übernehmen jene ZigBee Endgeräte, welche ihre Daten über das Netzwerk kommunizieren. Sie melden sich beim erstmaligen Verbinden bei einem ZigBee Router an und treten auf diese Art und Weise dem Netzwerk bei. Dieser Router stellt immer das Gateway dar, über dieses das Endgerät mit den anderen Teilnehmern kommuniziert.

(Farahin, 2008)

Aufgrund der Vielzahl an Einsatzszenarien, in denen ZigBee Netzwerke, verwendet werden können, wurden durch die ZigBee Alliance Profile definiert, die unterschiedliche Systemvoraussetzungen miteinschließen. (Zigbee, 2012) Diese Anwendungsprofile gliedern sich in vier Hauptgruppen, welche den jeweiligen Anwendungsgebieten zugeordnet werden. Darunter befinden sich die entsprechenden Teilgebiete und Teilanwendungsprofile, die die spezifischen Anwendungsszenarien darstellen.

ZigBee IP	ZSE 2.0	ZigBee Smart Energy
	ZGP	ZigBee Green Power
ZigBee RF4CE	ZRC	ZigBee Remote Control
	ZID	ZigBee Interface Devices
ZigBee Pro	ZLL	ZigBee Light Link
	ZHA	ZigBee Home Automation
	ZBA	ZigBee Building Automation
	ZTS	ZigBee Telecom Services
	ZRS	ZigBee Retail Services
	ZHC	ZigBee Health Care
	ZSE 1.x	ZigBee Smart Energy

Tabelle 2 ZigBee Anwendungsprofile (IT Wissen, 2015)

Die Profile sollen gewährleisten, dass die Endgeräte jeweils den Anforderungen entsprechen und es so zu keinen Schwierigkeiten beim Einsatz von ZigBee kommt.

In den letzten Jahren hat sich jedoch immer mehr das ZigBee Pro Anwendungsprofil bei den Herstellern durchgesetzt. Dies wird am häufigsten im Bereich von IoT eingesetzt. (Zigbee, 2012) Eine Weiterentwicklung, ZigBee 3.0, das auf ZigBee Pro basiert, bietet die bereits verfügbaren Funktionen und erweitert diese mit der Möglichkeit, alle Anwendungsprofile in einem Netzwerk zu vereinen. (Links, 2015)

Des Weiteren sind 250 unterschiedliche Nodes in einem ZigBee Pro Netzwerk möglich, sowie Mechanismen, falls Router im Netzwerk ausfallen, und diese Aufgabe anschließend von anderen übernommen wird. (NXP, 2016)

WLAN, Ethernet, Bluetooth und ZigBee werden im darauffolgenden Kapitel im Hinblick auf Sicherheit analysiert, indem Sicherheitsprobleme in existierenden IoT-Objekten aufgezeigt werden, die diese Technologien nutzen. Dies wird die Basis für das letzte Kapitel darstellen, indem das IoT-Security Framework entwickelt wird.

2.3.5 Datenaustauschformate

Um die Daten von und zu dem IoT-Produkt transportieren zu können, wurden verschiedene Standards zum Datenaustausch geschaffen. Die Architektur von IoT erlaubt eine horizontale Kommunikation. Um dies gewährleisten zu können, damit beispielsweise Endgeräte-übergreifende Workflows funktionieren, müssen Interfaces und Datenaustauschformate zwischen den einzelnen IoT-Endgeräten, Gateways und Cloudplattformen etabliert werden.

Diese Protokolle und Datenaustauschformate stellen unterschiedlichste Eigenschaften bereit, die je nach Einsatzszenario, implementiert werden. Die Abbildung 11 gliedert symbolhaft IoT-spezifische Protokolle in die Layer des ISO-OSI Modells ein. Die genannten Protokolle sind nicht erschöpfend, sondern stellen eine Auswahl dar. (Russell & Van Duren, 2016)

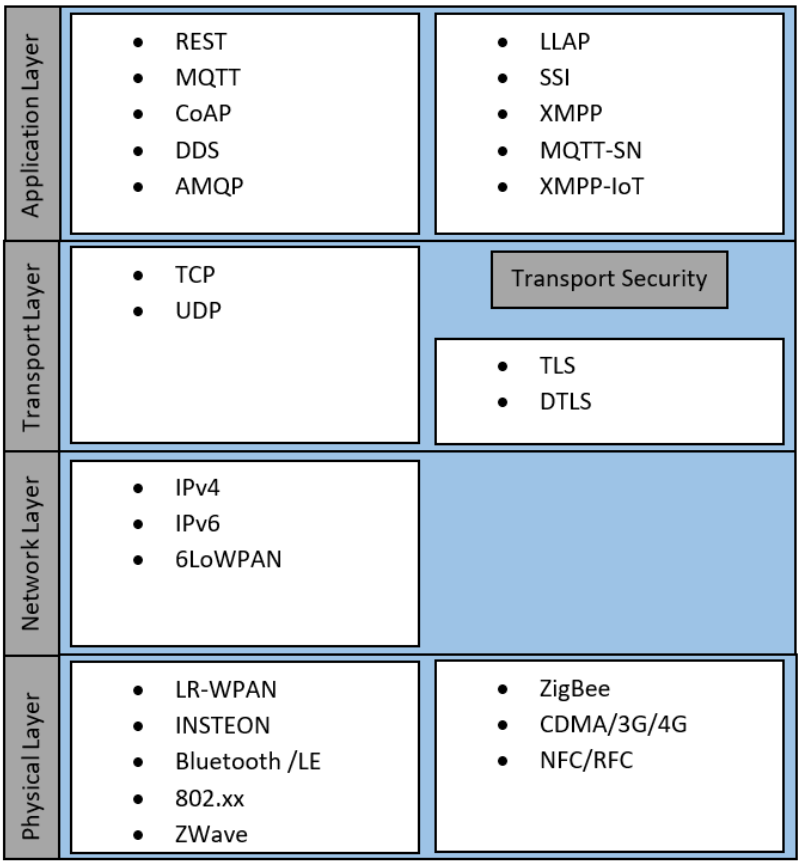


Abbildung 11 Einordnung IoT-Protokolle in das ISO/OSI-Modell (Russell & Van Duren, 2016)

Aufgrund der Vielzahl an Datenaustauschformaten und Messaging-Protokollen werden in diesem Abschnitt nur die am meist verbreiteten näher beleuchtet. Als Grundlage dient, wie in den vorherigen Abschnitten, die IoT-Survey aus dem Jahr 2016. (Skerret, 2016)

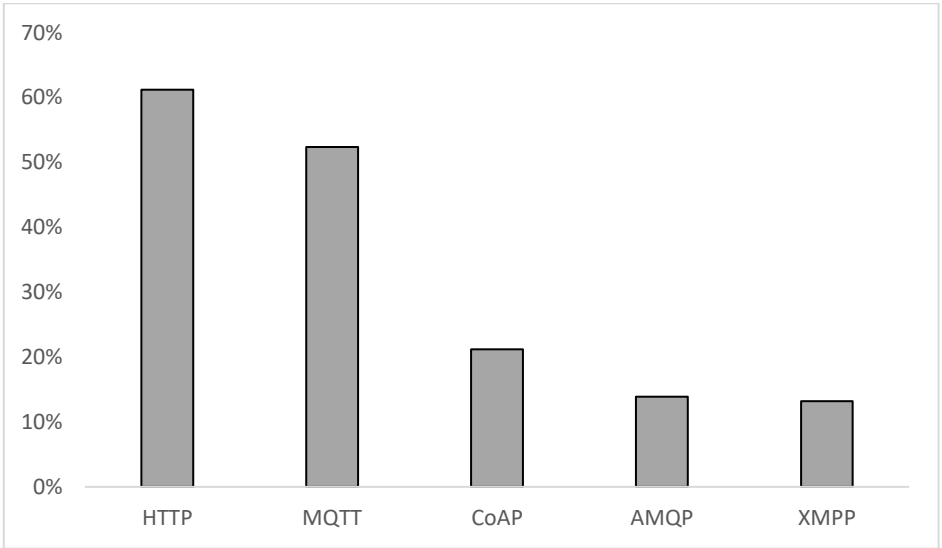


Abbildung 12 Verteilung: Austauschformate im IoT-Sektor (Skerret, 2016)

Laut dieser Umfrage nutzen 61,2% der Entwickler HTTP mit dazugehörigen REST (Representational State Transfer) –Schnittstellen, gefolgt von MQTT (Message Queue Telemetry Transport) mit 52,4%, danach CoAP (Constrained Application Protocol) mit 21,2% und AMQP

(Advanced Message Queuing Protocol) mit 13,9%. An letzter, dennoch erwähnenswerter Stelle, mit 13,2% liegt XMPP (Extensible Messaging and Presence Protocol), welches XML (Extensible Markup Language) basierend ist. Auf HTTP (Fielding, et al., 1999) und REST (Richardson & Ruby, 2007) wird in der weiteren Ausführung verzichtet, weil es sich um Standard-APIs handelt, welche die Grundfunktionalitäten des Internets darstellen.

MQTT beschreibt ein Publish/Subscribe Messaging-Modell, bei welchem Klienten sich für ein bestimmtes Thema (Topic) registrieren (subscribe). Dabei wird eine kontinuierliche Verbindung zum Broker-Server aufgebaut, um etwaige Nachrichten empfangen zu können. Die Nachrichten selbst werden zuerst direkt an den Broker gesendet und mit einer Topic-Header Information versehen, anhand welcher der Broker dann diese den einzelnen Abonnenten zusendet. (vergleiche Abbildung 13) Ein Beispiel für eine MQTT-Anwendung wäre ein Sensor-Netzwerk, in dem die Sensoren ihre Daten an den Broker senden und dieser dann diese an die jeweiligen Clients, wie eine Applikation, weiterleitet. (Cohn, Coppen, Banks, & Gupta, 2014)

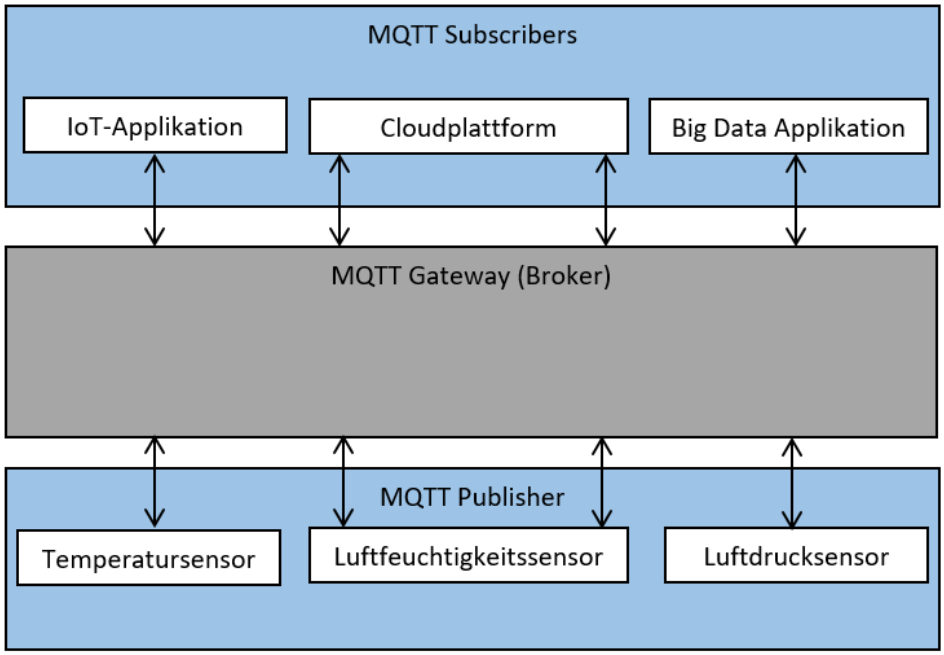


Abbildung 13 MQTT Architektur (Russell & Van Duren, 2016)

CoAP beschreibt ein weiteres IoT Messaging-Protokoll, das im Gegensatz zu MQTT nicht TCP basierend ist, sondern UDP (User Datagram Protocol) nutzt. Es stellt ein Set von unterschiedlichen Message-Typen bereit, die jeweils für spezielle Anwendungsfälle gedacht sind. Die Architektur von CoAP nutzt URI (Uniform Resource Indicators) um die jeweiligen

Klienten im Netzwerk identifizieren zu können. (Shelby, ARM, Hartke, & Bromann, 2014) (vergleiche Abbildung 14)

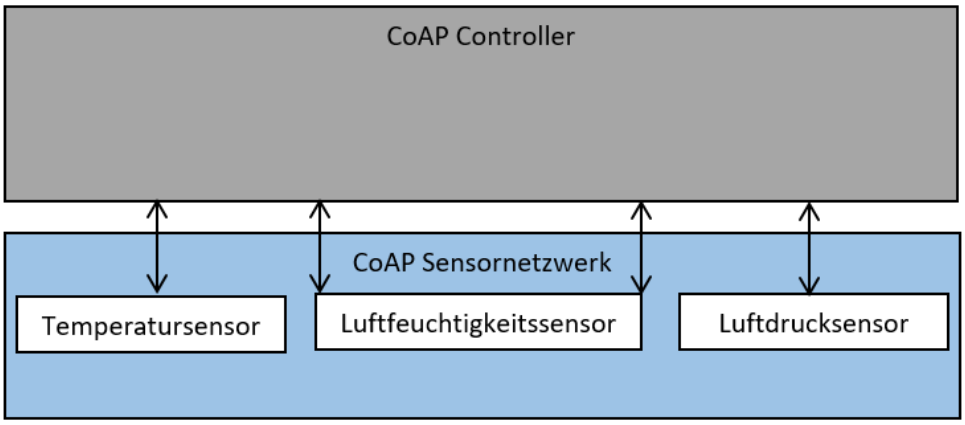


Abbildung 14 CoAP Architektur (Russell & Van Duren, 2016)

Die Paketgröße von CoAP ist kleiner als jene von HTTP-Daten. Bitfelder und Mappings dienen dazu, diese möglichst gering zu halten. Des Weiteren ist CoAP kompatibel zu HTTP und REST-Webressourcen, was durch Proxies, welche die Message-Typen transformieren, realisiert wird. (Jaffrey, 2014)

AMQP wurde entwickelt, um ein Queuing-System in der Server-zu-Server Kommunikation zu etablieren. Außerdem beinhaltet es Funktionalitäten, um einerseits einen Publish/Subscribe-Mechanismus bereitzustellen, andererseits eine Punkt-zu-Punkt-Verbindung zu implementieren. Der Nachrichtenaustausch erfolgt aufgrund der Queuing-Architektur asynchron. Die Nachrichten selbst werden von Erzeugern (Producern) zu Brokern in deren Warteschlange (Queue) übertragen. Die Broker übertragen anhand spezieller Regeln (Bindings) die Nachrichten an die entsprechenden Empfänger (Consumer). Nachrichten selbst werden solange in der Queue gehalten, solange der Empfänger den Erhalt der Nachricht nicht bestätigt hat. Es besteht die Möglichkeit, mit zusätzlichen Metadaten in den Nachrichten, Empfängern spezielle Kommandos zu übermitteln. (AMQP Alliance, 2011)

AMQP stellt vier unterschiedliche Austauschsysteme und Architekturen bereit.

- Topic
    - Vergleichbar mit einem Publish/Subscribe Mechanismus. Die Nachrichten werden in verschiedenen Warteschlangen (Queues) zwischengespeichert und von den Empfängern (Consumer) abgerufen.
- Headerbasis
    - Hier wird auf Basis der Headerinformationen die Nachrichten einer Warteschlange zugeordnet. Dies erlaubt eine granulare Zuordnung und Organisation von Nachrichten.
- Fanout
    - Beschreibt einen Broadcast-Mechanismus, bei dem die Nachricht an alle Warteschlangen übertragen wird.

- Direkt
    - Ist die Default-Architektur von AMQP, bei welcher Nachrichten anhand von Routing-Informationen mit einer Warteschlange verknüpft werden.

(Enz, 2016)

Die Austauschsysteme und Architekturen sind in Abbildung 15 symbolhaft dargestellt.

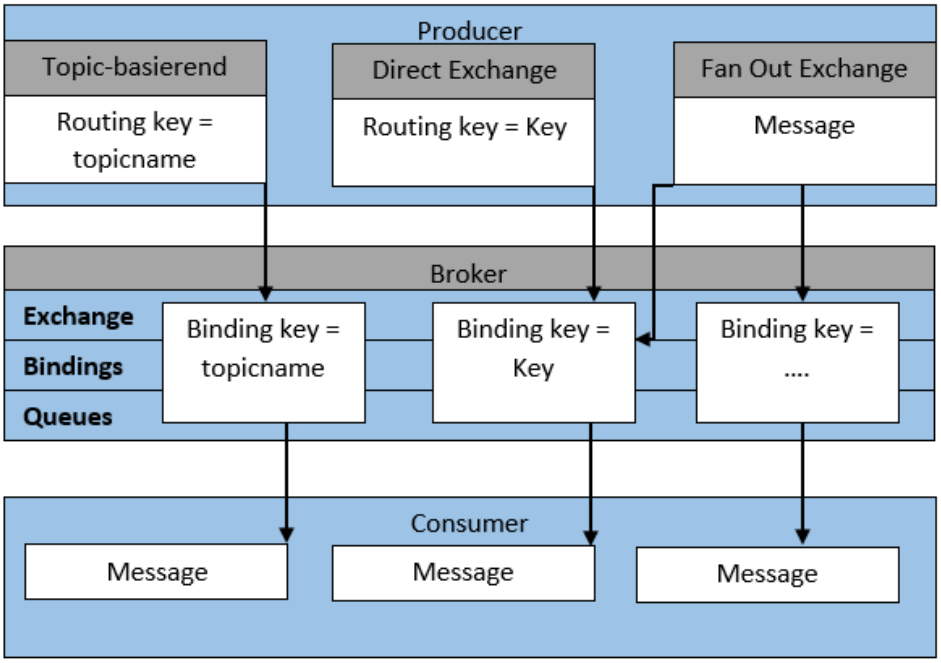


Abbildung 15 AMQP Architekturen (Wulf, 2014)

Aufgrund der Vielzahl an Protokollen und Datenaustauschformaten ist die Interoperabilität zwischen den einzelnen Systemen essentiell, weil es ansonsten, ähnlich wie bei M2M-Konzepten, in abgekapselten Systemen endet. (Zachariah, et al., 2015) Aus diesem Grund werden sogenannte Gateways eingesetzt, die die verwendeten IoT-spezifischen Protokolle in IP-routbare Protokolle transformieren und rücktransformieren. Diese architekturspezifische Eigenschaft birgt neben der Möglichkeit der Interoperabilität, Sicherheitsrisiken. (Folkens, 2014)

Gateways trennen lokale IoT-Netzwerke vom Internet. Sie stellen auch die Verbindung zu Cloudplattformen bereit, wodurch ein abgeschlossenes Ecosystem entsteht, bei dem die Endkundin und der Endkunde keinen Aufwand mehr tätigen muss, um ein funktionierendes System einrichten zu können. (Internet Society, 2015)

2.4 Big Data

IoT führt mit seinem Ansatz, alle Dinge des täglichen Lebens mit dem Internet zu verbinden, unweigerlich zu einer enormen Datenmenge, die generiert wird. Einer Studie von EMC (Gantz & Reinsel, 2013) zufolge steigt die Datenmenge von 2014 bis zum Jahr 2020 um den Faktor zehn.

Der zentrale Treiber, laut EMC-Studie (Gantz & Reinsel, 2013), sei die Sensorik, die in immer mehr Produkten Einzug findet. Dies können beispielsweise sowohl einfache Schrittzähler, als auch komplexe Verkehrssteuerungssyteme sein. Die erzeugte Datenmenge, die durch IoT-Objekte entstanden ist, wird auf aktuell zwei Prozent des weltweiten Datenvolumens geschätzt. Dieser Wert soll sich bis zum Jahr 2020 auf bis zu zehn Prozent verfünffachen. (Vilsbeck, 2014)

Von diesen erzeugten Daten seien laut EMC-Studie nur in etwa 22 Prozent nutzbar. Aus diesen 22 Prozent wird aktuell nur das Potential von fünf Prozent für Wissensgenerierung genutzt. (Gantz & Reinsel, 2013) Das zeigt die Notwendigkeit von intelligenten Algorithmen auf, die anhand von großen Datenmengen, Muster erkennen und daraus Wissen für den jeweiligen Anwendungsfall ableiten.

2.4.1 Einordnung in die IoT-Architektur

In der IoT-Architektur ist die Komponente Big Data in den Datenspeicherungs- und Verarbeitungs-Layer einzuordnen. Big Data-Systeme sind im Backend zu finden, in denen sie die Daten aus den IoT-Produkten erhalten und damit Analysen durchführen. (vergleiche Abbildung 16)

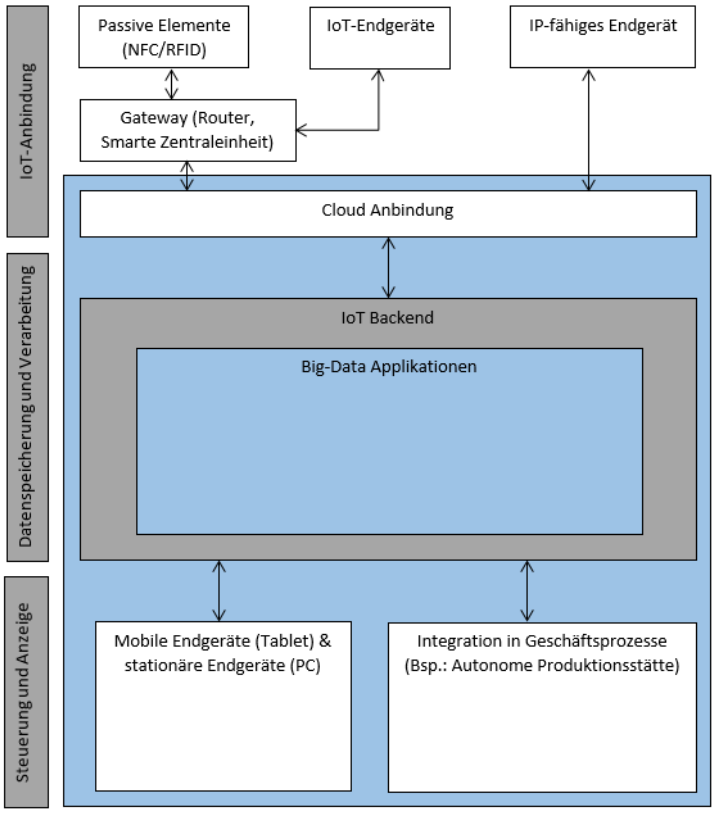


Abbildung 16 Einordnung von Big-Data in die IoT-Architektur (Müller, 2016)

Wie in Abbildung 16 symbolhaft dargestellt, ist Big Data eine Erweiterung des Applikation-Layers. Diese Applikationen sind auf Plattformen in der Cloud bereitgestellt, weil eine On-Premise Lösung für den Privatgebrauch, neben dem erhöhten Wartungs- und Konfigurationsaufwand, kostentechnisch nicht rentabel wäre. (Cecchinel, Jimenenz, Mosser, & Riveill, 2014)

Die Architektur einer Big Data Applikation selbst besteht wiederum aus einem eigenen Ecosystem. Dieses bringt Funktionalitäten zur Datentransformierung und Aufbereitung mit sich, welche vor der eigentlichen Analyse-Applikation geschalten sind. Die Analyse selbst kann mittels unterschiedlicher Algorithmen und Frameworks geschehen (vergleiche Abbildung 17) (beispielsweise Apache Spark (Apache Spark, 2017)). (Maier, 2013)

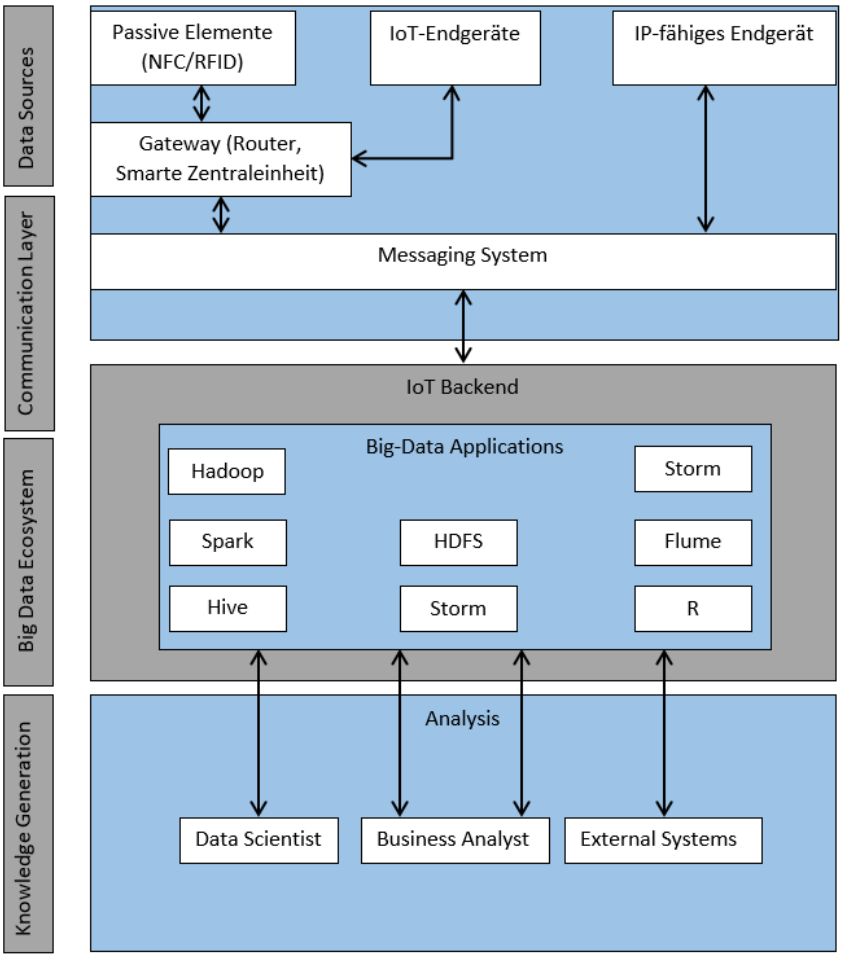


Abbildung 17 Big Data Architektur (Scott, 2015)

Big Data Komponenten selbst und die Plattform, die diese bereitstellt, liegen nicht im Handlungsspielraum der Endkundinnen und der Endkunden, weshalb diese nur für den Enterprise-Bereich (Stand: Juli 2017) von Bedeutung sind. IoT-Endgeräte, die für den Endkonsumenten-Bereich entwickelt wurden, werden, wenn dies überhaupt der Fall ist, mit bereits fertig konfigurierten Zugängen zu Big Data Plattformen ausgeliefert.

Diese stellen bereits vorkonfigurierte Mechanismen und Algorithmen bereit, die für den jeweiligen Anwendungsfall gedacht sind. Es ist jedoch anzumerken, dass einige Hersteller, Daten der angebotenen IoT-Produkte für unternehmenseigene Zwecke nutzen und hierfür Big Data Plattformen verwenden. (Hofmann & Trost, 2015) Da diese nicht in den Einflussbereich der

Endkundinnen und Endkunden fällt, wird auf eine weitere Ausführung verzichtet. Es wird allerdings nochmals in Bezug auf Datenschutz und Datensicherheit im folgenden Abschnitt der Aspekt beleuchtet, wenn die erfassten Daten missbräuchlich verwendet werden.

2.4.2 Risiken durch den Einsatz von Big Data

Der Einsatz von Big Data erlaubt es, Daten aus verschiedene Datenquellen, in unterschiedlichen Formaten, die in großer Menge vorliegen zu bearbeiten und analysieren. (Ward & Barker, 2013) Nutzt man diese neuen Möglichkeiten mit Daten, die durch IoT-Objekte erzeugt wurden, ergeben sich neben den Vorteilen, Muster und Verhalten zu erkennen, auch Nachteile, wie dem Tracking von Personen und deren Verhalten. (Strauß, 2015)

Dies geschieht häufig wegen der Tatsache, dass AGBs (Allgemeine Geschäftsbedingungen) nicht oder unvollständig gelesen werden und dadurch ein ungewolltes Sammeln von Daten stattfindet. Durch die wachsende Verbreitung von IoT-Produkten in den Haushalten vieler Menschen werden häufig große Datenmengen unbewusst erzeugt, die womöglich der einzelnen Person keinen Vorteil bringt, kombiniert man diese aber mit Daten anderer, lassen sich Muster erkennen, welche eventuell Teil der eigenen Persönlichkeit sind. (Weichert, 2013)

Problematisch erscheint zudem, dass Daten als das neue Öl bezeichnet werden. (Berger, 2017) Dies führt dazu, dass Unternehmen durch den Konkurrenzdruck gezwungen werden, die Daten ihrer Kunden zu analysieren. Diese Daten werden häufig als Telemetrie-Daten bezeichnet, die dazu genutzt werden, das eigene Produkt und die damit verbundenen Services zu verbessern. (Da Cunha, Agard, & Kusiak, 2006)

Ein weiteres Problem stellen die Plattformen und Datenmengen an sich dar. Diese können infolge fehlerhafter oder nicht korrekt gewarteter Sicherheitssysteme von unbefugten Dritten kompromittiert und für kriminelle Zwecke verwendet werden. (Pa Pa, et al., 2015)

Sobald Daten in großen Mengen, auch in anonymisierter Form, vorliegen, ist es möglich diese mit unterschiedlichsten Verfahren und Mining-Methoden zu de-anonymisieren. Eine Studie aus dem Jahr 2015 verwendete anonymisierte Kreditkartentransaktionen, die durch 1,1 Millionen Personen erzeugt wurden, um diese wieder den jeweiligen Personen zuordnen zu können. Das Ergebnis zeigte, dass diese Datenmenge ausreichte, um ca. 90% der Transaktionen wieder den Urheberinnen und Urhebern zuordnen zu können. (de Montjoye, Radaelli, Singh, & Pentland)

Wenn man diese Studie auf den Sektor von IoT überträgt, besteht hier ebenfalls die Gefahr der De-Anonymisierung. In keinem IT-Sektor weltweit sind die Datenzuwachsraten so groß, wie bei IoT. (Gantz & Reinsel, 2013) Kriminelle, Hacker oder staatsnahe Geheimdienste können sich dieser Daten mächtig machen und für jegliche Zwecke verwenden, um daraus Profit schlagen zu können, oder Wissen über die Person selbst und ihrem Verhalten zu generieren.

Aus diesem Grund fordern Datenschützerinnen und Datenschützer bereits seit Jahren klar und eindeutig formulierte AGBs, damit sich eine potentielle Kundin und ein potentieller Kunde über die Gefahren, die durch das Sammeln der Daten bestehen, im Klaren sind. (Ihlenfeld, 2010)

2.5 Einsatzszenarien von IoT

Durch die zunehmende Vernetzung und Verwendung von IoT-Objekten entstehen Möglichkeiten sowohl in allen Bereichen der Wirtschaft, als auch im privaten Kontext, die bisher noch nicht realisierbar waren. In Zukunft werden Wirtschaftssektoren zusammenwachsen, wodurch neue Geschäftsmodelle entstehen könnten.

Wegen der Vielzahl von möglichen Einsatzszenarien und der ständigen Weiterentwicklung der technischen Möglichkeiten wird in diesem Abschnitt auf die wichtigsten Einflussbereiche von IoT eingegangen. Diese wurden in einer Studie, die durch McKinsey in Auftrag gegeben wurde (Manyika, et al., 2015), eruiert. Ergänzt werden diese, aufgrund des Fokus dieser Arbeit, mit dem Einflussbereich im Consumer-Sektor.

Laut dieser Studie zählen zu den drei wichtigsten Einflussbereichen jene der vernetzen Produktionsstätten (bis zu 3,7 Billionen Dollar erzielbarer Mehrwert), der vernetzten und intelligenten Städte (geschätzt auf bis zu 1,7 Billionen Dollar Einsparungspotential) und jene der Gesundheitsbranche (bis zu 1,6 Billionen Dollar Einsparungspotential). Im Gegensatz dazu, auch wenn in den Medien und Fachpublikationen anders angenommen, liegt das Einsparungspotential im Smart Home Bereich, der im Consumer-Sektor angesiedelt ist, nur bei 300 Milliarden Dollar. (Manyika, et al., 2015)

2.5.1 IoT in Produktionsstätten

Industrien und ihre Produktionsstätten sind einem zunehmenden Wandel ausgesetzt. Die Verbreitung von Informationstechnologien wächst in Bereichen, die vor wenigen Jahren noch gänzlich ohne deren Unterstützung ausgekommen sind.

Dies beginnt bei der Anbindung an eine intelligente Stromversorgung (Stichwort: Smart Grid) und reicht bis zur vollständigen Vernetzung aller Produktionsobjekte, die am Wertschöpfungsprozess sowohl direkt als auch indirekt beteiligt sind. (Bi, Xu, & Wang, 2014) Diese umfassende Digitalisierung der Prozesse in den Produktionsstätten soll eine intelligentere, effizientere und Just-in-Time Produktion gewährleisten. (vergleiche Abbildung 18)

Ziel ist es in Zukunft Fertigungsanlagen und Logistikzentren zu entwickeln, welche gänzlich ohne menschliche Interaktion autark arbeiten. Dies soll auf Basis von Sensornetzwerken, autonomen Logistikfahrsystemen und intelligenten Algorithmen aufbauen und mittels M2M-Kommunikation mit anderen externen Systemen, wie beispielsweise einem externen Zulieferer, interagieren. Die Komponente Mensch soll sich in Zukunft gänzlich auf den Bereich der Entwicklung begrenzen und die Fertigung der Komponenten an Maschinen, Robotern und intelligenten Algorithmen übertragen. (Radziwon, Bilberg, Bogers, & Madsen, 2014)

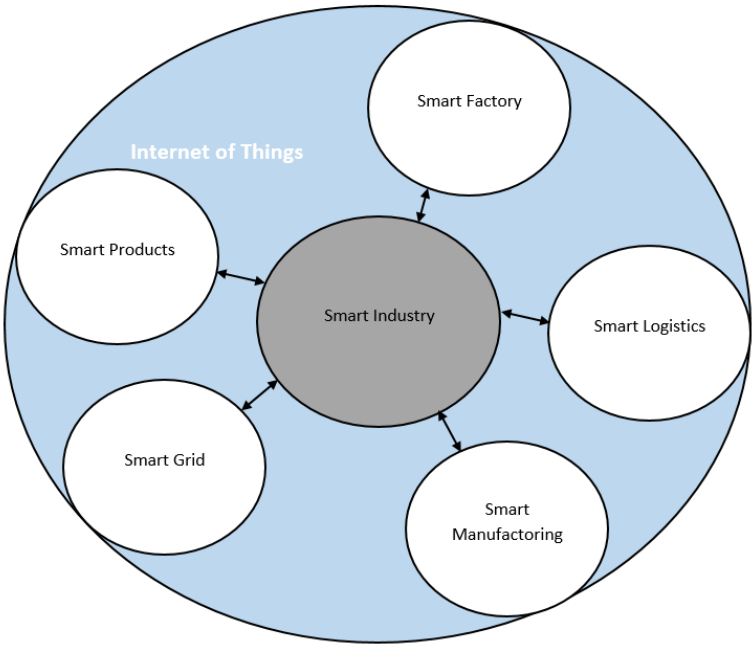


Abbildung 18 IoT und Smart Industry (Feike, 2013)

Neben der Kommunikation unter den einzelnen Objekten im Wertschöpfungsprozess, findet immer häufiger eine Kommunikation zwischen den Fertigungsanlagen und dem eigentlichen Produkt statt. So werden in Produktionsstätten der Automobilindustrie Fahrzeuge mit einem Barcode oder RFID-Tag versehen, wodurch eine neue Form der Transparenz im Produktionsablauf geschaffen wurde. (Baudin, 2005)

Eine weitere und schon weit verbreitete Anwendung von IoT in der Industrie ist die, der Preventive Maintenance. Dies beschreibt den Ansatz einer vorrausschauenden Instandhaltung, bei welchem Sensordaten ständig auf Muster von Verschleißerscheinungen analysiert und überwacht werden. (Xiaoli, Yunbo, & Guoxin, 2011) Das senkt die Zahl an ungeplanten Standzeiten um durchschnittschlich zwei Prozent. (Ismail & Paqin, 2013)

In Kombination mit Sensorwerten unterschiedlicher Produktionsanlagen und Big Data Algorithmen wird aus Preventive Maintenance, Predictive Maintenance. Diese nutzt mathematische Modelle, um vorherzusagen welche Bau- und Verschleißteile in welchem Zeitraum ausgewechselt werden müssen, um die Zeit des Produktionsstillstands so gering wie möglich halten zu können. (Xiaoli, Yunbo, & Guoxin, 2011)

2.5.2 IoT im urbanen Raum

Die städtische Infrastruktur ist im Begriff sich zu wandeln. Mehr und mehr Menschen ziehen in den großstädtischen Raum. Das Verkehrsaufkommen, das dadurch entsteht, lässt sich nicht mehr mit einfach getakteten Ampelregelungen kontrollieren. Es müssen moderne IoT-Architekturen eingesetzt werden, um den Verkehr am Fließen zu halten, sowie vorhandene Ressourcen und Infrastrukturen effizient nutzen zu können. (Foschini, Taleb, & Corradi, 2011)

Ein weiteres Einsatzszenario von IoT im städtischen Umfeld ist die Infrastruktursysteme granularer zu überwachen und steuern. Dazu gehören neben der bereits erwähnten Verkehrsinfrastruktur, Strom- und Wasserleitungen sowie das Abflusssystem. So können Daten, die mithilfe von Sensoren generiert wurden, bei der Entscheidungsfindung bei Wartungs- und Erweiterungsprojekten unterstützen. (Vermesan & Friess, 2014)

Des Weiteren können intelligente Parksysteme, die Sensoren, Displays und Cloudkomponenten nutzen, für weniger Verkehr auf den Straßen sorgen und eine effizientere Auslastung der örtlichen Infrastruktur gewährleisten. Wenn Sensoren ihren Status an Apps oder direkt an Fahrzeuge senden, könnte man neben dem Verkehr auch den CO^2-Austoss verringern. (Vermesan & Friess, 2014)

Intelligente Abfallbehälter können bei der Organisation der örtlichen Abfallentsorgung helfen, diese so effizient wie möglich zu gestalten. Dadurch kann jeder Behälter sein Gewicht für Abrechnungszwecke speichern, selbstständig eine Entleerung organisieren, oder der Eigentümerin und dem Eigentümer eine Mitteilung senden, falls dieser die Mülltrennung nicht ordnungsgemäß durchführt. (Medvedev, Fedchenkov, Zaslavsky, Anagnostopoulos, & Khoruzhnikov, 2015)

Durch die Adaptierung bestehender Stromnetze zu intelligenten Stromnetzen können die Erzeugung, Verteilung und Speicherung von elektrischer Energie besser organisiert werden. Dies wird, aufgrund von steigender E-Mobilität und dezentralen Photovoltaik-Anlagen, essentiell, um die Stabilität des Netzes gewährleisten zu können. (SmartGrid, 2015) Des Weiteren kann durch intelligente Beleuchtungssysteme, die nur bei Aktivität im näheren Umfeld aktiviert werden, der Energieverbrauch gesenkt werden. (Vermesan & Friess, 2014)

2.5.3 IoT im Gesundheitswesen

Der Gesundheitssektor sieht sich immer größer werdenden Herausforderungen gegenüber. Durch die steigende Lebenserwartung der Bevölkerung werden menschliche Ressourcen in der Gesundheitsversorgung knapp. (Nowossadeck, 2012)

Aus diesem Grund wird die IT-unterstützte Pflege und Behandlung wichtig, um der steigenden Anzahl an chronisch kranken Patientinnen und Patienten Herr zu werden. (Nowossadeck, 2012) Die medizinische Unterstützung soll zum richtigen Zeitpunkt, am richtigen Ort jeder Person zur Verfügung stehen und deren Lebensqualität verbessern. Des Weiteren ist dies unter dem Gesichtspunkt einer effektiven und effizienten Leistungserbringung zu betrachten. (Maksimovic, Vujovic, & Perisic, 2015)

Telemonitoring, das durch vernetzte Sensoren am und im Körper aktuelle Vitaldaten der Patientinnen und Patienten liefert, sorgt für eine kontinuierliche Krankheitsverlaufserfassung. Die Daten werden zentral in KIS (Krankenanstalten Informationssystemen) gespeichert und stehen dort für das behandelnde Personal bereit. Dadurch können die Behandlungsqualität und das daraus resultierende Behandlungsergebnis verbessert werden, ohne den Personalstand vergrößern zu müssen. Das Personal selbst kann sich auf die eigentlichen pflegerischen

Tätigkeiten konzentrieren und wird nicht durch notwendige Dokumentationsaufgaben behindert, die von den IoT-Objekten durchgeführt werden. (Chiuchisan, Costin, & Geman, 2014)

Des Weiteren können Sensoren zur Fernüberwachung von chronisch kranken Patientinnen und Patienten eingesetzt werden. Dieser Ansatz nennt sich AAL (Ambient Assisted Living), bei dem Patientinnen und Patienten, medizinische Sensoren tragen und damit wichtige Vitalparameter erfassen. Dies kann mit Umgebungssensoren ergänzt werden, die Stürze erkennen und Alarme absetzen können. (Dohr, Modre-Opsrian, & Drobics, 2010)

Die dabei erzeugten Daten werden lokal gesammelt und an medizinische Einrichtungen, falls dies gewünscht ist, übertragen. Dort können die Daten verarbeitet und wenn nötig, medizinische Hilfe organisiert werden. (Chiuchisan, Costin, & Geman, 2014)

2.5.4 IoT im Consumer-Bereich

Im Consumer-Bereich, auf welchen diese Arbeit ihren Fokus legt, existiert ein breites Spektrum an IoT-Objekten für jegliche Einsatzbereiche. Dies führt zu einem unübersichtlichen Dschungel an Systemen und Lösungen, die den Markt aktuell überfluten.

Das umfasst Fitnesstracker, Überwachungskameras, intelligente Haushaltsgeräte und ähnliche. Hersteller verknüpfen ihre Produkte mit Cloudapplikationen, damit auf die IoT-Objekte von überall aus, über Hersteller-spezifische Applikationen auf mobilen Endgeräten, zugegriffen werden kann. (Yun, Ahn, & Sung, 2015)

Der Trend hin zum Smart Home treibt die Vernetzung der Eigenheime ebenfalls voran, wodurch in den nächsten Jahren die Anzahl der vernetzten Endgeräte in den Haushalten stark ansteigen wird. Dies wird zu einer Steigerung der Komplexität der einzelnen IT-Infrastrukturen führen und Probleme im Bereich der IT-Sicherheit und des Datenschutzes mit sich führen. (Wurm, Hoang, & Arias, 2016)

2.6 Zusammenfassung

Das IoT-Ecosystem umfasst viele unterschiedliche Technologien, die in Kombination miteinander neue Einsatzszenarien erschließen, die mit bisherigen Methoden und Ansätzen nicht realisierbar waren. Durch den steigenden Vernetzungsgrad und einer immer tiefgreifenderen Digitalisierung aller Bereiche der Wirtschaft und des täglichen Lebens entstehen neue Anwendungsmöglichkeiten. Diese reichen von intelligenten Produktionsstätten bis zu Smart Cities, in welchen Sensoren den täglichen Verkehr regeln und dadurch die Umweltbelastungen reduzieren und vorhandene Infrastrukturen effizienter betreiben.

Die immer größer werdenden Datenmengen, die durch IoT erzeugt werden, können mit aktuellen Verfahren und Algorithmen nicht mehr bewältigt werden, wodurch IoT immer mehr mit dem Themengebiet von Big Data fusionieren wird. Eine weitere wichtige Komponente ist zudem die Cloud, in der sowohl die erzeugten Daten als auch Steuerungs- und Kontrollfunktionalitäten für die Endanwenderinnen und Endanwender bereitgestellt werden.

Darüber hinaus werden in aktuellen IoT-Produkten unterschiedliche Betriebssysteme, Protokolle und Übertragungswege genutzt. Dies führt zu einer fehlenden Interoperabilität unter den einzelnen Herstellern und deren Plattformen. Offen dokumentierte Standards wie MQTT versuchen dem entgegenzuwirken. Es wird aber noch Zeit in Anspruch nehmen, bis sich die Hersteller auf ein Übertragungsprotokoll geeinigt haben. Dies wird in Anbetracht der unterschiedlichen Einsatzgebiete und Szenarien durchaus eine Herausforderung sein, weil jeder Übertragungsweg und jedes Datenaustauschformat seine Vor- und Nachteile aufweist.

Vielmehr werden sich übergeordnete Standards durchsetzen, in der IoT-Gateways und Cloudplattformen unterschiedlicher Hersteller und Betreiber miteinander kommunizieren. Erste Schritte in diese Richtung wurden im Beispiel der Microsoft Azure Cloud-Architektur (Abschnitt 2.3.3) aufgeführt. Diese bietet Konvertierungs- und Transformationsfunktionalitäten an, mit deren Hilfe herstellerunabhängig zwischen den einzelnen IoT-Objekten kommuniziert werden kann.

Das erarbeitete Wissen, aus diesem Kapitel, wird im Folgenden, in dem aktuelle Sicherheitsprobleme von IoT-Consumer Produkten analysiert werden, als Basis herangezogen. Dabei wird jeweils ein Produkt eines Marktsegments aufgegriffen, die Schwachstellen der Sicherheitsimplementierungen analysiert, die anschließend für das IoT-Security Framework als Grundlage verwendet werden.

3 ANALYSE VON IOT-OBJEKTEN

Dieses Kapitel beschäftigt sich mit Sicherheitsproblemen und Risiken, die von aktuellen IoT-Produkten ausgehen. Hierbei werden IoT-Objekte aus dem Consumer-Marktsegment in ihrer Funktionalität beschrieben, die technische Architektur analysiert und die Risiken und Gefahren, die von diesem Produkt ausgehen, identifiziert.

Durch IoT verschwimmen die Grenzen zwischen dem Internet und dem realen Leben stärker denn je. Aus diesem Grund werden Angriffe, welche sich gegen die IT-Infrastruktur richten, sich auch immer mehr gegen den Alltag vieler Menschen richten und ein Risiko für die persönliche Sicherheit darstellen.

So können gekaperte IoT-Objekte, die zu einem Verbund an Rechner zusammengeschaltet werden, ganze Rechnernetzwerke durch gezielte DDoS (Distributed Denial of Service) - Attacken lahmlegen. Dies mag zwar für die einzelne Konsumentin und den einzelnen Konsumenten zuerst als unbedeutend erscheinen, heißt jedoch auch, dass diese und dieser für Schäden, die durch ihr und sein Eigentum entsteht, haftbar gemacht werden kann. (Heinrich, 2005)

Aus diesem Grund werden in diesem Kapitel einzelne Produkte jeden Marktsegments ausgewählt, um die komplexen Gefahren besser darstellen zu können.

Des Weiteren soll die Auswahl an unterschiedlichen IoT-Produkten dazu dienen, um jeweils ein spezielles Angriffsszenario oder eine Lücke in der Sicherheitsimplementierung aufzeigen zu können. Dies wird die Basis für das im Laufe dieser Arbeit entwickelte Security Frameworks sein, welches die einzelnen Problematiken aufgreift und in Risikogruppen gliedert.

3.1 Philips Hue

Das Philips Hue System wurde 2012 auf den Markt gebracht. Zu diesem Zeitpunkt war es nur mit Apple-Produkten kompatibel und wurde deshalb als erstes iOS (IPhone Operating System) gesteuertes LED (Light Emitting Diode) -System beworben. Seit Oktober 2015 ist das Hue System auch für Android-Endgeräte verfügbar.

Der Funktionsumfang des Philips Hue Ecosystem umfasst über mobile Applikationen steuerbare LEDs, die das RGB-Farbspektrum abbilden können und diese über verschiedenste Timer-und Dimerfunktionen kontrollierbar machen.

Die Applikation selbst, wird von Philips auf den diversen App-Plattformen bereitgestellt und verlangt mindestens ein iOS Endgerät ab Version 4.3 oder Android 2.3. Neben der Applikation wird eine Cloudplattform angeboten (www.meethue.com), zu welcher sich die Applikationen verbinden und dort Softwareaktualisierung erhalten können.

Des Weiteren bietet die Cloudplattform eine ortsunabhängige Kontrolle und Fernsteuerungsfunktion der LEDs an. Vordefinierte Beleuchtungsabläufe können mit anderen aus der Community stammenden Personen geteilt werden und Entwicklerinnen und Entwickler

haben die Möglichkeit über eine von Philips bereitgestellte SDK (Software Development Kit) eigene Applikationen zu entwickeln.

Neben den intelligenten LEDs wird ein Gateway, genannt The bridge, angeboten, was die Steuerung von mehreren LEDs erlaubt. Es ist zudem für die Anbindung an die Cloudplattform notwendig, weil es die mittels ZigBee kommunizierenden LEDs mit dem Internet verbindet. (vergleiche Abbildung 19) Es stellt APIs bereit, die eine direkte Ansteuerung der LEDs ohne Cloudplattform, erlauben. Als Übertragungsmedium wird ZigBee Light Link verwendet.

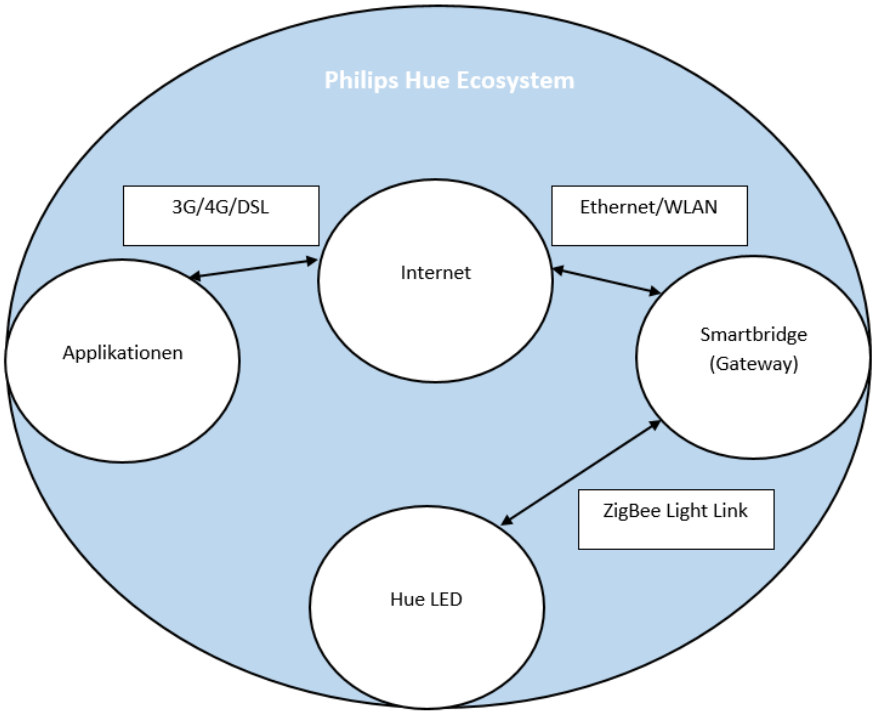


Abbildung 19 Philips Hue Ecosystem

Das Gateway, das die Berechtigungen zu den LEDs verwaltet, stellt Sicherheitsfunktionen bereit und kann bis zu 50 unterschiedliche Hue Endgeräte steuern. (Philips, 2016)

Im Alltagsgebrauch, falls sich die Nutzerin und der Nutzer im Umfeld der LED befinden, baut das Smartphone eine direkte Verbindung zur Bridge über WLAN auf. Ist dies nicht der Fall, muss die von Philips bereitgestellte Infrastruktur genutzt werden, um die IoT-Objekte steuern zu können.

Eine weitere Möglichkeit das Hue System zu steuern, ist die Plattform IFTT (If this than that) zu nutzen. Diese Plattform bietet Schnittstellen zu unterschiedlichen Systemen und IT-Services an und kann übergreifende Regeln und Workflows definieren. So ist es beispielsweise möglich die eigenen Hue Infrastruktur mittels Tweets oder Facebook-Postings zu steuern. (Philips, 2016)

Um über das Internet auf die Hue LEDs zugreifen zu können, muss ein Zugang auf der Philips Hue Webplattform erstellt werden. Der Registrierungsprozess fordert neben einem Namen und einer E-Mail-Adresse, ein Passwort, das eine Mindestkomplexität von sechs Zeichen verlangt.

Diese geringe Mindestlänge bietet ein erstes Einfallstor für Angreifer, weil man mittels Brute-Force Attacke hier nur rund 5 Milliarden unterschiedliche Möglichkeiten hat, um das Passwort erraten zu können. (Schröder, 2017) Brute-Force Attacken werden dadurch begünstigt, indem

man bei zweimaligem falschen Log-In-Versuch, nur eine Minute von einem neuerlichen Login blockiert wird. (Dhanji, 2013)

Als problematisch zeigt sich ebenso die Tatsache, dass viele Konsumentinnen und Konsumenten für viele ihrer virtuellen Zugänge dieselben Passwörter verwenden. Wenn Passwörter auch für IoT-Endgeräte wiederverwendet werden, könnten Angriffe auf IT-Unternehmen und deren Services schwerwiegende Folgen auf das reale Leben vieler Menschen haben.

Ein Szenario, bei dem einem IT-Dienstleister durch einen Angriff Kundendaten abgegriffen wurden und diese im Internet auf diversen Plattformen kursieren, zeigt, dass universal eingesetzte Passwörter, egal für welchen Service sie eingesetzt werden, Auslöser eines Domino-Effektes sein können. Dies kann von finanziellen Schaden bis hin zum vollständigen Verlust des Zuganges zum persönlichen virtuellen, wie auch realen Eigentum führen. (Ives, Walsh, & Schneider, 2004)

Ein weiteres Angriffsszenario kann über, die im vorherigen Abschnitte beschriebene (Abschnitt 3.1) Plattform IFTT durchgeführt werden. Wenn Nutzerinnen und Nutzer ihre Workflows bearbeiten und bereitstellen, könnten Unbefugte, die die Plattform kompromittieren, diese abändern oder gar missbrauchen. (Dhanji, 2013)

Auch die Kommunikation zwischen den LEDs und der Bridge (Gateway), die über das ZigBee Light Link Protokoll erfolgt, kann als Angriffspunkt identifiziert werden. Dazu muss der Masterkey, mit dem der Netzwerkschlüssel erzeugt wird, aufgezeichnet werden. Dies erfordert allerdings, dass sich Angreifer in unmittelbarer Nähe zu den jeweiligen Endgeräten aufhalten müssen, weil ZigBee nur für geringe Reichweiten entworfen wurde. (siehe Abschnitt 2.3.4) (Ronen, O'Flynn, Shamir, & Weingarten, 2016) und (O'Flynn, 2016)

Die oben angeführten Risiken zeigen deutlich mit welchen Konsequenzen zu rechnen ist, wenn grundlegende Dinge des Alltags, wie etwa Licht, mit dem Internet verbunden werden und es smart macht. Zwar zeigt die Update-Politik von Philips, dass sehr schnell auf Anmerkungen aus der Community in Form von Software-Updates reagiert wird, jedoch löst dies erst Probleme, nachdem diese der breiten Öffentlichkeit bekannt sind. (Ries, 2016)

Den Missbrauch von Accountdaten, die durch Brute-Force Attacken, erraten wurden, lässt sich durch den Einsatz von Schutzmechanismen, wie Captchas lösen. (Adams, Jourdan, & Levac, 2010) Generell sollte aber eine Zwei-Faktor Authentifizierung ins Auge gefasst werden. Licht zählt, je nach Einsatzort und dem Grad der Vernetzung, zur kritischen Infrastruktur, wodurch eine Authentifizierung, die nur auf dem Wissen eines Passwortes und Usernamens besteht, nicht mehr den geeigneten Sicherheitsgrad bietet. (Liu, Xiao, & Chen, 2012)

Jene Angriffspunkte, welche die Kommunikation zwischen der Bridge und den LEDs kompromittierten, zeigen, dass hier noch erhebliches Potential steckt, die Sicherheit in diesen ressourcenschonenden Standards voranzutreiben. Da nur die Funktion der LEDs beeinflusst und diese unautorisiert ferngesteuert werden kann, besteht hier kein direktes Risiko für die restliche IT-Infrastruktur. Des Weiteren ist es notwendig, eine Sichtverbindung von wenigen Metern zu den LEDs zu haben, um das System beeinflussen zu können. Das unsichere Datenübertragungsmedium Zigbee Light Link stellt ein Risiko für die Hue Infrastruktur, nicht aber

für die restliche IT-Infrastruktur, dar. Es existieren bereits (Stand: September 2017) erste Ansätze von Schadprogrammen, die die Firmware von Philips Hue Lampen überschreiben und diese lahmlegen, oder diese als WLAN-Störsender verwenden. (Ronen, O'Flynn, Shamir, & Weingarten, 2016)

Wesentliche Sicherheitsaspekte, die durch das Philips Hue System identifiziert wurden sind:

- Geringe Anforderungen an die Passwortkomplexität erlauben Brute-Force Angriffe,
- Sicherheitsmechanismen zur Bekämpfung von Brute-Force Angriffen sind wichtig, um Cloudplattformen vor dem Diebstahl von Zugangsdaten zu schützen,
- Reaktionszeit des Herstellers bei Bekanntgabe von Sicherheitsproblemen durch Dritte ist essentiell für die IT-Sicherheit,
- Kommunikationsverhalten des Herstellers zu seinen Kundinnen und Kunden über diverse Plattformen muss transparent gestaltet sein.

Diese Merkmale werden, mit jenen der anderen IoT-Produkte, die im Laufe dieses Kapitels analysiert werden, als Basis für das Security Framework dienen. Dazu werden die Aspekte in Gruppen zusammengefasst und systematisch dargestellt.

3.2 Foscam IP-Kameras

Die Zahl der Überwachungs- und IP-Kameras nimmt stetig zu. Dabei steigt auch die Anzahl der vernetzten Kameras, die ständig mit dem Internet verbunden sind. Dies ist zum einem auf das breite Angebote der verfügbaren Kameras zurückzuführen, zum anderen auf die gesunkenen Preisen. So gibt es bereits erste Angebote für IP-Kameras für weniger als 100€ (Stand: 2017).

Aufgrund des steigenden Preisdrucks unter den einzelnen Herstellern, wird bei vielen Produkten, vor allem in den niedrigeren Preissegmenten, bei der Sicherheit gespart. Unsichere IP-Kameras führen dazu, dass Videosignale unverschlüsselt und ohne jegliche Authentifikationsmechanismen im Internet verfügbar sind. So kam es in der jüngeren Vergangenheit vor, dass Hacker sich Zugang zu IP-Kameras verschafften und, falls die Kamera über diese Funktion verfügte, mit den Betroffenen über eine Gegensprechfunktionalität kommunizierten.

Neben dem unbefugten Zugriff auf das Audio- und Videosignal der Kameras, können diese genauso für andere Angriffsarten verwendet werden. So wurde im Jahr 2016 ein Botnetz mittels ungeschützter IoT-Objekte aufgebaut, mit welchem wichtige IT-Services, wie etwa Dyn, angegriffen wurden. Dieses Szenario zeigte auf, welche Gefahr von der zunehmenden Vernetzung ausgeht und wie einfach IoT-Objekte mit Schadsoftware infiziert werden können. In einem späteren Abschnitt wird nochmals konkret auf die Problematik von IoT-Objekt basierenden Botnetzen eingegangen. (siehe Abschnitt 4.1)

Teile dieses Botnetzes waren zum Großteil Geräte des chinesischen Herstellers Foscam. Dieser ist einer der größten Anbieter von IoT-Produkten und vor allem im Niedrigpreissegment angesiedelt.

In den Medien ist Foscam allerdings durch deren sorglosen Umgang mit der IT-Sicherheit und Privatsphäre ihrer Kundinnen und Kunden bekannt geworden. So wurde Anfang 2013 bekannt, dass Angreifer, die Zugang über das Webinterface hatten, mittels einer modifizierten URL (Uniform Ressource Locator) den gesamten Speicher einer IP-Kamera herunterladen konnten. Diese Datei konnte anschließend mit einem Hex-Editor geöffnet und entsprechende Zugangsdaten ausgelesen werden. (Krebs, Krebs on Security, 2016)

Die nächste Schwachstelle in den IoT-Produkten von Foscam ist die Standardkonfiguration des Benutzernamens und des Passworts. Diese sind nach wie vor bei allen Produkten admin und das Passwort ist gar nicht gesetzt. Normale Kundinnen und Kunden, die eine geringe IT-Affinität aufweisen, werden tendenziell diese Einstellungen beibehalten, weil sie schon über die erfolgreiche Installation erfreut sind und sich nicht weiter mit dem Thema IT-Sicherheit beschäftigen. Erst durch die Hinweise einiger Nutzerinnen und Nutzer im Foscam-eigenen Forum veranlasste den Hersteller dazu, im Jahr 2013 ein Firmware-Update bereitzustellen, die eine verpflichtende Passwortänderung nach dem ersten Login vorsieht. (Dhanjani, 2015)

Problematisch ist, dass dieses Firmware-Update nur über das Forum sowie in einem der unzähligen Untermenüpunkte der Website von Foscam angekündigt war. Eine Update-Benachrichtigung, die direkt im Webinterface des IoT-Objekts erscheint, ist bei Foscam nicht vorgesehen. Deshalb lässt sich daraus ableiten, dass eine nur geringe Anzahl an Kundinnen und Kunden, dieses Update installierten.

Eine solche Updatepolitik und Informationskampagne ist in Zeiten von automatisierten Updates, Update-Centern und Benachrichtigungen, welche die Nutzerin und den Nutzer über unterschiedliche Kanäle (E-Mail oder Smartphone-Benachrichtigung) erreichen, problematisch. Hier müssen die Hersteller in die Pflicht genommen werden und automatisierte Updatefunktionen anbieten, wodurch Lücken in deren Systeme global schnell geschlossen werden und die betroffenen Kundinnen und Kunden, nicht mit der Wartung und Pflege ihrer Systeme überfordert werden. (Dhanjani, 2015)

Foscam IoT-Objekte werden im Auslieferungszustand mit einem aktivierten dynamischen DNS (Domain Name Service) System ausgestattet. Dieser Service erlaubt es Kundinnen und Kunden direkt auf ihr IoT-Objekt über das Internet zugreifen zu können, auch wenn diese nicht über eine statische IP-Adresse verfügen. (Scherschel, Heise, 2017)

Diese Funktion wies in vielen Firmwares von Foscam Produkten Lücken auf, die es Unbefguten ermöglichten, sich Zutritt zum Webinterface zu verschaffen. Hierbei verwendete der integrierte dynamische DNS-Client von Foscam das UDP, um die jeweilig aktuelle IP-Adresse des Internetanschlusses der Kundin und des Kunden an den Foscam-Server zu übertragen. Das dafür notwendige Datenpaket beinhaltete den Benutzernamen und das Passwort, welche für den Zugang auf das Webinterface notwendig sind. Dies erfolgte jedoch unverschlüsselt, wodurch es Angreifern einfach gemacht wurde, mittels Phishing-Attacke, sowohl die aktuelle IP-Adresse des

IoT-Objekts, als auch die notwendigen Zugangsdaten zu erhalten. (Krebs, Krebs on Security, 2016)

Eine weitere Lücke in Systemen von Foscam IoT-Objekten wurde 2014 bekannt. Hier konnten sich Angreifer unbemerkt Zugriff auf das Webinterface verschaffen. Dies war möglich, weil sich die Authentifizierung umgehen lies, indem man die Felder für Benutzername und Passwort leer lies. Publik wurde dies durch einen Post im Foscam Forum. Foscam stellte darauf ein Firmware-Update bereit. Eine Kommunikation über den neuen Patch mit den Kundinnen und Kunden erfolgte jedoch, wie bereits zuvor erwähnt, nicht.

Laut einem Artikel der Website Heise.de aus dem Jahr 2016 (Dölle, 2016) werden bei Nutzung der hauseigenen mobilen Applikation und bei Konfiguration dieser, alle Daten inklusive Administrator-Benutzer, Passwort, Geräte-ID (Identifikation) und MAC-Adresse (Media-Access-Control-Adress) an die Server von Foscam übertragen. Diese werden von dort bei jedem Start der Applikation abgerufen.

Dies mag zwar für die Kundinnen und Kunden praktisch sein, weil diese einmalig ihre Daten eingeben und diese dann mit ihren Foscam-Cloud Zugang verknüpfen können. Problematisch wird es nur, wenn die von Foscam betriebene Infrastruktur kompromittiert und neben dem Administrationszugang auch die IP-Adressen jedes IoT-Objekts bekannt wird. Mit dem Administrationszugang hat man neben dem Zugang zur eigentlichen Funktion des IoT-Objekts die Möglichkeit IT-Infrastruktur Daten, wie WLAN-Passwörter auszulesen. Somit wäre eine IP-Kamera von Foscam ein Einfallstor in die private IT-Infrastruktur.

Zudem geht aus dem Artikel hervor, dass HTTPS (Hyper Text Transfer Protocol Secure) nicht korrekt implementiert ist, weil man mittels Man-in-the-Middle-Angriff, gefälschte Zertifikate in die Kommunikation zwischen Client und IoT-Objekt einbringen kann.

Des Weiteren werden bei Start der IP-Kamera bis zu zehn UDP- und verschlüsselte TCP-Verbindungen zu unterschiedlichen Servern im Internet aufgebaut. Da die darin enthaltenen Daten verschlüsselt sind und die Zieladressen nicht direkt Foscam zugeordnet werden können, erscheint hier der Verdacht, dass inkorrekt mit dem Datenschutz der Kundinnen und Kunden umgegangen wird. Vor allem ist das interessant, weil dabei Wert auf Verschlüsselung gelegt wird, bei der Sicherheit der Bedienung der IP-Kamera selbst wird jedoch nicht mit demselben Aufwand agiert.

Ein weiteres Sicherheitsproblem entsteht dann, wenn die IP-Kamera, die von außen über das Internet erreichbar sein soll, selbstständig UDP-Verbindungen nach außen aufbaut. Damit die verschickten UDP-Pakete beantwortet werden können, geben Router, aufgrund der UPnP (Universal Plug and Play) (Boucadair, France Telecom, Penno, Wing, & Cisco, 2013) Funktion, den verwendeten Port für eingehende Verbindungen frei, damit eingehende Daten an die Kamera weitergeleitet werden können. (vergleiche Abbildung 20) (Dölle, 2016)

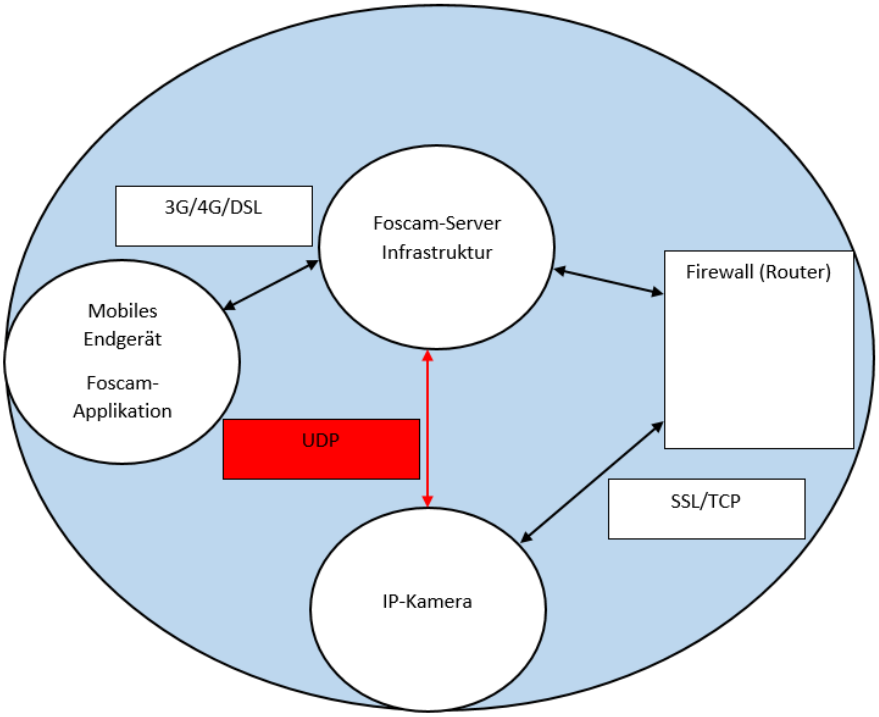


Abbildung 20 Foscam Firewall-Problematik

Vorteil bei dieser Methode, ein IoT-Objekt über das Internet erreichbar zu machen, ist der geringe Aufwand, der betrieben werden muss. Dies ist vorrangig für Kundinnen und Kunden interessant, die eine geringe IT-Affinität aufweisen und schnell und einfach einen Remote-Zugang zu ihren IoT-Produkten erzielen möchten. Es zeigt jedoch, dass dadurch bestehende IT-Sicherheitsfunktionen umgangen werden.

Foscam bietet neben dieser Lösung auch ein Proxy-System an, welches zu tragen kommt, wenn die UPnP-Funktion des Routers nicht aktiviert ist. Hier wird der Datenstrom zuerst auf die Foscam-eigenen Server übertragen und von dort direkt auf mobile Applikationen. (Dölle, 2016)

Produkte des Herstellers Foscam zeigen, welche Gefahren von einer fehlenden und/oder fehlerhaften Implementierung von Sicherheitsfunktionen ausgehen. Zwar mag es sein, dass diese Produkte aufgrund der vorher genannten Workarounds kundenfreundlich sind und der Kundin und dem Kunden dadurch Konfigurationsaufwand ersparen. Allerdings geht dies auf Kosten der Datensicherheit und des Datenschutzes.

Die teils gravierenden Sicherheitslücken, die in den letzten Jahren bei Produkten dieses Herstellers auftraten, weisen auf eine mangelnde Sicherheitsaffinität auf Seiten der Entwicklerinnen und Entwickler von Foscam hin. Der Umstand, dass Daten, die unbemerkt von Nutzerinnen und Nutzern zu Servern von Foscam verschlüsselt übertragen werden, lässt auf Verletzungen des Datenschutzes und der Privatsphäre schließen. Der Hersteller gab zu keiner Anfrage, welche von unterschiedlichen Reporterinnen und Reportern gestellt wurden, Auskunft über diese Datenverbindungen und welchen Zweck diese haben.

Eine der wichtigsten Erkenntnisse, die bei der Analyse der IoT-Produkte von Foscam auftrat, ist die Notwendigkeit, eine umfassende Update-Politik bei den einzelnen Herstellern zu etablieren.

Im Fall von Foscam sind Meldungen zu Updates nur in den zahlreichen Threads des Forums zu finden und werden nicht direkt mit den Kundinnen und den Kunden kommuniziert.

Bei Desktop und mobilen Endgeräten, wie Smartphones und Tablets, haben sich automatisierte Updates etabliert, wodurch eine Nutzerin und ein Nutzer nicht mehr dazu gezwungen ist, diese selbst aus dem Internet zu laden. Dies sollte auch bei IoT-Systemen von Beginn an der Fall sein. Das Philips Hue Ecosystem nutzt die mobile Anwendung auf dem Tablet und Smartphone, die der Nutzerin und dem Nutzer eine Benachrichtigung sendet, falls ein Update verfügbar ist. Ein solches Update-Erinnerungssystem fehlt gänzlich bei den IoT-Objekten von Foscam. Deshalb ergibt sich die Problematik von mangelhaft aktualisierten IoT-Systemen, die jederzeit von Dritten kompromittiert werden und ungewollte private Einblicke in das Leben ermöglichen können.

Ein weiterer wichtiger Punkt ist das Thema dynamische DNS-System. Diese sind im Bereich von privaten Internetzugängen sehr häufig anzutreffen, weil hier keine statischen IP-Adressen vergeben werden. Viele IoT-Hersteller stellen eine solche Funktion direkt im Auslieferungszustand bereit, um das Nutzungserlebnis so angenehm wie möglich zu gestalten. Dadurch soll die Zeitspanne zwischen Konfiguration und funktionierendem System verkürzt werden. Im Falle von Foscam wurde auf eine korrekte Implementierung eines dynamischen DNS-System vergessen, das gegen Angriffe von außen geschützt ist.

Falls es Bedarf an einem dynamischen DNS-System gibt, sollte vielmehr die interne Funktion des Routers oder Modems verwendet werden. Des Weiteren ist es ratsam einen freien und herstellerunabhängigen dynamischen DNS-Dienst zu nutzen, um sich nicht an einen Hersteller binden zu müssen. Damit umgeht man etwaige Sicherheitsprobleme, die von einem fahrlässig agierenden Hersteller ausgehen.

Vom Einsatz von Foscam-Produkten ist, sowohl im privaten als auch geschäftlichen Bereich abzuraten. Selbst die Deaktivierung der für Angriffe anfälligen Funktionen garantiert nicht, dass die IoT-Objekte gekapert oder für den Zugang durch unbefugte Dritte bereitstehen.

Wesentliche Sicherheitsaspekte, die durch Foscam IoT-Produkte identifiziert wurden sind:

- Update der Soft- und Firmware müssen effektiv mit den Kundinnen und Kunden kommuniziert werden,
- Automatische Updatefunktionalitäten gewährleisten die Aktualität und Sicherheit der IoT-Objekte,
- Dynamische DNS Systeme sollten unabhängig von Herstellern gewählt und mittels zentraler Hardware (Router/Modem) betrieben werden,
- Einrichtungskomfort darf nicht auf Kosten von Datenschutz und IT-Sicherheit gehen,
- Jegliche Umgehungen von IT-Sicherheitseinrichtungen sind tabu, auch wenn dadurch ein erhöhter Konfigurationsaufwand betrieben werden muss,
- Steuerung und Nutzung über mobile Endgeräte kann zu einem Sicherheitsproblem werden,

- Niedrigpreis-Produkte weisen tendenziell schwache Sicherheitseigenschaften auf und können eine Gefahr für bestehende IT-Infrastrukturen darstellen,
- Auslieferungskonfigurationen von IoT-Objekten stellen nicht die optimalen Sicherheitseinstellungen bereit, welche notwendig sind, um IT-Sicherheit gewährleisten zu können.

3.3 OEM-IoT-Produkte

OEM (Original Equipment Manufacturer) Produkte, beschreiben Erzeugnisse, die durch einen Erstausrüster hergestellt und durch eine Zweitfirma/einen Importeur unter deren Namen und Marke vertrieben werden. Diese Produkte werden häufig in Fernost produziert und unter bekannten Markennamen in Europa verkauft.

Im Bereich von IoT werden immer mehr Produkte von OEMs hergestellt, weil dadurch Unternehmen besser am dynamischen Markt agieren können, ohne dabei die eigene Produktion ständig anpassen zu müssen.

Bei vielen günstigen IP-Kameras ist es nicht mehr ersichtlich, wer der ursprüngliche Hersteller ist und für notwendige Sicherheitsupdates sorgen muss. Dies ist insofern entscheidend, weil gerade jene IoT-Objekte, die im niedrigen Preissegment angesiedelt sind, eine hohe Verbreitung aufweisen und deswegen eine globale Gefahr bestehen kann, die nicht nur die lokalen Netzwerke der Nutzerinnen und Nutzer gefährden könnte.

Ein Sicherheitsforscher hat im März 2017 eine OEM IP-Kamera analysiert und verschiedenste Sicherheitsprobleme und Lücken entdeckt. (Kim, 2017) Des Weitern entdeckte er mittels der IoT-Suchmaschine Shodan (Shodan, 2017), die in einem späteren Abschnitt genauer beschrieben wird (siehe Abschnitt 4.2), dass 185.000 IP-Kameras über das Internet erreichbar sind, die dieselben Lücken aufwiesen.

Eine dieser Lücken ist ein laufender Telnet Dienst, bei dem laut Spezifikation die gesamte Datenübertragung unverschlüsselt geschieht. Hier ist zudem ein Zugang eingerichtet, der keinem speziellen Zweck zugeordnet werden konnte und daher im Verdacht steht, eine Hintertür (Backdoor) für den Hersteller zu sein.

Für die Kommunikation über HTTPS (Rescorla, 2000) ist ein Schlüsselpaar eingerichtet, das von einem Apple Entwicklerzugang stammt und deshalb als nicht vertrauenswürdig zu betrachten ist. Seriöse Unternehmen bieten eigene Zertifikate an, welche nicht für Entwicklungszwecke gedacht sind. (Krebs, Krebs on Security, 2016)

Daneben sind unterschiedliche RCE (Remote Call Execution) entdeckt worden, welche einen Fernzugriff als Administrator ermöglichen. Hier existieren bereits detailreiche Dokumentationen im Internet, wie diese für einen unerlaubten Fernzugriff missbraucht werden können. (Szili, 2015)

Für die Streaming-Funktionalität wird RTSP (RealTime Streaming Protocol) (Schulzrinne, U, Netscape, Lanphier, & RealNetworks, 1998) als Übertragungsprotokoll genutzt, jedoch gänzlich ohne Authentifizierungsmechanismen. Somit wäre bei der Nutzung einer solchen IP-Kamera mit

aktivierten UPnP der Port für das Streaming offen und frei für all jene zugänglich, die die IP-Adresse herausfinden. (Kim, 2017)

Darüber hinaus ist eine Cloud-Funktion implementiert, die allerdings keine Funktionen für die Endkundin und den Endkunden bereitstellt. Die Funktion selbst baut Verbindungen zu unterschiedlichen Servern von Alibaba und der AWS Cloud auf. Aus der Datenanalyse ließ sich kein Rückschluss auf den Sinn und den Dateninhalt schließen, weil die Datenpakete verschlüsselt übertragen werden. (Kim, 2017)

Des Weiteren ist, wie bereits im Foscam-Fall beschrieben (siehe Abschnitt 3.2), eine Umgehung der Router-Firewall eingerichtet, indem ein UDP-Tunnel direkt zu den Servern aufgebaut und in der Folge die IP-Kamera außerhalb des Heimnetzwerkes erreichbar gemacht wird.

Gerade bei OEM-Produkten wird vielfach, aufgrund der geringen Gewinnmargen, auf eine langfristige Unterstützung mittels Softwareupdates verzichtet. Dies führt zu einer großen Anzahl an angreifbaren IoT-Objekten, die im Internet für jeden zur Verfügung stehen. Durch die Nutzung von IoT-Suchmaschinen können Hacker diese Objekte ausfindig machen und ihren Schadcode auf diese übertragen. Die IP-Kameras, die unterschiedliche Elemente des Privatlebens der Kundinnen und Kunden aufzeichnen und in das Internet streamen, stellen somit ein enormes Sicherheitsrisiko sowohl für die IT-Sicherheit, als auch für die Privatsphäre dar.

Ebenso problematisch ist die Updatesituation bei OEM-Produkten, weil die eigentlichen Hersteller der Endkundin und dem Endkunden meist unbekannt sind. Deshalb ergibt sich, ähnlich wie bei Foscam-Produkten, ein Wirrwarr an IoT-Objekten, die unterschiedliche Sicherheitspatches installiert haben.

Ein weiterer wichtiger Punkt ist der Support, der je nach Importeur, unterschiedlich gut sein kann. Hier ist es schwer einen direkten Ansprechpartner zu finden oder ein Forum, in dem eine aktive Community besteht.

Allgemein ist über offensichtliche OEM-Produkte zu sagen, dass diese in den meisten Fällen keine geeigneten Sicherheitseigenschaften bieten. Des Weiteren stehen viele dieser Produkte im Verdacht, Daten an Dritte zu übertragen, ohne das Einverständnis der Kundinnen und der Kunden.

Diese Funktionen werden oft als Cloud-Komponente in den Spezifikationen angegeben und werden deswegen von vielen Kundinnen und Kunden akzeptiert. Der Einsatz und die Aktivierung von integrierten, von Herstellern bereitgestellten, Cloudanwendungen sollte kritisch beäugt werden, weil diese vielfach als Hintertüren der Hersteller missbraucht werden.

Ein Blick in die AGBs und in die Kundenmeinungen und Foreneinträgen zu dem gewählten IoT-Objekt kann einen ersten Eindruck über die Datensicherheit und Sicherheitsfunktionen der Geräte liefern. Eine vollständige Sicherheit ist dennoch nicht gewährleistet.

Wesentliche Sicherheitsaspekte, die durch OEM IoT-Produkte identifiziert wurden sind:

- Schlechter (Langzeit-)Support, aufgrund der geringen Gewinnmargen,
- Cloudkomponenten enthalten oft Fernzugriff-Möglichkeiten für den Hersteller,
- Intransparente AGBs in Bezug auf übermittelte Daten,
- Vielfach werden Firewalls mittels UDP-Tunnel umgegangen, wodurch die bestehende IT-Sicherheitsinfrastruktur unterwandert wird.

3.4 Zusammenfassung

Die Analyse der drei unterschiedlichen IoT-Lösungen und damit verbundenen Herstellern zeigte auf, welche Herausforderungen in Bezug auf Sicherheit und Datenschutz in diesen Bereich angesiedelt sind.

Jedes dieser drei Beispiele beinhaltete unterschiedliche Angriffsszenarien und Lücken in der Implementierung von Sicherheitseigenschaften. Diese reichen von unverschlüsseltem Streaming des aktuellen Videosignals von IP-Kameras, bis hin zur Unterwanderung bestehender IT-Sicherheitslösungen, wie etwa Firewalls, durch Nutzung von UDP-Tunneln.

Wegen des Drucks auf die Hersteller, Produkte so einfach wie möglich für die Kundin und den Kunden zu designen und das Nutzungserlebnis zu steigern, werden häufig technische Mittel eingesetzt, die nicht im Einklang mit der IT-Sicherheit stehen.

So werden Cloudplattformen genutzt, um jegliche Passwörter der IoT-Infrastruktur abzulegen und damit mobile Applikationen einfacher bedienen zu können. Problematisch wird dieser Ansatz nur, wenn die Infrastruktur des Herstellers kompromittiert wird und dadurch Millionen von Zugangsdaten zu privaten WLANs und Cloudzugängen offengelegt werden.

Bezeichnungen wie sicher und geschützt, welche sich häufig auf den Verpackungen der IoT-Produkte finden lassen, sind oft nicht mehr als Werbeslogans, die kritisch hinterfragt werden müssen, um die verwendeten Sicherheitstechniken zu identifizieren und analysieren, ob diese wirklich so zu bezeichnen sind.

Wichtige Merkmale von aktuellen IoT-Produkten sind neben schnellen Updatezyklen, einer transparenten Kommunikation zwischen Kundinnen und Kunden mit dem Hersteller und korrekt implementierten Sicherheitsmerkmalen, auch ein ordnungsgemäßer Umgang mit den Daten der Kundinnen und Kunden, die bei jedem der oben genannten Hersteller, in deren Cloudplattform gespeichert werden. Diese Plattformen müssen entsprechend gewartet und betreut werden, weil sie sonst Hackern und unbefugten Personen, Zutritt zu diesen Daten ermöglichen.

Die Beispiele dienen als Basis für das nächste Kapitel, in dem die Folgen von Angriffen auf IoT-Infrastrukturen und Objekten beschrieben werden.

4 RISIKEN UNSICHERER IOT-SYSTEME

Dieses Kapitel beschäftigt sich mit den Risiken und Folgen von unsicheren IoT-Systemen und Objekten. IoT-Systeme sind in ähnlicher Weise bedroht wie Desktop- und mobile Computersysteme. Hier reicht die Bandbreite von Diebstahl von Zugangsdaten, unberechtigte Geldtransfers auf Konten Dritter, bis zu Trojanern und Viren, welche die Systeme lahmlegen und sie als Bots für Botnetze missbrauchen. Dadurch können Hacker diese Systeme verwenden, um beispielsweise Spam-E-Mails zu versenden, Kryptowährungen zu generieren, oder damit ganze IT-Services lahmzulegen. (Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015)

Wenn die Auswirkungen unsicherer Desktop-Systeme auf IoT-Produkte übertragen werden, so lässt sich in den letzten Monaten und Jahren erkennen, dass diese Systeme für Hacker und Kriminelle immer attraktiver werden.

Die Problematik der fehlenden Sicherheitsupdates und falsch konfigurierter Sicherheitseinstellungen trägt ihren Teil dazu bei, dass IoT-Objekte in Zukunft immer häufiger Ziel von Angriffen werden und für kriminelle Tätigkeiten verwendet werden. (Dlamini, Eloff, & Eloff, 2009)

Ein gängiges Szenario wäre, wenn kompromittierte IP-Kameras private Situationen aufzeichnen. Diese privaten Aufnahmen können anschließend als Druckmittel für jeweilige Erpressungsversuche genutzt werden.

Ähnliches geschieht bereits im Sektor von Desktop- und mobilen Systemen. Hier findet sogenannte Ransomware immer mehr Verbreitung. Ransomware verschlüsselt wichtige Daten der Nutzerinnen und der Nutzer und verlangt zur Entschlüsselungen einen Geldbetrag, der mit nicht nach verfolgbaren Kryptowährungen bezahlt werden muss. (Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015) Ein solches Szenario ist im Bereich von IoT ebenso denkbar, wobei private Einblicke das Druckmittel wären.

Neben Ransomware, stellen auch Botnetze, frei verfügbare Suchmaschinen, die spezielle für das Aufspüren von IoT-Objekten konzipiert sind und Angriffsszenarien auf kritische Infrastruktur, die Gefahren der IoT-Sicherheit dar. Diese Risiken werden in den nachfolgenden Abschnitten genauer behandelt.

4.1 Botnetze

Ein Botnetz besteht aus einer Reihe von unterschiedlichen Computern und Rechnern, die ohne das Wissen derer Benutzerinnen und Benutzer für bestimmte Zwecke verwendet werden. Diese Botnetze werden für kriminelle Aktivitäten, wie dem Versenden von Spam-E-Mails, dem automatisierten Abrufen von Werbenachrichten und dem Ausführen von DDoS-Attacken (Distributed Denial of Service) genutzt. (Welzel, Rossow, & Bos, 2014)

Botnetze entstehen durch die Infektion eines angreifbaren Systems, bei der Hacker Schadcode auf dem System ausführen, der im Hintergrund Fernsteuerungssoftware installiert. Diese

Fernsteuerungssoftware kontaktiert in regelmäßigen Abständen sogenannte C&C-Server (Command and Control), welche die jeweiligen Anweisungen an die Bots verteilen. (vergleiche Abbildung 21) Die C&C-Server werden von Hackern und Kriminellen gesteuert und für ihre Zwecke eingesetzt. (Cooke, Jahanian, & McPherson, 2005)

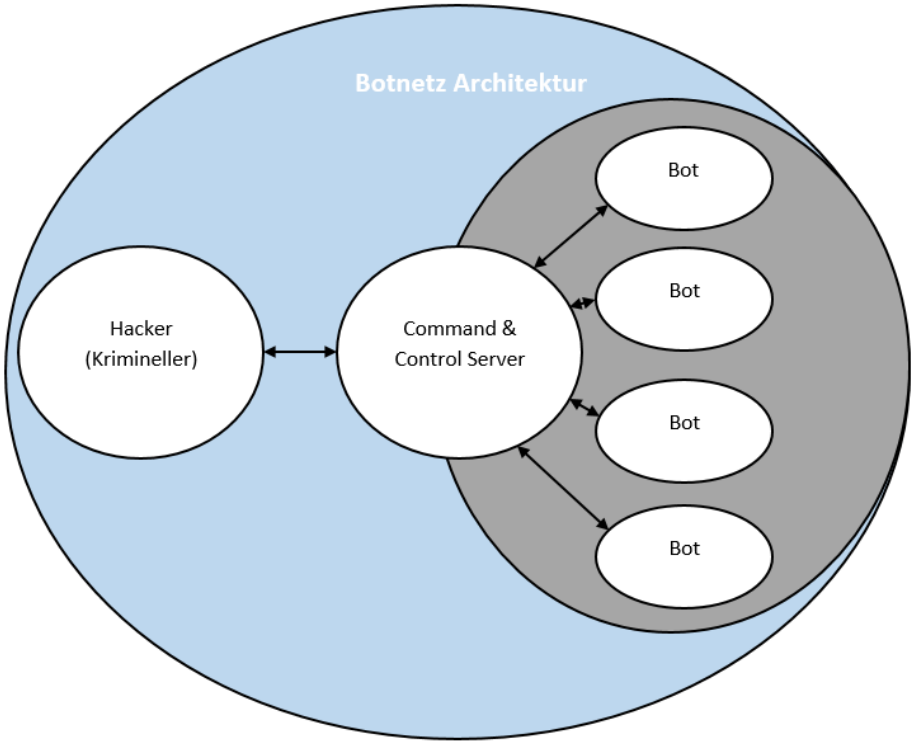


Abbildung 21 Botnetz Architektur (Cooke, Jahanian, & McPherson, 2005)

Botnetze verbeiten sich durch Malware, die Lücken in nicht aktuellen und schlecht gewarteten Systemen ausnützen, durch Downloads, die meist aus illegalen Quellen stammen, oder durch das Öffnen von infizierten E-Mail Anhängen. (Li, Jiang, & Zou, 2009)

Einer Studie zufolge, die durch den russischen Anti-Virus Hersteller Kaspersky durchgeführt wurde, waren im Jahr 2008 10% der weltweiten Computer, die mit dem Internet verbunden waren, Teil eines oder mehrerer Botnetze. (Lozhkin, 2014)

Das Erkennen, ob ein Computer Teil eines Botnetzes ist, kann eine Herausforderung darstellen, weil sich diese meist als Rootkit innerhalb des Betriebssystem selbst installieren und daher für Antivirenprogramme quasi unsichtbar sind. Auffälligkeiten sind aber: hohe Systemlast, die nicht durch die Nutzerin und den Nutzer ausgelöst wird, hoher Internetdatenverkehr und eine träge Systemperformance. (Karasaridis, Rexroad, & Hoeflin, 2007)

Botnetze können beträchtliche Ausmaße von wenigen hunderttausenden Bots bis zu Millionen Rechnern betragen, die ferngesteuert für Kriminelle interagieren. Das Botnetz Bredlop hatte bis zu 30 Millionen Bots und wurde zwischen Mai 2009 und Oktober 2010 betrieben. Zweck dieses Botnetzes war, Spam-E-Mails zu versenden. Dieses Botnetz schaffte es bis zu 3,6 Milliarden E-Mails pro Tag über die einzelnen Bots zu versenden. (Infosecurity-Magazine, 2010)

Neben dem Versenden von E-Mails ist das Durchführen von DDoS-Attacken eine häufige Anwendung von Botnetzen. Hier werden die Bots dazu genutzt, IT-Services lahmzulegen, indem

Millionen von ihnen diese versuchen zu besuchen, wodurch die Ressourcen der Services ausgelastet und nicht mehr für Kundinnen und Kunden erreichbar sind. (Cooke, Jahanian, & McPherson, 2005)

Solche Attacken wurden bereits auf Websites von Politikerinnen und Politkern, Finanzinstitutionen und wichtigen IT-Services gerichtet und haben Schäden in Millionenhöhe hinterlassen. (Spiegel Online, 2013), (Perlroth & Hary, 2013) und (Patalong, 2008)

Ein Botnetz, das im selben Ausmaß ähnlichen Schaden angerichtet hat, wurde 2016 entdeckt und nutzte dazu ausschließlich IoT-Objekte. Dieses Botnetz wird im folgenden Abschnitt (4.1.1) genauer beleuchtet.

4.1.1 Mirai

Mirai war das erste Botnetz, das ausschließlich IoT-Objekte infizierte und diese als Bots missbrauchte. Dazu wurden zu Beginn unter der Verwendung von frei verfügbaren IoT-Suchmaschinen (siehe Abschnitt 4.2) einzelne IoT-Objekte gesucht, welche aufgrund ihrer Konfiguration und Software geeignet waren unberechtigten Fernzugriff zu erlauben und den Schadcode auszuführen. Diese IoT-Objekte selbst scannten anschließend das Internet, um weitere infizierbare Objekte aufzufinden und an diese den Schadcode zu übertragen. Produktarten, die mit Mirai infiziert wurden, waren: IP-Kameras, Router und Digitale Satelliten Receiver. (Dobbins & Bjarnason, 2016)

Dazu nutzte Mirai unter anderem eine Liste, bestehend aus 60 unterschiedlichen Herstellern, die Standardusernamen und Standardpasswort beinhaltet. (Wei & Chow, 2016) Die eigentliche Funktion des IoT-Produkts war durch die Infektion nicht eingeschränkt, sodass viele Nutzerinnen und Nutzern nichts davon erfuhren. Einzig ein erhöhter Datenverkehr, der durch das IoT-Objekt erzeugt wurde und gelegentliche Leistungseinbußen, machten die Infektion bemerkbar. (Karasaridis, Rexroad, & Hoeflin, 2007)

Die Schadsoftware selbst blieb so lange auf dem IoT-Objekt, bis es neugestartet wurde. Dadurch lässt sich darauf schließen, dass die eigentliche Firmware nicht kompromittiert oder überschrieben wurde, sondern eine Funktion zum Bufferoverflow genutzt wurde, um den Programmcode in den RAM (Random Access Memory) zu laden. Ein Sicherheitsforscher entdeckte, dass ein bereits infiziertes IoT-Objekt nach einem Neustart in 98 Sekunden wieder neu infiziert wurde. (Coldewey, 2016)

Dies zeigt, wie schnell sich dieses Botnetz im gesamten Internet verbreitet hat und zudem, wie essentiell ein vollständig konfiguriertes IoT-Produkt ist, das nicht das Default-Passwort des Herstellers nutzt. Diese Tatsache wird in der Entwicklung des Security Frameworks nochmals aufgegriffen.

Nachdem das IoT-Objekt infiziert war und andere kompromittierbare Systeme suchte, hat es auf Anweisungen des C&C-Servers gewartet. Dieser sendete in unregelmäßigen Abständen die Programmteile, welche von den IoT-Objekten ausgeführt wurden. (Bertino & Islam, 2017)

Mirai wurde hauptsächlich zu DDoS-Attacken verwendet und erzeugte einen, bis dahin noch nicht dagewesenen Datenverkehr von 620-1000 Gbit/s, mit welchen unterschiedliche IT-Services überrannt wurden. Ziel war unter anderem der DNS-Provider Dyn, wodurch Kunden, wie GitHub, Twitter und Netflix, nicht für ihre Kundinnen und Kunden erreichbar waren. (ServerComparator, 2016) Die Urheberinnen und Urheber von Mirai boten ihr Netzwerk in zahlreichen Foren an. Als Zahlungsmittel wurde die Kryptowährung Bitcoin verwendet. (Dobbins & Bjarnason, 2016)

Die Anzahl der Bots im Mirai Netzwerk, welches im Jahr 2016 ihren Höhenpunkt hatte, wird auf 500.000 unterschiedliche IoT-Objekte weltweit geschätzt. (ServerComparator, 2016) Diese Bots erzeugten bei den eingesetzten Angriffen bis zu 1,75 Millionen HTTP-Anfragen pro Sekunde, mit welchen Websites und deren Serverapplikationen überlastet wurden. (Gierow, Golem, 2016)

Es gab außerdem Versuche das Botnetz zur Generierung von Kryptowährungen zu verwenden, dies wurde jedoch sehr bald verworfen, weil die Rechenleistung nicht ausreichend war. Kryptowährungen benötigen je nach Verbreitung, eine entsprechende Rechenleistung, um erfolgreich nach neuen Geldeinheiten schürfen zu können. IoT-Objekte hingegen verfügen weder über eine dezidierte Grafikeinheit noch über genügend Prozessorleistung, um dies effektiv betreiben zu können. (McMillen, 2017)

Anfang Oktober 2016 veröffentliche der Autor des Mirai Botnetzes und des dahinterliegenden Schadprogramms, den Quellcode. (Paganini, 2016) Seitdem wurde dieser als Basis vieler anderer IoT-Botnetze verwendet, die in ihrer Funktionsweise erweitert wurden und neue Lücken in den IoT-Objekten zur Infektion ausnutzen. (Scherschel, Heise, 2017)

So wurde eine neue Infektionsmethode entwickelt, welche infizierte Windows-Computer dazu nutzt, um in deren Netzwerken nach verwundbaren IoT-Endgeräten zu suchen und diese zu infizieren. (Securelist, 2017)

Seit der ersten Veröffentlichung des Mirai-Quellcodes, nahm die Anzahl der DDoS Angriffe, welche durch IoT-Objekte ausgelöst wurden, bis zum ersten Quartal 2017 um 2/3 zu. (Thoma, 2017) Dies zeigt die Gefahr, welche von ungeschützten IoT-Objekten ausgeht und damit grundlegende IT-Infrastrukturen und Services bedroht.

4.1.2 DDoS (Distributed Denial of Service)

Eine DDoS-Attacke nutzt im Gegensatz zu einer DoS (Denial of Service) -Attacke eine große Anzahl unterschiedlicher Hosts oder Bots, um einen IT-Service zu überlasten. Kriminelle und Hacker nutzen diese Art von Angriff, um damit kritische Infrastrukturen und Basis-IT-Services, wie DNS-Systeme, lahmzulegen. (Mirkovic & Reiher, 2004) Dabei wollen sie einerseits die Stärke ihrer Botnetze demonstrieren und andererseits in vielen Fällen Geldbeträge erpressen, um die Services wieder störungsfrei betreiben zu können. DDoS-Angriffe werden auch als Service in verschiedenen Untergrund-Foren angeboten, um damit Mitbewerberinnen und Mitbewerber zu schaden. (Lozhkin, 2014)

DDoS-Attacken und Angriffe werden von Kriminellen über C&C-Servern gesteuert. Diese verteilen die Angriffsziele und die Angriffsvarianten an die einzelnen Bots, welche dann den

eigentlichen Angriff ausführen. (vergleiche Abbildung 22) (Feinstein, Schnackenberg, & Balupari, 2003)

Die Bots selbst führen gezielte Zugriffe in geringen Abständen auf IT-Services aus, wodurch sowohl der Internetzugang als auch die Dienste der Services selbst an ihre Grenzen stoßen und dadurch für wirkliche Nutzerinnen und Nutzer nicht mehr erreichbar sind. (Mirkovic & Reiher, 2004)

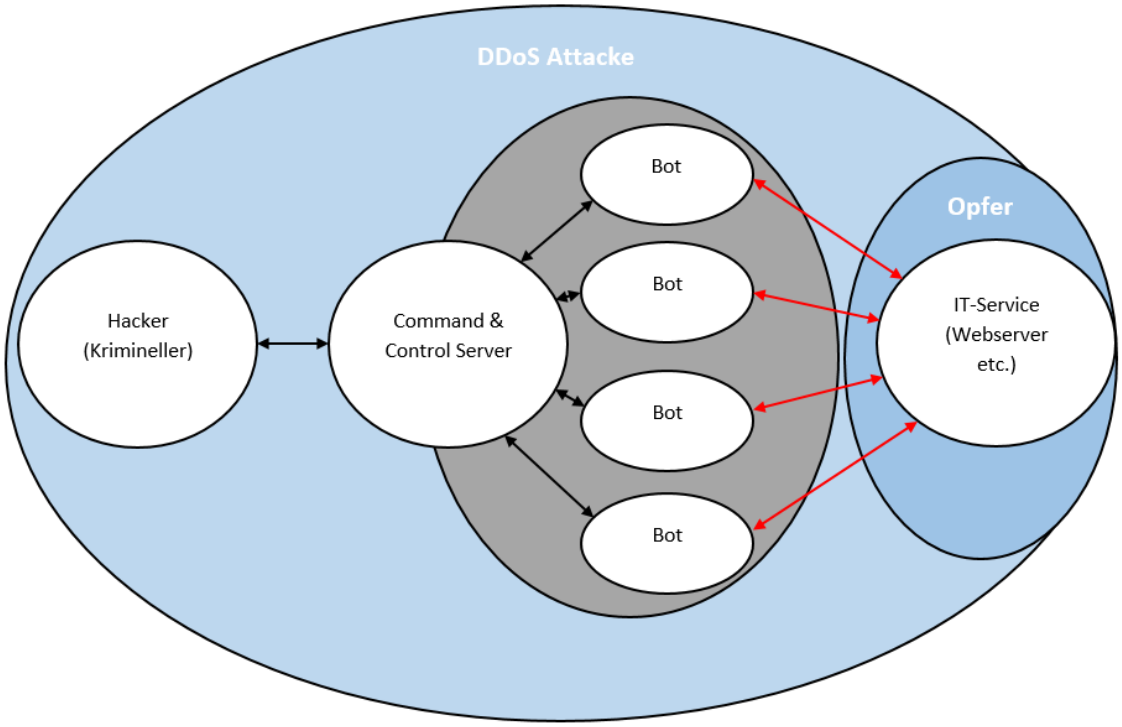


Abbildung 22 DDoS-Attacke Ablauf

Durch die Tatsache, dass die Zugriffe von vielen unterschiedlichen Hosts ausgehen, können einfache Algorithmen, die einzelne Zugriffe blockieren, einen solchen Angriff nicht abwehren. Dem kann auch eine Erhöhung der Kapazitäten nur temporär entgegenwirken, weil Botnetze aus immer mehr einzelnen Bots bestehen und kontinuierlich, auch aufgrund der steigenden Verbreitung von IoT-Objekten, wachsen. (Douligeris & Mitrokotsa, 2004)

Bereits im Jahr 2015 wurden IoT-Objekte verwendet, um ein Botnetz zu erzeugen, das für DDoS-Angriffe genutzt wurde. Hier wurden 900 IP-Kameras infiziert, die eine Lücke in deren Linux und BusyBox-Implementierung aufwiesen. Diese Kameras wurden dazu genutzt, 20.000 Anfragen pro Sekunde an einen Webserver zu senden und diesen damit zu überlasten. (Gayer, Wilder, & Zeifman, 2015)

Im Jahr 2014 wurden mehrere 100.000 IoT-Objekte, unter welchen Smart-TVs, Smarte Gefrierschränke und andere Haushaltsgeräte waren, genutzt um Spam-E-Mails zu versenden. Allerdings bestehen Zweifel daran, ob diese nur für diesen Zweck kompromittiert wurden, oder ob sie bereits Teil des ersten IoT-Botnetzes waren. (Ramesh, 2014)

Die Kombination aus Botnetzen und DDoS-Attacken, die auf Basis von IoT-Objekten basieren, zeigt, wie gefährdet ungeschützte und schlecht gewartet IoT-Produkte sind. Das Gefährdungs-

und Missbrauchspotential, das in jedem vernetzten IoT-Objekt steckt, wurde angesichts der Entdeckung von Mirai erstmals der breiten Öffentlichkeit bewusst. Aus diesem Grund wird im Kapitel Entwicklung des Security Frameworks (Kapitel 5), besonders auf die Gefahr von Botnetzen geachtet und entsprechende Gegenmaßnahmen angefügt.

4.2 IoT-Suchmaschinen

Suchmaschinen, die das Web nach Inhalten durchsuchen, haben einen festen Platz im Alltag vieler Menschen. Im Bereich von IoT hat sich in den letzten Jahren eine Plattform etabliert, welche auf Basis von Metadaten, nach IoT-Geräten im Internet sucht. Shodan, so der Name der Suchmaschine, wurde 2009 vom Softwareentwickler John Matherly entwickelt. (Bodenheim, Butts, Dunlap, & Mullins, 2014)

Shodan generiert seinen Suchindex auf Grundlage von Webserver- (Port 80, 8080, 443), SSH- (Secure Shell) (Port 23), FTP- (File Transfer Protocol) (Port 21) und RTSP- (Port 554) Portweiterleitungen. (Osborne, 2016) Diese Protokolle finden in den meisten IoT-Objekten Verwendung. Bei der Erstellung des Suchindex werden diese Ports gescannt und versucht Metadaten aus den Anmeldeseiten und Welcome-Pages zu extrahieren, die zu Beginn eines Login-Prozesses der Benutzerin und dem Benutzer angezeigt werden. (Verma, 2016) (vergleiche Abbildung 23)

Die Suchmaschine kann von jeder Person über das Internet benutzt werden. Sie ist limitiert auf zehn Ergebnisse ohne Registrierung und 50 Ergebnisse, wenn man sich registriert. Falls man mehr Ergebnisse auf seine Anfragen erhalten möchte, muss man sich direkt an den Entwickler wenden und den Grund dafür nennen. (Goldman, 2013)

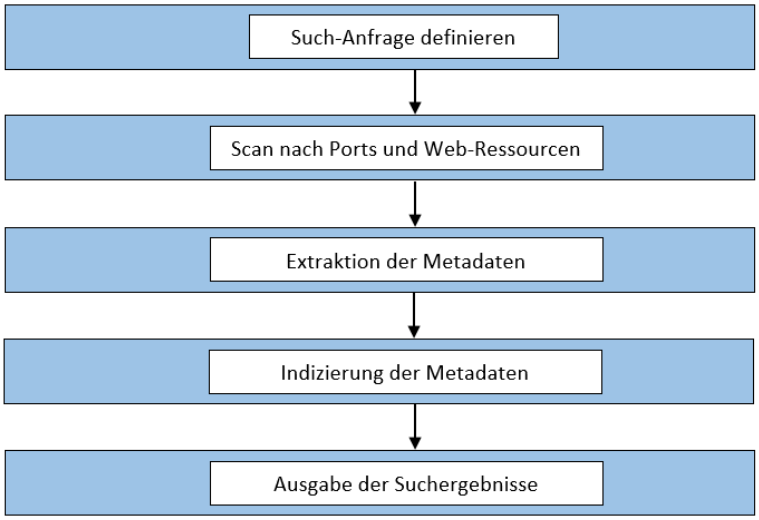


Abbildung 23 Ablauf: Shodan Suchanfrage

Die Legalität von Shodan wird von vielen Expertinnen und Experten in Frage gestellt, weil der Funktionsumfang dazu genutzt werden kann, angreifbare Systeme zu identifizieren. Das könnte

von Hackern und Kriminellen genutzt werden, um zukünftige Bots für deren Botnetze zu adressieren und deren Schadcode effektiv im Internet zu verbreiten. (Goldman, 2013)

Dadurch können über Shodan neben Verkehrskontrollsysteme auch Steuerungsanlagen für Tankstellen oder Kraftwerke gefunden und auf mögliche Auffälligkeiten in der Konfiguration geprüft werden. Würde eine neue Lücke in einem IoT-Objekt gefunden werden, könnten sowohl Sicherheitsanalystinnen und Sicherheitsanalysten als auch Hacker Shodan nutzen und mittels der passenden Metadaten nach weiteren kompromittierbaren Systemen suchen. (Brinkmann, 2013)

Shodan bietet die Möglichkeit, die Suche auf einzelne Länder einzuschränken und kann somit auch für Penetration-Tests genutzt werden, um potentiell gefährdete Systeme zu identifizieren und die Betreiberin und den Betreiber darüber zu informieren. Diese Suchergebnisse können anschließend in Kartenform dargestellt oder als XML-Datei exportiert werden. (Bodenheim, Butts, Dunlap, & Mullins, 2014)

Neben Shodan gibt es noch andere IoT-Suchmaschinen, wie Thingful.net. Diese besitzen jedoch nicht den Funktionsumfang, welchen Shodan bereitstellt. Sie können aber dazu genutzt werden, um beispielsweise IoT-Objekte in der Umgebung zu identifizieren. (Aceves & Larios, 2016)

IoT-Suchmaschinen zeigen einerseits auf, inwieweit IoT-Objekte bereits verbreitet sind, anderseits können diese von Hackern und Kriminellen genutzt werden, um Angriffsziele ausfindig zu machen. Folglich stellen IoT-Suchmaschinen eine Bedrohung dar, die sich nicht direkt auf die Sicherheit von IT-Systemen und IoT-Objekten auswirkt. Sie machen Lücken in Sicherheitsimplementierungen transparent, wodurch unbefugte Dritte erste Analysen durchführen können, bevor sie mit ihren Angriffen beginnen.

4.3 Kritische Infrastrukturen

Kritische Infrastrukturen sind laut BKA (Bundeskanzleramt) jene Infrastrukturen, welche von wesentlicher Bedeutung sind, um für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen zu sorgen und deren Störung oder Zerstörung zu schwerwiegenden Auswirkungen auf die Gesundheit, Sicherheit und oder wirtschaftliche und soziale Wohl der Bevölkerung oder das Stören der Funktion von staatlichen Einrichtungen beinhalten. (Bundeskanzleramt, 2014)

Durch die zunehmende Vernetzung werden kritische Infrastrukturen immer mehr durch Angriffe bedroht. Dies kann sowohl den öffentlichen Sektor, als auch den privaten betreffen. Die Konsequenzen sind jeweils sehr ähnlich und reichen vom Ausfall der Beleuchtung in privaten Wohnungen bis hin zu Black-Outs, die aufgrund von Angriffen auf Versorgungssysteme ausgehen. (Leopold, 2017)

Ein solcher Angriff kann auf Basis eines Botnetzes geschehen, das gekaperte IoT-Objekte nutzt, und für Chaos in Ländern und der Bevölkerung sorgt. Dieses Bedrohungspotential ist vielen Herstellern, sowie den Kundinnen und Kunden nicht bewusst.

Aus diesem Grund hat die EU (Europäische Union) 2015 eine Richtlinie beschlossen, in der Betreiber, kritischer Infrastrukturen dazu verpflichtet wurden, schwerwiegende IT-Vorfälle an die

Behörden zu melden. Dieses Gesetz gilt für die Bereiche der Energieversorgung, Transport, Finanzwesen, Gesundheitseinrichtungen, Wasserversorgung und digitale Dienstleistungen. (Gierow, Golem, 2015)

Des Weiteren wird dieses Gesetz für Plattformbetreiber wirksam, wie Cloud-Anbietern, E-Commerce-Plattformen oder Suchmaschinenprovider. Es besteht allerdings keine Pflicht, die betroffenen Kundinnen und Kunden, über diese Vorfälle zu berichten, was von Expertinnen und Experten stark kritisiert wird. (Gierow, Golem, 2015)

Diese Maßnahmen kann man weder als Prävention, noch als Schutz vor zukünftigen Angriffen sehen, sondern als transparente Einrichtung, um das Gefahrenpotential besser darstellen zu können.

Eine Studie, durchgeführt von Kaspersky im Jahr 2015, zeigte, dass die Gefahr von Cyberattacken mit der Komplexität eines Unternehmens zunehme. Der Studie zufolge seien über 220.000 industrielle Steuerungsanalage über das Internet erreichbar, wovon 91,6 Prozent unsichere Transportprotokolle und Datenaustauschformate verwenden. In den letzten fünf Jahren seien außerdem die Anzahl der Lücken in Steuerungsanlage um das zehnfache gestiegen. (Bordel, 2016)

So wurde im Jahr 2015 ein Angriff auf die IT-Systeme eines Energieversorgers in der Ukraine ausgeübt, bei dem die Hälfte der Haushalte in dieser Region ohne Strom auskommen mussten. Dies zeigt, wie angreifbar wichtige Einrichtungen der Gesellschaft sind und welche Auswirkungen diese haben. (Bordel, 2016)

Die Auswirkungen von Angriffen auf private IoT-Objekte und Infrastrukturen ist abhängig vom Grad der Vernetzung. Dies kann von nicht mehr funktionierenden Beleuchtungselementen (Stichwort: Philips Hue), bis zum Totalausfall aller smarten und intelligenten Komponenten führen.

Im industriellen Umfeld sind die Auswirkungen größer, weil gesamte Produktionsstätten ausfallen könnten. Selbst der Angriff auf ein System bringt hier den Wertschöpfungsprozess zum Erliegen, wodurch ein wirtschaftlicher Schaden entstehen würde.

Betrachtet man das Gefahrenpotential aus gesellschaftlicher Sicht, so ist dies eine Bedrohung, die den Alltag vieler Menschen einschränken und auch schädigen könnte. Wichtige Infrastrukturen wie Gesundheitseinrichtungen, Versorgungsanbieter oder einfache Verkehrssteuerungssysteme könnten aufgrund falsch konfigurierter oder fehlender Sicherheitsmechanismen kompromittiert werden und dadurch für Chaos in der Bevölkerung sorgen. Die Politik, die Unternehmen, aber auch jede einzelne Kundin und jeder einzelne Kunde sind hier gefordert, für geeignete Sicherheit bei den verwendeten IoT-Objekten und IT-Systemen zu sorgen.

4.4 Eingriffe in die Privatsphäre

Neben der Störung der Funktionalitäten von IoT-Objekten sind mögliche Eingriffe in die Privatsphäre der Benutzerinnen und Benutzer ein weiteres Problem unsicherer IoT-Systeme. Mittels IoT drängen immer mehr smarte Endgeräte und Produkte in den Alltag vieler Menschen. Smarte Fernseher, IP-Kameras und smarte Küchengeräte geben vor, das Leben der Menschen zu vereinfachen, indem sie mittels moderner Algorithmen und der Verbindung zum Internet versuchen, ihren Betrieb zu optimieren und von überall aus fernsteuerbar sind. (Reinwarth, 2017)

Viele IoT-Objekte sammeln Daten über den laufenden Betrieb, um laut Hersteller das Produkterlebnis stetig zu verbessern. Die Datenaufzeichnung findet sich in den AGBs und den Nutzungsbestimmungen der IoT-Produkte und deren Cloud-Plattformen wieder. (Weber, 2009)

Diese Form der Datenaufzeichnung wird von Datenschützerinnen und Datenschützer kritisiert, weil häufig nicht transparent dargestellt ist, welche Daten, für welchen Zweck, wann und an wen übermittelt werden. (Medaglia & Serbanati, 2010) Im Beispiel der Foscam-Produkte (Abschnitt 3.2) wurden Daten an Server nach China und in die USA übermittelt. Es gibt hier keine Belege oder Statements seitens des Herstellers, welche Daten übermittelt werden und zu welchem Zweck. (Dölle, 2016)

Neben der Datenaufzeichnung durch den Hersteller und der Cloud-Plattform Provider besteht die Möglichkeit, dass IoT-Objekte von unbefugten Dritten kompromittiert werden und Daten von der Nutzerin und dem Nutzer aufzeichnen. (Roman, Zhou, & Lopez, 2012)

Dieser illegale Eingriff in die Privatsphäre stellt ein großes Problem dar, weil viele IoT-Objekte teils an privaten Örtlichkeiten angebracht und platziert sind. Hier entsteht ein tiefer Eingriff in die Privatsphäre der Menschen, der für unterschiedlichste Zwecke verwendet werden kann. Ransomware, der Begriff wurde im Abschnitt 3.1 diskutiert, kann als Druckmittel private Fotos und Videos verwenden und damit drohen, diese der Öffentlichkeit zur Verfügung zu stellen, wenn ein gewisser Lösegeldbetrag nicht bezahlt wird.

Mittels der Kombination unterschiedlicher IoT-Objekten, die den Tagesablauf der Menschen verfolgen, besteht zudem die Möglichkeit, Bewegungsprofile und genaue Muster von täglichen Routinen abzuleiten. (Santos, Rodrigues, & Casal, 2016)

Es ist nicht absehbar, wie Daten aus IoT-Objekten, die legal oder illegal aufgezeichnet wurden, verwendet werden. Gerade Big Data Technologien können aus der großen Menge an verschiedenen Daten neue Erkenntnisse gewinnen. Deshalb ist ein sorgsamer und sparsamer Umgang mit Daten aus IoT-Objekten essentiell, um für genügend Privatsphäre zu sorgen. Sobald Daten aufgezeichnet und an Dritte übertragen wurden, können diese nur noch sehr schwer aus dem Internet und von den Servern entfernt werden.

4.5 Zusammenfassung

Dieses Kapitel fasste Bedrohungen, die von unsicheren IoT-Objekte und Systemen ausgehen, zusammen, welche sich sowohl auf den privaten als auch öffentlichen Bereich auswirken können. Ein Zusammenschluss aus kompromittierten IoT-Objekten zu einem Botnetz-Verbund kann wichtige IT-Services und Dienstleistungen mittels gezielter DDoS-Attacken lahmlegen. Deswegen sind weitere Internetdienste, die dieses IT-Services nutzen, wie einem DNS-Dienstleister, nicht mehr für ihre Kundinnen und Kunden erreichbar.

Durch die zunehmende Vernetzung wichtiger Industrien und kritischer Infrastrukturen entstehen neue Bedrohungsszenarien, welche zuvor nicht vorhanden waren. Ein IoT-Botnetz wie Mirai (Abschnitt 4.1.1) zeigt, welche Gefahr von ungesicherten IoT-Objekten ausgeht. Ein Worst-Case Szenario wäre ein Angriff auf kritische Infrastrukturen mittels eines Botnetzes, wodurch ganze Länder im Chaos versinken würden.

Im privaten Bereich können IoT-Objekte private Details aufzeichnen und an unbefugte Dritte weiterleiten, sofern das IoT-Objekt selbst unzureichend geschützt ist. Hier können Aufzeichnungen von IP-Kameras als Druckmittel eingesetzt werden, um einen Geldbetrag zu erpressen. Wichtige private Infrastrukturen, wie Heizung oder Licht können durch Dritte übernommen, gestört oder gar zerstört werden.

IoT-Suchmaschinen steigern darüber hinaus die Gefahr an neuen Angriffen. Sie machen es Hackern und technisch interessierten Personen einfach, nach kompromittierbaren IoT-Systemen zu suchen, die anschließend für illegale Zwecke missbraucht werden können.

Allgemein ist zu sagen, dass diese Suchmaschinen ebenso eine Transparenz-Funktion darstellen. Erst Shodan ermöglichte der breiten Öffentlichkeit, Einblick zu bekommen, wie unsicher aktuelle IoT-Objekte und in welchem Ausmaß diese verbreitet sind.

Botnetze und DDoS-Attacken stellen die größte Gefahr dar. Diese können nicht nur IT-Services betreffen, sondern ganze Länder, wie das Beispiel Ukraine zeigte (Abschnitt 4.3), in der das nationale Stromnetz für Stunden stillstand. Aus diesem Grund ist jede Benutzerin und jeder Benutzer von IT-Systemen und IoT-Objekten aufgefordert, entsprechende Sicherheitsfunktionen korrekt zu konfigurieren und Systeme vor möglichem Missbrauch und Angriffen zu schützen.

5 IOT-SECURITY FRAMEWORK

Dieses Kapitel beschreibt die Entwicklung des IoT-Security Framework, das Kundinnen und Kunden und spätere Nutzerinnen und Nutzern bei der Beurteilung der Sicherheitseigenschaften von IoT-Objekten unterstützen soll. Grundlage für dieses Security Framework bilden die vorhergehenden Kapitel, in welchen Basiswissen zu IoT vermittelt wurde, IoT-Objekte in Bezug auf ihre Sicherheit analysiert und Risiken und Bedrohung, welche von unsicheren IoT-Objekten ausgehen, beschrieben wurden.

Die Sicherheit beschränkt sich nicht auf die eigene Sicherheit des IoT-Objekts gegenüber Angriffen von außen, sondern beinhaltet auch die IT-Sicherheit der bestehenden Infrastruktur, die durch die Integration beeinflusst werden kann. Deshalb sollen Sicherheitsmerkmale neben aktuellem Betriebssystem und Firmware auch aktuelle Standards verwenden, wodurch die Sicherheit gewährleistet werden kann.

Die Zielgruppe dieses Security Frameworks ist der private Bereich, und somit die Gruppe der Endkundinnen und Endkunden. Es kann nicht für den betrieblichen Bereich genutzt werden, weil nicht auf geschäftsspezifische Besonderheiten eingegangen wird. Deshalb richtet sich dieses Security Framework ausschließlich an private Personen, kann aber als erster Anhaltspunkt für den geschäftlichen Bereich herangezogen worden.

Dieses Security-Framework soll als Basis der Beurteilung neuer IoT-Objekte dienen und die Kaufentscheidung in Bezug auf IT-Sicherheit unterstützen. Das Security Framework geht von einer sicheren, gewarteten und betreuten IT-Infrastruktur aus. Aus diesem Grund wird nicht auf die Sicherheit von IT-Infrastrukturen selbst eingegangen, sondern nur auf die Sicherheit von IoT-Objekten, die in diese integriert werden. Dieses neue IoT-Objekt soll weder die bestehende IT-Sicherheit gefährden noch sich selbst durch fehlende oder falsch konfigurierte Sicherheitsmerkmale.

Zuerst werden in Abschnitt 5.1 Objekte und Systeme identifiziert, die für ein sicheres IoT-System und eine IT-Infrastruktur notwendig sind. Notwendige Sicherheitsmerkmale und Voraussetzungen dieser Objekte und Systeme werden in Abschnitt 5.2 beschrieben.

Diese Sicherheitsmerkmale werden wegen ihrer Notwendigkeit und des Einflusses auf die Sicherheit von IT-Systemen und den IoT-Objekten beurteilt. Nach erfolgter Beurteilung werden die Sicherheitsmerkmale in Abschnitt 5.3 in Risikoklassen eingeteilt, die sich sowohl in ihrer Auswirkung auf die IT-Sicherheit als auch Privatsphäre sowie dem Gefahrenpotential unterscheiden.

Im Abschnitt 5.4 wird anschließend der Integrationsprozess eines IoT-Objekts in bestehende IT-Infrastrukturen beschrieben. Dieser Abschnitt beinhaltet außerdem die Operationalisierung der Hypothesen (Abschnitt 5.4.1), und die Beantwortung der Forschungsfrage (Abschnitt 5.4.2). Abschnitt 5.5 fasst die Ergebnisse des Security Frameworks zusammen.

5.1 Identifikation der betroffenen Objekte und Systeme

Wie im Abschnitt 2.3 beschrieben, besteht eine IoT-Architektur aus einer Kombination von unterschiedlichen Technologien und Komponenten. Diese sind sowohl physikalische Komponenten, wie IP-Kameras und Aktoren, als auch virtuelle Komponenten, zu denen die Software und Cloud-Plattformen zählen.

Die Abgrenzung zur bestehenden IT-Infrastruktur ist die Anbindung an das lokale Netzwerk und dem Internet. Aus diesem Grund ist die Verbindung zwischen IoT-Objekt und IoT-Gateway zu diesem Endgerät der Endpunkt der hier abgedeckten Objekte und Systeme. (vergleiche Abbildung 24)

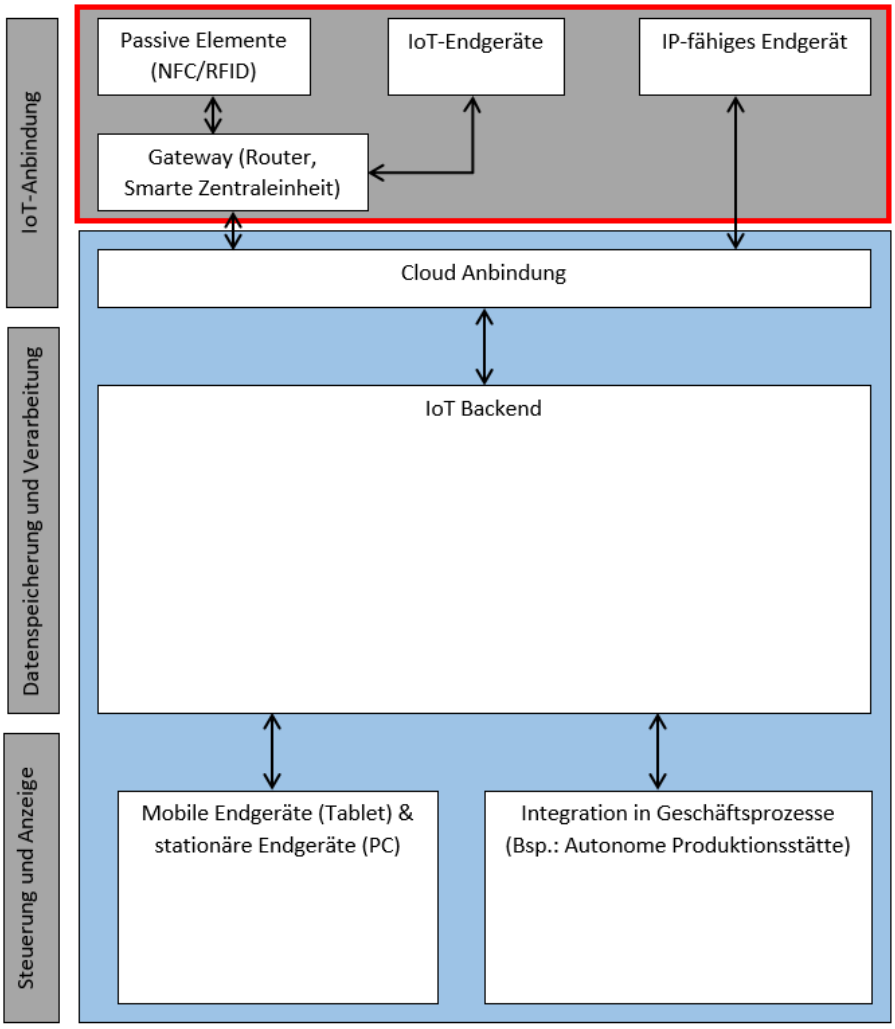


Abbildung 24 Abgrenzung - IoT Objekte (Müller, 2016)

Zu den physikalischen Objekten, die in diesem IoT-Framework behandelt werden, gehören:

- IoT-Objekte,
- IoT-Gateways, auch vielfach als Smart Gateways bezeichnet,
- Sensoren und Aktoren, welche mit den IoT-Objekten kommunizieren.

Jegliche Router, Switches und sonstige Netzwerkgeräte, welche die Verbindung zum lokalen Netzwerk und Internet bereitstellen, sind nicht Teil dieses IoT-Security Frameworks.

Zu den virtuellen Objekten und Systemen, die in diesem IoT-Security Framework behandelt werden gehören:

- Kommunikationstechnologien,
    - Übertragungsstandards (siehe Abschnitt 2.3.4),
    - Datenaustauschformate (siehe Abschnitt 2.3.5),
    - Datenübertragungsprotokolle,
- Cloudplattformen (siehe Abschnitt 2.3.3),
- Betriebssystem und Firmware des IoT-Objekts (siehe Abschnitt 2.3.2),
    - Webinterface,
    - Mobile Applikation,
- Integrierte Sicherheitsmechanismen und Verschlüsselungsmöglichkeiten.

Diese Gruppen von Objekten und Systemen werden in den nächsten Abschnitten als Basis dienen. Ein IoT-Ecosystem besteht aus unterschiedlichen Konstellationen und Kombination aus den oben genannten Objekten und Systemen.

Aus diesem Grund werden in den nächstfolgenden Abschnitten jeweils die Standardlösungen und Defacto-Standards in das Security Framework einbezogen, weil hierfür entsprechende Publikationen und Best-Practice Dokumentationen vorhanden sind.

Jegliche nicht dokumentierten und proprietären Systeme können nicht in das Security Framework einfließen. Da vielfach die Produktspezifikationen intransparent formuliert oder nicht verfügbar sind, ist eine Bewertung solcher IoT-Objekte nicht möglich.

5.2 Sicherheitsanforderungen

Dieser Abschnitt beschäftigt sich mit den Sicherheitsanforderungen, die ein IoT-Objekt und damit verbundene Technologien aufweisen müssen, um die Sicherheit der bestehenden IT-Infrastruktur und jene des Objekts selbst zu wahren.

Die hier aufgeführten Anforderungen basieren auf dem aktuellen Stand der Wissenschaft und Technik (Stand: Juli 2017), und kombinieren daneben das Wissen, welches in den vorhergehenden Kapiteln erarbeitet wurde.

Das Security Framework unterteilt diese Anforderungen in drei Kategorien, die in weiterer Folge beschrieben werden. Im Abschnitt 5.3 werden diese Anforderungen hinsichtlich ihrer Auswirkung auf die Sicherheit und der potentiellen Gefährdung in Risikoklassen eingeteilt. Anhand dieser können zukünftige Kundinnen und Kunden von IoT-Objekten das Gefährdungspotential dieser beurteilen und entsprechende Sicherheitsmaßnahmen ableiten.

5.2.1 Anforderungen an das IoT-Objekt

Die Anforderungen an das IoT-Objekt sind vielfältig und reichen von der Aktualität des Betriebssystems und der Firmware bis hin zur Transparenz der Kommunikation zwischen Kundinnen und Kunden mit dem Hersteller.

Zu Beginn ist es notwendig herauszufinden, wie aktuell das Betriebssystem und die Firmware des IoT-Objektes sind. Dazu besucht man die Hersteller-Website und ruft dort das aktuelle Datenblatt sowie Informationen über das Betriebssystem und die Firmware auf.

Oft bieten Hersteller sogenannte Downloadbereiche an, in denen Updates für das Betriebssystem und der Firmware zur Verfügung gestellt werden. Hier werden auch Release Notes und Versionshinweise bereitgestellt, welche wichtige Informationen zum Update beinhalten.

Allgemein lässt sich keine Aussage über das maximale Alter eines Betriebssystems und Firmware tätigen, ab wann diese veraltet und als kritische zu betrachten sind. Vielmehr ist es notwendig Recherche zu betreiben, bekannte Newsportale zum Thema IoT und IT-Sicherheit zu besuchen und CVE-Datenbanken (Common Vulnerabilities and Exposures) auf eingetragene Systemlücken zu prüfen.

Wenn keine Bedrohungen oder mögliche Lücken entdeckt werden, muss als nächstes der Update-Prozess des Betriebssystems und der Firmware betrachtet werden. Dieser soll so einfach wie möglich gestaltet sein und die Nutzerin und den Nutzer auf neue Updates aufmerksam machen, sobald diese verfügbar sind. Ist dieser Prozess so gestaltet, wie im Beispiel von Foscam (Abschnitt 3.2), muss eine Update-Strategie entwickelt werden, um die Sicherheit gewährleisten zu können. Der Transport- und der Upload-Prozess des Updates auf das IoT-Objekt muss verschlüsselt erfolgen, sodass diese nicht von außen kompromittiert werden können.

Neben dem Update-Prozess muss der Zugang zum Webinterface, der Steuerungs- und Konfigurationsseite verschlüsselt erfolgen. Dies ist mittels des Datenblatts und der Produktspezifikation zu analysieren, ob hier eine HTTPS-Verbindung möglich ist. (siehe Abschnitt 2.3.4)

Als nächstes gilt es, die Konfiguration und Anmeldemöglichkeiten zu betrachten. Hier ist es entscheidend, welche Passwortkomplexität angeboten und verlangt wird. Benötigt man ein Default-Passwort, das zu denen im Botnetz von Mirai (Abschnitt 4.1.1) verwendeten gehört, so ist dieses umgehend und vor dem Anschluss an das Internet zu ändern, da ansonsten das IoT-Objekt in wenigen Sekunden infiziert werden kann. (Abschnitt 4.1.2)

Ist eine ausreichende Mindestkomplexität des Passwortes gegeben und muss dieses auch nach dem ersten Login geändert werden. Als nächstes gilt es zu überprüfen, ob der Benutzername geändert werden kann und Rechte für die Benutzerinnen und Benutzer des IoT-Objekts eingeschränkt werden können. Damit kann gewährleistet werden, dass automatisierte Skripte und Botnetze sich nicht in das IoT-Objekt einloggen können, weil diese nur Default-Usernamen verwenden und der Zugriff deshalb nicht möglich ist. Das Minimumprinzip an Rechten gilt ebenso im Bereich von IoT, sodass hier, wenn möglich, unterschiedliche Benutzerkonten eingerichtet

werden können. Hiermit werden Administrationsfunktionen von den eigentlichen IoT-Funktionen getrennt. Des Weiteren wird die Problematik von wiederverwendeten Passwörtern umgegangen.

Bei IoT-Objekten, die zu den kritischen Infrastrukturen gehören oder diese überwachen und steuern, soll zudem eine Zwei-Faktor-Authentifizierung vorhanden sein. Diese garantiert die Sicherheit, auch nachdem Zugangsdaten möglicherweise durch Dritte ermittelt oder Sicherheitsmechanismen des IoT-Objekts kompromittiert wurden.

Neben sicheren Authentifizierungsmechanismen sind Mechanismen zur Erkennung von Angriffen in IoT-Objekten essentiell. Dazu gehört ein Mechanismus, der nach einer bestimmten Anzahl fehlerhafter Login-Versuche die Source-IP-Adresse blockiert. Das verhindert mögliche Brute-Force-Attacken, welche von vielen Schadprogrammen und Botnetzen durchgeführt werden, um Zugang zu neuen IoT-Objekten zu erhalten.

Als nächstes wird der Auslieferungszustand des IoT-Objekts analysiert. Hier gilt, ähnlich wie bei der Rechtekonfiguration, das Prinzip des Minimalismus. Dienste wie dynamische DNS, P2P (Peer to Peer) und UDP-Tunnel sollten, wenn möglich, deaktiviert sein. Dies ist bei Foscam nicht der Fall, wodurch Daten zu Beginn der Erstkonfiguration an Server übertragen werden (Abschnitt 3.2). Jegliche Umgehung von Sicherheitskonfigurationen eines Routers oder einer Router-Firewall gefährdet die Sicherheit aller Endgeräte in diesem Netzwerk. Dabei sollte keinesfalls Konfigurationskomfort vor IT-Sicherheit stehen, weil dies unweigerlich zu Lücken und Angriffspunkten im IT-System und Netzwerk führt.

Neben der Auslieferungskonfiguration ist der Prozess der Konfiguration selbst wichtig, damit das IoT-Objekt entsprechend einfach und sicher konfiguriert werden kann. IoT-Objekte, die aufgrund ihres Webinterfaces schwierig und unverständlich zu konfigurieren sind, stellen für jede Nutzerin und jeden Nutzer ein Problem da, welches schlussendlich zu einem ungeschützten und angreifbaren IoT-Produkt führen kann.

Jede Käuferin und jeder Käufer geht beim Kauf eines IoT-Objekts und der Inbetriebnahme dieses einen Vertrag mit dem Hersteller ein. Dabei akzeptierten sie und er die AGBs des Herstellers, die entweder in schriftlicher oder digitaler Form dem IoT-Objekt beiliegen.

Diese sollten immer gelesen werden, weil ein IoT-Objekt, je nach Einsatzzweck, private Einblicke und Daten erfassen kann. Aus diesem Grund ist es wichtig zu wissen, welche Daten, wie, an wen, wann übertragen werden. Ein möglicher Eingriff und daraus resultierende Verletzungen der Privatsphäre sollten vorab durch genaue Analyse der AGBs verhindert werden. Dabei hilft ebenfalls ein Blick in bekannte IoT-Portale und Magazine, jedoch ist dies kein Ersatz für die Analyse der AGBs und Vertragsdetails.

Abschließend ist der Hersteller im Allgemeinen zu betrachten. Generell gilt, je transparenter und kommunikativer dieser auf die Anregungen der Kundinnen und Kunden eingeht, umso sicherer und aktueller sind seine IoT-Objekte. OEM-Hersteller (Abschnitt 3.3) sind schwer ausfindig zu machen und der Importeur und Verkäufer bietet oft keinen technischen Support.

Deshalb fließt die Reputation des Herstellers in das IoT-Security Framework ein. Diese sorgt dafür, dass die Kundin und der Kunde bei möglichen Problemen und Fragen, qualitativ hochwertigen Support bekommt.

Die nachfolgende Tabelle (Tabelle 3) fasst die wichtigsten Eigenschaften eines sicheren IoT-Objekts zusammen.

Prozess:	**Eigenschaft:**	**Anforderung:**
1. Überprüfung des Betriebssystems/ Firmware	Aktualität des Betriebssystems/Firmware	Abhängig von bekannten Sicherheitslücken
2. Beurteilung des Update-Prozesses	Kommunikation von Updates	Automatische Updates/Updatebenachrichtig-ungen, sicherer Updateprozess (verschlüsselte Übertragung)
3. Beurteilung der Sicherheit des Webinterfaces	Verwendete Standards und Protokolle	Verschlüsselte Verbindung (HTTPS)
4. Beurteilung der Authentifizierungs-mechanismen	Passwortkomplexität, Benutzerzugänge, Rechteverwaltung	Hohe Mindestkomplexität der Passwörter, unterschiedliche Benutzerzugänge, granulare Rechteverwaltung, Einschränkung von Administrationsfunktionalitäten
5. Beurteilung der Schutzmechanismen vor Brute-Force Angriffen	Sicherheitsmechanismen	Automatische Blockierung des Logins ab einer bestimmten Anzahl von fehlerhaften Logins
6. Beurteilung des Auslieferungszustandes	Default-Konfiguration	Möglichst wenig aktive Dienste, sichere Default-Zugangsdaten, automatische Passwortänderung bei erstem Login
7. Beurteilung der Konfigurations-Möglichkeiten des Webinterfaces	Webinterface und Einstellungsmöglichkeiten	Intuitives Webinterface mit verständlichen Konfigurationsmöglichkeiten
8. Beurteilung der AGBs und Reputation des Herstellers	Kundenfreundlichkeit und transparente Kommunikation	Bereitstellung einer Plattform (Forum), aktive Kommunikation mit den Kundinnen und Kunden, verständliche und kundenfreundliche AGBs

Tabelle 3 Eigenschaften sicherer IoT-Objekte

5.2.2 Anforderungen an eine sichere Kommunikation

Dieser Abschnitt beschreibt die Anforderungen an eine sichere Kommunikation zwischen den IoT-Objekten selbst und einem IoT-Gateway, falls dieses Teil des IoT-Ecosystems ist. Hier wird zwischen zwei unterschiedlichen Bereichen unterschieden. Dazu wird einerseits die Kommunikation zwischen den IoT-Objekten selbst, und andererseits mit einem IoT-Gateway analysiert, sowie die Kommunikation der IoT-Objekte und der IoT-Gateways mit dem Internet, folglich einem Router oder anderen Netzwerkkomponenten.

Zu Beginn gilt es zu analysieren, welche Übertragungsstandards verwendet werden. Dazu nutzt man das Produktdatenblatt und Internetressourcen, die durch den Hersteller bereitgestellt werden. Hierzu muss zudem festgestellt werden, wie die Kommunikationsarchitektur des IoT-Objekts grundsätzlich strukturiert ist.

Dabei muss die gesamte Kommunikationsstruktur analysiert werden. Entscheidend ist, ob das IoT-Objekt direkt mit einem Router und dem Internet kommuniziert, oder ob ein IoT-Gateway dazu genutzt wird. Dies ist im Produktdatenblatt ersichtlich und entscheidend für den weiteren Verlauf des Analyseprozesses.

Die Kommunikation von IoT-Objekten untereinander oder mit einem IoT-Gateway kann über unterschiedliche Protokolle und Übertragungstechnologien erfolgen (siehe Abschnitt 2.3.4 und Abschnitt 2.3.5). Wenn Ethernet, oder WLAN angegeben werden, so ist auf die Sicherheitsimplementierungen zu achten, die bereitgestellt werden.

Basiert die Kommunikation auf WLAN, so ist auf eine aktuelle Implementierung von Sicherheitsstandards zu achten. Aktuell (Stand: Juli 2017) ist die sicherste WLAN-Verschlüsselung WPA2 (Wi-Fi Protected Access) (Lashkari, Danesh, & Samadi, 2009). Des Weiteren müssen Passwörter, die eine hohe Komplexität aufweisen sowie den vollen Zeichensatz verwenden, unterstützt werden. Ist dies nicht gegeben, kann die bestehende IT-Sicherheit nicht mehr im vollen Umfang garantiert werden, weil bestehende Passwörter in ihrer Komplexität verringert werden müssen. Eine mögliche Alternative wären abgrenzte Netzwerke, welche häufig durch eine Gast-WLAN-Funktion realisiert werden. (Yi, Quin, & Li, 2015)

Neben der Passwortkomplexität und der verwendeten Verschlüsselungstechnologie wird von vielen Expertinnen und Experten das Deaktivieren des SSID-Broadcasts (Service Set Identifier) empfohlen. Dies ist eine Möglichkeit sein WLAN vor anderen zu verbergen, wodurch sich niemand mit einer Standard-Software mit damit verbinden kann. Es schützt jedoch nicht vor professionellen Hackern, die mittels spezieller Hard- und Software den gesamten Datenstrom im WLAN-Frequenzband analysieren und anhand der Datenpakete die SSID extrahieren können. (Berghel & Uecker, 2004) und (Blumenthal, 2003)

Bieten IoT-Objekte die Funktion an, die WLAN-SSID manuell einzutragen, kann die bestehende Konfiguration der IT-Infrastruktur übernommen werden, falls nicht, und der SSID-Broadcast ist deaktiviert, muss eine Lösung gefunden werden, das IoT-Objekt in die Infrastruktur integrieren zu können. Hier könnte der ähnliche Ansatz verwendet werden, der im Absatz zuvor beschrieben wurde.

Erfolgt die Kommunikation über Bluetooth, muss die verwendete Bluetooth Spezifikation und Version eruiert werden. Aktuell (Stand: Juli 2017) ist Bluetooth-LE (Low Energy) weit verbreitet, was aber durch Proof-of-Concept Studien bereits kompromittiert wurde. Die Gefahr selbst ist örtlich einzugrenzen, weil der Angriff nur in räumlicher Nähe zum IoT-Objekt durchgeführt werden kann. (Ryan, 2013)

Ähnliches gilt für IoT-Objekte, die mittels ZigBee Profilen und ZWave kommunizieren. Diese Protokolle und Übertragungsstandards sind auf Energieeffizienz und kleine Datenpakete ausgerichtet und bieten daher schwache bis keine Sicherheitsmechanismen. (siehe Abschnitt 2.3.4) (Georgakakis, Nikolidakis, Vergados, & Douligeris, 2010), (Fouladi & Ghanoun, 2016) und (Boyle & Newe, 2007)

Ortsgebundene Übertragungstechnologien, die eine geringe Reichweite von wenigen Metern aufweisen, können eine Gefahr für die IT-Sicherheit bestehender Infrastrukturen sein. Angriffsvektoren, die Lücken in den Sicherheitsimplementierungen von solchen Übertragungsmedien nutzen, müssen zwingend nahe am jeweiligen IoT-Objekt und der Infrastruktur durchgeführt werden. Dies ist vor allem in dicht besiedelten Gebieten wie Großstädten einfach zu realisieren. Es sind bereits erste Publikationen veröffentlicht worden, die diesen Angriffsvektor nutzen und dadurch Angriffe realisiert haben. (Georgakakis, Nikolidakis, Vergados, & Douligeris, 2010), (Fouladi & Ghanoun, 2016) und (Boyle & Newe, 2007)

Der nächste Schritt beinhaltet die Analyse der Netzwerkfreigaben und Ports, die durch das IoT-Objekt benötigt werden. Hier versuchen IoT-Objekte häufig mittels UPnP vordefinierte Ports im Router, der diese Funktion aktiviert haben muss, freizuschalten.

Damit werden Sicherheitseinrichtungen, wie Router-Firewalls aufgeweicht, ohne dass die Nutzerin und der Nutzer dies bemerken. Aus diesem Grund ist die UPnP-Funktion vor einer Integration eines IoT-Objekts zu deaktivieren, falls dies noch nicht der Fall ist. (Selen, 2012)

Als nächstes ist zu analysieren, welche Ports im Auslieferungszustand bereits offen sind. Dazu können sogenannte Port-Scanner genutzt werden. Je nach Konfiguration können Ports für Webserver (80, 8080 oder 443) und zusätzliche Streaming-Ports geöffnet sein. Die Ergebnisse des Portscans müssen anschließend mittels Internet-Recherche analysiert werden. Dazu muss der Port seiner Anwendung und dem genutzten Protokoll zugeordnet werden. Das identifizierte Protokoll ist danach auf seine Sicherheit zu überprüfen. Hier gilt, dass jegliche Datenaustauschformate und Protokolle, die ihre Daten mittels Klartext übertragen, auszuschließen sind.

Dieser Vorgang ist sicherlich der schwierigste, weil Recherche in unterschiedlichen Literaturverzeichnissen und Quellen betrieben werden muss. Er ist essentiell für die weitere Konfiguration des IoT-Objekts, weil auf diese Weise unsichere Anwendungen und Übertragungsprotokoll erkannt und gegebenenfalls deaktiviert werden können.

Durch diesen Ablauf kann eine sichere und verschlüsselte Übertragung zwischen den IoT-Objekten selbst und einem IoT-Gateway sowie dem Internet, gewährleistet sein. Trotzdem sind klare Angriffspunkte erkennbar, die nur durch örtliche Nähe ausgenutzt werden können.

Die nachfolgende Tabelle (Tabelle 4) fasst die wichtigsten Eigenschaften einer sicheren Kommunikation zusammen:

Prozess:	**Eigenschaft:**	**Anforderung:**
9. Identifikation der Kommunikationsarchitektur	Direkte Internetverbindung, Nutzung von IoT-Gateways	
10. Identifikation der verwendeten Übertragungstechnologien und Datenaustauschformate	Verwendete Standards und Protokolle	Verschlüsselte Übertragung
11. Analyse der Sicherheitsmerkmale der Internetverbindung	Ethernet, WLAN, Sicherheitsstandards	Unterstützung aktueller Sicherheitsstandards, Unterstützung längerer Passwörter mit gesamten Zeichensatz, Unterstützung manueller SSID-Eintragung
12. Beurteilung der internen Kommunikation im IoT-Ecosystem	Verwendete Technologie und Standards	Verwendung aktueller Standards, Beurteilung der örtlichen Gegebenheiten
13. Analyse der notwendigen Port-Freigaben des IoT-Objekts	Verwendete Standards und Protokolle	Möglichst wenig offene Ports, Nutzung verschlüsselter Standards und Übertragungsprotokolle

Tabelle 4 Eigenschaften sicherer Kommunikation

5.2.3 Anforderungen an Cloud-Plattformen und externe Services

Dieser Abschnitt beschreibt die Sicherheitsanforderungen an eine IoT-Cloudplattform und externe Services, wie mobile Applikationen. Da diese von Herstellern gewartet und betrieben werden, können hier nur Basisanforderungen analysiert und bewertet werden.

Die Analyse und Bewertung der Cloudplattform und externer Services, die mit einem IoT-Objekt und IoT-Ecosystem verknüpft sind, beginnt mit der Feststellung, ob diese verpflichtend sind oder zusätzliche Funktionen darstellen, und diese für den Basisbetrieb nicht notwendig sind. Generell stellen verpflichtende externe Services immer ein Risiko dar, weil diese nicht im Einflussbereich der Kundin und des Kunden stehen.

Der nächste Schritt beinhaltet die Bewertung des Authentifizierungs- und Registrierungsprozesses. Dabei gelten dieselben Vorgaben, die im Abschnitt 5.2.2 bereits erläutert wurden. Hinzuzufügen ist die Analyse des Passwort-Recovery Prozesses. Dieser soll durch eine Geheimfrage geschützt sein, die nur durch die Besitzerin und den Besitzer beantwortet

werden kann. Des Weiteren soll der Zurücksetzungslink an eine vorher in der Plattform definierte private E-Mail-Adresse versendet werden, sodass weiteres Wissen notwendig ist, um das Passwort ändern zu können.

Neben der Sicherheit des Registrierungsprozesses ist der Schutz der Privatsphäre zu beurteilen. Dabei muss analysiert werden, welche Daten für eine Registrierung notwendig sind, und ob diese einen Eingriff in die Privatsphäre darstellen.

Als nächstes muss die Verbindung zur Plattform selbst, die über einen Webbrowser realisiert wird, bewertet werden. Hier ist auf eine verschlüsselte Verbindung via HTTPS zu achten. Neben dem Interface der Plattform sind mobile Applikationen auf ihre Sicherheit zu prüfen.

Hersteller stellen eigene Applikationen für diverse Plattformen bereit. Diese verfügen, wie im Beispiel von Foscam (siehe Abschnitt 3.2), über eine Authentifizierung mittels Cloud-Zugang. Das ist zwar für die Nutzerin und dem Nutzer komfortabel, reduziert jedoch die Sicherheit des IoT-Objekts, weil die eigentlichen Zugangsdaten auf den Servern des Herstellers gespeichert sind.

Von Vorteil wäre eine manuelle Konfiguration der Zugangsdaten der jeweiligen IoT-Objekten, ohne dass Daten auf Server übertragen werden müssen. Falls dem nicht so ist, können alternative Steuerungsapplikationen, welche die Protokolle des IoT-Objekts unterstützen, genutzt werden.

Zusätzlich zur Cloud-Plattform werden dynamische DNS-Dienste von IoT-Herstellern bereitgestellt, um diese direkt über das Internet erreichbar machen zu können. Diese sollten aus Sicherheitsgründen nicht genutzt werden, weil dadurch ein Angriffsvektor direkt am IoT-Objekt geöffnet wird. Eine sicherere Lösung ist es, einen dynamische DNS-Dienst direkt am Router oder Internetendpunkt zu aktivieren, weil diese über entsprechende Sicherheitsmechanismen verfügen und als zentraler Zugangspunkt agieren.

Zusammengefasst stellen Cloud-Plattformen und externe Services Komfortfunktionen bereit, die das Nutzungserlebnis verbessern und den Einstieg in die Welt von IoT erleichtern. Sie liegen allerdings nicht im Einflussbereich der Kundinnen und der Kunden, wodurch immer eine gewisse Intransparenz und Unsicherheit gegeben ist. Aus diesem Grund sollen Services, die auf Cloud-Plattformen und externen Applikationen basieren, gemieden werden, um mögliche Sicherheitsrisiken ausschließen zu können. Eine allgemeine Gefahr für eine IT-Infrastruktur besteht nur dann, wenn Zugangsdaten zu IoT-Objekten auf den Servern der Hersteller abgelegt sind und dort von unbefugten Dritten entwendet werden können.

Die nachfolgende Tabelle (Tabelle 5) fasst die wichtigsten Eigenschaften einer sicheren Cloudplattform und externen Services zusammen:

Prozess:	**Eigenschaft:**	**Anforderung:**
14. Identifikation der Notwendigkeit der Cloudplattform und externer Services	Funktionen verknüpft mit Cloud-Komponenten	Cloud-Plattformen und externe Services nicht zwingend erforderlich
15. Beurteilung des Authentifizierungs- und Registrierungsprozess	Verwendete Standards und Umgang mit Privatsphäre	Verschlüsselte Übertragung der Daten, wenig Daten für Registrierung notwendig
16. Analyse der externen Services	Dynamische DNS, Cloudapplikationen	Deaktivierung und Nutzung von dynamischen DNS-Diensten von Routern und Modems
17. Beurteilung der mobilen Applikationen	Verwendete Technologie und Standards	Verwendung aktueller Standards und Verschlüsselungen, Nutzung der manuellen Konfiguration
18. Analyse des Passwort-Recovery-Prozesses	Sicherheit des Prozesses	Nutzung von Sicherheitsfragen, Zwei-Faktor-Authentifizierung, E-Mail Link an private E-Mail-Adresse

Tabelle 5 Eigenschaften sicherer Cloud-Plattformen und externer Services

5.3 Risikoklassen

Dieser Abschnitt beinhaltet die Gliederung der IoT-Risikoklassen, welchen dementsprechende Sicherheitseigenschaften und Anforderungen zugeordnet werden. Anhand dieser Risikoklassen können zukünftige IoT-Kundinnen und IoT-Kunden IoT-Objekte bewerten und die Sicherheit dieser beurteilen.

Die Risikoklassen unterscheiden sich in ihren Anforderungen an die Sicherheit eines IoT-Objekts. Somit wird gewährleistet, dass IoT-Produkte objektiv beurteilt und verglichen werden können. Mit der richtigen Zuordnung eines IoT-Objekts zu einer Risikoklasse kann je nach Einsatzszenario das richtige Produkt ausgewählt werden.

Dieses IoT-Security Framework unterteilt IoT-Objekte in vier unterschiedliche Risikoklassen. Klasse 0 beschreibt ein sicheres IoT-Produkt ohne jegliche Einschränkung. Die darauffolgenden Klassen besitzen, je nach ihrem Gefahrenpotential eine geringere IT-Sicherheit, wobei Klasse 3 die unsicherste darstellt.

Die Klassen unterscheiden sich wie folgt:

- Klasse 0:
  - Aktuelles Betriebssystem und Firmware,
  - Schnelle Reaktion des Herstellers auf Sicherheitsprobleme (Updates),
  - Einfacher, transparenter und automatischer Updateprozess,
  - Sicheres Webinterface (hohe Mindestkomplexität, Passwort kann aus dem gesamten Zeichensatz bestehen, verschlüsselter Zugang),
  - Rechteverwaltung (eingeschränkte Konten getrennt von Administrator),
  - Sicherheitsmechanismen zur Erkennung und Verhinderung von Brute-Force Attacken,
  - Hersteller besitzt gute Reputation,
  - Sichere und verschlüsselte Kommunikation zwischen dem IoT-Produkt, einem IoT-Gateway und dem Internet,
  - Cloudkomponenten sind optional.

- Klasse 1:
  - Aktuelles Betriebssystem und Firmware,
  - Schnelle Reaktion des Herstellers auf Sicherheitsprobleme (Updates),
  - Manueller Updateprozess des Betriebssystems und der Firmware,
  - Sicheres Webinterface (hohe Mindestkomplexität, Passwort kann aus dem gesamten Zeichensatz bestehen, verschlüsselter Zugang),
  - Keine oder geringe Rechteverwaltungsmöglichkeiten (eingeschränkte Konten getrennt von Administrator),
  - Keine Sicherheitsmechanismen zur Erkennung und Verhinderung von Brute-Force Attacken,
  - Hersteller besitzt eine annehmbare Reputation,
  - Sichere, verschlüsselte Kommunikation zwischen dem IoT-Produkt, einem IoT-Gateway und dem Internet,
  - Cloudkomponenten sind optional.

- Klasse 2:
    - Aktuelles Betriebssystem und Firmware,
    - Langsame Reaktion des Herstellers auf Sicherheitsprobleme (Updates),
    - Manueller Updateprozess des Betriebssystems und der Firmware,
    - Sicheres Webinterface (jedoch geringe Mindestkomplexität, Passwort kann nicht aus dem gesamten Zeichensatz bestehen, verschlüsselter Zugang),
    - Keine oder geringe Rechteverwaltungsmöglichkeiten (eingeschränkte Konten getrennt von Administrator),
    - Keine Sicherheitsmechanismen zur Erkennung und Verhinderung von Brute-Force Attacken,
    - Hersteller besitzt keine annehmbare Reputation,
    - Sichere, verschlüsselte Kommunikation zwischen dem IoT-Produkt, einem IoT-Gateway und dem Internet,
    - Cloudkomponenten sind teilweise notwendig.

- Klasse 3:
    - Veraltetes Betriebssystem und Firmware,
    - Keine Reaktion des Herstellers auf Sicherheitsprobleme (Updates),
    - Manueller Updateprozess des Betriebssystems und der Firmware,
    - Unsicheres Webinterface (keine Mindestkomplexität, Passwort kann nicht aus dem gesamten Zeichensatz bestehen, verschlüsselter Zugang) ,
    - Keine Rechteverwaltungsmöglichkeiten,
    - Keine Sicherheitsmechanismen zur Erkennung und Verhinderung von Brute-Force Attacken,
    - Hersteller besitzt eine schlechte Reputation,
    - unsichere, unverschlüsselte Kommunikation zwischen dem IoT-Produkt, einem IoT-Gateway und dem Internet,
    - Cloudkomponenten sind für den Betrieb notwendig.

Wie aus den einzelnen Risikoklassen ersichtlich ist, nehmen sowohl die IT-Sicherheit als auch der Bedienungskomfort mit jeder Klasse ab. Deshalb ist es je nach Nutzerin und Nutzer unterschiedlich, welche Risikoklasse noch eine umfassende IT-Sicherheit gewährleisten kann. Allgemein ist von Risikoklasse 3 vollständig abzusehen, weil weder das Betriebssystem noch die Bedienung und Konfiguration als sicher zu betrachten sind.

Die Risikoklasse ist zudem im Zusammenhang mit dem Einsatzszenario zu betrachten. Isolierte Netzwerke, die über keinen direkten Zugang zum Internet verfügen, können nicht über das Internet angegriffen werden, wodurch eine niedrigere Risikoklasse zum Einsatz kommen könnten.

Je nach Risikoklasse können unterschiedliche Maßnahmen gesetzt werden, die dafür sorgen, dass die bestehende IT-Sicherheit nur in einem geringen Maße angepasst werden muss. Diese sind jedoch aufgrund der eingeschränkten IT-Infrastruktur von privaten Endkundinnen und Endkunden auf wenige Funktionen limitiert.

Diese Funktionen umfassen:

- virtuelle WLAN-Netzwerke
    - Gast-WLAN-Netzwerke, welche eine schwächere Verschlüsselung für IoT-Objekte bereitstellen,
- DMZ-Funktionalität (De-militarized Zone)
    - Eingeschränkter Netzwerkbereich, welcher nur über definierte Wege mit dem Internet kommunizieren darf und keinen Zugang auf das lokale Netzwerk hat,
- Manuelle Port-Freigaben
    - Zur Freischaltung von wichtigen Ports eines IoT-Objekts,
- VPN-Funktionalität (Virtual Private Network)
    - Um eine Portfreigabe zu vermeiden und trotzdem Zugriff auf das lokale Netzwerk und den IoT-Objekten zu erhalten.

Die Anzahl der Funktionalitäten ist abhängig von der verfügbaren IT-Infrastruktur. Der allgemeine Ansatz ist, ein IoT-Objekt, das nicht mit aktuellen Sicherheitsmechanismen umgehen kann, vom restlichen Netzwerk zu trennen und es trotzdem für alle erreichbar zu machen.

Solche Isolationsmaßnahmen schützen das IoT-Geräte jedoch nicht selbst vor Angriffen, wie sie von Mirai beispielsweise genutzt werden (siehe Abschnitt 4.1.1). Sie schützen nur das bestehende Netzwerk und die Infrastruktur vor dem IoT-Objekt.

Dabei sind die Nutzerin und der Nutzer gefragt, ob sie und er das Risiko eingehen möchte und der Bedarf besteht, ein unsicheres IoT-Objekt, trotz all der Gefahren und Risiken, in ihre und seine IT-Infrastruktur integrieren zu wollen.

Der Prozess der Integration eines IoT-Objekts in bestehende IT-Infrastrukturen wird im nächsten Abschnitt beschrieben. Dazu wird das bisher erarbeitete Wissen aufgegriffen und in einen umfassenden Prozess transformiert.

5.4 Integrationsprozess

Dieser Abschnitt beschäftigt sich mit dem Integrationsprozess, in dem ein IoT-Produkt in eine bereits bestehende IT-Infrastruktur eingebunden wird. Dabei steht die IT-Sicherheit des IoT-Produkts im Fokus sowie jene der bestehenden Infrastruktur, die durch die Integration nicht verringert werden darf.

Des Weiteren werden die der Arbeit zugrundeliegende Forschungsfrage und Hypothesen auf Basis des erarbeiteten Wissens ausgeführt und beantwortet. Dies geschieht in den Abschnitten 5.4.1 und 5.4.2. Der Integrationsprozess selbst gliedert sich in drei Prozessabschnitte, wobei jeder einen anderen Schwerpunkt aufweist und einen Teil des Produktlebenszyklus darstellt. Die Prozessabschnitte sind wie aufgeteilt:

1. Analyse des IoT-Objekts,
2. Konfiguration des IoT-Objekts,
3. Kontinuierliche Überwachung der IT-Sicherheit des IoT-Objekts.

Diese drei Prozessabschnitte beschreiben den Ablauf von der Analyse bis zum kontinuierlichen Überwachen der IT-Sicherheit des IoT-Objekts. Dies stellt einen geschlossenen Kreislauf dar, der gegebenenfalls bei einer Veränderung der IT-Sicherheit des IoT-Objekts mit dem ersten Prozessabschnitt neustartet.

Dadurch ist eine bleibende IT-Sicherheit des IoT-Objekts gewährleistet, die im Falle möglicher neuer Sicherheitslücken, entsprechende Analysen und Maßnahmen bereithält. Der Integrationsprozess entspricht dem Deming-Cycle (Johnson, 2002), ist jedoch für Endkundinnen und Endkunden optimiert worden. Die visuelle Darstellung des Prozesses kann im Anhang A gefunden werden.

Der erste Prozessabschnitt beschreibt jene Prozesse, die der Analyse des betrachteten IoT-Objekts dienen. Prozessergebnis ist die Beurteilung und Einordnung des IoT-Objekts in die im Abschnitt 5.3 entwickelten Risikoklassen. Inhalt des ersten Prozessabschnittes sind die Anforderungen, welche in den Abschnitte 5.2.1, 5.2.2. und 5.2.3 erarbeitet wurden.

Wurden diese Anforderungen korrekt bewertet und das IoT-Objekt einer Risikoklasse zugeordnet, kann mit dem zweiten Prozessabschnitt begonnen werden, der von der Konfiguration und Inbetriebnahme des IoT-Objekts handelt.

Dieser beginnt mit der Trennung des lokalen Netzwerks vom Internet, um das IoT-Objekt vor dem Internet vorerst zu isolieren. Damit verhindert man mögliche erste Angriffe von außen auf das IoT-Objekt, die im Abschnitt 4.1.1 beschrieben wurden. Ansonsten wäre ein IoT-Produkt, das sich im Auslieferungszustand befindet und mit dem Internet verbunden ist, schlimmstenfalls innerhalb weniger Minuten Teil eines globalen Botnetzes.

Der nächste Schritt beinhaltet die Aktualisierung des Betriebssystems und der Firmware des IoT-Objekts. Dies wird entweder über eine integrierte Update-Funktionalität durchgeführt oder mittels manuellem Download von der Hersteller-Website.

Befindet sich das aktuellste Betriebssystem und Firmware auf dem IoT-Objekt, kann mit dem nächsten Schritt begonnen werden. Dieser beinhaltet die sichere Konfiguration des IoT-Objekts.

Dazu müssen sichere Passwörter, welche aus mindestens acht Zeichen bestehen und Groß- und Kleinbuchstaben sowie Sonderzeichen beinhalten sollten, vergeben werden. (siehe Abschnitt 3.1) Der nächste Schritt besteht darin, die Benutzernamen und Rechte zu ändern, damit Administrationsfunktionen einem Administrationskonto zugeordnet sind und die restlichen Zugänge über diese nicht verfügen können.

Des Weiteren müssen alle Cloud-Dienste deaktiviert werden, die für den Basisbetrieb nicht notwendig sind. Je nach Architektur der bestehenden Infrastruktur müssen noch Zugangsdaten für ein WLAN eingetragen werden. Das Prozessergebnis dieses Abschnitts ist ein sicher konfiguriertes, mit aktuellem Betriebssystem und Firmware ausgestattetes IoT-Objekt, das in die bestehende Infrastruktur integriert werden kann.

Der letzte Prozessabschnitt bildet die kontinuierliche Überwachung der IT-Sicherheit des IoT-Objekts. In Folge soll gewährleistet werden, dass mögliche Updates umgehend eingespielt und damit Lücken in den Sicherheitsimplementierungen schnell behoben werden. Darüber hinaus müssen sich Kundinnen und Kunden über IoT-Plattformen im Internet über neue Bedrohungen oder mögliche Lücken in deren IoT-Objekten informieren (siehe Abschnitt 5.2.1).

Je nach Hersteller und IoT-Objekt ist der Aktualisierungsprozess automatisch im Betriebssystem integriert. Ist dies nicht der Fall, müssen Kundinnen und Kunden diesen manuell in periodischen Zyklen durchführen.

Entscheidend an diesem Prozess ist das ständige Monitoring des Sicherheitszustandes des IoT-Objekts. Wird eine Lücke identifiziert, welche nicht durch ein Update behoben wird, muss der Integrationsprozess nochmals durchlaufen und eine Einstufung in eine geeignete Risikoklasse aktualisiert werden.

5.4.1 Hypothesen

Die Hypothesen, die dieser Arbeit zugrunde lagen und es galt zu überprüfen waren wie folgt:

H1: IOT-Produkte gefährden die Sicherheit von bestehenden IT-Infrastrukturen, wenn diese nicht auf entsprechende Sicherheitsaspekte geprüft werden.

H0: IOT-Produkte gefährden die Sicherheit von bestehenden IT-Infrastrukturen nicht.

Auf Basis des erarbeiteten Wissens, das in den fünf Kapitel dargestellt wurde, stellen IoT-Produkte, welche nicht den erforderlichen Sicherheitskriterien entsprechen, ein Risiko und eine Gefährdung für bestehende IT-Infrastrukturen dar.

Einerseits werden ungeschützte IoT-Objekte für Botnetze missbraucht (siehe Abschnitt 4.1.1), führen Angriffe, gesteuert von Kriminellen durch, oder stellen private Einblicke in das Privatleben vieler Personen ins Internet bereit (siehe Abschnitt 4.4). Anderseits gefährden sie die Sicherheit aller im Netzwerk befindlichen Endgeräte, weil unbefugte Dritte sich Zugang zum IoT-Objekt verschaffen können und diese dadurch einen Angriffsvektor in das gesamte Netzwerk darstellen.

Unsichere IoT-Produkte stellen aber nicht nur eine Gefahr für die lokalen Infrastrukturen einzelner Personen und Haushalte dar, sie können mittels DDoS-Attacken auch globale IT-Services und grundlegende Dienstleistungen lahmlegen und dadurch für Chaos im Internet sorgen (siehe Abschnitt 4.1.1).

Besonders kritische Infrastrukturen sind einem hohen Risiko ausgesetzt, weil diese immer weiter vernetzt werden und durch Dritte über das Internet übernommen werden können. Im privaten Bereich zählen zu den kritischen Infrastrukturen, alle Versorgungsgüter, wie Strom, Licht, Wasser und Heizung (siehe Abschnitt 4.3).

IoT-Objekte, wie Philips Hue, welches Licht-Elemente mit dem lokalen Netzwerk und dem Internet vernetzen, stellen erste Einsatzszenarien im privaten Bereich von kritischen Infrastrukturen dar. Würden diese nicht über die nötigen Sicherheitsmechanismen verfügen, wären viele Haushalte im Dunklen, was zu nächtlichen Stunden durchaus eine Gefahr darstellt (siehe Abschnitt 3.1).

Zusammenfassend wurde durch diese Arbeit die H1-Hypothese bestätigt, weil unzureichend geschützte IoT-Produkte sich selbst und bestehende IT-Infrastrukturen in ihrer IT-Sicherheit gefährden.

5.4.2 Forschungsfrage

Die Forschungsfrage, welche diese Arbeit versuchte zu beantworten lautete:

Welche Sicherheitsmerkmale muss ein IOT-Produkt aufweisen, um in bestehende IT-Infrastrukturen eingebunden werden zu können, ohne die Sicherheitsrichtlinien und damit verbundene Maßnahmen zu kompromittieren und die Sicherheit dadurch zu gefährden?

Diese Sicherheitsmerkmale wurden auf Basis von publizierten Angriffsvektoren und Proof-of-Concept-Studien ermittelt. Aus diesen Angriffsvektoren wurden Sicherheitsmerkmale abgeleitet, welche in unterschiedliche Sicherheitsanforderung gegliedert und analysiert wurden (siehe Abschnitt 4).

Des Weiteren wurden Objekte, die das IoT-Ecosystem darstellen, eingrenzt und dadurch eine Isolation von bestehenden Netzwerken und Infrastrukturen geschaffen. Die Anforderungen gelten für das IoT-Objekt selbst, der Kommunikation zwischen dem IoT-Objekt, möglicher IoT-Gateways und dem Internet und für Cloud-Plattformen, welche von einigen IoT-Herstellern bereitgestellt werden (siehe Abschnitt 5).

Die Sicherheitsmerkmale werden in einem umfassenden Integrationsprozess dargestellt, der in drei Prozessabschnitte gegliedert ist. Dieser Prozess gewährleistet die IT-Sicherheit der IoT-Objekte selbst und jene der bestehenden IT-Infrastruktur. Des Weiteren beinhaltet der Prozess einen kontinuierlichen Monitoring-Prozess, der den aktuellen Sicherheitsstatus der IoT-Objekte ermittelt und diesen gegebenenfalls neu bewertet, was mit zusätzlichen Sicherheitsmaßnahmen verknüpft ist.

5.5 Zusammenfassung

Diese Kapitel befasste sich mit der Entwicklung eines IoT-Security Frameworks. Ziel des Frameworks ist es, IoT-Objekte aufgrund ihrer Sicherheitsmechanismen zu bewerten und in Risikoklassen einzuordnen. Dadurch sollen weniger IT-affine Personen die Sicherheit von IoT-Objekten bewerten können, ohne dass sie dazu tiefgreifendes Fachwissen erarbeiten müssen.

Basis des IoT-Security Frameworks war die Analyse verfügbarer IoT-Objekte und bekannte Sicherheitslücken in diesen Systemen. Daraus wurden Maßnahmen und Prozesse abgeleitet, die in drei Anforderungskategorien eingeordnet wurden und den Teil der Sicherheitsanforderungen bildeten.

Außerdem wurde auf Basis der identifizierten Angriffsvektoren und potentiellen Sicherheitslücken ein Integrationsprozess entwickelt, welcher den gesamten Produktlebenszyklus eines IoT-Objekts abbildet. Dieser ist unterteilt in drei Prozessabschnitten, wobei der erste die Analyse des potentiellen IoT-Objekts darstellt, der zweite die sichere Konfiguration und Inbetriebnahme und der dritte Abschnitt jenen des kontinuierlichen Monitorings der IT-Sicherheit des IoT-Objekts.

Bei möglichen neuen Bedrohungen, Angriffsvektoren und Lücken in den Sicherheitsimplementierungen, die nicht durch eine geänderte Konfiguration oder einem Update des Betriebssystems und der Firmware gelöst werden kann, muss diese Prozesskette erneut durchlaufen werden, wodurch eine Neubeurteilung des IoT-Objekts erfolgt.

Dies gewährleistet nach einem erfolgreichen Integrationsprozess eine bleibende IT-Sicherheit sowohl des IoT-Objekts als auch der bestehenden IT-Infrastruktur. Angelehnt an den Deming-Cycle bietet das IoT-Security Framework einen etablierten Sicherheits-Monitoring-Prozess, der neue Gefahren, die zum Zeitpunkt des Integrationsprozesses, nicht vorhanden oder publik waren, einbezieht und dadurch die Sicherheit wahrt.

Die Sicherheitsanforderungen an das IoT-Objekt, an die sichere Kommunikation sowie an eine mögliche Cloudplattform bilden das Fundament des IoT-Security Frameworks und sorgen für die notwendige Grundlage, ein IoT-Objekt beurteilen zu können.

Die Anforderungen selbst wurden in verständliche Prozesse integriert, wodurch weniger IT-affine Personen, diese als Checkliste verwenden und damit ihre potentiellen IoT-Produkte bewerten können.

Das IoT-Security Framework zeigt die Komplexität des IoT-Ecosystems. Es besteht aus vielen unterschiedlichen Technologien und kombiniert diese für den jeweiligen Einsatzbereich. Daher ergeben sich variantenreiche Angriffsvektoren, die versuchen die einzelnen Technologien zu unterwandern und so das System zu kompromittieren.

Dem wirkt das IoT-Security Framework entgegen, indem es einzelne Objekte und Technologien voneinander trennt und jeweils spezifische Anforderungen und Prozesse bereitstellt, die mögliche Lücken und Schwächen in den Sicherheitsmechanismen aufzeigen. Somit wird die IT-Sicherheit des IoT-Objekts selbst gewährleistet und die bestehender IT-Infrastruktur geschützt und die Sicherheit dieser nicht vermindert.

6 CONCLUSIO

Das Internet of Things erreicht immer mehr den Alltag vieler Menschen. Die IoT-Produkte versprechen ein einfacheres Leben, was durch die zunehmende Digitalisierung und Vernetzung ermöglich werden soll. Algorithmen steuern diese Objekte und sorgen dafür, dass der Mensch immer weniger die Kontrolle über sein Eigentum besitzt. Viele nehmen dies in Kauf und erwarten sich im Gegenzug mehr Freizeit und eine Steigerung der Effizienz durch den Einsatz von IoT-Technologien.

Die IoT-Technologie kombinieren unterschiedlichste Technologiewelten für Einsatzszenarien, die mit bisherigen Ansätzen nicht realisierbar waren. Dadurch können neue Bereich adressiert werden, welche bisher von der Digitalisierung nicht durchdrungen waren. Dies führt zu einer Steigerung der Anzahl von Endgeräte, welche mit dem Internet kommunizieren.

Forscherinnen und Forscher gehen davon aus, das im Jahr 2020, 50 Milliarden vernetzte Endgerät aktiv Teil des Internets werden. Sind es im Jahr 2017 noch Server, Computer und mobile Endgeräte, die den Hauptanteil an Internet-fähigen Endgeräten ausmachen, werden bis zum Jahr 2020 Produkte jeglicher Art, wie Überwachungskameras, Verkehrssteuerungssysteme und Teile von kritischer Infrastruktur, mit dem Internet kommunizieren.

Während die Notwendigkeit der IT-Sicherheit von Computern und mobilen Endgeräte der breiten Masse mittlerweile bekannt ist, ist dies im Bereich von IoT noch nicht der Fall. Automatische Updates und integrierte Sicherheitsmechanismen schützen Systeme von Desktops und mobilen Endgeräte, sowie deren Nutzerinnen und Nutzer.

Solche Mechanismen sind im Bereich von IoT-Produkten noch nicht in dem Maße verbreitet, wodurch ein Gefährdungspotential von diesen Objekten ausgeht. Des Weiteren beherrschen viele dieser Produkte nicht die notwendigen Sicherheitsstandards. Demzufolge gefährden ungeschützte und unsichere IoT-Produkte sich selbst und die bestehende IT-Infrastruktur, in der sie integriert werden.

Problematisch ist hierbei, dass sich dieser Tatsache nur wenige Menschen bewusst sind, weshalb bereits erste globale Botnetze, ungeschützte IoT-Objekte infizierten und diese für kriminelle Tätigkeiten missbrauchten. Betrachtet man die Vielzahl an unterschiedlichen IoT-Objekten und deren Verbreitung, kann man von ersten Epidemien sprechen, die sehr gefährlich sein können.

Solche Botnetze können neben dem Versenden von Spam-E-Mails, wichtige grundlegende IT-Services im Internet stören und diese mittels DDoS-Attacken lahmlegen. Dies kann zu einer Kettenreaktion führen, weil viele IT-Services, andere Dienstleistungen nutzen, um damit kosteneffizient arbeiten zu können.

IoT-Suchmaschinen zeigen die Verbreitung von IoT-Objekten auf. Sie erlauben es nach spezifischen IoT-Systemen zu suchen, welche Lücken in ihren Sicherheitsmechanismen aufweisen. Solche Suchmaschinen können einerseits von Sicherheitsforscherinnen und Sicherheitsforschern genutzt werden, um die Ausbreitung von IoT-Malware zu verhindern,

andererseits werden sie vielfach von Kriminellen missbraucht, um potentielle Opfer identifizieren zu können.

Das Gefährdungspotential und die steigende Anzahl an IoT-Produkten, welche in bestehende Infrastrukturen integriert werden, waren Grund ein IoT-Security Framework zu entwickeln, welches weniger IT-affinen Menschen erlaubt, die Sicherheit von IoT-Produkten beurteilen zu können.

Dazu wurden zu Beginn die Thematik IoT im Allgemeinen beleuchtet und abgegrenzt vom Themengebiet M2M (Machine-to-Machine). Des Weiteren wurden grundlegende Technologien und Architekturen analysiert. IoT ist sehr stark mit Big Data und Cloud-Technologien verknüpft, wodurch diese Themengebiete kompakt erfasst wurden.

Diese Grundlagen bildeten das Fundament für die Analyse von IoT-Produkte, die aktuell am Markt verfügbar sind und jeweils unterschiedliche Angriffsvektoren beinhalteten. Dazu wurde das Grundkonzept und die Architektur, die hinter dem jeweiligen IoT-Objekt stand, beleuchtet und anschließend die Sicherheitsmechanismen analysiert und beurteilt. Wegen der Vielzahl an unterschiedlichen IoT-Produkten und Herstellern wurde der Fokus auf drei unterschiedliche Produkte gelegt, wodurch mindestens ein Angriffsvektor jeweils variierte.

Auf Basis der identifizierten Schwachstellen und Lücken in den Sicherheitsimplementierungen wurden aktuelle Gefährdungen und Angriffe von Kriminellen und Hackern, die aktiv durchgeführt wurden und werden, erläutert.

Die Analyse zeigte, dass Botnetze aktiv, unsichere IoT-Objekte kompromittieren und diese für kriminelle Aktivitäten nutzen. Aufgrund der bereits weiten Verbreitung von IoT-Objekten, die mit dem Internet verbunden sind, ergibt sich ein enormes Gefährdungspotential, das kritische Infrastrukturen und wichtige IT-Services lahmlegen könnte. Im privaten Bereich wären wichtige Versorgungsgüter wie Strom, Wasser und Heizung von Angriffen gefährdet. Mögliche Eingriffe in die Privatsphäre, die durch ungeschützte IP-Kameras durchgeführt werden können, bilden hier ein weiteres Gefahrenpotential.

Um die IT-Sicherheit des IoT-Objekts selbst und jene der bestehenden Infrastrukturen zu wahren und diese im Falle einer Integration eines neuen IoT-Produkts nicht zu vermindern, wurden Sicherheitsanforderungen definiert. Diese gliedern sich in drei Anforderungskataloge, welche sich auf das IoT-Objekt, den Kommunikationsschnittstellen und den Cloudplattformen beziehen. Mithilfe dieses Anforderungskatalogs ist es weniger IT-affinen Personen möglich, die IT-Sicherheit des neuen IoT-Produkts zu bewerten und dieses in definierte Risikoklasse einordnen zu können.

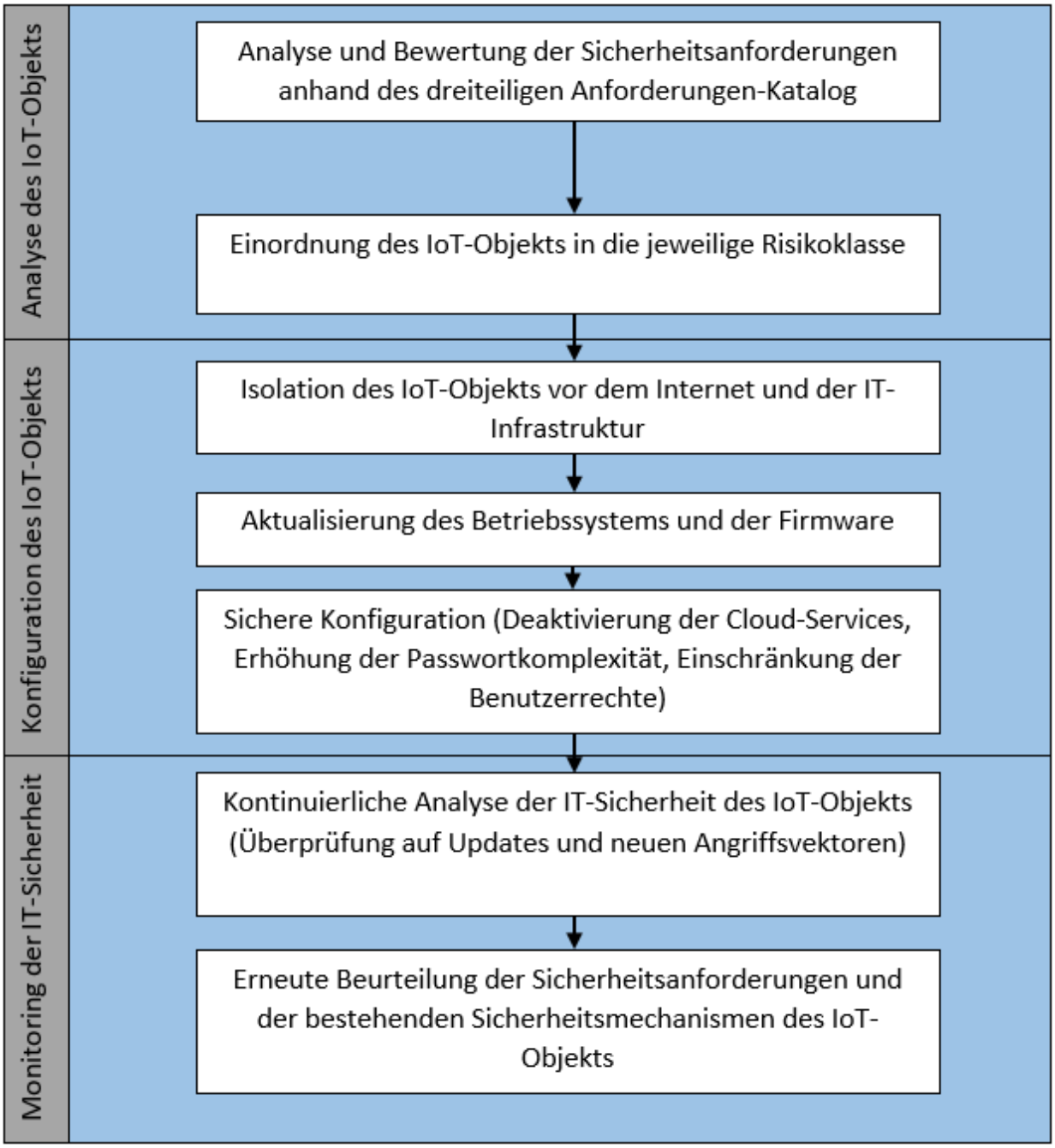
Die Risikoklassen fassen IoT-Objekte gleicher Sicherheitsmerkmale zusammen. Sie können genutzt werden, um das Risiko von IoT-Produkten bewerten zu können und entsprechende Prozesse und Konfigurationen zu implementieren, die Risiken vermindern.

Der Anforderungskatalog bildet den ersten Teil eines dreistufen Integrationsprozesses, welcher die IT-Sicherheit eines IoT-Objekts bereits bei der Integration in die bestehende Infrastruktur gewährleistet. Dieser Integrationsprozess bildet die Zusammenfassung des erarbeiteten Wissens, indem er alle potentiellen Angriffsvektoren direkt zu Beginn der ersten Interaktion mit

dem Netzwerk und Internet verhindert und erst bei erfolgter sicherer Konfiguration und Installation, diese erlaubt.

Es ist anzumerken, dass dieser Integrationsprozess zwar einen kontinuierlichen Monitoring-Prozess beinhaltet, der die IT-Sicherheit ständig überwachen soll, dies heißt aber nicht, dass jegliche neuen Angriffsvektoren, keinen Einfluss auf die IoT-Objekte haben können. IT-Sicherheit ist ein ständiger Verbesserungsprozess, welcher sich an aktuellen Gegebenheiten orientieren muss und deshalb keinesfalls als abgeschlossener Prozess betrachtet werden darf.

ANHANG A - Integrationsprozess



ABKÜRZUNGSVERZEICHNIS

AAL	Ambient Assited Living
AGB	Allgemeine Geschäftsbedingungen
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ARP	Adress Resolution Protocol
AWS	Amazon Web Services
BKA	Bundeskanzleramt
BSI	Bundesamt für Informationssicherheit
C&C	Command and Control
CDMA	Code Division Multiple Access
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DDS	Data Distribution Service
DMZ	De-militarized Zone
DNS	Domain Name Service
DSL	Digital Subscriber Line
DTLS	Datagram Transport Layer Security
EU	Europäische Union
FreeRTOS	Free Real-Time Operating-System
FTP	File Transfer Protocol
HDFS	Hadoop Distributed File System
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IFTT	If this than that
IoT	Internet of Things
IT	Informationstechnologie
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISO	Internationale Organisation für Normung
ITU	International Telecommunication Union
KIS	Krankenanstalten Informationssystem
LAN	Local Area Network
LE	Low Energy
LED	Light Emitting Diode
LLAP	LocalTalk Link Access Protocol
LPWAN	Low Power Wide Area Network

M2M	Machine to Machine
MAC	Media-Access-Control
MacOS	Macintosh Operating System
MIT	Massachusetts Institute of Technology
MQTT	Message Queue Telemetry Transport
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
OS	Operating System
OSI	Open Systems Interconnection Model
P2P	Peer to Peer
PC	Personal Computer
RAM	Random Access Memory
RCE	Remote Call Execution
REST	Representational State Transfer
RF	Radio Frequency
RFID	Radio-Frequency Identification
RIOT	Robust Internet of Things
RTR	Rundfunk und Telekom Regulierung
RTSP	RealTime Streaming Protocol
SDK	Software Development Kit
SSH	Secure Shell
SSI	Simple Server Interface Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UX	User Experience
VPN	Virtual Private Network
WLAN	Wireless Area Network
WPA	Wi-Fi Protected Access
XEROX PARC	Xerox Palo Alto Research Center Incorporated
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
ZBA	ZigBee Building Automation
ZGP	ZigBee Green Power
ZHA	ZigBee Home Automation
ZHC	ZigBee Health Care
ZID	ZigBee Interface Devices

ZLL	ZigBee Light Link
ZRC	ZigBee Remote Control
ZRS	ZigBee Retail Services
ZSE	ZigBee Smart Energy
ZTS	ZigBee Telecom Services

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Aceves, E., & Larios, V. M. (2016). *Data Visualization for Georeferenced IoT Open Data Flows for a GDL Smart City Pilot.* New York: IEEE.

Adams, C., Jourdan, G.-V., & Levac, J.-P. (2010). *Lightweight protection against brute force login attacks on Web applications.* Ottawa: IEEE.

Alliance, Z. (2004). *ZigBee Specification.* ZigBee Alliance.

Amazon AWS. (2017). Abgerufen am 07. Juli 2017 von https://aws.amazon.com/de/iot-platform/how-it-works/

AMQP Alliance. (2011). *AMQP Specification v1.0.*

Apache Spark. (2017). Abgerufen am 14. Juli 2017 von https://spark.apache.org/

ARM mbed OS. (2017). Abgerufen am 28. Juli 2017 von https://developer.mbed.org/

Barcena, M. B., & Wuesst, C. (2015). *Insecurity of the Internet of Things.* Symantec.

Baudin, M. (2005). *RFID applications in manufacturing .* Palo Alto: Manufacturing Management & Technology Institute.

Berger, R. (2017). *Sueddeutsche*. Abgerufen am 20. Juli 2017 von http://www.sueddeutsche.de/auto/vernetzte-autos-die-daten-eines-autos-sind-das-neue-oel-1.3469344

Berghel, H., & Uecker, J. (2004). *Wireless Infidelity II: Airjacking.* Nevada: ACM.

Berthelsen, E., & Morrish, J. (2014). *What's the difference between M2M and IoT?* Machina Research.

Bertino, E., & Islam, N. (2017). *Botnets and Internet of Things Security .* Purdue: IEEE.

Bi, Z., Xu, L. D., & Wang, C. (2014). *Internet of Things for Enterprise Systems of Modern Manufacturing.* IEEE.

Blumenthal, B. (2003). *Wireless LAN (IEEE 802.11) Security Gloassar.* Zürich: Wireless Forum.

Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). *Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices.* New York: Elsevier.

Bordel, S. (2016). *COM! Professional*. Abgerufen am 21. Juli 2017 von http://www.com-magazin.de/news/sicherheit/iot-gefaehrdet-kritische-infrastrukturen-1111874.html

Boucadair, M., France Telecom, Penno, R., Wing, D., & Cisco. (2013). *Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function.* Rennes: IETF.

Boyle, D., & Newe, T. (2007). *Security Protocols for Use with Wireless Sensor Networks: A Survey of Security Architectures .* Guadeloupe: IEEE.

Brand, L., Hülser, T., Grimm, V., & Zweck, A. (2009). *Internet der Dinge - Perspektiven für die Logistik.* Düsseldorf: VDI Technologiezentrum GmbH.

Brinkmann, M. (2013). *Ghacks*. Abgerufen am 08. Juli 2017 von https://www.ghacks.net/2013/04/09/shodan-a-search-engine-for-vulnerable-internet-devices/

Bundeskanzleramt. (2014). *Österreichisches Programm zum Schutz kritischer Infrastrukturen.* Wien: Republik Österreich.

Cecchinel, C., Jimenenz, M., Mosser, S., & Riveill, M. (2014). *An Architecture to Support the Collection of Big Data in the Internet of Things.* Sophia Antipolis: Univ. Nice Sophia Antipolis.

Chiuchisan, I., Costin, H. N., & Geman, O. (2014). *Adopting the Internet of Things technologies in health care systems.* IEEE.

Cohn, R. J., Coppen, J. R., Banks, A., & Gupta, R. (2014). *MQTT Version 3.1.1 Specifications.* Oasis Open.

Coldewey, D. (2016). *This security camera was infected by malware 98 seconds after it was plugged in.* New York: TechCrunch.

Contiki-Os. (2017). Abgerufen am 28. Juli 2017 von http://www.contiki-os.org/

Cooke, E., Jahanian, F., & McPherson, D. (2005). *The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets.* Michigan: University of Michigan.

Corporation, S. (2016). *An Internet of Things Reference Architecture.*

Da Cunha, C., Agard, B., & Kusiak, A. (2006). *Data mining for improvement of product quality.* Iowa: Institut National Polytechnique de Grenoble.

de Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. S. (kein Datum).

Dhanjani, N. (2015). *IoT-Hacking: Sicherheitslücken im Internet der Dinge erkennen und schließen.* Heidelberg: dpunkt.verlag.

Dhanji, N. (2013). *SECURITY EVALUATION OF THE PHILIPS hue PERSONAL WIRELESS LIGHTING SYSTEM.* Osborne McGraw-Hill.

Dlamini, M., Eloff, M., & Eloff, J. (2009). *Internet of things: emerging and future scenarios from an information security perspective.* Swaziland: Southern Africa Telecommunication Networks and Applications Conference.

Dobbins, R., & Bjarnason, S. (2016). *ARBOR Networks*. Abgerufen am 23. Juli 2017 von https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/

Dohr, A., Modre-Opsrian, R., & Drobics, M. (2010). *The Internet of Things for Ambient Assisted Living .* IEEE.

Dölle, M. (2016). *Heise*. Abgerufen am 14. Juli 2017 von https://www.heise.de/ct/ausgabe/2016-4-Passwortverrat-und-Firewall-Untertunnelung-bei-Foscam-Kameras-und-wie-man-es-unterbindet-3088868.html

Dominikus, S., & Schmidt, J.-M. (2011). *Connecting Passive RFID Tags to the Internet of Things.* Graz: University of Technology Graz.

Douligeris, C., & Mitrokotsa, A. (2004). *DDoS attacks and defense mechanisms: classification and state-of-the-art.* Athen: Elsevier.

Enz, R. (2016). *SIC-Software*. Abgerufen am 14. Juli 2017 von http://www.sic-software.com/iot-protokolle-mqtt-vs-amqp/

Farahin, S. (2008). *ZIGBEE WIRELESS NETWORKS AN TRANSCEIVERS.* Oxford: Elsevier Ltd.

Feike, T. (2013). *VLEXPlus*. Abgerufen am 14. Juli 2017 von http://www.vlexplus.com/erp-software/erp-industrie-40/

Feinstein, L., Schnackenberg, D., & Balupari, R. (2003). *Statistical approaches to DDoS attack detection and response.* Washington: IEEE.

Fielding, R., Irvine, U., Gettys, J., Compaq /W3C, Mogul, J., Compaq, . . . Berners-Lee, T. (1999). *Hypertext Transfer Protocol -- HTTP/1.1.* Juni.

Folkens, J. (2014). *Building a gateway to the Internet of Things.* Texas Instruments.

Forbes. (2014). Abgerufen am 14. Juli 2017 von https://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/#1e4176d7b919

Foschini, L., Taleb, T., & Corradi, A. (2011). *M2M-based metropolitan platform for IMS-enabled road traffic management in IoT.* Bologna: IEE.

Fouladi, B., & Ghanoun, S. (2016). *Security Evaluation of the Z-Wave Wireless Protocol.* London: NeoMinds.

FreeRTOS. (2016). Abgerufen am 09. Juli 2017 von http://www.freertos.org/about-RTOS.html

Gantz, J., & Reinsel, D. (2013). *THE DIGITAL UNIVERSE IN 2010: Big Data, Bigger Digital Shadows, and Biggest Growth in Far East.* EMC.

Gartner. (2016). Abgerufen am 10. Juli 2017 von https://www.gartner.com/newsroom/id/3291817

Gayer, O., Wilder, O., & Zeifman, I. (2015). *Imperva INCAPSULA*. Abgerufen am 14. Juli 2017 von https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html

Georgakakis, E., Nikolidakis, S. A., Vergados, D. D., & Douligeris, C. (2010). *An Analysis of Bluetooth, Zigbee and Bluetooth Low Energy and Their Use in WBANs.* Piräus: Springer.

Gierow, H. (2015). *Golem*. Abgerufen am 21. Juli 2017 von https://www.golem.de/news/schutz-kritischer-infrastrukturen-eu-beschliesst-erste-cybersecurity-richtlinie-1512-117907.html

Gierow, H. (2016). *Golem*. Abgerufen am 21. Juli 2017 von https://www.golem.de/news/ddos-was-cloudflare-vom-mirai-botnetz-sieht-1610-123749.html

GitHub. (2017). Abgerufen am 17. Juli 2017 von https://github.com/tinyos/tinyos-main

Goldman, D. (2013). *CNNTech*. Abgerufen am 16. Juli 2017 von http://money.cnn.com/2013/04/08/technology/security/shodan/index.html

Gronau, N., Thim, C., & Fohrholz, C. (2017). *Wettbewerbsfaktor Analytics im Internet der Dinge.* Potsdam: Universität Potsdam.

Hahm, O., Baccelli, E., & Tsiftes, N. (2015). *Operating Systems for Low-End Devices in the Internet of Things: a Survey.* HAL.

Hassel, M. (2015). *Incognito*. Abgerufen am 15. Juli 2017 von http://www.incognito.com/blog/iot-and-m2m-whats-the-difference/

Heinrich, J. (2005). *Heise*. Abgerufen am 19. Juli 2017 von https://www.heise.de/newsticker/meldung/Urteil-Server-Inhaber-haftet-fuer-DDoS-Angriffe-141629.html

Hofmann, M., & Trost, U. (2015). *BIG DATA Future - Chancen und Herausforderungen für die deu.* MHP.

IEEE. (2017). *Ethernet Standards.* IEEE.

Ihlenfeld, J. (2010). *Golem*. Abgerufen am 18. Juli 2017 von https://www.golem.de/1011/79580.html

Infosecurity-Magazine. (2010). Abgerufen am 19. Juli 2017 von https://www.infosecurity-magazine.com/news/bredolab-downed-botnet-linked-with-spamitcom/

International Electrotechnical Comission. (2015). *IoT 2020: Smart and secure IoT Platform.* IEC.

International Telecommunation Union. (2012). *Overview of the Internet of things.* ITU.

Internet Society. (2015). *The Internet of Things: An Overview.* Internet Society.

Ismail, N., & Paqin, R. (2013). *Maintenance, Repair, and Operations (MRO) in Asset Intensive Industries.* Aberdeen Group.

IT Wissen. (2015). Abgerufen am 18. Juli 2017 von http://www.itwissen.info/ZigBee-Profil-ZigBee-profile.html

ITPG. (2014). Abgerufen am 13. Juli 2017 von http://www.itpg.org/grcsolutions/it-security-framework-definition/

Ives, B., Walsh, K. R., & Schneider, H. (2004). *The domino effect of password reuse.* New York: Communications.

Jaffrey, T. (2014). *Eclipse*. Abgerufen am 13. Juli 2017 von https://eclipse.org/community/eclipse_newsletter/2014/february/article2.php

Johnson, C. N. (2002). *The Benefits of PDCA.* New York: ProQuest.

Jordan, S. (2015). *OPERATING SYSTEM BUILT FOR IOT.* San Jose: IEEE Standards Association.

Kale, C. J. (1991). *RFC 1180 - TCP/IP Tutorial.* IEEE.

Karasaridis, A., Rexroad, B., & Hoeflin, D. (2007). *Wide-scale Botnet Detection and Characterization.* New York: Usenix.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks.* Cham: Springer.

Kim, P. (2017). *PierreKim*. Abgerufen am 19. Juli 2017 von https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

Kiravuo, T., Sarela, M., & Manner, J. (2013). *A Survey of Ethernet LAN Security .* Helsinki: IEEE.

Krebs, B. (2016). *Krebs on Security*. Abgerufen am 29. Juli 2017 von https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/

Krebs, B. (2016). *Krebs on Security*. Abgerufen am 21. Juli 2017 von https://krebsonsecurity.com/2016/12/researchers-find-fresh-fodder-for-iot-attack-cannons/

Küchemann, D. (2014). *Betriebssystem für IoT-Geräte.* Münster: Universität Münster.

Lashkari, A. H., Danesh, M. S., & Samadi, B. (2009). *A survey on wireless security protocols (WEP, WPA and WPA2/802.11i).* Beijing: IEEE.

Leopold, H. (2017). *Cyber Security für kritische Infrastrukturen.* Wien: Springer.

Li, C., Jiang, W., & Zou, X. (2009). *Botnet: Survey and Case Study .* Taiwan: IEEE.

Liming, S. D., & Malin, J. R. (2015). *Windows 10 IoT - The Big Reboot.* Annabooks.

Links, C. (2015). *The Power of ZigBee 3.0 – All about the new and improved ZigBee 3.0.* August.

Liu, J., Xiao, Y., & Chen, P. C. (2012). *Authentication and Access Control in the Internet of Things .* Tuscaloosa: IEEE.

Lozhkin, S. (2014). *Securelist*. Abgerufen am 18. Juli 2017 von https://securelist.com/analysis-of-malware-from-the-mtgox-leak-archive/58553/?pubid=200883611

Magrassi, P. (2002). *Why a Universal RFID Infrastructure Would Be a Good Thing.* Gartner.

Maier, M. (2013). *Towards a Big Data Reference Architecture.* Eindhoven: Eindhoven University of Technology.

Maksimovic, M., Vujovic, V., & Perisic, B. (2015). *A custom Internet of Things healthcare system .* IEEE.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE.* San Francisco: McKinsey&Company.

McMillen, D. (2017). *Security Intelligence*. Abgerufen am 18. Juli 2017 von https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/

Medaglia, C. M., & Serbanati, A. (2010). *An Overview of Privacy and Security Issues in the Internet of Things.* Rom: Springer.

Medvedev, A., Fedchenkov, P., Zaslavsky, A., Anagnostopoulos, T., & Khoruzhnikov, S. (2015). *Waste Management as an IoT-Enabled Service in Smart Cities.* Springer.

Micrium Embedded Software. (2013). Abgerufen am 18. Juli 2017 von https://www.micrium.com/iot/iot-rtos/

Microsoft. (2016). *Microsoft Azure IoT -Reference Architecture.* Microsoft.

Minerva, R., Biru, A., & Rotondi, D. (2015). *Towards a definition of the Internet of Things (IoT).* Turin: IEEE.

Mirkovic, J., & Reiher, P. (2004). *A taxanomy of DDoS attack and DDoS defense mechanisms.* New York: ACM.

Müller, S. (2016). *Internet of Things (IoT) - Ein Wegweise durch das Internet der Dinge.* München: Books on Demand GmbH.

Nowossadeck, E. (2012). *Demografische Alterung und Folgen für das Gesundheitswesen .* Robert Koch-Institut .

NXP. (2016). *ZigBee 3.0 - Facilitating the Internet of Things.* NXP.

O'Flynn, C. (2016). *A LIGHTBULB WORM? Details of the Philips Hue Smart Lighting Design.* Black Hat USA.

Osborne, C. (2016). *ZDNet*. Abgerufen am 18. Juli 2017 von http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/?tag=nl.e539&s_cid=e539&ttag=e539&ftag=TRE17cfd61

Pa Pa, Y. M., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C. (2015). *IoTPOT: Analysing the Rise of IoT Compromises.* Saarland: Saarland University.

Paganini, P. (2016). *Security Affairs*. Abgerufen am 17. Juli 2017 von http://securityaffairs.co/wordpress/51868/malware/mirai-botnet-source-code.html

Patalong, F. (2008). *Spiegel Online*. Abgerufen am 17. Juli 2017 von http://www.spiegel.de/netzwelt/web/hack-attacke-auf-georgien-ehrenamtliche-angriffe-a-572033.html

Perlroth, N., & Hary, Q. (2013). *New York Times*. Abgerufen am 19. Juli 2017 von http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html

Philips. (2016). *FACTSHEET Philips hue - die intelligenteste LED-Birne der Welt.* Philips.

Radziwon, A., Bilberg, A., Bogers, M., & Madsen, E. S. (2014). *The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions.* Science Direkt.

Raji, R. (1994). *Smart networks for control.* IEEE.

Ramesh, S. (2014). *Proofpoint*. Abgerufen am 17. Juli 2017 von http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799

Reinwarth, M. (2017). *ZDNet*. Abgerufen am 17. Juli 2017 von http://www.zdnet.de/88288201/iot-und-smart-home-privatsphaere-im-intelligenten-zuhause/

Rescorla, E. (2000). *HTTP Over TLS.* East Palo Alto: IETF.

RF Wireless World. (2015). Abgerufen am 19. Juli 2017 von http://www.rfwireless-world.com/IoT/IoT-architecture.html

Richardson, L., & Ruby, S. (2007). *RESTful Web Services.* Sebastopol: O'Reilly Media, Inc.

Ries, U. (2016). *Heise*. Abgerufen am 21. Juli 2017 von https://www.heise.de/security/meldung/Hacker-Spass-mit-Hue-Leuchten-3289481.html

RIOT-OS. (2017). Abgerufen am 21. Juli 2017 von https://www.riot-os.org/

Roman, R., Zhou, J., & Lopez, J. (2012). *On the features and challenges of security and privacy in distributed internet of things.* Singapore: Elsevier.

Ronen, E., O'Flynn, C., Shamir, A., & Weingarten, A.-O. (2016). *IoT Goes Nuclear: Creating a ZigBee Chain Reaction.* Halifax: Dalhousie University.

Rundfunk und Telekom Regulierung. (2016). *M2M und IoT - Regulierungsdialog.* RTR.

Russell, B., & Van Duren, D. (2016). *Practical Internet of Things Security.* Birmingham: Packt Publishing.

Ryan, M. (2013). *Bluetooth: With Low Energy comes Low Security.* New York: iSEC Partners.

Samulat, P. (2015). *Computerwoche*. Abgerufen am 19. Juli 2017 von https://www.computerwoche.de/a/iot-hype-oder-geschaeftsmodell,3219122

Santos, J., Rodrigues, J. J., & Casal, J. (2016). *Intelligent Personal Assistants Based on Internet of Things Approaches.* Lissabon: IEEE.

Scherschel, F. A. (2017). *Heise*. Abgerufen am 28. Juli 2017 von https://www.heise.de/newsticker/meldung/Mirai-Botnetz-lernt-neue-Tricks-3670226.html

Scherschel, F. A. (2017). *Heise*. Abgerufen am 29. Juli 2017 von https://www.heise.de/security/meldung/Netzwerkkameras-von-Foscam-sind-nach-wie-vor-Sicherheitsrisiken-3739735.html

Schreiber, D. V., & Leser, A. (Hrsg.). (2008). *Wichtiges Werk.* Graz: Wissensverlag.

Schröder, H. (2017). *1PW*. Abgerufen am 14. Juli 2017 von http://www.1pw.de/brute-force.html

Schulzrinne, H., U, C., Netscape, Lanphier, R., & RealNetworks. (1998). *Real Time Streaming Protocol (RTSP).* New York: IETF.

Scott, J. (2015). *MapR*. Abgerufen am 28. Juli 2017 von https://mapr.com/blog/apache-spark-hadoop-based-big-data-architecture-infographic/

Securelist. (2017). Abgerufen am 17. Juli 2017 von https://securelist.com/newish-mirai-spreader-poses-new-risks/77621/

Security, U. D. (2016). *Strategic Principles For Securing the Internet of Things (IOT).* USA: Homeland Security.

Selen, K. (2012). *UPnP security in Internet gateway devices.* Helsinki: University of Technology Helsinki.

ServerComparator. (2016). Abgerufen am 15. Juli 2017 von https://servercomparator.com/vpn/blog/dyn-mirai-ddos-complete-story

Shelby, Z., ARM, Hartke, K., & Bromann, C. (2014). *The Constraint Application Protocol (CoAP).* Bremen: Juni.

Shodan. (2017). Abgerufen am 18. Juli 2017 von https://www.shodan.io/

Skerret, I. (2016). *IoT Developer Survey.*

Skerrett, I. (2017). *IoT Developer.* Eclipse IoT Working Group.

SmartGrid. (2015). Abgerufen am 24. Juli 2017 von https://www.smartgrid.gov/the_smart_grid/smart_grid.html

Spiegel Online. (2013). Abgerufen am 18. Juli 2017 von http://www.spiegel.de/netzwelt/web/spamhaus-vs-cyberbunker-ddos-attacken-bremst-internet-a-891177.html

SRI Consulting Business Intelligence. (2014). *Technology roadmap: The Internet of Things.*

Statista. (2017). Abgerufen am 15. Juli 2017 von https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Strauß, S. (2015). *Big Data - Risiken und Nebenwirkungen.* Wien: Institut für Technologie-Abschätzung.

Szili, D. (2015). *Jumpes-Jump*. Abgerufen am 14. Juli 2017 von https://jumpespjump.blogspot.co.at/2015/09/how-i-hacked-my-ip-camera-and-found.html

Thoma, J. (2017). *Golem*. Abgerufen am 23. Juli 2017 von https://www.golem.de/news/link11-ddos-angriffe-nehmen-wegen-iot-botnetzen-weiter-zu-1707-129004.html

University, C. M. (2014). *The "Only" Coke Machine on the Internet.* The Carnegie Mellon University.

Verma, S. (2016). *Searching Shodan For Fun And Proit.* New York: Exploit-DB.

Vermesan, O., & Friess, P. (2014). *Internet of Things - From Research and Innovation to Market Deployment.* River.

Vilsbeck, C. (2014). *Tecchannel*. Abgerufen am 15. Juli 2017 von https://www.tecchannel.de/a/datenmengen-explodieren-durch-sensordaten,2056615

Walker, T. E. (2015). *A Cloud for the Internet of Things - AWS IoT.* Amazon AWS.

Ward, J. S., & Barker, A. (2013). *Undefined By Data: A Survey of Big Data Definitions.* St Andrews: University of St Andrews.

Weber, R. H. (2009). *Internet of Things – New security and privacy challenges.* Hong Kong: Elsevier.

Wei, J., & Chow, M. (2016). *DDoS on Internet of Things - a big alarm for the future.* Medford: Tufts University.

Weichert, T. (2013). *Big Data und Datenschutz.* Kiel: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein .

Weiser, M. (1988). *Ubiq*. Abgerufen am 23. Juli 2017 von http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

Welzel, A., Rossow, C., & Bos, H. (2014). *On measuring the impact of DDoS botnets.* Amsterdam: EuroSec.

Wood, A. (2015). *The Guardian*. Abgerufen am 19. Juli 2017 von https://www.theguardian.com/media-network/2015/mar/31/the-internet-of-things-is-revolutionising-our-lives-but-standards-are-a-must

Wulf, J. (2014). *Red Hat*. Abgerufen am 21. Juli 2017 von https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/2/html-single/Messaging_Programming_Reference/index.html

Wurm, J., Hoang, K., & Arias, O. (2016). *Security analysis on consumer and industrial IoT devices .* Macau: IEEE.

Xiaoli, X., Yunbo, Z., & Guoxin, W. (2011). *Design of Intelligent Internet of Things for Equipment Maintenance.* Shenzhen: IEEE.

Yi, S., Quin, Z., & Li, Q. (2015). *Security and Privacy Issues of Fog Computing: A Survey.* New York: Springer.

Yun, J., Ahn, I. Y., & Sung, N. M. (2015). *A device software platform for consumer electronics based on the internet of things.* Gyeonggi-do: IEEE.

Zachariah, T., Klugman, N., Campbell, B., Adkins, J., Jackson, N., & Dutta, P. (2015). *The Internet of Things Has a Gateway Problem.* Ann Arbor: University of Michigan.

Zigbee. (2012). Abgerufen am 20. Juli 2017 von http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeepro/