Sicherheit im IoT

Projektarbeit

im Fach Cyber Security

Von

Dominik Deschner

Christian Iosif Schlier

Annika Stempfle

Jochen Welte

Hochschule Aalen

Hochschule für Technik und Wirtschaft

UNIVERSITY OF APPLIED SCIENCES

Prof. Roland Hellmann

23.06.2023

Kurzfassung

Im Zuge dieser Arbeit werden unterschiedlichen Blickwinkel der Sicherheit von IoT-Lösungen betrachtet. Zunächst werden drei unterschiedliche, reale Sicherheitsvorfälle aus dem Sektor IoT analysiert und gezeigt, welche Herangehensweisen Angreifer nutzten sowie welche Auswirkungen und Folgen die Angriffe nach sich gezogen haben. Danach werden unterschiedliche Arten von Schwachstellen und Bedrohungen im Kontext von IoT erläutert, um basierend darauf darzulegen, welche Sicherheitsmaßnahmen dazu beitragen können die Sicherheit von IoT-Anwendungen zu erhöhen. Im letzten Abschnitt dieser Arbeit werden die zuvor erarbeiteten Grundlagen anhand eines Praxisbeispiels aus dem Bereich Smart Home angewandt und die Erkenntnisse dieser Arbeit im Rahmen eines Fazits bewertet.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
CDR	Corporate Digital Responsibility
CoAP	Constrained Application Protocol
CPS	Cyber-physisches System
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
IIoT	Industrial Internet of Things
IoT	Internet of Things
LoRaWAN	Long Range Wide Area Network
MITM-Angriff	Man-in-the-Middle-Angriff
PAKE	Password Authenticated Key Exchange
SAE	Simultaneous Authentication of Equals
SSL	Secure Socket Layer
TLS	Transport Layer Security
WLAN	Wireless Local Area Network
WPA3	Wi-Fi Protected Access 3

Einleitung und Zielsetzung

Der unaufhaltsame Einzug von IoT-Geräten in unser aller Leben verändert nicht nur öffentliche Orte, sondern auch die Arbeitswelt oder unser Zuhause durch die Omnipräsenz von durchgängig mit dem Internet verbundenen, smarten Geräten, welche sich durch Sensorik ein genaues Bild ihrer Umwelt machen können und eine physische Brücke in den Cyberspace bilden. Nach Desktop-Computer, Smartphone und Virtual Reality Anwendungen beschleunigt das IoT die Verschmelzung und Symbiose zwischen der echten und den virtuellen Welten. Von enormen Produktivitätssteigerungen in der Industrie, verbesserter medizinischer Versorgung durch Telemedizin oder Erleichterungen im Alltag durch smarte Geräte und Gebäude könnten die Erwartungen an die Mehrwehrte des IoT kaum positiver sein. Jedoch birgt diese Entwicklung auch Schattenseiten und fundamentale Herausforderungen für die IT-Sicherheit.

Ziel dieser Arbeit ist es ein tiefgehendes Verständnis für diese Sicherheitsthematik im IoT zu schaffen. Dazu werden zunächst die allgemeinen Grundlagen zum Feld IoT dargelegt, bevor konkrete Sicherheitsvorfälle der jüngeren Vergangenheit aufgezeigt werden. Darauf aufbauend folgt die Erläuterung der Bedrohungen im IoT und die Erarbeitung von geeigneten schützenden Sicherheitsmaßnahmen. Abschließend werden diese Erkenntnisse am Praxisbeispiel Smart Home anschaulich vertieft.

1 Grundlagen des IoT

Der Themenkomplex Industrie 4.0/IoT stellt eine essenzielle, begriffliche Grundlage dieser Arbeit dar. Für einige der im Rahmen dieser Arbeit referenzierten Begrifflichkeiten lassen sich in der Literatur keine einheitlichen, konsistenten Definitionen finden [1, p. 113, 2, pp. 2788-2789, 3, p. 98]. Daher werden im Folgenden Definitionen erarbeitet, welche im Kontext dieser Arbeit als Basis dienen sollen.

1.1 Internet of Things

Unter Internet of Things, oder zu Deutsch Internet der Dinge, wird eine Ansammlung physischer Dinge, die über eine Netzwerkverbindung untereinander oder mit Diensten in der Cloud oder auf dem Edge-Layer kommunizieren können, verstanden [4, p. 2, 5, p. 11]. Diese IoT-Geräte sind mit Sensoren, Aktuatoren und Software ausgestattet und somit in der Lage Informationen über ihre Umgebung zu sammeln, zu verarbeiten und mit dieser zu interagieren. Einzelne Datenpunkte sind eindeutig mit der realen Welt verknüpft und über die Internetverbindung ist es möglich diese IoT-Gerätschaften konkret zu adressieren und fortlaufend mit diesen in Verbindung zu stehen, womit eine engere Verknüpfung zwischen der physischen Welt und Computersystemen erreicht wird [2, p. 2787].

Das Internet der Dinge findet unter anderem in folgenden Bereichen Anwendung:

- Smart Cities
- Smart Homes
- Effiziente Transportsysteme
- Vorhersage von Naturkatastrophen
- Industrieanwendungen
- Medizintechnik

Diese exemplarische, nicht vollständige Auflistung skizziert bereits die Tragweite und Omnipräsenz von IoT-Geräten in unterschiedlichen Gebieten des Alltags vieler Menschen [6, p. 138]. Dies lässt sich ebenso anhand der Anzahl von aktiven IoT-Geräten belegen. In Abbildung 1 wird die Anzahl aktiver IoT- und Nicht-IoT-Geräte in den Jahren 2010 – 2025 dargestellt bzw. prognostiziert. Hierbei sticht heraus, dass bereits 2020 mehr IoT-Verbindungen gezählt wurden als Konventionelle. Entsprechend der Prognose wird sich die Anzahl der IoT-Geräte zwischen 2020 und 2025 in etwa verdreifachen. Der pervasive Charakter und das daraus resultierende disruptive Potenzial des IoT wird auch in der Forschung anerkannt [3, p. 97, 5, p. 10] und untermauert die Relevanz dieser Technologie.

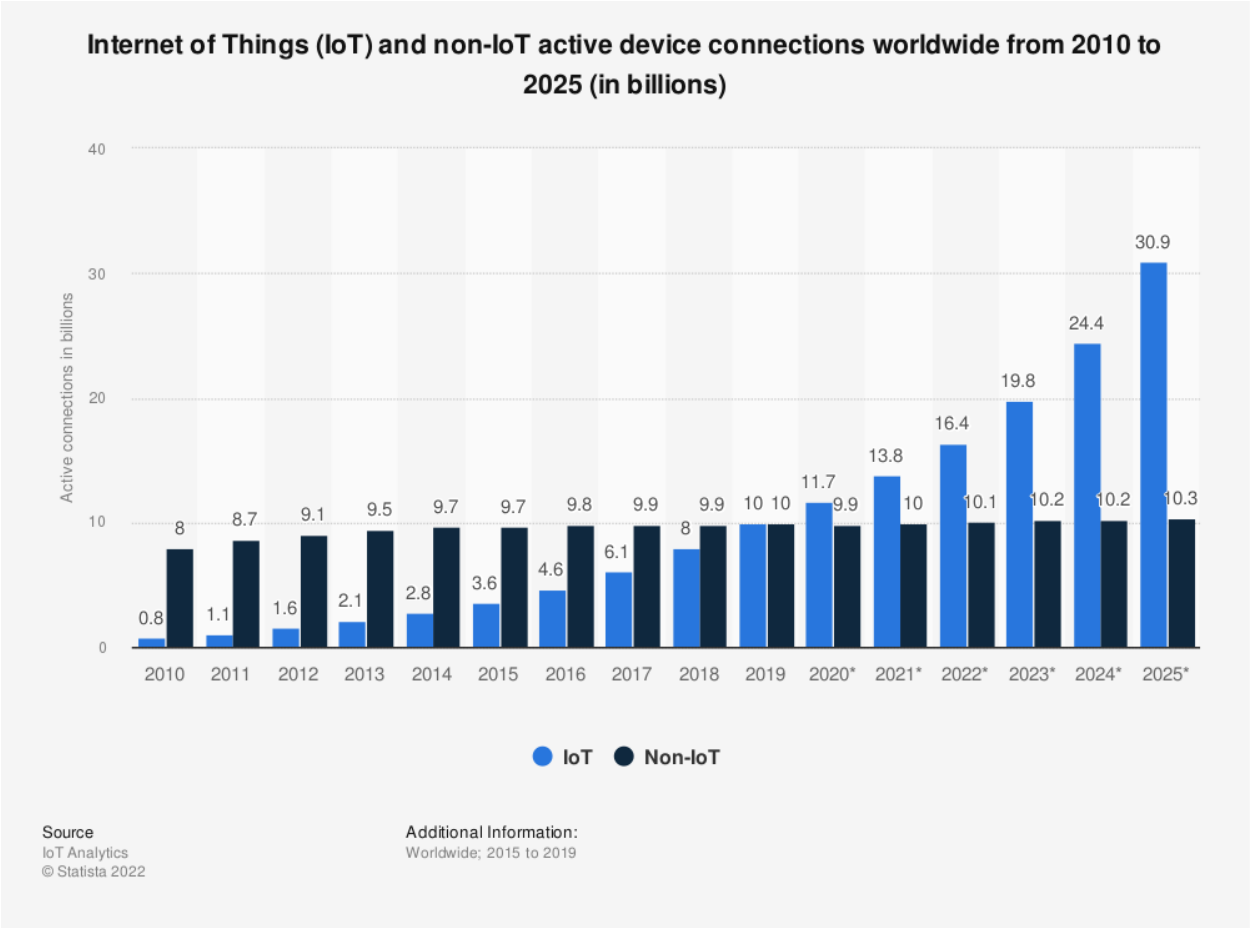

Abbildung 1 Entwicklung von IoT-Verbindungen gegenüber Nicht-IoT-Verbindungen [7]

1.2 IoT Systemarchitektur

Zur Beschreibung des Aufbaus von IoT-Systemen existiert keine holistische Architektur. Vielmehr ist das IoT durch Verwendung verschiedenster Technologien, Schnittstellen und Standards geprägt [8, p. 474]. Auch die interdisziplinare Betrachtung des Internets der Dinge führt dazu, dass in der Forschung unterschiedliche Architektur-Modelle existieren, die in Abhängigkeit zur akademischen Zielsetzung unterschiedliche Aspekte und Blickwinkel repräsentieren. Daher wird im Folgenden ein, für diese Arbeit dienliches, Architekturmodell zur Analyse und Beschreibung von Bedrohungen im IoT definiert und ein Überblick über die relevanten, technischen Aspekte der einzelnen Schichten gegeben.

IoT-Systeme lassen sich, wie in Abbildung 2 dargestellt in drei unterschiedliche Schichten aufgliedern.

Abbildung 2 Dreischichtiges IoT-Architekturmodell [3, p. 101, 8, p. 475]

1.2.1 Geräteschicht

Die Geräteschicht stellt die unterste Schicht eines IoT-Systems dar und umfasst alle Geräte oder Informationsträger, welche es dem System ermöglichen Daten über dessen Umwelt zu sammeln, Informationen zu gewinnen und mit dieser zu interagieren. Dabei werden unterschiedliche Sensoren-Gattungen wie z.B. Temperatur-, Luftfeuchtigkeit-, Druck- oder Näherungssensoren eingesetzt [4, pp. 70-72, 8, pp. 475-476]. Ebenso kann die Geräteschicht durch die Verwendung von Aktuatoren Einfluss auf die Umwelt nehmen, indem z.B. Ventile geöffnet oder geschlossen werden [9, p. 35].

Bei der Geräteschicht handelt es sich um eine heterogene Ansammlung unterschiedlichster Geräte von verschiedenen Herstellern, welche sowohl in Hinblick auf deren technischen Merkmale wie Rechenkapazität, Netzwerkanbindung oder Betriebssystem als auch in Bezug auf deren Verantwortlichkeit im IoT-System hoch variant ist. Einerseits finden sich batteriebetriebene Sensoren, die mit niedriger Abtastrate ihre Messwerte via Funk übertragen in dieser Ebene wieder, andererseits sind leistungsstarke Edge-Gateways welche Sensordaten auswerten, verarbeiten und an die Anwendungsschicht übertragen ebenso Teil der Geräteschicht [8, pp. 475-476, 9, p. 35]. Je nach Anwendungszweck des IoT-Systems können Teilnehmer der Geräteschicht lokal, regional oder sogar global verteilt sein.

1.2.2 Netzwerkschicht

Zentrale Verantwortlichkeit der Netzwerkschicht ist die Harmonisierung und Übertragung von Daten aus der Geräteschicht an die Anwendungsschicht. Die heterogene Fragmentierung der Geräteschicht schlägt auf die dort verwendeten Kommunikationsprotokolle und Datenformate durch, welche in der Netzwerkschicht vor der Übertragung zur

Anwendungsschicht normiert werden. Weiterhin ist das verwendete Übertragungsmedium wie z.B. UMTS, WLAN, Ethernet Bestandteil der Netzwerkschicht [8, pp. 476-477].

Weiterhin ermöglicht die Netzwerkschicht die Kommunikation zwischen einzelnen Teilnehmern der Geräteschicht und ermöglicht so einen bidirektionalen, horizontalen Austausch zwischen IoT-Geräten [9, pp. 36-37].

1.2.3 Anwendungsschicht

In der Anwendungsschicht werden die zuvor gesammelten, normierten und übertragenen Daten zusammengeführt, verarbeitet und gespeichert. Diese Schicht ist auf einem zentralen, von allen IoT-Geräten erreichbaren IT-System, wie z.B. einem Rechenzentrum oder der Cloud bereitgestellt und kann einzelne IoT-Geräte adressieren und z.B. Aktuatoren ansteuern [8, p. 477].

Auf der Anwendungsschicht werden Erkenntnisse, Benachrichtigungen und Berichte aus den gesammelten Daten generiert und den Anwendern über das Internet in Form von Web- oder Mobilanwendungen bereitgestellt [9, p. 37].

1.3 Industrie 4.0 und Industrial Internet of Things (IIoT)

Nachdem in den vorhergehenden Abschnitten ein Basis-Verständnis für das Internet der Dinge und dessen strukturellen Aufbau geschaffen wurde, erfolgt nun die nähere Betrachtung des industriellen Internets der Dinge, dem Begriff "Industrie 4.0." und dessen historische Entwicklung.

„Industrie 4.0“ beschreibt die dem IoT-Modell zugrundeliegende Konnektivität zwischen physischen Objekten und der Informationstechnologie. Genauer gibt der Begriff die intelligente Vernetzung von Maschinen und Abläufen in der Industrie mithilfe von Informations- und Kommunikationstechnologie zu wieder [10]. Nach dieser Definition ist "Industrie 4.0" als industrieller Teilbereich des Internets der Dinge zu betrachten (= engl. Industrial Internet of Things kurz IIoT). Die Nummer "4.0" im Begriff "Industrie 4.0" verdeutlicht, dass es sich um die vierte industrielle Revolution handelt. Die Basis für die vierte industrielle Revolution bildeten andere vorausgehende und gesellschaftsverändernde industrielle Revolutionen:

Die erste industrielle Revolution, die im 18. Jahrhundert stattfand, markierte den ersten bedeutenden Wandel in der industriellen Produktionsweise. Die Einführung der Dampfmaschine ermöglichte es, menschliche und tierische Muskelkraft bei der Herstellung von Gütern durch mechanische Energie zu ersetzen. Im Verlauf des 19. Jahrhunderts setzte sich die arbeitsteilige Massenfertigung flächendeckend durch, was später als zweite industrielle Revolution bezeichnet wurde. Durch die Einführung von Produktionslinien und die Anwendung von Spezialisierung konnte die Effizienz und Produktivität in der Herstellung erheblich gesteigert werden. Dies führte zu einer weiteren Beschleunigung des industriellen Fortschritts und einer massiven Veränderung der wirtschaftlichen Landschaft. Die dritte industrielle Revolution basiert auf kommerziell nutzbarer Computertechnik und

den Fortschritten in der Elektrotechnik. Die Verwendung und Kombination dieser beiden Techniken ermöglichten ab den 1950er bis 1960er – Jahren weitere revolutionäre Fortschritte in der Automatisierung von Produktionsabläufen. [11]

Die vierte industrielle Revolution begann in den 2000er-Jahren als sogenannte cyber-physische Systeme die physische und digitale Welt erstmals miteinander verknüpften. Erstmalig wurde ihr im Jahr 2011 auf der Hannover Messe der Name "Industrie 4.0" verliehen. [12]

Die vier erläuterten industriellen Revolutionen sind in Abbildung 3 aus [11] übersichtlich dargestellt:

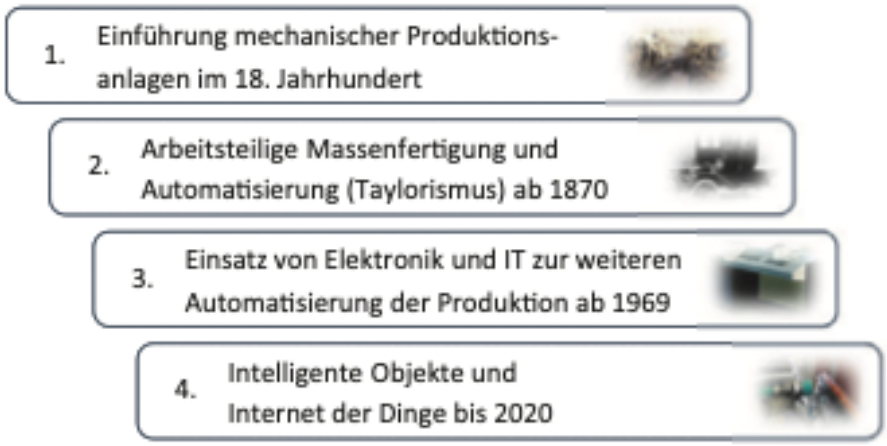

Abbildung 3 Die vier technologiegetriebenen Revolutionen der Industrie aus [11]

1.4 Cyber-physische Systeme (CPS)

Industrie 4.0 ist die Aufforderung an die Industrie ihre eigenen vernetzten und intelligenten Produktionsprozesse mithilfe von Informations- und Kommunikationstechnologie zu entwickeln. Hierfür werden die bereits im vorherigen Abschnitt erwähnten cyber-physischen Systeme (=CPS) eingesetzt. Diese werden nun näher erläutert.

Cyber-physische Systeme realisieren die Verbindung der physischen mit der digitalen Welt. Dazu werden physische und informationstechnische Elemente mithilfe von Dateninfrastruktur miteinander verbunden. Die verbindende Dateninfrastruktur ist typischerweise das Internet. Die darüber in Echtzeit kommunizierten Daten werden zweckorientiert verarbeitet und ermöglichen, dass CPS selbst geeignete Handlungen wählen und durchführen können. [13]

Ein rudimentäres, aber anschauliches Beispiel für ein solches CPS, können Fenster-Jalousien sein, die sich mithilfe von Sensorik, Software und Aktuatoren selbstständig regulieren. Dieses Beispiel ist in Abbildung 4 grafisch dargestellt und mit den im folgenden beschriebenen Element-Nummern versehen. Die Außen-Fenster-Jalousien sind mit

Sensoren ausgestattet, die aktuelle Informationen wie die Stärke der Sonneneinstrahlung, Außen- und Raumtemperatur erfassen (1). Diese erfassten Informationen werden über ein Netzwerk in Echtzeit an eine Software kommuniziert (2). Sie kann anhand von definierten Gesichtspunkten (z.B. das Ziel Heizkosten im Innenraum zu senken) entscheiden, wann die Außen-Fenster-Jalousien geöffnet bzw. geschlossen werden sollen (3). Der aus dieser Erkenntnis resultierende Handlungsbefehl wird über das Netzwerk an die Motorik der Jalousien gemeldet (4), welche dann den mechanischen Vorgang des Schließens oder des Öffnens vornimmt (5).

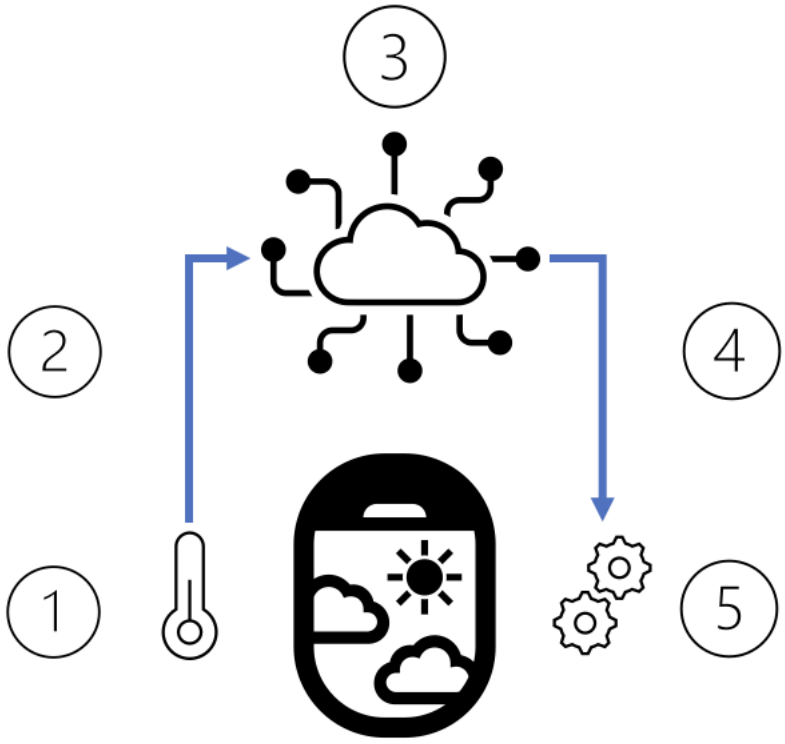

Abbildung 4 eigenes Beispiel eines cyber-physischen Systems: „Jalousie“

Vergleicht man nun die Elemente des Beispiels „Jalousie“ mit dem Ebenen-Modell aus Absatz 1.2 wird deutlich, in welcher Form die Ebenen des IoT in der Praxis ineinandergreifen: Die Geräteschicht bilden im Beispiel die Jalousie selbst, die Sensorik (1) und die Aktuatoren (5). Die Netzwerkschicht ist in Form der Übertragenen Daten (2) und Handlungsbefehle (4) abgebildet und die Anwendungsschicht ist die ausgelagerte Software, die die Daten verarbeitet und Maßnahmen ableitet (3). Die folgende Abbildung 5 verdeutlicht diese Zuordnung der Elemente zu den charakteristischen IoT-Schichten am Beispiel „Jalousie“:

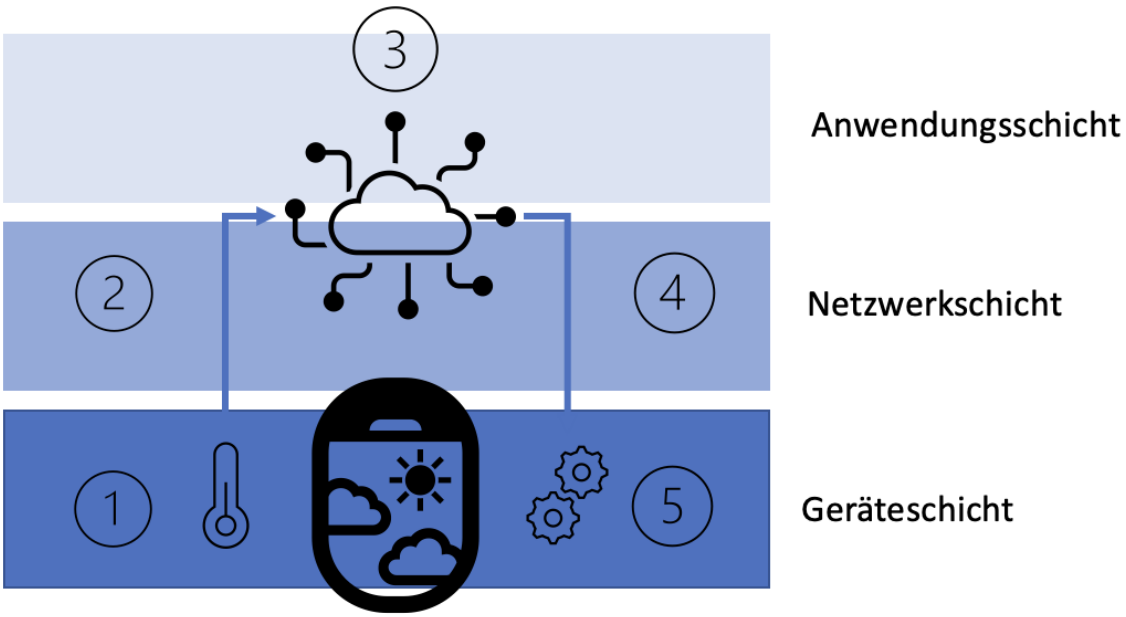

Abbildung 5 eigene Darstellung der IoT-Ebenen am Praxisbeispiel "Jalousie"

In diesem Kapitel wurde ein Verständnis für die Begriffe Internet der Dinge (IoT) und Industrie 4.0 (IIoT), sowie deren mögliche Ausprägungen geschaffen. Es wurden die charakteristischen Schichten des IoT und cyberphysische Systeme vorgestellt, die mithilfe des Beispiels „Jalousie“ plastisch erläutert wurden. Das so geschaffene Verständnis für die Elemente des IoT bildet die Grundlage für die nachfolgende Arbeit.

2 Analyse vergangener IoT-Sicherheitsvorfälle

Durch die ständig wachsende IoT und Industrie 4.0 nehmen die Zahl der Angriffe auf Schwachstellen in den mit dem Internet vernetzten Geräten zu. Durch den Glasfaserausbau und das schnellere Internet haben Hacker die Möglichkeit, leichter in Geräten, die mit dem Internet verbunden sind durchzudringen. Im Folgenden werden drei IoT-Sicherheitsvorfälle analysiert.

2.1 Reaper oder IoTroop 2017

Reaper oder IoTroop war ein Botnetz, dass etwa eine Million IoT-Geräte im Jahr 2017 mit einer Schadsoftware infizierte. Im folgenden Jahr wurden viele DDoS-Angriffe auf das Finanzdienstleistungssektor durchgeführt. Das IoTroop (IoT-Botnetz) kompromittierte TVs, Router, DVRs und IP-Kameras von Anbieter wie GoAhead, MikroTik oder Ubiquity. Der Angriff erfolgte auf 139 Ländern verstärkt in den USA, Russland, China und Brasilien, wo die meisten anfällige IoT-Geräte von MikroTik benutzt wurden. Wie in Abbildung 6 dargestellt nutzten die Angreifer unterschiedliche Sicherheitslücken aus, um die Kontrolle über die Geräte zu übernehmen und ein Botnetz zu bilden. Dabei wurden infizierte Geräte dazu genutzt, weitere Geräte anzugreifen und in das Botnetz aufzunehmen. [14]

Im Gegensatz zum Mirai-Botnetz nutzte Reaper eine Vielzahl von bekannter Exploits und Schwachstellen, um IoT-Geräte zu infizieren und zu kontrollieren. Reaper führte aufwendigere konservative TCP-SYN-Scans an einer Reihe verschiedener Ports durch, mit jeweils eine IP. Der SYN-Scan wurde immer in der gleichen Reihenfolge durchgeführt und die Quell-IP und der Quellport des Scans blieben während der gesamten Lebensdauer des Bots gleich. [15]

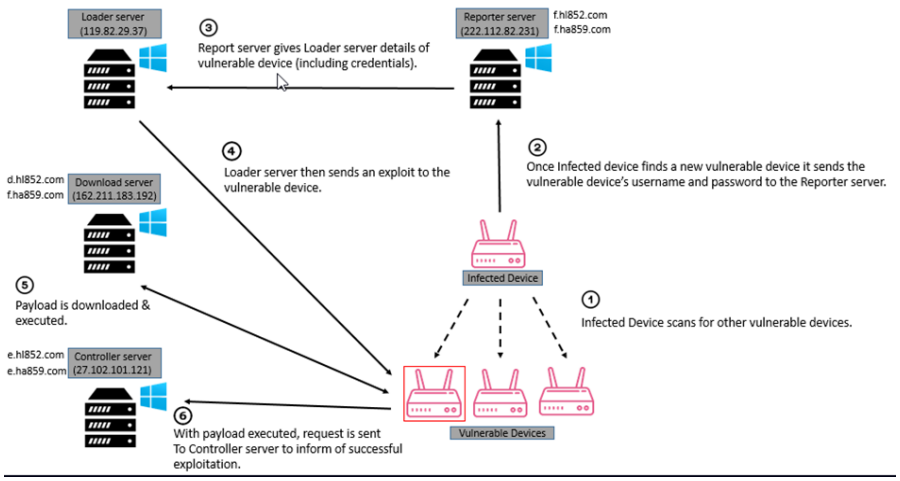

Abbildung 6 Diagramm der Malware-Verbreitungsinfrastruktur [16]

Der IoTroop-Angriff hatte erhebliche Auswirkungen auf die betroffenen Geräte und die globale IoT-Sicherheit. Das Botnetz erreichte eine beeindruckende Größe und hatte das Potenzial für massive DDoS-Angriffe. Die betroffenen Geräte waren anfällig für Fernsteuerung und konnten für kriminelle Aktivitäten wie Datenlecks, Ransomware-Verbreitung und den Diebstahl persönlicher Informationen genutzt werden.

2.2 Mirai Botnet-Angriff 2016:

Der Mirai-Botnet-Angriff im Jahr 2016 war einer der signifikantesten Angriffe auf das Internet der Dinge (IoT) Sicherheit. Das Mirai-Botnet wurde von einer Gruppe von Hackern verwendet, um unsichere IoT-Geräte wie Überwachungskameras und Router zu infizieren. Die betroffenen Geräte wurden dann zu einem Botnetz zusammengeschlossen, das verwendet wurde, um massive Distributed-Denial-of-Service (DDoS)-Angriffe auf verschiedene Ziele durchzuführen. Die Angriffe beeinträchtigten eine Reihe von Websites und Diensten, darunter Twitter, Spotify und Reddit. Der Vorfall verdeutlichte die Schwachstellen unsicherer IoT-Geräte und die Notwendigkeit einer verbesserten Sicherheit in diesem Bereich.

Der Mirai-Bot wurde im August 2016 von einer Forschungsgruppe namens MalwareMustDie gegründet. Bei dem Angriff wurden ca. 600.000 IoT Geräte in 164 Länder infiziert. In Abbildung 7 ist die weltweite Ausbreitung des Mirai-Botnets visualisiert und zeigt, dass sich die Infektionen nicht auf einzelne Länder beschränken, sondern sich global auswirken.

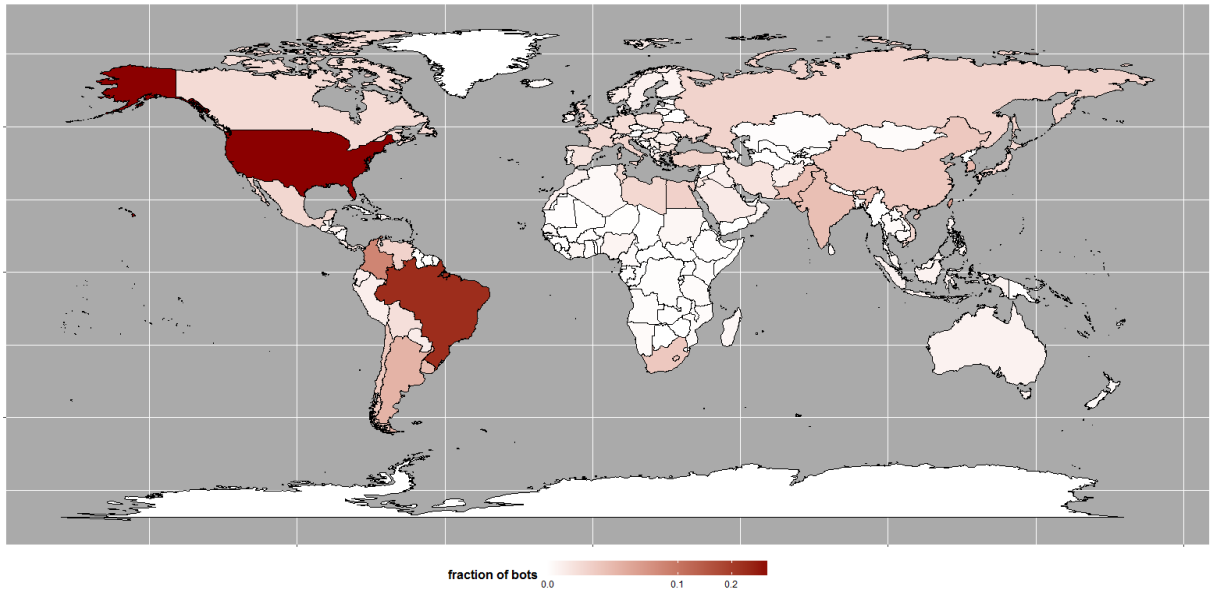

Abbildung 7 Globale Verbreitung von Mirai-Bots [18]

Die Website des PC-Sicherheitsberaters Brian Krebs wurde von zahlreichen Anfragen von insgesamt 620 Gbit/s im September 2016 betroffen. In der gleichen Zeit konzentrierte sich ein deutlich größerer DDoS-Angriff mit Mirai-Malware mit einer Höchstgeschwindigkeit von 1,1 Tbit/s auf den französischen Webhosting- und Cloud-Service-Anbieter OVH. Nach der Veröffentlichung des Mirai-Quellcodes durch den Hersteller kurze Zeit später boten

Programmierer Mirai-Botnetze mit mehr als 400.000 gleichzeitig angeschlossenen Geräten zur Miete an. Es folgten weitere komplexere Mirai-Angriffe, allen voran einer im Oktober 2016 gegen den Dienstleister Dyn, der viele Websites wie Netflix, Twitter, Reddit und Spotify lahmlegte. [19]

Es wurde von Dyn, bestätigt, dass es zwei verschiedene Angriffe waren. Der erste Angriff konzentrierte sich hauptsächlich auf den US-Osten und der zweite erfolgte Weltweit. In November waren es schon 600.000 infizierte IoT Geräte wie Überwachungskameras, Router, Smart-TVs oder andere smarte Systeme die Teil des aktiven Botnetzes wurden. [20]

Die Funktion des Mirai-Botnetzes ist komplex da der Bot die Malware ist, die IoT Geräte verunreinigt. Die Schadsoftware wird auf falsch konfigurierte oder ohne Sicherheit geupdatete IoT Geräte übertragen. Der Command-and-Control-Server (C&C) stellt dem Botmaster eine integrierte Administrationsoberfläche zur Verfügung, um den Zustand des Botnetzes zu überprüfen und neue DDoS-Angriffe zu koordinieren.

Wie in Abbildung 8 dargestellt ist der Loader für die Verteilung von ausführbaren Dateien und die Infektion verwundbarer Geräte verantwortlich. Dabei kann die Malware für unterschiedliche Plattformen und Prozessorarchitekturen (ARM, MIPS, x86 etc.) ausgeliefert werden. Der Berichtsserver unterhält eine Datenbank mit Erkenntnissen über alle Geräte im Botnetz. Frisch kontaminierte Geräte sprechen regelmäßig direkt damit und bilden zusammen ein Botnetz. [19]

Betrieb und Kommunikation des Mirai-Botnetzes. Mirai verursacht einen verteilten Denial-of-Service (DDoS) auf einer Reihe von Zielservern, indem es sich ständig auf Internet-of-Things-Geräte (IoT) ausbreitet.

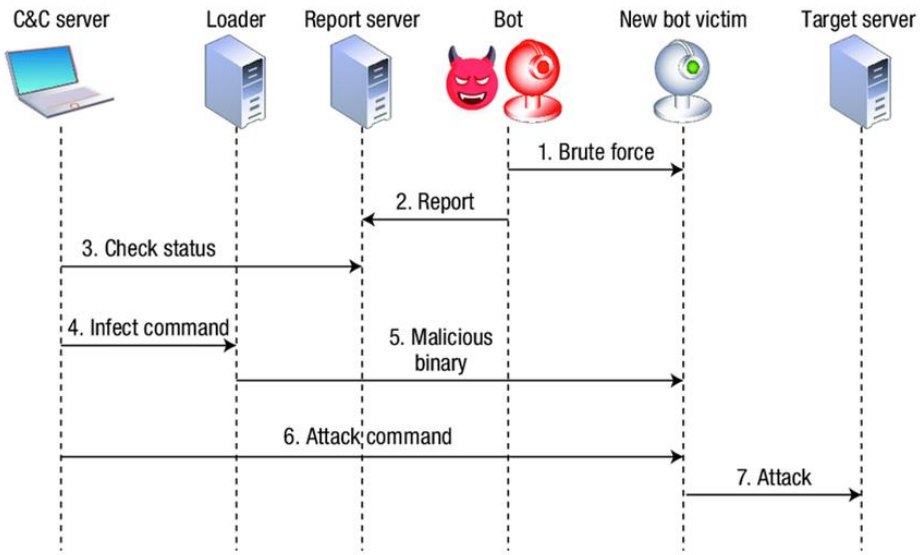

Abbildung 8 Mirai Botnet Ablauf einer Infektion [21]

Der Mirai Botnet-Angriff und die Durchführung des Angriffs durch Ausnutzung von Schwachstellen wie Standardbenutzernamen und Passwörter in unsicheren IoT-Geräten und die verursachten Schäden verdeutlichen die Notwendigkeit eines besseren Schutzes und einer stärkeren Sicherheitsinfrastruktur für IoT-Systeme. Unternehmen und Organisationen, die von den Angriffen betroffen waren, erlitten erhebliche finanzielle Verluste und sahen sich gezwungen, ihre Sicherheitsmaßnahmen zu überdenken und zu verbessern.

2.3 Stuxnet-Angriff 2010:

Der Stuxnet-Angriff Code-Name „Olympische Spiele“ auf eine Urananreicherungsanlage in Natanz, Iran im Jahr 2010 ist einer der komplexesten und bekanntesten IoT Cyberangriffe aller Zeiten. Der Stuxnet-Angriff wurde durch eine hochentwickelte Malware ein Computerwurm durchgeführt, der speziell für die Sabotage von industriellen Steuerungssystemen von den Regierungen der USA und Israels entwickelt wurde. Die Malware nutzte Schwachstellen und gezielte Angriffstechniken, um sich in das Zielsystem einzuschleusen und zu verbreiten. Die Stuxnet-Malware infizierte USB-Sticks und Netzwerke, um sich Zugang zu den Zielcomputern und Rotoren der Zentrifuge zu verschaffen. [22]

Wie in Abbildung 9 dargestellt, nutzte die Malware Schwachstellen in Windows-Betriebssystemen an der Siemens Step7 Software aus, wodurch der Wurm Zugriff auf die industriellen Programmlogiksteuerungen erhielt. Dadurch konnten die Entwickler des Wurms verschiedene Maschinen an den Industriestandorten steuern und auf wichtige Industrieinformationen zugreifen. Stuxnet manipulierte die Programmierung der Nuklearzentrifugen mithilfe eines Rootkits, um die Drehzahl von Motoren zu ändern und diese zu beschädigen. Die Schäden an den Rotoren der Zentrifuge traten langsam im Laufe der Zeit auf und liefen in Schritten von 15 oder 50 Minuten, getrennt durch 27 Tage Normalbetrieb. Die Folge waren nicht ordnungsgemäß angereichertes Uran sowie rissige und zerstörte Rotorrohre in den Zentrifugen, was zum totalen Ausfall der betroffenen Maschinen führte. Dies hatte ernsthafte Auswirkungen auf die Leistung und der Zentrifugen, was zu Störungen im Nuklearprogramm des betroffenen Landes führte. Die Schäden an den Rotoren der Zentrifuge traten langsam im Laufe der Zeit auf und liefen in Schritten von 15 oder 50 Minuten, getrennt durch 27 Tage Normalbetrieb. Die Folge waren nicht ordnungsgemäß angereichertes Uran sowie rissige und zerstörte Rotorrohre in den Zentrifugen. [23]

Bei diesem Cyberangriff, auf die industriellen SCADA-IoT-Geräte wurden irreversible Schäden bei über 1.000 Urananreicherungszentrifugen am iranischen Atomprogramm verursacht. Der Stuxnet-Virus hat nicht nur das Netzwerk beschädigt, sondern die ganze Iranische Urananreicherungsanlage inklusive der Endgeräte.

Der Angriff hatte enorme Auswirkungen auf den Iran und sein Atomprogramm da die restlichen Zentrifugen auch abgeschaltet werden mussten und somit die Uran-Anreicherung verzögert wurde. [24]

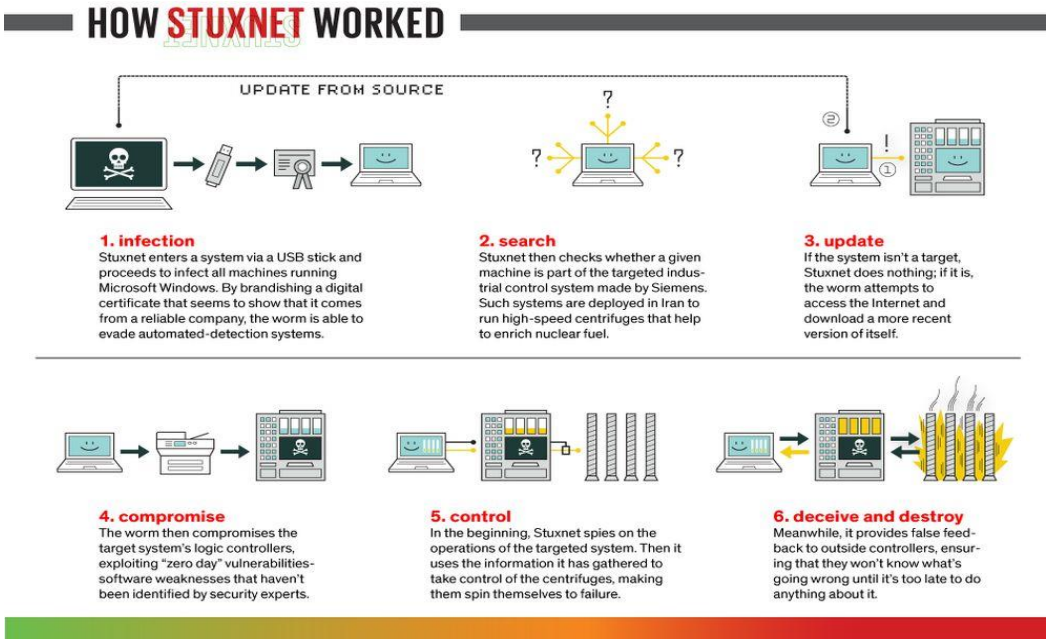

Abbildung 9 Die Funktion von Stuxnet [25]

2.4 Fazit zur Analyse der 3 vergangener IoT-Sicherheitsvorfälle:

Die Analyse der entstandenen IoT-Sicherheitsvorfälle, durch den Reaper oder IoTroop, Mirai Botnet und des Stuxnet, verdeutlicht die zunehmende Bedrohung und Verwundbarkeit von IoT-Geräten und -Infrastrukturen, insbesondere in der Digitalisierung und Industrie 4.0. Unzureichende Sicherheitsmaßnahmen und bekannte Schwachstellen in IoT-Geräten, können zu erheblichen Schäden führen. Die untersuchten Vorfälle zeigen die Dringlichkeit der Verbesserung der IoT-Sicherheit. Hersteller müssen sicherstellen, dass ihre Geräte sicher entwickelt und konfiguriert werden. Benutzer sollten regelmäßige Sicherheitsupdates durchführen, starke Passwörter verwenden und Geräte von Drittanbietern sorgfältig überprüfen.

Trotz der Vorteile und guten Aussichten des Internets der Dinge gibt es einige ungelöste Sicherheitsprobleme, sowie rechtliche Vorschriften zur Netzwerk- und Gerätesicherheit, die beachtet werden müssen. Die schnelle Entwicklung und Verbreitung von IoT-Technologien eröffnen immense Chancen, bringen jedoch auch erhebliche Risiken mit sich da fast täglich neue IoT-Geräte mit unentdeckten Schwachstellen auf den Markt kommen.

3 Maßgebliche Bedrohungen im IoT

Sicherheit ist bereits während der Anfänge des Internet of Things in der Literatur als ein fundamentaler Erfolgsfaktor und gleichzeitig als existenzielle Gefahr identifiziert worden. Im vorherigen Kapitel wurde gezeigt, dass trotz dieser frühen Erkenntnis, offensichtliche Angriffsvektoren existieren und bereits in der Vergangenheit ausgenutzt wurden [2, pp. 2787-2788, 26, p. 27]. Dieses Kapitel befasst sich mit der systematischen Analyse von Angriffsvektoren in IoT-Systemen.

IoT-Systeme bestehen aus unterschiedlichen, distinkt abzugrenzenden Schichten, welche durch die horizontale Integration heterogener Komponenten entstehen. Dementsprechend können unterschiedliche Bedrohungen und Schwachstellen für einzelne Schichten identifiziert werden. Im Folgenden werden die, in Absatz 1.2 definierten, architektonischen Schichten hinsichtlich relevanter Schwachstellen und Angriffsvektoren analysiert.

3.1 Geräteschicht

Auf der Geräteebene sind verschiedenartige Systeme zu finden, welche ihre Umwelt überwachen und mit dieser interagieren. Im Vergleich zu konventionellen IT-Systemen stellt die Geräteschicht ein wesentliches Differenzierungsmerkmal des IoT dar, woraus sich wesentliche Herausforderungen bezüglich deren Sicherheit ableiten lassen.

Die Teilnehmer der Geräteschicht sind physisch verteilt und ggf. in die Umgebung des Alltags der Verwender eingebettet, was eine feingranulare Zugriffskontrolle zu den Systemen selbst kaum ermöglicht. Entsprechend hoch ist das Risiko, dass sich ein Angreifer physischen Zugriff zu einem IoT-Gerät verschaffen kann [27, p. 8186, 28, p. 407]. Heterogenität stellt ein wesentliches Merkmal der Geräteschicht dar. Daraus ergibt sich, dass unterschiedliche Protokolle und Schnittstellen eingesetzt werden müssen, um Interkonnektivität zwischen den einzelnen Geräten herzustellen [29, pp. 152-153]. Viele IoT-Geräte operieren mit stark limitierter Rechenkapazität verglichen mit konventionellen Computersystemen, welche Rechenleistung im Überfluss bereitstellen. Das führt dazu, dass aufwändige Sicherheitsmechanismen aufgrund von Ressourcenknappheit häufig nicht oder nur unzureichend implementiert werden können [30, pp. 4-5].

Im Folgenden werden daraus resultierende Schwachstellen und Bedrohungen genauer erläutert.

3.1.1 Node Capture Attack

Als Node Capture Attack wird eine Reihe von Angriffen bezeichnet, welche das Ziel hat Verschlüsslungsparameter von Teilnehmern der Geräteschicht zu extrahieren und die Kommunikation innerhalb des IoT-Systems zu überwachen und zu manipulieren [31, p. 133].

In Abbildung 10 werden die drei Angriffsphasen visualisiert. Zunächst erlangt der Angreifer physische Kontrolle über ein Gerät. Danach werden sensible Informationen, durch die Anwendung von Reverse Engineering Praktiken, extrahiert und der Eindringling ist in der Lage sich als das gekaperte Gerät auszugeben und die interne Kommunikation des IoT-Systems zu infiltrieren. Abhängig von dem eingesetzten Authentifizierungs-Protokoll ist es möglich Geheimnisse von weiteren Netzteilnehmern abzugreifen und deren Identität ebenfalls zu übernehmen [32, pp. 517-518].

Ein erfolgreich durchgeführter Node Capturing Angriff ist häufig das Fundament für weitere Angriffe auf das IoT-Netzwerk, da der Angreifer nun in der Lage innerhalb des Netzwerks zu kommunizieren und gezielt Schwachstellen auszunutzen. Der physische Zugriff auf IoT-Geräte stellt in den meisten Fällen keine große Hürde dar, weshalb diese Schwachstelle zu Beginn eines Angriffs ausgenutzt wird, um weiter in das System einzudringen.

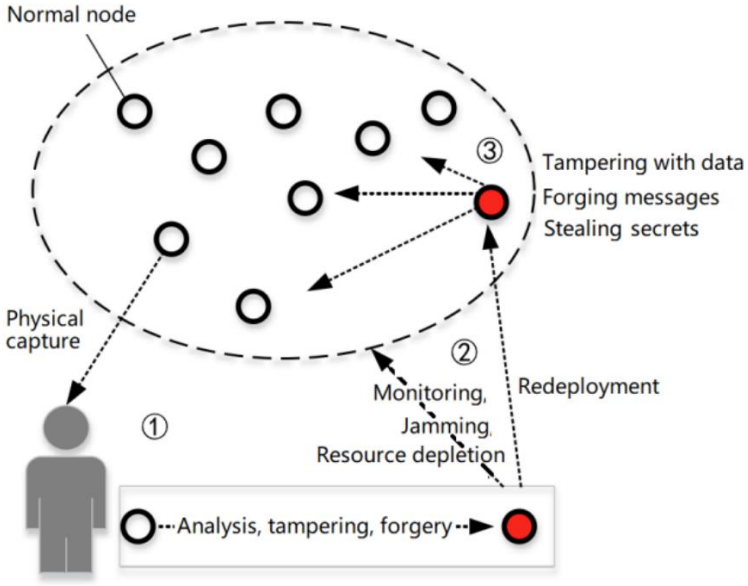

Abbildung 10 Phasen Node Capturing Angriff [31, p. 133]

3.1.2 Man-in-the-Middle

Als Man-in-the-Middle (MITM) werden unterschiedliche Angriffe bezeichnet, bei denen ein Angreifer den Netzwerkverkehr, der für einen anderen Netzwerkteilnehmer bestimmt ist, auf sich selbst umleitet. Dadurch ist er in der Lage die Kommunikation abzuhören, zu manipulieren oder zu terminieren [33, pp. 16-18].

Besonders im Kontext der Geräteschicht von IoT-Anwendungen finden sich häufig keine adäquaten Gegenmaßnahmen für Man-in-the-Middle Angriffe wie z.B. authentifizierte SSL-Verschlüsselung [33, p. 20]. Dadurch kann ein Angreifer die Möglichkeit gezielt in die Kommunikation eines IoT-Geräts einzugreifen auch dafür nutzen weitere Angriffe auf das System durchzuführen, z.B. dadurch, dass eine Firmwaredatei beim Download des Updates auf das Gerät manipuliert, wird so dass Schadcode ausgeführt wird [34, p. 2].

Für die Durchführung von MITM-Angriffen werden unterschiedliche Technologien wie z.B. ARP Cache Poisoning, DNS Spoofing oder SSL-Hijacking eingesetzt und ggf. kombiniert, welche vor allem in TCP/IP basierten Computernetzwerken Anwendung finden [33, p. 18]. Jedoch zeigt die aktuelle Forschung, dass MITM-Angriffe auch in für IoT-Systeme relevanten Übertragungstechnologien wie z.B. LoRaWAN [35, 36] oder Bluetooth Low Energy [37, 38] umsetzbar sind.

3.1.3 Side-Channel Attack

Während der Datenverarbeitung auf einem Computersystem entstehen abseits der gewünschten Berechnungsergebnisse einfach zugängliche, zusätzliche Signale, die von einem Angreifer abgegriffen und dazu verwendet werden können geheime Informationen zu entwenden. Diese Signale können über unterschiedliche Kanäle wie z.B. Überwachung von Netzwerkverkehr, Energieverbrauch oder elektromagnetische Impulse generiert werden. Abseits der physischen Ebene können auch durch Software, die ohne administrative Berechtigungen oder in einer Sandbox ausgeführt wird, Informationen gesammelt werden, die dazu führen, dass die Privatsphäre des Nutzers kompromittiert wird. So kann z.B. die Überwachung des Lage- und Beschleunigungssensors Aufschluss auf die Tastatureingabe geben. Auch frei zugreifbare Informationen des Betriebssystems können dazu verwendet werden andere Anwendungen bzw. den Benutzer auszuspähen [39, pp. 1613-1614]

[40] haben gezeigt, dass es möglich ist durch die Messung elektromagnetischer Emissionen zu erkennen, welche Aktivität auf einem Gerät ausgeführt wird. Auch Bilder, die auf ein Display dargestellt werden, können über diesen Kanal abgefangen werden und darüber Benutzereingaben überwacht werden [41]. Durch die Überwachung des Energieverbrauchs besteht die Möglichkeit private kryptografische Schlüssel zu extrahiert [42].

Side Channel Angriffe bieten einerseits ein hohes Bedrohungspotenzial, da diese nicht auf das Vorhandensein konkreter Schwachstellen in Soft- oder Hardware angewiesen sind, sondern universell angewandt werden können. Insbesondere weil alle Architekturschichten von IoT-Systemen betroffen sein können. Angreifer können unter Umständen physischen Zugriff zu IoT-Geräten erlangen und so passive Messungen durchführen, aber auch auf der Anwendungsschicht stellen Side Channel Angriffe eine Gefahr dar. Spectre [43] und Meltdown [44] sind hervorragende Beispiele dafür, dass diese Angriffsgattung auch in der Cloud eine relevante Bedrohung darstellt.

Die Tragweite von Side Channel Angriffen ist durch deren praktische Umsetzbarkeit limitiert. Viele Angriffstechniken funktionieren im Moment unter Laborbedingungen, lassen sich aber für konkrete Angriffe schwer umsetzten, da Messequipment platziert werden oder eine Reihe von Vorbedingungen erfüllt werden muss. Jedoch können weitere Fortschritte im Bereich der künstlichen Intelligenz dazu führen, dass immer mehr Side Channel Angriffe praktikabel werden und stellen somit eine erhebliche Gefahr für IoT-Systeme dar [40, p. 113586].

3.1.4 Malware Injection

Unter dem Begriff „Malware Injection“ lassen sich Angriffe mit der Intention Code oder Befehle des Angreifers auszuführen und Malware auf dem Zielsystem zu installieren zusammenfassen. Dadurch kann die Kontrolle über das jeweilige System übernommen werden und somit dessen Integrität, Verfügbarkeit und Vertraulichkeit kompromittiert werden [39, pp. 1617-1619].

Die erfolgreiche Durchführung einer Malware Injection bedingt das Ausnutzen einer auf dem Zielsystem vorhandenen Schwachstelle. Aufgrund der großen Heterogenität auf der Geräteebene lassen sich eine Vielzahl von möglichen Angriffsvektoren identifizieren [39, pp. 1617-1619, 45, p. 433]:

- SQL-Injection
- Cross Site Scripting
- Cross Site Request Forgery
- Server Site Request Forgery
- Remote Code Execution
- Manipulierte Firmwareupdates
- Brute-Force Passwort Cracking

Nach erfolgreicher Installation der Malware hat der Angreifer die Möglichkeit physischen Schaden an der Umgebung des IoT-Geräts anzurichten, sensible Daten auszulesen, das Gerät für eigene Zwecke wie DDoS oder Cryptomining zu missbrauchen oder das Gerät physisch zerstören [46, p. 725]. Infizierte IoT-Geräte werden in vielen Fällen teil eines Botnets, welches es dem Angreifer erlaubt eine große Anzahl an gehackten Geräten zu kontrollieren. Damit das Botnet immer weiter wächst enthält Botnet-Malware in der Regel Funktionalität, die nach weiteren verwundbaren Geräten in der Nähe des gehackten Gerätes oder im Internet sucht und dieses ebenfalls mit Schadsoftware infiziert [45, pp. 433-434].

3.2 Netzwerkschicht

Im vorherigen Abschnitt wurden Schwachstellen auf der Geräteebene von IoT-Systemen erläutert. Zur Kommunikation mit der Anwendungsschicht wird die Netzwerkschicht verwendet, welche den Transport von Daten zwischen den beiden Schichten realisiert. Für die Übertragung in der Netzwerkschicht stehen unterschiedlichste Protokolle, Übertragungsmedien und Standards bereit.

Mögliche Schwachstellen und Angriffsvektoren ergeben sich aus der Kombination der verwendeten Technologien. So besteht in TCP/IP basierten Netzwerken die Möglichkeit hierfür spezifische Schwachstellen, wie z.B. ARP Cache Poisoning oder TCP Syn Flood auszunutzen [47]. Dies trifft auch auf die genutzte Übertragungstechnologie wie z.B. LTE zu [48]. Die zuvor referenzierten Bedrohungen existieren nicht nur im Kontext einer IoT-Anwendung. Im Folgenden werden relevante Protokolle zur Datenübertragung im IoT auf Schwachpunkte analysiert.

Folgende Protokolle zur Übertragung von Anwendungsdaten haben sich im IoT etabliert [49, p. 1]:

- MQTT (Message Queuing Telemetry Transport)
- HTTP (Hypertext Transfer Protocol)
- AMQP (Advanced Message Queuing Protocol)
- CoAP (Constrained Application Protocol)

Besonders das MQTT-Protokoll ist einerseits weit verbreitet [50, p. 138] und bietet nicht nur im Vergleich zu den anderen Protokollen wenig Sicherheitsmechanismen, sondern ist auch durch unterschiedliche, protokollspezifische Schwachstellen verwundbar. MQTT bietet lediglich einen optionalen und trivialen Mechanismus zur Client-Authentifizierung, basierend auf der Abfrage von Benutzername und Passwort, welche auf Protokollebene unverschlüsselt übertragen werden. Dadurch können diese Daten unter Umständen von einem Angreifer abgehorcht werden. Verschlüsselte Kommunikation kann optional via TLS aktiviert werden [51, pp. 538-539]. Weiterhin existieren unterschiedliche Denial of Service Angriffe, welche es ermöglichen den MQTT-Server unter Last zu setzten und zum Absturz zu bringen [50, p. 140, 52, pp. 2-3]. Ein erfolgreicher DoS Angriff kann entsprechend dazu führen, dass die Kommunikation, zwischen der Geräte- und der Anwendungsebene einer IoT-Anwendung gestört wird, da keine Daten mehr über den MQTT-Server ausgetauscht werden können. Die übrigen Protokolle erzwingen eine verschlüsselte und authentifizierte Verbindung nicht, unterstützen hierfür jedoch fortschrittliche Mechanismen wie DTLS, TLS oder SASL [49, p. 5].

Es lässt sich resümieren, dass alle in diesem Abschnitt betrachteten Protokolle der Netzwerkschicht zwar mindesten grundlegende Sicherheitsstandards unterstützen, deren Nutzung jedoch nicht obligatorisch ist. Daher besteht weiterhin die Möglichkeit, dass durch mangelnde Erfahrung der Plattformbetreiber, Fehlkonfiguration oder wirtschaftliche Erwägungen unverschlüsselt kommuniziert wird. Dementsprechend ist es möglich, dass die Netzwerkschicht von einem Angreifer abgehört wird und diese sensiblen Daten abgreifen und manipulieren kann, um ggf. weitere Schwachstellen in den anderen beiden Schichten des IoT-Systems auszunutzen.

3.3 Anwendungsschicht

Ein Teil der Datenverarbeitung von IoT-Systemen findet in der öffentlichen Cloud statt. Weiterhin werden auf der Anwendungsschicht unterschiedliche Dienste in Form von Web- oder Mobileanwendungen bereitgestellt, die es ermöglichen mit dem IoT-System zu interagieren. Daraus lässt sich ableiten, dass grundsätzlich alle Bedrohungen für Cloud-, Web- und Mobileapps auch für die Anwendungsschicht von IoT-Systemen relevant sind [53, p. 39]. In Tabelle 1 sind einige Beispiele für Schwachstellen auf der Anwendungsschicht dargestellt, um die Diversität der Bedrohungslage auf der Anwendungsschicht hervorzuheben. Mishra et al. haben ein umfassendes Modell zur Beschreibung von Schwachstellen von Cloudsystemen entworfen in welchem 32 spezifische Schwachstellen

definiert werden [54]. Auch im Bereich von Webanwendungen lässt sich eine Vielzahl von Schwachstellen identifizieren, so beschreiben Silva et al. [55] in ihrer Taxonomie von Webschwachstellen 21 unterschiedliche Angriffsvektoren

Cloud	***Fehlkonfiguration*** von Clouddiensten ist eine wesentliche Ursache von Sicherheitsvorfällen im Kontext von Cloudanwendungen. Durch mangelndes Verständnis der Administratoren, Änderung von Standardeinstellungen oder auch fehlende Überwachung der Konfiguration kann die Fehlkonfiguration von Clouddiensten dazu führen, dass sensible Daten oder geschützte Dienste wie Datenbanken, öffentlich zugänglich werden [56, p. 6].
	Schwachstellen in der Virtualisierung oder Container Isolation stellen eine erhebliche Bedrohung von Cloudanwendungen dar. Hardwareabstraktion in Gestalt von Virtualisierung oder Containerisierung ist eine Schlüsseltechnologie von Cloudsystemen, da sie es ermöglichen, dass sich unterschiedliche Anwendungen die Hardware des Cloud Service Providers teilen und dennoch voneinander abgeschottet sind. Schwachstellen auf dieser Ebene können dazu führen, dass ein Angreifer diese Isolation umgehen kann und auf fremde Systeme zugreifen kann, die ebenfalls in der Cloud betrieben werden [57, pp. 2-3, 58, pp. 151-152].
	Die ***Bedrohung durch einen böswilligen Insider*** ist auch im Cloudumfeld relevant, da Insider bei unterschiedlichen Parteien ein Sicherheitsrisiko darstellen. Einerseits kann ein Insider beim Cloudanbieter direkt die Sicherheit aller gehosteten Systeme kompromittieren. Aber auch Insider bei IT-Dienstleistern, die Clouddienste bereitstellen und schlussendlich auch Insider im eigenen Unternehmen mit Zugriff auf Cloudmanagement-Portale können für Sicherheit von Cloudanwendungen eine erhebliche Bedrohung darstellen [57, p. 3, 59, p. 295].
Web-anwendungen	***Defekte Zugriffskontrolle*** stellt in Webanwendungen nach Erkenntnissen des OWASP-Projekts die häufigste Schwachstelle dar. Somit können Angreifer die Authentifizierungs- bzw. Autorisierungsmechanismen in einer Anwendung so manipulieren oder umgehen, dass sie auf geschützte Daten zugreifen können, oder Operationen ausführen für die höhere Privilegien benötigt werden [60].
	Code Injektion Schwachstellen ermöglichen es einem Angreifer eigene Befehle in die Webanwendung einzuschleusen und auszuführen. Dadurch können bspw. SQL-Datenbankabfragen so manipuliert werden, dass sensible Daten ausgegeben werden oder eigener JavaScript-Code

	des Angreifers in die Webanwendung eingebettet werden, um Daten aus dem Browser des Anwenders zu stehlen [61].
	Durch ***fehlerhafte Verwendung von Kryptografie*** sind Webanwendungen ebenfalls bedroht. Ein Beispiel für diese Art von Schwachstelle ist die Verwendung von schwachen oder vorhersehbaren, kryptografischen Schlüsseln. Dadurch können Angreifer potenziell verschlüsselte Daten lesen oder manipulieren[62].

Tabelle 1: Beispiele für Schwachstellen in der Anwendungsschicht

In der Anwendungsschicht von IoT-Systemen arbeiten unterschiedliche Konzepte wie Cloudtechnologie und Webanwendungen zusammen. Beide Bereiche sind hinsichtlich deren Schwachstellen und Bedrohungen tiefgehend erforscht. Gerade der Betrieb in der Cloud amplifiziert die Schwachstellen von Webanwendungen, da diese nicht nur global erreichbar und damit Schwachstellen schneller erkannt und ausgenutzt werden können, sondern auch durch zusätzliche Angriffsvektoren wie z.B. Fehlkonfiguration bedroht werden.

3.4 Ganzheitliche Betrachtung

Bereits 2019 veröffentlichten Meneghello et al. eine kritische Analyse bzgl. Schwachstellen in Smart Devices in dem sie das Akronym IoT von „Internet of Things“ in „Internet of Threats“, also als Internet der Bedrohungen umdeuteten [27]. In diesem Kapitel haben wir wesentliche Angriffsflächen von IoT-Lösungen zusammengefasst und in Kapitel 3 dargelegt, dass diese nicht nur theoretisch existieren, sondern auch in der Praxis für erfolgreiche Attacken genutzt werden. Es lässt sich daraus schließen, dass wesentliche Herausforderungen bzgl. Design und Implementierung sicherer IoT-Systeme weiterhin bestehen oder Lösungsansätze in der Breite nicht zum Einsatz kommen. Daher scheinen die Bedrohungen im IoT ebenso zahlreich, wie die Dinge selbst, vorhanden zu sein.

Die zugrunde liegenden Ursachen für Schwachstellen in IoT-Systemen sind bekannt [39, pp. 1625-1626], daher stellt sich die Frage, welche Maßnahmen und Technologien zur ganzheitlichen Verbesserung der Sicherheit von IoT-Systemen, unter Berücksichtigung ökonomischer Faktoren, umgesetzt werden können. In diesem Bereich besteht signifikantes Potenzial für weitere Forschung. Die Kombination einer Vielzahl von unterschiedlichen Komponenten und Technologien im IoT stellt eine wesentliche Herausforderung für die Systemsicherheit dar, da sich potenzielle Schwachstellen und Angriffsvektoren aufsummieren und in Wechselwirkung zueinander deutlich mehr oder schwerwiegendere Angriffsszenarien ermöglichen. Auch die Verwendung von künstlicher Intelligenz bietet nicht nur enorme Chancen, sondern kann ebenso bedrohlich für ein System sein [63].

Über die technischen Schwachstellen hinaus ist es besonders im IoT-Kontext relevant die Endanwender und Administratoren für die mannigfaltigen Bedrohungen zu sensibilisieren und ebenso die Hersteller von IoT-Lösungen zu verpflichten auftretende Schwachstellen zeitnah, auch nach Ende des wirtschaftlichen Lebenszyklus, zu beheben. Eine holistische und

pragmatisch umsetzbare Sicherheitsarchitektur ist insbesondere aufgrund der komplizierten und verteilten Struktur essenziell. Nur wenn alle Architekturebenen gegen Angriffe gehärtet sind, kann das System als Ganzes die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten seiner Nutzer sicherstellen.

4 Sicherheitsmaßnahmen im IoT

In diesem Kapitel wird der Bereich "Internet der Dinge" aus der Perspektive der IT-Sicherheit beleuchtet. Wie bereits im ausführlichen vorherigen Kapitel 2 "Bedrohungen..." beschrieben, birgt auch das **Internet der Dinge** in einem Unternehmen Sicherheitslücken. Gerade durch die zunehmende Vernetzung von Alltagsgegenständen wie Smart-TVs, Heizungsthermostaten, Rollläden und Verbrauchszählern, die immer häufiger in Haushalten anzutreffen sind, erhöht sich die Abhängigkeit von dieser Technologie und damit auch die Anfälligkeit für Cyberangriffe erheblich. Cyberbedrohungen passen sich an diese neue Technologie an und nutzen Schwachstellen und Sicherheitsdesignfehler in IoT-Geräten zu ihrem Vorteil aus. [64]

4.1 Vorbeugemaßnahmen im IoT

Es ist von entscheidender Bedeutung, angemessene IT-Sicherheitsschutzmaßnahmen rund um das Internet der Dinge zu implementieren. Unternehmen sollten daher die folgenden Vorbeugemaßnahmen gemäß der BSI-Checkliste etablieren, um diese Herausforderung zu bewältigen:

- ✓ Software und Sicherheitsupdates müssen immer im Unternehmen aktuell sein
- ✓ Es sollten keine Standardpasswörter verwendet werden
- ✓ Eine zentrale Firewall sollte im Unternehmen integriert und aktiviert werden
- ✓ Um die zentrale Routersicherheit zu gewährleisten, sollte das voreingestellte Passwort geändert werden. Zudem ist es wichtig, verfügbare Updates einzuspielen und auf aktuelle Firmware zu achten.
- ✓ Für die IoT-Geräte ist es wichtig, verschlüsselte Kommunikation zu verwenden, um die Sicherheit zu gewährleisten. Dies kann beispielsweise durch die Verschlüsselung mittels HTTPS oder TLS erfolgen.
- ✓ Um die Sicherheit zu erhöhen, ist es ratsam, die Verbindung von Smart Home-Geräten mit dem Internet nur dann herzustellen, wenn ein Fernzugriff unbedingt erforderlich ist. Ansonsten sollten sich die Geräte auf das eigene Heimnetzwerk beschränken und die lokale Nutzung ermöglichen.
- ✓ Für Unternehmen ist es ratsam, ein separates Netzwerk für IoT-Geräte einzurichten und ein VPN (Virtual Private Network) zu nutzen. Dies ermöglicht eine sichere und verschlüsselte Kommunikation zwischen den IoT-Geräten und anderen Netzwerkressourcen des Unternehmens. Durch die Verwendung eines separaten Netzwerks können potenzielle Angriffe auf IoT-Geräte isoliert werden, um das Risiko einer Kompromittierung des gesamten Unternehmensnetzwerks zu minimieren. Das VPN gewährleistet zudem die sichere Übertragung von Daten und schützt vertrauliche Unternehmensinformationen vor unbefugtem Zugriff.

- ✓ Bei geschäftlichen IoT-Geräten ist es wichtig, die Privatsphäre zu schützen. Vor dem Kauf sollten Unternehmen überprüfen, welche Daten gesammelt und wie sie gespeichert werden. Es ist ratsam, Geräte mit Datenschutz- und Datensicherheitsvorkehrungen zu wählen. Transparenz seitens der Hersteller in Bezug auf die Datensammlung und -verarbeitung ist entscheidend, um die Privatsphäre der Unternehmen zu wahren.
- ✓ Im geschäftlichen Kontext ist die physische Sicherheit von großer Bedeutung. Es ist wichtig sicherzustellen, dass Unbefugte von außen nur schwer oder gar nicht auf die Geräte zugreifen können. Hierzu können Maßnahmen wie der Einsatz von sicherheitsrelevanten Zugangskontrollen, Überwachungssystemen und die Platzierung der Geräte an sicheren Standorten gehören. Durch diese Vorkehrungen wird das Risiko von unbefugtem Zugriff und potenziellen physischen Angriffen auf die IoT-Geräte minimiert, was wiederum die Sicherheit und den Schutz der geschäftlichen Daten gewährleistet.
- ✓ Beim Homeoffice ist es empfehlenswert, ein separates WLAN für IoT-Geräte einzurichten. Dadurch wird eine klare Trennung zwischen den IoT-Geräten und anderen Geräten in Ihrem Netzwerk gewährleistet. Dies erhöht die Sicherheit, da potenzielle Sicherheitslücken bei IoT-Geräten isoliert werden können, ohne das gesamte Netzwerk zu gefährden.
- ✓ Im Arbeitsumfeld sollten Sie besonders auf die Weitergabe und den Schutz persönlicher Daten achten.

Bei vielen der genannten Punkte ist eine Abwägung zwischen Komfort, Funktionalität und Sicherheitsaspekten erforderlich. [64]

4.2 IT-Sicherheit und Datenschutz im IoT

Abseits rein technischer Schutzmaßnahmen ist es weiterhin empfehlenswert auch den Datenschutz auf die Verwendung des Internets der Dinge abzustimmen. Hierbei sind folgende Punkte besonders zu berücksichtigen:

- Verlässliches und transparentes Datenschutzniveau
- Zweckbindung, Datensparsamkeit und Transparenz
- Kultur des Einverständnisses gegenüber Kunden
- Die Weitergabe von personenbezogenen Informationen auf das Nötigste beschränkt werden.
- Beschränkung der Weitergabe von personenbezogenen Informationen auf das Nötigste
- Veröffentlichung verbindlicher Leitlinien für die datenschutzkonforme Umsetzung des Internet of Things
- Transparente Information über etwaige Änderungen dieser Leitlinien und ihrer Umsetzungsanforderungen

- Datenschutzgrundsätze wie Privacy by Design, Anonymisierung, frühzeitige Löschung, Transparenz und Einwilligung
- Zukünftiger Datenschutz in Prozessketten mit klarer Abgrenzung der datenschutzrechtlichen Verantwortung und höchster Transparenz
- Kundendatenschutz mit besonderem Fokus auf Bewegungsprofile, freiwillige Einwilligungen und Löschung von Daten
- Arbeitnehmerdatenschutz, insbesondere im Kontext der Mensch-Maschine-Schnittstelle

Durch die Berücksichtigung dieser Maßnahmen wird ein angemessenes Maß an IT-Sicherheit und Datenschutz im Zusammenhang mit dem Internet der Dinge im Unternehmen gewährleistet. [65]

4.3 Sicherheitsmaßnahmen im IoT mit Cloudanwendungen

Ein wichtiger Bestandteil ist der Einsatz von Cloudanwendungen im Einklang mit der IoT im Unternehmen. Dabei sollte eine sichere Bereitstellung von Geräten und eine sichere Konnektivität zwischen den Geräten und der Cloud gewährleistet werden, um den Schutz der Daten während der Verarbeitung und Speicherung in der Cloud zu gewährleisten. Zudem sollten bei der Sicherheit der Geräte weitere Merkmale berücksichtigt werden, wie die Geräteheterogenität oder Fragmentierung, die Konnektivität mit wertvollen Unternehmenstechnologien und die Herausforderungen bei der Sicherheit älterer Geräte.

Ein wichtiger Aspekt ist auch, die eigenen IoT-Bereitstellungen besser zu schützen. Dazu gehören Maßnahmen wie die Einbindung aller Teams und Infrastrukturen, um einen umfassenden Ansatz von den physischen Geräten und Sensoren bis zu den Daten in der Cloud zu verfolgen. Es ist wichtig, spezielle Vorbereitungen für die Sicherheit von Geräten mit Ressourcenbeschränkungen zu treffen und eine intelligente Sicherheitsanalyse und -korrektur durchzuführen, um den Sicherheitsstatus aller mit der IoT-Lösung verbundenen Komponenten zu überwachen.

Des Weiteren sollte ein Fokus auf den Schutz der Kunden- und Geschäftsdaten gelegt werden, indem alle vernetzten Datenspeicher und sonstigen Dienste mit IoT-Berührungspunkten nachverfolgt werden, um sicherzustellen, dass die IoT-Apps ebenfalls geschützt sind und die implementierten IoT-Sicherheitsmaßnahmen wirksam sind. [66]

Ein weiterer sinnvoller Ansatz besteht darin, die Logdateien von IoT-Geräten wie Heimgeräten, Heizungssteuerungen oder Zutrittsberechtigungen sicher in der Cloud zu speichern. Dies ermöglicht es eine zentrale Überwachung und Analyse der Daten, um potenzielle Angriffe frühzeitig zu erkennen. Durch den Einsatz einer Ende-zu-Ende-Verschlüsselung können die Daten in der Cloud umfassend geschützt werden. Die Umsetzung dieser Sicherheitsmaßnahmen im Zusammenhang mit IoT und Cloud-Benutzung trägt wesentlich zur Steigerung der Informationssicherheit bei und schließt Sicherheitslücken effektiv. [67]

Speziell beim Einsatz von Cloud Computing in der Industrie 4.0 stellt die sichere Übertragung von Daten und Steuerbefehlen zwischen dem Cloud-Service und den einzelnen Maschinen einen wichtigen Sicherheitsaspekt dar. Es ist erforderlich, dass diese Übertragung über einen sicheren Kanal erfolgt. Darüber hinaus sollten die Speicherung, Nutzung, Verarbeitung und Weitergabe der Daten in der Cloud abgesichert werden, wie in Abbildung 11 dargestellt. [68]

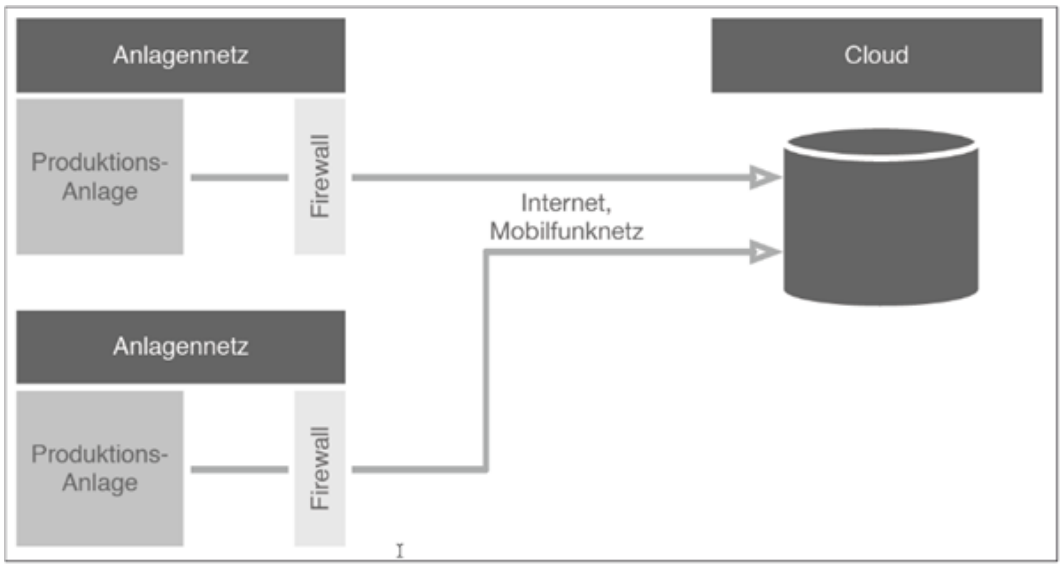

Abbildung 11 Die Cloud als zentraler Datenspeicher für Daten aus den Produktionsanlagen [68]

Zusätzlich könnte die Informationssicherheit durch den Einsatz einer Datenplattform für I4.0-Anwendungen in Verbindung mit der Cloud (siehe Abbildung 12) gesteigert werden.

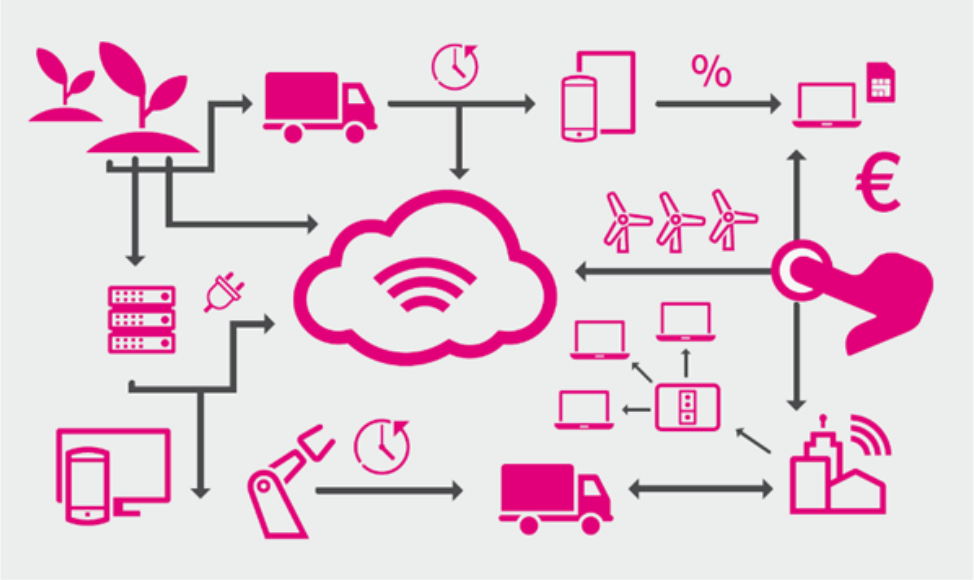

Abbildung 12 Datenplattformen für Industrie 4.0-Anwendungen - Die Rolle des Cloud Computing im IoT [69]

Diese Plattformen sind besonders geeignet, um die großen Mengen an neuen Massendaten, die durch die Vernetzung von Geräten, Gegenständen und (Produktions-)Prozessen über das Internet auf Systeme, Server und Speicher gelangen, zu speichern und zu verarbeiten. Die hohe Skalierbarkeit ermöglicht eine flexible Nutzung von Rechenkapazitäten, die sich theoretisch unbegrenzt ausdehnen lassen und die Verarbeitungsfähigkeiten von internen Serversystemen in der Regel deutlich übersteigen.

Durch den Einsatz des Verschlüsselungsprotokolls Transport Layer Security (TLS) kann eine sichere Grundlage für alle Transportwege von und zur Cloud-Plattform geschaffen werden. Für sämtliche Geräte im IoT sollte grundsätzlich die Ende-zu-Ende-Verschlüsselung (E2E) eingesetzt werden. Es ist auch wichtig, dass Cloud-Dienstleister sichere und standardisierte Interaktionsmöglichkeiten zwischen verschiedenen Clouds schaffen, um die Kommunikationsfähigkeit zwischen den zahlreichen unterschiedlichen Regelkreisen und (Teil-)Prozessen im IoT sicherzustellen.

Es ist jedoch wichtig anzumerken, dass trotz des Einsatzes von Cloud-Lösungen die Verantwortung für die physische Sicherheit von Maschinen und Geräten weiterhin bei den Unternehmen liegt, da sowohl Maschinen als auch Netzwerkübergänge potenzielle Angriffsziele darstellen. [69]

4.4 Sicherheitslösungen bei der Nachhaltigkeit bei IoT Geräte

Auch im Hinblick auf ökologische Nachhaltigkeit gibt es Lösungsansätze zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT-Geräten. Diese Ansätze können in vier Bereiche unterteilt werden:

Regulierung und Transparenz

- Update-Pflicht für Hersteller/innen: Hersteller von IoT-Geräten sollten verpflichtet werden, regelmäßige Updates bereitzustellen.
- Konkretisierung des Bereitstellungszeitraums von Updates: Hersteller müssen angeben, wie lange sie Updates für ihre Geräte bereitstellen werden.
- Trennung der verschiedenen Update-Arten: Es ist wichtig, die verschiedenen Arten von Updates (funktionserhaltend, funktionsändernd, Sicherheit, Content) klar voneinander zu trennen und separat bereitzustellen. Jedes Update sollte klare Informationen darüber enthalten, welche Veränderungen am Produkt vorgenommen werden und insbesondere, ob es sich um ein Sicherheitsupdate handelt. Dadurch erhalten die Benutzer eine bessere Übersicht und können die Updates entsprechend ihrer Bedürfnisse und Prioritäten durchführen.
- Möglichkeit zum Betrieb der Geräte ohne externe Abhängigkeiten: IoT-Geräte sollten auch offline und ohne externe Dienste funktionieren können.
- Aufrechterhaltung von Cloud-Diensten für eine Mindestnutzungsdauer: Cloud-Dienste, die Teil des IoT-Ökosystems sind, sollten für eine angemessene Zeitdauer aufrechterhalten werden.
- Gütesiegel für Cyber-Sicherheit bei IoT-Geräten: Ein verpflichtendes Gütesiegel soll die Sicherheit von IoT-Geräten für Verbraucher/innen erkennbar machen.
- Regulierung von Security-by-Design-Ansätzen: Die Anwendung von Security-by-Design-Prinzipien bei der Entwicklung von IoT-Geräten sollte gesetzlich vorgeschrieben werden.
- Stärkung der Anwendung und Durchsetzung bestehender gesetzlicher Regelungen: Bestehende gesetzliche Normen zur IT-Sicherheit sollen besser umgesetzt werden, anstatt neue Regelungen einzuführen.

Diese Vorschläge zielen darauf ab, die Regulierung und Transparenz im Zusammenhang mit IoT-Geräten zu verbessern, um die Sicherheit und den Schutz der Hersteller/innen zu gewährleisten.

Sensibilisierung der Verbraucher

- Anstupsen der Verbraucher/innen mit Warnhinweisen: Durch Warnhinweise auf Geräten oder über verbundene Apps können Verbraucher/innen auf Sicherheitsmaßnahmen, wie regelmäßige Updates, aufmerksam gemacht werden.
- Öffentlichkeitskampagne zur Erhöhung des Bewusstseins für Sicherheitsrisiken bei IoT-Geräten: Durch eine Kampagne wird das Verständnis der Verbraucher/innen für

die Sicherheitsrisiken bei der Nutzung von IoT-Geräten verbessert und die Berücksichtigung von Sicherheitsaspekten bei der Kaufentscheidung gefördert.
- Digitale Bildung für Verbraucher/innen zur sicheren Nutzung von IoT-Geräten: Durch digitale Bildungsangebote werden das Verständnis und Bewusstsein der Verbraucher/innen für die Cyber-Sicherheit von IoT-Geräten gestärkt.

Sensibilisierung der Hersteller

- Know-how in die Unternehmen bringen: KMU fehlt oft das Wissen in Bezug auf IT-Sicherheit. Ein allgemeines Lastenheft mit vorgegebenen Sicherheitsanforderungen könnte dazu beitragen, dass eingekaufte Lösungen hinsichtlich Sicherheit überprüft und erforderliche Vorkehrungen getroffen werden.
- Hervorhebung der Sicherheit als Wettbewerbsvorteil: Durch Transparenz und Information können Verbraucher/innen den Druck auf Hersteller/innen erhöhen, sichere Geräte zu entwickeln.
- Wertediskussion zu Corporate Digital Responsibility (CDR): Eine Diskussion über die Verantwortung von Unternehmen in der digitalen Gesellschaft kann positive Auswirkungen auf die IT-Sicherheit von IoT-Geräten haben.
- Strategische Klageführung (Strategic Litigation): Klagen gegen Hersteller/innen, die Sicherheitsanforderungen nicht erfüllen, können zur Durchsetzung von gesetzlichen Bestimmungen beitragen.

Technische Lösungsansätze

- Automatisierung von Sicherheitsupdates: Forschung betreiben, um effektive Updateprozeduren für displaylose Consumer-IoT-Geräte zu entwickeln.
- Förderung der Forschung zur sicheren Entwicklungsmethoden und praktisch nutzbaren IT-Sicherheitstechnologien: Bereitstellung von Security-Frameworks, Konzepten und Tools, um Unternehmen bei der Umsetzung von IT-Sicherheitskonzepten zu unterstützen. Förderung der Entwicklung von IT-Sicherheitstechnologien.
- Einrichtung einer öffentlichen Stelle zur Behebung von Sicherheitslücken bei IoT-Geräten: Eine öffentliche Stelle, wie z. B. beim BSI angesiedelt, könnte die Verwaltung von Sicherheitslücken übernehmen und Sicherheitsupdates für Verbraucher bereitstellen.
- Durch die Förderung und Finanzierung von Open-Source-Projekten im IoT wird eine nachhaltige Entwicklung unterstützt, indem Ressourcen und Wissen geteilt werden, um ressourcenschonende Technologien voranzutreiben. [70]

Die Gewährleistung von Cybersicherheit bei IoT-Geräten und die Verlängerung ihrer sicheren Nutzungsdauer sind jedoch eine gemeinsame Aufgabe der gesamten Gesellschaft. Hierbei sollten insbesondere Politik und Industrie, aber auch die Verbraucher eng zusammenarbeiten und einbezogen werden. Durch eine gezielte Regulierung, transparente Informationen, bewusste Verbraucherentscheidungen und technologische Innovationen

können dazu beitragen, die Nachhaltigkeit von Consumer-IoT-Geräten zu verbessern und ihre Lebensdauer zu verlängern. [71]

Aufgrund dieser Risiken, Bedrohungen und IT-Sicherheitslücken im Zusammenhang mit der Industrie 4.0 bedarf es wirkungsvoller Gegenmaßnahmen. Diese umfassen unter anderem die Abschottung von Systemen, die Einschränkung von Zugangsberechtigungen, den Einsatz von Verschlüsselungsverfahren sowie die Schaffung eines Sicherheitsbewusstseins unter den Mitarbeitern. [69]

4.5 Zentrale Sicherheitsschutzmaßnahmen mit IoT

Schließlich sollten im Rahmen der Sicherheitsschutzmaßnahmen die folgenden zentralen Maßnahmen implementiert werden, um eine umfassende Sicherheit im Zusammenhang mit dem Internet der Dinge zu gewährleisten. Diese Maßnahmen dienen dazu, mögliche Risiken zu minimieren und ein hohes Maß an Schutz zu bieten: [72]

Maßnahmen	**Beschreibung**
Die Inbetriebnahme in sicherer Konfiguration	Verzicht auf unnötige Produktfunktionen, Aktivierung von Sicherheitsmechanismen, Langfristige Gewährleistung der IT-Sicherheit, Aktualisierung auf den neuesten Patchstand, Unterstützung von Virenschutz-Lösungen
Die Fernwartung durch Hersteller/ Integrator	Es sollten technische Authentisierungsmaßnahmen implementiert werden, um eine sichere Fernwartung zu gewährleisten. Zudem ist es wichtig, geeignete kryptographische Algorithmen einzusetzen.
Absicherung von Feld-geräten u. Netze	Absicherung von Feldgeräten und Netze umfasst Maßnahmen zur Sicherheit und Integrität von Geräten und Daten. Dazu gehören Zugriffsschutz, Verschlüsselung, Firewalls und Updates zur Bekämpfung von Bedrohungen.
Datensicherung	Bei der Datensicherung sind folgende Aspekte zu beachten: Das Zeitintervall legt fest, ob die Sicherung täglich, wöchentlich oder monatlich durchgeführt wird. Auch der Zeitpunkt ist entscheidend, ob die Sicherung beispielsweise nachts oder sonntags erfolgt. Des Weiteren ist der Umfang der zu sichernden Daten ebenfalls relevant. Es kann entschieden werden, ob vollständige Sicherungen oder inkrementelle Sicherungen durchgeführt werden sollen. Auch die Anzahl der aufzubewahrenden Generationen ist bedeutsam. Diese kann je nach Art der Sicherung variieren. Zum Beispiel könnten Tagessicherungen nach sieben Tagen

	gelöscht werden, während Wochensicherungen über mehrere Monate aufbewahrt werden. Das Speichermedium ist für die Datensicherung relevant. Dabei muss entsprechend der Datenmenge ausgewählt werden. Hierbei können DVDs, Bänder oder Festplatten zum Einsatz kommen. Um die Integrität zu gewährleisten, sollten zusätzlich zu den eigentlichen Daten Metadaten gesichert werden. Diese Metadaten ermöglichen die Feststellung von Veränderungen an den Stammdaten. Die Zuständigkeit für die Durchführung und Überwachung der Sicherung sollte ebenfalls festgelegt werden. Durch die Berücksichtigung dieser Aspekte wird eine effektive und zuverlässige Datensicherung ermöglicht.

Tabelle 2 Sicherheitsschutzmaßnahmen Internet der Dinge I

Maßnahmen	**Beschreibung**
Schutz vor Schadsoftware (Malware)	Es ist wichtig, Virenschutzprogramme zu installieren, sicher zu konfigurieren und regelmäßig zu aktualisieren. Dies beinhaltet die Installation von Virenschutz-programmen auf Firewalls sowie die zeitnahe Aktualisierung der Viren-Signaturen. Durch diese Maßnahmen wird eine effektive Abwehr von Viren und schädlicher Software gewährleistet, um die Sicherheit des Systems zu gewährleisten.
Härtung der IT-Systeme	Vermeidung von Standard-Benutzerkonten und -Passwörter und stattdessen individuelle Benutzerkonten einzurichten. Darüber hinaus sollten unnötige Software und Dienste entfernt werden, um potenzielle Angriffsflächen zu reduzieren. Es ist wichtig, die Standard-Einstellungen und die Hardware-Konfiguration anzupassen, um die Sicherheit zu erhöhen und spezifische Anforderungen zu erfüllen. Durch diese Maßnahmen wird das Risiko von unbefugtem Zugriff und unerwünschten Aktivitäten minimiert.
Patchmanagement	Das Konfigurationsmanagement umfasst die Erfassung und Verwaltung aller Komponenten im Betrieb. Der Patchmanagement-Plan ermöglicht die Auswahl, Verteilung und Installation von Software-

	Aktualisierungen. Die Patch-Verifikation gewährleistet die Kompatibilität der Patches. Im Ernstfall ermöglicht die Software-Wiederherstellung eine schnelle Systemwiederherstellung. So werden Integrität, Sicherheit und Stabilität der IT-Systeme gewährleistet.
Authentisierung, Zugriffs-kontrolle, Protokollierung/ Auswertung	Technische Authentisierung, Passwortverwaltung, Zutrittskontrolle, Missbrauchsvermeidung und kryptographische Algorithmen sind wichtige Aspekte der IT-Sicherheit. Sie gewährleisten eine sichere Identifizierung, Passwortsicherheit, Zugangskontrolle und Datenverschlüsselung. Zusammen schützen sie die Systeme vor unbefugtem Zugriff und gewährleisten die Sicherheit sensibler Informationen.
Logging / Monitoring	Logging und Monitoring überwachen Systemaktivitäten, um Sicherheitsvorfälle zu erkennen und unautorisierten Zugriff zu verhindern. Dabei ermöglichen protokollierte Informationen eine detaillierte Analyse und frühzeitige Maßnahmen bei Bedrohungen.
Mobile Datenträger	Beim Umgang mit mobilen Datenträgern sollten technische Maßnahmen ergriffen werden, um die Nutzung einzuschränken. Dazu gehören Funktionen des Betriebssystems oder zusätzliche Software wie Device Control - Port Control und Device Management. Eine Wechseldatenträgerschleuse (Quarantäne-PC) ist empfehlenswert. Für spezielle Anforderungen wie Wartungsnotebooks oder BIOS-Härtung können Sonderregelungen angewendet werden, z.B. sichere Konfiguration, Deaktivierung unnötiger Funktionen und Aktivierung von Passwörtern. Die Deaktivierung der Autorun-Funktion auf allen Systemen ist wichtig, um die Verbreitung von Schadprogrammen über mobile Datenträger zu verhindern.

Tabelle 3 Sicherheitsschutzmaßnahmen Internet der Dinge II

Zudem können im Bereich Industrie 4.0 des Internet of Things (IoT) bei der Umsetzung von Schutzmaßnahmen im Unternehmen folgende Perspektiven berücksichtigt werden:

- R**echtliche Sicht**: sollten folgende Maßnahmen zur IT-Sicherheit umgesetzt werden: einheitliche rechtliche Pflichten zur IT-Sicherheit und prüffähige Standards, Gewährleistung von Rechtsicherheit durch datenschutzrechtliche Rechtsgrundlagen für Datenströme bei Industrie 4.0, Verwendung von Musterklauseln und Mustereinwilligungen für Industrie 4.0 hinsichtlich Haftung sowie Datenschutz und Schutz von Betriebs- und Geschäftsgeheimnissen, sowie die Schaffung eines rechtlichen Rahmens für IT-Sicherheits-Zertifizierung.
- Bezogen auf **betriebliche/organisatorische Sicht** sollten folgende Maßnahmen umgesetzt werden: Konzeption geeigneter Aus- und Weiterbildungsangebote, Hinterfragen etablierter Strukturen und Prozesse im Rahmen des Risikomanagements, Umsetzung bewährter organisatorischer IT-Sicherheitsmaßnahmen, Übernahme der Verantwortlichkeit für die Büro-IT und Produktions-IT mit automatisierten Prozessen durch das zentrale Sicherheitsmanagement, sowie Auf- bzw. Ausbau von Fähigkeiten zur Prävention, Detektion und Reaktion in Unternehmen, um Cyberangriffe von Hackern auf externe Schnittstellen, Übergabe- und Zugangspunkte erfolgreich zu verhindern.
- Bezogen auf **technische Sicht** sollten folgende Maßnahmen umgesetzt werden: Verschlüsselung sensibler Daten in Verbindung mit der zweifelsfreien Authentisierung von "Mensch" und "Maschine", Durchführung von Integritätsprüfungen, Entwicklung einer integrierten Methodik für Safety & Security, Verwendung hardwarebasierter Sicherheitsanker, Verarbeitung anfallender Massendaten von intelligenten Sensoren mittels Datenanalyseprogrammen (Data Mining), Umsetzung von Speicher- und Sicherheitsanforderungen durch den Einsatz von Datenplattformen wie der Cloud der Dinge, die auch die Steuerung von Maschinen und automatisierten Prozessen übernehmen.

Bezogen auf **standardisierte Sicht** sollten folgende Maßnahmen umgesetzt werden: Erarbeitung einer Struktur für IT-Sicherheitsstandards, Engineering von sicheren IT-Systemen, Integration technischer Standards mit ISMS-Standards (Information Security Management System), Erarbeitung integrierter Standards für Safety & Security, die sowohl die IT-Sicherheit (Security) als auch die Betriebssicherheit (Safety) umfassen und regelmäßig überprüft und aktualisiert werden. [72]

5 Praxisbeispiel IoT–Sicherheit im Bereich Smart Home

In den vorangegangenen Kapiteln wurde ein grundlegendes Verständnis für die Sicherheit im IoT geschaffen. Es wurden konkrete Sicherheitsvorfälle im IoT Umfeld vorgestellt, maßgebliche Bedrohungen analysiert und entsprechend geeignete Sicherheitsmaßnahmen erarbeitet.

Zur Vertiefung und Übermittlung dieser Erkenntnisse wird nun an dem konkreten IoT-Beispiel Smart Home gezeigt, wie Anbieter und Konsumenten Sicherheitsvorkehrungen treffen können, um die genannten Bedrohungen und Angriffe zu vermeiden. Ziel des Kapitels ist es, die vorherigen abstrakten Themen an einem Fallbeispiel zu konkretisieren und zu veranschaulichen. Im Sinne dieser Kapitelzielsetzung sollen einzelne Lösungsmöglichkeiten plastisch veranschaulicht werden. Eine vollständige Darstellung der zuvor aufgeführten Möglichkeiten (vgl. Kapitel 4) ist an dieser Stelle aufgrund des Arbeitsumfangs und der Vielzahl an Lösungen, an dieser Stelle nicht möglich.

Zunächst wird nun der Bereich des Smart-Home näher erläutert um anschließend die dortigen Schutzmöglichen entlang der IoT-Schichten für die Akteure „Anbieter“ und „Nutzer“ aufzuzeigen.

5.1 IoT - Smart Home

Das Internet der Dinge ist in vielen Branchen vertreten. Die bekanntesten IoT-Einsatzbereiche wurden bereits in Absatz 1.1 aufgeführt. Für die plastische Veranschaulichung von IoT und dessen Sicherheitsthematik wird aus dieser Auflistung der Bereich Smart Home gewählt. Hintergrund für diese Auswahl ist die Annahme, dass das vorhandene Umfeld „Zuhause“ (= engl. Home), das durch die Einbindung in das IoT zum sog. Smart Home wird, für die Lesenden dieser Arbeit aufgrund eigener Erfahrungen leicht zugänglich ist. Das Zuhause im Allgemeinen ist laut Duden -Begriffsdefinition eine „Wohnung, in der jemand zu Hause ist [und sich wohlfühlt]“ [73]. Dieses Zuhause kann durch die Integration von IoT-Elementen zu einem Smart Home werden. Genauer beschrieben ist ein Smart Home (deutsch: intelligentes Zuhause) eine Wohnstätte, in die ein Kommunikationsnetzwerk integriert ist, das die elektrischen Geräte und deren Dienstleistungen so miteinander verbindet, dass es möglich ist diese fernzusteuern, zu überwachen oder auf sie zuzugreifen [74]. Eine Fernsteuerung kann sowohl innerhalb als auch von außerhalb der Wohnstätte erfolgen. Ein Smart Home verfügt über die drei Elemente ein internes Netzwerk, eine intelligente Steuerung und eine Hausautomatisierung verfügen [74]. Sie verkörpern das dreischichtige IoT-Architekturmodell aus Abbildung 2 in der Realität des Smart Homes. Abbildung 13 verdeutlicht die Zuordnung der Smart Home – Elemente zu den drei strukturellen IoT-Schichten: Die IoT-Geräteschicht bildet die Hausautomatisierung, das interne Netzwerk stellt die Netzwerkschicht dar und die intelligente Steuerung verkörpert die Anwendungsschicht.

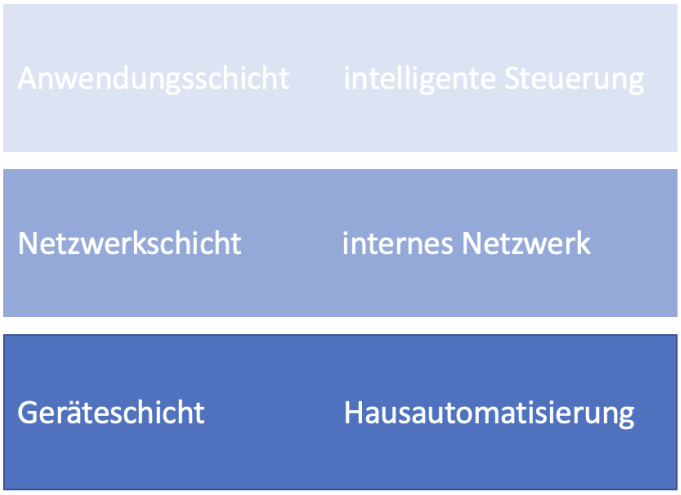

Abbildung 13 eigene Skizze: Smart Home und IoT-Dreischichten-Modell

Die Vielfalt an Smart Home - Geräten ist breit gefächert. Sie reicht von intelligenten Türschlössern über Staubsauerrobotern bis hin zu intelligenten Klimageräten. Die folgende Abbildung 14 aus [75] vermittelt einen ersten Eindruck über die Arten und die Einsatzbereiche von Smart Home- Produkten. Die Smart Home Lösungen reichen von Sicherheitssystemen über Küchengeräte und Energieregulatoren bis hin zu Haushaltgeräten, die alle über ein Netzwerk miteinander verbunden sind.

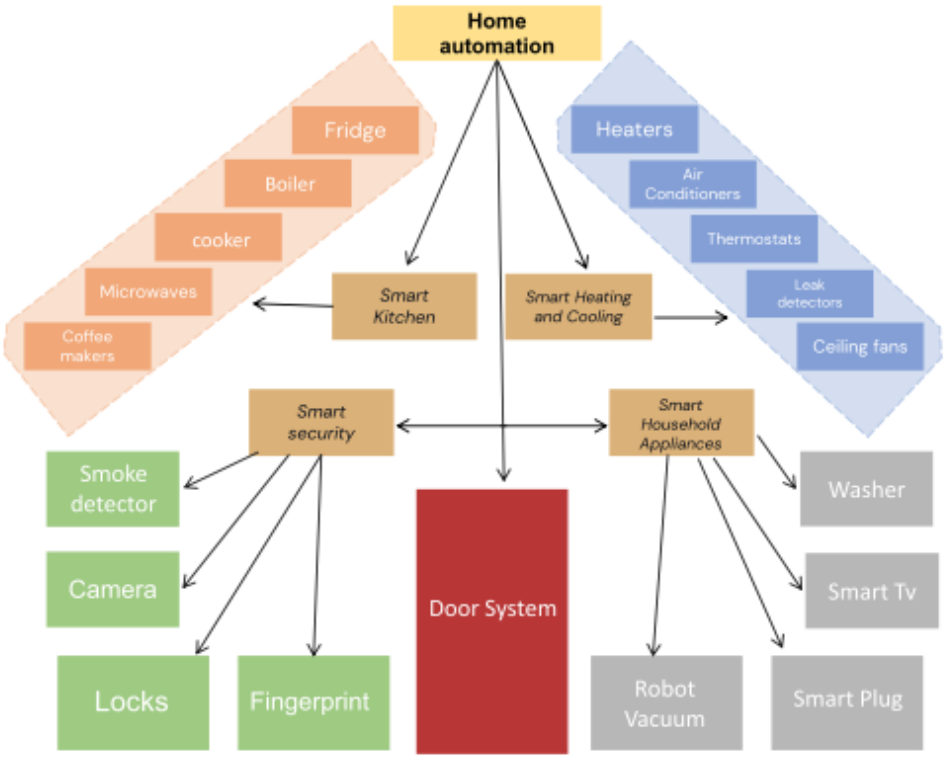

Abbildung 14 Smart Home Geräte und Bereiche aus [75]

Innerhalb eines „Smart Homes“ kommunizieren die Geräte über ein Netzwerk miteinander und können über eine zentrale mobile Nutzer-Anwendung gesteuert werden. Diese wird in der Regel auf Smartphones, Tablets oder Computern bedient und ist der zentrale Berührungspunkt eines Users mit seinem eigenen Smart Home. [75]

Verwender von Smart Home Produkten möchten sich und ihre Privatsphäre schützen [75]. Das allgemein vorhandene Sicherheitsbewusstsein für das eigene Zuhause äußert sich beispielsweise schon durch das Verschließen der eigenen Eingangstüre, um das Zuhause vor dem Eindringen fremder Personen zu schützen. Einen solchen Schutz vor dem Eindringen Fremder Personen in die Privatsphäre müssen auch Smart Home Systeme gewährleisten.

Abstrahiert man das Beispiel der verschlossenen Haustüre in den Smart Home-Bereich, ist es die Aufgabe der Anbieter das Produkt – im Beispiel die Türe – mit Sicherheitsmechanismen (Türschloss und dazugehöriger Schlüssel) auszustatten. Der Nutzer wiederum ist dafür verantwortlich die Sicherheitsmechanismen zu verwenden, um sich und seine Privatsphäre zu schützen. In der Analogie der Haustüre bleibend gilt, dass der Bewohner des Zuhauses nur dann von der möglichen Schutzwirkung der Türe profitiert, wenn er die vorhandenen Möglichkeiten nutzt, die Türe schließt und mithilfe des Schlüssels versperrt. Die folgende Abbildung 15 skizziert diese beschriebene Verantwortlichkeit von „**Produktanbieter-Verantwortung**“ und „**Produktnutzer-Verantwortung**“ anhand des verwendeten Beispiels „Haustüre“ noch einmal grafisch. Dort wird anhand der skizzierten Türe deutlich, dass der Produktanbieter das Sicherheitsprodukt zur Verfügung stellt. Der Verwender trägt jedoch die Verantwortung dafür, die vorhandenen Sicherheitsmöglichkeiten zu nutzen und den Schutz zu aktivieren.

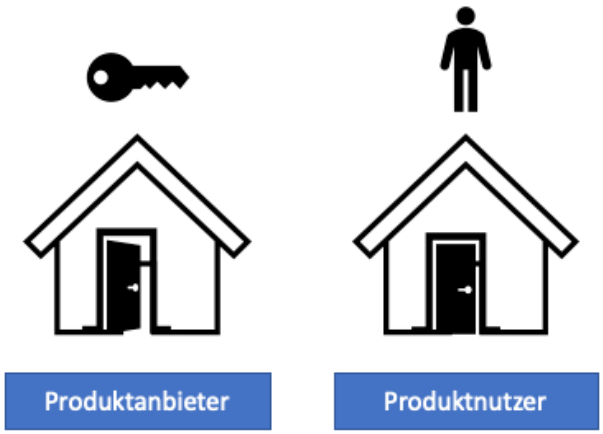

Abbildung 15 eigene Skizze: Beispiel der rollenabhängigen Verantwortungsbereiche für Sicherheit am Beispiel „Haustüre“

Wie im erarbeiteten Beispiel verdeutlicht, sind Verantwortlichkeiten für Schutzvorkehrungen rollenabhängig. Aus diesem Grund wird nun aufgezeigt, welche Sicherheitsvorkehrungen (vgl. Kapitel 4) die Akteure Smart Home- Produkt-Anbieter und -Nutzer treffen können, um den maßgeblichen Bedrohungen des IoT (vgl. Kapitel 2 und 3) entgegenzuwirken.

5.2 Sicherheitsvorkehrungen im IoT-Bereich Smart Home

Die Sicherheitsvorkehrungen im IoT-Bereich Smart Home werden nun entlang der drei strukturellen IoT-Schichten (vgl. Abbildung 2 und Abbildung 13) plastisch dargestellt. Zudem werden sie unterteilt, nach Vorkehrungen, die durch den

- Produktanbieter
- Produktnutzer

vorzunehmen sind. Diese Zuordnung von möglichen Maßnahmen zu den Akteuren dient dazu, die Verantwortlichkeiten für Sicherheitsmaßnahmen anhand der jeweiligen Möglichkeiten klar zu benennen um Angriffe wie in Kapitel 2 aufgeführt, erfolgreich abwehren zu können (vgl. Abbildung 15).

5.2.1 Geräteschicht – Hausautomatisierung

Im Bereich des Smart Homes bilden alle physischen Objekte die Geräteschicht. Viele Beispiele dafür sind in Abbildung 14 aufgeführt und auch in Absatz 1.4 wurde bereits ein Geräte-Beispiel „Jalousien“ genannt. Bereits auf und an Smart Home Geräten können die Akteure die Sicherheitsvorkehrungen treffen, die nun näher erläutert werden.

5.2.1.1 Schutzvorkehrungen Smart Home Anbieter - Geräteschicht

Smart Home -Produktanbieter können sog. EDGEAI -Technik in ihre Geräte integrieren und so die Leistung und Sicherheit des Systems erhöhen. Der Begriff EDGEAI ist eine Zusammensetzung aus den Begriffen EDGE und AI. EDGE-Computing beschreibt eine dezentrale Datenverarbeitungsstruktur, bei der die Berechnungen nicht in der Cloud, sondern nahe an der Datenquelle, z.B. direkt auf dem Endgerät, erfolgen. „AI“ steht für Artificial Intelligence (= deutsch: künstliche Intelligenz). EDGEAI ermöglicht es, dass die Berechnungen und Erkenntnisse der jeweils verwendeten künstlichen Intelligenz direkt auf dem Gerät durchgeführt werden können, ohne dass eine Internetverbindung zwingend benötigt wird.[76] Beispielsweise ermöglicht die EDGEAI -Technik in einer Sicherheitskamera, dass Bewohner und Besucher automatisch und in Echtzeit anhand von Gesichtserkennung oder mithilfe der Analyse von Bewegungsmustern identifiziert und kategorisiert werden. Sobald nicht kategorisierte Personen sich Zutritt zum überwachten Objekt verschaffen, können Sicherheitskameras mit EDGEAI -Technik dies in Echtzeit erkennen und kommunizieren. Beispielsweise identifiziert das sog. CNN-Modell (=Convolutional Neural Network-Model) Personen anhand ihrer Bewegungsmuster mit einer Genauigkeit von über 99,8% [75]. Eine Bewegungsanalyse kann Bewegungsobjekte auch dann analysieren und identifizieren, wenn keine Gesichter zu erkennen sind.

Die Vorteile von EDGEAI-Technik liegen gegenüber einer Komplett-Berechnung der AI-Erkenntnisse in der Cloud-Umgebung in der hohen Datenverarbeitungsgeschwindigkeit (Latenz), einer geringeren Bandbreitenanforderung (da nur die Ergebnisse kommuniziert werden), einer hohen Skalierbarkeit und einem geringeren Energieverbrauch.[75]

Dass die Verarbeitung und die Speicherung sensibler Daten, wie die Kamerabilder des eigenen Zuhauses oder Biometrische Erkennungsmerkmale, direkt und dezentral auf dem Gerät des Users und nicht in der Cloud stattfindet, erhöht das Vertrauen der Nutzenden in die Datensicherheit [77]. Dadurch, dass die Entscheidungsfindung der jeweiligen AI direkt auf dem Gerät stattfinden kann, ist es ausreichend, wenn nur das Ergebnis (bspw. eine Warnmeldung) über das Internet kommuniziert werden. So wird nicht nur der Datenfluss reduziert, auch die Sensibilität der Daten, die bei einem möglichen „Man-in-the-Middle Angriff" (vgl. Absatz 3.1.2) in der Kommunikation abgegriffen werden können, ist deutlich geringer, als wenn alle Basis-Daten (z.B. Videos, biometrische Informationen) kommuniziert werden würden.

Vor weiteren Geräteschicht-betreffenden Angriffen, wie der sog. Malware Injection (vgl. Absatz 3.1.4) können Hersteller ihre Produkte schützen, indem sie die Produktsoftware kontinuierlich mit Blick auf die neuesten Sicherheitserkenntnisse aktualisieren (vgl. Absatz 4.4).

5.2.1.2 Schutzvorkehrungen Smart Home Nutzer - Geräteschicht

Besitzer von Smart Home Produkten, können ihre Geräte vor allem vor physischem Schaden und körperlichen Zugriff durch Fremde schützen, indem sie bei der Montage auf eine erschwerte Zugänglichkeit des Produktes achten. Sie können Sicherheitskameras bspw. so anbringen, dass sie nicht einfach erreicht und demontiert werden können. Auch können sie diese so installieren, dass sie nicht sofort einsehbar sind. Weiterhin sollten sie die Zugangsdaten zu ihren Geräten oder ihrem WLAN-Netzwerk physisch so aufbewahren, dass sie für Gäste nicht direkt ersichtlich sind (vgl. Absatz 4.1).

5.2.2 Netzwerkschicht – internes Netzwerk

Die Netzwerkschicht stellt die Verbindende Schicht zwischen den physischen IoT-Produkten und einem dazugehörigen Cloud-Service dar. Im Bereich Smart-Home können folgende Sicherheitsaspekte vor Angriffen auf der Netzwerkebene schützen:

5.2.2.1 Schutzvorkehrungen Smart Home Anbieter - Netzwerkschicht

Anbieter können sicherstellen, dass sie für die Kommunikation zwischen Client und Server sichere Übertragungsprotokolle wie TLS, DTLS, SSASL (vgl. Absatz 3.2) oder https (vgl. Absatz 4.1) nutzen [75]. Für die Kommunikation von Geräten innerhalb des jeweiligen Netzwerks, sollte weiterhin sichergestellt sein, dass die Firmware aller Smart Home-Produkte das WPA3-Sicherheitsprotokoll verwendet[75]. WPA3 nutzt den sog. Simultaneous Authentification of Equals-Algorithmus (kurz SAE) und basiert auf dem sog. Password Authenticated Key Exchange (kurz PAKE). Dabei installieren alle Teilnehmer einen kryptografischen Schlüssel, der auf der Grundlage der Kenntnis eines gemeinsamen Passworts basiert. Es sind keine Zertifikate oder eine zentrale Autorität notwendig. Das reduziert das Risiko von Passwort-basierten Offline-Wörterbuch-Angriffen [78] wie dem Mirai Botnet-Angriff (vgl. Absatz 2.2).

5.2.2.2 Schutzvorkehrungen Smart Home Nutzer - Netzwerkschicht

Das Beispiel des Mirai Botnet Angriffs 2016 (vgl. Absatz 2.2) zeigte eindrücklich, wie Angreifer Netzwerke infiltrieren können, indem sie die Standard-Login-Daten und Geräte-Namen nutzen. Smart-Home-Nutzende können, dem auf der Netzwerkebene beispielsweise entgegenwirken, indem sie für ihren Router einen neuen Namen vergeben, der nicht mehr dem Namen oder dem Modell des Herstellers entspricht oder ähnelt. Außerdem sollte ein Name verwendet werden, der keine persönlichen Informationen wie bspw. die Adresse oder den Familiennamen enthält. Suchen Angreifer nach Hersteller Router-Namen, so ist sichergestellt, dass der eigene Router nicht in deren Suchergebnis fällt. [75]

Bei der Router-Auswahl sollte darauf geachtet werden, dass auch dieser das WPA3-Sicherheitsprotokoll (vgl. Absatz 5.2.2.1) verwendet, damit die vorher beschriebene WPA3-Kommunikation der Smart-Home-Produkte auch genutzt werden kann.

Zudem sollte für die IoT-Geräte ein eigenes Netzwerk angelegt werden, das von dem Netzwerk getrennt ist, in dem bspw. die genutzten Rechner oder Smartphones verwaltet werden. Diese Netzwerktrennung bewirkt, dass bei einem möglichen Hacking des einen Netzwerkes, die Geräte und Informationen des anderen Netzwerkes weiterhin geschützt bleiben. [75]

5.2.3 Anwendungsschicht – intelligente Steuerung

Die Anwendungsschicht im Smart Home Bereich besteht aus allen digitalen Oberflächen, die dem Nutzer im Zusammenhang mit seinen Smart Home Produkten zur Verfügung stehen. Das sind beispielsweise die Bedienungsoberflächen zu den Gerätefunktionen, Einstellungsbereiche, Login-Oberflächen und Update-Mitteilungen. Sie können wie folgt geschützt werden.

5.2.3.1 Schutzvorkehrungen Smart Home Anbietende - Anwendungsschicht

Smart Home Anbietende designen und entwickeln nicht nur die Produkte und deren Funktionen, sondern auch die dazugehörigen Bedienungsoberflächen. Dabei sollten sie mit Blick auf die digitale Sicherheit ihrer angebotenen Smart Home Systeme, folgende Funktionen und Punkte berücksichtigen:

Wie in Absatz 5.2.1.1 erwähnt, ist es wichtig kontinuierliche Sicherheitsupdates für die Geräte zur Verfügung zu Stellen. Da Hersteller-Updates jedoch auch andere Inhalte, wie Design-Änderungen oder neue Funktionen enthalten, ist es wichtig in den Anwendungen übersichtlich und leicht erkennbar aufzuzeigen, ob ein Update sicherheitsrelevante Inhalte enthält. Dadurch kann der User entscheiden, ob das jeweilige Update für ihn und seine Sicherheit relevant ist. Außerdem wäre eine Einstellung, die sicherheitsrelevante Updates automatisiert installiert vorteilhaft. So muss der User Sicherheitsupdates nicht manuell auswählen bzw. ausführen (vgl. Absatz 4.4).

Smart Home-steuernde Mobile Apps auf Mobilgeräten benötigen, anders als Webanwendungen, nicht zwingend eine Internetverbindung, um Kontakt zu den IoT-

Geräten aufzunehmen. Eine Alternative zur Internetverbindung kann beispielsweise eine Bluetooth-Verbindung sein [79]. Ermöglicht der Hersteller eine solche „internetlose“ Verbindung, kann der User eine Remote-Steuerung seiner IoT-Devices ausschalten, wenn er sich selbst in der Nähe seines Smart Home Systems befindet, und die Geräte können durch EDGEAI-Technik und bspw. eine Bluetooth-Verbindung weiterhin mit allen Funktionen genutzt werden, ohne dass eine Verbindung zum Internet besteht (vgl. Absatz 4.4).

Wie in Absatz 4.5 erläutert sollten Mobile Apps es auch ermöglichen, die verschiedenen Funktionen der Smart-Home Geräte individuell an- und abzuschalten, sodass nur die tatsächlich verwendeten Funktionen genutzt werden. Genau wie die Funktionen der Geräte, soll auch die Verwaltung der Daten für den User transparent aufbereitet und auswählbar sein. In Absatz 4.2 ist an dieser Stelle die Rede von „Privacy by Design“. Das bedeutet, dass der User in der jeweiligen Anwendung festlegen kann, welche seiner Daten verarbeitet und gespeichert werden können. Ein Beispiel für eine „Privacy by Design““-Einstellung ist die Regionen Auswahl in dem die Rechner der jeweiligen Cloud liegen. Diese Einstellung ist deshalb, für Nutzer relevant, da die Datenschutzrichtlinien regional stark variieren. [80]

Weiterhin sollten die Anwendungen sicherstellen, dass der User das Default-Passwort ändern muss. Es sollen nur sichere Passwörter zulässig sein [81] und jedes Gerät mit einem eigenen Passwort geschützt werden [75]. Zudem sollten die Login-Versuche in der Cloud dokumentiert und analysiert werden, um den Nutzer frühzeitig über mögliche Angriffsversuche zu informieren (vgl. Absatz 4.5).

5.2.3.2 Schutzvorkehrungen Smart Home Nutzer - Anwendungsschicht

Die Nutzer von Smart Home -Anwendungen, sollten die vom Hersteller eröffneten Sicherheitsmöglichkeiten nach ihrem individuellen Bedürfnis nutzen. Dazu gehört es im Besonderen die Update–Funktionalitäten des jeweiligen Gerätes zu nutzen und Sicherheitsupdates automatisiert zuzulassen. Außerdem sollten sie alle nicht genutzten Funktionen, wie die bspw. eine Sprachsteuerung abschalten. Dies gilt im Besonderen für die Remote-Steuerfähigkeit des eigenen Smart Homes. Solange keine ortsunabhängige Steuerung benötigt wird und andere Verbindungsmöglichkeiten existieren, müssen die Geräte nicht mit dem Internet verbunden werden. [75]

Außerdem sollten Smart Home-Nutzende sicherstellen, dass sie für die dafür verwendeten Accounts und Geräte sichere und unterschiedliche Passwörter erstellen. Jeder IoT Account und jede Smart Home Anwendung sollte mit einem eigenen Passwort geschützt werden. Das stellt sicher, dass im Fall eines erfolgreichen Hacking-Angriffes auf eine Anwendung die anderen Anwendungen und Geräte nicht betroffen sind. [75]

Für die Verwaltung und Erstellung von unterschiedlichen, sicheren Passwörtern wird empfohlen einen Passwortmanager zu verwenden [75]. Passwortmanager sind in der Lage selbst sichere Passwörter zu generieren, sie und die dazugehörigen Benutzerdaten automatisch in die jeweiligen Login-Fenster einzufüllen und abzuspeichern. Die Verwaltung eines Passwortmanagers kann bspw. innerhalb eines Browser oder auch über eine Cloud

erfolgen, sodass ein Nutzer seine Passwörter Geräteübergreifend zur Verfügung stehen[82]. Da die im Passwortmanager verwalteten Passwörter automatisch in die jeweiligen Login-Fenster gefüllt werden, müssen die Nutzer die Passwörter selbst nicht mehr zwingend alle Passwörter kennen. Das ermöglicht es auch Smart Home- Nutzenden für jede Identifikation unterschiedliche, sichere Passwörter zu verwenden, ohne alle Passwörter dauerhaft selbst kennen zu müssen [75]. Durch die Verwendung verschiedener, sicherer Passwörter kann Bedrohungen bei Authentifizierungsmechanismen (vgl. Absatz 3.3) wie beim Mirai-Botnet-Angriff (vgl. Absatz 2.2) vorgebeugt werden.

5.3 Realisierung der Sicherheitsvorkehrungen im Smart Home-Bereich

Im vorherigen Abschnitt wurden geeignete Schutzvorkehrungen aufgezeigt, die Smart Home Anbietende und Nutzende gegen Cyberangriffe treffen können. Diese werden in Tabelle 4 in Kurzform übersichtlich strukturiert dargestellt:

IoT-Schicht	Anbieter	Nutzer
Geräte-schicht	• EDGEAI -Technik • Kontinuierliche Produktsoftwareupdates	• Schutz vor physischen Schaden • Schutz vor physischer Zugänglichkeit
Netzwerk-schicht	• Sichere Übertragungsprotokolle verwenden	• Umbenennen des Routers • Router mit Sicherheitsprotokoll wählen • Eigenes Netzwerk für IoT-Geräte einrichten
Anwendungs-schicht	• Updateinhalte deutlich kennzeichnen • Mobile Apps zusätzlich mit anderen Verbindungsmöglichkeiten als dem Internet ausstatten • Datenverwaltung individuell konfigurierbar gestalten • Passwort-Zulässigkeit an sichere Kriterien binden	• Sicherheitsrelevante Updates automatisiert zulassen • verschiedene Passwörter sicher gestalten • Passwortmanager verwenden

Tabelle 4 Zusammenfassung Smart Home Sicherheitsvorkehrungen Anbieter und Nutzer

Abschließend wird nun untersucht, was die Parteien Anbieter und Nutzer dazu bewegt, diese Möglichkeiten auch zu realisieren.

Damit die Parteien diese Vorkehrungen auch vornehmen, benötigen sie neben der Kenntnis über die Möglichkeiten, auch ein entsprechendes Verantwortungsbewusstsein und die Motivation diese Vorkehrungen umzusetzen (vgl. Abbildung 15). Besonders das eigene Verantwortungsbewusstsein für Sicherheitsvorkehrungen ist in der Regel jedoch nur

bedingt ausgeprägt und die Sicherheitsverantwortung wird oftmals bei den jeweils anderen Akteuren gesucht. Beispielsweise geben IoT-Produkt-Hersteller an, die Sicherheit von Produkten deshalb nicht zu erhöhen, weil Kunden nicht bereit seien die Kosten dafür zu tragen [83]. Die Anbieter-Seite hat demnach ein besonders kostengetriebenes Interesse daran, Sicherheitsvorkehrungen gegen Hacking Angriffe in ihre angebotenen Smart Home - Geräte und - Anwendungen zu integrieren.

Forschende des Karlsruhe Institute of Technology konnten feststellen, dass die Zahlungsbereitschaft für Schutzvorkehrungen und die Bereitschaft den Zeitaufwand für deren Konfiguration aufzubringen bei Smart Home - Kunden dann steigt, wenn die wahrgenommene Bedrohung zunimmt [84]. Gelingt es also das Bewusstsein für die akuten Sicherheitsrisiken (vgl. Kapitel 3) bei Smart Home Kunden zu schärfen, so steigt deren Zahlungsbereitschaft für Sicherheitsvorkehrungen. Wie bereits in Absatz 5.1 am Beispiel des Abschließens der eigenen Haustür beschrieben wurde, ist ein grundsätzliches Verständnis für Schutzvorkehrungen bei Privatpersonen bereits vorhanden. Anbieter können darauf aufbauend beispielsweise Smart Home Sicherheits-Kampagnen ins Leben rufen, in denen sie über die besonderen Gefahren eines digitalen Zuhauses aufklären und ihre dafür angebotenen Schutzfunktionen verständlich aufzeigen. Weiterhin können Sie ihre Sicherheitsfunktionen so gestalten, dass die Nutzer einen möglichst geringen Zeitaufwand für deren Konfiguration benötigen. Dies kann bspw. durch die genannten automatisierten Sicherheitsupdates geschehen (vgl. Absatz 5.2.3.1). Trotz der zahlreichen Angebotsmöglichkeiten von Sicherheitsvorkehrungen müssen Smart Home Nutzende sich darüber bewusst sein, dass sie selbst den Sicherheitsgrad ihrer generierten Daten maßgeblich mitbestimmen. Die aufgezeigten Möglichkeiten bieten ihnen auch nur dann Schutz, wenn sie auf den jeweiligen Ebenen realisiert werden.

6 Fazit und Ausblick

Im Rahmen dieser Arbeit wurde ein umfassendes Bild zum Thema „Sicherheit im IoT“ geschaffen. Dazu wurde zunächst der Begriff IoT, sowie dessen charakteristische Systemarchitektur erläutert. Nach der historischen Einordnung der IoT-Relevanz für die Industrie wurden die im Zentrum des IoT stehenden Cyber-Physischen Systeme dargelegt. Die Gefahren im IoT wurden durch die explizite Betrachtung von drei großen Sicherheitsvorfällen in der jüngeren Vergangenheit deutlich. Das grundsätzliche Vorgehen der Angreifer wurde in jeweiligen Szenarien detailliert erläutert und die Konsequenzen der einzelnen Angriffe aufgeführt. Eine darauf aufbauende Analyse zeigte die Bedrohungen auf, die zu solchen Sicherheitsvorfällen führen können. Dies erfolgte durch die Untersuchung von verschiedenen Angriffsarten und deren Abläufen. Nachdem ein Verständnis für die Angriffe und Bedrohungen im IoT geschaffen wurde, wurden zahlreiche Maßnahmen vorgestellt, die die Sicherheit im IoT gewährleisten. Diese zahlreichen Maßnahmen wurden explizit für die jeweiligen Ebenen des IoT aufgezeigt. Die so gewonnen Erkenntnisse sind am Praxisbeispiel Sicherheit im IoT im Smart Home -Bereich plastisch dargestellt worden. Die individuellen Sicherheitsmaßnahmen wurden den Verantwortungsgruppen und IoT-Schichten zugeordnet und deren Umsetzung am Ende kritisch eingeordnet.

Der sukzessive Arbeitsaufbau ermöglichte es ein Verständnis für die Sicherheitsthematik im IoT zu schaffen, indem die reellen Vorfälle und Bedrohungen analysiert und dagegen schützende Sicherheitsvorkehrungen plastisch aufgezeigt wurden.

Mit der zunehmenden Verbreitung des IoT in immer mehr Branchen und Lebensbereichen, steigt auch die Komplexität der Bedrohungslage für IoT-Systeme. Aufbauend auf dieser Arbeit können nun die individuellen Sicherheitslücken in verschiedenen Bereichen ermittelt und untersucht werden. Im Besonderen sollte dabei die Thematik der Sicherheitsverantwortlichkeiten der individuellen IoT-Akteure, deren Komplexität in der Regel über die Rollen „Anbieter“ und „Nutzer“ hinaus geht, untersucht werden.

7 Literaturverzeichnis

References

[1] D. Trotta and P. Garengo, “Industry 4.0 key research topics: A bibliometric review,” in *2018 7th International Conference on Industrial Technology and Management (ICITM 2018): March 7-9, 2018 Oxford, UK*, Oxford, United Kingdom, 2018, pp. 113–117.

[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[3] J. H. Nord, A. Koohang, and J. Paliszkiewicz, “The Internet of Things: Review and theoretical framework,” *Expert Systems with Applications*, vol. 133, pp. 97–108, 2019, doi: 10.1016/j.eswa.2019.05.014.

[4] A. Rayes and S. Salam, *Internet of Things From Hype to Reality*. Cham: Springer International Publishing, 2019.

[5] A. Samuel and C. Sipes, “Making Internet of Things Real,” *IEEE Internet Things M.*, vol. 2, no. 1, pp. 10–12, 2019, doi: 10.1109/IOTM.2019.1907777.

[6] K. Chopra, K. Gupta, and A. Lambora, “Future Internet: The Internet of Things-A Literature Review,” in *Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects: COMITCon 2019 : 14th-16th February 2019*, Faridabad, India, 2019, pp. 135–139.

[7] IoT Analytics, “Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 (in billions),” Nov. 2020. Accessed: Apr. 2 2023. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[8] D. Navani, S. Jain, and M. S. Nehra, “The Internet of Things (IoT): A Study of Architectural Elements,” in *2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, Jaipur, India, 2017, pp. 473–478.

[9] C. Patel and N. Doshi, *Internet of things security: Challenges, advances and analytics*. Boca Raton: CRC Press Taylor & Francis Group, 2019.

[10] A. Borgmeier, A. Grohmann, and S. F. Gross, *Smart Services und Internet der Dinge Geschäftsmodelle, Umsetzung und Best Practices: Industrie 4.0 Big Data Machine Learning Blockchain Additive Fertigung Kooperations-Ökosysteme,* 2nd ed. München: Hanser, 2022. [Online]. Available: https://www.hanser-kundencenter.de/fachbuch/artikel/9783446469259

[11] G. Reinhart, Ed., *Handbuch Industrie 4.0: Geschäftsmodelle Prozesse Technik*. München: Carl Hanser Verlag, 2017. [Online]. Available: http://www.hanser-elibrary.com/doi/book/10.3139/9783446449893

[12] H. Kagermann, W.-D. Lukas, and W. Wahlster, “Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution,” *vdi-nachrichten*, 2011, p. 2, 2011. https://www-live.dfki.de/fileadmin/user_upload/DFKI/Medien/News_Media/Presse/

Presse-Highlights/vdinach2011a13-ind4.0-Internet-Dinge.pdf (accessed: May 29 2023).
[13] F. Kellner, B. Lienland, and M. Lukesch, *Produktionswirtschaft*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2022.
[14] Kevin Townsend, *Financial Services DDoS Attacks Tied to Reaper Botnet.* [Online]. Available: https://www.securityweek.com/financial-services-ddos-attacks-tied-reaper-botnet (accessed: Jun. 14 2023).
[15] Pascal Geenens, *Why the World is Under the Spell of IoT_Reaper* (accessed: Jun. 14 2023).
[16] *IOTROOP BOTNET: THE FULL INVESTIGATION* (accessed: Jun. 14 2023).
[17] Joan Soriano, *Linux.IotReaper Analysis* (accessed: Jun. 14 2023).
[18] Black Lotus Labs, *How The Grinch Stole IoT.* [Online]. Available: https://blog.lumen.com/how-the-grinch-stole-iot/ (accessed: Jun. 14 2023).
[19] A. Pandian, T. Senjyu, S. M. S. Islam, and H. Wang, *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018)*. Cham: Springer International Publishing, 2020.
[20] LILY HAY NEWMAN, *The Botnet That Broke the Internet Isn't Going Away* (accessed: Jun. 14 2023).
[21] Constantinos Kolias, *DDoS in the IoT: Mirai and other botnets* (accessed: Jun. 14 2023).
[22] Mariusz Antoni Kaminsky, *Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme.* [Online]. Available: https://www.academia.edu/43954570/Operation_Olympic_Games_Cyber_sabotage_as_a_tool_of_American_intelligence_aimed_at_counteracting_the_development_of_Irans_nuclear_programme (accessed: 17.06.23).
[23] Perry Lea, *A Review of IoT Exploits & Cyber Attacks* (accessed: Jun. 14 2023).
[24] C. Levine, *Conceptualizing Financial Loses as a Result of Advanced Persistent Threats* (accessed: Jun. 14 2023).
[25] DAVID KUSHNER, *THE REAL STORY OF STUXNET* (accessed: Jun. 14 2023).
[26] National Intelligence Council, Ed., “Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025,” National Intelligence Council, 2008. Accessed: Apr. 10 2023. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA519715.pdf
[27] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, “IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, 2019, doi: 10.1109/JIOT.2019.2935189.
[28] Y. Shah and S. Sengupta, “A survey on Classification of Cyber-attacks on IoT and IIoT devices,” in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, 2020, pp. 406–413.
[29] S. K. K, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, “Security Enhancements to System on Chip Devices for IoT Perception Layer,” in *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2017, pp. 151–156.

[30] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, 2020, doi: 10.1109/JIOT.2020.2997651.

[31] J. Wang, C. Liu, L. Zhou, L. Tian, and X. Yu, “Early Detection of Node Capture Attack in the Internet of Things,” in *2021 IEEE 4th International Conference on Electronics and Communication Engineering (ICECE)*, Xi'an, China, 2021, pp. 132–135.

[32] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, “Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks,” *IEEE Trans. Dependable and Secure Comput.*, vol. 19, no. 1, pp. 507–523, 2022, doi: 10.1109/TDSC.2020.2974220.

[33] Z. Čekerevac, Z. Dvorak, L. Prigoda, and P. Čekerevac, “INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS – SECURITY AND ECONOMIC RISKS,” *MEST Journal*, vol. 5, no. 2, 15-5, 2017, doi: 10.12709/mest.05.05.02.03.

[34] P. Vennam, S. K. Mouleeswaran, S. Shamila, and S. R. Kasarla, “A Comprehensive Analysis of Fog Layer and Man in the Middle Attacks in IoT Networks,” in *IEEE MysuruCon-2022: 2nd edition of the flagship international conference series of IEEE Mysore Subsection : 16th & 17th October 2022*, Mysuru, India, 2022, pp. 1–5.

[35] J. Thomas, S. Cherian, S. Chandran, and V. Pavithran, “Man in the Middle Attack Mitigation in LoRaWAN,” in *Proceedings of the 5th International Conference on Inventive Computation Technologies (ICICT 2020): 26-28, February 2020*, Coimbatore, India, 2020, pp. 353–358.

[36] A. A. Olazabal, J. Kaur, and A. Yeboah-Ofori, “Deploying Man-In-the-Middle Attack on IoT Devices Connected to Long Range Wide Area Networks (LoRaWAN),” in *IEEE ISC2 2022: 8th IEEE International Smart Cities Conference 2022 : 26-29 September 2022, Aliathon Resort, Paphos, Cyprus*, Pafos, Cyprus, 2022, pp. 1–7.

[37] M. A. Yurdagul and H. T. Sencar, “BLEKeeper: Response Time Behavior Based Man-In-The-Middle Attack Detection,” in *2021 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 2021, pp. 214–220.

[38] R. Cayre, F. Galtier, G. Auriol, V. Nicomette, M. Kaaniche, and G. Marconato, “InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections,” in *51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks: DSN 2021 : proceedings : 21-24 June 2021, virtual event*, Taipei, Taiwan, 2021, pp. 388–399.

[39] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, “Edge Computing Security: State of the Art and Challenges,” *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019, doi: 10.1109/JPROC.2019.2918437.

[40] A. P. Sayakkara and N.-A. Le-Khac, “Electromagnetic Side-Channel Analysis for IoT Forensics: Challenges, Framework, and Datasets,” *IEEE Access*, vol. 9, pp. 113585–113598, 2021, doi: 10.1109/ACCESS.2021.3104525.

[41] Y. Hayashi, “State-of-the-art research on electromagnetic information security,” *Radio Sci.*, vol. 51, no. 7, pp. 1213–1219, 2016, doi: 10.1002/2016RS006034.

[42] J. G. Ponsam, S. J. B. Gracia, G. Geetha, S. Karpagaselvi, and M. Safa, "Side Channel Analysis - A Demonstrative Approach on a 128-Bit AES Algorithm," in *IEEE Second International Conference on Power, Energy, Control and Transmission Systems: 10.12.2020 & 11.12.2020 : proceedings*, Chennai, India, 2020, pp. 1–6.
[43] P. Kocher *et al.,* "Spectre Attacks: Exploiting Speculative Execution," Jan. 2018. [Online]. Available: https://arxiv.org/pdf/1801.01203
[44] M. Lipp *et al.,* "Meltdown," Jan. 2018. [Online]. Available: https://arxiv.org/pdf/1801.01207
[45] Y. Xu, Y. Jiang, L. Yu, and J. Li, "Brief Industry Paper: Catching IoT Malware in the Wild Using HoneyIoT," in *2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, Nashville, TN, USA, 2021, pp. 433–436.
[46] A. Borys, A. Kamruzzaman, H. N. Thakur, J. C. Brickley, M. L. Ali, and K. Thakur, "An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet," in *2022 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2022, pp. 725–729.
[47] Y. Li and K. Jiang, "Prospect for the Future Internet: A Study Based on TCP/IP Vulnerabilities," in *2012 International Conference on Computing, Measurement, Control and Sensor Network (CMCSN 2012): Taiyuan, China, 7 - 9 July 2012 ; [proceedings*, Taiyuan, China, 2012, pp. 52–55.
[48] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 283–302, 2014, doi: 10.1109/SURV.2013.041513.00174.
[49] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *2017 IEEE International Systems Engineering Symposium (ISSE)*, Vienna, Austria, 2017, pp. 1–7.
[50] E. Atilgan, I. Ozcelik, and E. N. Yolacan, "MQTT Security at a Glance," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, Ankara, Turkey, 2021, pp. 138–142.
[51] M. M. Raikar and M. S M, "Vulnerability assessment of MQTT protocol in Internet of Things (IoT)," in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, Jalandhar, India, 2021, pp. 535–540.
[52] M. Hadded, G. Lauras, J. Letailleur, Y. Petiot, and A. Dubois, "An Assessment Platform of Cybersecurity Attacks against the MQTT Protocol using SIEM," in *2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, 2022, pp. 1–6.
[53] M. N, V. K R, and E. R. B, "Short Paper : Current Challenges in IoT Cloud Smart Applications," in *2021 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, NJ, USA, 2021, pp. 36–40.
[54] N. Mishra and R. K. Singh, "Taxonomy & Analysis of Cloud Computing Vulnerabilities through Attack Vector, CVSS and Complexity Parameter," in *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, GHAZIABAD, India, 2019, pp. 1–8.

[55] C. Silva *et al.,* "Towards a taxonomy for security threats on the web ecosystem," in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, Istanbul, Turkey, 2016, pp. 584–590.
[56] H. Baron, J. Buker, S. Heide, A. Kaluza, S. Mahmud, and J. Yeoh, "The State of Cloud Security Risk, Compliance, and Misconfigurations," 2021. Accessed: May 12 2023. [Online]. Available: https://cloudsecurityalliance.org/artifacts/state-of-cloud-security-risk-compliance/
[57] S. Kumari, K. Solanki, S. Dalal, and A. Dhankhar, "Analysis Of Cloud Computing Security Threats and Countermeasures," in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, 2022, pp. 1–6.
[58] A. Tomar, D. Jeena, P. Mishra, and R. Bisht, "Docker Security: A Threat Model, Attack Taxonomy and Real-Time Attack Scenario of DoS," in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2020, pp. 150–155.
[59] P. Padma, R. Akshaya, H. Akshaya, and R. Harini, "Perlustrate Study on Cloud Security and Vulnerabilities," in *2021 4th International Conference on Computing and Communications Technologies (ICCCT)*, Chennai, India, 2021, pp. 293–296.
[60] OWASP® Foundation, *OWASP Top 10 2021 - A01 Broken Access Control.* [Online]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/ (accessed: May 12 2023).
[61] OWASP® Foundation, *OWASP Top 10 2021 - A03 Injection.* [Online]. Available: https://owasp.org/Top10/A03_2021-Injection/ (accessed: May 12 2023).
[62] OWASP® Foundation, *OWASP Top 10 2021 - A02 Cryptographic Failures.* [Online]. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ (accessed: May 12 2023).
[63] M. Xue, C. Yuan, H. Wu, Y. Zhang, and W. Liu, "Machine Learning Security: Threats, Countermeasures, and Evaluations," *IEEE Access*, vol. 8, pp. 74720–74742, 2020, doi: 10.1109/ACCESS.2020.2987435.
[64] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Bürgerbroschüre - Das Internet der Dinge sicher nutzen," 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Brosch_A6_Internet_der_Dinge.pdf?__blob=publicationFile&v=5
[65] Pape, Sebastian, Wagner, Frank, "- IT-Sicherheit (und Datenschutz) im Internet der Dinge," 2016. [Online]. Available: https://www.researchgate.net/publication/307855918_IT-Sicherheit_und_Datenschutz_im_Internet_der_Dinge
[66] Microsoft Corporation, *IoT-Sicherheit – eine Übersicht: Der Schutz Ihrer Daten und Geräte im Internet der Dinge.* [Online]. Available: https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-is-iot/security/ (accessed: May 20 2023).

[67] TeamDrive Systems GmbH, *Das Internet der Dinge – Datensicherheit auf höchstem Niveau.* [Online]. Available: https://teamdrive.com/blog-de/das-internet-der-dinge-datensicherheit (accessed: May 20 2023).
[68] F. A. ClAUDIA ECKERT, *IT-Sicherheit und Industrie 4.0: Vernetzung, Big Data und Cloud.* [Online]. Available: https://www.im-io.de/wp-content/uploads/2015/12/Fraunhofer_Datability.pdf (accessed: May 20 2023).
[69] Deutsche Telekom AG, "Sicherheit im Industriellen Internet der Dinge," [Online]. Available: https://cloud.telekom.de/resource/blob/data/90710/77058f7ebdf65ba1873642c561f3f3fc/sicherheitsspecial-m2m-sicherheit-whitepaper.pdf
[70] Bitkom e.V., "Open-Source-Leitfaden: Praxisempfehlungen für Open-Source-Software Version 3.0," 2022. [Online]. Available: https://www.bitkom.org/sites/main/files/2022-06/220624-Bitkom-Leitfaden-Open%20Source-3.0_0.pdf
[71] BSI, "Ergebnisbericht Workstream „Digitales Mindesthaltbarkeitsdatum"," 2022. [Online]. Available: https://www.dialog-cybersicherheit.de/storage/uploads/ws21-endprodukte/WS2%20-%20Digitales%20Mindesthaltbarkeitsdatum.pdf
[72] Bundesministeriums für Wirtschaft und Energie, "IT-Sicherheit-für-die-Industrie-4-0: Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten," 2016. [Online]. Available: https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/autonomik-IT%20Sicherheit%20Studie%20HMI%202016%20langfassung.pdf?__blob=publicationFile&v=7
[73] Cornelsen Verlag GmbH, *Zuhause ▷Rechtschreibung, Bedeutung, Definition, Herkunft | Duden.* [Online]. Available: https://www.duden.de/rechtschreibung/Zuhause (accessed: Jun. 16 2023).
[74] L. Jiang, D.-Y. Liu, and B. Yang, "Smart home research," in *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826)*, Shanghai, China, 2004, pp. 659–663.
[75] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 281–292, 2023, doi: 10.1109/OJVT.2023.3234069.
[76] R. Singh and S. S. Gill, "Edge AI: A survey," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 71–92, 2023, doi: 10.1016/j.iotcps.2023.02.004.
[77] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, "BioSec: A Biometric Authentication Framework for Secure and Private Communication Among Edge Devices in IoT and Industry 4.0," *IEEE Consumer Electron. Mag.*, vol. 11, no. 2, pp. 51–56, 2022, doi: 10.1109/MCE.2020.3038040.
[78] E. Chatzoglou, G. Kambourakis, and C. Kolias, "How is your Wi-Fi connection today? DoS attacks on WPA3-SAE," *Journal of Information Security and Applications*, vol. 64, 259-284, 2022, doi: 10.1016/j.jisa.2021.103058.

[79] R. Hellmann, *IT-Sicherheit: Methoden und Schutzmaßnahmen für sichere Cybersysteme,* 2nd ed. Berlin, Boston: De Gruyter Oldenbourg, 2023. [Online]. Available: https://www.degruyter.com/isbn/9783110767186
[80] T. Liedtke, *Informationssicherheit*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2022.
[81] M. Kofler *et al., Hacking & Security: Das umfassende Handbuch,* 3rd ed. Bonn: Rheinwerk Verlag, 2023. [Online]. Available: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=7152444
[82] USENIX Association, *23rd USENIX Security Symposium: August 20 - 22, 2014, San Diego, CA*. Berkeley, Calif.: USENIX Association, 2014. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14
[83] S. Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke*. Wiesbaden: Springer Fachmedien Wiesbaden, 2021.
[84] R. Duezguen *et al.,* "How to Increase Smart Home Security and Privacy Risk Perception," in pp. 997–1004.