HAW HAMBURG

MASTER THESIS
Svenja Dittmers

Sicherheitsanalysen im Kontext von IoT: praktische und aktuelle Lösungsansätze

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Svenja Dittmers

Sicherheitsanalysen im Kontext von IoT: praktische und aktuelle Lösungsansätze

Masterarbeit eingereicht im Rahmen der Masterprüfung
im Studiengang *Master of Science Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr. Bettina Buth

Eingereicht am: 10.08.2023

Svenja Dittmers

Thema der Arbeit

Sicherheitsanalysen im Kontext von IoT: praktische und aktuelle Lösungsansätze

Stichworte

IoT, Sicherheit, Analysen, Schwachstellen, Bedrohungen, Penetrationtest

Kurzzusammenfassung

Inhalt dieser Arbeit ist es einen Überblick des aktuellen Forschungsstandes im Bereich Sicherheitsanalysen im Kontext des Internet of Things (IoT) zu geben. Zu diesem Zweck wird eine systematische Literaturrecherche durchgeführt, um die erforderlichen Informationen zu sammeln. Dabei sollen Fragen zu aktuellen und neuen Lösungsansätzen beantwortet werden, sowie die aktuellen Herausforderungen und die Entwicklung von Sicherheitsanalysen im Kontext IoT. Im Anschluss daran erfolgt eine kritische Bewertung der erfassten Daten.

Svenja Dittmers

Title of Thesis

Security analyses in the context of IoT: practical and current solution approaches

Keywords

IoT, Security, Analysis, Vulnerability, Threats, Penetrationtesting

Abstract

The purpose of this work is to provide an overview of the current state of research in the field of security analyses within the context of the Internet of Things (IoT). For this purpose, a systematic literature review is conducted to gather the necessary information. This aims to address questions concerning current and novel solutions, as well as the current challenges and the evolution of security analyses in the IoT context. Subsequently, a critical evaluation of the collected data will be carried out.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

6LoWPAN IPv6 over Low power Wireless Personal Area Network.

ACM Association for Computing Machinery.

AMQP Advanced Message Queuing Protocol.

BLE Bluetooth Low Energy.

COAP Constrained Application Protocol.

CRC Cyclic Redundancy Checks.

CVE Common Vulnerabilities and Exposures.

CVSS Common Vulnerability Scoring System.

CWE Common Weakness Enumeration.

DREAD Damage, Reproducibility, Exploitability, Affected Users, Discoverability.

DTLS Datagram Transport Layer Security.

GPS Global Positioning System.

IoT Internet of Things.

KI Künstliche Intelligenz.

LoRaWAN Long Range Wide Area Network.

LTE Long Term Evolution.

MQTT Message Queuing Telemetry Transport.

NFC Nearfield Communication.

NVD National Vulnerability Database.

PASTA Process for Attack Simulation and Threat Analysis.

REST Representational State Transfer.

RFID Radio Frequency Identificaion.

RPL Routing Protocol for Low power and Lossy Networks.

SCADA Supervisory Control and Data Acquisition.

SLR Systematische Literaturrecherche.

SOAP Simple Object Access Protocol.

STRIDE Spoofing, Tampering, Repudiation,Information disclosure, Denial of Service, Elevation of Privileges.

WSN Wireless Sensor Network.

XML Extensible Markup Language.

XMPP Extensible Messaging and Presence Protocol.

1 Einleitung

Der schnelle Wachstum des Internet of Things (IoT) über die letzten Jahre hat die Art und Weise der Interaktion mit Geräten und Diensten revolutioniert. Durch die geringen Kosten und die Einfachheit der Bereitstellung von IoT-Geräten, nimmt das Verbreitung der IoT-Geräte stetig zu [1]. Dabei finden sie vermehrt Anwendung in verschiedenen Bereichen unseres Alltags. Von Home Assistant wie Amazons Alexa[50], Türschlössern [67], Webkameras [3] bis hin zu industriellen Anlagen, wie intelligente Stromnetze [58] oder der Automobilindustrie [38]. Durch das breite Anwendungsfeld entstehend neue Herausforderungen in Bezug auf die Sicherheit, welche vielfältig und komplex sind. Die Interaktion von heterogenen Geräten und die Menge an erfassten Daten schaffen neue Bedrohungen, Schwachstellen und somit potenzielle Angriffsvektoren, die es zu adressieren gilt. Schwachstellen definieren sich hierbei durch die Verwundbarkeit von IoT-Firmware, Anwendungen oder Diensten, die von einem Angreifer ausgenutzt werden können. Bedrohungen wird als eine potenzielle Gefahr definiert, die Auswirkungen auf Integrität, Vertraulichkeit oder Verfügbarkeit von Systemen, Daten oder Ressourcen haben können[32]. Sicherheitsanalysen sind bewährte Praktiken um Schwachstellen oder Bedrohungen zu identifizieren und diesen entgegenzuwirken.
Ziel dieser Arbeit ist es Sicherheitsanalysen im Bereich IoT zu analysieren. Einerseits erfolgt eine Betrachtung der zeitlichen Entwicklung von Sicherheitsanalysen. Aber auch werden Herausforderungen berücksichtigt, die sich aus der Komplexität und Dynamik des IoT-Umfelds ergeben. Ebenso wird der Fokus auf bestehende Techniken und Ansätze gelegt, sowie ein Blick auf zukünftige Technologien, die zur Verbesserung beitragen könnten, gerichtet. Der Fokus liegt hierbei auf den IoT-Geräten und Systemen und weniger auf Web- oder mobilen Anwendungen die im Zusammenhang mit IoT stehen.
Um diese Fragen zu beantworten wird eine systematische Literaturrecherche durchgeführt. Die Erkenntnisse aus dieser Arbeit sollen dazu beitragen, einen Überblick über das Thema Sicherheitsanalysen im Bereich IoT zu liefern.

1.1 Motivation

Die Motivation zum Thema dieser Arbeit rührt von den zunehmenden Einsatzbereichen von IoT-Geräten. Das Verständnis für Sicherheit im Bereich IoT kann dazu beitragen, dass IoT-Systeme sicherer werden und Sicherheit des IoT generell weiter in den Fokus rückt. Durch die stetig wachsende Bedrohungslandschaft ist die Identifizierung von Schwachstellen und Bedrohungen unerlässlich, um gezielte Gegenmaßnahmen zu entwickeln. Ebenso erforderlich ist die Untersuchung und Bewertung bestehender Ansätze und Technologien im Zusammenhang mit dem Thema. Dies dient dazu ihre Effektivität aufzuzeigen und gegebenenfalls Schwachstellen in den Methoden zu aufzudecken.

1.2 Wissenschaftliche Relevanz

Die wissenschaftliche Relevanz von Sicherheitsanalysen im Kontext der IoT liegt in der Notwendigkeit der stetig zunehmenden Sicherheitsrisiken und den daraus resultierenden Herausforderungen, die im Zusammenhang mit IoT-Geräten und Systemen auftreten. Gerade die rasante Entwicklung von IoT trägt dazu bei, dass IoT widerstandsfähiger gegenüber aktuellen und zukünftigen Bedrohungen gemacht werden muss. Ebenso gilt es ein Bewusstsein für das Thema Sicherheit und Sicherheitsanalysen in diesem Bereich zu schaffen.

1.3 Definition Sicherheit im Kontext IoT

Da sich diese Arbeit mit Sicherheitsanalysen im Kontext von IoT beschäftigt, ist es wichtig vorab den Begriff Sicherheit zu definieren.
Im Allgemeinen lässt sich sagen, dass Sicherheit alle Techniken umfasst, die darauf abzielen, Informationen in IT-Systemen zu behalten, sie wiederherzustellen und vor Angriffen zu schützen. Dabei gibt es verschiedene Mechanismen die dabei helfen sollen dies zu gewährleisten: Authentifizierung, Vertraulichkeit, Integrität, Autorisierung und Verfügbarkeit [32].
Im Kontext von IoT stellt die Sicherheit eine besondere Herausforderung dar, da es sich um eine Anhäufung unterschiedlicher Geräte, Hersteller und Anwendungen handelt. Außerdem muss die Verbindung zwischen dem Gerät, der Cloud und anderen Netzwerken adäquat abgesichert werden. Zusätzlich stellt sich die Herausforderung der begrenzten

Energie- und Rechenkapazität sowie des beschränkten Speicherplatzes bei IoT-Geräten dar. Da die IoT-Geräte immer von überall erreichbar sein müssen, sind sie vielen Angriffsvektoren ausgesetzt und durch ihre physische Erreichbarkeit auch solchen, die normalen IT-Systemen oftmals nicht ausgesetzt sind. Durch ihre weitreichenden Einsatzmöglichkeiten gilt es besonders Daten, Infrastruktur und das Gerät selbst zu schützen. Diese zu schützenden Werte oder Objekte werden in der IT-Sicherheit Assets genannt.
Abbildung 1.1 zeigt, welche Komponente in den einzelnen Schichten eines IoT-Systems zum Einsatz kommen. In der untersten Schicht befinden sich die IoT-Knoten. Das können Mikrocontroller, Sensoren oder Aktoren, die Daten sammeln oder generieren, sein. Diese haben oft nur eine geringe Speicher - und Verarbeitungskapazität und enthalten keine eingebauten Sicherheitsmechanismen. In der Netzwerkschicht befinden sich die nötigen Komponenten, um die von den Sensoren und Aktoren generierten und gesammelten Daten weiter zu leiten. Dabei kommen drahtlose Übertragungstechnologien, wie Bluetooth Low Energy (BLE), ZigBee, WiFi, Long Range Wide Area Network (LoRaWAN), oder Mobilfunkstandards wie Long Term Evolution (LTE) oder 5G zum Einsatz. In der darüber liegenden Schicht befindet sich die Middleware. Sie ist eine Abstraktionsschicht zwischen der Netzwerkschicht und der Anwendungsschicht. Und in der obersten Schicht befinden sich die Anwendungen, die für die Endnutzer gedacht sind. Die Technologien der einzelnen Schichten sind notwendig für ein funktionierendes IoT-System, jedoch bringen sie vorhandene Sicherheitsrisiken mit sich[31].

Die zuvor erwähnten Sicherheitsmechanismen finden auch im Bereich IoT Anwendung. Der Schutz von Informationen und Daten vor unbefugtem Zugriff fällt unter den Begriff der Vertraulichkeit. Die Prävention unbefugter Manipulation wird durch Maßnahmen zur Gewährleistung der Integrität erreicht, während die Sicherstellung von Funktionalität und Zugang zum System unter den Aspekt der Verfügbarkeit fällt. Authentifizierungs- und Autorisierungsmechanismen dienen der Zugriffskontrolle von Nutzern, Diensten und anderen Geräten.
Der Sicherheitsbegriff im Kontext IoT bezieht sich auf die zuvor genannten Sicherheitsmechanismen, sowie auf die einzelnen Technologien in den verschiedenen Schichten des IoT-Systems.

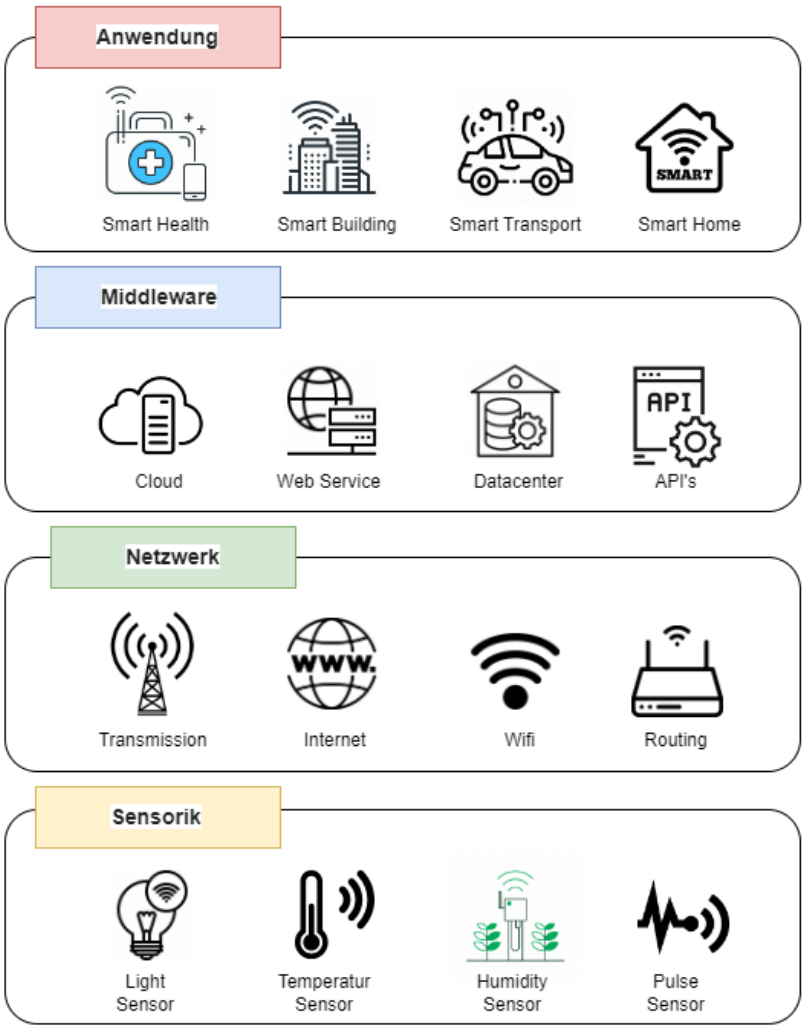

Abbildung 1.1: Schichten im IoT-System mit Beispielen zu jeder Schicht

1.4 Fragestellungen

Aufgrund der potenziellen Gefahren die IoT-Geräte und Systeme ausgesetzt sind, ergibt sich die Notwendigkeit Sicherheitsanalysen durchzuführen. Diese Analysen helfen dabei, Schwachstellen zu identifizieren, angemessene Sicherheitsmaßnahmen zu implementieren und die Integrität, Vertraulichkeit und Verfügbarkeit der IoT-Systeme zu gewährleisten. Dabei ergeben sich folgende Forschungsfragen, die im Laufe der Thesis beantwortet werden sollen:

Thesis Frage 1: Wie haben sich Sichereitsanalysen im Kontext von IoT entwickelt?
Es handelt sich um eine Beobachtung der Entwicklung von Sicherheitsanalysen im Zusammenhang mit dem IoT. Dabei wird der zeitliche Kontext berücksichtigt, um herauszufinden, wie sich die Forschung im Bereich der IoT-Sicherheit und Sicherheitsanalysen in den letzten Jahren verändert hat.

Thesis Frage 2: Herausforderungen: Welche Lösungsansätze versprechen in der Praxis eine Verbesserung bei Sicherheitsanalysen von IoT?
Aufbauend auf die vorhergegangene Fragestellung, beschäftigt sich diese mit den Herausforderungen bei Sicherheitsanalysen von IoT und sucht nach Lösungsansätzen, die in der Praxis eine Verbesserung versprechen. Es gilt herauszufinden, wie sich Herangehensweisen an Sicherheitsanalysen entwickelt haben und welche Technologien zur Verbesserung oder Ergänzung bestehender Methoden eingesetzt wurden.

Thesis Frage 3: Bewertung: Wie effektiv sind die aktuellen Lösungsansätze?
Die letzte Frage, aufbauend auf den zuvor entwickelten Fragen, zielt auf die Bewertung der aktuellen Lösungsansätze hinsichtlich ihrer Effektivität ab.

1.5 Forschungsmethode

Die Methodik dieser Arbeit besteht aus einer qualitativen Forschung auf Grundlage einer Systematische Literaturrecherche (SLR). Die Literaturrecherche lehnt sich dabei an die Methodik von Kitchenham und Charters und findet in Kapitel 3 Anwendung. [36].

1.5.1 Systematische Literaturrecherche

Bei einer SLR werden relevante Arbeiten zu einer bestimmten Thematik, oder Fragestellung identifiziert, evaluiert und interpretiert. Die Gründe für solch eine Methode können verschieden sein. Hauptsächlich bieten sie einen umfassenden Überblick über ein bestimmtes Themengebiet, oder Forschungsfrage. Aber auch um Lücken in der aktuellen Forschung zu identifizieren [14]. Auch dienen sie zur Untersuchung theoretischer Hypothesen und inwieweit empirische Belege diese unterstützen oder widerlegen. Die

Vorteile liegen dabei in einer klar definierten Methodik. Jedoch erfordern sie wesentlich mehr Aufwand, als normale Literaturübersichten. Ebenso stellt sich die Entwicklung eines Durchführungs-Protokolls, welches so gut es geht von Voreingenommenheit befreit ist, als eine Herausforderung dar [36].
Um eine erfolgreiche SLR durchzuführen bedarf es einer guten Planung. Dabei sollte sich mit der Motivation befasst werden, aus der die Recherche heraus entsteht. Anschließend sollte eine oder mehrere Forschungsfragen formuliert werden, auf die die Recherche aufgebaut wird. Der Aufbau und Ablauf eines solchen wird im folgenden Abschnitt näher erläutert.

1.5.2 Herangehensweise

Die Herangehensweise der Forschungsmethode für diese Thesis besteht aus drei Phasen: Vorbereitung, Datensammlung und Evaluierung der Ergebnisse.

Vorbereitung: In dieser Phase wird eine oder mehrere Forschungsfragen definiert. Dabei handelt es sich um die in 1.4 beschriebenen Forschungsfragen. Anschließend wird eine Suchstrategie entwickelt, mit der nach relevanten Forschungsarbeiten gesucht wird. Dies bezieht sich auf Quellen, wie einschlägigen Bibliotheken, sowie Stichwörtern mit denen gesucht wird. Ebenfalls werden Kriterien zur Inklusion und Exklusion von Arbeiten definiert. Anschließend wird eine Bewertungsliste für die Arbeiten festgelegt. Diese zielt darauf ab, die Qualität der identifizierten Arbeiten zu bewerten und somit jene zu bestimmen, die am relevantesten sind um die Forschungsfragen zu beantworten. Die letzten beiden Punkte in der Vorbereitungsphase beschäftigen sich mit dem Plan der Datenextrahierung, also wie man an die relevanten Daten gelangt und der Datenzusammenführung.

Datensammlung: In dieser Phase geht es um die Durchführung der Datensammlung. Ziel ist es so viele Arbeiten wie möglich zu finden, die Information zur Beantwortung der Forschungsfrage liefern. Bei der Suche ist es wichtig den sogenannten Publikation's Bias zu beachten. Häufig werden Forschungsarbeiten veröffentlicht, die positive Ergebnisse präsentieren, während Arbeiten mit negativen Ergebnissen seltener veröffentlicht werden. Die Einschätzung darüber, was als positiv oder negativ zu bewerten ist, liegt beim Forschenden.
Um die Datensammlung nachvollziehbar zu machen, wird die Suche dokumentiert.

Bei der Auswahl der Arbeiten werden auf die zuvor definierten Kriterien zur Exklusion und Inklusion zurückgegriffen.Anschließend wird dieser Datensatz den Kriterien der Bewertungsliste unterzogen. Die Auswahl der Arbeiten ist ein mehrstufiger Prozess, bei dem am Ende ein Set an Arbeiten zusammen kommt, die analysiert werden um die Forschungsfragen zu beantworten.

Evaluierung: In dieser Phase geht es um die anschließende Analyse der gesammelten Arbeiten. Dabei werden die Arbeiten hin gelesen um Informationen und Daten zur Beantwortung der Forschungsfragen zu erhalten. Die Zusammenfassung der Ergebnisse wird in diesem Fall deskriptiv geschehen, da sich Daten in der Informatik und im Bereich der Sicherheitsanalysen schwer in messbare Zahlen zusammenfassen lassen. Nachdem alle Informationen zusammengetragen wurden, folgt eine Diskussion.

2 Grundlagen

Dieses Kapitel befasst sich mit den Grundlagen zu dem Thema Sicherheit im Kontext IoT und untersucht Bedrohungen, Schwachstellen, Anforderungen an die Sicherheit und Sicherheitsanalysen. Der erste Abschnitt widmet sich den Bedrohungen von IoT, die mit der zunehmenden Vernetzung der Geräte einhergehen. Dabei wird auf verschiedene Angriffe eingegangen. Der darauf folgende Abschnitt befasst sich mit den Anforderungen an die Sicherheit von IoT. Der Hauptaugenmerk liegt hierbei auf den technischen Aspekten. Abschließend werden Sicherheitsanalysen im Kontext von IoT betrachtet. Dies umfasst die Analyse von Schwachstellen in IoT-Geräten und Systemen, sowie die Erkennung von Bedrohungen.

2.1 Sicherheit im Kontext IoT

Wie in Kapitel 1.3 beschrieben, lässt sich ein IoT-System in vier Ebenen aufteilen. Die Ebene der Sensorik steht an unterster Stelle und ist am nächsten an der Hardware der Geräte dran. Darauf folgt die Netzwerkebene, die zur Übertragung der Daten dient. An dritter Stelle steht die Middleware-Ebene, die als Bindeglied zwischen dem Netzwerk und den Anwendungen fungiert. Abschließend folgt die Anwendungsschicht, die die Ebene darstellt, auf der die Endnutzer interagieren. Die unterschiedlichen Technologien jeder Ebene bringen Sicherheitsrisiken und Bedrohungen mit sich, die sich auf das gesamte IoT-System auswirken können. Im folgenden werden auf einige mögliche Angriffe der einzelnen Ebenen eingegangen.

2.1.1 Angriffe und Bedrohungen

Die Sensorikebene ist unmittelbar mit der Hardware verbunden, wodurch sie unter anderem anfällig für physische Angriffe wird. Da die IoT-Knoten sich unter anderem in frei

zugänglichen Umgebungen befinden können, besteht die Möglichkeit, dass ein Angreifer Sensoren mühelos verändern, beschädigen oder das Übertragungssignal unterbrechen kann. Einige der Technologien, die in dieser Ebene zum Einsatz kommen sind Radio Frequency Identificaion (RFID), Wireless Sensor Network (WSN), Global Positioning System (GPS) etc.

Unbefugter Zugriff auf Tags: Ein Angreifer kann durch fehlende oder mangelnde Authentifizierungsmechanismen in RFID Chips unbefugten Zugriff erlangen und Daten einsehen, verändern oder löschen [32].

Node-Capture-Angriff: Wenn ein Angreifer einen IoT-Knoten übernommen hat, kann er diesen steuern oder ersetzen und dabei schwerwiegenden Einfluss auf das gesamten IoT-System nehmen [32].

Tag-Cloning: Tags finden Anwendung an verschiedenen Objekten um Informationen zu präsentieren. Diese lassen sich mit einigen wenigen Hacking-Techniken leicht ändern, indem der Tag reproduziert wird und so manipuliert wird, dass nicht zwischen Original und manipuliertem unterschieden werden kann [24].

False-Data-Injection-Angriff: Sobald ein Angreifer einen Knoten übernommen hat, sendet er manipulierte Daten an andere IoT-Geräte oder Knoten und beeinflusst damit die Anwendung und das Netzwerk [35].

Malicious-Code-Injection-Angriff: Ein Angreifer schleust falschen Code in den Speicher des Gerätes, um die Funktion des Knotens zu verändern oder es als Eintrittspunkt für weitere Angriffe nutzen [35].

Side-Channel-Angriff: Neben direkten Angriffen auf die Knoten, können auch Informationen zu den Prozessoren oder Stromversorgung genutzt werden um dem IoT-System Schaden zuzufügen. Dabei kann ein Angreifer Laser oder Magnete nutzen, um dem Knoten Schaden zuzufügen [31].

Booting-Angriff: Während des Bootvorgang's ist das System an anfälligsten, da Sicherheitsmaßnahmen oft noch nicht im Einsatz sind. Dadurch [31].

Firmware-Updates: Ein Angreifer greift in den Prozess des Firmware-Updates ein und manipuliert die Firmware oder spielt seine eigene Firmware auf. Ziel ist es weitere Angriffe auf das System durchzuführen [31].

Sleep-Deprivation-Angriff: Da die Knoten oft batteriebetrieben sind, treten sie bei Nichtnutzung in den Schlafmodus, um so Ressourcen zu sparen. Es wird versucht die Knoten daran zu hindern, in den Schlafmodus zu wechseln, um die Batterie zu verbrauchen und somit den Knoten zum Abschalten zu zwingen [18].

Die Netzwerkschicht ist verantwortlich für die Datenübertragung. Die Signalübertragung und Kommunikation erfolgen in der Regel drahtlos. Angriffe die sich auf die Netzwerkebene konzentrieren zielen oft auf die Verfügbarkeit von Netzwerkressourcen ab, oder auf das Abgreifen von Informationen. Kommunikationstechnologien, die in dieser Ebene zum Einsatz kommen sind unter anderem Bluetooth, BLE, Zigbee, Z-Wave, LoRaWAN, Nearfield Communication (NFC) oder auch Glasfaser, mobile Kommunikationstechnik oder Infrarottechnik.

Spoofing: Einem Angreifer gelingt es durch Vortäuschung einer anderen Identität in das IoT-System einzudringen und andere zu täuschen um manipulierte und böswillige Daten zu senden [24].

Sinkhole-Angriff: Der Angreifer lässt einen kompromittierten Knoten für die Nachbarknoten attraktiv aussehen. Ziel ist es, dass Daten der anderen Knoten fallen gelassen werden und die des kompromittierten Knoten bevorzugt werden um den Datenverkehr zu manipulieren [32].

Denial-of-Service-Angriff: Ein Angreifer versucht das Netzwerk zum Stillstand zu bringen, indem er durch erhöhten Datenverkehr die Ressourcen erschöpft. Ziel ist es, das System unerreichbar zu machen. [46].

Access-Angriff: Ziel ist es unautorisierten Zugang zum Netzwerk zu erhalten und Daten zu sammeln, um diese für weitere Angriffe zu nutzen [35].

Routing-Angriff: Ein Angreifer leitet die Kommunikation über einen bestimmten Kanal auf eine Ressource um die in seinem Besitzt oder unter seiner Kontrolle ist, um Daten abzugreifen. Der Sinkhole-Angriff zählt auch zu den Routing Angriffen [35].

Die Middleware-Ebene fungiert als eine Zwischenebene zwischen dem Netzwerk und der Anwendung. Sie stellt unter anderem Schnittstellen für Anwendungen, besteht aus persistentem Datenspeicher und stellt Systeme die Daten für die Anwendungsebene vorbereiten, z.B. mit Maschinellem Lernen. Technologien die in dieser und der Anwendungsebene Einsatz finden sind unter anderem Message Queuing Telemetry Transport (MQTT),

Advanced Message Queuing Protocol (AMQP) oder Constrained Application Protocol (COAP).

Man-In-The-Middle-Angriff: In IoT-Systemen kommt das MQTT-Protokoll zum Einsatz. Es arbeitet mit einem Publish-Subscribe-Modell und ein MQTT-Broker agiert als Proxy, wodurch Nachrichten ohne ein Ziel zu nennen versendet werden können. Ein Angreifer könnte versuchen den Broker unter seine Kontrolle zu bringen und somit auch die gesamte Kommunikation über MQTT[31].

SQL-Injection-Angriff: Bei einem SQL-Injection-Angriff fügt ein Angreifer böswillige SQL-Statements in Anwendungen um so an Daten aus einer Datenbank zu gelangen. Ziel ist es Daten abzugreifen, zu verändern oder zu löschen [31].

Signature-Wrapping-Angriff: Webservices nutzen Extensible Markup Language (XML)-Signaturen um bestimmte Elemente gegen unbefugten Zugriff abzusichern. Dabei werden nur die Elemente signiert. Ein Angreifer kann dies ausnutzen, indem er den signierten Wert verschiebt und einen bösartigen Wert an dessen Stelle einfügt. Die Signatur bleibt dabei erhalten und der Webservice führt die modifizierte Anfrage aus [33].

Cloud-Maleware-Injection: Ein Angreifer versucht ein von ihm modifizierten Service, Anwendung oder Virtuelle Maschine in die Cloud-Umgebung einzubringen. Sobald die Umgebung diese als valide ansieht, können Nutzer den manipulierten Service anfragen, ohne zu wissen, was dahinter steckt. Ebenso kann ein Angreifer versuchen einen Virus oder Trojaner in die Cloud-Umgebung einzuschleusen. Sobald dieser ausgeführt wird, kann der Virus sich ausbreiten und weitere Services oder die Hardware der Cloud infizieren [33].

Cloud-Flooding: Eine Charakteristik der Cloud ist es, dass sie skalierbar Ressourcen zur Verfügung stellt. Ein Angreifer kann mit einem Denial-of-Service-Angriff versuchen alle Ressourcen in Anspruch zu nehmen und so die Cloud-Umgebung überlasten, sodass kein Zugriff mehr möglich ist [33].

Die Anwendungsschicht ist die Schnittstelle zum Endnutzer. Der Nutzer kann entweder via Smartphone, Laptop oder Computer auf die Anwendungen zugreifen. Auf dieser Ebene treten einige Sicherheitsrisiken auf, die auf anderen Ebenen nicht auftreten, beispielsweise Datendiebstahl oder Datenschutzprobleme.

Phishing: Ein Angreifer versucht an personenbezogene Daten oder Authentifizierungsdaten zu gelangen. Das kann über eine modifizierte Webseite geschehen, oder durch eine E-Mail mit bösartigem Anhang bei dem ein Opfer getäuscht wird, um sensible Daten preiszugeben.

Access-Control: Ein Angreifer versucht, die Zugriffskontrollmechanismen einer Anwendung zu umgehen oder zu manipulieren, um Zugriff zu erlangen, oder seine Zugriffsberechtigungen zu erhöhen. Oder Zugriffsberechtigungen anderer Nutzer zu verringern [35].

Sniffing-Angriff: Ein Angreifer versucht über ein Sniffing-Tool Wissen über den Netzwerkverkehr zu erlangen, um so eventuelle sensible Daten abzugreifen die für weitere Angriffe missbraucht werden können [32].

Bösartige Skripte: Bösartige Skripte sind oft die Eintrittspunkte eines Angreifers. Durch Cross-Stie-Scripting versucht ein Angreifer ein bösartiges Skript in das System zu schleusen um Daten des Nutzers zu stehlen [32].

Reverse-Engineering: Ein Angreifer analysiert ein Gerät oder System um herauszufinden wie es funktioniert und welche Sicherheitsmechanismen es hat. Dies dient dazu mögliche Schwachstellen oder Sicherheitslücken zu identifizieren, die ausgenutzt werden können [32].

Abbildung 2.1 zeigt eine Übersicht der möglichen Angriffe und Bedrohungen gegenüber der einzelnen IoT-Ebenen.

2.1.2 Schwachstellen

Schwachstellen im Bereich IoT stellen eine bedeutende Herausforderung dar. Ihre Komplexität resultiert aus der Vielzahl heterogener Komponenten von unterschiedlichen Herstellern, die daran beteiligt sind. Hinzu kommen die vielen unterschiedlichen Technologien, die zum Einsatz kommen und Schwachstellen haben können. Ebenfalls können begrenzte Ressourcen wie Batteriekapazität, Datenübertragung und Gerätespeicherplatz Schwachstellen in IoT-Geräten verursachen.
Laut dem OWASP Internet-of-Things Projekt sind die folgenden Punkte die 10 häufigsten Schwachstellen [2]:

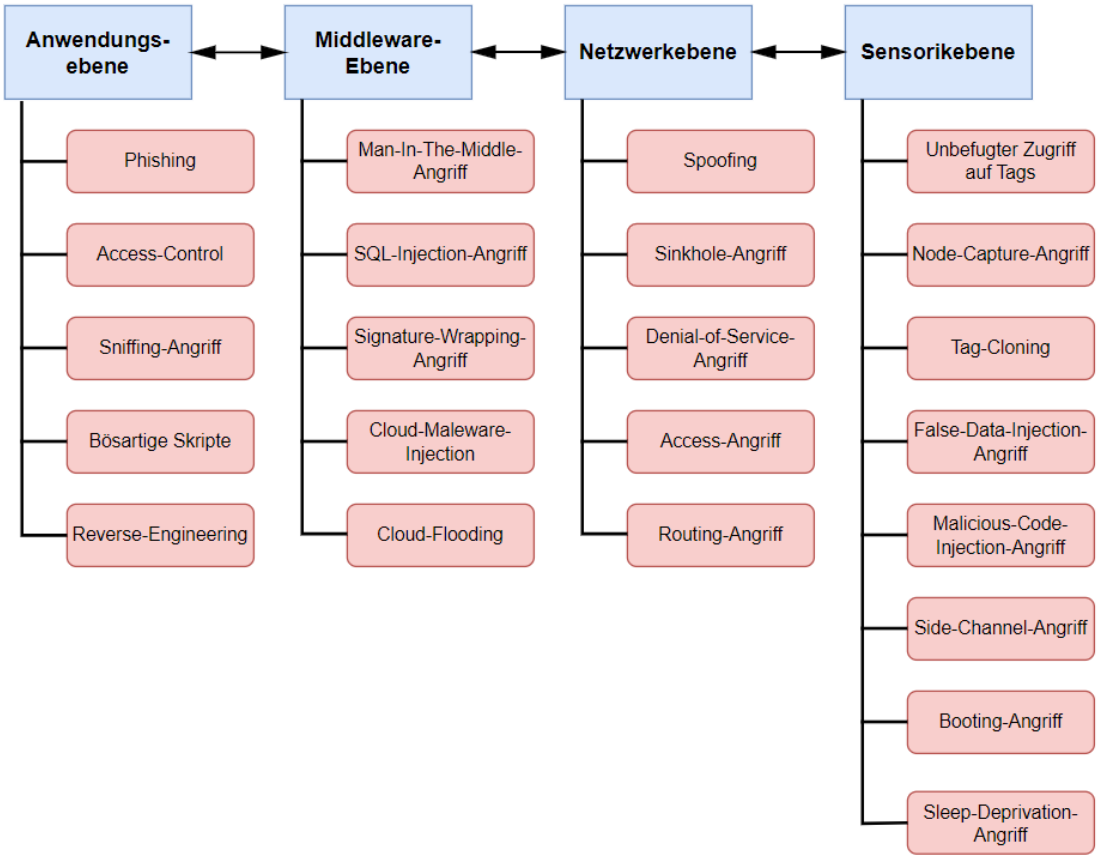

Abbildung 2.1: Zusammenfassung der möglichen Angriffe und Bedrohungen gegenüber IoT

1. **Passwörter** Schwache und leicht zu erratende Passwörter lassen sich durch Bruteforce-Angriffe herausfinden. Auch fest kodierte Passwörter werden nach Auslieferung des Gerätes oft nicht geändert.

2. **Netzwerkdienste** Unsichere Netzwerkdienste, die nicht abgeschaltet werden oder dem Internet ausgesetzt sind, sodass sie unbefugten Zugriff und das Abgreifen von Daten ermöglichen.

3. **Schnittstellen** Webanwendungen, Cloud-Anwendungen oder mobile Anwendungen nutzen Schnittstellen. Oftmals mit fehlender Authentifizierung, Autorisierung, sowie schwache Verschlüsselungsalgorithmen und fehlende Eingabe - und Ausgabefilter.

4. **Updates** Viele IoT-Geräte erhalten keine oder unregelmäßige Sicherheitsupdates. Hierzu zählt auch der Mangel an Validierung der Firmware bei einem Firmwareupdate, oder Rollback-Mechanismen.

5. **Privatsphäre** Mangelnder Schutz der Privatsphäre bezieht sich auf den Schutz sensibler und privater Daten, die über den Nutzer oder die Nutzerin gespeichert werden.

6. **Datenübertragung** Fehlende oder unzureichende Zugriffskontrolle oder Verschlüsselung von Daten, kann zu unsicherer Datenübertragung und Speicherung führen.

7. **Geräte-Management** Darunter fallen unterschiedliche Services, wie die Asset-Management, Update-Management, Systemüberwachung, Reaktionsmöglichkeiten oder Außerbetriebnahme eines Gerätes.

8. **Standardeinstellungen** Geräte die mit Standardeinstellung ausgeliefert werden und verhindert wird, dass diese und weitere Konfigurationen angepasst oder verändert werden können.

9. **physische Absicherung** Manipulationen an Hardware, Diebstahl oder die Installation von bösartigen Geräten können die Integrität und Sicherheit der IoT-Infrastruktur gefährden.

2.2 Anforderungen an IoT-Sicherheit

Durch die Verbreitung von IoT-Systemen, ihre Heterogenität und Interkonnektivität ihrer Netze entstehen neue Anforderungen an die Sicherheit. Diese beziehen sich auf Authentifizierung, Zugriffs - und Identitätsmanagement, Netzwerksicherheit und sichere Kommunikation, Datensicherheit und Datenschutz, sowie auf Ausfallsicherheit und Wiederherstellung. Jede dieser Anforderungen muss auf den verschiedenen Ebenen berücksichtigt werden, um die Sicherheitsanforderungen zu erfüllen. Auch finden manche Mechanismen sich mehrfach in den Anforderungen wieder. Es gilt zu beachten, dass sich einige Mechanismen in verschiedenen Bereichen wiederholen. Zum Beispiel trägt Verschlüsselung nicht nur zur Netzwerksicherheit bei, sondern auch zur Datensicherheit.

2.2.1 Geräteauthentifizierung und Zugriffskontrolle

Durch die Besonderheit der ad-hoc Netzwerke von IoT-Systemen und der Peer-to-Peer-Verbindung der einzelnen Geräte, stellt Authentifizierung der Geräte, Zugriffskontrolle und Trust-Management eine besondere Herausforderung dar. Nicht nur die Nutzer müssen sich bei den Anwendungen authentifizieren, auch die Geräte müssen sich untereinander authentifizieren und identifizieren. Dies dient zur Legitimation der übertragenen Daten und Anfragen [35]. Herkömmliche Methoden sind oft zu komplex, da sie z.B. rechenintensive kryptografische Berechnungen erfordern, um Verschlüsselung und Entschlüsselung durchzuführen. Weshalb leichtgewichtige Authentifizierungsverfahren erforderlich sind.
Beim Trust-Management geht es um das Vertrauen zwischen interagierenden Identitäten und Objekten. Hierbei werden Technologien verwendet, die bei der Authentifizierung von Daten und Geräten unterstützen. Kryptografische Algorithmen und Protokolle sind unerlässlich. Ebenfalls übernimmt das Trust-Management die Verwaltung von Schlüsseln und Zertifikaten, die für die Authentifizierung erforderlich sind, einschließlich deren Erzeugung, Aktualisierung und Zurückweisung [32]. Zugriffskontrolle bezieht sich auf die Erlaubnis zur Nutzung spezifischer Ressourcen im System. Der Hauptaugenmerk der Zugriffskontrolle liegt auf der Regelung der Zugriffsberechtigung für Nutzer und Objekte. Angesichts des potenziell hohen Bedarfs an Rechenleistung und Speicherplatz könnten Mechanismen möglicherweise in die Cloud verlagert werden. Zudem gestaltet sich die Suche nach einer universellen Lösung aufgrund der Heterogenität der IoT-Systeme als nicht trivial. Werden die Charakteristiken von IoT-Geräten betrachtet, so wird klar, dass entsprechende Zugriffsmechansimen einfach und skalierbar gehalten werden müssen. Ebenfalls sollten sie ein ausgeglichenes Maß an Identitäts- und Datenschutzmanagement bieten, sowie nach dem Prinzip der geringsten Privilegien arbeiten [6].

2.2.2 Netzwerksicherheit und Integrität

Es existieren zwei wesentliche Verbindungstypen: die Kommunikation zwischen den Geräten selbst sowie die Verbindung eines Geräts mit einem Nutzer oder einer Nutzerin. Dabei erstrecken sich die Geräte über ein Netzwerk, welches aus unterschiedlichen Arten von Netzwerkinfrastruktur besteht. Dies schließt drahtlose Kommunikation, kabelgebundene Verbindungen sowie öffentliche oder private Netzwerke ein.
Ein wichtiger Faktor ist die Ende-zu-Ende Verschlüsselung. Kommunikationsprotokolle

wie IPv6 over Low power Wireless Personal Area Network (6LoWPAN) und IPv6 sind leichtgewichtige Protokolle die im IoT-Bereich Anwendung finden und eine solche Form der Verschlüsselungen mit sich bringen [30].
Wie auch in normalen Netzwerken, kann es für IoT-Netzwerke hilfreich sein Firewalls oder Intrusion-Detection-Systeme für die Filterung des Netzwerkverkehrs einzusetzen. Jedoch haben solche Ansätze oft Schwierigkeiten bei der Erkennung von ungewöhnlichem Datenverkehr in einem IoT-System. Ebenso können Techniken zur Regulierung der Übertragungsrate zur Netzwerksicherheit beitragen, indem sie Latenzen optimieren und eine rechtzeitige Erkennung bei Überlastung ermöglichen [32]. Generell erhöht die Integration angemessener Mechanismen zur Erkennung von Bedrohungen die Netzwerksicherheit erheblich. Ebenso trägt die Implementierung geeigneter Verschlüsselungssysteme, auch Wahrung der Datenintegrität bei. Letzteres lässt sich ebenfalls durch Fehlererkennung auf den einzelnen Geräten selbst realisieren. Leichtgewichtige Mechanismen, wie Cyclic Redundancy Checks (CRC) oder Prüfsummen können hier zum Einsatz kommen [8].

2.2.3 Datensicherheit und Datenschutz

IoT-Geräte generieren, sammeln und übertragen eine Menge Daten. Darunter befinden sich auch sensible Informationen über einen Nutzer, eine Nutzerin, oder auch der Standort des Gerätes. Dabei durchlaufen die Daten drei Phasen. 1) Datensammlung, 2) Datenzusammenführung und 3) Datenextration und -Analyse. Um die Sicherheit der Information zu wahren kommen in den drei Phasen verschiedene Mechanismen zum Einsatz, wie Verschlüsselung. Bei der Datenzusammenführung werden Mechanismen zur Anonymisierung oder Verschlüsselung eingesetzt. Jedoch lassen sich auch hier keine Standardtechnologien einsetzen, da die Durchführung von Verschlüsselung und Entschlüsselung rechenintensiv sein kann. Dies kann die begrenzte Energiekapazität eines IoT-Geräts schnell erschöpfen und die Batterielaufzeit erheblich verkürzen. Ebenfalls kann der Kommunikationsaufwand zur Vereinbarung der Sicherheitsparameter problematisch sein, da IoT-Geräte sich oft in Umgebungen mit eingeschränkter Netzwerkkapazität arbeiten [32].

2.2.4 Ausfallsicherheit und Wiederherstellbarkeit

Da IoT-Geräte an verschiedenen Orten platziert sein können, müssen sie auch vor physischen Angriffen geschützt werden. Die Daten der Geräte müssen zu jeder Zeit bereit

stehen, um die Funktionen aufrecht zu erhalten. Dabei bedarf es bestimmten Mechanismen um Übertragungswege und Dienste nach ihrer Robustheit auszuwählen. Ebenso bedarf es Mechanismen zur Wiederherstellung des Systems nach einem Ausfall [60].
Die Robustheit erstreckt sich jedoch nicht nur auf der Ebene der Sensorik, sondern zieht sich durch alle Ebenen. Ein implementierter Mechanismus in diesem Zusammenhang ist die partitionstolerante Redundanz. Auf diese Weise können Daten, die in der Cloud verarbeitet werden, gleichzeitig auf Edge-Knoten gespeichert und bei Bedarf auch dort verarbeitet werden. Ein weiterer Mechanismus zur Ausfallsicherheit ist das kontinuierliche Überwachen der Systemressourcen, um Ausfälle rechtzeitig zu erkennen oder zu verhindern. Mechanismen zur Wiederherstellbarkeit zielen darauf ab, dass System in seinen funktionalen Zustand zurück zu versetzen. Ein möglicher Ansatz besteht darin, Anwendungen periodisch Kontrollpunkte erstellen zu lassen, was eine Wiederherstellung zu einem früheren Zustand ermöglicht [16].

2.3 Sicherheitsanalysen im Kontext IoT

Sicherheitsanalysen im Bereich IoT sind essenziell, um die vielfältigen und sich stetig weiterentwickelnden Sicherheitsherausforderungen zu bewältigen. Sie ermöglichen die Identifikation von Schwachstellen, Bedrohungen und Risiken, um angemessene Schutzmaßnahmen zu entwickeln und sicherzustellen, dass die Integrität, Vertraulichkeit und Verfügbarkeit der Systeme und Daten gewahrt bleiben.
Angreifer können Sicherheitslücken ausnutzen, um die Geräte unter ihre Kontrolle zu bringen, oder die sensiblen Daten abzugreifen. Viele der durchgeführten und aufgedeckten Angriffe auf IoT-Geräte wurden nur durch Zufall entdeckt. Um dem entgegen zu wirken, sollte während der Entwicklung eine systematische Sicherheitsanalyse durchgeführt werden. Jedoch lassen sich die gängigen Methoden zur Sicherheitsanalyse schwer auf IoT-Systeme abbilden. Diese Methoden haben Schwierigkeiten, die komplexen Beziehungen und Abläufe innerhalb des Systems adäquat abzubilden, und berücksichtigen nur unzureichend die Vielfalt und Dynamik, die in diesen Systemen herrscht.
Es gibt mehr Forschungsarbeiten die sich mit einem Teilaspekt befassen als solche, die das System gesamtheitlich betrachten. Zamfir et al., 2016 [70] befassten sich mit den Sicherheitsherausforderungen der standardisierten Kommunikationsprotokolle MQTT und COAP. Rahman et al., 2016 [48] befassten sich mit den IoT-Protokollen 802.15.4, 6LoWPAN und Routing Protocol for Low power and Lossy Networks (RPL) und analysierten deren Sicherheitsprobleme. Anschließend haben sie COAP umfassender analysiert und sich

mit dessen Sicherheitsstatus und dem Einsatz von Datagram Transport Layer Security (DTLS) beschäftigt. Marksteiner et al., 2017 [42] haben sich mit den gängigen Protokollen im Bereich Smart-Home befasst, die Sicherheitsmerkmale hervorgehoben und miteinander verglichen.
Neben Analysen die sich mit den Protokollen befassen gibt es auch Arbeiten, die sich auf die Schwachstellenanalyse fokussieren. Die Arbeit von Xie et al., 2017 [63] beschäftigt sich mit den Methoden zur Erkennung von Schwachstellen in IoT-Firmware. Dabei gehen sie auf die statische Analyse, Fuzzing, symbolische Ausführung und umfangreiches Testen ein. Ebenfalls behandelt die Arbeit von Feng et al., 2023 [26], die Identifizierung von Schwachstellen in der IoT-Firmware. Eceiza et al., 2021 [21] untersuchen Fuzzing-Techniken zur Aufdeckung von Schwachstellen und beleuchten deren Anwendbarkeit insbesondere im Kontext des IoT. Eine weitere Methode der Sicherheitsanalyse ist die Bedrohungsanalyse. Die Arbeit von Omotosho et al., 2019 [44] befasst sich mit der Bedrohungsmodellierung von IoT-Geräten im Gesundheitsbereich. Dabei werden die Bedrohungen mit Hilfe des Spoofing, Tampering, Repudiation,Information disclosure, Denial of Service, Elevation of Privileges (STRIDE)-Modells identifiziert und mit dem Risiko-Bewertungsmodell DREAD eingestuft. Salzillo et al., 2021 [53] befassen sich mit der Bredohungsanalyse des MQTT-Protokoll und einem anschließend geplanten Penetrationstest. Eine weitere Arbeit die sich mit der Bedrohungsanalyse im Bereich IoT befasst ist die von Atamli et al., 2014[12], die auf der Grundlage von IoT-Anwendungsfällen basiert. Asif et al., 2021 [12] erstellen eine Bedrohungsanalyse auf Komponentenebene für die Landwirtschaftliche Infrastruktur mit Hilfe von STRIDE. Der Beitrag von Wolf et al., 2021 [62] stellt einen Ansatz zur Bedrohungsanalyse mit Hilfe des PASTA-Modells vor.
Zusätzlich zur Untersuchung bestimmter Protokolle sowie der Analyse von Schwachstellen und Bedrohungen beschäftigt sich die Forschung auch mit der genauen Betrachtung ausgewählter IoT-Geräte, wie in den Arbeiten von [50] und [67] ersichtlich ist.
In dem folgenden Kapitel wird auch die Risiken von Sicherheitslücken in IoT-Geräten und deren Einsatzgebieten eingegangen, sowie auf die Relevanz von Sicherheitsanalysen zur Identifikation von Schwachstellen. Anschließend wird die Vorgehensweise, mit Fokus auf der Bedrohungsanalyse und Schwachstellenanalyse, beschrieben, sowie auf die besondere Bedeutung von Penetrationstest eingegangen.

2.3.1 Risiken von Sicherheitslücken

Sicherheitslücken in den IoT-Geräten können schwerwiegende Folgen haben. Angreifer können Daten entwenden und Identitätsdiebstahl begehen. Zudem könnten sie Nutzer und Nutzerinnen sowie Unternehmen erpressen oder die gestohlenen Daten missbrauchen.
Im medizinischen Bereich werden IoT-Geräte zum Beispiel zur Überwachung und Versorgung von Patienten eingesetzt. Eine Sicherheitslücke in diesen Geräten kann dafür sorgen, dass Anweisungen zum Stoppen des Gerätes gesendet werden. Es wäre gefährlich, ein medizinisches Gerät abzuschalten, welches für den Patienten lebensnotwendig ist, wie z.B. ein Herzschrittmacher [47]. Eine Besonderheit bei IoT-Geräten ist, dass sie auch physischen Sicherheitslücken ausgesetzt sein können, da sie auch in kritischen Infrastrukturen, wie Energieversorgungsnetze eingesetzt werden. Diese sorgen für eine effizientere und an den Verbrauch angepasste Versorgung und dienen zur Integration erneuerbarer Energien. Ein Eindringen in das Versorgungsnetz kann zur Folge haben, dass es komplett ausfällt und somit wirtschaftlichen und physischen Schaden anrichten. Durch die Sammlung der Daten können Aktivitätsmuster der Menschen erstellt werden und durch die Manipulation von Daten können Abrechnungen verfälscht werden [58].
Im privaten Bereich werden Geräte oft zur Verbesserung des Komforts eingesetzt. Risiken von Sicherheitslücken können hier Auswirkungen auf die Privatsphäre haben, oder aber auch physischer Natur sein. So können Angreifer Türschlösser manipulieren und in Häuser einbrechen, oder durch intelligente Kameras das Haus ausspähen. Auch lassen sich Mikrowellen oder Herde durch Manipulation in Brand setzten [27].
Neben Angriffen die in den Anwendungsbereichen von IoT-Geräten auftreten können, können die IoT-Geräte auch für Netzwerkangriffe oder Botnetze zweckentfremdet werden. Eines der bekanntesten Beispiele ist das Mirai-Botnetz, welches nach Sicherheitslücken in den Geräten sucht, um dann Schadcode aufzuspielen und diese anschließend für Denial-Of-Service-Angriffe zu missbrauchen [34].

2.3.2 Relevanz von Sicherheitsanalysen zur Identifikation von Schwachstellen

Sicherheitsanalysen beziehen sich auf die Untersuchung und Bewertung von Sicherheitsaspekten. Sie dienen dazu Risiken, potenzielle Schwachstellen und Bedrohungen zu identifizieren, um anschließend angemessene Sicherheitsmaßnahmen zu entwickeln und anzu-

wenden.
Da IoT-Geräte oft miteinander und mit dem Internet verbunden sind, sowie auch in kritischen Infrastrukturen eingesetzt werden, sind sie anfällig für die verschiedensten Sicherheitsprobleme. Umso wichtiger ist es daher Sicherheitsanalysen durchzuführen.
Die Identifizierung von Schwachstellen in der Entwicklungsphase ermöglicht es den Herstellern und Entwicklern rechtzeitig geeignete Gegenmaßnahmen zu ergreifen, um die Sicherheit vor Auslieferung zu verbessern. Ebenfalls lässt sich durch Sicherheitsanalysen der Schutz vor Angriffen verbessern.Dabei werden mögliche Angriffsvektoren erkannt und bewertet. Dies kann von der Abwehr unbefugter Zugriffe über die Absicherung der Kommunikation bis hin zur Identifikation und Implementierung von Abwehrmechanismen gegen Angriffe reichen. Durch die große Menge an Daten, die durch die Geräte erfasst werden, kann die Sicherheitsanalyse dazu beitragen, diese angemessen zu schützen. Durch Identifizierung von Risiken und Implementierung geeigneter Maßnahmen kann der Missbrauch von persönlichen und sensiblen Daten verhindert werden, sowie die Integrität geschützt werden. Neben den zuvor genannten Punkten unterstützt die Sicherheitsanalyse auch die Einhaltung von Standards und Sicherheitsvorschriften. Dies ist besonders in Branchen wie dem Gesundheitswesen, der Automobilindustrie oder kritischen Infrastrukturen von großer Bedeutung, um den Schutz von Nutzern und Nutzerinnen zu gewährleisten.[13]

2.3.3 Vorgehensweisen

Bei dem Vorgehen von Sicherheitsanalysen im Bereich IoT gibt es keine klar definierte Vorgehensweise. Die Tatsache, dass zahlreiche unterschiedliche Komponenten und Technologien zu einem IoT-Gerät gehören, erschwert es IoT-Geräte eine umfassende Analyse für das gesamte IoT-Gerät durchzuführen. Da es unterschiedliche Herangehensweisen an eine Sicherheitsanalyse gibt, wird im Folgenden auf Methoden in der Schwachstellen- und Bedrohungsanalyse eingegangen.

Schwachstellenanalyse Diese soll helfen Schwachstellen im System, einem Netzwerk oder der Anwendung zu identifizieren, zu messen und anschließend auf Grundlage des Risikos, das sie darstellen zu klassifizieren. Zu Anfang wird immer der Umfang des zu Analysierenden Assets definiert. Dabei handelt es sich um physische oder virtuelle Komponenten, Ressourcen oder Entitäten innerhalb des IoT-Ökosystems, die eine Wertigkeit oder Bedeutung in Bezug auf die Funktionalität, die Daten oder die Dienste des Systems haben. Anschließend werden weitere

wichtige Informationen zusammengetragen. Dabei konzentriert sich die Schwachstellenanalyse auf Softwarekomponenten wie Firmware oder Anwendungen, sowie auf den Netzwerkprotokollen. In Abhängigkeit davon, ob sich das Asset auf der Anwendungs-, Middleware-, Netzwerk- oder Sensor-Ebene befindet, erweisen sich bestimmte Methoden als geeigneter für die Analyse. Des Weiteren kann die Analyse in passive und aktive Ansätze unterteilt werden. Bei der passiven Schwachstellenanalyse werden systemspezifische Merkmale mit Schwachstellen in einschlägigen Datenbanken verglichen, wie der National Vulnerability Database (NVD) von National Institute of Standards and Technology. Die Aktive hingegen untersucht Geräte aktiv. Darunter fallen Port-Scans, Überwachung des Netzwerkverkehrs, SQL Injection etc. Hierfür gibt es eine Vielzahl von Open-Source-Tools die als Unterstützung dienen (Nmap, Burpesuite, Kali Linux etc.) [54].
Angriffsgraphen finden Anwendung bei der Schwachstellenanalyse von vernetzten Systemen. Dabei werden Informationen über Schwachstellen der einzelnen Hosts gesammelt und in Verbindung mit den Netzwerkinformationen werden Angriffsgraphen erstellt. Dabei kann in einen zustandsbasierten Graphen und einem Exploit abhängigen Graphen unterschieden werden. Die Graphen sollen dabei helfen Ressourcen aufzudecken die kompromittiert werden können, und potenzielle Angriffswege aufzudecken [23].
Eine sehr effektive Methode in der Schwachstellenanalyse ist das Fuzzing. Dabei handelt es sich um eine automatisierte Testtechnik, die darauf abzielt, Schwachstellen in Software durch Einfügen spezieller, unerwarteten und zufälliger Eingaben zu identifizieren. Die Eingaben sollen unerwartetes Verhalten hervorrufen und so Schwachstellen aufdecken. Der Prozess wird meist durch ein automatisiertes Fuzzing-Tool durchgeführt, welches den Prozess überwacht und anschließend auswertet [22].
Aufgrund potenzieller Schwachstellen in der Hardware von IoT-Geräten ist die Analyse in einer speziellen Testumgebung angebracht. Darüber hinaus eignen sich Testumgebungen auch für die Verhaltensanalyse, insbesondere wenn sie simuliert oder virtuell sind. In Testumgebung ist es möglich, die Analyse unter kontrollierten Konditionen durchzuführen, was die Simulation und Überwachung verschiedener Szenarien ermöglicht [7]. Auch in der Schwachstellenanalyse kommt Maschinelles Lernen bzw. Künstliche Intelligenz zum Einsatz. Angesichts der enormen Datenmenge, die von IoT-Geräten erzeugt wird, stellen sie einen idealen Lern-Datensatz dar. Es kann dabei zur Identifikation von Anomalien, zur Erkennung von wiederkehrenden Mustern und zur Prognose von spezifischen Werten verwendet werden, die poten-

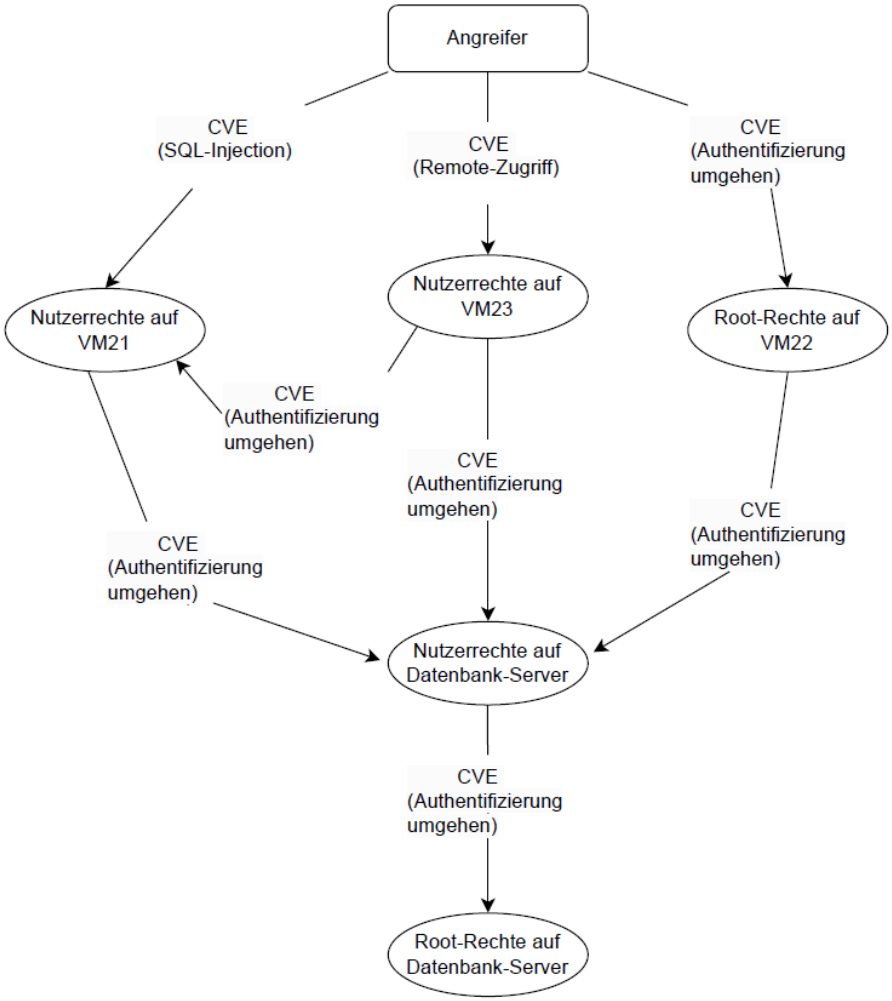

Abbildung 2.2: Angriffsgraph eines Angriffs auf einen Datenbank-Server

zielle Schwachstellen verursachen könnten [7]. Zur Erkennung von Schwachstellen in Anwendungen oder der Firmware, können sowohl statische als auch dynamische Analysen eingesetzt werden. Die statische Analyse bezieht sich auf die Analyse des Quellcodes, Binärdateien oder Dokumentationen, ohne dass das Programm dabei ausgeführt wird. Dabei wird der Code auf bestimmte Muster, Konstrukte oder bekannte Schwachstellen geprüft. Bei der dynamischen Analyse wird die Software während der Laufzeit überprüft, oder bei Ausführung bestimmter Testszenarien [69]. Mithilfe von Honeypots werden gezielt Angreifer angelockt, um deren Vorgehensweise und die von ihnen gewählten Pfade nachzuvollziehen. Hierbei wird ein

IoT-Gerät simuliert und bewusst als attraktives Ziel für einen Angreifer gestaltet. Dadurch können Angriffe analysiert werden und etwaige Schwachstellen frühzeitig erkannt werden[7]. Eine weitere Methode zur Schwachstellenanalyse ist der Penetrationtest. Dieser wird in Kapitel 2.3.4 genauer erläutert.

Bedrohungsanalyse Potenzielle Schwachstellen, über die ein IoT-Gerät kompromittiert werden kann, werden Angriffsflächen genannt. Diese können sich sowohl in der Hardware als auch der Software befinden und betreffen auch die drahtlose Kommunikation. Je mehr Angriffsflächen ein Gerät bietet, desto höher die Wahrscheinlichkeit einer Kompromittierung. Eine Angriffsfläche ist mit einem bestimmten Risiko, einer Wahrscheinlichkeit und einer Auswirkung verbunden. Im Wesentlichen handelt es sich um Bedrohungen, die das Potenzial haben, ein Gerät negativ zu beeinflussen. Die Bedrohungsanalyse, oder auch Bedrohungsmodellierung soll dabei helfen alle Angriffsflächen aufzudecken. Dabei werden die Bedrohungen identifiziert, klassifiziert und bewertet [55].
Die Bedrohungsanalyse beginnt immer mit der Identifikation des Assets. Das können zu schützende Daten oder Informationen sein, oder Ressourcen die es zu schützen gilt. Als nächstes erfolgt eine Architekturübersicht des IoT-Gerätes. Dabei werden die Funktionalitäten sowie Anwendungen, aber auch die physische Architektur dokumentiert. Ein Verständnis dafür zu entwickeln, wie und über welche Kanäle Daten übertragen werden und welche Technologien eingesetzt werden, kann dazu beitragen, potenzielle Angriffsvektoren und Angriffsmöglichkeiten auf das Gerät zu erkennen. Darauf folgt eine Zerlegung des IoT-Gerätes hinsichtlich der einzelnen Komponenten. Das Ziel ist es, die Begrenzungen und Schnittstellen zu erkennen, um potenzielle Eintrittspunkte für Angriffe zu identifizieren. Im Anschluss an die Analyse des Datenflusses und der Identifizierung potenzieller Eintrittspunkte besteht die Aufgabe darin, die damit verbundenen Gefahren zu erkennen. Dabei können Modelle wie STRIDE, Process for Attack Simulation and Threat Analysis (PASTA), Common Vulnerability Scoring System (CVSS) oder Angriffsbäume hilfreich sein, um diese Gefahren zu identifizieren. Angriffsbäume helfen dabei, das Gesamtbild eines Angriffes zu erfassen, indem eine Abfolge von Schritten und Aktionen dargelegt wird, die ein Angreifer unternehmen könnte, um an sein Ziel zu gelangen. Im nächsten Schritt werden die ermittelten Bedrohungen dokumentiert, wobei eine umfassende Beschreibung der Bedrohungen, ihrer Ziele, der verwendeten Angriffstechniken und möglicher Gegenmaßnahmen erfolgt. Der abschließende Schritt

umfasst die Bewertung der Bedrohungen hinsichtlich ihrer Wahrscheinlichkeit und potenziellen Auswirkungen. Bewertungssysteme wie Damage, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD) können hierbei unterstützend eingesetzt werden [29].

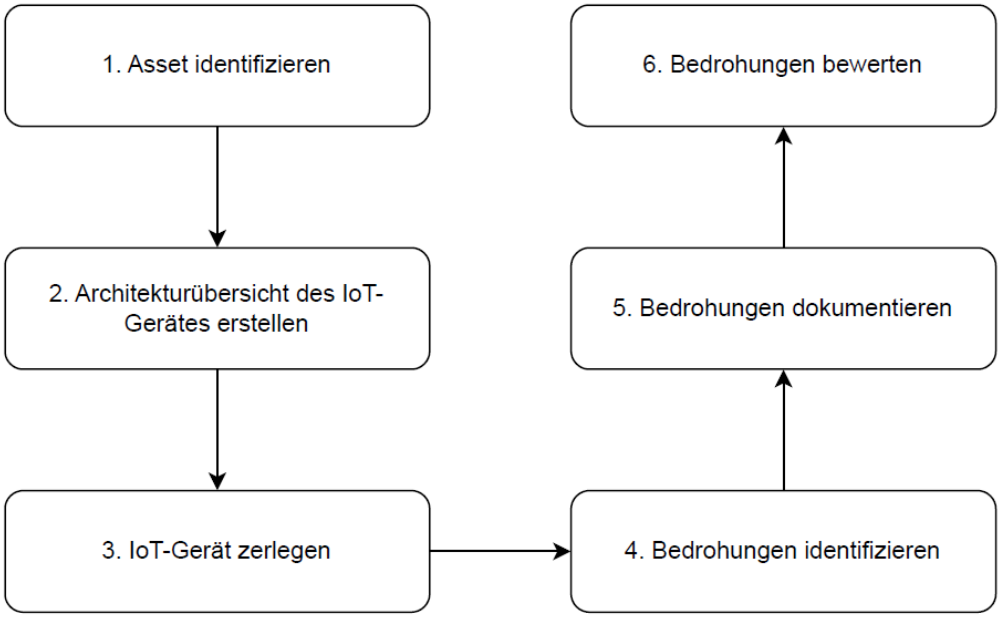

Abbildung 2.3: Prozessschritte der Bedrohungsanalyse [29]

Das von Microsoft entwickelte STRIDE-Modell unterteilt die Gefahren in sechs Kategorien. STRIDE steht dabei für:

Spoofing: Der Versuch durch eine falsche Identität Zugang zu einem System zu erlangen. Dies kann entweder durch gestohlene Zugangsdaten erfolgen, oder durch falsche IP-Adressen.

Tampering: Die unbefugte Veränderung von Daten.

Repudiaton: Die Möglichkeit von Nutzern, rechtmäßig oder unrechtmäßig, bestimmte Aktionen oder Transaktionen abzustreiten.

Information disclosure: Die unerwünschte Offenlegung von Daten. Dabei kann jede Information für den Angreifer von Nutzen sein.

Denial of Service: Der Prozess der Nichtverfügbarkeit eines Systems oder eine Anwendung.

Elevation of privilege: Die Übernahme von höheren privilegierten Zugriffsrechten.

Das PASTA-Framework wurde entwickelt, um die bestehenden Lücken zwischen der Geschäftslogik und den technischen Risiken zu füllen. Dabei beinhaltet die Bedrohungsmodellierung verschiedene Abstraktionsebenen, die sowohl höhere Ebenen wie die Geschäftslogik als auch die tieferen Ebenen wie konkrete Angriffsvektoren einschließt. Insbesondere im IoT-Bereich ist ein umfassendes Verständnis der abstrakten Systemarchitektur und der zugrunde liegenden Geschäftsziele unerlässlich. Eine weitere Methode ist das Modellieren von Angriffsbäumen. Dabei stellt die Wurzel den Grund des Angriffs dar. Die Blätter bilden die verschiedenen Möglichkeiten ab, diesen auszuführen. Dafür wird jedes zu schützende Asset in mehrere diskrete Wurzeln abgebildet. Durch die Zerlegung eines Angriffs in einzelne Schritte ermöglicht ein Angriffsbaum die Identifizierung von potenziellen Schwachstellen, die in jedem Schritt ausgenutzt werden könnten. Ebenso bieten sie eine Möglichkeit komplexe Angriffszenarien zu visualisieren[62].
Bei CVSS handelt es sich um eine Methode der zur Bewertung der Gefahren. Dabei wird mit einem nummerischen Bewertungssystem gearbeitet, um den Schweregrad der Bedrohung, basierend auf einer Schwachstellenanalyse, zu klassifizieren. Die erste Gruppe umfasst die Basis, die in sechs Unterbereiche geteilt ist und bewertet die Eigenschaften einer Schwachstelle bezüglich der Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit. Die zweite Gruppe ist zeitlich ausgerichtet und beinhaltet drei Unterbereiche. Diese richtet sich an den zeitlichen Kontext und die aktuelle Situation, in der die Schwachstelle bewertet wird. Die dritte Gruppe ist umweltbezogen und besteht aus fünf Bereichen, welche sich auf die Umgebung, in der die Schwachstelle auftritt fokussiert [62].
Das DREAD-Bewertungssystem geht von 1 - 3, wobei 1 für ein niedriges Risiko steht, 2 für ein mittleres Risiko und 3 für ein hohe Risiko [29]. DREAD steht für

Damage potentioal: Die Höhe des Schadens, bei einem erfolgreichen Angriff.

Reproducibility: Die Wahrscheinlichkeit einen Angriff nachstellen zu können.

Exploitability: Die Wahrscheinlichkeit einen Angriff auszuführen.

Affected users: Die grobe Anzahl der betroffenen Nutzer, bei einem erfolgreichen Angriff.

Discoverability: Die Wahrscheinlichkeit eine Schwachstelle ausfindig zu machen.

Sowohl bei der Schwachstellenanalyse als auch bei der Bedrohungsanalyse für IoT-Geräte gibt es keine state-of-the-Art Methode. Es ist wichtig hierbei eine auf das Gerät angepasste und sinnvolle Methode auszuwählen. Neben den zuvor beschriebenen Analysen gibt es noch die Penetrationstest, die ebenfalls eine wichtige Rolle in der Sicherheitsanalyse einnehmen. Diese wird im Folgenden beschrieben.

2.3.4 Bedeutung von Penetrationstest

Ein Penetrationstest, oft als "Pen-Testäbgekürzt, ist eine proaktive Sicherheitsmaßnahme, bei der versucht wird die Schwachstellen und Sicherheitslücken zu identifizieren, indem simulierte Angriffe und Angriffsszenarien durchgeführt werden. Dabei werden verschiedene Techniken und Tools eingesetzt. Anders als bei herkömmlichen Pen-Test müssen im IoT-Bereich mehrere Komponenten betrachtet werden. Dies bezieht sich auf das Gerät selbst, sowie auf die Kommunikation und Anwendungen. Die Abbildung 2.4 zeigt den Ablauf eines Pen-Tests.

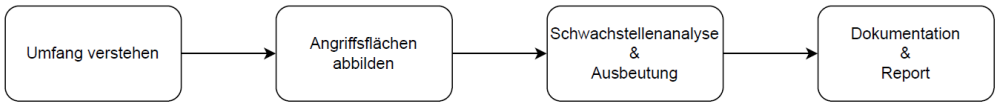

Abbildung 2.4: Ablauf eines Penetration-Tests aus [28]

Zu Beginn muss der Umfang des Pen-Test festgelegt werden. Das beinhaltet den zeitlichen Rahmen, sowie die Umgebung in der dieser stattfinden soll. Ebenso wird hier festgelegt, ob es sich um einen White-Box-Test handelt, also alle Informationen zur Architektur, Netzwerkdiagramm, Technologien etc. offen liegen. Ob es sich um einen Black-Box-Test handelt, bei dem keine Informationen vorhanden sind. Oder ob es sich um einen Grey-Box-Test handelt, bei dem nur einige wenige Informationen zur Verfügung stehen. Die Besonderheit des Pen-Tests von IoT-Geräten besteht außerdem darin, dass eventuell

mehrere Geräte bereitgestellt werden müssen, da auch die Hardware, wie Mikrocontroller oder Chips getestet werden und diese unter Umständen nicht reparable Schäden durch das Testen erleiden. Nachdem der Umfang definiert wurde, werden die Angriffsflächen des zu testenden Objektes abgebildet.
Dabei werden alle möglichen Eintrittspunkte, die ein Angreifer ausnutzen kann, herausgearbeitet. Hierfür ist es besonders wichtig, alle Informationen über das Gerät zu sammeln, von der Architektur des Chips, zu Kommunikationsprotokollen, Schnittstellen, dem Firmware-Update Prozess bis hin zur verwendeten Hardware, mobilen Anwendungen, Cloud-Anwendungen und Web-Anwendungen.
IoT-Geräte lassen sich für einen Pen-Test in Embedded System, Firmware und Software und Kommunikation unterteilen. Bei dem Embedded System handelt es sich um das "Ding", welches für die Datensammlung, -analyse und -verarbeitung zuständig ist. Um die Angriffsflächen herauszufinden, gilt es sich zu Fragen welche Funktionen das Gerät hat und zu welchen Informationen es Zugriff hat. Firmware und Software stellen die Softwareseite Komponenten des IoT-Geräts dar. Dies umfasst nicht nur die Firmware selbst, sondern auch mobile und Cloud-Anwendungen. Besonders wichtig sind hierfür die API's und den von den Anwendungen verarbeiteten Daten zu. Die Angriffsflächen konzentrieren sich insbesondere auf die Anwendungen selbst. Bei der letzten Sektion handelt es sich um die Kommunikation zwischen den Geräten und den Anwendungen. Das beinhaltet Kommunikationsprotokolle. Im Bereich IoT sind dies unter anderem Representational State Transfer (REST), Simple Object Access Protocol (SOAP), COAP MQTT, BLE, 6LoWPAN, WiFi, Z-Wave oder ZigBee. Je nach Protokoll bedarf es bestimmter Hardware um Tests durchzuführen. Bei der Kommunikation der IoT-Geräte ist es wichtig zu verstehen, welche Protokolle von welchen Komponenten genutzt werden. Auch ist die Kopplung von Geräten ein wichtiger Punkt. Dabei ist zu klären, wie diese erfolgt, welches Gerät sie initiiert und auf welchen Frequenzen die Geräte senden und empfangen.
Ziel der Abbildung von Angriffsflächen ist es, visuell darzustellen, wo und wie potenzielle Schwachstellen und Angriffspunkte in einem System oder einer Anwendung existieren. In diesem Schritt bietet es Vorteile, sich in die Denkweise eines potenziellen Angreifers zu versetzen. Wie in Kapitel 2.1.2 erwähnt können Schwachstellen in IoT-Geräten unterschiedliche Ursachen haben. Daher ist ein Penetration-Test eine geeignete Methode Schwachstellen ausfindig zu machen. [29]

3 Forschungsmethode

Dieses Kapitel befasst sich mit der Forschungsmethode der SLR. Ziel ist es die zuvor formulierten Forschungsfragen sorgfältig und konkret zu beantworten. Durch eine umfassende Analyse, basierend auf den gesammelten Arbeiten, werden die relevantesten Arbeiten identifiziert, die zur Beantwortung beitragen können. Im weiteren Verlauf werden die einzelnen Schritte der durchgeführten SLR beschrieben und das Rechercheprotokoll erstellt. Zu Erst wird die Vorbereitung beschrieben und anschließend auf die Vorgehensweise bei der Datensammlung eingegangen. Nach erfolgreicher Durchführung der Suche, sowie Anwendung der Auswahlkriterien und Qualitätsbewertung der Arbeiten, wird eine Tabelle erstellt, die die erforderliche Literatur enthält, um die Forschungsfragen zu beantworten. Die Vorgehensweise der einzelnen Schritte ist in Abbildung 3.1 dargestellt.

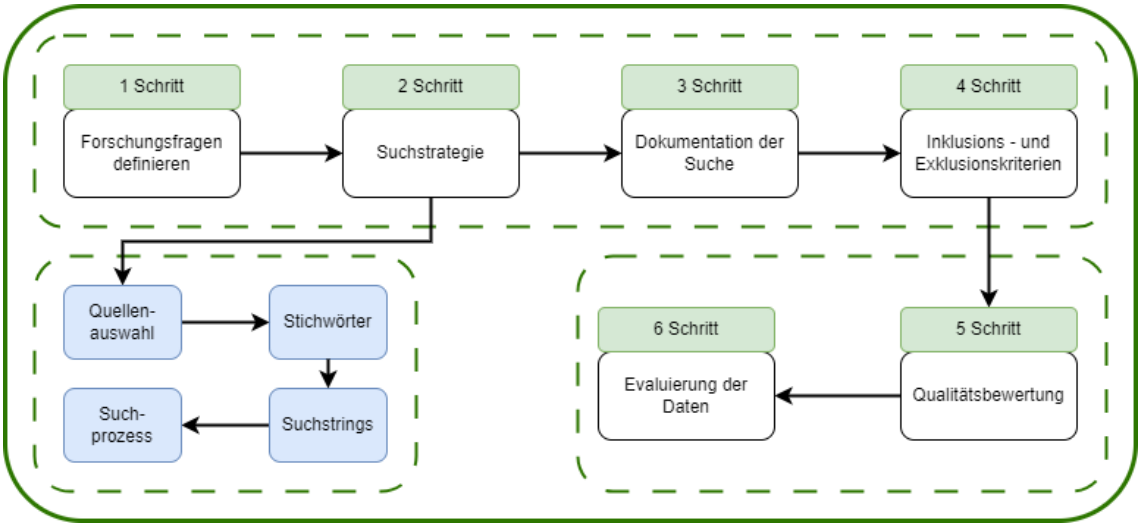

Abbildung 3.1: Schritte der systematischen Literaturrecherche

3.1 Vorbereitung

Die Vorbereitung ist essenziell für eine gute SLR. In diesem Schritt des Protokolls geht es um die Auswahl der Quellen, sowie die Auswahl der Stichwörter. Anschließend werden die Kriterien zur Inklusion und Exklusion definiert, sowie eine Reihe an Merkmalen zur Qualitätsbewertungen. Zu Letzt wird der Vorgang der Suchstrategie beschrieben.

3.1.1 Quellenauswahl

Bei der Quellenauswahl wurde die Wahl auf die vier Datenbanken, die Tabelle 3.1 zu entnehmen sind, beschränkt. Auf weitere Quellen wurde verzichtet, da davon auszugehen ist in den genannten Datenbanken alle relevanten Arbeiten zu finden und um die Zahl der möglichen Duplikate gering zu halten. Bei Association for Computing Machinery (ACM) und IEEE Xplore handelt es sich um Datenbanken bei denen ausschließlich wissenschaftliche Publikationen aus Fachzeitschriften, Konferenzberichte und Büchern rund um die Themen Informatik, Ingenieurwesen, Elektronik zu finden sind. ScienceDirect umfasst wissenschaftliche Arbeiten aus Fachzeitschriften rund um die Naturwissenschaften.

Datenbank	**Link oder Webseite**
ACM	https://dl.acm.org
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
Science Direct	https://www.sciencedirect.com

Tabelle 3.1: Online Datenquellen

3.1.2 Stichwörter definieren

Die Stichwörter werden nach Schwachstellenanalyse, Bedrohungsanalyse und Penetrationtest aufgeteilt, um möglichst relevante Arbeiten die Sicherheitsanalysen im Kontext IoT behandeln zu identifizieren. Ebenfalls werden Arbeiten über Fallstudien gesucht, da diese sich auch oft mit Schwachstellen und Bedrohungsanalysen beschäftigen. Die verwendeten Schlüsselwörter sind in englischer Sprache verfasst, da die meisten relevanten Veröffentlichungen auf diesem Gebiet in englischer Sprache verfasst sind. Aus diesem

Grund wurde bewusst darauf verzichtet, gezielt nach deutschen Arbeiten zu suchen. Zudem wurden synonyme Suchbegriffe ausgewählt, da z.B. für "Vulnerability Analysis" auch "Vulnerability Assessment" genommen werden kann. Tabelle 3.2 listet eine Übersicht der verwendeten Stichwörter.

Sicherheitsanalyse Technik	**Stichwörter**
Schwachstellenanalyse	IoT
	Internet of Things
	Vulnerability Analysis
	Vulnerability Assessment
Bedrohungsanalyse	IoT
	Internet of Things
	Threat Modeling
	Threat Analysis
	Threat Assessment
Penetrationtest	IoT
	Internet of Things
	Penetration
Fallstudie	Iot
	Internet of Things
	Security
	Case Study

Tabelle 3.2: Stichwörter nach Sicherheitsanalyse-Techniken

Aus den definierten Stichwörtern werden anschließend mit Boolesche Operatoren Suchstrings gebildet die in die Suchmaschinen der Quellen eingegeben werden.

Schwachstellenanalyse: (IoT OR Internet of Things) AND (Vulnerability AND (Analysis OR Assessment))

Bedrohungsanalyse: (IoT OR Internet of Things) AND (Threat AND (Modeling OR Analysis OR Assessment))

Penetrationtest: (IoT OR Internet of Things) AND Penetration

Fallstudien: (IoT OR Internet of Things) AND Case Study AND Security

3.1.3 Auswahlkriterien

Nachdem die Arbeiten mit den zuvor erstellen Suchstrings in den ausgewählten Datenbanken zusammengetragen wurden, werden die Inklusions- und Exklusionskriterien angewandt. Diese Kriterien dienen dazu, irrelevante Arbeiten auszusortieren, sodass am Ende ein Set an Arbeiten zusammen kommt, auf welches die Qualitätsbewertung angewendet werden kann. Angewandt werden die Kriterien auf den Titel und die Zusammenfassung der Arbeit. Tabelle 3.3 zeigt die Inklusions- und Exklusionskriterien auf. Bei Duplikaten der selben Arbeit wurde die aktuellste Arbeit ausgewählt.

Inklusionskriterien
Arbeiten in englischer Sprache
Arbeiten die sich explizit mit einem IoT-Gerät oder IoT-Protokoll befassen
Arbeiten die ein Framework vorstellen
Arbeiten die mindestens zwei der Suchwörter im Titel enthalten
Arbeiten die eine Fallstudie an einem IoT-Gerät oder IoT-Protokoll vornehmen
Arbeiten die im Zeitraum von 2013 - 2023 veröffentlicht wurden
Exklusionskriterien
Arbeiten die nicht den Inklusionskriterien entsprechen
Doppelte Studien
Arbeiten die sich allgemein gehalten mit Sicherheitsanalysen befassen
Übersichtsarbeiten (Literatur Reviews)
Der Volltext ist nicht verfügbar oder zugänglich
Grau-Literatur

Tabelle 3.3: Inklusions- und Exklusionskriterien

3.1.4 Qualitätsbewertung

Um die Auswahl an Arbeiten zu verbessern, wird nach den Inklusions- und Exklusionskriterien eine Qualitätsbewertung vorgenommen. Hierfür wird eine Checkliste mit Fragen

erstellt, anhand derer jede Arbeit überprüft wird, um einen relevanten Beitrag zur Beantwortung der Forschungsfragen zu leisten. Dabei wird sich neben der Zusammenfassung und Einleitung auch die Schlussfolgerung angesehen, sowie falls vorhanden der praktische Teil. Tabelle 3.4 gibt einen Überblick über die Fragen.

Frage-ID	**Frage**
1	Wurden die Ziele in der Arbeit klar definiert?
2	Deckt die Arbeit Antworten auf die Forschungsfragen ab?
3	Befasst sich die Arbeit mit einer der Sicherheitsanalyse-Techniken?

Tabelle 3.4: Checkliste zur Qualitätsbewertung

3.2 Datensammlung

Die Datensammlung erfolgte, in dem die zuvor geformten Suchstrings in die Suchmaschinen der ausgewählten Datenbanken eingegeben wurden. Das Inklusionskriterium des Zeitraums von 2013-2023 wurde schon während der Suche eingegrenzt.
Um eine Übersicht über die Ergebnisse zu erhalten wurden diese in eine Excel-Tabelle mit folgenden Informationen gespeichert: Titel, Autoren, Jahr, Zielsetzung der Arbeit, Quelle (ACM, IEEE Xplore, ScienceDirect), Art der Arbeit (Konferenz, Fachzeitschrift, etc.), Sicherheitsanalyse Technik, Anwendungsbereich (IoT-Protokoll, IoT-Gerät, IoT-System, etc.) und gegebenenfalls Kommentar.
Insgesamt ergab die Suche 79 Arbeiten, 13 von ACM, 49 von IEEE Xplore und 17 von ScienceDirect. Anschließend wurden die Kriterien zur Inklusion und Exklusion aus Tabelle 3.3 angewendet. Die Tabelle 3.5 zeigt eine Übersicht der Anzahl an Ergebnissen.

Nach Anwendung der Inklusions- und Exklusionskriterien, werden die verbleibenden Arbeiten der Qualitätsbewertung unterzogen, die mithilfe der genannten Checkliste aus Tabelle 3.4 durchgeführt wird. Dies ermöglicht es, die Zuverlässigkeit und Validität der ausgewählten Arbeiten zu beurteilen und eine solide Grundlage für die Beantwortung der Forschungsfrage zu schaffen.

Datenbank	Inkludiert	Exkludiert	Total
ACM	8	5	13
IEEE Xplore	27	22	49
Science Direct	4	13	17
Total	39	40	79

Tabelle 3.5: Übersicht der Anzahl an Ergebnissen

3.3 Evaluierung der Metadaten

Durch sorgfältige Prüfung der Zusammenfassung, Einleitung, dem Methodik-Teil und des Fazits auf die Qualitätskriterien aus Tabelle 3.4 wurde eine Liste mit den Arbeiten erstellt, die zur Beantwortung der Forschungsfragen beitragen. Das endgültige Set an Arbeiten wird in Tabelle 3.9 dargestellt. Dabei wurde nach der Sicherheitsanalysetechnik, also Schwachstellen- oder Bedrohungsanalyse oder Penetrationtesting sortiert. Ebenfalls wurde der Anwendungsbereich erwähnt, sowie das Jahr der Veröffentlichung.

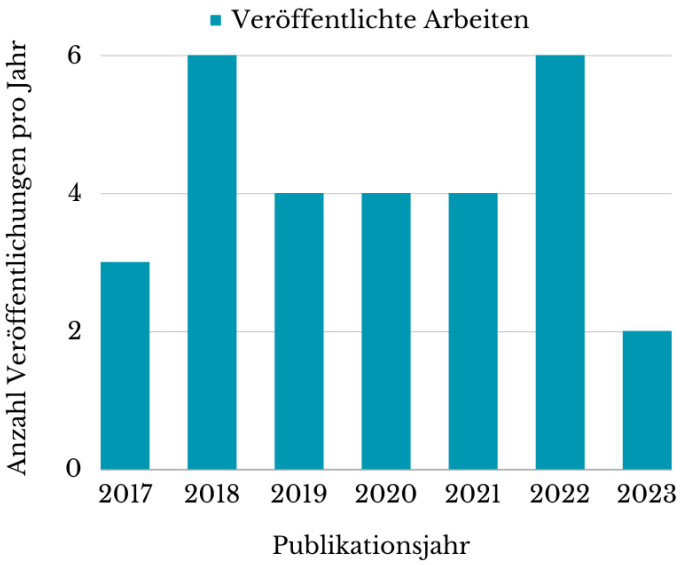

Abbildung 3.2: Forschungstrend IoT Sicherheitsanalysen

Für die Beantwortung der Forschungsfrage 1 ist wichtig den Forschungstrend zu betrachten. Die Anzahl der ausgewählten relevanten Forschungsarbeiten in Bezug auf die Jahre ist in Abbildung 3.2 dargestellt. Hierbei ist es wichtig zu betonen, dass die Darstellung nur den Trend der einbezogenen Arbeiten widerspiegelt. Durch die spezifischen Suchbegriffe wurden nur ein geringer Teil an Arbeiten untersucht, welche keinen allgemeingültigen Trend des gesamten Forschungsbereich von Sicherheitsanalysen im Kontext von IoT aufzeigen können.

Die Verteilung der Arbeiten nach Herausgeber ist in Abbildung 3.3 zu sehen. Dabei wird deutlich, dass die Mehrzahl der Arbeiten auf IEEE Xplore erschienen sind, mit 67,9%. Darauf folgt ACM mit 21,4% und ScienceDirect mit nur 21,4%. Es ist wichtig hervorzuheben, dass ScienceDirect eine breite Palette von Arbeiten beherbergt, die entweder kostenpflichtig sind oder eine Anmeldung erfordern, um darauf zuzugreifen.

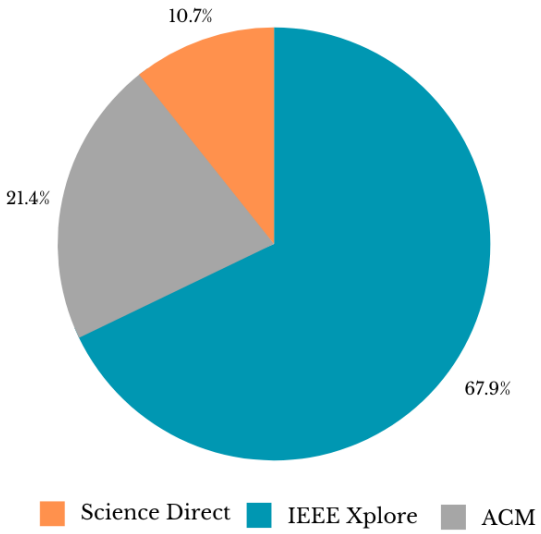

Abbildung 3.3: Verteilung der ausgewählten Arbeiten nach Herausgeber

Abbildung 3.4 zeigt die Verteilung der Arbeiten nach Art bei den einzelnen Herausgebern. Dabei ist auffällig, dass die meisten Arbeiten Konferenzberichte (Conference Paper) sind. Arbeiten die in einer Fachzeitschrift (Journal) erschienen sind, waren am wenigsten

vertreten. Bei ACM und Science Direct waren die veröffentlichten Arbeiten Forschungsberichte (Research Article).

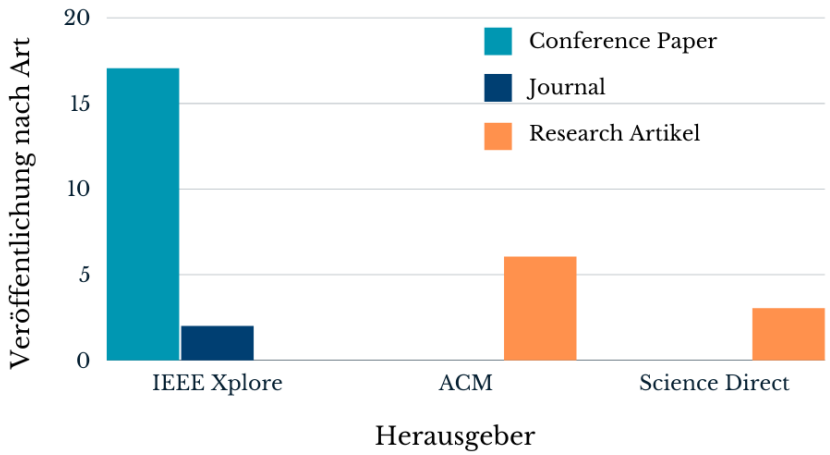

Abbildung 3.4: Verteilung der ausgewählten Arbeiten nach Art und Herausgeber

Zusammenfassend lässt sich sagen, dass Arbeiten zu Sicherheitsanalysen im Kontext IoT ein Thema ist, mit dem sich in der Forschung beschäftigt wird. Für die Anzahl an IoT-Geräten die weltweit in verschiedenen Bereichen, unter anderem auch kritischen Infrastrukturen wie Smart-Grid oder im Gesundheitsbereich, fällt die Anzahl an Sicherheitsanalysen jedoch sehr gering aus. Was während der systematischen Literaturrecherche auch auffällig war, ist die Tatsache, dass die Taxonomie im Bereich Sicherheitsanalysen nicht sehr stringent ist. Daher wird im kommenden Kapitel auf die Entwicklung der Sicherheitsanalysen im Zusammenhang mit IoT eingegangen. Ebenfalls wird auf die Herausforderungen, sowie eingesetzten Technologien zur Verbesserung der Sicherheitsanalysen eingegangen. Anschließend erfolgt eine Bewertung der aktuellen Lösungsansätze.

Titel	**Anwendungs-bereich**	**Jahr**	**Referenz**
An Auditing Framework for Vulnerability Analysis of IoT System	Framework	2019	[43]
Vulnerability assessment of MQTT protocol in Internet of Things (IoT)	MQTT-Protokoll	2021	[49]
A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow	Framework	2018	[61]
Attack graph — Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT	6LoWPAN	2018	[52]
Power Measurement-Based Vulnerability Assessment of IoT Medical Devices at Varying Countermeasures for Cybersecurity	IoT in der Medizin	2021	[10]
Risk Prediction of IoT Devices Based on Vulnerability Analysis	Framework	2022	[45]
Security Vulnerability Assessment of Power IoT Based on Business Security	Smart-Grid	2020	[25]
Vulnerability Assessment of Objective Function of RPL Protocol for Internet of Things	RPL-Protokol	2018	[56]

Tabelle 3.6: Arbeiten zur Schwachstellenanalyse

Titel	Anwendungsbereich	Jahr	Referenz
An Ensemble Approach for IoT Firmware Strength Analysis using STRIDE Threat Modeling and Reverse Engineering	IoT-Firmware	2022	[66]
STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems	IoT in der Industrie	2021	[11]
A Threat Model and Security Recommendations for IoT Sensors in Connected Vehicle Networks	IoT im Fahrzeug	2022	[38]
Vulnerability and Threat Assessment Framework for Internet of Things Systems	Framework	2023	[17]
STRIPED: A Threat Analysis Method for IoT Systems	Framework	2022	[59]
Threat-Modeling-Guided Trust-Based Task Offloading for Resource-Constrained Internet of Things	IoT-System	2022	[19]
Requirements and Recommendations for IoT/IIoT Models to Automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing	Framework	2019	[9]
Threat model for securing internet of things (IoT) network at device-level	IoT-Gerät	2020	[51]
Evidence identification in IoT networks based on threat assessment	Smart-Home	2017	[4]

Tabelle 3.7: Arbeiten zur Bedrohungsanalyse

Titel	Anwendungs-bereich	Jahr	Referenz
Penetration Testing for Internet of Things and Its Automation	Framework	2018	[20]
A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments	Framework	2021	[37]
Attack Surface Modeling and Assessment for Penetration Testing of IoT System Designs	Framework	2018	[41]
Penetration Testing Framework for IoT	Framework	2019	[64]
IoT-PEN: A Penetration Testing Framework for IoT	Framework	2020	[65]
PETIoT: PEnetration Testing the Internet of Things	Framework	2022	[15]

Tabelle 3.8: Arbeiten zum Penetrationtesting

Titel	Anwendungs-bereich	Jahr	Referenz
Penetration Testing for IoT Security: The Case Study of a Wireless IP Security CAM	IoT-Gerät	2023	[5]
Testing IoT Security: The Case Study of an IP Camera	IoT-Gerät	2020	[3]
IoT security vulnerability: A case study of a Web camera	IoT-Gerät	2018	[57]
Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System	IoT-Gerät	2017	[40]
Security analysis of Internet-of-Things: A case study of august smart lock	IoT-Gerät	2017	[68]

Tabelle 3.9: Arbeiten mit Fallstudien

4 Ergebnisse

Das vorliegende Kapitel präsentiert die Ergebnisse der vorangegangenen systematischen Literaturrecherche um die anfangs formulierten Forschungsfragen zu beantworten. Durch die gezielte und strukturierte Literaturrecherche wurden einige relevante Forschungsarbeiten zu dem Thema identifiziert und einer Analyse unterzogen. Dieser Abschnitt soll die wesentlichen Erkenntnisse vorstellen und eine Beantwortung auf die Forschungsfragen liefern. Dabei wird zunächst die Entwicklung der Sicherheitsanalysen im zeitlichen Kontext beschrieben. Anschließend wird auf die aktuellen Herausforderungen eingegangen und zu Letzt die praktischen Lösungsansätze beschrieben.

4.1 Zeitliche Entwicklung von Sicherheitsanalysen im Kontext IoT

Da die Verwendung von IoT rasant wäschst und auch die Angriffe gegenüber den Systemen und Geräten immer mehr werden, stellt sich die Frage, wie sich die Sicherheitsanalysen im Bereich IoT zeitlich verändert haben. Während der systematischen Sicherheitsanalyse wurde ein Zeitraum von 2013 bis 2023 gewählt, jedoch lässt sich auf Grundlage der einbezogenen Arbeiten kein deutlicher Trend feststellen. In Bezug auf Sicherheitsanalysen, wie Schwachstellenanalyse, Bedrohungsanalyse oder Penetrationtesting, zeigt die Literaturrecherche, dass bei den Veröffentlichungen weder eine signifikante Zu- noch Abnahme stattfand. Jedoch lässt sich mit dem endgültigen Datensatz keine eindeutige Aussage über die Entwicklung treffen.
Um dennoch eine Einschätzung über die zeitliche Entwicklung geben zu können, wurden andere systematische Literaturarbeiten hinzugezogen. So haben Liao et al., 2020 [39] eine Literaturrecherche zu Sicherheitsanalysen von IoT-Geräten durch den Einsatz von Mobile Computing durchgeführt. Für die Untersuchung wurden 117 Veröffentlichungen im

Zeitraum von 2011 bis 2019 in Betracht gezogen. Die zeitliche Analyse zeigt eine deutliche Zunahme zu dem Thema.

4.1.1 Fortschritte und Entwicklungen in der Sicherheitsanalyse

Im Bereich der Sicherheitsanalysen lässt sich auf Grundlage der ausgewählten Literatur keine eindeutige Aussage treffen.
Es lässt sich jedoch sagen, dass der Fokus in den Anfängen des IoT weniger auf Sicherheit und Sicherheitsanalysen lag [66]. Der rasante Anstieg an IoT-Geräten und der damit verbundene Anstieg an Einsatzbereichen trägt dazu bei, dass der Sicherheit und Sicherheitsanalysen in den Fokus rücken. Durch die Verarbeitung von persönlichen Daten der Nutzer, sowie des zunehmenden Einsatzes von IoT-Geräten im industriellen Bereich und in kritischer Infrastruktur ist es unumgänglich, Sicherheitsanalysen durchzuführen und entsprechende Abwehrmechanismen gegen potenzielle Angriffe zu etablieren. Angesichts der wachsenden Vernetzung und des umfassenden Einsatzes von IoT ergeben sich ernste Sicherheitsrisiken, die nicht nur die Privatsphäre und Vertraulichkeit der Nutzerdaten gefährden, sondern auch die Integrität und Verfügbarkeit bedrohen können.
Auch zeigt sich eine Entwicklung der Sicherheitsanalyse-Techniken. So werden zwar traditionelle Techniken eingesetzt, jedoch ist eine Anpassung an IoT notwendig um best mögliche Ergebnisse zu erzielen. Auch gehen die Analysen von einem einzigen Gerät zur Gesamtheit der Geräte über und betrachten auch die Verbindungen untereinander [4]. In Anbetracht des Mirai-Botnets wurde deutlich, dass die Untersuchung der Vernetztheit von IoT-Geräten von entscheidender Bedeutung ist [34].
Auch wenn Penetrationtests häufig noch manuell an einem Gerät durchgeführt werden [57], [40], [68], so fangen Forschungsarbeiten an, sich mit Frameworks in diesem Bereich auseinander zu setzen [43], [17]. Auch Automatisierung spielt eine signifikante Rolle in der Entwicklung der Sicherheitsanalyse. Durch die immer größer werdenden IoT-Systeme und die steigende Zahl an Daten, wird es unmöglich manuelle Sicherheitsanalysen durchzuführen [45].
Die Integration von Künstlicher Intelligenz in Sicherheitsanalysen ermöglicht eine effiziente Erkennung und Abwehr von Bedrohungen. KI-gestützte Algorithmen können Muster und Anomalien in großen Datenmengen von IoT-Geräten erkennen, um verdächtiges Verhalten zu identifizieren und Sicherheitslücken frühzeitig zu entdecken [43], [45], [56].
Zusammenfassend lässt sich festhalten, dass Sicherheitsanalysen im Kontext IoT eine

Entwicklung durchlaufen, um den spezifischen Schwachstellen und Bedrohungen gerecht zu werden. Die Integration von neuartigen Technologien wie künstlicher Intelligenz und maschinellem Lernen verspricht dabei einen Mehrwert. Trotz dieser vielversprechenden Ansätze ist jedoch erkennbar, dass diese Wege bisher nur in begrenztem Umfang erforscht wurden, was zeigt, dass die Entwicklung noch in den Anfängen steckt und weiterführende Untersuchungen erforderlich sind.

4.2 Sicherheitsanalysen in IoT

Im folgenden Abschnitt werden die Ergebnisse der systematischen Literaturrecherche im Hinblick auf aktuelle Herausforderungen der Sicherheitsanalysen vorgestellt. Dabei liegt der Fokus auf der Identifikation von Schwachstellen, sowie der Identifizierung und Bewertung von Bedrohungen.

4.2.1 Aktuelle Herausforderungen

In diesem Abschnitt werden die Herausforderungen, mit denen die Analysen der untersuchten Arbeiten konfrontiert sind, näher betrachtet. Dabei wurden die Arbeiten analysiert und aufgezeigt, wo die Analysen Probleme aufgewiesen haben. Dabei geht es um die Identifikation von Schwachstellen der IoT-Geräte, Protokolle und Systeme, sowie die Herausforderungen die bei der Entwicklung eines Frameworks auftreten. Aber auch um die Identifikation und Bewertung von Bedrohungen, sowie die Herausforderungen die in diesem Kontext auftreten.

4.2.1.1 Identifikation von Schwachstellen

Schwachstellenanalyse

Die Schwachstellenanalyse im Bereich IoT ist mit einigen Herausforderungen verbunden. Die analysierten Arbeiten, die sich mit der Schwachstellenanalyse auseinandergesetzt haben, Tabelle 4.1, haben gezeigt, dass sich hauptsächlich auf Grund der Heterogenität und der Komplexität der IoT-Geräte keine allumfassende Schwachstellenanalyse durchgeführt wird. Die Vielzahl an eingesetzten Technologien, Geräten und Anwendungen, sowie die komplexen IoT-Systeme mit den unterschiedlichen Schichten erschwert es eine allumfassende Analyse von Schwachstellen durchzuführen.

Anwendungsbereich	**Erläuterung**	**Referenzen**
Framework	Haben sich mit der Umsetzung eines Frameworks zur Schwachstellenanalyse auseinandergesetzt	[43],[61],[45]
Protokoll	Schwachstellenanalyse von MQTT und RPL-6LoWPAN	[49],[52],[56]
IoT-Gerät	Schwachstellenanalyse eines medizinischen IoT-Messwandlers	[10]
IoT-System	Schwachstellenanalyse eines Supervisory Control and Data Acquisition (SCADA)-Systems für den Stromsektor	[25]

Tabelle 4.1: Anwendungsbereiche der Schwachstellenanalyse

Hauptsächlich konzentrieren sich die Arbeiten auf bestimmte Protokolle, oder sehr spezifische Aspekte eines Gerätes oder Systems. So wurde in der Arbeit von Raikar et al., 2021[49] das MQTT-Protokoll auf Schwachstellen untersucht. Hierbei wurde eine manuelle Schwachstellenanalyse in einer Testumgebung mit Hilfe des Open-Source-Tools "Zeek" durchgeführt und aufgezeigt, dass ein Angreifer Kontrolle über das Protokoll erlangen kann und somit den Datentransfer zwischen einem Service und dem Gerät beeinflussen kann. Die Arbeit von Sahay et al., 2018 [52] befasst sich mit dem Routing Protokoll RPL. Im Detail führen sie eine Schwachstellenanalyse der Rang-Eigenschaft, die RPL besitzt durch. Bei der Rang-Eigenschaft handelt es sich um einen Mechanismus der helfen soll den Routing-Pfad der gesendeten Pakete zu optimieren. Es wurde ein Angriffsgraph auf Grundlage vorheriger

Schwachstellenanalysen im Bereich RPL erstellt. Auch hier wurde wieder auf eine Testumgebung zurückgegriffen und das Protokoll gegen 4 verschiedene Angriffe getestet. Dabei konnten sie aufzeigen, dass ein Angreifer das Netzwerk kompromittieren kann und Ressourcen erschöpft werden können, indem ein Parameter eines Ranges manipuliert wurde. Ebenfalls mit dem RPL befasst sich die Arbeit von Semedo et al., 2018. Diese haben die Sicherheitsanalyse ebenfalls in einer Testumgebung durchgeführt und konnten eine Netzwerkkompromittierung, sowie die Isolation einer Netzwerkkomponente ausführen. Bei den Schwachstellenanalysen der Protokolle zeigt sich, dass diese oftmals in einer Testumgebung durchgeführt werden. Diese spiegeln oftmals nicht den realen Einsatz eines IoT-Gerätes wieder und bringen meist einige Vorbedingungen mit sich, ohne die ein Testszenario nicht durchführbar wäre. Ebenfalls werden diese Analysen oft manuell und mit Hilfe von meist Open-Source-Tools durchgeführt.

Die Arbeit von Arpaia et al., 2021 [10] führt eine Schwachstellenanalyse eines medizinischen IoT-Messwandlers durch. Dabei richten sie Angriffe gegen einen IoT-Mikrocontroller, der durch eine Softwareimplementierung von AES-128 und Schutzmaßnahmen gegen Strom-Angriffe geschützt ist. Der Angriff wird mit unterschiedlichen Sicherheitsmaßnahmen durchgeführt. Auch hier wurde auf einen sehr spezifischen Aspekt eines IoT-Gerätes eingegangen. Fei et al., 2021 [25] führen eine Schwachstellenanalyse eines SCADA-Systems für den Stromsektor durch. Hierfür wird ein Angriffsbaum erstellt, der anschließend für die Modellierung von Angriffen gegen das System genutzt wird. Angriffsbäume lassen sich im Bereich IoT zwar anwenden und können für bestimmte Fälle auch sinnig erscheinen, jedoch können sie sehr schnell sehr groß und komplex werden. Je nachdem wie viele Geräte berücksichtigt werden in der Analyse und wie deren Abhängigkeiten sind.

Die verbleibenden Arbeiten von Nadir et al., 2019 [43], Wang et al., 2018 [61] und Oser et al., 2022 [45] stellen Ansätze für die Entwicklung von Frameworks vor. Zum Einen wurde deutlich, dass existierende entweder Frameworks kommerziell oder sehr zeitaufwändig sind. Zudem gibt es kaum bis keine Frameworks die sich sowohl mit Schwachstellen von Software, Hardware und Kommunikation gleichzeitig beschäftigen. Die Frameworks müssen für eine Vielzahl an unterschiedlichen Geräten angepasst sein, sowie deren Hard- und Software-Anforderungen. Ebenfalls sollte die durchgeführte Schwachstellenanalyse reproduzierbar sein. Da die vorgestellten Frameworks auf öffentliche Quellen, wie der NVD zurückgreifen um die

Ergebnisse mit den dort gelisteten Schwachstellen zu vergleichen, ist es nicht möglich mit ihnen Zero-Day Schwachstellen zu erkennen. Abschließend lässt sich sagen, dass die Ansätze der Frameworks darauf hindeuten, dass sie Schwachstellen in der Software und der Kommunikation der IoT-Geräte erkennen können. Was sie jedoch außer Acht lassen, ist die physische Komponente.

Penetrationtest & Fallstudien

Tabelle 4.2 zeigt die Arbeiten, der Penetrationtests und Fallstudien.

Anwendungs-bereich	**Erläuterung**	**Referenzen**
Framework	Haben sich mit der Umsetzung eines Frameworks zur Schwachstellenanalyse auseinandergesetzt	[15],[20],[37], [41], [64],[65]
IoT-Gerät	Schwachstellenanalysen von IoT-Kameras, IoT-Steckdose und IoT-Türschloss	[3],[57], [5] [40],[68]

Tabelle 4.2: Anwendungsbereiche der Penetrationtests & Fallstudien

Abdalla et al., 2020 [3], Seralathan et al., 2018 [57] und Almazrouei et al., 2023 [5] haben sich mit der Analyse von Schwachstellen von IoT-Kameras befasst. Beide Tests wurden manuell mit Hilfe verschiedener Open-Source-Tools durchgeführt. Dabei haben sich Schwachstellen in der Anwendung der Kameras und der Kommunikation ausgenutzt um Anmeldeinformationen zu bekommen, sowie sensitive Daten abgreifen, die unverschlüsselt versendet wurden. Die Arbeit von Ling et al., 2017 [40] hat eine Analyse einer IoT-Steckdose durchgeführt und konnte durch eine Schwachstelle in einem Kommunikationsprotokoll die Steckdose kompromittieren. Der Angriff wurde in einer Testumgebung durchgeführt und mit Hilfe von tcpdump die Netzwerkkommunikation mitgeschnitten. Ye et al., 2017 [68] haben ein IoT-Türschloss auf Schwachstellen untersucht und vier Angriffe gegen das Schloss ausgeführt. Dabei sind sie, anders als die vorherigen Fallstudien, nicht über das IoT-Gerät selbst gegangen, sondern haben sich mit der mobilen Anwendung auf dem Smartphone beschäftigt.
Alle vier Fallstudien wurden manuell mit Hilfe von Open-Source-Tools durchgeführt. Dabei wird deutlich, dass auch hier wieder nur Analysen bestimmter Aspekte oder Objekte der Geräte durchgeführt wurden. So bedarf es bei dem Türschloss

über ein Smartphone mit "root"-Zugriff um an die bestimmten Daten zu gelangen. Ebenfalls wurden die IoT-Geräte in bestimmten Testumgebungen getestet, bei denen wieder der physische Aspekt nicht beachtet wurde.

Bei den Arbeiten, die sich mit Penetrationtests befasst haben, lassen sich auch unterschiedliche Herangehensweisen feststellen. So wird in der Arbeit von Bella et al., 2023 [15] ein Framework namens PETIoT vorgestellt. Dabei haben sie sich auf den methodischen Ansatz der Angriffsketten fokussiert. Diese beschreiben den Prozess den ein Angreifer durchlaufen muss, um sein Ziel zu erreichen und soll dabei helfen Schwachstellen in einem System zu erkennen. Es wurde ein Tool-Kit aus Open-Source-Tools erstellt. Chu et al., 2018 [20] schlagen eine Herangehensweise vor, die auf Grundlage von "Belief-Desire-Intention" aufbaut. Dabei werden Ziele und Pläne zum Testen eines Objektes festgelegt, sowie Sets aller möglichen Optionen, die in dem Penetration test vorkommen, sowie ein Set an möglichen Aktionen und ein Set an Umgebungsinformationen. Ein BDI-Agent kann sozusagen während des Penetrationtests mit dem Ziel interagieren. Die Arbeit von Koroniotis et al., 2021 [37] befassen sich mit der Entwicklung eines Penetrationtest-Frameworks auf Basis von maschinellem Lernen. Durch Informationssammlung sollen schneller Anomalien und Schwachstellen entdeckt werden. Die gefundenen Schwachstellen werden anschließend durch Fuzzing getestet. Dieser Ansatz ist der erste, der auch den Aspekt der physischen Schwachstellen mit aufgreift. Mahmoodi et al., 2018 [41] beschreiben ein Framework, dessen Ansatz Angriffsflächen und Angriffsverhalten beschreibt. Virtuelle Prototypen eines Gerätes stellt ein Modell eines physischen Gerätes da. Durch die Simulation eines Gerätes können Angriffe mit verschiedenen Systemalternativen durchgeführt werden. Das Framework ermöglicht es somit verschiedene Sicherheitskonzepte zu vergleichen und potenzielle Schwachstellen sichtbar zu machen. Die letzten beiden Arbeiten von Yadav et al., 2019 [64] und Yadav et al., 2020 [65] befassen sich mit einem Penetrationtest-Framework, welches das komplette Netzwerk mit dem ein IoT-Gerät interagiert betrachtet. Dabei sollen die beiden entwickelten Frameworks eine Ende-zu-Ende Verbindung untersuchen. Also von Gerät, über die Kommunikation von Gerät zu Kontrolleinheit zum Cloud-Server, sowie die Kommunikation von Cloud zur Anwendung. Auch hier wird mit Angriffsgraphen gearbeitet um die Wege eines möglichen Angreifers nachvollziehen zu können.

Auch bei den Penetrationtests und den Fallstudien zeigten sich einige Heraus-

forderung. Auch die vorgestellten Frameworks und Beispiele können keine Wege aufzeigen, wie gegen Zero-Day Schwachstellen vorgegangen werden kann. Ebenso stellt auch hier die Heterogenität der IoT-Geräte eine Herausforderung dar. Zwar lassen sich Frameworks mit einigen Geräten testen, aber je mehr dazu kommen, desto mehr Anpassungen bedarf es, um die richtigen Tools für die entsprechenden Technologien und Hard- sowie Software bereit zu stellen. Des weiteren funktionieren die gewählten Methoden zwar für die vorgestellte Arbeit, jedoch bleibt meist offen, wie skalierbar die Frameworks mit den angewandten Methoden letztendlich sind.
Die Identifikation von Sicherheitsschwachstellen im IoT-Bereich stellt keine einfach zu bewältigende Aufgabe dar, wie aus den verschiedenen Ansätzen in den zuvor beschriebenen Arbeiten hervorgeht.

4.2.1.2 Bewertung von Risiken und Bedrohungen

Die Bewertung von Risiken und Bedrohungen von IoT-Geräten und Systemen steht vor ähnlichen Herausforderungen wie die Identifikation von Schwachstellen. Tabelle 4.3 zeigt eine Übersicht der Arbeiten, die sich mit der Analyse und Modellierung von Bedrohungen auseinandergesetzt haben.

Anwendungs-bereich	**Erläuterung**	**Referenzen**
Framework	Entwicklung eines Frameworks zur Analyse von Bedrohungen im IoT-Bereich	[17],[59],[9]
IoT-Gerät	Analyse von Bedrohungen an einem IoT-Sensor und drei unterschiedlichen IoT-Geräten	[38],[51]
IoT-System	Analyse von Bedrohungen in unterschiedlichen Anwendungsbereichen, wie Smart Home oder Agrarsektor	[66],[19],[4],[11]

Tabelle 4.3: Anwendungsbereiche der Analyse von Bedrohungen

Kuri et al., 2022 [38] haben eine Analyse der Bedrohungen für Sensoren in vernetzten Fahrzeugen durchgeführt, bei dem eine Referenzarchitektur für ein vernetztes Fahrzeugnetzwerk genutzt wird um System-Assets und Einstiegspunkte für einen Angriff zu identifizieren. Anschließend wird eine Analyse durch STRIDE eines Fahrzeugsensors durchgeführt. Herausforderungen und Einschränkungen hängen oft von spezifischen architek-

tonischen Gestaltungsentscheidungen des Systems und der Verfügbarkeit von Rechenressourcen ab. Die Arbeit von Rizvi et al., 2020 [51] stellt eine Bedrohungsanalyse so wie anschließende Bewertung von drei unterschiedlichen IoT-Geräten aus drei unterschiedlichen Anwendungsbereichen vor und fokussieren sich dabei auf die Geräteebene. Dabei wurde die Bedrohungsanalyse ohne eine wirkliche Methode durchgeführt, sondern erfolgte deskriptiv.

Bei den Arbeiten rund um IoT-Systeme haben Yaqub et al., 2022 [66] eine Bedrohungsanalyse von IoT-Firmware durchgeführt und die ausnutzbaren Parameter ebenfalls mit STRIDE modelliert und anschließend Reverse-Engineering durchgeführt um Informationen über die Images zu erhalten. Dafür haben sie 4364 IoT-Firmware-Images untersucht. Dieses Vorgehen wurde von Tools unterstützt. Dennoch ist die Untersuchung von Firmware-Images sehr zeitintensiv und lässt sich schwer auf andere Szenarien abbilden. Bradbury et al., 2022 [19] analysieren Bedrohungen von IoT-Netzwerken in Hinblick auf Bedrohungen gegenüber Rand-Knoten, die zu Abweichungen vom erwarteten Verhalten führen können. Dabei gehen sie auch auf die Problematik ein, dass bei einer Bedrohungsanalyse einige Beschränkungen auftreten, wie etwa dass oftmals eine situationsabhängig Sichtweise eingenommen wird. Daher können einige Bedrohungen nicht aufgezeigt oder berücksichtigt werden, da sie so in der vorherrschenden Laborbedingung nicht auftauchen. Ebenfalls ist eine manuelle Bedrohungsanalyse vom Wissensstand des Durchführenden abhängig, da sie auf Expertise und Erfahrung basiert. Bei einer manuellen Analyse muss der Durchführende über ein fundiertes Verständnis von Sicherheitskonzepten, Methoden, Bedrohungen und -Gegenmaßnahmen verfügen. Die Qualität und Genauigkeit der Analyse hängt daher direkt von den Kenntnissen, Fähigkeiten und Erfahrungen ab. Akatyev et al., 2019 [4] führten eine Bedrohungsanalyse für nutzerzentrierte IoT-Geräte im Smart-Home-Bereich durch. Dabei modellieren sie Anwendungsfälle um Bedrohungen und Risiken zu erkennen und führen anschließend eine Analyse basierend auf STRIDE und DREAD durch. Die Herausforderung, auf die in der Arbeit auch eingegangen wird ist, dass IoT-Geräte oft ihren Netzwerkstatus ändern, welches eine Analyse erschweren kann. Ebenso wird erwähnt, dass in Bedrohungsanalysen rund um IoT oftmals die physische Komponente nicht betrachtet wird, obwohl diese, sofern einfach zu erreichen, am meisten Bedrohungen ausgesetzt ist. Die Arbeit von Asif et al., 2021 [11] führten eine ganzheitliche Bedrohungsanalyse im Bereich der Landwirtschaft auf Komponentenebene durch. Dabei nutzen sie ebenfalls STRIDE um die Bedrohungen zu modellieren und um anschließend die identifizierten Bedrohungen einer Risikobewertung zu vollziehen. Allerdings vernachlässigen sie dabei die Bedrohungsanalyse der Cloud, der Sensoren und der

IoT-Knoten. Wie auch schon bei der Schwachstellenanylse ist auffällig, dass eine gesamtheitliche Analyse eines IoT-Systems oder Gerätes selten durchgeführt wird.

Die letzten drei Arbeiten haben sich mit der Entwicklung von Frameworks zur Bedrohungsanalyse befasst. In der Arbeit von Beyrouti et al., 2023 [17] wird ein Ansatz eines Frameworks zur Schwachstellen- und Bedrohungsanalyse vorgestellt. Diese arbeitet mit externen Datenbanken und stellt eine Liste an Common Weakness Enumeration (CWE) zusammen um diesen anschließend Common Vulnerabilities and Exposures (CVE)'s zuzuordnen. Darauf wird dann für jedes CVE ein Angriffsmuster für eine oder mehrere Komponenten des IoT-Systems identifiziert. Der Vorgang wurde manuell vollzogen, weswegen die Zuordnung von CVE zu Angriffsmuster erhebliche Arbeit erfordert. Srikumar et al., 2022 [59] stellen ein Framework vor, welches auf STRIDE basiert, aber den Faktor der physischen Bedrohungen mit betrachten soll. Sie erwähnen auch, dass exestierende Analysetechniken sich nur schwer auf IoT anwenden lassen und Datenflussdiagramme durch ihre Abstraktion den physischen Aspekt nicht darstellen können. Mit dem entwickelten Framework wurde eine Bedrohungsanalyse eines IoT-Gerätes durchgeführt und zum Vergleich auch eine mit STRIDE. Dabei wurde deutlich, dass das entwickelte Framework wesentlich mehr Bedrohungen, gerade im physischen Bereich, erkennen konnte. Die letzte Arbeit die sich mit der Bedrohungsanalyse befasst ist von Ankele et al., 2019 [9] bei der auf Anforderungen und Empfehlungen für Bedrohungsanalyse und Penetrationtesting im industriellen IoT-Sektor eingegangen wird. Dabei gehen sie auch auf die Automatisierung von Sicherheitstests ein. Diese sind oft umständlich, da die meisten Tools keine Software-APIs oder standardisierte Ausgabeformate bereitstellen. Aus diesem Grund ist es oft erforderlich, dass Sicherheitsprüfer und Penetrationstester die Ergebnisse manuell interpretieren und entsprechend den Ausgaben der Werkzeuge handeln.

Abschließend lässt sich sagen, dass die Herausforderungen bei der Identifikation von Schwachstellen, sowie bei der Bewertung von Bedrohungen und Risiken den gleichen Problemen entgegenstehen. Die Heterogenität, die physische Komponente IoT, die Ressourcenbeschränkung und die dynamische Umgebung in der sich ein Gerät befinden kann stellen hierbei die Hauptfaktoren dar, die es zu bewältigen gilt. Einige der vorgestellten Arbeiten befassen sich mit den genannten Aspekten, liefern jedoch keine eindeutigen Lösungsvorschläge. Da Sicherheitsanalysen von IoT noch ein vergleichsweise neues Forschungsfeld sind, ist diese Tatsache nicht überraschend. Dennoch ist es wichtig, diese

Punkte zu berücksichtigen, um Sicherheitsanalysen an IoT anzupassen und die bestehenden Techniken und Methoden weiterzuentwickeln. Der bestehende Mangel an Standardisierung lässt zum Schluss führen, einen einheitlichen Rahmen für die Durchführung von Bedrohungs- und Schwachstellenanalysen zu entwickeln. Die Weiterentwicklung dieser im IoT-Bereich und die Einführung von standardisierten Vorgehensweisen sind entscheidend, um eine effektive Sicherheitsstrategie für IoT-Geräte und -Systeme zu gewährleisten. Diese Erkenntnisse bilden eine Grundlage für die Anpassung und Verbesserung von Sicherheitsanalysen im Bereich IoT.
Daher werden im folgenden auf die bestehenden, sowie neuen Ansätze der Sicherheitsanalyse eingegangen.

4.2.2 Praktische Lösungsansätze

In diesem Abschnitt werden die Lösungsansätze die in den Arbeiten verwendet wurden näher beschrieben. Dabei werden bewährte Techniken und Methoden der Schwachstellenanalyse untersucht, darunter automatisierte Scanning-Tools, Penetrationstests, Angriffsgraphen, Fuzzing, Reverse Engineering und Hardware-Hacking. Methoden und Techniken der Bedrohungsanalyse sind unter anderem die Anwendung von STRIDE-Modell, weiteren Techniken zur Bedrohungsmodellierung und Risikobewertungstechniken zur Identifizierung und Klassifizierung von potenziellen Bedrohungen. Neue Ansätze zur Verhaltensanalyse von IoT-Geräten und die Automatisierung tragen dazu bei, den Bedrohungserkennungsprozess zu verbessern. Des weiteren werden neue Ansätze und Technologien vorgestellt, die zur Weiterentwicklung der Sicherheitsanalyse im IoT-Bereich beitragen. Die Anwendung von KI und maschinellem Lernen zur Erkennung von Anomalien und verdächtigem Verhalten, die Nutzung der Blockchain-Technologie zur Verbesserung der Datensicherheit und Integrität sind Beispiele für die neuesten Entwicklungen.

4.2.2.1 Bestehende Ansätze und Technologien

In den Arbeiten, die sich auf Schwachstellen fokussieren, wurden Technologien und Ansätze thematisiert, die auch in der Sicherheitsanalyse von normalen IT-Systemen Anwendung finden. Schaubild 4.1 stellt eine Übersicht über die Technologien inklusive der Arbeiten, in denen sie thematisiert wurden, dar.

Scanning-Tools werden eingesetzt um potenzielle Schwachstellen zu identifizieren. In

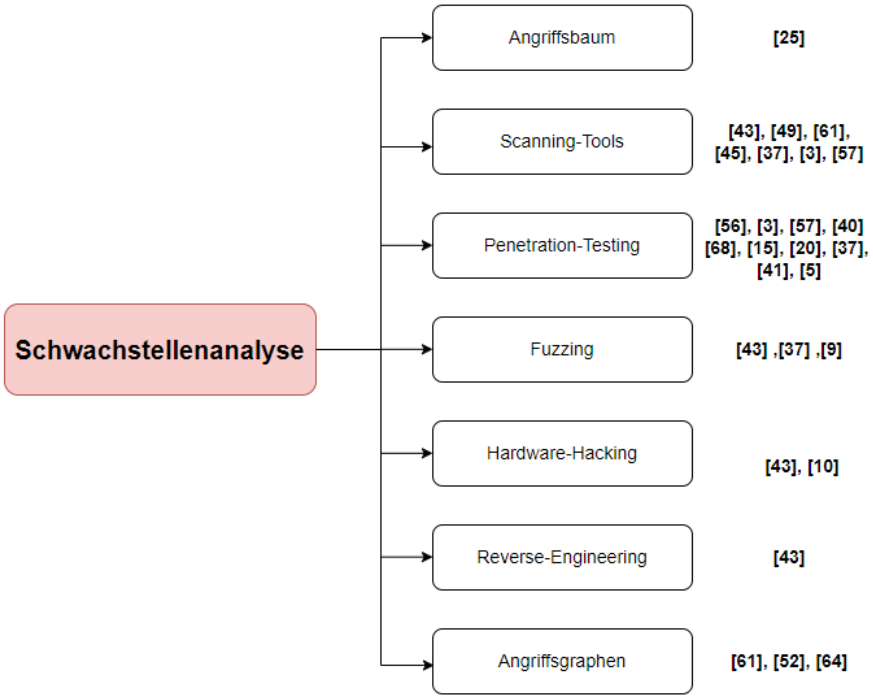

Abbildung 4.1: Ansätze und Technologien der Schwachstellenanalyse

mehreren Fällen wurde die Software Nessus genannt, die als Schwachstellen- und Netzwerkscanner dient. Ebenfalls fand das Open-Source-Tool Zeek Erwähnung in mehreren Arbeiten. Dabei handelt es sich um eine Software mit der sich der Netzwerkverkehr analysieren lässt. Beide Tools wurden eingesetzt um in einem IoT-Gerät Schwachstellen ausfindig zu machen, um diese anschließend auszunutzen. Weitere Tools, die im Penetration-Testing Anwendung finden und auch zu den Scanning-Tools gezählt werden können, sind Wireshark und Nmap. Bei Ersterem handelt es sich um ein Netzwerk-Tool, welches den Datenverkehr analysiert und helfen kann Sicherheitsprobleme im Netzwerk zu identifizieren, wie Botnet-Angriffe. Beim Penetrationtesting wurde öfter auf Kali-Linux verwiesen. Diese Linux-Distribution wurde speziell für Penetrationtests entwickelt und bietet eine Sammlung an Tools und Programmen, um Schwachstellen zu identifizieren und auszunutzen. Darunter befinden sich auch Schwachstellen-Scanner, aber auch Sniffer und Reverse-Enigneering-Tools.
Fuzzing fand in zwei Arbeiten Erwähnung. Zum Einen bei der Erstellung eines Frameworks zur Schwachstellenerkennung, welches mit einer Abfolge verbundener Tools und Software arbeitet, um Schwachstellen zu erkennen. Zum Anderen bei der Entwicklung eines Penetrationtesting Frameworks, welches auf maschinelles Lernen zurückgreift.

Hier wird Fuzzing zum Testen der identifizierten Schwachstellen eingesetzt. Reverse-Engineering wird zur Analyse von Firmware und Software eingesetzt, um potenzielle Schwachstellen ausfindig zu machen. In den untersuchten Arbeiten fand Reverse-Engineering nur bei der Erstellung des Frameworks, welches auf eine Abfolge von Tools basiert, Anwendung. Dabei soll Reverse-Engineering helfen Schwachstellen in der Firmware ausfindig zu machen.
Bei Hardware-Hacking handelt es sich um die Untersuchung der physischen Komponenten. Dies fand ebenfalls Anwendung in dem Framework, welches auf einer Abfolge von Tools aufgebaut ist. Es soll dabei behilflich sein Pins und Debug-Schnittstellen zu identifizieren um anschließend Code zu extrahieren, oder die Firmware auszulesen.
Drei der Arbeiten befassten sich mit Angriffsgraphen. Sie werden dazu eingesetzt Angriffszenarien und Abhängigkeiten zwischen einzelnen Schwachstellen darzustellen und somit einen gesamten Angriffspfad von Eintrittspunkt zum Ziel zu visualisieren. Zum Einen wurde der Angriffsgraph bei der Schwachstellenanalyse eines Industrie IoT-Gerätes angewandt, zum anderen bei der Schwachstellenanalyse bei RPL. Basierend auf den erstellten Graphen wurden erfolgreich Angriffe durchgeführt. Ebenfalls findet der Angriffsgraph Erwähnung bei der Entwicklung von Frameworks, welches eine Ende-zu-Ende Schwachstellenanalyse durchführen soll. Der Graph soll dabei helfen Schwachstellen zu entdecken, damit diese anschließend kombiniert werden können, um so einen Angriff von der Sensorik-Ebene bis zur Anwendungs-Ebene ausführen zu können. Der Angriffsbaum kommt bei einer Arbeit zum Einsatz. Dabei dienen die Kosten und der Schwierigkeitsgrad eines Angriffes sowie die Enteckungswahrscheinlichkeit einer Schwachstelle, die zu dem Angriff führen kann, als Bewertungsmerkmale. Darauf Aufbauend wird eine Schwachstellenanalyse an einem SCADA-System durchgeführt.

Genauso wie bei der Schwachstellenanalyse wurden etablierte Methoden der Bedrohungsanalyse ebenfalls auf den Bereich des IoT angewendet. Tabelle 4.2 zeigt die Übersicht der Arbeiten verteilt auf die Techniken.
STRIDE wurde dabei am Meisten für die Bedrohungsmodellierung eingesetzt. Dabei wird diese Methode in zwei Arbeiten im Rahmen der Framework-Entwicklung eingesetzt. In einem Fall wird sie genutzt um anfangs Parameter zu identifizieren, die potenziellen Angriffen ausgesetzt sind. Anschließend erfolgt eine Korrelation dieser Parameter mit Informationen aus einem Sicherheitsaudit. Die Zusammenführung dieser Erkenntnisse dient dann zur Identifikation möglicher Bedrohungen. Bei dem zweiten Framework handelt es sich um eine Erweiterung des STRIDE-Modells zu STRIPED, welches die physischen Bedrohungen denen IoT-Geräte ausgesetzt sind mit einbeziehen soll. Die Arbeit hat erge-

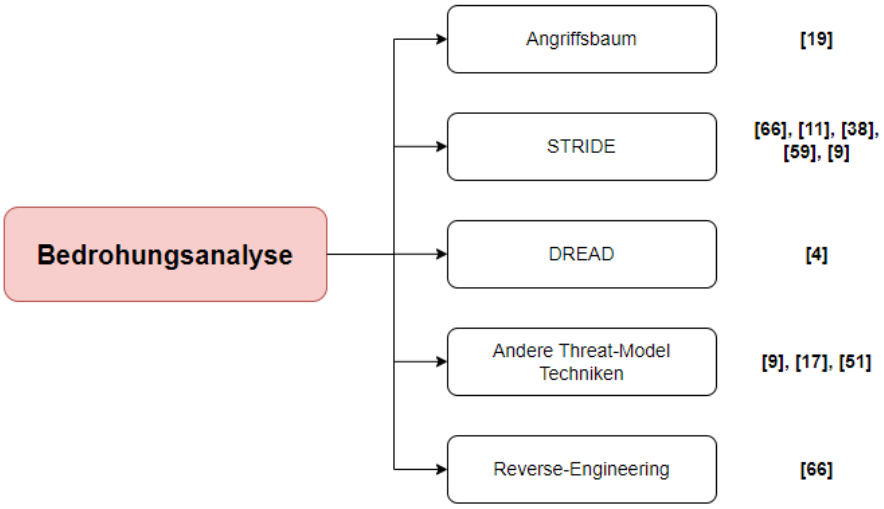

Abbildung 4.2: Ansätze und Technologien der Bedrohungsanalyse

ben, dass STRIPED die Bedrohungen rund um die physische Komponenten identifizieren kann, im Gegensatz zu STRIDE. Ebenfalls wird diese Methode bei der Bedrohungsmodellierung von IoT-Geräten eingesetzt. Dabei beruht die Modellierung in zwei Fällen auf ein vorher definiertes Datenfluss-Diagramm. Es soll helfen die Abstraktion besser zu verstehen. Eine weitere Arbeit nutzt STRIDE zur Bedrohungsmodellierung um anschließend eine Risikobewertung mit DREAD durchzuführen. Dabei wurde die Bedrohungsmodellierung auf die spezifischen Eigenschaften die IoT mit sich bringt angepasst.
Weitere Arten Bedrohungen zu identifizieren kann durch einen Angriffsbaum geschehen. In der Arbeit, in der diese Methode Anwendung findet wurden zuvor drei Bedrohungsakteure, denen das System ausgesetzt sein könnte, beschrieben. Anhand derer wurde für jedes Szenario ein Angriffsbaum erstellt.
In der Bedrohungsanalyse wird ebenfalls das Reverse Engineering eingesetzt. In diesem Zusammenhang soll es bei einem Framework eingesetzt werden, um nach einer erfolgreichen Bedrohungsmodellierung zusätzliche Bedrohungen insbesondere für die Firmware zu erkennen.
Weitere Methoden umfassen die Anwendung von CWE. So werden in einer Arbeit mittels CWE Risiken klassifiziert, die daraufhin entsprechenden Komponenten zugeordnet werden. Anschließend werden relevante Schwachstellen abgeleitet, auf Grund derer Angriffspfade für die bedrohten Komponenten erstellt wird. Ebenso kann die Bedrohungsmodellierung deskriptiv geschehen. Dabei wurde IoT im Gesamten in drei große An-

wendungsbereiche aufgeteilt und anhand eines IoT-Gerätes, welches in diesem Bereich Anwendung findet, wurden die möglichen Bedrohungen beschrieben.

Die untersuchten Arbeiten haben verschiedene etablierte Techniken und Methoden der Sicherheitsanalyse angewandt. Diese wurden entweder direkt übernommen oder speziell auf den IoT-Bereich zugeschnitten. Insbesondere bei der Entwicklung von Frameworks lag der Fokus auf der individuellen Anpassung.

4.2.2.2 Neue Ansätze und Technologien

In diesem Abschnitt soll auf neue Ansätze und Technologien eingegangen werden, die als Ergänzung oder Verbesserung der bisherigen Ansätze und Technologien für Sicherheitsanalysen im Bereich IoT dienen können. Wenige der untersuchten Arbeiten haben neue Ansätze vorgestellt, oder sind näher auf solche eingegangen. Lediglich eine Arbeit hat sich intensiver mit der Weiterentwicklung der gängigen Methode zur Bedrohungsmodellierung STRIDE auseinandergesetzt. Wie bereits im vorherigen Abschnitt erläutert wurde, wird versucht, den physischen Aspekt des IoT in die Analyse einzubeziehen. Dabei wurde deutlich, dass diese Herangehensweise Bedrohungen identifiziert, die durch Anwendung vonSTRIDE nicht erfasst worden wären [59].
Ebenfalls wurde der Einsatz von Automatisierung des öfteren erwähnt, jedoch nicht im Detail genauer untersucht. Dabei kann der Einsatz bestimmter Tools oder Skripte zur schnelleren Erkennung und Abwehr von Angriffen beitragen. Die manuell durchgeführten Schwachstellenanalysen sind zeitaufwendig und schwer zu skalieren. Hier kann Automatisierung eine Lösung bieten, da Analysen kontinuierlich und in kürzerer Zeit durchgeführt werden können. Ebenso gewährleistet sie Kontinuität und dient Fehlerreduzierung. Ein weiterer Vorteil von Automatisierung ist die Kostenreduktion, sowie die effiziente Nutzung von Ressourcen. Es sei jedoch darauf hingewiesen, dass Automatisierung nur in gut erforschten Bereichen eingesetzt werden kann, da sie auch bei komplexen Szenarien und Bedrohungen ihre Grenzen hat [64].
Eine weitere Technologie auf die verwiesen wurde ist die des maschinellen Lernens oder Künstliche Intelligenz (KI). Diese kann dabei helfen Anomalien und Bedrohungen in Echtzeit zu erkennen. Durch Erlernen der normalen Verhaltensmuster von IoT-Geräten oder Systemen können sie ungewöhnliche Aktivitäten erkennen. Gerade im Bereich IoT kann diese Art der Technologie von Nutzen sein, da IoT-Geräte und Systeme Unmengen an Daten produzieren, die zum Training des KI-Modells genutzt werden können. Da-

durch können sie unter anderem auch Angriffsmuster aufdecken, die bei einer manuellen Sicherheitsanalyse übersehen werden könnte [37].
Zusammenfassend kann man sagen, dass die Arbeiten der Literaturrecherche recht wenig neue Ansätze und Technologien besprochen haben. Zwar wurde für die Schwachstellenanalyse als auch die Bedrohungsanalyse Ansätze von neuen Frameworks vorgestellt, doch basierten diese meist auf bestehenden Technologien und Methoden der Sicherheitsanalyse. Grund hierfür könnten unter anderem die in Kapitel 4.2.1 genannten Aspekte sein. Neue Ansätze für komplexe IoT-Geräte und Systeme zu entwickeln und einzusetzen erfordert Zeit und Ressourcen. Ebenfalls muss die Ressourcenbeschränkung der Geräte selbst bedacht werden. So müssen neue Ansätze und Technologien ressourceneffizient Arbeiten und gleichzeitig eine Verbesserung bestehender Ansätze darstellen. Auch wenn neue Ansätze effektiver gegenüber etablierten sind, so darf auch hier nicht vergessen werden, dass diese erst erprobt werden müssen und es einige Zeit bedarf, bis sie den Herausforderungen von IoT angepasst wurden. Dennoch gilt es, trotz dieser Herausforderungen weiter an effektiven und auf IoT-Geräte angepasste Sicherheitsanalysen zu forschen und zu entwickeln.

5 Diskussion

Ziel dieser Arbeit war es die Sicherheitsanalysen im Kontext von IoT näher zu betrachten. Hierbei wurde sowohl die Entwicklung der Sicherheitsanalyse in den vergangenen Jahren betrachtet, als auch auf die aktuellen Lösungsansätze mit ihren Herausforderungen und methodischen Herangehensweisen analysiert. In diesem Kapitel soll auf die gewonnenen Erkenntnisse der voran gegangenen Arbeit eingegangen werden. Zunächst erfolgt eine prägnante Zusammenfassung der durchgeführten systematischen Literaturrecherche, gefolgt von der Darlegung der daraus resultierenden Ergebnisse. Dabei werden nicht nur die positiven Resultate betrachtet, sondern auch die auftretenden Herausforderungen der Untersuchung näher betrachtet. Ebenfalls erfolgt eine kritische Reflexion über den Ablauf der Arbeit mit etwaigen Einschränkungen.
Dabei wird zunächst die Entwicklung von Sicherheitsanalysen näher betrachtet, gefolgt von einer Evaluierung der aktuellen Lösungsansätze, mit Fokus auf die Effektivität bestehender Ansätze.
Eine Auseinandersetzung mit den Ergebnissen, Herausforderungen und Diskussion ermöglicht eine umfassende Bewertung des Themas der Sicherheitsanalysen im IoT-Kontext in Bezug auf ihre Entwicklung und aktuelle Anwendung.

5.1 Entwicklung von Sicherheitsanalysen im Kontext von IoT

Um die Forschungsfragen beantworten zu können wurde zunächst eine systematische Literaturrecherche durchgeführt. Das genaue Vorgehen wird in Kapitel 3 näher erläutert. Um möglichst relevante Arbeiten zur Beantwortung der Forschungsfragen zu finden, wurde vorab ein detaillierter Plan erstellt. Dieser Plan beinhaltet spezifische Quellen, Schlagwörter und zusätzliche Kriterien, anhand derer die Relevanz von Arbeiten bestimmt wurde. Nachdem die Datenbanken durchsucht wurden und die gesammelten Arbeiten den Kriterien unterzogen wurden, blieben nur 39 Arbeiten über, die genauer analysiert wurden

um die Forschungsfragen beantworten zu können.
Ein wichtiger Aspekt dieses Auswahlverfahrens betrifft den Zeitraum der Veröffentlichung der Arbeiten, der auf den Zeitraum von 2013 bis 2023 festgelegt wurde. Diese zeitliche Begrenzung diente dazu, die erste Forschungsfrage zu beantworten, die sich mit der Entwicklung von Sicherheitsanalysen im Kontext des IoT befasst. Aus den zu analysierenden Arbeiten konnte jedoch kein klar erkennbarer Trend abgeleitet werden. Dies kann auf die sehr spezifischen Auswahlkriterien zurückzuführen sein, was dazu führte, dass die Anzahl der zu analysierenden Arbeiten sehr begrenzt war und sich daraus kein Trend ableiten lässt. Ein weiterer Faktor, der die Ergebnisse beeinflusst hat, ist die Tatsache, dass im Bereich der Sicherheitsanalyse häufig Synonyme verwendet werden, insbesondere in der englischsprachigen Literatur. Dies führte dazu, dass Arbeiten, die als relevant eingestuft werden könnten, nicht berücksichtigt wurden, da sie nicht mit den zuvor festgelegten Suchstrings überein stimmten.
Um eine klarere Aussage über die zeitliche Entwicklung treffen zu können, hätte es einer umfangreicheren Literaturrecherche bedarf. Da IoT in vielen Bereichen Anwendung gefunden hat, ist davon auszugehen, dass auch die Sicherheit und somit die Zahl der Sicherheitsanalysen von IoT-Geräten und IoT-Technologien zunehmen wird.

5.2 Bewertung der aktuellen Lösungsansätze

In diesem Absatz soll eine Bewertung der aktuellen Lösungsansätze erfolgen. Um die aktuellen Lösungsansätze der IoT Sicherheitsanalysen zu identifizieren, wurden die ausgewählten Arbeiten der Literaturrecherche genauer betrachtet. Dabei wurden die Arbeiten in Schwachstellenanalyse, Bedrohungsanalyse und Penetrationtesting unterteilt. Grund hierfür ist, dass es je nach Analyse unterschiedliche Methoden und Techniken gibt. Penetrationtesting lässt sich zwar zur Schwachstellenanalyse zählen, es wurde sich aber für eine gesonderte Betrachtung dieser Sicherheitsanalyse-Technik entschieden um die Methoden besser vergleichen zu können.
Dabei lassen sich die Lösungsansätze zum Einen auf einen bestimmten Anwendungsbereich einteilen, wie IoT-Protokoll, IoT-Gerät oder System, oder aber auf die Entwicklung eines Frameworks. Ebenso wurden Fallbeispiele untersucht, die die Vorgänge beim Penetrationtesting aufzeigen sollen. Dabei wurde deutlich, dass im Bereich IoT etablierte Methoden der Sicherheitsanalysen angewandt wurden. Dennoch zeigte sich, dass IoT als Ganzes einige Herausforderungen mit sich bringt.
Bei der Schwachstellenanalyse lassen sich die Herausforderungen auf die Heterogenität

der Geräte, sowie die Ressourcen-Beschränkung zurückführen. Es gibt eine Vielzahl an Technologien, Protokollen und Standards, die von verschiedenen Herstellern entwickelt wurden. Diese Vielzahl erschwert die nahtlose Integration und Kommunikation zwischen den Geräten. Dies erhöht auch die Angriffsfläche für potenzielle Sicherheitsbedrohungen und schafft Schwachstellen, die von Angreifern ausgenutzt werden können. Durch die begrenzten Ressourcen stehen oftmals geringer Speicherplatz, sowie geringe Rechenleistung zur Verfügung. Gängige Sicherheitsmethoden lassen sich daher schwer auf IoT-Geräte übertragen und integrieren. Sicherheitsfunktionen werden aufgrund von technischen Einschränkungen nicht aktiviert, was die Anfälligkeit gegenüber Angriffen erhöhen kann. Ebenso ist die Datenrate in den Netzwerken, sowie die Packetgröße oftmals beschränkt, sodass manche Mechanismen nicht eingesetzt werden können. Aber auch Sicherheitsupdates können auf Grund von Verbindungsproblemen zu dem IoT-Gerät nicht aufgespielt werden. Dieses Problem betrifft auch den Updatemechanismus der Firmware.
Eine große Herausforderungen der IoT-Geräte ist, dass sie physisch zugänglich sind. So kann ein Angreifer bei physischem Zugriff das Gerät manipulieren, oder gar stehlen. Auch kann versucht werden die Firmware zu manipulieren oder aktualisieren, um so Schwachstellen auszunutzen oder eine Hintertür einbauen. Ebenfalls können Angreifer versuchen die Daten direkt aus dem IoT-Gerät zu stehlen, was zur Datenschutzverletzung führt. Auch kann der physische Zugriff Auswirkungen auf das gesamte Netzwerk haben. Sollten Angreifer Zugriff auf ein IoT-Gerät erlangen, so können sie dies als Einstiegspunkt nutzen um Zugriff auf das Netzwerk zu erlangen.
Ähnlich wie bei der Sicherheitsanalyse mangelt es bei der Bedrohungsanalyse von IoT auch an der Betrachtung der physischen Komponente des IoT. Zwar wiesen zwei Arbeiten darauf hin, diese auch zu betrachten, dennoch wird sie oft nicht mit gedacht. Daher ist das Gerät oft fragiler und anfälliger für Bedrohungen, als die Software die auf ihr läuft. Die Bedrohungsanalyse ist im Bereich der Sicherheit eine gängige Praxis. Allerdings ist sie für den IoT-Bereich noch nicht ausgereift genug, und es kommt häufig vor, dass Bedrohungen übersehen werden. Eine weitere Beobachtung ist, dass die in den durchgeführten Arbeiten verwendeten Taxonomien oft voneinander abweichen, was es erschwert, Vergleiche durchzuführen und die Analysen effektiv zu bewerten. Ebenfalls ist die Funktionalität der IoT-Geräte und Systeme das, was es in der realen Welt ausmacht. Daher werden Bedrohungen oft nicht identifiziert, da die meisten Analysen in einer extra konzipierten Testumgebung durchgeführt werden. Ein weiterer Punkt ist, dass die IoT-Technologien sich rasant entwickeln und die Bedrohungsanalysen angepasst werden müssen. Des weiteren darf das menschliche Verhalten nicht vernachlässigt werden. Die Interaktion von Menschen mit IoT-Geräten kann zu Sicherheitsrisiken führen,

sei es durch fahrlässiges Verhalten oder soziale Manipulation. So kann z.B. ein Patient mit einem medizinischen IoT-Gerät sich dieses selbst entfernen, ohne wirklich böswillige Absichten zu haben. Die Bewertung der Effektivität der bestehenden und angewandten Ansätze wird im Folgenden näher erläutert.

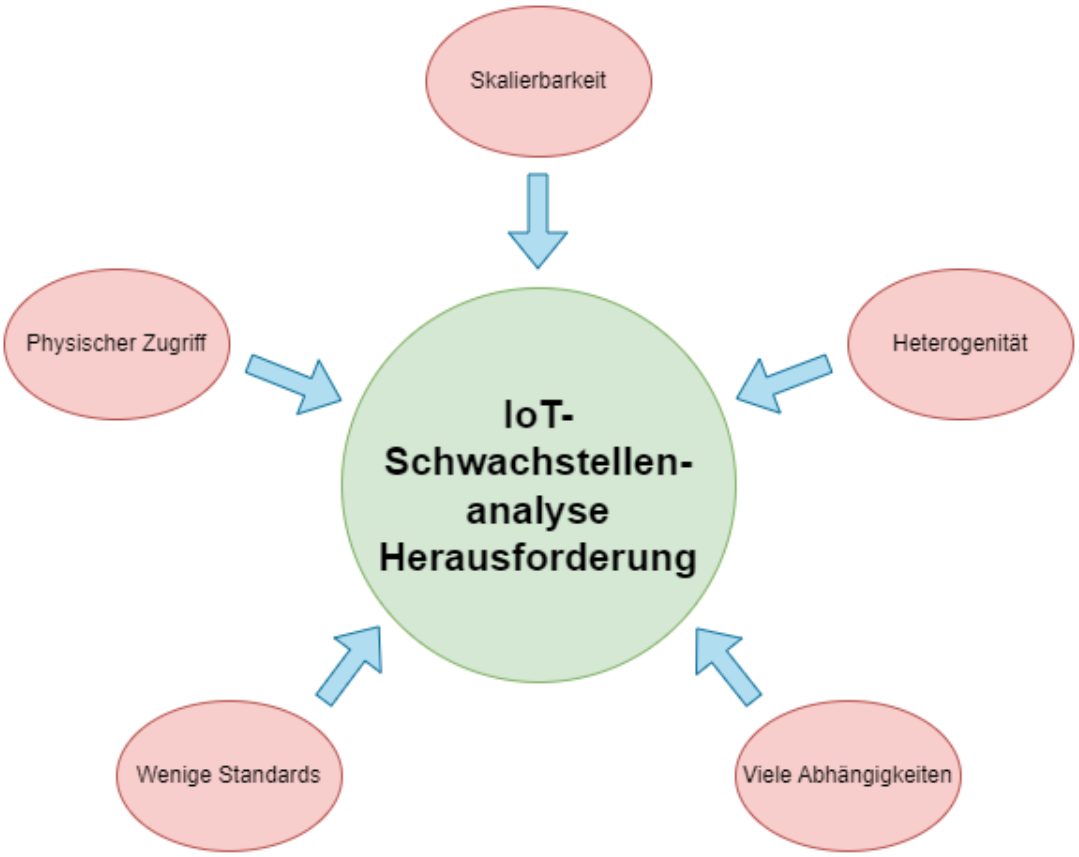

Abbildung 5.1: Übersicht der Herausforderungen bei Sicherheitsanalysen im Bereich IoT

5.2.1 Effektivität der bestehenden Ansätze

Im Bereich IoT gibt es einige Faktoren, die die Effektivität von Sicherheitsanalysen beeinflussen. Zum Einen sollte betrachtet werden, wie gut die eingesetzten Methoden bei der Identifizierung von Schwachstellen und Bedrohungen sind. Aber nicht nur bekannte Schwachstellen und Bedrohungen sollten gut identifizierbar sein. Gerade IoT bringt eine Vielzahl neuer Bedrohungen mit sich, da z.B., anders als in normalen IT-Systemen, die physische Komponente eine große Rolle spielt.

Die angewandten Lösungsansätze lieferten relativ gute Ergebnisse. Dennoch darf nicht außer Acht gelassen werden, dass die Analysen auf einen genau definierten Rahmen festgelegt wurden. Keine der Analysen wurde in einem Umfeld durchgeführt, dass nicht gewisse Vorbedingungen voraussetzt. Das führt dazu, dass Schwachstellen und Bedrohungen übersehen werden, da sie nicht Teil des Versuchaufbaus sind.
Viele der Arbeiten konzentrieren sich zudem oft auf spezifische Aspekte von IoT-Geräten oder Technologien und vernachlässigen dabei häufig den physischen Zugriff auf IoT-Geräte, obwohl gerade in kritischen Infrastrukturbereichen oder im medizinischen Bereich schwerwiegende Konsequenzen drohen könnten, falls die Geräte dort kompromittiert werden. Einige der untersuchten Arbeiten haben versucht diesen Aspekt zu berücksichtigen und konnten zum Teil Erfolge erzielen und aufweisen, dass der neu entwickelte Ansatz effektiver gegenüber dem etablierten Ansatz ist.
Die Tatsache, dass IoT-Geräte oft in größeren Netzwerken oder Ökosystemen interagieren und somit zahlreiche Abhängigkeiten zu anderen Geräten bestehen, stellt die Schwachstellenanalyse vor weitere Herausforderungen. In diesem Zusammenhang können die Geräte als Einstiegspunkt genutzt werden, wenn Schwachstellen ausgenutzt werden und somit das gesamte System gefährden. Ebenso kann ein IoT-System aus mehreren IoT-Geräten bestehen, was dazu führt, dass Analysen skalierbar sein müssen. Denn IoT-Systeme können aus einer nicht vorher fest definierten Anzahl an Geräten bestehen. Ebenso können die Verbindungen und Beziehungen der Geräte sich ändern.
Darüber hinaus erschwert der Mangel an Standards für IoT-Technologien und Hardware- sowie Software-Komponenten eine standardisierte Durchführung von Schwachstellenanalysen. Punkte die in den analysierten Arbeiten eher wenig Beachtung fanden, waren unter anderem die Anpassungsfähigkeit von den angewandten Methoden an bereits bestehende IoT-Anwendungen und Umgebungen. Da es sich bei Sicherheitsanalysen idealerweise um einen fortlaufenden Prozess handelt, sollte diese auch durchgeführt werden, während die Geräte oder Systeme schon im Einsatz sind. Denn es kann vorkommen, dass die Bedingungen sich ändern und neue Bedrohungen oder Schwachstellen auftauchen.
Abschließend lässt sich sagen, dass die eingesetzten Methoden zur Durchführung der Schwachstellen- und Bedrohungsanalyse im Bereich IoT anwendbar sind, sofern sie einen bestimmten Aspekt des IoT betrachten. Es mangelt dennoch an einer ganzheitlichen Lösung zur Identifizierung von Schwachstellen und Identifikation sowie Bewertung von Bedrohungen.

5.2.2 Ausblick

Nach Betrachtung und Bewertung der bestehenden Lösungsansätze lässt sich sagen, dass die Forschung zum Thema Sicherheitsanalysen im Bereich IoT noch einige Herausforderungen zu bewältigen hat. Ein wichtiger Aspekt besteht darin, dass Analysetools und Methoden zur Identifizierung von Schwachstellen und Bedrohungen im IoT-Bereich den physischen Aspekt des IoT-Geräts berücksichtigen sollten, da dieser einen erheblichen Anteil ausmacht. Zudem sollten Datenbanken zu CVSS und CWE Schwachstellen und Bedrohungen die speziell IoT betreffen aufnehmen. Des Weiteren muss sich auf Standardisierung fokussiert werden. Die Vielzahl an Herstellern und Akteuren im IoT-Bereich erfordert eine individuelle Anpassung von Sicherheitsanalysen für jedes einzelne Gerät oder System. Dies hat zur Folge, dass Sicherheitsbewertungen und -maßnahmen mühsam für jede spezifische Komponente durchgeführt werden müssen. Um diesem Problem zu begegnen, sollte sich insbesondere auf den Aspekt der Standardisierung fokussiert werden. Ein solcher Standardisierungsansatz könnte dazu führen, dass bestimmte IoT-Geräte, Systeme und Anwendungen gewisse gemeinsame Merkmale aufweisen. Dies würde ermöglichen, dass Sicherheitsanalysen in verschiedene Bereiche unterteilt werden können. Durch die Einführung von Standards könnte eine gewisse Homogenität in Bezug auf Sicherheitsanforderungen und -bewertungen erreicht werden, was die Effizienz von Sicherheitsmaßnahmen und -analysen erhöhen würde. Gleichzeitig hätte die Implementierung von Automatisierung das Potenzial, die zeitintensiven und ressourcenintensiven manuellen Sicherheitsanalysen auf effizientere Weise durchzuführen. Ebenso können neue Technologien wie maschinelles Lernen hierbei unterstützend wirken, gerade in Anbetracht der vielen Daten mit denen IoT-Geräte und Systeme arbeiten. Eine effizientere Anomalieerkennung und Mustererkennung kann zu frühzeitigem Erkennen von Angriffen führen.

6 Fazit

Das Ziel dieser Arbeit ist es Sicherheitsanalysen im Kontext von IoT näher zu betrachten und näher auf die Entwicklung dieser einzugehen. Ebenso sollten Herausforderungen, die Sicherheitsanalysen im Bereich IoT mit sich bringen näher betrachtet werden, sowie aktuelle und neue Lösungsansätze zur Umsetzung beschrieben werden. Um dies zu erreichen wurde eine systematische Literaturrecherche durchgeführt, welche relevante Arbeiten liefern soll, um die Fragestellungen adäquat zu beantworten. Die Literaturrecherche wurde detailliert protokolliert und anschließend ausgewertet. Dabei zeigte sich zum Einen, dass die Literaturrecherche im Hinblick auf die zeitliche Entwicklung einen zu kleinen Umfang hatte um eine klare Tendenz erkennbar zu machen. Dennoch konnten einige wissenswerte Informationen zu Herausforderungen bei Sicherheitsanalysen im Bereich IoT gesammelt werden. Ebenso wurde deutlich, dass etablierte Ansätze und Technologien sich auch zum Teil auf IoT übertragen lassen. Dennoch muss betont werden, dass es in dem Bereich noch viele offene Fragen und Herausforderungen gibt, die es zu bewältigen gilt. Gerade mit dem Aspekt im Hintergrund, dass IoT immer öfter und in immer mehr Bereichen im alltäglichen Leben, der Industrie und kritischen Infrastruktur Anwendung findet. Ganzheitliche Sicherheitsanalysen lassen sich zwar schwer umsetzen, jedoch sollte an Lösungen gearbeitet werden um diese effektiver zu gestalten. Einige Vorschläge und neue Technologien, die in dieser Arbeit vorgestellt wurden könnten dabei behilflich sein.

Literaturverzeichnis

[1] *Internet der Dinge - Deutschland.* https://de.statista.com/outlook/tmo/internet-der-dinge/deutschland. – Letzter Zugriff: 08.08.2023

[2] *OWASP Internet of Things Project.* https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10. – Letzter Zugriff: 08.08.2023

[3] Abdalla, Peshraw A. ; Varol, Cihan: Testing IoT Security: The Case Study of an IP Camera. In: *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 2020, S. 1–5

[4] Akatyev, Nikolay ; James, Joshua I.: Evidence identification in IoT networks based on threat assessment. In: *Future Generation Computer Systems* 93 (2019), S. 814–821. – URL https://www.sciencedirect.com/science/article/pii/S0167739X17300857. – ISSN 0167-739X

[5] Almazrouei, Omar ; Magalingam, Pritheega ; Kamrul Hasan, Mohammad ; Almehrzi, Majed ; Alshamsi, Ahmed: Penetration Testing for IoT Security: The Case Study of a Wireless IP Security CAM. In: *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, 2023, S. 1–5

[6] Alramadhan, Mousa ; Sha, Kewei: An Overview of Access Control Mechanisms for Internet of Things. In: *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 2017, S. 1–6

[7] Anand, Pooja ; Singh, Yashwant ; Selwal, Arvind ; Alazab, Mamoun ; Tanwar, Sudeep ; Kumar, Neeraj: IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. In: *IEEE Access* 8 (2020), S. 168825–168853

[8] Andrea, Ioannis ; Chrysostomou, Chrysostomos ; Hadjichristofi, George: Internet of Things: Security vulnerabilities and challenges. In: *2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, S. 180–187

[9] Ankele, Ralph ; Marksteiner, Stefan ; Nahrgang, Kai ; Vallant, Heribert: Requirements and Recommendations for IoT/IIoT Models to Automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. New York, NY, USA : Association for Computing Machinery, 2019 (ARES '19). – URL https://doi.org/10.1145/3339252.3341482. – ISBN 9781450371643

[10] Arpaia, Pasquale ; Bonavolontà, Francesco ; Cioffi, Antonella ; Moccaldi, Nicola: Power Measurement-Based Vulnerability Assessment of IoT Medical Devices at Varying Countermeasures for Cybersecurity. In: *IEEE Transactions on Instrumentation and Measurement* 70 (2021), S. 1–9

[11] Asif, Md. Rashid A. ; Hasan, Khondokar F. ; Islam, Md Z. ; Khondoker, Rahamatullah: STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems. In: *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, 2021, S. 1–6

[12] Atamli, Ahmad W. ; Martin, Andrew: Threat-Based Security Analysis for the Internet of Things. In: *2014 International Workshop on Secure Internet of Things*, 2014, S. 35–43

[13] Atamli, Ahmad W. ; Martin, Andrew: Threat-Based Security Analysis for the Internet of Things. In: *2014 International Workshop on Secure Internet of Things*, 2014, S. 35–43

[14] Beelmann, Andreas: *Systematische Reviews und Meta-Analysen*. S. 687–717. In: Niederberger, Marlen (Hrsg.) ; Finne, Emily (Hrsg.): *Forschungsmethoden in der Gesundheitsförderung und Prävention*. Wiesbaden : Springer Fachmedien Wiesbaden, 2021. – URL https://doi.org/10.1007/978-3-658-31434-7_25

[15] Bella, Giampaolo ; Biondi, Pietro ; Bognanni, Stefano ; Esposito, Sergio: PETIoT: PEnetration Testing the Internet of Things. In: *Internet of Things* 22 (2023), S. 100707. – URL https://www.sciencedirect.com/science/article/pii/S2542660523000306. – ISSN 2542-6605

[16] Berger, Christian ; Eichhammer, Philipp ; Reiser, Hans P. ; Domaschka, Jörg ; Hauck, Franz J. ; Habiger, Gerhard: A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. In: *ACM Comput. Surv.* 54 (2021), sep, Nr. 7. – URL https://doi.org/10.1145/3462513. – ISSN 0360-0300

[17] Beyrouti, Mohammad ; Lounis, Ahmed ; Lussier, Benjamin ; Bouadallah, Abdelmadjid ; Samhat, Abed E.: Vulnerability and Threat Assessment Framework for Internet of Things Systems. In: *2023 6th Conference on Cloud and Internet of Things (CIoT)*, 2023, S. 62–69

[18] Bhattasali, Tapalina ; Chaki, Rituparna ; Sanyal, Sugata: Sleep Deprivation Attack Detection in Wireless Sensor Network. In: *ArXiv* abs/1203.0231 (2012)

[19] Bradbury, Matthew ; Jhumka, Arshad ; Watson, Tim ; Flores, Denys ; Burton, Jonathan ; Butler, Matthew: Threat-Modeling-Guided Trust-Based Task Offloading for Resource-Constrained Internet of Things. In: *ACM Trans. Sen. Netw.* 18 (2022), feb, Nr. 2. – URL https://doi.org/10.1145/3510424. – ISSN 1550-4859

[20] Chu, Ge ; Lisitsa, Alexei: Penetration Testing for Internet of Things and Its Automation. In: *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, S. 1479–1484

[21] Eceiza, Maialen ; Flores, Jose L. ; Iturbe, Mikel: Fuzzing the Internet of Things: A Review on the Techniques and Challenges for Efficient Vulnerability Discovery in Embedded Systems. In: *IEEE Internet of Things Journal* 8 (2021), Nr. 13, S. 10390–10411

[22] Eceiza, Maialen ; Flores, Jose L. ; Iturbe, Mikel: Fuzzing the Internet of Things: A Review on the Techniques and Challenges for Efficient Vulnerability Discovery in Embedded Systems. In: *IEEE Internet of Things Journal* 8 (2021), Nr. 13, S. 10390–10411

[23] Fang, Zheng ; Fu, Hao ; Gu, Tianbo ; Hu, Pengfei ; Song, Jinyue ; Jaeger, Trent ; Mohapatra, Prasant: Towards System-Level Security Analysis of IoT Using Attack Graphs. In: *IEEE Transactions on Mobile Computing* (2022), S. 1–15

[24] Farooq, M. U. ; Waseem, Muhammad ; Khairi, Anjum ; Mazhar, Sadia: A Critical Analysis on the Security Concerns of Internet of Things (IoT). In: *International Journal of Computer Applications* 111 (2015), S. 1–6

[25] Fei, Jiaxuan ; Chen, Kai ; Yao, Qigui ; Guo, Qian ; Wang, Xiangqun: Security Vulnerability Assessment of Power IoT Based on Business Security. In: *Proceedings of the 2020 1st International Conference on Control, Robotics and Intelligent System*. New York, NY, USA : Association for Computing Machinery, 2021 (CCRIS '20), S. 128–135. – URL https://doi.org/10.1145/3437802.3437825. – ISBN 9781450388054

[26] Feng, Xiaotao ; Zhu, Xiaogang ; Han, Qing-Long ; Zhou, Wei ; Wen, Sheng ; Xiang, Yang: Detecting Vulnerability on IoT Device Firmware: A Survey. In: *IEEE/CAA Journal of Automatica Sinica* 10 (2023), Nr. 1, S. 25–41

[27] GhaffarianHoseini, AmirHosein ; Dahlan, Nur D. ; Berardi, Umberto ; GhaffarianHoseini, Ali ; Makaremi, Nastaran: The essence of future smart houses: From embedding ICT to adapting to sustainability principles. In: *Renewable and Sustainable Energy Reviews* 24 (2013), S. 593–607. – URL https://www.sciencedirect.com/science/article/pii/S1364032113001342. – ISSN 1364-0321

[28] Gupta, Aditya: In: *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things*. Berkeley, CA isbn= : Apress, 2019

[29] Guzman, Aaron ; Gupta, Aditya: *IoT Penetration Testing Cookbook: Identify Vulnerabilities and Secure Your Smart Devices*. Packt Publishing, 2017. – ISBN 1787280578

[30] HaddadPajouh, Hamed ; Dehghantanha, Ali ; M. Parizi, Reza ; Aledhari, Mohammed ; Karimipour, Hadis: A survey on internet of things security: Requirements, challenges, and solutions. In: *Internet of Things* 14 (2021), S. 100129. – URL https://www.sciencedirect.com/science/article/pii/S2542660519302288. – ISSN 2542-6605

[31] Hassija, Vikas ; Chamola, Vinay ; Saxena, Vikas ; Jain, Divyansh ; Goyal, Pranav ; Sikdar, Biplab: A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. In: *IEEE Access* 7 (2019), S. 82721–82743

[32] Jabraeil Jamali, Mohammad A. ; Bahrami, Bahareh ; Heidari, Arash ; Allahverdizadeh, Parisa ; Norouzi, Farhad: *IoT Security.* S. 33–83. In: *Towards the Internet of Things: Architectures, Security, and Applications.* Cham : Springer International Publishing, 2020. – ISBN 978-3-030-18468-1

[33] Jamil, Danish ; Zaki, Hassan: Security issues in cloud computing and countermeasures. In: *International Journal of Engineering Science and Technology (IJEST)* 3 (2011), 04

[34] Kelly, Christopher ; Pitropakis, Nikolaos ; McKeown, Sean ; Lambrinoudakis, Costas: Testing And Hardening IoT Devices Against the Mirai Botnet. In: *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2020, S. 1–8

[35] Khan, Naqash A. ; Awang, Azlan ; Karim, Samsul Ariffin A.: Security in Internet of Things: A Review. In: *IEEE Access* 10 (2022), S. 104649–104670

[36] Kitchenham, Barbara ; Charters, Stuart: Guidelines for performing Systematic Literature Reviews in Software Engineering. 2 (2007), 01

[37] Koroniotis, Nickolaos ; Moustafa, Nour ; Turnbull, Benjamin ; Schiliro, Francesco ; Gauravaram, Praveen ; Janicke, Helge: A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments. In: *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021, S. 887–894

[38] Kuri, Sajib K. ; Islam, Tarim ; Jaskolka, Jason ; Ibnkahla, Mohamed: A Threat Model and Security Recommendations for IoT Sensors in Connected Vehicle Networks. In: *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, S. 1–5

[39] Liao, Bin ; Ali, Yasir ; Nazir, Shah ; He, Long ; Khan, Habib U.: Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. In: *IEEE Access* 8 (2020), S. 120331–120350

[40] Ling, Zhen ; Luo, Junzhou ; Xu, Yiling ; Gao, Chao ; Wu, Kui ; Fu, Xinwen: Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. In: *IEEE Internet of Things Journal* 4 (2017), Nr. 6, S. 1899–1909

[41] Mahmoodi, Yasamin ; Reiter, Sebastian ; Viehl, Alexander ; Bringmann, Oliver ; Rosenstiel, Wolfgang: Attack Surface Modeling and Assessment for Penetration Testing of IoT System Designs. In: *2018 21st Euromicro Conference on Digital System Design (DSD)*, 2018, S. 177–181

[42] Marksteiner, Stefan ; Exposito Jimenez, Víctor J. ; Valiant, Heribert ; Zeiner, Herwig: An overview of wireless IoT protocol security in the smart home domain. In: *2017 Internet of Things Business Models, Users, and Networks*, 2017, S. 1–8

[43] Nadir, Ibrahim ; Ahmad, Zafeer ; Mahmood, Haroon ; Asadullah Shah, Ghalib ; Shahzad, Farrukh ; Umair, Muhammad ; Khan, Hassam ; Gulzar, Usman: An Auditing Framework for Vulnerability Analysis of IoT System. In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, 2019, S. 39–47

[44] Omotosho, Adebayo ; Haruna, Benjamin ; Olaniyi, Olayemi: Threat Modeling of Internet of Things Health Devices. In: *Journal of Applied Security Research* 14 (2019), 04, S. 1–16

[45] Oser, Pascal ; Heijden, Rens W. van der ; Lüders, Stefan ; Kargl, Frank: Risk Prediction of IoT Devices Based on Vulnerability Analysis. In: *ACM Trans. Priv. Secur.* 25 (2022), may, Nr. 2. – URL https://doi.org/10.1145/3510360. – ISSN 2471-2566

[46] Padmavathi, Dr. G. ; Shanmugapriya, Mrs. D.: *A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks*. 2009

[47] Rahman, Mahmudur ; Carbunar, Bogdan ; Banik, Madhusudan: Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device. In: *CoRR* abs/1304.5672 (2013). – URL http://arxiv.org/abs/1304.5672

[48] Rahman, Reem A. ; Shah, Babar: Security analysis of IoT protocols: A focus in CoAP. In: *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, 2016, S. 1–7

[49] Raikar, Meenaxi M. ; S M, Meena: Vulnerability assessment of MQTT protocol in Internet of Things (IoT). In: *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, 2021, S. 535–540

[50] Rak, Massimiliano ; Salzillo, Giovanni ; Romeo, Claudia: Systematic IoT Penetration Testing: Alexa Case Study. In: *Italian Conference on Cybersecurity*, 2020

[51] Rizvi, Syed ; Pipetti, Ryan ; McIntyre, Nicholas ; Todd, Jonathan ; Williams, Iyonna: Threat model for securing internet of things (IoT) network at device-level. In: *Internet of Things* 11 (2020), S. 100240. – URL https://www.sciencedirect.com/science/article/pii/S2542660520300731. – ISSN 2542-6605

[52] Sahay, Rashmi ; Geethakumari, G. ; Modugu, Koushik: Attack graph — Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT. In: *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 2018, S. 308–313

[53] Salzillo, Giovanni ; Rak, Massimiliano ; Moretta, Felice: Threat Modeling Based Penetration Testing: The Open Energy Monitor Case Study. In: *13th International Conference on Security of Information and Networks*. New York, NY, USA : Association for Computing Machinery, 2021 (SIN 2020). – URL https://doi.org/10.1145/3433174.3433181. – ISBN 9781450387514

[54] Samtani, Sagar ; Yu, Shuo ; Zhu, Hongyi ; Patton, Mark ; Chen, Hsinchun: Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. In: *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, S. 25–30

[55] Seeam, Amar ; Ogbeh, Ochanya S. ; Guness, Shivanand ; Bellekens, Xavier: Threat Modeling and Security Issues for the Internet of Things. In: *2019 Conference on Next Generation Computing Applications (NextComp)*, 2019, S. 1–8

[56] Semedo, Felisberto ; Moradpoor, Naghmeh ; Rafiq, Majid: Vulnerability Assessment of Objective Function of RPL Protocol for Internet of Things. In: *Proceedings of the 11th International Conference on Security of Information and Networks*. New York, NY, USA : Association for Computing Machinery, 2018 (SIN '18). – URL https://doi.org/10.1145/3264437.3264438. – ISBN 9781450366083

[57] Seralathan, Yogeesh ; Oh, Tae T. ; Jadhav, Suyash ; Myers, Jonathan ; Jeong, Jaehoon P. ; Kim, Young H. ; Kim, Jeong N.: IoT security vulnerability: A case study of a Web camera. In: *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 2018, S. 172–177

[58] Sha, Kewei ; Alatrash, Naif ; Wang, Zhiwei: A Secure and Efficient Framework to Read Isolated Smart Grid Devices. In: *IEEE Transactions on Smart Grid* 8 (2017), Nr. 6, S. 2519–2531

[59] Srikumar, Kamakshi ; Kashish, Komal ; Eggers, Kolja ; Díaz Ferreyra, Nicolás E. ; Koch, Julian ; Schüppstuhl, Thorsten ; Scandariato, Riccardo: STRIPED: A Threat Analysis Method for IoT Systems. In: *Proceedings of the 17th International Conference on Availability, Reliability and Security*. New York, NY, USA : Association for Computing Machinery, 2022 (ARES '22). – URL https://doi.org/10.1145/3538969.3538970. – ISBN 9781450396707

[60] Vasilomanolakis, Emmanouil ; Daubert, Jörg ; Luthra, Manisha ; Gazis, Vangelis ; Wiesmaier, Alex ; Kikiras, Panayotis: On the Security and Privacy of Internet of Things Architectures and Systems. In: *2015 International Workshop on Secure Internet of Things (SIoT)*, 2015, S. 49–57

[61] Wang, Huan ; Chen, Zhanfang ; Zhao, Jianping ; Di, Xiaoqiang ; Liu, Dan: A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow. In: *IEEE Access* 6 (2018), S. 8599–8609

[62] Wolf, Andreas ; Simopoulos, Dimitrios ; D'Avino, Luca ; Schwaiger, Patrick: *The PASTA threat model implementation in the IoT development life cycle*. 2021

[63] Xie, Wei ; Jiang, Yikun ; Tang, Yong ; Ding, Ning ; Gao, Yuanming: Vulnerability Detection in IoT Firmware: A Survey. In: *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, 2017, S. 769–772

[64] Yadav, Geeta ; Allakany, Alaa ; Kumar, Vijay ; Paul, Kolin ; Okamura, Koji: Penetration Testing Framework for IoT. In: *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 2019, S. 477–482

[65] Yadav, Geeta ; Paul, Kolin ; Allakany, Alaa ; Okamura, Koji: IoT-PEN: A Penetration Testing Framework for IoT. In: *2020 International Conference on Information Networking (ICOIN)*, 2020, S. 196–201

[66] Yaqub, Muhammad S. ; Mahmood, Haroon ; Nadir, Ibrahim ; Shah, Ghalib A.: An Ensemble Approach for IoT Firmware Strength Analysis using STRIDE Threat Modeling and Reverse Engineering. In: *2022 24th International Multitopic Conference (INMIC)*, 2022, S. 1–6

[67] Ye, Mengmei ; Jiang, Nan ; Yang, Hao ; Yan, Qiben: Security analysis of Internet-of-Things: A case study of august smart lock. In: *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017, S. 499–504

[68] Ye, Mengmei ; Jiang, Nan ; Yang, Hao ; Yan, Qiben: Security analysis of Internet-of-Things: A case study of august smart lock. In: *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017, S. 499–504

[69] Yu, Miao ; Zhuge, Jianwei ; Cao, Ming ; Shi, Zhi jun ; Jiang, Lin: A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. In: *Future Internet* 12 (2020), S. 27

[70] Zamfir, S. ; Balan, T. ; Iliescu, I. ; Sandu, F.: A security analysis on standard IoT protocols. In: *2016 International Conference on Applied and Theoretical Electricity (ICATE)*, 2016, S. 1–6

Erklärung zur selbstständigen Bearbeitung

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Ort	Datum	Unterschrift im Original