HOCHSCHULE DER MEDIEN

Herausgeber Prof. Dr. Barbara Dörsam

Schriftreihe Bachelor-Resümee

Forschungsbereich **IoT-Entwicklung**

Entwicklung eines Sicherheitsleitfadens für IoT-Entwickler

Erstellung und Ausarbeitung eines Sicherheitsleitfadens für Entwickler zur Erhöhung der Sicherheit von IoT-Anwendungen

Mike Buchhammer

Impressum

Hochschule der Medien

Nobelstrasse 10

70569 Stuttgart

www.hdm-stuttgart.de

0711 8923-0

Autor

Mike Buchhammer

Betreuer

Prof. Dr. Barbara Dörsam

Datum

August 2022

Wirtschaftsingenieurwesen Medien

www.hdm-stuttgart.de/wing

hitzges@hdm-stuttgart.de

0711/8923-2634

Layout

Jochen Riegg

Fotos und Illustrationen

Innenteil: Mike Buchhammer

Bachelor-Resümee

Entwicklung eines Sicherheitsleitfadens für IoT-Entwickler

Erstellung und Ausarbeitung eines Sicherheitsleitfadens für Entwickler zur Erhöhung der Sicherheit von IoT-Anwendungen

Mike Buchhammer

August 2022

Der Autor

Mike Buchhammer studierte an der Hochschule der Medien Wirtschaftsingenieurwesen Medien mit dem Schwerpunkt Digital Publishing Technologies. Im Rahmen seiner Arbeit wurde ein Sicherheitsleitfaden für IoT-Entwickler entwickelt, der die Sicherheit von IoT-Anwendungen erhöhen soll und anhand seiner Anwendung auf das Studentenprojekt Happy Plants evaluiert wurde.

Inhaltsverzeichnis

1. Einführung

In dieser stets expandierenden Welt des Internet of Things (IoT) stellt die Sicherheit einen zentralen Faktor dar, da sich die Angriffsflächen auf umfassende und komplexe Weise vergrößern, wenn Milliarden neuer Geräte miteinander vernetzt werden. Bereits im Jahr 2021 waren über 12 Milliarden IoT-Endgeräte im Einsatz [1]. Das Gefährliche dabei ist jedoch, dass das IoT selbst oftmals nicht sicher ist. So zeigte der IoT Threat Report 2020 von Palo Alto Networks & Unit 42 auf, dass 57% aller IoT-Geräte für mittlere oder schwere Angriffe anfällig sind [2]. Die Gefahr, die vom IoT ausgeht, sind sich viele Menschen gar nicht bewusst.

Mit dieser Bachelorarbeit wird das Ziel verfolgt, die Sicherheit von IoT-Anwendungen zu erhöhen. Dazu wird auf Basis des 5-Schichten-Modells ein Sicherheitsleitfaden aus Entwicklersicht erstellt, der auf die Sicherheitsrisiken der einzelnen Ebenen eingeht und entsprechende Sicherheitsmaßnahmen dafür bietet.

Diese Publikation erläutert kurz das Vorgehen der zugrunde liegenden Bachelorarbeit und fasst die wichtigsten Ergebnisse zusammen.

2. Vorgehen

Im Rahmen dieser Bachelorthesis wurden für die Erstellung des Sicherheitsleitfadens verschiedene IoT-Referenzarchitekturen herangezogen und das 5-Schichten-Modell aufgrund seiner Anwendbarkeit auf das Studentenprojekt als IoT-Referenzarchitektur für die Arbeit bzw. den Leitfaden bestimmt. Durch das 5-Schichten-Modell konnten die Risiken der einzelnen Ebenen besser betrachtet, differenziert und analysiert sowie entsprechende Sicherheitsmaßnahmen für diese vorgestellt werden. Diese Sicherheitsmaßnahmen wurden durch Sekundärforschung erarbeitet und bildeten den Sicherheitsleitfaden. Abschließend wurde der Sicherheitsleitfaden auf das Studentenprojekt Happy Plants angewendet und anhand dieser Anwendung evaluiert.

5-Schichten-Modell

Wu et al. entwickelten das 5-Schichten-Modell, indem sie die technologische Architektur des Internets und die logische Struktur des „Telecommunications Management Network“ mit den spezifischen Merkmalen des IoT kombiniert haben. Dieses besteht aus dem Perception Layer, dem Transport Layer, dem Processing Layer, dem Application Layer und dem Business Layer [3].

1. **Perception Layer**

   Die Hauptfunktion des Perception Layers ist die Erfassung der physikalischen Eigenschaften, wie z.B. Temperatur oder Standort von Objekten durch Sensoren, die Umwandlung dieser Daten in digitale Signale und die Ausführung der Befehle des Processing Layers [4, p. 15]. Zu den Schlüsseltechniken dieser Ebene gehören die Sensortechnik, RFID-Technologie, 2D-Barcode, etc.

2. **Transport Layer**

   Der Transport Layer überträgt die empfangenen Daten des Perception Layers über verschiedene Netzwerke, wie z. B. drahtlose oder kabelgebundene Netzwerke, an das Verarbeitungszentrum.

Die wichtigsten Techniken der Ebene sind FTTx, 3G, Wifi, Bluetooth, Infrarot-Technologie, etc. Außerdem werden Protokolle, wie IPv6 (Internet Protocol Version 6), für die Adressierung von Daten verwendet.

3. Processing Layer

Der Processing Layer ist für die Speicherung, Analyse und Verarbeitung der Informationen des Transport Layers zuständig. Die Haupttechniken der Schicht stellen Datenbanken, intelligente Verarbeitung, Cloud Computing, Ubiquitous computing, etc. dar, wobei Cloud Computing und Ubiquitous computing zu den primären Technologien gehören. Während Cloud Computing die Nutzung von IT-Ressourcen über das Internet beschreibt [5], handelt es sich beim Ubiquitous computing um die Allgegenwärtigkeit von kleinsten, miteinander drahtlos vernetzten Computern, die in Alltagsgegenstände eingebaut werden können [6].

4. Application Layer

Der Application Layer baut auf den verarbeiteten Daten des Processing Layers auf und entwickelt verschiedene Anwendungen für das IoT, wie beispielsweise intelligente Transporte, Logistikmanagement, Identitätsauthentifizierung, standortbezogene Dienste (LBS), etc. Dabei wird das Ziel verfolgt, eine Vielzahl von Anwendungen für jede Branche bereitzustellen.

5. Business Layer

Der Business Layer agiert als Manager des gesamten Systems. Das bedeutet, dass die Schicht für die Verwaltung und Kontrolle der Anwendungen, Geschäfts- und Gewinnmodelle des IoT zuständig ist. Die Ebene legt fest, wie Informationen erstellt, gespeichert und geändert werden können [7]. Außerdem ist diese Schicht für den Schutz der Privatsphäre des Nutzers zuständig.

Studentenprojekt Happy Plants

Bei Happy Plants handelt es sich um ein Studentenprojekt aus der Vorlesung TP Softwareentwicklung im Studiengang Wirtschaftsingenieurwesen Medien an der Hochschule der Medien. Hierfür hatte eine Gruppe von Studenten eine Botanik-Webapp zum Management der eigenen Pflanzen entwickelt. In dieser App können die Pflanzen registriert und eine ToDo-Liste für den Verbraucher erstellt werden. Diese ToDo-Liste beinhaltet Aufgaben, wie beispielsweise „Pflanze gießen“, „Pflanze umtopfen“, etc. Für die Beschaffung dieser Daten sind drei Sensoren zuständig. Dabei handelt es sich jeweils um einen Temperatur-, Bodenfeuchtigkeits- und Lichtverhältnis-Sensor, die über Kabel an einem Raspberry Pi angeschlossen sind. Der Raspberry Pi schickt die gesammelten Daten als JSON per HTTPS POST über eine feste IP-Adresse an den Webserver, der mit Node.js betrieben wird. Danach speichert der Webserver die Daten in eine MongoDB Datenbank. Die Anwendung definiert Algorithmen, die anhand der gespeicherten Daten eine ToDo-Liste erstellen. Außerdem stellt die Anwendung die Sensordaten in Echtzeitdiagrammen dar. Die ToDo-Liste und die Diagramme werden anschließend auf Abruf von dem Webserver zu einem Browser oder zu einer App geschickt. Der Aufbau des Projekts sowie die Anwendung des 5-Schichten-Modells auf dieses wird in Abbildung 1 dargestellt.

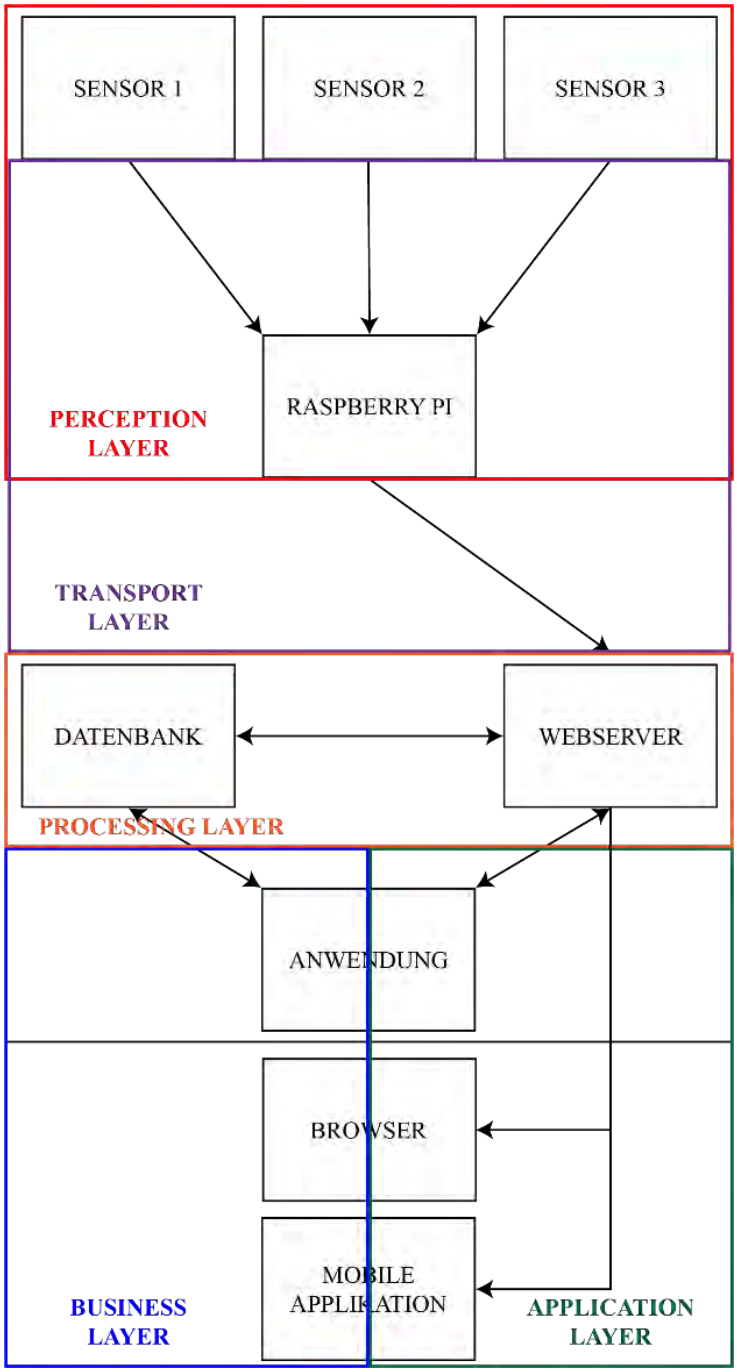

Abbildung 1 Anwendung des 5-Schichten-Modells auf den Aufbau des Studentenprojekts

Der Perception Layer beinhaltet die Sensoren und den Raspberry Pi. Im Transport Layer werden die Signale der Sensoren an den Raspberry Pi übertragen. Der Raspberry Pi wiederum übersetzt diese Signale in digitale Werte und leitet diese an den Webserver weiter. Im Processing Layer werden die Daten vom Webserver entgegengenommen und in die Datenbank gespeichert. Während die meisten Komponenten des Projekts einer festen Ebene zugewiesen werden kann, ist dies bei der Anwendung sowie dem Browser und der mobilen Applikation nicht der Fall. Diese können aufgrund ihrer unterschiedlichen Aufgaben gleichzeitig dem Application Layer und dem Business Layer zugeordnet werden. So ist der Application Layer für die Erstellung der ToDo-Liste und die Darstellung der Echtzeitdaten der Anwendung sowie die Umsetzung der GUI bei Browser und mobiler Applikation zuständig. Während der Business Layer hingegen für die Benutzer- und Pflanzenverwaltung der Anwendung und die Festlegung einer GUI für Browser und mobile Applikation verantwortlich ist.

3. Ergebnisse

Sicherheitsleitfaden

Der Sicherheitsleitfaden wird in Form einer Checkliste dargestellt, die die jeweiligen Sicherheitsmaßnahmen der fünf Ebenen, für die Entwicklung einer sichereren IoT-Anwendung, beinhaltet und nach ihrer Wichtigkeit, für die Sicherheit der Ebene, von oben nach unten priorisiert.

1. **Perception Layer**
   - 1.1. Implementierung eines Ruhezustand-Mechanismus als Maßnahme gegen Angriffe zur Energieerschöpfung
   - 1.2. Kennzeichnung der Aktualität der Nachrichten als Maßnahme gegen Replay-Attacken
   - 1.3. Verwendung eines Authentifizierungsprotokoll als Maßnahme gegen das Klonen von IoT-Geräten
   - 1.4. Verwendung eines Verschlüsselungsalgorithmus als Maßnahme gegen Abhören
   - 1.5. Einschränkung der ein- und ausgehenden Verbindungen als Maßnahme gegen die Bildung von Botnetzen
2. **Transport Layer**
   - 2.1. Verwendung eines Sicherheitsprotokolls
   - 2.2. Implementierung eines passenden und sicheren IoT-Netzes
   - 2.3. Veränderung der Größe des Datenverkehrs als Maßnahme gegen Traffic Analysis
   - 2.4. Identitätsauthentifizierung als Maßnahme gegen Sybil-Angriffe
3. **Processing Layer**
   - 3.1. Gewährleistung eines sicheren Systems
   - 3.2. Gewährleistung eines sicheren Netzzugangs
   - 3.3. Implementierung einer sicheren Datenspeicherung
4. **Application Layer**
   - 4.1. Validierung der Benutzereingaben als Maßnahme gegen Cross-Site-Scripting
   - 4.2. Filtern der Benutzereingaben und parametrisierte Abfragen als Maßnahmen gegen SQL-Injection
   - 4.3. Verwendung eines sicheren Kommunikationsprotokoll
   - 4.4. Verwendung einer Autorisierungsinfrastruktur als Maßnahme gegen DoS-Angriffe
   - 4.5. Maßnahmen gegen Phishing-Angriffe
5. **Business Layer**
   - 5.1. Einführung von regelmäßigen Softwareupdates
   - 5.2. Durchführung von Sicherheitstests
   - 5.3. Maßnahmen gegen Brute-Force- und Wörterbuchangriffe

Sollten nicht alle Sicherheitsmaßnahmen aufgrund von personellen oder zeitlichen Gründen umsetzbar sein, dann sind diese fünf Maßnahmen zu priorisieren, da sie zumindest ein gutes Schutzniveau bieten:

5.1. Einführung von regelmäßigen Softwareupdates
2.1. Verwendung eines Sicherheitsprotokolls
2.2. Implementierung eines passendes und sicheren IoT-Netzes:
4.1. Validierung der Benutzereingaben als Maßnahme gegen Cross-Site-Scripting
4.2. Filtern der Benutzereingaben und parametrisierte Abfragen als Maßnahmen gegen SQL-Injection

Evaluierung des Sicherheitsleitfaden anhand der Anwendung auf das Studentenprojekt Happy Plants

In erster Linie ist festzuhalten, dass dieser Sicherheitsleitfaden keinen Anspruch auf Vollständigkeit erhebt. Jedoch kann von einem sichereren IoT-System gesprochen werden, sobald die Maßnahmen des Sicherheitsleitfaden auf das System angewendet wurden. Hierbei sollte allerdings bedacht werden, dass es sich bei dieser Sicherheit nur um eine Momentaufnahme handelt. Sicherheitsmaßnahmen, die heute noch Schutz bieten, können in ein paar Jahren schon komplett nutzlos sein, sobald neue Sicherheitsgefahren auf den Markt kommen. Aus diesem Grund kann dieser Sicherheitsleitfaden in Zukunft nicht blind übernommen werden. Stattdessen muss von der Entwicklerseite geprüft werden, ob diese Maßnahmen auch noch den nötigen Schutz bieten.

Nichtsdestotrotz bietet der Sicherheitsleitfaden viele Möglichkeiten zur Abwehr gegen IoT-Sicherheitsgefahren, die nicht nur Tools, wie AES, TLS, etc., sondern auch Softwareimplementierungen bzw. Funktionen beinhalten. Für die Implementierung der Funktionen benötigt der Entwickler großes Verständnis, nicht nur für die Architektur des IoT-Systems, sondern auch für die Funktionen selbst. Neben dem Verständnis muss der Entwickler ebenso in der Lage sein, die Funktion in der Programmiersprache der Anwendung implementieren zu können. Dadurch, dass einige Sicherheitsmaßnahmen selbst entwickelt werden und ein Teil der Tools, wie z.B. AES, 6LoWPAN nicht kostenpflichtig ist, stellen die Kosten der Sicherheitsmaßnahmen des Leitfadens selbst keine große Hürde für die Sicherheit dar. Hier sollte jedoch beachtet werden, dass die Dienstleistung für die Implementierung dieser Gegenmaßnahmen, aufgrund der benötigten Expertise, den Großteil der Kosten ausmachen wird. Die große Anzahl von Sicherheitsmaßnahmen gestaltet die Bewältigung von IoT-Anwendungen gerade für Privat- oder Einzelpersonen als sehr schwierig, weshalb für die Umsetzung aller Sicherheitsmaßnahmen des Leitfadens Entwicklerteams benötigt werden. Diese implementieren zu Beginn die Sicherheitsmaßnahmen, reevaluieren danach stets die Sicherheit der Anwendung und versorgen diese mit Sicherheitsupdates. Die Größe dieser Entwicklerteams sollte anhand des Umfangs und der Komplexität der IoT-Anwendung festgemacht werden.

4. Fazit

Der Leitfaden selbst trägt nur einen kleinen Teil zur Sicherheit vom IoT bei. Um die Sicherheit weiter zu erhöhen, müssen zusätzliche Maßnahmen getroffen werden. Daher wäre die Einführung und Durchsetzung eines internationalen Standards für IoT-Systeme von großer Bedeutung. Dieser könnte Maßnahmen, wie beispielsweise regelmäßige und verifizierte Softwareupdates, Sicherheitstest vor der Markteinführung, eine anerkannte Architektur sowie sichere und einheitliche Software und Protokolle beinhalten [8]. Alternativ kann der Vorschlag von Arne Schönbohm, dem Chef des Bundesamts für Sicherheit in der Informationstechnik, für die Einführung eines Mindesthaltbarkeitsdatums in Betracht gezogen werden. Hierdurch sind die Hersteller für die Sicherheit ihrer Produkte verantwortlich und würden dementsprechend nicht mehr so leichtsinnig damit umgehen. Außerdem würden sich dadurch mehr Endnutzer über die möglichen Gefahren informieren, sowie ein breiteres Verständnis für die Thematik entwickeln, wodurch weniger anfällige IoT-Systeme im Umlauf wären [9].

Auf welche Weise die Sicherheit von IoT erhöht wird, spielt keine Rolle, stattdessen ist es viel wichtiger, dass Maßnahmen getroffen werden, damit das IoT in Zukunft als sicher gelten kann. Gerade die Gefahren von IoT werden sich in den nächsten Jahren nur noch vergrößern, sobald nochmals komplexere IoT-Systeme, wie Smart Cities oder selbstfahrende Autos auf den Markt kommen. Sollten diese IoT-Geräte oder IoT-Systeme nicht angemessen gesichert werden, können dadurch Menschen in Lebensgefahr gebracht werden [10].

5. Referenzen

[1] M. Hasan, „State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally," IoT Analytics GmbH, 18 Mai 2022. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/. [Zugriff am 1 Juli 2022].

[2] Unit 42, „2020 Unit 42 IoT Threat Report," Palo Alto Networks, 10 Mai 2020. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/. [Zugriff am 1 Juli 2022].

[3] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun und H.-Y. Du, „Research on the architecture of Internet of Things," *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE),* Bd. 5, pp. 484-487, 2010.

[4] C.-K. Wu, Internet of Things Security: Architectures and Security Measures, Singapur: Springer Singapore, 2021.

[5] Bundesministerium für Wirtschaft und Klimaschutz, „Cloud Computing," 2022. [Online]. Available: https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Themen/Cloud-Computing/cloud-computing. [Zugriff am 30 Juli 2022].

[6] R. Lackes und M. Siepermann, „Ubiquitous Computing," Springer Gabler | Springer Fachmedien Wiesbaden GmbH, [Online]. Available: https://wirtschaftslexikon.gabler.de/definition/ubiquitous-computing-48216. [Zugriff am 30 Juli 2022].

[7] M. Burhan, R. Rehman, B. Khan und B.-S. Kim, „IoT Elements, Layered Architectures and Security," *Sensors,* Bd. 18, Nr. 9, p. 2796, 2018.

[8] R. Mahmoud, T. Yousuf, F. Aloul und I. Zualkernan, „Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST),* 2015.

[9] A. Straßheim und S. Schreiber, „IoT-Penetrationstest," *Datenschutz und Datensicherheit - DuD,* Bd. 41, Nr. 10, pp. 623-627, 2017.

[10] M. Salat, „The dark side of IoT devices," Avast PLC, 16 Oktober 2017. [Online]. Available: https://blog.avast.com/the-dark-side-of-iot-devices. [Zugriff am 2 Juli 2022].

[11] R. Singh, „What is NoSQL Injection Attack and How to Prevent It?," Indusface, 9 März 2021. [Online]. Available: https://www.indusface.com/blog/what-is-nosql-injection-attack-and-how-to-prevent-it/. [Zugriff am 9 August 2022].