Hochschule Rhein-Waal
Fakultät: Kommunikation und Umwelt
Studiengang: Verwaltungsinformatik
Modul: Workshop 2: Wissenschaftliches Schreiben

Aufgabe 3

-

Exposé

zur Abschlussarbeit mit dem Thema:
Gefahren durch das Internet der Dinge

Linus Wolf - 28611

7. Mai 2025

1 Einleitung

Das Internet der Dinge (Internet of Things - IoT) beschreibt die zunehmende Vernetzung von Alltagsgegenständen, Geräten und Maschinen über das Internet oder in separaten lokalen Netzwerken. Während diese Entwicklung auch Vorteile mit sich bringt, wie z. B. Automatisierung, Effizienzsteigerung und neue Geschäftsmodelle, entstehen gleichzeitig ernstzunehmende Risiken. In dieser Arbeit soll sich mit genau diesen Schattenseiten und auch den sicherheitskritischen und datenschutzrelevanten Aspekte beschäftigt werden.

2 Forschungsfrage und Zielsetzung

Als Forschungsfrage wurde so formuliert: „Gibt es in den Liegenschaften des Rechenzentrum der Finanzverwaltung des Landes NRW (RZF NRW) IoT-Signale und wie soll zukünftig auf Gefahren im Zusammenhang mit dem IoT hingewiesen werden?"

Die Zielsetzung dabei ist die Untersuchung der Liegenschaften auf aktive IoT-Signale und Auswertung der Daten. Zudem sollen Handlungshinweise für die Hausleitung erstellt werden, sowie Informationsmaterialien für die Belegschaft.

3 Stand der Forschung

Statista nennt 18,87 Milliarden IoT-Verbindungen für das Jahr mit steigender Tendenz, wie in Abbildung 1 zu sehen ist. Jede Verbindung ist ein potentieller Zugang zu einem Netzwerk. Die Absicherung dieser Verbindungen wird hauptsächlich den Herstellern überlassen, die für die richtige Implementierung von Sicherheitsfeatures verantwortlich sind.

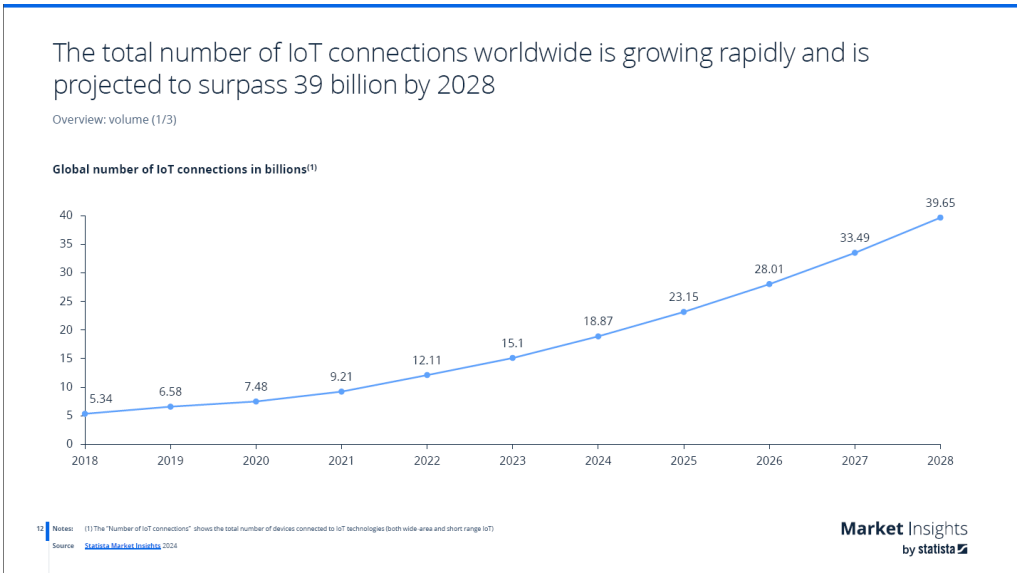

Abbildung 1: IoT-Verbindungen weltweit

Das BSI schreibt in seinem Bericht zur Lage der Internetsicherheit in Deutschland aus dem Jahr 2024: „Neben klassischen Bürocomputersystemen können Angreifer auch alle anderen internetfähigen Geräte mit einem Schadprogramm infizieren und in ein Botnetz integrieren. Das betrifft zum Beispiel Geräte wie Smartphones, Tablets, Router oder auch IoT-Geräte wie zum Beispiel Fernseher, Set-Top- Boxen, Webcams etc."[Bundesamt für Sicherheit in der Informationstechnik 2024, S. 15]

4 Methodik

Für die zwei Bereiche der Forschungsfrage werden verschiedene Methodiken angewendet.

Bei der Untersuchung der Liegenschaften wird ein physisches Experiment durchgeführt und anschließend die Daten aus diesem Experiment ausgewertet.

Für die Handlungsempfehlungen und Information findet eine Literaturrecherche statt und falls sich geeignete Interviewpartner finden auch Einzelinterviews.

5 Gliederung

Neben den üblichen Bestandteilen einer Abschlussarbeit sind die folgenden Kapitel vorgesehen

Grundlagen Die theoretischen Grundlagen werden erarbeitet und technische Prinzipien erklärt

Aufbau des Experiments Vorstellung des technischen Equipments

Durchführung des Experiments Beschreibung der eigentlichen Durchführung des Experiments

Datenauswertung Auswertung der Daten und Rückschlüsse aus dem Experiment

Experteninterview Beschreibung und Auswertung der Kernaussagen aus dem oder den Interviews

Handlungsempfehlung für die Hausleitung Darstellung des Experiments und Handlungsempfehlungen

Handreichung für Mitarbeiter Ausarbeitung über den Umgang mit IoT-Geräten in der Behörde

6 Zeitplan

12 Wochen vor Abgabe Anmeldung der Arbeit, erste Literaturrecherche, Anfragen an Interviewpartner

11-10 Literaturrecherche, Erarbeitung von Grundlagen und Interviewfragen

9-6 Vorbereitung, Durchführung und Auswertung des Experiments

5 Späteste Durchführung von Interviews

4-3 Auswertung der Interviews, Schreiben von Informationsmaterial und Handlungsempfehlungen

2 Korrekturlesen

1 Puffer

0 Druck und Abgabe

7 Schlussbemerkung

Das Thema Gefahren des Internet of Things hat durch die stark ansteigende Anzahl an Geräten und Verbindungen ein Risiko- und Sicherheitspotential. Das BSI zeigt dies in seinem jährlich erscheinenden Berichten, zuletzt im Jahr 2024. Durch den einfachen Zugang zu solchen Geräten in Form von Küchenutensilien, Leuchtmitteln und anderen Formen können diese ohne böswillige Absicht in die Arbeitsumgebung der Behörde eingebracht werden. In den Netzwerken der Behörde sind auf Grund seiner Operationen zahlreiche Programmierer und Administratoren aktiv. Entsprechend häufig sind Adminaccounts und es besteht die Gefahr, dass die Geräte in ein Netzwerk eingepflegt wurden oder das sie als Einfallstore zu absichtlichen IoT-Netzwerken in der Behörde benutzt werden. Dies soll hier erforscht werden und entsprechende Empfehlungen und Informationen erarbeitet werden.

8 Literatur

2021 5th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS): 16 -18 December 2021 : proceedings-2021 (2021). Piscataway, NJ: IEEE. ISBN: 978-1-6654-0610-9. DOI: 10.1109/CSITSS54238.2021.

Abrishamchi, Mohammad Ali Nassiri et al. (2017). „Side channel attacks on smart home systems: A short overview“. In: *Proceedings IECON 2017 - 43nd Annual Conference of the IEEE Industrial Electronics Society*. Piscataway, NJ: IEEE, S. 8144–8149. ISBN: 978-1-5386-1127-2. DOI: 10.1109/IECON.2017.8217429.

Akhgar, Babak et al. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Rockland, MA: Elsevier Science & Technology Books. ISBN: 9780128008119. URL: https://ebookcentral.proquest.com/lib/hrw/detail.action?docID=1744499.

Bundesamt für Sicherheit in der Informationstechnik (2015). *Die Lage der IT-Sicherheit in Deutschland 2015*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.html (besucht am 18. 04. 2025).

– (2018). *Die Lage der IT-Sicherheit in Deutschland 2018*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.html (besucht am 18. 04. 2025).

Bundesamt für Sicherheit in der Informationstechnik (2021). *Die Lage der IT-Sicherheit in Deutschland 2021*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.html (besucht am 18. 04. 2025).

– (2024). *Die Lage der IT-Sicherheit in Deutschland 2024*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html?nn=129410 (besucht am 18. 04. 2025).

Chantzis, Fotios et al. (2021). *Practical IoT hacking: The definitive guide to attacking the internet of things*. San Francisco: No Starch Press. ISBN: 9781718500907.

Cilfone, Antonio et al. (2019). „Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies“. In: *Future Internet* 11.4. ISSN: 1999-5903. DOI: 10.3390/fi11040099.

Davis, Brittany D. et al. (2020). „Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study“. In: *IEEE Internet of Things Journal* 7.10, S. 10102–10110. DOI: 10.1109/JIOT.2020.2983983.

Gessler, Ralf und Thomas Krause (2015). *Wireless-Netzwerke für den Nahbereich: Eingebettete Funksysteme: Vergleich von standardisierten und proprietären Verfahren*. 2., aktualisierte u. erw. Aufl. 2015. Wiesbaden: Springer Fachmedien Wiesbaden. ISBN: 978-3-8348-2075-4. DOI: 10.1007/978-3-8348-2075-4.

Goodman, Marc (2015). *Future crimes: A journey to the dark side of technology - and how to survive it*. London: Bantam Press. ISBN: 9780593073667.

Hern, Alex (2018-01-28). „Fitness tracking app Strava gives away location of secret US army bases“. In: *The Guardian* 2018. URL: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (besucht am 18. 04. 2025).

Herwig, Oliver (2022). *Home Smart Home: Wie wir wohnen wollen*. Basel: Birkhäuser. ISBN: 9783035624441. URL: https://www.degruyter.com/isbn/9783035624441.

Khan, L. A. et al. (2010). „Speaker recognition from encrypted VoIP communications“. In: *Digital Investigation* 7.1-2, S. 65–73. ISSN: 17422876. DOI: 10.1016/j.diin.2009.10.001.

Ling, Zhen et al. (2017). „Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System“. In: *IEEE Internet of Things Journal* 4.6, S. 1899–1909. DOI: 10.1109/JIOT.2017.2707465.

Mandiberg, Michael (2012). *The Social Media Reader*. 1. Aufl. New York: New York University Press. ISBN: 9780814763025. URL: https://ebookcentral.proquest.com/lib/hrw/detail.action?docID=865738.

Marmura, Stephen M. E. (2018). *QC WikiLeaks Paradigm: Paradoxes and Revelations*. Cham: Springer International Publishing (2018) und Imprint: Palgrave Pivot. ISBN: 978-3-319-97139-1. DOI: 10.1007/978-3-319-97139-1.

Proceedings IECON 2017 - 43nd Annual Conference of the IEEE Industrial Electronics Society: China National Convention Center, Bejing, China, 29 October-01 November, 2017 (2017). Piscataway, NJ: IEEE. ISBN: 978-1-5386-1127-2.

Putman, C.G.J. et al. (2018). *Business Model of a Botnet*. DOI: 10.1109/PDP2018.2018.00077. URL: https://arxiv.org/pdf/1804.10848.

Sinha, Shivanshi und Yojna Arora (2020). „Ethical hacking: The story of a white hat hacker". In: *Int. J. Innov. Res. Comput. Sci. Technol.* 8.3.

Sivapriyan, R. et al. (2021). „Analysis of Security Challenges and Issues in IoT Enabled Smart Homes". In: *2021 5th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*. Piscataway, NJ: IEEE, S. 1–6. ISBN: 978-1-6654-0610-9. DOI: 10.1109/CSITSS54238.2021.9683324.

Statista (2021). *Digital & Trends : Smart Home*.

Veeraraghavan, Prakash et al. (2020). „NAT++: An Efficient Micro-NAT Architecture for Solving IP-Spoofing Attacks in a Corporate Network". In: *Electronics* 9.9, S. 1510. DOI: 10.3390/electronics9091510.

Weidenbach, Peter und Johannes vom Dorp (2020). *Home Router Security Report 2020*. Hrsg. von Frauenhofer FKIE. URL: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf (besucht am 18. 04. 2025).

Yi, Gangman et al., Hrsg. (2014). *Computer science and its applications: Ubiquitous information technologies*. Bd. v.330. Lecture Notes in Electrical Engineering Ser. Heidelberg: Springer. ISBN: 978-3-662-45402-2. URL: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=1968234.

Ziegler, Sébastien (2019). *Internet of Things Security and Data Protection*. Internet of Things Ser. Cham: Springer. ISBN: 9783030049843. URL: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5735503.