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

Aufgabe 2
Exzerpt

Linus Wolf - 28611

20. April 2025

Linus Wolf, Verwaltungsinformatik, 8. Semester
Workshop 2: Wissenschaftliches Schreiben
ZIEGLER, SÉBASTIEN (Hrsg.) 2019: „INTERNET OF THINGS SECURITY AND DATA PROTECTION", CHAM(CH): SPRINGER, S. 1-7

Hauptthese: In den zukünftigen Jahren werden kleine Geräte das Internet of Things massiv wachsen lassen. Jedes Gerät kann damit eine potentielle Schwachstelle darstellen und entweder als Einfallstor oder als Ziel für einen Angriff gelten. Gleichzeitig werden sich die Angriffsvektoren verschieben und es sind entsprechend Maßnahmen zu ergreifen.

Internet of Things Cybersecurity Paradigm Shift, Threat Matrix and Practical Taxonomy [1-7]

[1-3]

Netzwerke lassen sich grob in 4 Bereiche einteilen. PAN (Personal Area Network), LAN (Local), WAN (Wide) und Cloud Bereiche. [Einzelne Definitionen lassen sich hier später entnehmen]; [Abbildung auf S. 2]

„By identifying and specifying the source of each category of attack and its ultimate target, we can differentiate several profiles and patterns." (S. 2)

Das Ziel von Angriffen lässt sich in 4 Kategorien einteilen. Zugriff auf Information (A - Access), Vorübergehende Beeinträchtigung (B - Bother), Code, Daten oder Informationen ändern (C - Change), Ziel zerstören (D - Destroy)

[3]

Klassisch lassen sich Angriffs- und Zielvektoren in eine Matrix anordnen. [Abbildung auf S.4][Klassische Angriffsvektoren von L, C oder W auf L oder C]

[3-5]

„With an expected 50 billion plus connected devices, Internet of Things deployments will be massive. It will substantially extend the surface of risk and increase the likelihood that a hacker will find a weak point." (S. 3)

„Internet of Things devices are often constrained devices. The prime concern [...] is energy-saving [...]. This leads to simplified code [...]. Such constraints directly impact the security [...]." (S.3) [Sinngemäß gekürzt]

IoT-Geräte werden auch in öffentlich zugänglichen Bereichen eingesetzt, dies erlaubt physischen Zugriff darauf. Bsp: Sicherheitskamera, Leuchtmittel.

IoT-Geräte nutzen eine Vielzahl von Protokollen zur Kommunikation.

„Cognitive bias: There is also a misperception and underestimation of the risks related to Internet of Things deployments. Internet of Things devices are too often perceived as simple and dumb and not containing strategic information. It is a serious misinterpretation if you consider that Internet of Things devices are connected to the network of the company and constitute new access points that are often physically accessible to outsiders with a lower level of security in terms of authentication and encryption." (S. 5)

[5-6]

Beschreibung von möglichen Angriffsszenarien und Angriffsvektoren. [Auffallend dabei sind Direktangriffe von W oder C auf P unter Umgehung des LAN und die direkte Attacke innerhalb eines IoT-Netzwerks]

[6-7]

Neue Sicherheitsmatrix mit deutlicher Hervorhebung von IoT-Attacken aus und in den Bereich P. [Abbildung S. 7]