SafeWise
18.06.2022

Modul 3: OT-Security

IoT

Der Begriff IoT (Abkürzung für „Internet Of Things“, zu Deutsch: „Internet der Dinge) beschreibt die Vernetzung von Alltagsgegenständen über das Internet, um so einen Datenaustausch zu ermöglichen.[1] „Dinge“ können in diesem Falle viele Arten von Geräten sein: Vom Smartphone bis zur komplexen Industriemaschine.[2]

Bestes Beispiel für dieses Konzept ist das sogenannte „Smart-Home“: Hier kommunizieren einzelne Geräte über das Internet, um Dinge im Haus zu steuern. Beispielsweiße meldet so der Wechselrichter einer Solaranlage an ein zentrales Steuersystem, dass nun überdurchschnittlich viel Strom produziert wird, welches dann die Steckdose aktiviert, an welcher die Waschmaschine angeschlossen ist.[3]

Bei großen Industrieanlagen werden durch die Vernetzung eine effektivere Fehlerfindung und Behebung, sowie eine sicherere Qualitätskontrolle möglich.[4]

Selbstverständlich wirft eine Welt, in der alle Geräte über ein Netzwerk verbunden sind, einige Sicherheitsfragen auf. Hier ist vor allem der Datenschutz zu beachten: Smart-Home-Geräte wie Alexa oder der Amazon-Dot, welche auf Spracherkennung basieren, stehen schon länger im Verdacht, durchgehend ihre Umgebung akustisch aufzuzeichnen. Es sind auch Rückrufaktionen von Teddybären bekannt, da diese die Stimmen der Kinder aufzeichneten und an den Hersteller sendeten.[5] Wissenschaftler haben bereits einige Sicherheitslücken im Smart-Home-System des großen Herstellers Samsung aufgedeckt.[6]

Aber auch Hacker-Attacken werden durch die Vernetzung bedrohlicher. So können zum Beispiel Einbrecher smarte Türen und Fenster nutzen, um sich ganz entspannt per Computer Zutritt zu Gebäuden zu verschaffen. Im industriellen Bereich können ganze Anlagen durch das Einspielen von Maleware lahmgelegt werden.

Schützen kann man sich vor diesen Gefahren vor allem durch separate Netzwerke für die jeweiligen Geräte. In machen Anwendungsbereichen (wie zum Beispiel der Industrie) sollte man sich gut überlegen, ob überhaupt ein Zugriff auf das Internet für die Geräte nötig ist, oder ob ein lokales Netzwerk für die Kommunikation untereinander nicht ausreichend ist.

1 https://www.youtube.com/watch?v=yLZbzbO_7yQ

2 https://www.oracle.com/de/internet-of-things/what-is-iot/

3 https://www.sma.de/fileadmin/content/global/Solutions/Documents/Smart_Home/SMART_HOME-KDE132641W.p

4 https://www.oracle.com/de/a/ocom/docs/applications/scm/iot-case-study-titan-international.pdf

5 https://www.avast.com/de-de/c-iot-security-risks

6 https://www.businessinsider.com/samsung-smartthings-platform-iot-security-issues-internet-of-things-2016-5

Hacker

Nach Wau Holland ist ein Hacker jemand der „[…] versucht einen Weg zu finden, wie man mit einer Kaffeemaschine einen Toast zubereiten kann“. [1] Diese Darstellung mag einem beim ersten Lesen zwar überspitzt und nicht besonders hilfreich vorkommen, sie beschreibt aber anschaulich das, was die Gruppe der Hacker ausmacht: Die Suche nach Antworten und der Drang, Zugang zu Wissen zu erhalten, der ihnen sonst verwehrt wird. Dabei nutzen sie die Schwachstellen der digitalen Welt und bewegen sich nicht selten in rechtlichen Grauzonen[2].

Eine weit verbreitete Einteilung der Hacker ist die in White- und Grey- und Black- Hats. Diese basiert in erster Linie auf der Gesetzmäßigkeit Ihres Verhaltens. Während die „White-Hats“ sich ausschließlich im Rahmen der Gesetze bewegen, in dem sie zum Beispiel beauftragte Sicherheitstests durchführen, schrecken die „Grey- und Black-Hats“ nicht davor zurück, wissentlich gegen Gesetze zu verstoßen.

Innerhalb und auch außerhalb der Szene hat sich auch der Begriff des „Skriptkiddies“ implementiert. Dieser Bezeichnet einen Hacker, welcher nicht über tieferes Wissen über die Materie verfügt und so mithilfe von vorgefertigten Programmen und Anleitungen Schaden anrichtet.[3]

Seinen Ursprung findet das Hacking bereits in den 20er Jahren im Bereich der Amateur-funker, als diese damit begannen, Telefonnetze zu manipulieren, um beispielsweiße Gratisanrufe zu erhalten. Das Computerbasierte Hacking entwickelt sich dann Ende der 60er Jahre am MIT, als dort die ersten Studenten damit beginnen Veränderungen an Soft- und Hardware vorzunehmen. Ihre Absicht war hier allerdings in erster Linie, diese zu Verbessern. [4]

Juristisch ist dann Hacking in Deutschland im StGB (Strafgesetzbuch) abgedeckt. Es handelt sich hier bei allen Vergehen um Antragsdelikte, dass heißt es muss immer vom geschädigten ein Strafantrag gestellt werden, bevor eine Ermittlung aufgenommen wird.

1 https://ftp.fau.de/cdn.media.ccc.de/contributors/ulm/chaosseminar/200302-hacker/cs-200302-hacker_slides.pdf

2 https://www.spiegel.de/thema/hacker/

3 https://www.heise.de/tp/features/The-Kids-are-out-to-play-3449304.html

4 https://www.morgenpost.de/printarchiv/panorama/article105315120/Geschichte-des-Hackens.html