St. Pölten University of Applied Sciences

/informatik & security

/fh/// st. pölten

Abschlussbericht

Projekt: Evaluierung Smarthome/IoT-Sicherheit

Tobias Dam
Stand: 24. Juni 2021

Inhalt

Seite

1 Beschreibung

Dieser abschließende Bericht stellt die Ergebnisse der beiden Arbeitspakete des gemeinsamen Projektes „Evaluierung Smarthome/IoT-Sicherheit“ der Arbeiterkammer Niederösterreich und der Fachhochschule St. Pölten dar.

2 Arbeitspaket 1

2.1 Kurzbeschreibung

Im Rahmen dieses Arbeitspakets wurden IoT-basierte Geräte in Hinblick auf Sicherheit und Datenschutz untersucht.

2.2 Geräte

Die in der folgenden Tabelle aufgelisteten Geräte wurden gemeinsam von den Projektpartnern ausgewählt und anschließend analysiert.

Planet Buddies Wireless Speaker – Olive the Owl
Tuya Wi-Fi Smart Device – Siren Alarm 3 in 1
Xplora 4 – Smartwatch Blue
LoraTap – Smart Garage Door Opener
Smart Valve controller
Intelligent lock cylinder
Kamtron Wireless IP Camera
Playbrush Smart Sonic
Amazon Echo Dot 3 Generation
Mi Smart Band 5
Oral-B Smart 5 5000N
Active Era Smart Scales

Snaptain S5C 4-Axis Drone
Kyvol Cybovac Robot Vacuum Cleaner E20
Medion Saugroboter mit Lasernavigation – MD 18861
Princess Smart Aerofryer

2.3 Ergebnisse

Es wurde der Netzwerkverkehr der Geräte und der zugehörigen Android Applikationen aufgezeichnet und ausgewertet und nach Möglichkeit wurde die verschlüsselte Kommunikation der Apps mithilfe von TLS Interception überprüft. In einzelnen Fällen wurde die Applikationsdatei selbst geprüft. Einige Verbindungen konnten nicht analysiert werden, da die Daten in einer unbekannten Codierung oder eventuell verschlüsselt übertragen wurden oder die Applikation mit speziellen Maßnahmen geschützt wurde.

Die festgestellten übertragenen personenbezogenen Daten sind in den jeweiligen Datenschutzerklärungen vermerkt. Eine Ausnahme bildet der Medion Saugroboter MD 18861, welcher nicht in der zugehörigen Datenschutzerklärung enthalten ist. Sie enthält jedoch Angaben zu den erfassten Daten eines ähnlichen Modells.

Es konnten keine sicherheitsrelevanten Aktionen der Geräte im Heimnetzwerk festgestellt werden, wie beispielsweise eine Suche nach den vorhandenen Geräten im Heimnetzwerk, Angriffe oder ähnliches. Die smarte Sirene, der Garagenöffner und der Valve Controller des Herstellers Tuya senden Pakete an alle Geräte im Heimnetzwerk aus, erhielten jedoch in unseren Tests keine Antworten. Es wird vermutet, dass diese nach einer zentralen Steuereinheit oder ähnlichem suchen.

Der Planet Buddies Wireless Speaker verfügt über keine Verbindung zum Internet, kann jedoch von jeder Person übernommen werden, sobald dieser die aktuelle Verbindung zu dem Smartphone verliert. In Kombination mit einem vorhandenen Amazon Echo Dot können somit Befehle zur Steuerung verbundener Smarthome-Geräte von Angreifern getätigt werden.

Ein weiteres mögliches Sicherheitsproblem bietet die lose und sehr leicht abnehmbare Abdeckung des Smart Doorlock. Die Abdeckung des Knaufs, welcher an der Außenseite montiert werden muss, ist lediglich mit Magneten befestigt. Unter der Abdeckung befindet sich ein einfach wirkender, mechanischer Schließmechanismus, der mithilfe von Lockpicking Werkzeugen angegriffen werden kann.

Die detaillierte, technische Evaluierung befindet sich in dem separaten Dokument „Geraete_Summary.pdf“.

Weiters wurden Empfehlungen zur Auswahl und zur Verwendung von Smarthome-Geräten erarbeitet und in dem Dokument „Smarthome_Kauf.docx“ bereitgestellt.

3 Arbeitspaket 2

3.1 Kurzbeschreibung

Erstellung eines Smarthome-Honeypots und Analyse der Zugriffe auf diesen.

3.2 Aufbau und Betrieb des Honeypots

Der Honeypot wurde innerhalb der Fachhochschule St.Pölten auf einem Server mit einer separaten externen IPv4 Adresse betrieben. Dafür wurde eine Instanz der quelloffenen Smarthome-Verwaltungslösung Home Assistant mittels Docker betrieben. Der Honeypot war über die freie Domain my-smarthome.tk per HTTPS (Port 443) über eine verschlüsselte Verbindung erreichbar. Zusätzlich wurde der Honeypot mit dem Standardport der Home Assistant Lösung 8123 betrieben und konnte auch direkt über die externe IP-Adresse erreicht werden, um den Anschein zu erwecken, dass die Instanz mit geringem technischem Wissen in Betrieb genommen wurde. Alle Zugriffe und Antworten wurden zur Vereinfachung der Analyse im Standard-Webserver Format und zusätzlich in dem JSON Format aufgezeichnet.

3.3 Ergebnisse

Der Honeypot, wie in Abschnitt 3.2 beschrieben, wurde über den Zeitraum vom 15.03.2021 bis zum 07.06.2021 betrieben und alle Zugriffe dabei aufgezeichnet.

Insgesamt wurden 2415 Anfragen an den Honeypot aufgezeichnet, wobei 2378 Anfragen an die Domain my-smarthome.tk per HTTPS (Port 443) gesandt wurden und 37 Anfragen unverschlüsselt and den Standardport 8123.

Die Zugriffe weisen keine Merkmale auf, welche auf gezielte Angriffe auf Smarthome Lösungen oder automatisiertes Aufspüren solcher hindeuten.

Die überwiegende Anzahl der Zugriffe kam über ein „normales“ Besuchen der Startseite des Honeypots zustande. Ein Bruteforce der Passworteingabe kann ausgeschlossen werden, da lediglich 14 hierfür infrage kommende Anfragen (HTTP POST) aufgezeichnet wurden und diese durch die Webseite selbst ausgelöst wurden.

Die Zugriffe auf Port 443 gingen von 357 und jene auf Port 8123 von 16 unterschiedlichen IP-Adressen aus und die meisten Zugriffe können aufgrund der Zuordnung der IP-Adresse zu einem Land den Vereinigten Staaten von Amerika zugeordnet werden. Abbildung 1 stellt die Verteilung der Zugriffe über unterschiedliche Länder für Port 443 und Port 8123 dar.

31 Zugriffe auf Port 443 und 1 Zugriff auf Port 8123 konnten aufgrund des angegebenen User Agents (Browserkennung) eindeutig als Webcrawler identifiziert werden. 1035 Zugriffe auf Port 443 und 24 Zugriffe auf Port 8123 sind aufgrund des User Agents mithilfe von Programmbibliotheken beziehungsweise Webbrowsern ohne Benutzeroberfläche erstellt worden. Es handelt sich vermutlich um eigens erstellte Applikationen, welche unter anderem ebenfalls für Webcrawling eingesetzt werden.

118 Zugriffe auf 21 unterschiedliche URI Pfade, welche häufig bei WordPress Blogs zu finden sind, wurden auf Port 443 registriert. Diese Zugriffe sind typisch für die automatisierte Erkennung von WordPress Blogs und einige der verwendeten Pfade können in weiterer Folge auch für Bruteforce Angriffe genutzt werden. Alle Zugriffe verwendeten einen üblichen unauffälligen User Agent und wurden von insgesamt 32 unterschiedlichen IP-Adressen getätigt. Die Verteilung der Zugriffe zur WordPress Erkennung über die unterschiedlichen Länder ist in Abbildung 2 dargestellt.

Zusätzlich wurden 27 Zugriffe auf 3 verschiedene URI Pfade auf Port 443 aufgezeichnet, welche aufgrund der URI Pfade mit hoher Wahrscheinlichkeit Webcrawlern beziehungsweise Bots zugeordnet werden können. Diese Zugriffe wurden von insgesamt 26 unterschiedlichen IP-Adressen getätigt.

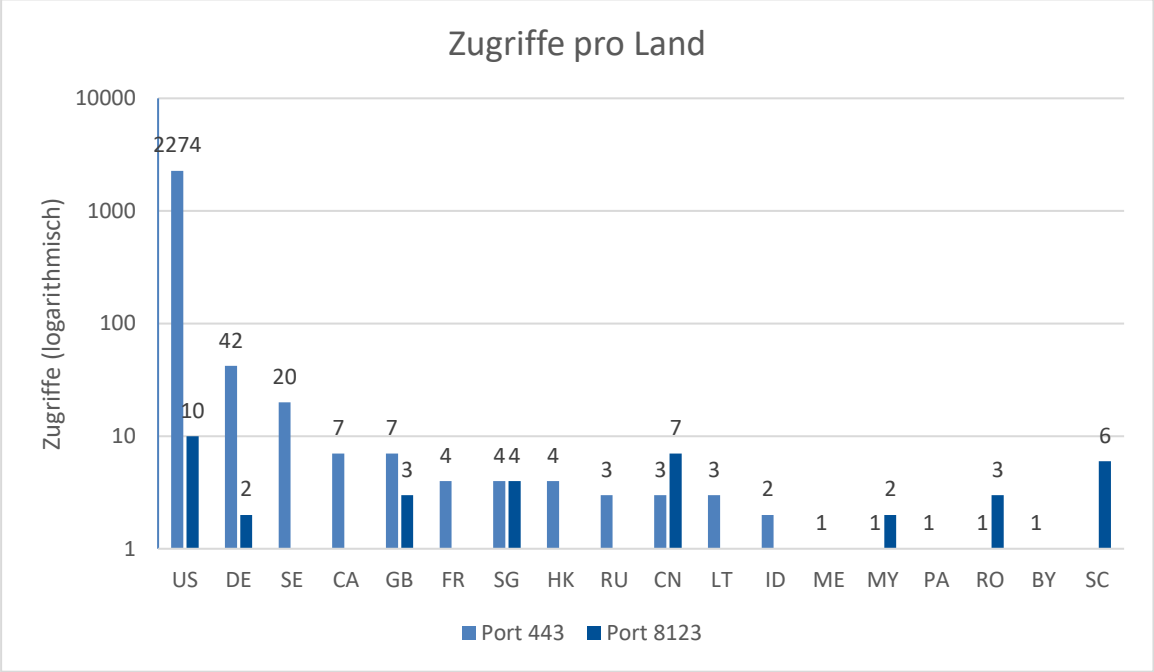

Abbildung 1

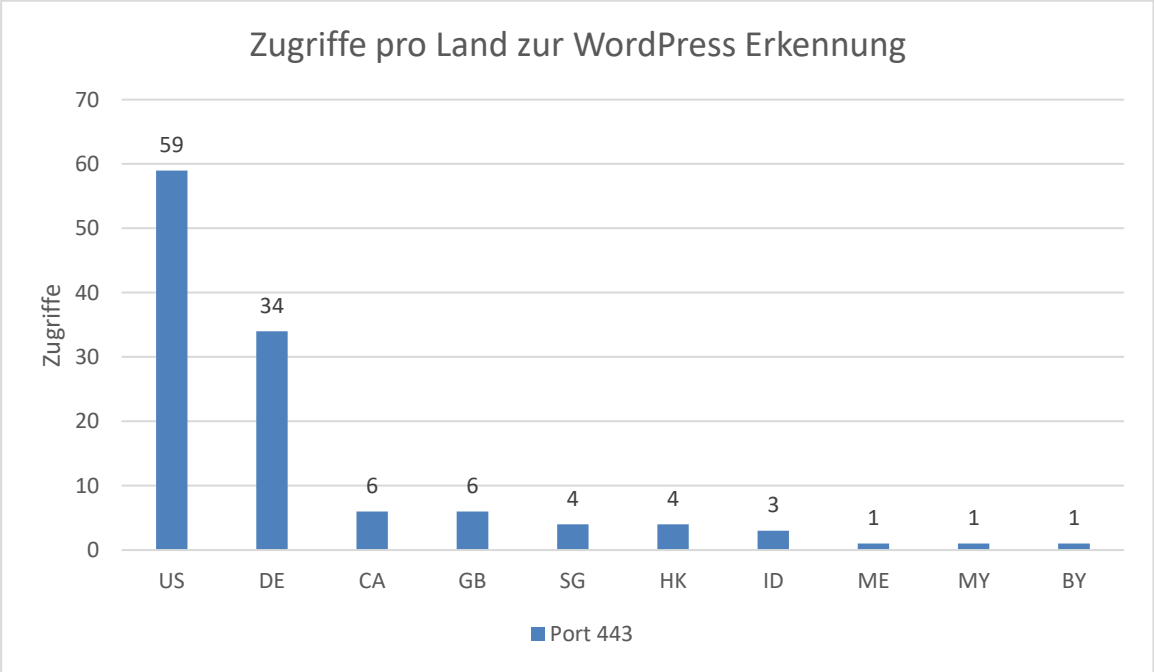

Abbildung 2