Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

IoT-Isolation über Mini-Router

Version 1.0 vom 23.05.2018
Peter Aufner – peter.aufner@iaik.tugraz.at

Abstract/Zusammenfassung: Dieses Projekt befasst sich mit dem Schutz des Heimnetzwerkes vor potentiellen Gefahren durch IoT Geräte. Hierfür werden die IoT Geräte vom restlichen Heimnetzwerk mittels eines extra Mini Routers getrennt. Der Fokus liegt auf der Anwenderfreundlichkeit einer sicheren Lösung. Durch die intensive Verwendung von Cloud-Diensten verschiedener Anbieter macht es für die Endanwenderin/den Endanwender keinen ersichtlichen Unterschied, ob die IoT Geräte im gleichen Netzwerk wie die restlichen Geräte im Heimnetzwerk sind oder nicht.

Inhaltsverzeichnis

1. Motivation

IoT Geräte erfreuen sich zunehmender Beliebtheit. Es wurden inzwischen viele Geräte, die üblicherweise im Haushalt zu finden sind, um 'smarte' Funktionen erweitert. Diese greifen oftmals auf eine Internetanbindung zurück. Das klingt auf den ersten Blick harmlos, jedoch bedeutet es, dass diese Geräte, ähnlich wie Computer, mit dem und über das Heimnetzwerk kommunizieren. Siehe Abbildung 1: Heimnetzwerk mit IoT Geräten. Da sie oftmals nicht mit Updates zur Behebung von möglichen Schwachstellen versorgt werden, stellen sie eine reale Bedrohung für andere Geräte im Heimnetzwerk, sowie die Privatsphäre der Besitzerin/des Besitzers dar.

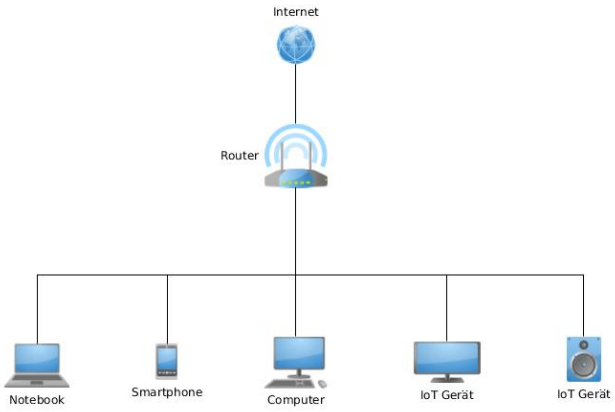

Abbildung 1: Heimnetzwerk mit IoT Geräten

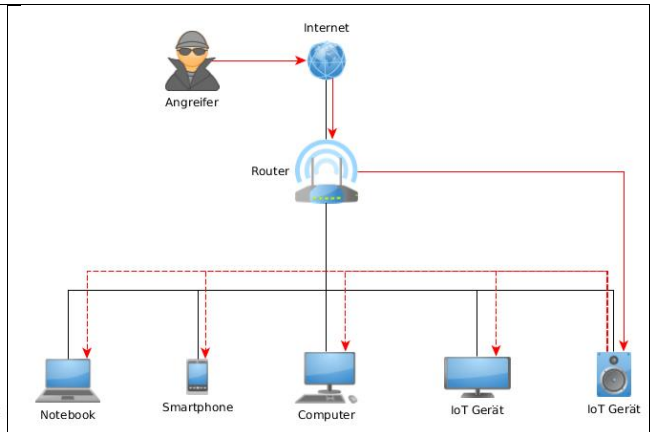

Abbildung 2: Angriff auf IoT Geräte im Heimnetzwerk

Gelingt es einem Angreifer beispielsweise eine smarte Steckdose zu übernehmen, kann er fortan den gesamten Datenverkehr im Heimnetzwerk mitlesen, eventuelle Schwachstellen auf anderen Geräten im Heimnetzwerk ausnutzen oder persönliche Daten exfiltrieren. Siehe Abbildung 2: Angriff auf IoT Geräte im Heimnetzwerk. Auch wenn die Anwenderin/der Anwender seine Computer im Heimnetzwerk softwareseitig auf dem neuesten Stand hält, schützt das nicht vor allen Angriffen. Ein möglicher Angriff ergibt sich durch Dateifreigaben, die aus Komfortgründen nicht durch Passwörter geschützt sind. Die ungeschützten Inhalte können von einem infizierten IoT Gerät ausgelesen und an Dritte weitergereicht werden. Für einen umfangreicheren Angriff können die IoT Geräte als Sprungbrett genutzt werden um andere Geräte mit unbekannten oder sehr aktuellen Schwachstellen anzugreifen. Das kann auch eine Anwenderin/einen Anwender treffen, die/der sicherheitstechnisch immer am neuesten Stand ist. Das Szenario als Sprungbrett stellt die größte Gefahr für das Heimnetzwerk dar, gelingt dies einem Angreifer, kann er sich in dem Heimnetzwerk bewegen, als wäre er im eigenen Heim und kann darüber hinaus auch die gesamte Kommunikation im Heimnetzwerk manipulieren.
Umgekehrt, wenn sich der Angreifer, beispielsweise ein technisch versierter Gast, im Heimnetzwerk befindet, könnte er den Datenverkehr der IoT Geräte überwachen und so Beobachtungen über das Nutzungsverhalten der Gastgeber ableiten.
Würde ein/e sicherheitsorientierte/r Anwender/in darauf verzichten die smarten Geräte ins Heimnetzwerk anzubinden oder ihnen zumindest verbieten, mit dem Internet zu kommunizieren, würde auffallen, dass sie sich bei weitem nicht mehr so vielseitig benutzen und miteinander verbinden ließen. Vor allem Assistenten, wie der Echo Dot, würden komplett nutzlos, da ihre gesamte Funktionalität von Cloud Servern zu Verfügung gestellt werden. Andere Geräte können eventuell noch daheim genutzt werden, aber ein Zugriff aus der Ferne, z.B. um mittels Überwachungskamera nach dem Rechten zu sehen, wäre dann nicht mehr möglich.

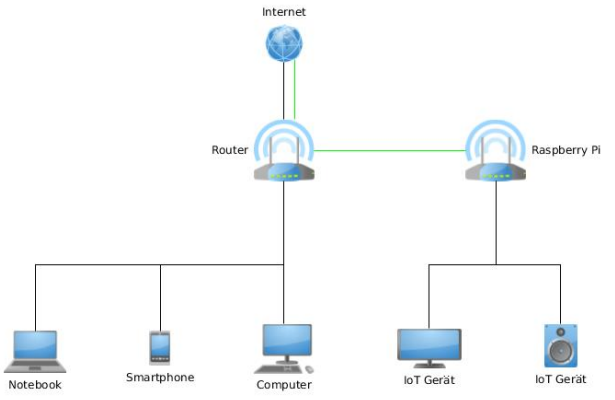

Abbildung 3: Heimnetzwerk mit separatem Netzwerk für IoT Geräte

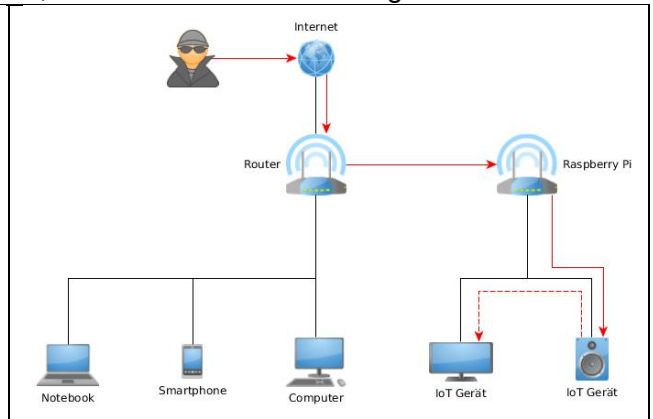

Abbildung 4: Angriff auf IoT Geräte in separatem Netzwerk

Darum wird in diesem Bericht ein Weg dargestellt, mit dem man IoT Geräte nutzen kann, ohne die Sicherheit des restlichen Netzwerks in Gefahr zu bringen, sowie einige Erfahrungen, die damit gemacht werden konnten.
Die Grundidee ist, den IoT Geräten ein eigenes Netzwerk zu Verfügung zu stellen, das ihnen weiterhin erlaubt, mit dem Internet zu kommunizieren. Dabei werden sie von den restlichen Geräten im Heimnetzwerk abgeschottet. Siehe Abbildung 3: Heimnetzwerk mit separatem Netzwerk für IoT Geräte. Aus Sicht der IoT Geräte existieren somit keine Computer mehr. Wenn ein Angreifer es schaffen sollte, eines der Geräte zu übernehmen, könnte er ausschließlich auf die anderen IoT Geräte zugreifen, das Heimnetzwerk bliebe aber geschützt. Siehe Abbildung 4: Angriff auf IoT Geräte in separatem Netzwerk.
Die Installation beruht auf einem Raspberry Pi. Diese Wahl wurde getroffen, da das Gerät mit Kosten von ca. €50 relativ günstig und gleichzeitig ein vollwertiger Computer ist. Dadurch erlaubt er eine umfangreichere Konfiguration als es ein ähnlich teurer Router zulassen würde.
Neben der Funktion als Gateway für IoT Geräte kann der Raspberry Pi auch andere Funktionen übernehmen, wie einen Webserver zu Verfügung zu stellen, um beispielsweise einen eigenen Dateiserver zu betreiben. Der andere Vorteil besteht darin, dass der Raspberry Pi sehr lange mit Updates versorgt wird. Heute ist es noch möglich die installierte Software auf der ersten Version des Raspberry Pis auf den gleichen Stand zu bringen, wie die letzte Generation. Dies schützt vor allem davor, später ein weiteres Gerät zu haben, welches potentiell nicht mit Updates versorgt wird.

2. Getestete Geräte

Die Möglichkeit zur Isolation von IoT Geräten wurde mit einer ausgewählten Kombination von drei Artikeln getestet, welche ein realistisches IoT Szenario in einem Heimnetzwerk abbilden sollen:

- Ein Amazon Echo Dot [1] wird als ‚Schaltzentrale' für das Netzwerk von IoT Geräten genutzt. Neben der Möglichkeit dem Sprachassistenten Alexa via dem Echo Dot Fragen zu stellen und Aufgaben zu erteilen, erlaubt er auch andere IoT Geräte zu steuern. So wird es möglich komplexe Abläufe mit einem einzigen Sprachbefehl zu orchestrieren.
- Philips Hue [2] ist eine Standardlösung zum Betrieb von smarten Leuchtkörpern im Haushalt. Es besteht aus einer Basisstation und vielen Lampen, welche beliebig gruppiert werden können.
- Eine TP-Link Sicherheitskamera [3] kann beispielsweise zur Überwachung des Heims in Abwesenheit, oder als Babymonitor genutzt werden.
- Die Auswahl an Geräten wird durch eine IoT Steckdose abgerundet. Hier wurde gezielt ein einfaches und billiges Produkt gewählt, um eine möglichst hohe Bandbreite an Preissegmenten und Produktqualitäten abzudecken.

Diese Kombination aus Geräten stellt sich als guter Einstieg für Anforderungen, die von einem smarten Heim erwartet werden, dar. Mit Philips Hue und der Steckdose könnte beispielsweise das Wohnzimmer zum abendlichen Fernsehen vorbereitet werden. Der Echo Dot erlaubt das mit einem einzigen Sprachbefehl durchzuführen. Inzwischen kann die Überwachungskamera genutzt werden um sicherzustellen, dass es dem im Nebenzimmer schlafenden Kind gut geht.

2.1. Amazon Echo Dot

Amazon Echo ist ein Lautsprecher mit eingebautem Mikrofon. Er erlaubt es mittels Sprachbefehlen verschiedene Aufgaben zu vollziehen. Einige Fähigkeiten funktionieren bereits, wenn man nur ein Echo oder Echo Dot besitzt, beispielsweise "Alexa, wie spät ist es". Das wird mit der momentanen Uhrzeit beantwortet. Ebenso ist es möglich wissensbezogene Fragen zu stellen, beispielsweise "Alexa, wie hoch ist der Eiffelturm?". Anfragen dieser Art werden mit Informationen von diversen Internetquellen, wie Wikipedia, beantwortet. Ebenso kann auf viele Funktionen, die vor allem für Amazon Prime Kunden interessant sind, zugegriffen werden. Zum Beispiel kann Musik abgespielt werden, Artikel in den Amazon Einkaufswagen gelegt werden, etc.
Während diese Anwendungsfälle durchaus interessant sind, erreicht Echo erst einen vollen Funktionsumfang, wenn er mit so genannten 'Skills' erweitert wird. Diese erlauben es mit einer Vielzahl anderer IoT Geräte zu interagieren. Mit der richtigen Kombination aus IoT Steckdosen, Lichtschaltern und anderen Geräten ist es so möglich komplexe Abläufe mit einem einzigen Befehl zu orchestrieren. Zum Beispiel könnte man einen Befehl "Alexa, bereite Wohnzimmer vor" so definieren, dass die Lichter gedimmt werden, der Fernseher und das Multimediasystem, sowie eine

Spielkonsole eingeschaltet werden. Man muss sich dann nur noch hinsetzen und die Geräte benutzen.
Der Ablauf eines solchen Befehls erfordert einiges an Kommunikation mit dem Internet. Die vormals erwähnten Skills greifen üblicherweise auf eine Kombination von Cloud Angeboten diverser Hersteller zurück. Beschränken wir uns nur auf das Ein- und Ausschalten einer IoT Steckdose: Um das via Echo zu ermöglichen, muss als Erstes die Steckdose mit Alexa kompatibel sein. Anschließend ist es notwendig einen Account in der Cloud des Herstellers anzulegen. Anschließend wird die Skill online für Alexa aktiviert. Dabei bittet Alexa um Zugangsdaten für den Account des Steckdosenherstellers. Damit sind die beiden Technologien verbunden. Teilt man einem Echo mit, dass die Steckdose aufgedreht werden soll, führt das dazu, dass Echo mit der Alexa Cloud kommuniziert. Diese erkennt den Befehl und leitet ihn weiter an die Cloud des Steckdosenherstellers, welche dann wiederum an die Steckdose daheim den Befehl schickt sich einzuschalten.
Die Ersteinrichtung von Alexa ist mittels Webbrowser am PC oder Smartphone App möglich.

2.2. Philips Hue
Hue ist ein System für IoT Lampen. Es setzt sich aus einer Basisstation und mehreren Lampen zusammen. Die Basisstation kann ausschließlich per LAN in das Heimnetzwerk angebunden werden. Zur Kommunikation mit den Lampen wird das ZigBee Protokoll genutzt. Dieses stellt ein standardisiertes Protokoll zur Steuerung kabellos angebundener IoT Geräte dar. Die Lampen können via App in beliebige Gruppen zusammengefasst werden, sodass eine Station genügt um, je nach Funkreichweite, die Lampen im gesamten Heim zu steuern. Die Steuerung der Lampen erfolgt via Smartphone App. Es ist darüber hinaus möglich Hue mit Alexa zu kombinieren. Hierfür ist es notwendig einen Philips Hue Account anzulegen und die eigene Basisstation zu registrieren. Dann kann mittels Alexa Skill der Account angebunden werden und die Steuerung der Lampen via Spracheingaben an Echo erfolgen.
Für die Ersteinrichtung wird unbedingt ein Smartphone mit Android oder iOS und installierter Philips Hue App benötigt.

2.3. TP-Link NC200 WLAN Cloud-Sicherheitskamera
Die Sicherheitskamera von TP-Link erlaubt die Videoüberwachung eines beliebigen Bereiches. Sie kann via Ethernet oder W-LAN an das Netzwerk angebunden werden. Die Kamera kann prinzipiell auch ohne Internetanbindung genutzt werden. Sie stellt ein Webinterface zur Verfügung, über welches das Video der Kamera abgerufen werden kann. Alternativ ist es auch möglich, den Videofeed via Smartphone App zu betrachten. Es besteht optional die Möglichkeit, die Kamera in der TP-Link Cloud, zu registrieren um von einem beliebigen Standort Zugriff auf das gelieferte Bild zu haben.
Die Ersteinrichtung erfolgt via Web Interface der Kamera oder Smartphone App.

2.4. 'No-Name' Wi-Fi Smart Socket
Bei dieser IoT Steckdose handelt es sich um ein sehr einfaches Gerät, das per W-LAN in das Heimnetzwerk integriert wird. Sie erlaubt via Smartphone App eine Steckdose ein- oder auszuschalten. Zusätzlich verfügt die Steckdose über eine eigene Cloud, die eFamily Cloud, welche es auch erlaubt, die Steckdose aus der Ferne zu bedienen. Wieder ist es möglich, mittels Alex Skill die Steckdose mit Sprachkommandos von Alexa zu steuern. Hierbei wird der eFamily Cloud Account mit Alexa verbunden.

3. Beobachtungen
In diesem Abschnitt werden einige Erfahrungen mit dem Betrieb von IoT Geräten in einem separaten Netzwerk beschrieben. Die Beobachtungen werden in 3 Phasen aufgeteilt: Einrichtung des separaten Netzwerks, Einrichtung der IoT Geräte, tägliche Verwendung.

3.1. Einrichtung des separaten Netzwerks
Die Einrichtung des separaten Netzwerkes erfordert das meiste technische Verständnis. Für die Konfiguration des Raspberry Pi ist zumindest ein grundlegendes Verständnis der Linux Kommandozeile und der Konfiguration des eigenen Heimnetzwerkes notwendig. Sind beide

Voraussetzungen erfüllt, lässt sich die Einrichtung anhand der Anleitung binnen ein bis zwei Stunden nachvollziehen.
Ebenso muss man bei seinem bestehenden Router in der Lage sein, dem Raspberry Pi eine statische IP Adresse zuzuweisen und ihn in die DMZ (DeMilitarized Zone) zu setzen. Die DMZ ist der Schlüssel zu dem Projekt, da sie den Raspberry Pi am restlichen Netzwerk vorbei direkt ins Internet anbindet. Darum ist es wichtig, den Raspberry Pi vor diesem Schritt entsprechend abzusichern.

3.2. Einrichtung der IoT Geräte

Im Allgemeinen empfiehlt es sich zur Einrichtung von IoT Geräten ein Smartphone mit der dazugehörigen App zu verwenden. Die getesteten IoT Geräte stellen im Auslieferungszustand ein eigenes W-LAN zu Verfügung, welches automatisch von der App erkannt wird. Anschließend ist es möglich das Gerät in das vorgesehen W-LAN einzubinden. Außerdem weisen Apps oftmals auf die Verfügbarkeit von Firmware Updates hin und erlauben, diese mit einem Druck einzuspielen. Der Hinweis auf ein vorhandenes Update fehlte beispielsweise im Web Interface der TP-Link Sicherheitskamera.
Der Echo Dot und die TP-Link Sicherheitskamera bieten auch eine Konfiguration via Browser am Computer an. Bei Philips Hue fehlt dieses Feature allerdings vollends. Möchte man IoT Geräte nutzen, sollte man davon ausgehen ein Smartphone besitzen zu müssen oder sehr genau acht zu geben, ob die Verwendung ohne Smartphone möglich ist. Hierfür empfiehlt sich die Gebrauchsanweisung vorab von der Herstellerwebseite zu beziehen.
Ein Problem mit der bestehenden Einrichtung stellt die Philips Hue Basisstation dar: Die Basisstation kann ausschließlich per LAN angebunden werden. Beim Raspberry Pi ist der einzige LAN Anschluss jedoch bereits zur Anbindung an den bestehenden Router belegt. Das Problem könnte mittels Anschluss eines weiteren Ethernet Adapters gelöst werden, was für diesen Test jedoch nicht durchgeführt wurde, darum blieb Philips Hue im regulären Heimnetzwerk.
Bei der Einrichtung ist weiters zu beachten, dass jeder Hersteller seine eigene Cloud zu Verfügung stellt. Will man über getrennte Netzwerke auf die Geräte zugreifen oder sie mit einem Assistenten wie den Echo Dot integrieren, ist es notwendig bei jeder Cloud einen Zugang anzulegen. Gutes Passwortmanagement ist hier besonders wichtig um sich vor einer Übernahme der IoT Infrastruktur bei Fehlverhalten eines Anbieters zu schützen.
Besonders brisant wird dies, wenn es um die Sicherheitskamera geht. Wird die Cloud Anbindung der Kamera kompromittiert, könnte sie von einem Angreifer beispielsweise genutzt werden um einen Einbruch so zu planen, dass niemand zu Hause anwesend ist.

3.3. Tägliche Verwendung

Alle IoT Geräte wurden mit den entsprechenden Clouds der Hersteller verbunden. Dadurch ist die Bedienung der Geräte mit dem Smartphone oder Echo Dot sehr komfortabel. Die Abtrennung vom regulären Heimnetzwerk, in dem sich üblicherweise auch das Smartphone befindet, fällt nicht auf.

Durch den Umstand, dass Philips Hue im regulären Heimnetzwerk angeschlossen ist, konnte auch festgestellt werden, dass trotz der Grenze zwischen dem Echo Dot und Philips Hue die Integration zur Sprachsteuerung problemlos gelingt. Das funktioniert, da in Wirklichkeit alle Befehle zuerst an die Amazon Cloud geschickt werden, welche sie an die Philips Cloud weiterreicht, um sie dann an die lokale Hue Basisstation zu übergeben. Umgekehrt bedeutet das auch, dass mit einer massiven Einschränkung der Funktionalität zu rechnen ist, falls die Internetverbindung unterbrochen wird.

Die Vernetzung der IoT Geräte mittels Echo Dot und dem dahinterstehenden Cloud Dienst Alexa führt insgesamt zu einem sehr angenehmen Nutzungserlebnis. Alexa kann mittels so genannten Skills erweitert werden, welche selbst für die getestete ‚No-Name' Steckdose zu Verfügung stehen.

4. Zusammenfassung des Aufbaus

Für die Isolation der IoT Geräte vom restlichen Heimnetzwerk wurde ein Raspberry Pi als W-LAN Router eingerichtet. Dieser wurde an den bestehenden Router angeschlossen und vom restlichen Heimnetzwerk unter Verwendung der DMZ Funktion abgetrennt. IoT Geräte wurden dann mit dem W-LAN des Raspberry Pi verbunden. Auf diesem Weg werden sie vom restlichen Heimnetzwerk

abgeschottet und bleiben trotzdem über das Internet zugänglich. Außerdem ist so sichergestellt, dass sie in ihrem vollen Funktionsumfang genutzt werden können. Eine detaillierte Anleitung zum Aufbau ist als separates Dokument beiliegend verfügbar.

5. Conclusio

Es ist möglich IoT Geräte mit zusätzlicher Hardware abgeschottet in das Heimnetzwerk einzubinden. Der Aufwand für die erste Installation der vorgeschlagenen Lösung ist für technisch versierte Personen mit relativ geringem Zeit- und Arbeitsaufwand möglich. Durch die Abschottung wird es unmöglich Computer und Smartphones im Heimnetzwerk via Schwachstellen in IoT Geräten anzugreifen.
Mit den getesteten Geräten fällt einzig der Mehraufwand bei der Installation auf. Hierbei ist es notwendig sein Smartphone oder Computer in das separate W-LAN einzubinden um das neue IoT Gerät zu konfigurieren.
Der tägliche Betrieb funktioniert einwandfrei. Solange eine Verbindung zu dem Internet besteht, können Smartphones und Computer, wie gehabt, in ihrem LAN sein und die IoT Geräte bleiben in ihrem abgeschotteten W-LAN. Ohne Internetverbindung wäre es notwendig mit einem Gerät in das IoT W-Lan zu wechseln um die Geräte bedienen zu können.

Referenzen

[1] Amazon, „Echo Dot,“ [Online]. Available: https://www.amazon.de/dp/B01DFKBG54/ref=nav_shopall_k_echo_biscuit. [Zugriff am 14 05 2018].

[2] Philips, „Hue,“ [Online]. Available: https://www2.meethue.com/de-at. [Zugriff am 14 05 2018].

[3] TP-Link, „NC200 Cloud Sicherheitskamera,“ [Online]. Available: https://www.tp-link.com/at/products/details/NC200.html. [Zugriff am 14 05 2018].