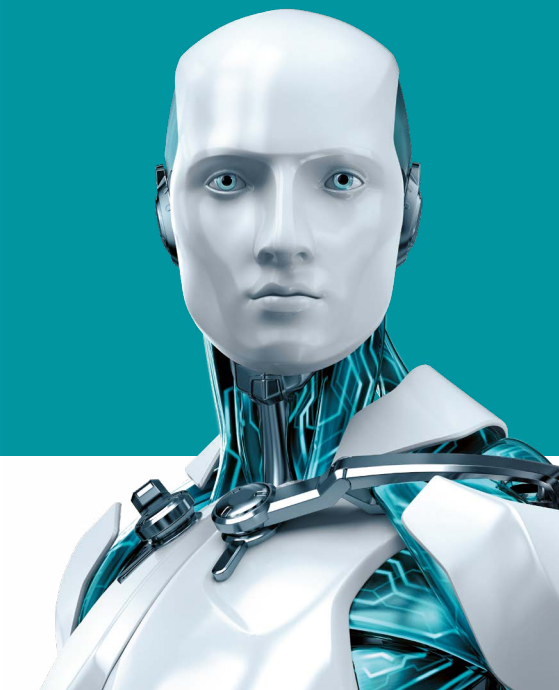
INTERNET DER DINGE – SMARTES HEIM MIT PRIVATSPHÄRE?

Autor:
Tony Anscombe

Researcher:
Juraj Bartko, Ivan Bešina, **Miloš Čermák,**
Milan Fránik, Štefan Svorenčík, **Kacper Szurek**



ENJOY SAFER TECHNOLOGY™

INHALT

1. ÜBER DAS INTERNET DER DINGE

Mit dem Begriff „Internet der Dinge" („Internet of Things" = IoT) werden wortwörtlich alle möglichen Dinge bezeichnet, die mit dem Internet verbunden sind und üblicherweise am Arbeitsplatz oder aber Zuhause genutzt werden. Fragt man dabei nach konkreten IoT-Geräten, fallen die Antworten sehr unterschiedlich aus und reichen von Smartphones, intelligenten Glühlampen über Fitness-Tracker und smarte Lautsprecher bis hin zu Geschirrspülern oder Sensoren zur Messung der Wasserqualität.

Mit Aufkommen des IoT-Trends wurde bezüglich der zu erwartenden Verbreitung mit großen Zahlen jongliert. Der ehemalige ***CEO von Ericsson, Hans Vestberg*** prophezeite 2010, dass es bis 2020 50 Milliarden vernetzte Geräte geben würde. Acht Jahre und das Abklingen des Hypes später haben wir es mit etwas moderateren Prognosen zu tun. Heute geht ***Ericsson von 29 Milliarden vernetzten Geräten bis 2022 aus***, von denen 18 Milliarden konkret unter den Begriff des Internets der Dinge fallen.

Während das Rätselraten rund um die Zahlen weitergehen wird, scheint sicher zu sein, dass die meisten dieser Geräte auf den Verbrauchermarkt abzielen. In einem Smart Home können die intelligenten Helfer den Alltag vereinfachen, bergen allerdings auch Risiken für die Privatsphäre und Sicherheit der Konsumenten. Denn die in den Produkten verbauten Sensoren – Mikrofone, Kameras, GPS-Schnittstellen usw. – sind ein vielversprechendes Ziel für Cybergangster. Erlangen Kriminelle die Kontrolle über dieses Zubehör, könnten sie weitere Geräte im Netzwerk angreifen oder sensible und persönliche Daten abfangen.

In diesem Whitepaper wollen wir dem Trend zum Smart Home als Teil des Internets der Dinge auf den Grund gehen und insbesondere Bedenken bezüglich der Privatsphäre beleuchten. Dabei bleiben wir so objektiv wie möglich und sprechen Probleme offen an.

Da es keine allgemeingültige Definition dessen gibt, was genau ein Smart Home ist, haben wir uns ein paar ausgewählte Produkte angeschaut, die sich unserer Meinung nach heute in einem vernetzten Heim finden lassen könnten.

Ein echtes Smart Home bedarf natürlich einer großen Umgestaltung und eines beachtlichen finanziellen Aufwands. Ziel ist die Schaffung einer Umgebung, die sich automatisch und ohne direkte Nutzerinteraktion dem eigenen Lebensstil anpasst. Für viele Verbraucher besteht der Reiz darin, Strom- und Energiekosten zu senken oder aber den Luxus zu steigern.

Für die meisten von uns ist das echte Smart Home ein Konzept der Zukunft. Viele Haushalte verfügen über einzelne IoT-Geräte, die hier und da einen bestimmten Nutzen oder Komfort bieten, aber ein ganzheitliches intelligentes Heim ist für viele noch Science Fiction. Eine große Herausforderung hierbei liegt beim Zusammenspiel der verschiedenen Geräte, das zur Schaffung eines rundum vernetzten Systems notwendig ist.

Allen IoT-Geräten ist gemein, dass sie eine Menge Daten erheben und verarbeiten. Das allein rechtfertigt die Bedenken vieler Verbraucher bezüglich des Risikos, dass Daten versehentlich oder durch kriminelle Aktivitäten in die falschen Hände geraten könnten.

Erst kürzlich hat der 20-jährige Australier, ***Nathan Ruser, via Twitter*** gezeigt, welche Sicherheitsrisiken mit smarten Geräten verbunden sein können. Am 27. Januar 2018 hatte der Student auf ein Problem mit der ***Fitness-App von Strava*** aufmerksam gemacht. Die App nutzt die GPS-Koordinaten seiner Nutzer zur Anzeige von beliebten Laufstrecken, Fahrradrouten oder sonstigen Fitnessaktivitäten. Bei der Installation wird die anonyme Bereitstellung der Daten standardmäßig zugelassen. Wie Ruser zeigte, war es über die App möglich, die regelmäßige Joggingroute der US-Soldaten am Militärflugplatz in Bagram, Afghanistan zu erkennen. Dieses Beispiel verdeutlicht, dass die Sammlung und Verknüpfung von Daten für einen nützlichen Zweck zu ungeahnten Sicherheitsproblemen führen kann. Mit der App können Nutzer fernab der heimischen Laufstrecke problemlos eine Joggingroute finden, die potenziellen Konsequenzen für Sicherheit und Privatsphäre sind allerdings nicht auf den ersten Blick erkennbar.

2. INTELLIGENT VERNETZT – DAS SMART HOME

Ob Knight Rider, Star Trek oder Terminator – in den Köpfen von Science Fiction Autoren existiert schon lange eine Welt, die sich über vernetzte intelligente Technologien steuern lässt. Mit der Zunahme an smarten Geräten wie Kameras, Waagen und Sensoren, ganzen Home Management Systemen, Herzschrittmachern und Autos wird diese Vision immer mehr zur Realität. Wie weit man dabei gehen kann, zeigt die kalifornische Stadt San Jose. Hier hat man sich dem Projekt verschrieben, über vernetzte intelligente Verkehrsmittel und Infrastrukturen ***zu einer „Smart City" zu werden,*** die seinen Bürgern neben optimaler Mobilität noch mehr Sicherheit und Lebensqualität bietet.

Aber auch im Eigenheim sind die Möglichkeiten schon heute schier unendlich. Dabei ist der Aufbau eines Smart Homes im Prinzip relativ simpel. Man hat ein Gerät und ein Netzwerk, mit dem das Gerät verbunden ist. Hinzu kommt ein weiteres Gerät – meistens ein Smartphone – über das das erste Gerät gesteuert wird. Dazu bedarf es eines Cloud-Dienstes, der die Daten speichert und die Kommunikation zwischen den beiden Geräten, in der Regel mithilfe einer App, ermöglicht. Darüber hinaus kann eine weitere Komponente in Form eines Management-Systems integriert werden, das über ein Master-Gerät oder einen Hub als zentrale Schnittstelle die Verwaltung aller vernetzten Smart-Geräte ermöglicht. Eine Gruppe von ESET Experten hat sich die Aufgabe gestellt, einige dieser beliebten IoT-Geräte auf Herz und Nieren zu prüfen.

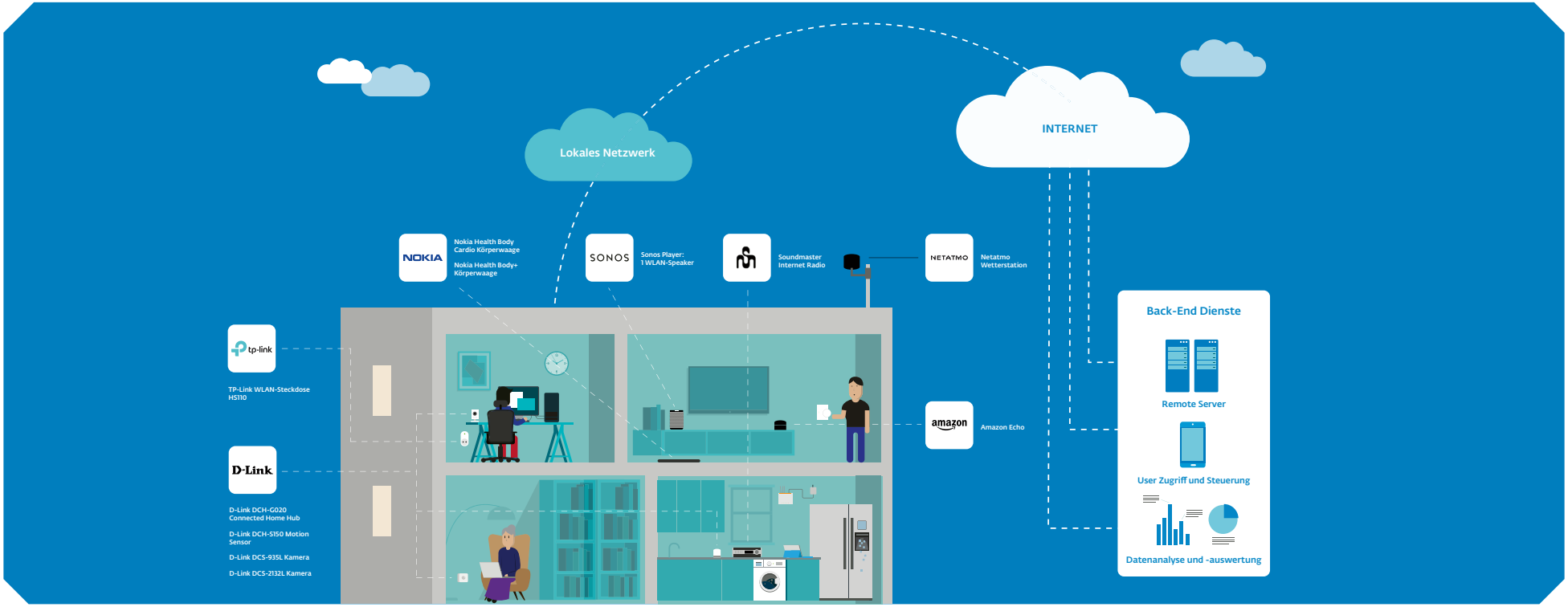


Abb. 1: Geräte und Verbindungen in unserem Smart Home

3. DATENSCHUTZ VS. SAMMELWUT?

Jeder Hersteller sollte über eine Datenschutzerklärung oder ein ähnliches Dokument verfügen, in dem erklärt wird, wie und wozu Daten vom Gerät oder den Diensten gesammelt werden. In einigen Fällen waren die Richtlinien schwer zu finden, sehr kompliziert oder aber allzu vage formuliert. Andere Hersteller haben sich sichtlich bemüht, ihre Dokumente benutzerfreundlich zu gestalten.

Viele Unternehmen tendieren in ihren Datenschutzerklärungen dazu, weit mehr Daten aufzuzählen, als tatsächlich gesammelt werden. Das ist vermutlich der Tatsache geschuldet, dass man diese komplexen Dokumente meist nicht ohne umfangreiche juristische Unterstützung aufsetzten, ändern und aktualisieren kann. Um eine möglichst lange Nutzung der Richtlinien zu gewährleisten, werden also schon Daten genannt, die eventuell erst zukünftig gesammelt werden.

In diesem Whitepaper sollen die Gründe und der Umfang der Datenerhebung an sich nicht bewertet werden. Uns interessiert in Anbetracht der Menge und Qualität der gesammelten Daten viel mehr, wie groß das Risiko ist, dass sensible Informationen entweder unwissentlich durch den Nutzer oder aufgrund krimineller Aktivitäten preisgegeben werden.

Wir gehen davon aus, dass die meisten Geräte und Dienste grundlegende persönliche Daten wie Name, Adresse, Geburtsdatum, E-Mail-Adresse und Telefonnummer sammeln. Die darüber hinaus aufgeführten Daten haben wir den jeweiligen Datenschutzbestimmungen entnommen. Häufig werden hier Phrasen wie „nicht begrenzt auf" verwendet, womit sich Unternehmen das Recht zusichern, mehr als die von ihnen genannten Daten zu erheben.

Beim Einsatz von Geräten, die über den Dienst eines Drittanbieters steuerbar sind, werden die Daten oftmals von beiden beteiligten Herstellern gesammelt. Die Produkte von D-Link können beispielsweise über Amazons Alexa gesteuert werden. Über einen einfachen Befehl wie „Alexa, schalte die Kamera in der Garage an" erhalten sowohl die mydlink-App als auch Amazon die Anweisung und somit Informationen darüber, welche Geräte sich in welchen Räumen befinden. Natürlich ist es sehr bequem, all seine Geräte über eine einzige zentrale Stelle zu steuern. Allerdings kann diese eine Entität dann ein ziemlich umfangreiches Profil über mich und meinen Lebensstil erstellen.

4. ZWO, EINS, SICHERHEITSRISIKO

Haben wir Schwachstellen gefunden? Ja.

Wir haben insgesamt zwölf Produkte von sieben Herstellern getestet. Im Folgenden werden elf davon näher betrachtet. Beim nicht genannten Produkt haben wir im Zuge unserer Untersuchung signifikante Sicherheitslücken gefunden, über die wir den Hersteller informiert haben. Im Sinne von „Responsible Disclosure" möchten wir dem Unternehmen die Möglichkeit geben, die Mängel zu beheben. Bei diesem Produkt handelt es sich um ein Steuergerät zur Verwaltung von Bewegungssensoren, Heizungsreglern, Rollladenmotoren und Smart-Steckdosen. Zu den gefundenen Problemen gehörten:

- *Die Anmeldung am lokalen Netzwerk ist nicht gut abgesichert. Bei der voreingestellten Option zur automatischen Anmeldung werden weder Nutzer-ID noch Passwort abgefragt. Der Hersteller benennt das Problem in einer Sicherheitsmeldung und empfiehlt, diese Option zu deaktivieren.*

- *Wie bei fast allen Smart Home Systemen können die verbundenen Geräte über einen Cloud-Dienst zentral gesteuert werden. Die Kommunikation mit diesem Dienst ist allerdings nicht verschlüsselt.*
- *Der Cloud-Dienst des Anbieters bietet die Möglichkeit, eine VPN (Virtual Private Network) Verbindung zum Gerät herzustellen. Anschließend können die Netzwerkkonfigurationen geändert werden. So könnte ein Unbefugter Zugriff auf das lokale Netzwerk des Nutzers erlangen.*
- *Der Zugang zum Cloud-Dienst erfordert eine Registrierung. Werden die Zugangsdaten des Nutzers kompromittiert, stellt der VPN-Zugang zum Netzwerk ein erhebliches Sicherheitsrisiko dar.*

Die Prüfung der verbleibenden elf Geräte hat gezeigt, dass sich Interessierte vor dem Kauf umfangreich informieren sollten. Die ***D-Link Kameras*** und die ***Smart-Steckdosen von TP-Link*** beispielsweise haben gut dokumentierte Schwachstellen. Bei Kameras besteht die größte Sorge in einer fehlenden Verschlüsselung des Video-Streams und, wie in diesem Fall, einer schwachen Authentifizierung.

Es gibt durchaus sichere Kameras, bei denen der Video-Stream sowohl in Echtzeit als auch nach Speicherung verschlüsselt wird. Die hier getesteten Kameras sind von einem bekannten Hersteller, die Marke selbst sagt also nicht immer etwas über die Sicherheit der Produkte aus.

5. UND WAS IST MIT MEINER PRIVATSPHÄRE?

Gibt es Bedenken bezüglich der Privatsphäre? Ja.

Jedes Gerät benötigt zur Bereitstellung seiner Funktionen bestimmte Daten und in den meisten Fällen schienen die erhobenen Informationen in diesem Zusammenhang sinnvoll. Lediglich für das Soundmaster Internet Radio konnten wir keine Datenschutzerklärung oder andere Nutzungsbedingungen finden, was uns stutzig gemacht hat. Ohne Richtlinien kann es schließlich keine informierte Einwilligung geben.

Unsere größte Sorge bezieht sich auf die sprachgesteuerten intelligenten Assistenten – in diesem Fall Alexa. Diese Helfer können für Cyberkriminelle eine wahre Schatztruhe sein, da sie mit allen anderen Geräten interagieren. Unabhängig vom Umgang mit den Daten durch den Dienst oder Amazon selbst, könnte ein Angreifer durch einen zielgerichteten Phishing-Angriff die Zugangsdaten zum Amazon-Account stehlen und anschließend auf Alexa und alle hier gespeicherten Daten zugreifen.

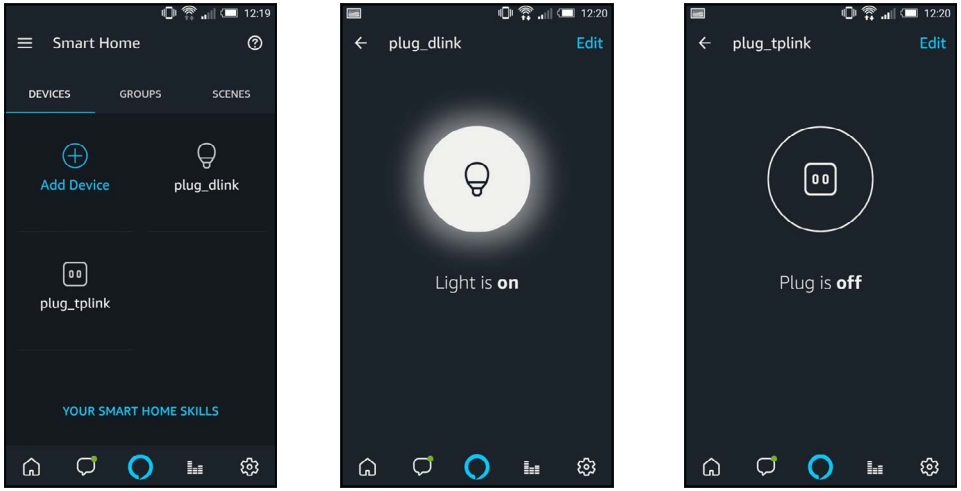


Abb. 2: Beispiele für Smart Home Funktionen in der Alexa App

Alexa, kannst du abgesichert werden? Vielleicht.

Entscheiden Sie sich für diesen charmanten, folgsamen Assistenten, sollten Sie ***bei der Konfiguration*** ein paar Dinge beachten:

- *Verzichten Sie auf Einkäufe per Sprachbefehl oder nutzen Sie zumindest eine PIN.*
- *Bringen Sie Alexa bei, Ihre Stimme zu erkennen und beschränken Sie die Steuerung allein auf Ihre Befehle.*
- *Wenn Sie gerade keine Hilfe benötigen, schalten Sie Alexa ab oder das Mikrofon stumm.*

6. DIE GETESTETEN GERÄTE: STÄRKEN UND SCHWÄCHEN

Amazon

Amazon Echo (2. Generation)

Amazon Echo ist ein Freisprechassistent, über den Sie mit Alexa kommunizieren können, um Fragen zu stellen, Befehle zu erteilen oder Geräte in Ihrem Smart Home zu steuern, die mit diesem Helfer kompatibel sind.

Amazon Echo ist ein Lautsprecher, der zudem über sieben Mikrofone und Mechanismen zur Geräuschunterdrückung verfügt, damit Alexa Ihre Anweisungen überall im Raum hört – selbst wenn Musik läuft.

Immer mehr Hersteller unterstützen Alexa. Über sogenannte Skills können die Geräte und Dienste anderer Anbieter über den intelligenten Assistenten zentral gesteuert werden.

Alexa Nutzungsbedingungen

https://www.amazon.de/gp/help/customer/display.html?nodeId=201809740

Amazon verarbeitet und speichert

> Ihre Alexa Interaktionen
> Spracheingaben
> Musikwiedergabelisten
> Ihre Alexa-To-do und -Einkaufslisten

Informationen über Alexa-fähige Produkte

> Gerätetyp
> Name
> Gerätespezifikationen
> Status
> Netzwerkverbindung
> Standort

Amazon kann für bestimmte unterstützte Produkte automatisierte Updates im Namen der jeweiligen Hersteller vornehmen.

Hinweis: Die genannten Informationen beziehen sich ausschließlich auf Amazons Echo und Alexa. Es handelt sich nicht um eine generelle Amazon Datenschutzerklärung.

Sicherheit & Privatsphäre

Wer einen Amazon Echo Lautsprecher besitzt, schätzt vermutlich den zuvorkommenden und hilfsbereiten Assistenten Alexa. In Bezug auf die Schaffung eines Smart Homes ist dieses Gerät derzeit wohl unentbehrlich. Sowohl direkt als auch indirekt über die Verbindung mit anderen Geräten stellt Alexa eine Vielzahl an Diensten bereit und ermöglicht unter anderem Wiedergabe von Musik, Vorlesen von Nachrichten, Prüfung Ihres Kalenders, Erstellung einer To-do-Liste und sogar Einkäufe über Ihren Amazon Account.

Amazon Echo ist sprachgesteuert. Das Gerät bleibt so lange inaktiv, bis Sie Alexa durch einen Befehl zum Leben erwecken. Die Anweisung wird zur Analyse und Generierung einer passenden Reaktion an Amazon geleitet. Diese Interaktionen werden mit Ihrem Amazon Account verbunden und können jederzeit geprüft werden.

Nutzt man Alexa zur Steuerung des Produkts oder Dienstes eines anderen Anbieters, so erhält dieser nicht die komplette Audioanfrage, sondern lediglich die konkrete Anweisung. Damit diese Kommunikation funktioniert, muss der Drittanbieter eine Verbindung mit Alexa bereitstellen. Hierbei spricht man auch von sogenannten Alexa Skills.

Alle Interaktionen mit Alexa werden in Ihrem Amazon Account abgespeichert. Die Audioaufnahmen können Sie entweder einzeln in der Alexa App oder aber gebündelt über die Amazon Webseite löschen. Die Frage ist aber, ob die Nutzer engagiert genug sind, um die Interaktionen regelmäßig zu prüfen und als zu persönlich eingestufte Aufnahmen zu löschen. Wir befürchten, dass das nicht der Fall ist.

Über die Interaktionen erhält Amazon unter Umständen ziemlich umfangreiche Informationen über Ihre Interessen, Vorlieben, Hobbies usw. Mit diesen Daten lässt sich dann ein Profil erstellen, das ziemlich konkrete Details über Ihren Lebensstil preisgibt. Unabhängig davon, dass viele Unternehmen ein Interesse an diesen Informationen haben könnten, sind sie insbesondere für Cyberkriminelle sehr wertvoll. An dieser Stelle sei allerdings nochmals darauf hingewiesen, dass Sie als Nutzer die Kontrolle haben und Amazon die Informationen transparent bereitstellt. Audioaufnahmen lassen sich jederzeit abspielen und löschen. Und sollten Sie sich allzu große Sorgen machen, können Sie Alexa entweder komplett ab- oder zumindest stummschalten.

Angesichts wiederkehrender Meldungen über gestohlene Zugangsdaten kann ein Helfer wie Alexa Grund zur Sorge sein. Denn bei der Quantität und Qualität der gespeicherten Informationen könnte der unautorisierte Zugriff auf Ihren Amazon Account verheerende Folgen haben.

Aber keine Panik! Es gibt einige Vorsichtsmaßnahmen, die Sie ergreifen können.

- *Nutzen Sie die Spracherkennung, damit Alexa ausschließlich auf Ihre Befehle hört.*
- *Löschen Sie die Audioaufnahmen vergangener Interaktionen.*
- *Verzichten Sie auf Geräte, die allzu persönliche Daten verarbeiten.*
- *Schalten Sie Alexa ab, wenn Sie gerade keine Hilfe benötigen.*
- *Schützen Sie Ihren Amazon Account mit einer Zwei-Faktor-Authentifizierung. Damit verhindern Sie unerlaubte Zugriffe, selbst wenn Ihre Zugangsdaten gestohlen werden.*

D-Link

Geräte

DCH-G020 Connected Home Hub

Der DCH-G020 Connected Home Hub fungiert als Bindeglied zwischen Ihrem bestehenden WLAN und den verbundenen mydlink-Geräten. Wird er zusammen mit mydlink Home Sensoren eingesetzt, kann er das Öffnen von Türen oder Fenstern sowie Bewegungen in Ihrem Heim melden. Über die mydlink Home App lässt sich der Hub einrichten und verwalten.

DCH-S150 Motion Sensor

Der DCH-S150 Motion Sensor erkennt Bewegungen und lässt sich mit anderen Geräten verbinden, um bestimmte Aktionen durchzuführen. Kombiniert mit einer Kamera kann beispielsweise ein Video aufgenommen oder mit einer Smart-Steckdose das Licht angeschaltet werden. Meldungen können auf Mobilgeräten oder per Mail bereitgestellt werden.

DCS-935L Kamera

Die DCS-935L Kamera ist eine smarte Kamera, die hochauflösende Videos aufnimmt und über eine Nachtsichtfunktion sowie Geräusch- und Bewegungs-Sensorik verfügt. Meldungen können auf Mobilgeräten oder per Mail bereitgestellt werden. Über den Cloud-Service mydlink lassen sich die Bilder im Webbrowser oder auf dem Mobilgerät kostenlos einsehen.

DCS-2132L Kamera

Die DCS-2132L Kamera ermöglicht eine direkte Übertragung von Videobildern und verfügt über ein Mikrofon sowie Lautsprecher. Sie hostet ihren eigenen Webserver und besitzt eine eingebaute CPU. So können die Aufnahmen von jedem Webbrowser aus via Internet abgerufen werden.

Bei mydlink handelt es sich um den Cloud-Dienst von D-Link, über den sich alle kompatiblen Geräte zentral konfigurieren, steuern und überwachen lassen. Per App oder Webbrowser kann man auf den Dienst zugreifen.

Datenschutzrichtlinie

https://www.mydlink.com/privacyPolicy?lang=de

Alle mydlink Produkte sammeln manche oder alle der folgenden Daten:

> Sprache
> Geräusche
> Gesichter
> Temperatur
> Umgebungslicht
> Feuchtigkeit und Nässe
> CO2-Gehalt
> Niederschlag
> Geräuschpegel
> Bewegung der Produktsensoren
> Nutzungsdaten von Programmen
> App-Einstellungen
> Zeitplanung
> Warnmeldungen
> Benachrichtigungen
> Produktstandort innerhalb der Räumlichkeiten
> SSID (WLAN Name)
> WLAN Kennwort
> Audio- und Videosignale

Mit Amazon Echo kompatibel?

Ja

Sicherheit & Privatsphäre

Sowohl die Kommunikation von Ihrem Smartphone zum mydlink Cloud-Dienst als auch die Verbindungen zwischen D-Link Geräten und Servern sind verschlüsselt.

Allerdings werden Firmware-Updates nicht über https, sondern per http bereitgestellt. Ein Angreifer könnte den Transfer abfangen und das Updatepaket mit Schadcode infizieren. Unsere Versuche, das Update zu manipulieren, um die Kontrolle über die Geräte zu übernehmen oder gewisse Funktionalitäten zu ändern, endeten jedoch damit, dass das Paket nicht installiert wurde. Das spricht dafür, dass es vor der Installation geprüft und damit ein gewisser Schutz gewährleistet wird.

Die untersuchten Kameras haben Schwachstellen, die zum Teil bereits aus anderen Tests bekannt sind. AV-Test hat die DCS-2132L Kamera beispielsweise mit nur einem von fünf möglichen Sternen bewertet und auf einige grobe Sicherheitsprobleme hingewiesen. Bedauerlicherweise bestehen ein Jahr nach dem Test noch immer die gleichen Schwachstellen, z.B. die einfache http-Authentifizierung sowie eine unzureichende und

umkehrbare Verschlüsselung des Video-Streams, der sich über eine öffentliche IP-Adresse abrufen lässt. Zwar ist die Kommunikation zwischen Kamera und mydlink-App verschlüsselt, allerdings hat das für die Sicherheit und Privatsphäre der Anwender nur einen bedingten Nutzen, wenn der Video-Stream selbst unzureichend geschützt ist und abgefangen werden kann. Die Reichweite dieses Problems hängt wohl davon ab, wo die Kamera genutzt wird. Am Strand zur Beobachtung der Wellen ist das keine große Sache, Zuhause im Wohnzimmer schon eher.

Netatmo

Netatmo Wetterstation

Die Netatmo Wetterstation besteht aus einem Außenmodul mit Echtzeit-Zugriff auf die aktuelle Wetterlage und einem Innenmodul, das Informationen über den Zustand im Raum, z.B. zur Luftqualität und -feuchtigkeit, bereitstellt. Nutzer können ihre Daten für andere Anwender freigeben und haben online Zugriff auf die Wetterdaten der Außenmodule aller anderen Netatmo-Stationen.

Nutzungsbedingungen

https://www.netatmo.com/de-DE/terms

Die ausschließlich auf Englisch verfügbaren Nutzungsbedingungen sind nicht so detailliert wie bei anderen Herstellern. Es werden eher generalisierend verschiedene Datenkategorien als konkrete Beispiele an erhobenen Informationen benannt. Für Nutzer ist es deshalb schwierig zu erkennen, welche Daten nun tatsächlich gesammelt, gespeichert und geteilt werden.

Bei Nutzung der Produkte und Dienste werden die folgenden Daten erhoben:

> Persönliche Daten und Messwerte
> Informationen über die Art der Nutzung
> Ihre Aktivitäten mit den Diensten
> IP-Adresse

Netatmo behält sich vor, anonymisierte persönliche Daten an Dritte weiterzugeben.

Mit Amazon Echo kompatibel?

Ja

Sicherheit & Privatsphäre

Netatmo stellt eine Wetterkarte bereit, auf der man die Daten aller Stationen einsehen kann. Entscheiden Sie sich für die Teilnahme, werden die Daten Ihres Außenmoduls ***auf der Karte angezeigt*** – die Daten Ihres Innenmoduls bleiben privat. Nehmen Sie nicht an der Wetterkarte teil, ist Ihr Gerät nur für Sie sichtbar.

Bevor Sie sich für eine Freigabe Ihrer Daten entscheiden, sollten Sie sich bewusst machen, dass der Standort Ihres Geräts ziemlich genau angegeben wird. In den Details auf der rechten Seite wird der Straßenname benannt und wenn man in die Karte reinzoomt, erkennt man irgendwann auch die Hausnummer.

Ist die Preisgabe der Adresse ein Sicherheitsrisiko? Ja. Denken Sie nur an den sogenannten Support-Betrug, bei dem sich Kriminelle am Telefon als Microsoft-Mitarbeiter ausgeben und behaupten, dass der Computer eines Nutzers mit Malware befallen sei. Ziel ist oftmals die Installation einer Schadsoftware, über die die Betrüger auf das Gerät zugreifen und Daten

stehlen können. Nun stellen Sie sich vor, Kriminelle hätten die Möglichkeit, mit ziemlich großer Wahrscheinlich Besitzer von Wetterstationen ausfindig zu machen. Vermutlich würden sich viele Nutzer von einem Anruf eines vermeintlichen Netatmo-Mitarbeiters täuschen lassen.

2015 wurde das Problem bekannt, dass die WLAN-Zugangsdaten im Klartext kommuniziert wurden. Netatmo hat die Sicherheitslücke mit einem Firmware-Update behoben. Einmal verbunden, lädt das Gerät automatisch die neueste Version aus der Cloud herunter. Der Transfer findet zwar nicht über SSL statt, wird aber mit einer proprietären Verschlüsselung geschützt, was immerhin sicherer ist als gar keine Verschlüsselung zu nutzen.

Nokia Health

Geräte

Nokia Health Body+ Körperwaage

Nokia Health Body+ ist eine Körperwaage, die neben Gewicht und BMI den prozentualen Körperfett- und Wasseranteil sowie Muskel- und Knochenmasse angibt. Über die Health Mate App können Nutzer ihre Gewichtsentwicklung verfolgen und erhalten Ratschläge zur Erreichung ihrer persönlichen Ziele.

Nokia Health Body Cardio Körperwaage

Über die Funktionen von Nokia Health Body+ hinaus bietet die Body Cardio Variante die Möglichkeit, durch Nachverfolgen der Herzfrequenz die Herz-Kreislauf-Gesundheit zu kontrollieren.

Datenschutzerklärung

https://health.nokia.com/de/de/legal/privacy-policy

Bei Nutzung der Nokia Health Produkte und Dienste werden laut Datenschutzerklärung unter Umständen die folgenden Daten erhoben:

Identitätsdaten

> IP-Adresse
> Videos und Bilder von Ihnen

Aktivitätsdaten

> Anzahl Ihrer Schritte
> Zurückgelegte Entfernungen
> Anzahl von Schwimmzügen
> Menge an verbrannten Kalorien
> Aktivitätstyp
> Aktivitätsniveau
> Uhrzeit der sportlichen Betätigung

Daten zu Körpermessgrößen

> Ihr Gewicht
> Muskelanteil
> Fettanteil
> Herzfrequenz
> Atemfrequenz
> Blutdruck

Umgebungsdaten

> Geräuschpegel
> Lichtstärke
> Temperaturniveau
> CO2-Konzentration

Standortdaten

Mit Amazon Echo kompatibel?

Ja

Sicherheit & Privatsphäre

Vor allem bei Gesundheitsdaten sollte die Privatsphäre eine zentrale Rolle spielen. In der globalen Datenschutzerklärung heißt es sinngemäß:

Manche Dienste ermöglichen das Teilen persönlicher Daten mit anderen Nutzern des Dienstes oder mit anderen Diensten und deren Nutzern. Bitte überlegen Sie vorsichtig, bevor Sie persönliche Daten oder andere Informationen für andere Nutzer verfügbar machen.

Bei so persönlichen Daten scheint eine Preisgabe eher unangemessen. Allerdings ist es vorstellbar, dass sich jemand mit dem Wunsch nach Gewichtsverlust davon motivieren lässt, Informationen über erreichte Ziele mit anderen zu teilen. Man sollte sich aber bewusst sein, dass man durch die Veröffentlichung der Daten die Kontrolle über ihre Verbreitung verliert.

Das Urteil unseres Research Teams lautet, dass die Geräte relativ gut gesichert sind. Im Zuge der Prüfung haben wir versucht, die Kommunikation zwischen sowohl der Waage als auch der Health Mate App und dem Cloud-Dienst abzufangen, um an die Daten zu gelangen.

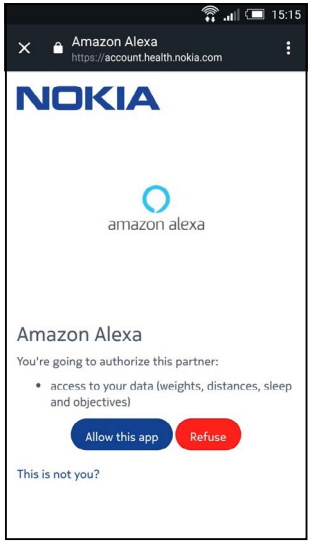
Zwar konnten wir einen Man-in-the-Middle (MitM) Angriff zwischen App und Cloud durchführen, allerdings mussten wir dafür das Android-Gerät rooten und ein MitM Root-Zertifikat installieren. Da die Waage mit dem Android-Gerät kommuniziert und Firmware-Updates über die App bereitgestellt werden, konnten wir die Updates mit der MitM-Attacke abfangen. Der Download ist mit SSL verschlüsselt und wird direkt vom Android-Gerät auf die Waage übertragen. Wir konnten Änderungen an der Firmware vornehmen und über die Bluetooth-Verbindung auf der Waage anwenden. Allerdings mussten wir dazu den Setup-Knopf auf der Waage drücken. Ein Angriff aus der Ferne war also nicht möglich, der physische Zugriff war notwendige Voraussetzung.

Insgesamt ist es ziemlich unwahrscheinlich, dass ein Angreifer Zugriff auf das Smartphone erlangt, es rootet, anschließend den Firmware-Download abfängt und modifiziert, um schließlich den Setup-Knopf auf der Waage zu drücken und die neue Firmware zu installieren. Und selbst dann wären die abgefangenen Daten ohne weiteres Reverse Engineering belanglos.

Ein merkwürdiges Feature der Waage ist die Möglichkeit zur Anzeige des Wetterberichts. Über das Smartphone wird Ihr Standort bereitgestellt, sodass Ihnen beim Wiegen gleichzeitig auch die örtliche Wettervorhersage angezeigt wird. Ob das ein Risiko für Ihre Sicherheit und Privatsphäre darstellt, bleibt abzuwarten. Aber man kann hinterfragen, ob es notwendig ist, dass die Waage Ihren Standort kennt.

Die größten Risiken bestehen darin, dass Nutzer von sich aus zu viele Informationen preisgeben oder aber Drittanbieter Zugriff auf diese sensiblen Daten erhalten – und damit ist insbesondere Amazon Echo gemeint. Sind die Nokia Waagen mit Amazon Echo verbunden, können Sie Alexa nach Daten aus Ihrer Health Mate App fragen. Auf der englischen Seite zu den Alexa Skills steht bei der Nokia Health Mate App sinngemäß die ***folgende Meldung***:

Hinweis: Ihre Nokia Health Daten werden von Alexa und Amazon, Inc. nicht erhoben oder gespeichert, allerdings enthalten die in Ihrem Amazon Account erfassten Sprachinteraktionen unter Umständen Nokia Health Daten.



Erlauben Sie Alexa bzw. Amazon, auf Ihren Nokia Health Mate Account zuzugreifen, erhalten Sie die oben angezeigte Mitteilung. Sie werden darauf hingewiesen, dass Alexa Zugriff auf persönliche Daten erhält, einschließlich Gewicht, Entfernung, Schlaf und Ziele.

Wie Sie dem Hinweis von Amazon bezüglich der Nokia Health Daten bereits entnehmen konnten, werden die Informationen ausschließlich in Form von Aufzeichnungen der Sprachinteraktionen in Ihrem Amazon Account gespeichert. Wie wir weiter oben bereits geschrieben haben, haben Sie jederzeit die Kontrolle und können diese Interaktionen in Ihrer Alexa App prüfen, abhören und löschen.

Das Problem hierbei besteht darin, dass viele Nutzer vermutlich gar nicht wissen, dass die Sprachinteraktionen gespeichert werden. Und falls doch, ist das regelmäßige Löschen für die meisten vermutlich zu aufwendig und eine häufig aufgeschobene Aufgabe.

Sonos

Sonos PLAY: 1 WLAN-Speaker

Sonos PLAY:1 ist ein WLAN-Lautsprecher, der ohne Bluetooth-Verbindung zu Ihrem Mobilgerät, also völlig unabhängig, Musik abspielen kann. Über Amazon Echo lassen sich Lieder, Playlisten und Radiosender per Sprachbefehl abspielen. Mehrere Lautsprecher in unterschiedlichen Räumen können synchronisiert werden und den gleichen Song abspielen oder unabhängig voneinander Musik streamen.

Datenschutzerklärung

https://www.sonos.com/de-de/legal/privacy

Laut Erklärung sammelt Sonos unter Umständen die folgenden Daten:

Produkttyp
Typ des Controller-Geräts
Betriebssystem des Controllers
Informationen zur Software-Version
Eingangsquelle (Line-in-Audioeingang)
Signaleingang (z.B. Dolby)
Informationen zu WLAN-Antennen
Audioeinstellungen
Produktausrichtung
Raumnamen, die Sie Ihrem Sonos Produkt gegeben haben
Mithilfe der Sonos Trueplay Technologie vorgenommene Anpassungen
Temperatur Ihres Produkts
WLAN-Informationen (z.B. Signalstärke)
Musikdienste, die mit Ihrem Sonos System verbunden sind (bei einigen Diensten einschließlich des Benutzernamens – aber nicht des Passworts)
Wie häufig Sie die Sonos App im Vergleich zu einem anderen Controller nutzen
Interaktionen innerhalb der Sonos App
Wie häufig Sie die Controller des Geräts verwenden
Standortdaten, wenn die Sonos App in Gebrauch ist
Wie lange das Sonos Produkt eingesetzt wird
Einsatzdauer von Musikdiensten
Informationen zur Produkt- oder Raumgruppierung
Steuerungsinformationen wie Wiedergabe, Pause, Lautstärkeregelung oder das Überspringen von Tracks
Informationen über Tracks, Playlisten oder Radiosenderdaten und zur Sonos Playlist oder Sonos Favoriten

Mit Amazon Echo kompatibel?

Ja

Sicherheit & Privatsphäre

Da der Lautsprecher nicht über Bluetooth, sondern via WLAN funktioniert, ist kein Koppelgerät wie ein Smartphone notwendig, das sich stets in einem gewissen Abstand zum Speaker befindet. So funktionieren auch die Audiofunktionen des Smartphones unabhängig.

Die mit dem Gerät verbundene Sonos (oder jede andere?) App übermittelt die netzwerkweite Anfrage, Audio abzuspielen. Da sich der Lautsprecher im permanenten Zuhörmodus befindet, wird er diese Anfrage erhalten und die geforderte Musik abspielen.

Zur Nutzung der App ist ein Sonos Account notwendig. Der Lautsprecher verbindet sich regelmäßig mit den Sonos Servern. Dabei gibt es zwei Verbindungen, von denen die eine permanent ist und die andere stündlich aufgebaut wird. Beide werden über eine Verschlüsselung geschützt. Die permanente Verbindung wird benötigt, damit Sprachbefehle an Amazon Alexa zum Abspielen von Liedern über den Sonos Speaker ausgeführt werden können.

In der Datenschutzerklärung von Sonos steht, dass Interaktionen mit der App und verbundenen Musikdiensten erfasst werden. Das ist wenig verwunderlich, da nahezu alle Dienste über eine Funktion zur Song-Empfehlung verfügen.

Weiter heißt es, dass die Raumnamen gespeichert werden, die Sie den verschiedenen Lautsprechern zuweisen. Das macht Sinn, da Sie nur so bestimmen können, von welchem Gerät ein bestimmter Song abgespielt werden soll. Achten Sie jedoch darauf, dass Sie über die Raumnamen nicht zu viel über sich preisgeben. Die Benennung eines Lautsprechers im Kinderzimmer nach dem Namen Ihres Kindes könnte beispielsweise im Fall von unerlaubten Zugriffen dazu führen, dass Fremde wertvolle Informationen über Ihre Familie erhalten.

Es gibt eine neue Version des Speakers – Sonos One. Hierbei handelt es sich nicht mehr nur um einen Lautsprecher, sondern auch um eine Steuereinheit, die Amazon Echo ersetzen soll. In diesem Fall wäre in Bezug auf die Datenschutzerklärung klar, dass zu den erhobenen Daten keine Interaktionen mit Alexa gehören.

Wörlein

Soundmaster Internet Radio IR4000SW

Mit dem Soundmaster Internet Radio IR4000SW können Nutzer via WLAN aus einer Vielzahl an Radiosendern auswählen, sortiert nach Genres, Ländern und Popularität. Zudem lässt sich über den PC eine Favoritenliste erstellen.

Datenschutzerklärung

Wir konnten keine Datenschutzerklärung zu den Produkten finden. Es gibt ausschließlich eine ***Erklärung*** für die Besucher der Unternehmenswebseite. Die Webseite ist zwar auf Englisch verfügbar, sodass auch englisch-sprachige Nutzer die Produkte kaufen können, allerdings existiert die Datenschutzerklärung nur auf Deutsch.

Mit Amazon Echo kompatibel?

Nein

Sicherheit & Privatsphäre

Ohne Datenschutzerklärung können wir uns ausschließlich auf die Erkenntnisse aus unserer Untersuchung beziehen. Bei der Einrichtung der Internetverbindung auf dem Gerät wird das WLAN-Passwort nach Eingabe im Klartext angezeigt. Ihnen sollte also kein Fremder bei der Konfiguration des Radios zuschauen. Wird das Gerät an einem öffentlichen Platz eingesetzt, z.B. im Büro oder in einem Laden, kann man sich die WLAN-Zugangsdaten einfach über die Einstellungen anzeigen lassen. Mit dem Prinzip von Security by Design hat das leider nicht allzu viel zu tun.

Bei der Auswahl eines Radiosenders wird in Klartext eine Anfrage an mediayou.net gesendet. Hierbei handelt es sich offenbar um ein Portal,

über das man auf verschiedene Internetradios zugreifen kann. Mediayou erkennt die IP-Adresse des verbundenen Geräts, den angefragten Radiosender sowie den Beginn und die Länge der Radionutzung.

Auf Mediayou lässt sich keine Datenschutzerklärung finden. Selbst wenn Sie einen Account erstellen, erhalten Sie weder eine Datenschutzerklärung noch sonstige Nutzungsbedingungen. Recherchen darüber, wem die Domain gehört, waren vergeblich. Die Domain-Details waren ironischerweise gut geschützt.

Wenn man nicht genau weiß, welche Daten erhoben und gespeichert werden, muss man vom Schlimmsten ausgehen – dass das Unternehmen alles Mögliche sammelt und an Dritte verkauft. In Zeiten, in denen Daten ein wertvolles Gut sind und Identitätsdiebstahl zu einem zunehmenden Problem wird, kann man das nicht akzeptieren.

TP-Link

TP-Link WLAN-Steckdose HS110

Mit der TP-Link WLAN-Steckdose lässt sich die Stromverbindung von nicht-smarten Geräten über das Smartphone steuern. So können Sie kosteneffizient ein Smart Home schaffen und beispielsweise das Licht oder Ihren Wasserkocher ferngesteuert an- und ausschalten, ohne dass Sie ein neues intelligentes Gerät kaufen müssen.

Datenschutzerklärung

Für die Nutzung der TP-Link Produkte steht ausschließlich eine ***englische Erklärung*** bereit. Hier werden die folgenden Daten genannt:

Firmware-Versionen
IP-Adresse
MAC-Adresse
Andere identifizierende Informationen wie Namen und Bilder, die Sie Account-Nutzern zuordnen
Ihr Standort
Geräte
Details zu Geräteeinstellungen
Demografische Informationen
Details zu Drittanbieter-Accounts
Zeitpläne
Audio-/Video-Aufnahmen
Nutzung von Drittanbieter-Geräten, z.B. wenn ein Bewegungssensor eine Bewegung meldet
Art des Geräts oder Dienstes, von dem Informationen empfangen werden
Vom Nutzer erstellte Geräte-, Gruppen- und Standortnamen
Informationen über Mobilgerät

Mit Amazon Echo kompatibel?

Ja

Sicherheit & Privatsphäre

Bei der Auswahl der Geräte für unser Smart Home haben wir auf Preis, Verfügbarkeit und Popularität geachtet. Ein an sich nicht smartes Gerät zu nutzen und über die Stromquelle zu steuern, ist sowohl kostengünstig als auch bequem. Stellen Sie sich beispielsweise vor, Sie nutzen eine intelligente Steckdose für Ihren Wasserkocher, schalten diesen abends an und aktivieren am nächsten Morgen die Steckdose über Ihr Smartphone oder per Sprachbefehl.

Das Gerät hat allerdings einige Schwachstellen, die gut dokumentiert sind. Dazu gehören eine leicht umkehrbare Verschlüsselung der Kommunikation zwischen Steckdose und TP-Link Kasa App, die für die Steuerung genutzt wird, sowie Probleme bei der Zertifikatsvalidierung und potenzielle Man-in-the-Middle Angriffe.

Darüber hinaus war TP-Link von der WPA2-Sicherheitslücke namens KRACK betroffen, die im Oktober 2017 von zwei Researchern veröffentlicht wurde. In einer ***Stellungnahme*** des Unternehmens von Januar 2018 heißt es, dass das Problem für HS110 behoben wurde und Anwender, die die aktuelle Firmware nutzen, die über die Kasa App bereitgestellt wird, geschützt sind.

Insbesondere bei Anbietern und Produkten, über die bereits mehrere Sicherheitsprobleme veröffentlicht wurden, sollten Anwender vorsichtig sein. Auf den ersten Blick ist die kostengünstige Möglichkeit, nicht-vernetzte Geräte über eine intelligente Steckdose ins Smart Home zu integrieren, sehr verlockend. In diesem Fall leidet aber unter Umständen Ihre Sicherheit und Privatsphäre.

7. FAZIT – GIBT'S DAS AUCH IN SICHER?

Ist es möglich, ein sicheres Smart Home zu schaffen? Unter Umständen.

Ziel dieses Projekts war die Nachstellung eines Smart Homes, wie es heute in einem klassischen Haushalt umgesetzt werden könnte. Im Vorfeld haben wir uns gefragt, welche Konsequenzen es hätte, wenn wir keine Probleme fänden. Das wäre ein enormer Sprung in der Entwicklung des Internets der Dinge gewesen. Allen, die an der Schaffung eines Smart Homes interessiert sind, hätten wir sagen können: „Los geht's!" Leider ist es anders gekommen, wobei das Fazit nicht ganz dem entspricht, was wir erwartet hätten.

Absolute Sicherheit gibt es nicht und so hat auch jedes Gerät und jede Software potenzielle Schwachstellen. Wir können Unternehmen allerdings danach bewerten, wie sie auf die Offenlegung von Sicherheitsproblemen reagieren – ob sie schnell Updates veröffentlichen oder aber erst spät neue Firm- bzw. Software bereitstellen. Natürlich sollten sich Nutzer in jedem Fall für Hersteller entscheiden, die verantwortungsvoll mit Schwachstellen umgehen. Mit gesundem Menschenverstand und einer kleinen Portion Vorsicht ist es durchaus möglich, ein sicheres Smart Home einzurichten. Wenn Sie das Projekt angehen und die verschiedenen Komponenten auswählen, sollten Sie die folgenden Hinweise berücksichtigen.

- *Informieren Sie sich darüber, ob es bekannte Sicherheitslücken für die Geräte bzw. Dienste gibt, für die Sie sich interessieren. Eine schnelle Suche über Google mit den folgenden Suchbegriffen kann Aufschluss geben:*

[Gerätename] Sicherheitslücke
[Hersteller + Gerätename] Sicherheitsproblem
[Hersteller + Gerätename] Datenschutz Problem

- *Informieren Sie sich über die Herstellerwebseite oder Google, wie Updates der Firmware bereitstellt werden: Werden sie automatisch eingespielt oder erhalten Sie zumindest per App oder Mail eine Meldung über verfügbare neue Versionen?*
- *Lesen Sie die Datenschutzerklärung. Nur wenn Sie wissen, welche Daten erhoben, gespeichert und geteilt werden, können Sie entscheiden, ob ein Gerät ans gesamte Netzwerk angeschlossen oder doch lieber isoliert werden sollte. Erscheint beides unsicher, verzichten Sie am besten ganz auf das Gerät.*
- *Beim Teilen von Daten in sozialen Netzwerken oder den Systemen des Anbieters ist Vorsicht geboten. Informationen über Ihren Standort, das Gerät und Nutzungsmuster helfen Cyberkriminellen dabei, Betrüge oder zielgerichtete Angriffe durchzuführen.*
- *Sprachgesteuerte intelligente Assistenten sind nützlich – aber auch allwissend. Überlegen Sie, wieviel Sie Ihrem Helfer erzählen bzw. wie viele Daten über Ihre Anfragen gesammelt werden.*

Jeder Nutzer hat eine andere Meinung darüber, welche Informationen mit anderen geteilt werden können und welche nicht. Man sollte sich jedoch bewusst machen, dass es nicht immer nur um die Bewertung einzelner Daten geht, sondern um die Vielzahl der erhobenen und miteinander verknüpften Informationen. Welche Konsequenzen hat es, wenn ein Unternehmen umfassende Kenntnis über Lebensstil, Gesundheit und Interessen hat? Überlassen Nutzer die Verantwortung im Umgang mit ihren Daten ausschließlich den Unternehmen, müssen sie auf eine Selbstregulierung der Branche hoffen oder aber auf den Gesetzgeber, der über Regelungen wie der neuen ***Datenschutzgrundverordnung*** einen rechtlichen Rahmen vorgibt.

Februar 2018

ENJOY SAFER TECHNOLOGY™

ESET, spol. s r.o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
Slovak Republic