Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Das Internet der Dinge (IoT)
- Probleme mit dem IoT
- Schützen Sie Ihre IoT Geräte

Internet der Dinge (IoT)

Was ist das Internet der Dinge (IoT)

In der Vergangenheit war Technik relativ einfach, man hat seinen Computer ans Internet angeschlossen und ihn für seine täglichen Aktivitäten genutzt. Dann hat sich die Technik weiterentwickelt, mobile Endgeräte wie Smartphones und Tablets haben unser Leben bereichert. Mit diesen Geräten haben Sie die Rechenkraft eines Computers in Ihrer Hosentasche. Durch ihre hohe Mobilität stellen diese mobilen Endgeräte aber auch andere Herausforderungen an die Sicherheit. Den nächsten Schritt der technischen Weiterentwicklung stellt das Internet der Dinge (engl. Internet of Things, Kurzform IoT) dar. IoT beschreibt das Verbinden von Alltagsgeräten mit dem Internet. Dies reicht von Türklingeln und Glühbirnen bis zu Spielzeugpuppen und Thermostaten. Diese, mit dem Internet verbundenen, Geräte machen unser Leben um einiges einfacher. Zum Beispiel schaltet sich das Licht in Ihrer Wohnung automatisch ein, sobald Ihr Smartphone erkennt, das Sie sich in der Nähe Ihrer Wohnung befinden. Der IoT Markt entwickelt sich mit einer rasanten Geschwindigkeit und neue Geräte schießen wie Pilze aus dem Boden. Wie auch mobile Endgeräte, stellen IoT Geräte spezielle Anforderungen an die Sicherheit. In diesem Newsletter werden wir auf die Risiken eingehen und aufzeigen, wie Sie Ihre IoT Geräte, Ihr Heim und schlussendlich Ihre Familie absichern können.

Gastautor

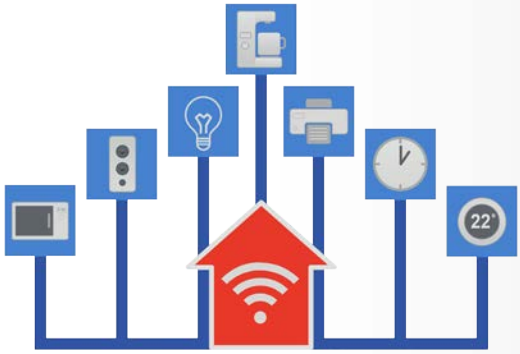
James Lyne (**@jameslyne**) ist der globale Leiter der IT-Sicherheitsforschung der Firma Sophos. Als selbsternannter „gewaltiger Computerfreak“, erstreckt sich seine technische Kompetenz über eine Vielzahl von Sicherheitsthemen. Er ist zertifizierter Trainer beim SANS Institute und oft Hauptredner bei Konferenzen.

Probleme mit dem IoT

Die Macht des IoT liegt in der Schlichtheit der Geräte. Sie verbinden beispielsweise Ihre Kaffeemaschine mit der Steckdose und schon fragt sie nach einer Verbindung mit Ihrem drahtlosen Heimnetzwerk. Jedoch birgt diese Einfachheit Risiken. Das größte Problem besteht darin, dass die Hersteller solcher Geräte keine Erfahrung im Bereich IT Sicherheit haben, ihre Expertise besteht darin, Haushaltsgegenstände zu produzieren. Oder es handelt sich um Startup Unternehmen, welche ein Produkt so schnell und effizient wie möglich entwickeln und an den Markt bringen wollen, wie es z.B. auf Plattformen wie Kickstarter meist der Fall ist. Diese Firmen konzentrieren sich auf Profit und nicht auf IT Sicherheit. Das Resultat ist der Verkauf von Geräten die mit wenig bis gar keinen Sicherheitsfeatures ausgestattet sind. So kann es sein, dass diese Geräte mit einem nicht veränderbaren Standardpasswort versehen sind, welches vielen bekannt und eventuell bereits im Internet nachlesbar ist. Erschwerend kommt hinzu, das viele der Geräte keine Option oder Möglichkeit der Konfiguration

Internet der Dinge (IoT)

anbieten. Sie müssen also mit dem Auslieferungszustand leben. Um es noch schlimmer zu machen, ist es schwierig diese Geräte zu aktualisieren bzw. fehlt einigen sogar die Möglichkeit dies zu tun. Viele der von Ihnen genutzten IoT Geräte können schnell überholt sein, besitzen aber Schwachstellen die dann nicht mehr behoben werden und sind somit auf Dauer verwundbar.



The Internet of Things

Behalten Sie den Überblick über die IoT Geräte in Ihrem Netzwerk, isolieren Sie diese soweit möglich, halten Sie sie auf dem aktuellsten Stand und schützen Sie sie mit einem starken Passwort.

So schützen Sie Ihre IoT Geräte

Was können Sie tun? Wir wollen auf jeden Fall, dass Sie die Vorteile von IoT Geräten sicher und effizient nutzen können. Diese Geräte bringen wundervolle Funktionen mit sich, die Ihr Leben erleichtern, Ihnen Geld sparen und eventuell die physische Sicherheit Ihres Heims erhöhen. Im Zuge des rasanten Wachstums der IoT Technologie werden Sie wahrscheinlich nicht daran vorbei kommen, IoT Geräte zu kaufen bzw. zu nutzen. Nachfolgend wollen wir Ihnen einige Punkte näher bringen, die Ihnen helfen Ihre IoT Geräte und sich selbst zu schützen.

- **Verbinden Sie nur Geräte, die Sie auch wirklich nutzen**: Am einfachsten schützen Sie Ihr IoT Gerät, in dem Sie es nicht an das Internet anschließen. Wenn Ihr Gerät keine Onlineverbindung benötigt, dann verbinden Sie es auch nicht mit Ihrem drahtlosen Netzwerk.
- **Separieren Sie Ihr drahtloses Netzwerk**: Wenn Ihr IoT Gerät mit dem Netzwerk verbunden sein muss, dann denken Sie darüber nach ein separates Netzwerk nur für diese Geräte zu erstellen. Viele drahtlose Zugangspunkte erlauben das Erstellen von zusätzlichen Netzwerken, wie z.B. einem Gastnetzwerk. Eine weitere Möglichkeit ist der Erwerb eines zusätzlichen drahtlosen Zugangspunkts, welcher nur für IoT Geräte zugänglich ist. Somit betreiben Sie diese Geräte in einem isolierten Bereich, aus dem sie keine Bedrohung für Ihr zentrales Heimnetzwerk darstellen (welches das Hauptziel für Cyberkriminelle ist), in dem sich Ihr Computer oder Ihre mobilen Endgeräte befinden.
- **Aktualisieren Sie, wenn möglich**: Genau wie Ihren Computer und Ihre mobilen Endgeräte sollten Sie auch Ihre IoT Geräte auf dem aktuellsten Stand halten. Wenn diese Geräte eine Option haben sich automatisch zu aktualisieren, dann aktivieren Sie diese.
- **Starke Passwörter**: Ändern Sie jedes Passwort auf Ihren IoT Geräten in ein einzigartiges und starkes Passwort, das nur Sie kennen. Machen Sie sich keine Gedanken, wenn Sie sich all die Passwörter nicht merken können, wir können es auch nicht. Überlegen Sie sich einen Passwort Manager zu benutzen, in dem Sie all Ihre Passwörter sicher ablegen können.

Internet der Dinge (IoT)

- **Privatsphäre Einstellungen**: Wenn Ihre IoT Geräte es ermöglichen, Einstellungen zur Privatsphäre zu konfigurieren, dann limitieren Sie die Menge an Information die sie bereitstellen. Eine Möglichkeit wäre, alle Optionen zur Informationsweitergabe zu deaktivieren.
- **Erwägen Sie einen Austausch**: Es wird der Zeitpunkt kommen, an dem Sie Ihre IoT Geräte ersetzen müssen, da sie Schwachstellen besitzen die nicht mehr behoben werden oder neuere Geräte auf dem Markt sind, die viel mehr Sicherheit eingebaut haben.

Es gibt keine Patentlösung die für alle Geräte zutrifft, daher lohnt es sich nach dem optimalen Weg und nach Veröffentlichungen zur Absicherung von IoT Geräten zu suchen. Leider wird der Punkt IT Sicherheit bei der Entwicklung der meisten IoT Geräte vernachlässigt, was dazu führt, dass viele Hersteller keine Informationen zur IT Sicherheit Ihrer Geräte bereitstellen. Das Bewusstsein im Bereich IT Sicherheit wächst jedoch und somit auch unsere Hoffnung, dass die Zahl der Hersteller, welche IT Sicherheit in ihre IoT Geräte einbauen, steigt, und sie auch mehr Informationen zur Verfügung stellen, wie diese Geräte geschützt und aktualisiert werden können.

Weiterführende Informationen

Starke Passwörter:	https://securingthehuman.sans.org/ouch/2015#april2015
Passwort-Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Absicherung Ihres neuen Tablets:	https://securingthehuman.sans.org/ouch/2016#january2016
Absicherung Ihres Heimnetzwerks:	https://securingthehuman.sans.org/ouch/2016#february2016

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley