OUCH! | August 2018

OUCH!

SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Jedermann

Smart Home Geräte

Was sind Smart Home Geräte?

Traditionell konnten sich nur wenige Ihrer Geräte zu Hause mit dem Internet verbinden, wie z.B. Ihr Laptop, Ihr Smartphone oder Ihre Spielekonsole. Doch heute verbinden sich immer mehr Geräte mit dem Internet, von Glühbirnen und Lautsprechern bis zu Ihrem Fernseher, Schlössern an Ihrer Tür oder sogar Ihrem Auto. Bald könnte fast jedes Gerät in Ihrem Haus mit dem Internet verbunden sein. Diese angeschlossenen Geräte heißen oft Internet of Things (IoT, "Internet der Dinge") oder Smart Home Geräte. Sie bringen zwar viel Komfort, aber auch ihre eigenen Gefahren mit sich.

Worin besteht das Problem?

Je mehr Geräte mit dem Heimnetzwerk verbunden sind, desto mehr kann schief gehen. Hacker können Ihre Geräte so programmieren, dass sie andere angreifen, Anbieter können umfangreiche Informationen über Ihre Aktivitäten sammeln, oder Ihre Geräte könnten infiziert werden und Sie aussperren. Viele der Unternehmen, die diese Geräte herstellen, haben keine Erfahrung mit Cybersicherheit und sehen Sicherheit als Kostenfaktor an. Daher haben viele der von Ihnen erworbenen Geräte wenig oder gar keine Sicherheit eingebaut. Beispielsweise haben einige Geräte Standardkennwörter, die allgemein bekannt sind, oder Sie können sie nicht aktualisieren oder konfigurieren.

Wie kann man sich schützen?

Was können Sie also tun? Wir möchten auf jeden Fall, dass Sie die angeschlossenen Geräte sicher und zuverlässig nutzen können. Diese Geräte können wunderbare Funktionen bieten, die Ihr Leben einfacher machen. Darüber hinaus bleibt Ihnen angesichts der Entwicklung der Technik möglicherweise keine andere Wahl, als intelligente Geräte zu verwenden. Hier sind die wichtigsten Schritte, die Sie unternehmen können, um sich zu schützen.

Schließen Sie nur das an, was Sie benötigen: Der einfachste Weg, ein Gerät zu sichern, ist, es nicht mit dem Internet zu verbinden. Wenn Ihr Gerät nicht online sein muss, verbinden Sie es nicht mit Ihrem WLAN-Netzwerk. Muss Ihnen der Toaster wirklich Benachrichtigungen auf Ihr Handy senden?

Behalten Sie den Überblick: Welche Geräte haben Sie mit Ihrem Heimnetzwerk verbunden? Sie sind sich nicht sicher oder können sich nicht erinnern? Schalten Sie Ihr drahtloses Netzwerk aus und beobachten Sie, was nicht mehr funktioniert. Das ist keine hundertprozentige Methode, aber Sie werden überrascht sein, wie viele Geräte Sie vergessen haben.

Bleiben Sie auf dem Laufenden: Genau wie bei Ihrem Computer und Ihren mobilen Geräten ist es wichtig, auch die anderen im Heimnetz befindlichen Geräte auf dem neuesten Stand zu halten. Wenn Ihr Gerät die Möglichkeit hat, sich automatisch zu aktualisieren, aktivieren Sie diese Option.

Passwörter: Ändern Sie die Passwörter auf Ihren Geräten in eine eindeutige, starke Passphrase, die nur Sie kennen. Sie müssen sie wahrscheinlich nur einmal eingeben. Sie können sich so viele Passphrasen nicht merken? Keine Sorge, wir auch nicht. Verwenden Sie einfach einen Passwortmanager, um sie alle sicher zu speichern.

Datenschutz-Optionen: Wenn Ihr Gerät es Ihnen erlaubt, Datenschutzoptionen zu konfigurieren, begrenzen Sie die Menge der gesammelten oder freigegebenen Informationen. Eine Möglichkeit besteht auch darin, den Informationsaustausch vollständig zu deaktivieren.

Markenhersteller: Kaufen Sie Ihre Geräte von Unternehmen, die Sie kennen und denen Sie vertrauen. Suchen Sie nach Produkten, die die Sicherheit unterstützen, z. B. die automatische Aktualisierungen bieten und die Standardpasswort und Datenschutzeinstellungen ändern lassen.

Immer zuhören: Wenn ein Gerät Ihre Sprachbefehle annehmen kann, hört es ständig zu. Beispielsweise können Ihre Alexa- und Google Home-Geräte sensible Gespräche aufzeichnen. Bedenken Sie das, wenn Sie festlegen, wo Sie die Geräte in Ihrem Haus aufstellen wollen, und prüfen Sie die Datenschutzoptionen.

Gast-Netzwerk. Erwägen Sie, Ihre Smart Home-Geräte in ein separates "Gast"-WLAN-Netzwerk einzubinden und nicht in das primäre WLAN, das Sie für Ihre Computer und Mobilgeräte verwenden. Wenn ein Smart Device infiziert ist, bleiben Ihre Computer oder mobilen Geräte in Ihrem Hauptnetzwerk sicher.

Es gibt keinen Grund, sich vor neuen Technologien zu fürchten, solange Sie die damit einhergehenden Risiken kennen. Mit diesen wenigen einfachen Schritten können Sie dazu beitragen, ein weitaus sichereres Smart Home zu schaffen.

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.

Gast-Autor

Robert M. Lee *(@RobertMLee) ist SANS Certified Instructor und Autor der Kurse FOR578 - Cyber Threat Intelligence und ICS515 - ICS Active Defense and Incident Response. Er ist zudem CEO und Gründer von Dragos, eines auf die Cybersicherheit von Industriesystemen spezialisierten Unternehmens.*

Ressourcen

Passphrasen:	https://www.sans.org/u/GEB
Passwort-Manager:	https://www.sans.org/u/GEG
Absicherung Ihres Heimnetzwerks:	https://www.sans.org/u/GEL

 Redaktionsleitung: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley