وای! | اوت 2018

OUCH!

SANS SECURITY AWARENESS

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

تجهیزات مرتبط با خانه هوشمند

تجهیزات خانه هوشمند چیست؟

بطور سنتی تنها تعداد معدودی از تجهیزات منزل شما نظیر لب تاپ، گوشی هوشمند، یا کنسولهای بازی توانایی اتصال به اینترنت را دارند. اما امروزه، از لامپ روشنایی و اسپیکر و تلوزیون گرفته تا قفل روی در و حتی ماشین هم امکان اتصال به اینترنت را دارند. به زودی، کلیه وسایل موجود در منزل شما خواهند توانست به اینترنت متصل شوند. این تجهیزات را اغلب به اسم اینترنت اشیا(IoT) و یا تجهیزات خانه هوشمند میشناسند. همانطور که این تجهیزات متصل میتوانند راحتی بسیاری را فراهم میکنند، میتوانند مخرب نیز باشند.

مشکل چیست؟

هر چقدر دستگاه های بیشتری به شبکه خانگی متصل باشند، میتوانند عامل بروز مشکلات بیشتر نیز باشند. هکرها میتوانند با برنامه ریزی بعضی تجهیزات به وسایل دیگر حمله کنند، سازندگان میتوانند اطلاعات ارزشمندی از فعالیت های شما بدست بیاوردند، یا دستگاه های شما ممکن است آلوده شده و قفل شوند. بسیاری از شرکت های سازنده این تجهیزات تجربه ای در خصوص امنیت سایبری ندارند و به امنیت از منظر هزینه اضافی نگاه میکنند. در نتیجه، بسیاری از تجهیزاتی که خریداری میکنید یا امنیت ناچیزی دارند و یا اصلا به امنیت آنها فکر نشده است. بعنوان مثال، برخی تجهیزات داری رمزعبور پیش فرضی هستند که شناخته شده بوده و یا شما امکان به روز رسانی و یا پیکربندی آن را ندارید.

چگونه میتوانیم از خودمان محافظت کنیم

سوال این است که چه کاری میتوانیم انجام بدهیم.آنچه ما از شما میخواهیم این است که تجهیزات خود را بصورت امن به شبکه متصل کنید. این تجهیزات میتوانند قابلیت های جالبی را در آسانتر کردن زندگی برای شما فراهم کنند. به عبارت دیگر، با پیشرفت تکنولوژی ممکن است چاره ای جز استفاده از تجهیزات هوشمند وجود نداشته باشد. در ذیل به قدم هایی اشاره میشود که میتواند برای محافظت از شما بکار گرفته شود.

تنها ابزاری را که نیاز دارید متصل کنید: ساده ترین راه برای امن نگه داشتن یک وسیله این است که آن را به اینترنت متصل نکنید. اگر نیازی به آنلاین بودن یک وسیله نیست، آن را به شبکه بی سیم خود متصل نکنید. از خود بپرسید که آیا واقعا توستر شما که برای برشته کردن نان استفاده میشود نیازی به ارسال وضعیت خود به موبایل شما را دارد؟

بدانید چه وسایلی به اینترنت متصل هستند: آیا میدانید چه تجهیزاتی به شبکه خانگی شما متصل هستند؟ مطمئن نیستید و یا به خاطر ندارید؟ شبکه بی سیم خود را خاموش کنید و سپس بررسی کنید که چه وسایلی از کار افتاده اند. با این روش ممکن است همه تجهیزات متصل شده به شبکه را پیدا نکنید ولی متعجب خواهید شد از اینکه چه تعداد وسایل متصل به اینترنت را فراموش کرده بودید.

به روز نگه دارید: همانگونه که کامپیوتر و یا موبایل خود را به روز نگه میدارید، بسیار مهم است که همه تجهیزات قابل اتصال به اینترنت را نیز به روز نگه دارید. اگر تجهیزات شما قابلیت دریافت خودکار به روز رسانی را دارند، آن را فعال کنید.

رمز عبور: برای کلیه تجهیزات خود رمز عبور منحصر بفرد و قوی انتخاب کنید که فقط خودتان میدانید. به احتمال زیاد تنها یک بار نیاز به وارد کردن این رمز عبور خواهید داشت. آیا نمیتوانید رمز عبور همه تجهیزات را بخاطر بسپارید؟ نگران نباشید، ما هم نمیتوانیم. راه حل آن استفاده از نرم افزار های مدیریت رمزعبور است که بتوان بصورت امن آنها را ذخیره نمود.

گزینه های حریم خصوصی: اگر تجهیزات شما امکان پیکربندی گزینه های حریم خصوصی را میدهد، میزان اطلاعاتی را که آن دستگاه جمع آوری و یا به اشتراک میگذارد محدود کنید. یک راه حل غیر فعال کردن همه قابلیت های اشتراک گذاری اطلاعات است.

فروشنده: این تجهیزات را از شرکتی که میشناسید و به آن اعتماد دارید تهیه کنید. تجهیزاتی را انتخاب کنید که گزینه های امنیتی نظیر امکان فعال کردن به روز رسانی اتوماتیک، امکان تغییر رمزعبور و یا امکان تغییر دادن تنظیمات حریم خصوصی را پشتیبانی میکنند.

همیشه گوش دادن: اگر دستگاهی بتواند دستورات را بصورت صوتی دریافت کند پس همیشه به صدا ها گوش میکند. بعنوان مثال تجهیزات خانگی Google و یا Alexa میتوانند مکالمات حساس را گوش کنند. توجه داشته باشید که این تجهیزات را در چه نقطه ای از منزل خود قرار میدهید و حتما گزینه های بخش حریم خصوصی را بررسی کنید.

شبکه مهمان: بهتر است تجهیزات هوشمند خانگی را در یک شبکه مجزای بیسیم که برای مهمان ایجاد کرده اید قرار دهید و آن را از شبکه بی سیم که کامپیوتر و موبایل شما به آن وصل است جدا کنید. به این ترتیب اگر یک دستگاه هوشمند آلوده شود، کامپیوترو یا موبایل شما که در شبکه بی سیم جداگانه ای بودند، امن باقی خواهند ماند.

هیچ دلیلی برای ترس از استفاده از فن آوری های جدید وجود ندارد ولی لازم است خطراتی را که ممکن است ایجاد کنند بشناسید. با بکار بردن این روشهای ساده میتوانید خانه های هوشمند به مراتب امن تری بسازید.

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

سردبیر مهمان

رابرت ام لی(@RobertMLee) مدرس مورد تایید SANS و نویسنده Cyber Threat Intelligense – FOR578 و ICS - ICS515 Active Defense and Incident Response میباشد. رابرت همچنین موسس و مدیر شرکت امنیت سایبری صنعتی Dragos است.

منابع

عبارات عبور: https://www.sans.org/u/GEB

مدیریت رمزعبور: https://www.sans.org/u/GEG

امنیت شبکه های خانگی: https://www.sans.org/u/GEL