ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

اینترنت وسایل (IOT)

اینترنت وسایل (IOT) چیست؟

سردبیر مهمان

جیمز لین (**@jameslyne**) رییس جهانی تحقیقات امنیت در شرکت Sophos است. او خود را علاقمند مفرط و متخصص گستره وسیعی از انواع حوزه های امنیتی میداند. او مدرس مورد تایید موسسه SANS است و اغلب موضوعات اصلی کنفرانس های صنعتی را ارائه می دهد.

در گذشته تکنولوژی نسبتا ساده بود، فقط کامپیوترتان را به اینترنت وصل می کردید و از آن برای فعالیت های روزانه استفاده می کردید. بعد ها تکنولوژی با ورود دستگاههای موبایل به زندگی ما مثل تلفن های هوشمند و تبلت ها پیشرفت کرد. این دستگاهها اکنون قدرت کامپیوترهای دسکتاپ را در جیب شما قرار می دهند. در حالیکه این دستگاههای موبایل قابلیت جابجایی بسیار بیشتری دارند، مشکلات امنیتی خاص خودشان هم دارند.

اکنون پیشرفت بزرگ بعدی اینترنت وسایل است. اینترنت وسایل یا بطور خلاصه IOT , تماما در مورد اتصال دستگاههای هر روزه به اینترنت است. دستگاههایی از زنگ های در و لامپ ها گرفته تا عروسکها و ترموستات ها. اینگونه دستگاههای متصل بهم زندگی ما را بسیار ساده تر خواهند کرد- برای مثال، هنگامی که تلفن شما تشخیص می دهد به خانه نزدیك شده اید لامپ منزل بطور خودکار روشن می شود. بازار IOT با وسایلی که بطور هفتگی ظاهر می شوند با سرعت شگفت انگیزی در حال رشد است. اما دستگاههای IOT هم مثل دستگاههای موبایل با مشکلات امنیتی خاص شان می آیند. در این شماره ما کمك می کنیم که ریسك را بشناسید و کارهایی که می توانید انجام دهید تا دستگاههای IOT تان و در نهایت خانواده تان امن باشند.

مسائل IOT

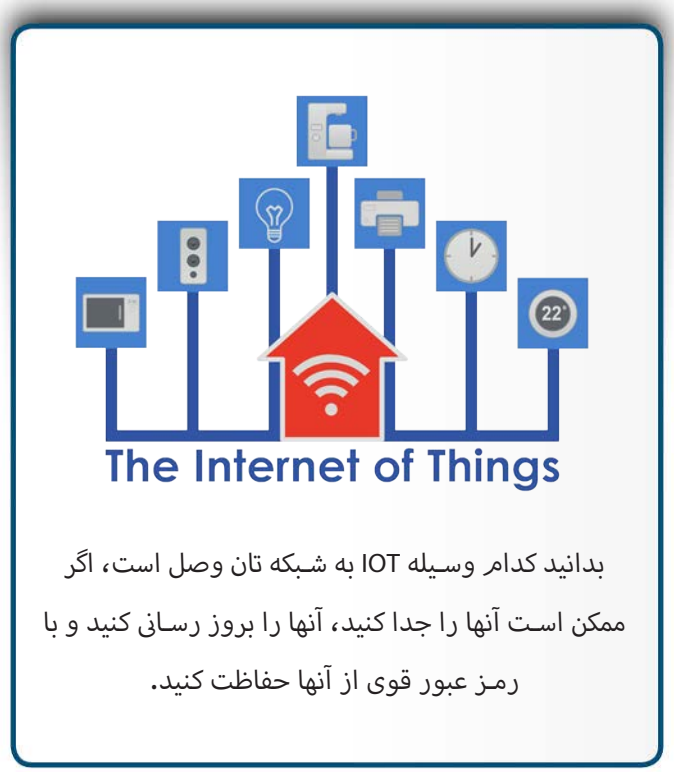
نقطه قوت IOT اینست که بیشتر این دستگاهها ساده هستند. مثلا به سادگی ماشین قهوه تان را به برق می زنید و دستگاه از شما می پرسد که آیا به شبکه اینترنت بی سیم خانگی وصل شود. اما اینهمه سادگی هزینه دارد. بزرگترین مشکل IOT اینست که شرکت های متعدد سازنده آنها هیچ تجربه امنیتی ندارند، تخصص آنها ساخت وسایل و دستگاههای خانگی است. یا شاید شرکت های نو پایی هستند که تلاش می کنند که از سریع ترین راه ممکن موثر ترین وسیله را بسازند مثل شرکت Kickstarter. اینگونه شرکت ها بر سود بیشتر تمرکز دارند نه امنیت سایبری. دو نتیجه، بسیاری از دستگاههای IOT ملاحظات امنیتی در آنها یا بسیار ناچیز است یا اصلا لحاظ نشده است. مثلا بعضی از آنها رمز عبور های پیش فرض دارند که رمزی هم نیستند یا حتی در اینترنت موجود است و قابل تغییر هم نیست. بعلاوه، بسیاری از این وسایل گزینه تغییر ندارند و شما مجبورید با همان وضعیتی که وسیله را دریافت کرده اید کنار بیایید. بد تر اینکه بروز رسانی بسیاری از این وسایل مشکل است یا حتی غیر ممکن است. در نتیجه بسیاری از این دستگاههای IOT که استفاده می کنید ممکن است سریعا

اینترنت وسایل (IOT)

از رده خارج شوند بخاطر ضعف های معلومی که قابل درست شدن نیست و باعث آسیب پذیری همیشگی شما می شود.

محافظت از دستگاههای IOT

پس چکار می توان کرد؟ حتما کاری کنید تا کارایی دستگاههای IOT بطور امن و موثر زیاد شود. این دستگاهها امکانات بسیار خوبی که زندگی را ساده تر می کنند برای ما فراهم می کنند. مثلا صرفه جویی در پول و احتمالا افزایش امنیت فیزیکی منزل. بعلاوه، چنانکه تکنولوژی رشد می کند شما مجبورید از وسایل IOT استفاده کنید. اینها قدم هایی هستند که می توانید برای حفاظت از دستگاهها و خودتان بردارید.



بدانید کدام وسیله IOT به شبکه تان وصل است، اگر ممکن است آنها را جدا کنید، آنها را بروز رسانی کنید و با رمز عبور قوی از آنها حفاظت کنید.

- **فقط چیزی را که احتیاج دارید به اینترنت وصل کنید:** ساده ترین راه برای امن کردن وسیله IOT اینست که آنرا به اینترنت وصل نکنید. اگر احتیاج ندارید که دستگاهتان آنلاین باشد، آنرا به شبکه اینترنت بی سیم وصل نکنید.
- **شبکه های اینترنت بی سیم را سوا کنید:** اگر می خواهید دستگاههای IOT به اینترنت وصل باشند شبکه اینترنت بی سیم جداگانه برایشان در نظر بگیرید. بسیاری از دستگاههای اتصال به اینترنت بی سیم توانایی ایجاد چند شبکه مجزا را دارند مثل شبکه مهمان. گزینه دیگر خرید دستگاه اینترنت بی سیم دیگری فقط برای دستگاههای IOT است. اینکار دستگاههای IOT را در شبکه های جدا شده قرار می دهد که نمی توان از آنها برای آسیب زدن یا حمله به هیچ کامپیوتر یا دستگاه موبایلی که به شبکه اولیه یا شبکه منزل (که هنوز شبکه اصلی مورد علاقه مجرمان سایبری است) استفاده کرد.
- **هر وقت ممکن شد بروز رسانی کنید:** درست مثل کامپیوتر و دستگاه موبایل، دستگاههای IOT تان را بروز نگهدارید. اگر دستگاه IOT گزینه بروز رسانی خودکار دارند، آنرا فعال کنید.
- **رمز عبور قوی:** تمام رمز عبور های دستگاه IOT را تبدیل به جمله عبور قوی و منحصر بفردی که فقط خودتان می دانید تبدیل کنید. نمی توانید همه جمله های عبور را به یاد داشته باشید؟ نگران نباشید، ما هم نمی توانیم. از نرم افزار مدیریت رمز عبور برای ذخیره امن همه رمز عبور هایتان استفاده کنید.
- **گزینه حریم خصوصی:** اگر دستگاه IOT اجازه تشکیل گزینه حریم خصوصی می دهد حجم اطلاعاتی را که به اشتراک می گذاری را محدود کنید. یک گزینه برای از کار انداختن هرگونه قابلیت به اشتراک گذاری می باشد.

اینترنت وسایل (IOT)

- **جایگزینی را در نظر داشته بگیرید:** گاهی بهتر است دستگاه IOT جدیدی که امنیت تو کار بیشتری دارد را با دستگاه در حال حاضرتان که اشکالات شناخته شده زیادی دارد که قابل تصحیح هم نیستند جایگزین کنید.

یك راه حل برای همه دستگاهها وجود ندارد، پس ارزش دارد که در مورد بهترین روش و هر گونه مطلب منتشر شده در مورد امن کردن دستگاهها تحقیق کنیم. متاسفانه بیشتر IOT ها بدون در نظر گرفتن نکات امنیت سایبری توسعه پیدا کرده اند در نتیجه بخش عمده ای از تولید کنندگان اطلاعات امنیتی زیادی منتشر نمی کنند. چنانکه آگاهی در مورد امنیت سایبری افزایش پیدا می کند، امیدواریم فروشندگان IOT بیشتر و بیشتری را شاهد باشیم که نکات امنیتی را برای ساخت دستگاههایشان لحاظ می کنند و اطلاعات بیشتری در مورد چگونگی حفاظت و بروز رسانی آنها ارائه می دهند.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: http://www.securingthehuman.org

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

جمله عبور: https://securingthehuman.sans.org/ouch/2015#april2015

نرم افزار مدیریت رمز عبور: https://securingthehuman.sans.org/ouch/2015#october2015

امن سازی تبلت: https://securingthehuman.sans.org/ouch/2016#january2016

امن کردن شبکه خانگی: https://securingthehuman.sans.org/ouch/2016#february2016

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

ترجمه شده توسط : سعید میرجلیلی