OUCH! | اغسطس 2018

SANS SECURITY AWARENESS

OUCH!

نشرة الوعي الأمني الإخبارية الشهرية للجميع

أجهزة المنزل الذكية

أجهزة المنازل الذكية أو ما يعرف بإنترنت الأشياء (IoT)

إن عدد الأجهزة المتصلة بالإنترنت سابقا كان محصوراً على أجهزة الكمبيوتر المحمول، الهواتف الذكية أو أجهزة التحكم بالألعاب. ولكن اليوم فإن كل أجهزة المنزل أصبحت متصلة بالإنترنت على سبيل المثال لا الحصر بدءًا من المصابيح، مكبرات الصوت، التلفاز، أقفال الأبواب الذكية، وأيضا السيارات. يطلق على الأجهزة المتصلة بالإنترنت مسمى انترنت الأشياء (IoT) أو أجهزة المنزل الذكي. بقدر ما توفره هذه الأجهزة المتصلة من الراحة، فإنها تجلب أيضًا مخاطر أمنية جديدة.

اذن ما المشكلة؟!

كلما زاد عدد الأجهزة المتصلة بشبكة الانترنت، زادت المخاطر الأمنية. بحيث يستطيع الهاكر (قراصنة الانترنت) استخدام هذه الأجهزة إما في مساعدته باختراق أجهزة أخرى، أو أن يتم اختراقها وتعطيلها عن الخدمة، كما يستطيع منتجي هذه الأجهزة جمع معلومات تفصيلية عن الأنشطة التي تقوم بها. ونظرا لأن العديد من الشركات المصنعة لأجهزة انترنت الأشياء لا تمتلك خبره في مجال أمن الفضاء الالكتروني (cyber security) ونظرتها المادية تجاه توفير الاحتياجات الأمنية لهذه الأجهزة نتج عن ذلك توفر القليل من الاحتياطات الأمنية أو عدم توفرها أصلا. وعلى سبيل المثال فإن بعض الأجهزة تحتوي على كلمات مرور افتراضية معروفة جيدًا أو لا يمكنك تغيير الاعدادات الافتراضية لها لتصبح سهلة الاختراق.

كيف احمي نفسي

اذاً ما الذي يمكنك فعله؟ بالتأكيد نحن نريدك ان تستفيد من الأجهزة المتصلة بإنترنت الاشياء بصوره آمنه ومحميه، فاستخدام هذه الأجهزة سيوفر لنا مزايا رائعة الامر الذي يجعل حياتنا أسهل. أضف الى ذلك ان هذه التقنية تتطور سريعا الامر الذي سيجعلنا بمرور الوقت لا نملك خيارا إلا أن نتعامل مع الأجهزة الذكية المتصلة بإنترنت الاشياء. اليك بعض الخطوات الأساسية التي يمكنك اتباعها لتحمي نفسك:

اربط الأجهزة التي تحتاج فقط، بالشبكة: ان أسهل الطرق لحماية الأجهزة هي عدم ربطها بالإنترنت. فما دمت لست بحاجه لأن يكون جهازك على الانترنت، فببساطه تجنب ربطه بالشبكة اللاسلكية Wi-Fi في بيتك. ترى هل يهمك حقيقة ان يقوم جهاز تحميص الخبز ان يرسل لك تنبيها على جوالك !؟

كن على دراية بالأجهزة المتصلة: اي الأجهزة في البيت قمت بربطها بشبكتك المنزلية؟ لست متأكدا او لا تتذكر؟ حسناً، قم بفصل نقطه الاتصال بالشبكة اللاسلكية وتفقد الأجهزة التي ما عادت تعمل. قد لا تضمن هذه الطريقة كشف كل الأجهزة المتصلة لكنك في النهاية ستفاجئ بعدد الأجهزة التي قمت بربطها ونسيت ذلك بمرور الوقت.

ابقها محدثة على الدوام: كأي جهاز حاسوب او جوال، إنه من الضروري جدا ابقاء انظمه التشغيل المدمجة في اجهزتك محدثه باخر الاصدارات. لذلك ان كانت اجهزتك تتيح تحديث انظمتها اوتوماتيكياً فندعوك للتأكد من تفعيل هذه الخاصية.

كلمات المرور: لا تتوانى أبدا عن تغيير كلمة المرور الافتراضية على أجهزتك، قم باستبدالها بكلمة مرور فريدة وقويه لا يعلمها غيرك. عادة هذه العملية لن تحتاج للقيام بها أكثر من مره واحده. لكن هناك مشكله! ألا تستطيع تذكر كلمات المرور الكثيرة لكل هذه الأجهزة؟ معك حق، ولا حتى نحن!، لذا نقترح عليك استخدام أحد برمجيات ادارة وحفظ كلمات المرور لتسهيل هذه المهمة.

خيارات الخصوصية: ان كانت الأجهزة تتيح لك اعداد خيارات الخصوصية، فقم بتحديد كم البيانات التي تقوم بجمعها ومشاركتها من المستخدمين. نقترح عليك ان تقوم بتعطيل الخيار الذي يسمح بإتاحة او مشاركه المعلومات.

المصنّعين والباعه: احرص دوما على شراء المنتج من شركات تثق بها وتعرفها. ابحث دائما عن المنتج الذي يدعم خصائص الامان والتحديث المستمر للمنتج. كأن يتيح نظام تشغيل الجهاز ميزه التحديثات الالية علاوة على امكانيه تعديل كلمات المرور وتخصيص اعدادات الخصوصية.

التصنت الدائم: ان كان الجهاز يتحسس صوتك بصوره دائمة كجهاز اليكسا او جوجل هوم، اللذان يمكنهما تسجيل محادثاتك الحساسة في اي وقت. فعليك ان تقرر بناء على ذلك مكان تواجد هذا النوع من الأجهزة في بيتك مع مراجعه خيارات الخصوصية فيها.

الشبكات المعزولة (شبكه الضيوف): حاول استضافه وربط اجهزه المنزل الذكية على شبكات معزولة عن الشبكة الأصلية في بيتك او في مكان العمل والتي تربط عليها عادة اجهزه الكمبيوتر والجوالات المحمولة. بهذه الطريقة تكون قد عزلتها تماما في حال اخترق اي منها او اصابه فايروس فلن يؤثر على الشبكة الأصلية مما يضمن ابقائها آمنة.

ليس هناك من سبب يجعلك تخشى من التقنيات الحديثة لكن يتعين عليك ان تتفهم المخاطر التي قد تشكلها. هذه الخطوات القليلة والبسيطة سابقه الذكر يمكنها ان تساهم في بناء بيت ذكي أكثر أمانا.

الضيف المحرر

روبرت لي Robert M. Lee (@RobertMLee)هو الرئيس التنفيذي ومؤسس لشركة دراجوس لأمن الفضاء الالكتروني والصناعي كما يعمل أيضا مدرس معتمد لمؤسسة SANS و مؤلف لمحتوي دورة تدريبية بعنوان FOR578 متخصصة في تهديدات الفضاء الالكتروني إضافة لدورة تدريبية بعنوان ICS – ICS515 متخصصة في مجال الدفاع والاستجابة للحوادث.

مصادر إضافية

عبارات المرور (باللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_aa.pdf

تطبيقات إدارة كلمات المرور(باللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_aa.pdf

حماية شبكة المنزل الخاص بك(باللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201602_aa.pdf