SANS SECURITY AWARENESS

آوتش! | (كانون الثاني) يناير ٢٠١٨

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- شبكة الواي فاي
- الأجهزة المنزلية
- كلمات المرور
- النسخ الاحتياطي

جعل المنزل آمن من الهجمات الإلكترونية

مقدمة

قبل عدة سنوات كان جعل المنزل أمن الكترونيا شيء بسيط، حيث يوجد شبكة واي فاي وبعض أجهزة حاسوب مرتبطة بها. الان أصبحت التقنية أكثر تعقيدا ودخلت في كل شيء تقريبا من حياتنا. من أجهزة المحمول الي أجهزة الألعاب الي ترموستات الحرارة وربما الثلاجة. فيما يلي أربع محاور هامة لجعل المنزل آمن الكترونيا.

المحرر الضيف

مات برومیلي Matt Bromiley يعمل في الاستجابة لحالات الطوارئ الناتجة عن الهجمات الالكترونية، حيث يتعامل مع جميع أنواع الاختراقات وتسرب البيانات. يعمل أيضا مدرس لدي SANS لدورة التحقيقات الجنائية الالكترونية المتقدمة والتصرف في حالات الطوارئ FOR508. تابع مات علي تويتر **@mbromileyDFIR**.

شبكة واي فاي

أصبح وجود شبكة واي فاي منزلية أمراً شائعاً. فهذه الشبكة هي ما تُمكن الأجهزة المختلفة من الاتصال بالإنترنت. يتم التحكم في معظم الشبكات اللاسلكية المنزلية بواسطة موجه الإنترنت Router أو نقطة وصول لاسلكية Access Point. كلاهما يعمل بنفس الطريقة من خلال بث الإشارات اللاسلكية، والأجهزة في منزلك تتصل بالإنترنت عبر هذه الإشارات. هذا يعني أن تأمين شبكة واي فاي هو جزء أساسي من حماية منزلك. نوصي باتخاذ الإجراءات التالية:

- غير كلمة المرور الافتراضية لحساب Admin لموجه الإنترنتRouter أو نقطة الوصول اللاسلكية Access Point ، حساب Admin يستطيع التحكم بالإعدادات الخاصة شبكة واي فاي.
- تأكد من أن الأشخاص الذين تثق بهم فقط يمكنهم الاتصال بشبكتك اللاسلكية. قم بذلك عن طريق تفعيل خيارات الأمان القوية. حاليا الخيار الأفضل هو استخدام آلية أمنية تسمى WPA2. من خلال تفعيلها سيتوجب على من يريد الربط مع الشبكة إدخال كلمة مرور، وسيتم تشفير جميع بيانات التي يتم تبادلها من خلال الشبكة اللاسلكية.
- تأكد من استخدام كلمة مرور قوية للاتصال بشبكتك اللاسلكية وأنها مختلفة عن كلمة مرور admin. تذكر أنك تحتاج إلى إدخال كلمة المرور مرة واحدة عند توصيل جهاز جديد بالشبكة، اذ أن الجهاز سيقوم بتخزينها لاستخدامها للاتصال بالشبكة بعد ذلك.
- العديد من الشبكات اللاسلكية تدعم ما يسمى بشبكة الضيوف. هذا يسمح للزوار بالاتصال بالإنترنت، ولكن يحمي الشبكة المنزلية الخاصة بك لأنه لا يمكنهم من الاتصال بأي من الأجهزة الأخرى على الشبكة. إذا قمت بإضافة شبكة ضيوف، تأكد من تمكين WPA2 وكذلك كلمة مرور خاصة لهذه الشبكة.

جعل المنزل آمن من الهجمات الإلكترونية

إن كنت غير متأكد من كيفية تنفيذ هذه الخطوات يمكنك طلب المساعدة من مزود خدمة الإنترنت الخاص بك أو زيارة موقع الويب الخاص بهم، والتحقق من الوثائق التي تأتي مع جهاز التوجيه الإنترنت Router أو نقطة الوصول اللاسلكية Access Point ، أو الرجوع إلى موقع الويب الخاص بها.

اتبع هذه النصائح البسيطة لجعل المنزل آمن الإنترنت: قم بتامين شبكه واي فاي الخاصة بك ، قم بتمكين التحديث التلقائي ، استخدام عبارات مرور قوية، وقم بعمل نسخ احتياطية دورية لجميع الملفات والبيانات الهامة.

الأجهزة المنزلية

عليك التأكد من أن جميع الأجهزة المرتبطة مع الشبكة اللاسلكية تم تأمينها بشكل جيد. قد تكون هذه العملية بسيطة أن كان هناك جهاز أو جهازين فقط. لكن اليوم يمكن توصيل كل شيء تقريباً بالشبكة مثل الأجهزة اللوحية الذكية، أجهزة التلفاز، أجهزة الألعاب، أجهزة مراقبة الأطفال، السماعات وحتى السيارة. بقم بحصر جميع هذه الأجهزة ثم قم بتأمينها جميعاً. أفضل طريقة لعمل ذلك هو تمكين التحديثات التلقائية كلما كان ذلك ممكنا. مجرمو الشبكة يطورون باستمرار وسائل وطرق لاختراق الأجهزة وأنظمة التشغيل الخاص بها. بتفعيل التحديثات التلقائية، أجهزة الحاسوب والأجهزة الأخرى تتلقي أخر التحديثات الأمنية مما يصعب كثيراً على المخترقين عملهم.

كلمات المرور

من المهم استخدام كلمة مرور قوية وفريدة لكل جهاز من الأجهزة والحسابات المرتبطة بشبكة الإنترنت. هل تعبت من محاولات الحصول على كلمات مرور معقدة؟ كلنا كذلك!، بدلا من ذلك استخدم عبارات مرور. هذا النوع من كلمات المرور يستخدم سلسلة من الكلمات سهلة التذكر، مثل«Where is my coffee?» أو « sunshine-doughnuts-happy-lost». كلما زاد طول عبارة المرور كان ذلك أفضل وأقوى. كلمة مرور فريدة معناه استخدام كلمة مرور مختلفة لكل حساب مرتبط بالإنترنت. بهذه الطريقة لو تم كشف كلمة مرور لحساب واحد، تبقي الحسابات و الأجهزة الأخرى أمنة. وإذا كنت لا تستطيع تذكر كل تلك الكلمات الفريدة والقوية، لا تقلق، حتى نحن لا نستطيع ذلك. نحن نوصي باستخدام تطبيق إدارة كلمات المرور، وهو عبارة عن تطبيق لحفظ كلمات المرور وتسهيل استخدامها.

أخيرا، قم بتفعيل التحقق بخطوتين كلما كان ذلك ممكناً، خصوصا للحسابات المرتبطة بالإنترنت. التحقق بخطوتين أقوي بكثير. فهو يستخدم كلمات المرور- لكن أيضا يستخدم وسيلة إضافية، مثلا رقم خاص يُرسل الي جهازك المحمول أو تطبيق على جهازك الذكي يولد

جعل المنزل آمن من الهجمات الإلكترونية

ذلك الرقم. التحقق بخطوتين هي طريقة سهلة وفعالة لحماية نفسك أثناء اتصالك بالإنترنت.

النسخ الاحتياطي

رغم كل الاحتياطات التي نتخذها قد نتعرض أحياناً للاختراق. إذا حدث ذلك، غالبا الطريقة الوحيدة لاستعادة ملفاتك الشخصية هي استعاداها من النسخ الاحتياطي. تأكد دائما من عمل نسخ احتياطية دورية لجميع الملفات والبيانات الهامة. معظم الأجهزة الذكية المحمولة تدعم النسخ الاحتياطي علي التخزين السحابي. كذلك تتوفر تطبيقات للنسخ الاحتياطي لأجهزة الحاسوب سهلة في الاستخدام وبأسعار مناسبة.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة securingthehuman.sans.org/ouch/archives.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

عدد أوتش حول" عِبَارات المُرور": https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_aa.pdf

عدد أوتش حول "تطبيقات إدارة كلمات المرور": https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201709_aa.pdf

عدد أوتش حول "التحقق بخطوتين": https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_aa.pdf

عدد أوتش حول "النسخ الاحتياطي": https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201708_aa.pdf

مجلس التحرير: والت سكريفن، فيل هوفمان، كاثي كليك، شيريل كونلي

ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور