النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- شبكتك اللاسلكية
- نظام أسماء النطاقات المفتوح
- الأجهزة

تأمين الشبكة المنزلية

نظرة عامة

قبل عدة سنوات كانت الشبكات المنزلية إلى حد ما بسيطة، وغالباً نقطة وصول لاسلكية واحدة وجهاز حاسب أو اثنين تستخدم لتصفح الإنترنت أو لتشغيل الألعاب الإلكترونية. إلا أن الشبكات المنزلية ازدادت تعقيدا. وهذا لايخص فقط ربط المزيد من الأجهزة بالشبكات المنزلية، ولكن مجالات استخدامها تنوعت كذلك. سنقوم في هذا العدد بالحديث عن بعض الخطوات الأساسية لإنشاء شبكة منزلية أكثر أمانا.

المحرر الضيف

كيفن جونسون هو الرئيس التنفيذي لشركة سِكيور آيدياز (Secure Ideas)، ويدير موقع **MySecurityScanner.com**. وهو كذلك مدرب بارز بمعهد «سانْس». للمزيد من المعلومات يمكن زيارة: **www.secureideas.com**

شبكتك اللاسلكية

تشتمل معظم الشبكات المنزلية على شبكة لاسلكية (والتي تسمى غالباً «واي- فاي» (Wi-Fi)). ويمَكنك ذلك من الربط اللاسلكي لأي من الأجهزة الخاصة بك بالإنترنت، بما في ذلك أجهزة الحاسب المحمولة والأجهزة اللوحية إضافةً إلى أجهزة التلفاز ووحدات التحكم الخاصة بالألعاب الإلكترونية. وليتم ذلك، تحتاج الشبكة اللاسلكية الخاصة بك إلى ما يسمى بنقطة الوصول اللاسلكية. يتم توصيل نقطة الوصول اللاسلكية بموجه الإنترنت بواسطة سلك (تتضمن عدد من موجهات الإنترنت نقطة وصول لاسلكية) وتُرسِل إشارات لاسلكية تُمَكن الأجهزة الخاصة بك من الاتصال بها. عندما يتم ربط هذه الأجهزة بنقطة الوصول اللاسلكية، يصبح بإمكانها الإتصال بأجهزة أخرى على الشبكة المنزلية بالإضافة إلى الإتصال بالإنترنت. ونتيجة لذلك، تعتبر نقطة الوصول اللاسلكية إحدى الأجزاء الرئيسية من الشبكة المنزلية، ولذلك نوصي بالخطوات التالية لتأمينها.

- بالنسبة لمعظم نقاط الوصول اللاسلكية، التسجيل الإفتراضى لدخول «المسؤول» بما في ذلك كلمة المرور يكون معروفا، وغالبا ما تنشر هذه المعلومات على الإنترنت. لذلك، تأكد من تغيير كلمة المرور الإفتراضية بحيث لا يعرفها أحد غيرك. تأكد من أن كلمة المرور الجديدة مختلفة عن كلمات المرور لحساباتك الأخرى.
- خيار آخر سوف تحتاج إليه وهو تكوين إسم الشبكة اللاسلكية الخاصة بك. هذا هو الإسم الذي تتعرف عليه الأجهزة عند البحث عن الشبكات اللاسلكية المحلية. إعط للشبكة الخاصة بك إسما فريدا بحيث يمكنك التعرف عليه بسهولة، ولكن تأكد من أنه لا يحتوي على أي معلومات شخصية. بالنسبة لخيار جعل الشبكة مخفية (أو غير باثة) فهو لا يفيد كثيراً حيث أن معظم أدوات المسح اللاسلكية يستخدمها مهاجمون مهرة تمكنهم بسهولة من إكتشاف تفاصيل الشبكة المخفية.
- الخطوة التالية هي التأكد من أن الأشخاص الذين تعرفهم و تثق بهم هم الذين يمكنهم فقط الإتصال وإستخدام الشبكة

تأمين الشبكة المنزلية

اللاسلكية الخاصة بك، وأن هذه الإتصالات مشفرة. نريد أن نكون على يقين من أن الجيران أو الغرباء لا يمكنهم الإتصال أو مراقبة الشبكة الخاصة بك. يمكنك بسهولة تخفيف هذه المخاطر من خلال تأمين الإتصال بنقطة الوصول اللاسلكية. حاليا أفضل خيار هو إستخدام الآلية الأمنية المعروفة ب «WPA2». ببساطة عند تفعيلك لهذه الألية يحتاج كل مستخدم إلى كلمة مرور للإتصال بالشبكة، ويتم تشفير المعلومات المتبادلة بين المستخدم ونقطة الوصول. تأكد من أنك لا تستخدم أساليب حماية قديمة مثل «WEP». كذلك لا تترك شبكتك المنزلية مفتوحة، فالشبكة المفتوحة تسمح لأي شخص للإتصال بالشبكة اللاسلكية دون أي مصادقة.

لحماية الشبكة المنزلية تأكد أن لديك شبكة لاسلكية آمنة، وأنك تستخدم نظام أسماء النطاقات المفتوح أو خدمة مماثلة، أن جميع الأجهزة على الشبكة تحتوي أحدث أنظمة التشغيل الخاصة بها.

- تأكد من أن كلمات المرور التي تستخدم للاتصال بالشبكة اللاسلكية قوية ومن الصعب تخمينها، وأنها تختلف عن كلمة مرور مسؤول الشبكة. تذكر أنه على الأرجح سوف تقوم بإدخال كلمة المرور مرة واحدة فقط لكل جهاز، وسوف يقوم الجهاز بتخزين تلك الكلمة واستخدامها كلما قمت بالاتصال بالشبكة .
- توفر العديد من نقاط الوصول اللاسلكية خاصية شبكة الضيف والتي تسمح للزوار باستخدام نقطة الوصول اللاسلكية الخاصة بك بغرض الوصول إلى الإنترنت ، لكنها لا تسمح لهم بالاتصال بأي من الأجهزة الموجودة على الشبكة. إذا قمت بتفعيل هذه الخاصية، تأكد من تمكين خيار WPA2 وحدد كلمة مرور مختلفة خاصة بشبكة الضيف.
- إذا كنت لا تستطيع تذكر كلمات مرور كثيرة نقترح أن تستخدم أحد تطبيقات إدارة كلمات المرور لتخزينها بشكل آمن .

نظام أسماء النطاقات المفتوح

بعد الانتهاء من إعداد الشبكة اللاسلكية ننصحك باعداد الشبكة المنزلية لاستخدام نظام أسماء النطاقات المفتوح (أو خدمة مماثلة مثل نورتون ConnectSafe للمنزل) . عند كتابة اسم موقع ما في المتصفح يقوم خادم أسماء النطاقات بتحويل الاسم إلى عنوان الانترنت الخاص بالخادم الذي يحتوي على الصفحة المطلوبة. نظام أسماء النطاقات المفتوح (Open DNS) والخدمات المماثلة لديها سجل بالمواقع المؤذية وتقوم بمنع أي جهاز متصل بالشبكة المنزلية من زيارة هذه المواقع. بالإضافة إلى ذلك، هذه الأنظمة غالبا ما تعطي لك القدرة على فلترة وحجب المواقع المشكوك فيها. ما يجعل هذا النهج فعالا جدا هو أنك لا تحتاج لتثبيت برامج معينة على الأجهزة، ما تحتاجه فقط أن تعد نقطة الوصول اللاسلكية بشكل صحيح .

تأمين الشبكة المنزلية

الأجهزة

الخطوة التالية هي تأمين الأجهزة التي تتصل بالشبكة المنزلية. كان هذا العمل سهلا في السابق عندما كان عدد الأجهزة التي تتصل بالشبكة المنزلية قليلا. أما هذه الأيام فالعديد من الأجهزة الإلكترونية يمكنها الاتصال بالشبكة مثل أجهزة التلفزيون، وأجهزة الألعاب الإلكترونية وأجهزة مراقبة الأطفال والسماعات وميزان الحرارة وربما حتى سيارتك. ستفاجأ بعدد الأجهزة التي تستخدم الشبكة المنزلية الخاصة بك. أفضل طريقة للحفاظ على كل من هذه الأجهزة آمنة التأكد من أنها دائما تستخدم أحدث نسخة من نظام التشغيل الخاص بها. تأكد من تفعيل خيار التحديث التلقائي كلما أمكن ذلك. إذا لم يكن ذلك متاحا، عليك بمراجعة وتحديث أنظمة التشغيل بشكل دوري. بالإضافة إلى ذلك، تأكد من زيارة موقع مزود خدمة الإنترنت الخاص بك، لأنه قد يوفر أدوات وخدمات مجانية لمساعدتك على تأمين شبكة منزلك.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول الى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة http://www.securingthehuman.org.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة المتخصصين في أمن المعلومات بكلية علوم وهندسة الحاسب الآلي بجامعة الملك فهد للبترول والمعادن.

مصادر إضافية

نظام أسماء النطاقات المفتوح.(باللغة الانجليزية):
http://www.opendns.com/
نورتون ConnectSafe .(باللغة الانجليزية):
https://dns.norton.com/dnsweb/dnsForHome.do
المسح الأمني للشبكات .(باللغة الانجليزية):
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
إدارة كلمات المرور .(باللغة الانجليزية):
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي
ترجمها إلى العربية: طلال موسى الخروبي، محمد حسيني صقلي، فرج أحمد عز الدين، حكيم عديش، زبير بيق.