خبرنامه ماهیانه برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- شبکه بی سیم
- OpenDNS
- دستگاههای شما

تضمین امنیت شبکه خانگی

مقدمه

چندین سال قبل، شبکه های خانگی چیزی بیش از یک دستگاه دسترسی بی سیم و یک یا دو کامپیوتر برای اتصال به اینترنت و یا بازیهای آنلاین نبودند. ولی اکنون شبکه های خانگی خیلی پیچیده شده اند. نه تنها دستگاه های بیشتری را به شبکه های خانگیمان متصل میکنیم، بلکه استفاده های بیشتری هم از آنها میکنیم. در این شماره، برخی از گام های اساسی و ساده برای ایجاد یک شبکه خانگی امن تر را توضیح میدهیم.

سردبیر مهمان

کوین جانسون مدیر عامل شرکت Secure Ideas، مدیر سایت MySecurityScanner.com و مدرس ارشد موسسه SANS است. برای اطلاعات بیشتر میتوانید به سایت www.secureideas.com مراجعه کنید.

شبکه بی سیم خانگی

تقریبا همه شبکه های خانگی با یک شبکه بی سیم (گاهی اوقات شبکه Wi-Fi نامیده می شود) شروع می شوند. چون با شبکه بی سیم میتوان هر یک از دستگاه های خود را اعم از لپ تاپ ها، رایانه لوحی، کنسول های بازی و تلویزیون را به اینترنت وصل کرد. برای استقرار این شبکه بی سیم نیاز به چیزی به نام نقطه دسترسی بی سیم (WAP: Wireless Access Point) است که دستگاهی فیزیکی است که به روتر اینترنت شما متصل میشود (WAP میتواند با روتر اینترنت شما یکپارچه باشد و دستگاهی جداگانه نباشد) که سیگنال های بی سیم میفرستد تا دستگاه ها بتوانند بدون سیم به اینترنت وصل شوند. وقتی دستگاه شما به نقطه دسترسی بی سیم متصل شود، سپس از آنجا می تواند به دستگاه های دیگر که در شبکه خانگی شما یا اینترنت هستند متصل شوند. بنابراین نقطه دسترسی بی سیم بخش کلیدی شبکه خانگی شما است و مراحل زیر را برای امن کردن آن توصیه می کنیم.

- نام کاربری مدیریت و رمز عبور پیش فرض بسیاری از نقاط دسترسی بی سیم به راحتی قابل بدست آوردن هستند، حتی اغلب روی اینترنت منتشر شده اند. به همین دلیل حتما نام کاربری و رمز عبور پیش فرض مدیریت دستگاه نقطه دسترسی را به رمز عبوری که فقط شما می دانید تغییر دهید. حتما رمز عبوری منحصر به فرد که برای موارد دیگری استفاده نکرده اید انتخاب کنید.
- گزینه دیگری که نیاز به تنظیم دارد نام شبکه بی سیم است (SSID هم گفته میشود) این نامی است که دستگاههای داخل شبکه خانگی شما زمانی که شبکه بی سیم محلی را جستجو می کنند آنرا خواهند دید. سعی کنید نامی منحصر به فرد انتخاب کنید تا به راحتی بتوانید آن را بیابید، اما مطمئن شوید که هیچ اطلاعات شخصی در نام شبکه نگنجانید. بعضی سعی میکنند که نام شبکه را مخفی کنند تا دیگران نام شبکه را در بین شبکه های بی سیم موجود نبینند، ولی این کار ارزش چندانی ندارد چون اکثر برنامه های شبکه بی سیم یاب و یا هکرهای ماهر به راحتی می توانند نام و اطلاعات مربوط به یک شبکه مخفی را کشف کنند.

© The SANS Institute 2013

تضمین امنیت شبکه خانگی

- گام بعدی این است که مطمئن شوید که فقط افرادی که می شناسید و اعتماد دارید می توانند به شبکه بی سیم شما متصل شوند و استفاده کنند، همچنین ارتباطات در این شبکه رمز شده باشد. مطمئن شوید که همسایگان و یا غریبه ها نمی توانند به شبکه شما متصل و یا بر آن نظارت داشته باشند. به راحتی می توانید این خطرات را با فعال ساختن رمزنگاری قوی ارتباطات بر روی نقطه دسترسی بی سیم خود کاهش دهید. در حال حاضر بهترین گزینه استفاده از مکانیزم امنیتی WPA2 است. با فعال کردن ساده این مورد، هر کس بخواهد به شبکه وصل شود، نیاز به رمز عبوری برای اتصال به شبکه خانگی است، و وقتی صحت رمز وارد شده تصدیق شد آن ارتباطات رمز شده هستند. دقت کنید که از روشهای امنیتی قدیمی منسوخ مثل استفاده WEP نکنید، یا اینکه بدون هیچ تنظیم امنیت شبکه را اصطلاحا باز نگه دارید. باز گذاشتن شبکه به هر کسی اجازه میدهد تا به شبکه بی سیم شما بدون هیچ احراز هویت وصل شود.

برای محافظت از شبکه خانگی خود، مطمئن شوید که یک شبکه بی سیم امن دارید، از OpenDNS یاخدمات مشابه استفاده میکنید، و تمام دستگاههای موجود بر روی شبکه خانگی شما به روزرسانی شده اند.

- حتما از رمز عبوری قوی برای اتصال به شبکه های بی سیم استفاده شود که سخت بتوان حدس زد و متفاوت از رمز عبور مدیر شبکه است. در نظر داشته باشید که به احتمال زیاد تنها باید یک بار کلمه عبور را برای هر یک از دستگاه های خود وارد کنید، چون دستگاههای شما آنها را ذخیره و به حافظه میسپارند.
- بسیاری از نقاط دسترسی بی سیم از آنچه به نام شبکه مهمان شناخته میشود پشتیبانی میکنند. شبکه مهمان به میهمانان اجازه اتصال به نقطه دسترسی بی سیم شما و از آنجا دسترسی به اینترنت را میدهند، اما آنها نمی توانند به هیچ کدام از دستگاه های موجود در شبکه خانگی شما متصل شوند. اگر شبکه مهمان اضافه کرده اید، حتما تنظیمات WPA2 را فعال کنید و رمز عبور متفاوتی را برای این شبکه در نظر بگیرید.
- اگر نمی توانید کلمات عبور مختلف به یاد داشته باشید از یک برنامه مدیریت رمز عبور برای ذخیره امن آنها استفاده کنید.

OpenDNS

هنگامی که شبکه های بی سیم خود را تنظیم میکنید، توصیه می کنیم که شبکه خانگی خود را طوری تنظیم کنید تا از OpenDNS به عنوان سرویس دهنده DNS استفاده کند و یا سرویس های مشابهی مانند Norton ConnectSafe for Home. وقتی آدرسی را در مرورگرتان وارد میکنید این DNS است که میداند که مرورگر شما به کدام سرور در اینترنت وصل شود. خدماتی مثل OpenDNS وب سایتهای آلوده را شناسایی، و از اتصال دستگاههای متصل به شبکه خانگی بی سیم شما به طور تصادفی به این وب سایت های آلوده را متوقف می کند. علاوه بر این، این خدمات اغلب به شما توانایی فیلتر کردن و مسدود کردن وب سایت های دلخواهتان را میدهد. چیزی که این روش را بسیار موثر میکند این است که نیازی به نصب نرم افزار بر روی دستگاه شما وجود ندارد، شما تنها تنظیمی را در نقطه دسترسی بی سیم خود انجام میدهید.

© The SANS Institute 2013

تضمین امنیت شبکه خانگی

دستگاههای شما

گام بعدی دانستن این است که چه دستگاههایی به شبکه خانگی شما متصل شده اند و اطمینان حاصل کنید که این دستگاه ها امن می باشند. قبلا خیلی ساده بود وقتی فقط چند دستگاه متصل میشدند. ولی در حال حاضر، تقریبا هر چیزی می تواند به شبکه خانگی اتان، از جمله تلویزیون، کنسول های بازی، مانیتور اطفال، بلندگو، دماسنج خانه ، و یا شاید حتی ماشین شما متصل شوند. وقتی تمام دستگاه های موجود به شبکه خانگی خود وصل میکنید، ممکن است شگفت زده شوید که چه تعداد دستگاه متصل به شبکه تان است. بهترین راه برای حفظ امنیت همه این دستگاه ها این است که حتما همیشه آخرین نسخه از سیستم عامل روی آنها نصب باشد. مطمئن باشید که بروز رسانی خودکار را فعال کنید اگر امکان آن هست. اگر این گزینه وجود ندارد به صورت ماهیانه به روز رسانی را انجام دهید. علاوه بر این، به وب سایت سرویس دهنده اینترنت خود مراجعه کنید چون ممکن است آنها ابزارهای رایگان و خدماتی برای کمک به امن تر کردن شبکه خانگی شما فراهم کنند.

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 syscurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

:OpenDNS

http://www.opendns.org

:Norton ConnectSafe

http://dns.norton.com/dnsweb/dnsForHome.do

اسکنر های امنیت شبکه:

http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx

نرم افزار مدیریت رمز عبور:

http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

!OUCH توسط برنامه «زندگی امن» موسسه SANS تحت مجوز Creative Commons BY-NC-ND ۳.۰ منتشر و توزیع شده است. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. برای اطلاعات بیشتر، لطفا با ouch@securingthehuman.org تماس بگیرید.

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

ترجمه شده توسط : سعید میرجلیلی