SANS SECURITY AWARENESS
SafeNet Network & Security Services
شبکه امن اندیشه فردا

وای! ژانویه 2018

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- شبکه بی سیم
- تجهیزات
- رمز عبور
- شتیبان گیری

ایجاد یک خانه سایبری امن

مقدمه

چندین سال پیش، ایجاد یک خانه سایبری امن کار راحتی بود. بیشتر خانه ها شامل فقط یک شبکه بی سیم و چندین کامپیوتر بودند. امروزه تکنولوژی بسیار پیچیده تر شده و در تمام بخشهای زندگی ما از گوشی های هوشمند و کنسول های بازی گرفته تا تجهیزات گرمایشی و حتی یخچال ها اینترنت وارد شده است. در ذیل چهار قدم ساده برای ایجاد یک خانه سایبری امن را تشریح خواهیم داد :

سردبیر مهمان

مت برواملی مسئول پاسخگویی به حوادث روزانه است که در خصوص رخنه های امنیتی با مشتریان کوچک و بزرگ در ارتباط است. وی بعنوان مدرس SANS دوره ی FOR508(Advanced Digital Forensics and Incident Response) را آموزش میدهد. برای تماس با مت از آدرس **@mbromileyDFIR** استفاده کنید.

شبکه بی سیم

تقریبا در تمامی خانه ها شبکه های بی سیم (وای فای) وجود دارد. همه ابزار الکترونیکی از این طریق به اینترنت وصل میشوند. اکثر شبکه های بی سیم توسط روتر های اینترنتی و یا اکسس پونت ها کنترل میشوند. هر دوی این تجهیزات با انتشار سیگنالهای بی سیم موجب اتصال تجهیزات موجود در منزل به این سیگنال ها میشوند. مفهوم این جمله این است که امن کردن شبکه های بی سیم بخش اساسی در جهت محافظت از خانه شماست. پیشنهاد میشود قدمهای ذیل را برای بالا بردن امنیت آن بکار بگیرید.

- رمز عبور پیش فرض مدیر شبکه را در روتر و اکسس پوینت خود که برای کنترل شبکه بی سیم استفاده میشوند، تغییر دهید. حساب مدیریتی چیزیست که به شما اجازه پیکربندی تنظیمات را برای شبکه بی سیم میدهد.
- مطمئن شوید تنها افرادی میتوانند به شبکه بی سیم شما وصل شوند که به آنها اعتماد دارید. این کار با فعال کردن امنیت قوی قابل انجام است. در حال حاضر بهترین گزینه برای این کار استفاده از مکانیزمی به نام WPA2 میباشد. با فعال کردن این گزینه، جهت اتصال به شبکه خانگی نیاز به رمز عبور خواهد بود و به محض اتصال فعالیت های آنلاین رمزنگاری خواهند شد.
- اطمینان حاصل کنید که رمزعبوری که برای اتصال به شبکه بی سیم استفاده میشود یه رمز عبور قوی است و با رمز عبور مدیریت دستگاه فرق دارد. بخاطر داشته باشید که شما برای متصل کردن تجهیزات به شبکه بی سیم تنها یکبار این رمز را وارد میکنید، به این دلیل که این رمزعبور در دستگاه ها ذخیره خواهد شد.
- بسیاری از شبکه های بی سیم دارای قابلیتی به نام شبکه میهمان نیز هستند که برای میهمانان اجازه اتصال به اینترنت را فراهم میکنند، در عین حال از اتصال آنها به شبکه خانگی جلوگیری کرده و اجازه اتصال آنها به تجهیزات دیگر موجود در شبکه خانگی را

ایجاد یک خانه سایبری امن

نمیدهند. در صورتیکه نیاز دارید شبکه میهمان را اضافه کنید، مطئن شوید که قابلیت WPA2 را فعال کرده و رمز عبوری متفاوت با رمز عبور شبکه خانگی وارد کرده اید.

اگر نمیدانید که چطور باید این کارها را انجام بدهید با شرکت سرویس دهنده خود تماس بگیرید و یا به وب سایت آنها سر بزنید. همچنین میتوانید کتابچه راهنمایی که به همراه روتر و یا اکسس پوینت شما می آید را چک کرده و یا به وب سایت شرکت سازنده آنها مراجعه کنید.

با برداشتن چهار قدم ساده، خانه سایبری امن ایجاد کنید: امن کردن شبکه وای فای، فعال کردن بروز رسانی اتوماتیک، استفاده از عبارات عبور منحصربفرد، و فعال کردن پشتیبانها.

تجهیزات شما

قدم بعدی این است که بدانید چه تجهیزاتی به شبکه بی سیم شما متصل هستند و اطمینان حاصل کنید که همه آنها امن هستند. در گذشته با داشتن یک یا دو دستگاه کامپیوتر این کار بسیار ساده تر بود. ولی امروزه تقریبا هر چیزی نظیر تلفن های هوشمند، تلویزیون، کنسول های بازی، بلندگو ها و یا شاید ماشین شما، قابلیت اتصال به شبکه خانگی را دارند. زمانیکه کلیه تجهیزات موجود در شبکه خانگی را شناسایی کردید، مطمئن شوید همه آنها ایمن هستند. بهترین روش برای این کار این است که قابلیت بروزرسانی اتوماتیک را فعال کنید. حمله کنندگان سایبری دائما به دنبال ضعف های جدید در تجهیزات و سیستم عامل های مختلف میگردند. با فعال کردن بروزرسانی اتوماتیک، تجهیزات شما همیشه داری اخرین نسخه از نرم افزار بوده که کار را برای ورود هکرها به آن سخت تر میکند.

رمز های عبور

قدم بعدی استفاده از رمزعبور قوی و منحصر بفرد برای کلیه تجهیزات و حساب های آنلاین است. کلمات کلیدی در اینجا عبارات «قوی» و «منحصربفرد» هستند. آیا از استفاده از رمزهای عبور پیچیده که به سختی میتوان آنها را حفظ کرد و یا حتی تایپ کرد خسته شده اید؟ بجای آن از عبارات عبور استفاده کنید. عبارات عبور نوعی رمز عبور است که از چند کلمه که به سادگی قابل حفظ کردن است تشکیل میشود، عباراتی نظیر "Where is my coffee" و یا "sunshine-doughnuts-happy-lost" از نمونه های عبارات عبور است. عبارات عبور طولانی تر قوی تر هستند. رمز عبور منحصربفرد به معنی استفاده از رمزهای عبور متفاوت برای هر دستگاه و یا حساب آنلاین است. به این ترتیب اگر یک رمزعبور فاش شود، کلیه حسابهای دیگر و تجهیزات دیگر ایمن خواهد بود. نگران نباشید که نمیتوانید همه آن رمزهای عبور قوی و منحصربفرد را به خاطر بسپارید. برای این کار پیشنهاد میشود از نرم افزارهای مدیریت رمز عبور استفاده کنید. مدیریت رمزعبور برنامه ویژه ای است که بصورت رمزشده و امن میتوانید کلیه پسورد های شما را ذخیره کند.

در نهایت، اگر میتوانید قابلیت احراز هویت چند عاملی را علی الخصوص برای حسابهای آنلاین خود فعال کنید. احراز هویت دوعاملی راهکاری بسیار قوی است. در این روش علاوه بر رمز عبور قدم دیگری نیز برای احراز هویت اضافه میشود. این قدم اضافه میتواند ارسال یک کد

ایجاد یک خانه سایبری امن

به گوشی هوشمند شما و یا یک برنامه بر روی گوشی هوشمند شما باشد که یک کد برای شما تولید کند. احراز هویت دوعاملی مهمترین قدمی است که میتوانید برای محافظت از حساب های خود بردارید و این کار آسان تر از آن چیزیست که شما تصور کنید.

پشتیبان گیری

گاهی اوقات، بدون در نظر گرفتن اینکه چقدر مراقب هستید، ممکن است هک شوید. اگر این اتفاق بیافتد، احتمالا تنها راهی که میتوانید اطلاعات شخصی خود را بازیابی کنید استفاده از پشتیبان های قبلی است. اطمینان حاصل کنید که بصورت مرتب از اطلاعات مهم خود پشتبان میگیرید و بررسی کنید که آن اطلاعات قابل بازیابی است. بیشتر موبایل ها قابلیت پشتیبان گیری اتوماتیک بر روی سیستم ابری را دارند. برای بیشتر کامپیوترها نیز ممکن است نیاز به خرید برنامه و یا سرویس های پشتیبان گیری داشته باشید که عموما ارزان قیمت بوده و به سادگی قابل استفاده هستند.

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: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

عبارات عبور: https://securingthehuman.sans.org/ouch/2017#april2017
مدیریت رمز عبور: https://securingthehuman.sans.org/ouch/2017#september2017
احراز هویت چند عاملی: https://securingthehuman.sans.org/ouch/2017#december2017
پشتیبانها: https://securingthehuman.sans.org/ouch/2017#august2017

هیأت تحریریه : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی