OUCH!
SANS SECURITY AWARENESS
ماهنامه آگاهی از امنیت اطلاعات برای شما

چهار قدم ساده برای امن ماندن

مقدمه

استفاده راحت و امن از تکنولوژی میتواند به نظر سخت و گیج کننده برسد. با این وجود، صرفنظر از اینکه از چه تکنولوژی و یا چگونه استفاده میکنید، چهار قدم ساده میتواند به شما کمک کند تا امن و امان بمانید.

1. خود شما: مهمتر از هر چیزی، باید بدانید که تکنولوژی به تنهایی نمیتواند از شما بطور کامل محافظت کند، خود شما بهترین دفاع هستید. مهاجمان آموخته اند که ساده ترین روش برای بدست آوردن آنچه میخواهند، هدف قرار دادن خود شماست، نه رایانه و یا سایر تجهیزات شما. اگر میخواهند پسورد و یا کارت اعتباری شما را بدست بیاورند و یا کنترل دستگاه شما را بدست بگیرند، تلاش میکنند تا با فریب شما در قالب ایجاد حس فوریت، به آنچه میخواهند برسند. بعنوان مثال، آنها میتوانند با شما تماس بگیرند و وانمود کنند که از بخش پشتیبانی فنی مایکروسافت هستند و ادعا کنند که دستگاه شما آلوده شده است، درحالیکه آنها مجرمان سایبری هستند و از شما میخواهند به آنها اجازه دسترسی به دستگاه خود را بدهید. یا شاید برای شما یک ایمیل هشدارارسال کنند که نمیتوانند بسته پستی شما را تحویل دهند و از شما بخواهند با کلیک کردن بر روی یک لینک، آدرس پستی خود را تایید کنید، درحالیکه با فریب دادن شما میخواهند وارد یک سایت مخرب شوید تا دستگاه شما هک شود. در نهایت بهترین دفاع در قبال مهاجمان خود شما هستید. با استفاده از عقل سلیم میتوانید حملات را تا حد زیادی کم و یا متوقف کنید.

2. عبارات عبور: سرعت محاسبات مدرن باعث شده تا رمز عبور 8 کاراکتری منسوخ و آسیب پذیرشوند. زمانیکه یک سایت از شما میخواهد تا رمز عبور برای خودتان ایجاد کنید، بجای رمز عبور یک عبارت عبور قوی و منحصر بفرد درست کنید. عبارت عبور یک نوع رمز عبور است که از یک سری کلمات استفاده می کند که به راحتی می توان به خاطر سپرد ، مانند «باران زنبور عسل بوربون». هرچه عبارت عبور طولانی تر باشد ، قوی تر است. عبارت عبور منحصر به فرد به معنای استفاده از عبارات مختلف برای هر دستگاه یا حساب آنلاین است. به این ترتیب اگر یک عبارت به خطر بیافتد ، حساب ها و دستگاه های دیگر شما همچنان ایمن هستند. اگر نمیتوانید کلیه عبارات عبور خود را به خاطر بسپارید میتوانید از برنامه های مدیریت پسورد استفاده کنید. مدیریت پسورد برنامه های ویژه ای هستند که با استفاده از آنها میتوانید کلیه عبارات عبور خود را بصورت امن و رمزگذاری شده ذخیره کنید(بهمراه بسیاری از قابلیت های دیگر).

در نهایت، قابلیت تایید دو مرحله ای (که احراز هویت دوعاملی و یا چند عاملی نیز گفته میشوند) را فعال کنید. این قابلیت علاوه بر رمز عبور، قدم دیگری هم برای تایید هویت اضافه میکند، مثلا ارسال کد به تلفن هوشمند و یا برنامه ای که کد را برای شما تولید میکند. تایید دو مرحله ای احتمالا مهمترین قدمی است که شما میتوانید برای محافظت از حساب های آنلاین خود بردارید و استفاده از آن بسیار آسان تر از آن است که فکرش را بکنید.

3. بروزرسانی: اطمینان حاصل کنید که هر کامپیوتر، تلفن همراه، برنامه و اپلیکیشنی که استفاده میکنید با اخرین نسخه نرم افزاری خود اجرا میشوند. مهاجمان سایبری دائما در حال جستجو برای آسیب پذیری های جدید در نرم افزار ها و یا تجهیزات شما هستند. زمانیکه یک آسیب پذیری را کشف کنند، برنامه های خاصی را برای سوء استفاده از آنها و هک کردن دستگاه ها بکار خواهند گرفت. در عین حال، شرکت های تولید کننده آن نرم افزار ها نیز به شدت در حال تلاش هستند تا با ارائه بروزرسانی های جدید این آسیب پذیری ها را برطرف نمایند. با اطمینان از اینکه کامپیوترها و تجهیزات همراه شما به سرعت این آپدیت ها را نصب کرده اند، موجب خواهید شد تا هک کردن شما به مراتب سخت تر شود. با فعال کردن بروزرسانی خودکار، همیشه بروزبمانید. این قاعده باید بر روی هر تکنولوژی که به اینترنت وصل میشود، نظیر تلوزیون اینترنتی، مانیتور کودکان، دوربین های امنیتی، روترهای خانگی، کنسول های بازی و حتی خودروی شما اعمال گردد.

4.پشتیبان گیری و بازیابی: گاهی اوقات هر چقدر هم که مراقب باشید ممکن است هک شوید. در این صورت، اغلب تنها راه بازیابی اطلاعات شخصی، استفاده از نسخه پشتیبان است. اطمینان حاصل کنید که بصورت منظم از اطلاعات مهم پشتیبان تهیه میکنید و مطمئن شوید که میتوانید اطلاعات خود را از نسخه پشتیبان بازیابی کنید. بیشتر سیستم عامل ها و تجهیزات همراه از قابلیت پشتیبان گیری خودکار بر روی هارد درایو خارجی و یا سیستم ابری حمایت میکنند.

سردبیر مهمان

استیو آنسون، مدرس مورد تایید SANS، راهنمایی هایی را برای تیم های امنیتی آی تی و سازمانها در سراسر دنیا فراهم میکند تا وضعیت امنیتی خود را بهبود ببخشند. استیو نویسنده کتاب Applied Incident Response است که به زودی منتشر میشود و در سایت www.AppliedIncidentResponse.com منابع رایگان برای متخصصان امنیت فراهم میکند.

منابع

مهندسی اجتماعی: https://www.sans.org/u/W3G

کلاهبرداری های شخصی: https://www.sans.org/u/W3Q

رمزهای عبور را ساده کنید: https://www.sans.org/u/W3V

پشتیبان بگیرید: https://www.sans.org/u/W40