ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

بله، شما هدف هستید!

مقدمه

سردبیر مهمان

اریک کنراد (Eric Conrad) ، رئیس و CTO در شرکت Backshore Communications و نویسنده اصلی کتابهای راهنمای مطالعه CISSP (ویرایش دوم) و یازده ساعت CISSP (ویرایش دوم) است . او همچنین در تالیف مواد درسی دوره شش روزه نظارت مستمر و عملیات امنیتی (SEC511) در SANS همکاری کرده است.

تصور غلط رایج در بین بسیاری از مردم این است که آنها هدف برای جرایم اینترنتی نیستند: همچنین اینکه آنها و یا رایانه های آنها چیز با ارزشی ندارد. که خیلی دور از واقعیت است. اگر شما کامپیوتری، دستگاه تلفن همراه، حسابی آنلاین، آدرس ایمیل، کارت اعتباری، یا نوع دیگری از فعالیت های آنلاین دارید، شما ارزش اقتصادی برای مجرمان اینترنتی دارید. در این خبرنامه ما توضیح میدهیم که چرا شما یک هدف هستید، و شما چطور مورد حمله قرار میگیرید، و چگونه می توانید از خود حفاظت کنید.

چرا شما هدف قرار میگیرید؟

جرائمی مانند کلاه برداری، سرقت هویت و یا اخاذی از زمانی که تمدن وجود داشته است آنها هم وجود داشته اند، آنها بخشی از زندگی روزمره ما هستند. هدف جنایتکار همواره یکسان بوده است: بهره اقتصادی بیشتر تا آنجا که ممکن است ، هر چه راحت تر و با خطر هر چه کمتر. در گذشته، مجرمان این مشکل را داشتند که آنها اغلب محدود به مکان بودند همچنین نیاز تماس فیزیکی با قربانیان داشتند. این امر نه تنها مجرمان را در انتخاب هدف محدود میکرد، بلکه مجرمان در معرض مقدار زیادی خطر بودند. با این حال، جرم و جنایت اساسا با ظهور اینترنت و فن آوری های آنلاین تغییر کرده است. در حال حاضر مجرمان اینترنتی به راحتی می توانید تقریبا هر کس در جهان ، با هزینه کم و یا هیچ هزینه ای، و با خطر بسیار کمی هدف قرار دهند. علاوه بر این، مجرمان اینترنتی بسیار سازمان یافته و کارآمد شده اند، که آنها را قادر می سازد تا موثرتر از همیشه باشند.

مجرمان اینترنتی می دانند که هرچه کارت های اعتباری بیشتری سرقت کنند، حسابهای بانکی بیشتری میتوانند هک کنند و یا کلمه عبور بیشتری را بدست آورند، و در نتیجه پول بیشتری بدست آورند. آنها به معنای واقعی کلمه برای هک هر کس که متصل به اینترنت از جمله شما تلاش خواهند کرد. هک میلیون ها نفر در سراسر جهان ممکن است بسیار سخت به نظر برسد، اما با استفاده از ابزار خودکار برای انجام تمام کار بطور شگفت انگیزی آسان است. به عنوان مثال، آنها ممکن است پایگاه اطلاعاتی از میلیون ها ایمیل بسازند و با استفاده از ابزار خودکار پیام های فیشینگ به هر یک از آن آدرسها ارسال کنند. ارسال اینگونه ایمیل ها هزینه تقریبا ناچیزی برای مجرمان دارد: آنها به سادگی از کامپیوترهای دیگر هک شده، شاید حتی کامپیوتر شما، برای انجام کار کثیف خود استفاده کنند. این هم نمونه دیگری از همین دلیل که چرا کامپیوتر شما

بله، شما هدف هستید!

برای آنها ارزشمند است ، اگر هیچ چیز دیگری نتواند برای هک و یا آسیب به دیگران مورد استفاده قرار گیرد، در نهایت، این مجرمان نمی دانند چه کسی قربانی حملات ایمیل خود قرار می گیرند، اما آنها می دانند ایمیل بیشتر مساوی با قربانیان بیشتر است. یا شاید مجرمان به معنای واقعی کلمه هر کامپیوتر در اینترنت (یک بار دیگر با استفاده از رایانه های هک شده برای انجام اسکن) اسکن میکنند ، و به دنبال هر کامپیوتر و یا دستگاهی که آنها می توانند هک کنند میگردند. به یاد داشته باشید ، که شما خاص نیستید و شما هم مورد هدف هستید. در عوض، این مجرمان همه را هدف قرار میدهند همه آنهایی که می توانند، که ممکن است شما هم باشید.

وقتی ویندوز ایکس پی دیگر پشتیبانی نشود، بهترین راه برای محافظت از خود، نصب یک سیستم عامل جدید است که فعالانه توسط فروشنده آن پشتیبانی میشود، و اطمینان از به روز بودن مداوم آن است.

چگونه از خود محافظت کنید

هنگامی که مجرمان اینترنتی در تلاش برای هک مردم در سراسر جهان هستند، آنها به طور معمول از روشهای نسبتا ساده استفاده میکنند. خوشبختانه، شما هم با انجام برخی گامهای به همان اندازه ساده می توانید یک راه طولانی به سوی حفاظت از خودتان بروید. برخی از گامهایی که توصیه می کنیم عبارتند از:

- خودتان: در نهایت، شما در خط اول دفاع در برابر هر حمله سایبری می باشید. بسیاری از حملات با خرابکار کامپیوتری شروع به تلاش برای فریب شما میکنند، مانند فریب شما به باز کردن ضمیمه ایمیل آلوده و یا فریب شما به دادن رمز عبور خود از طریق تلفن. تامل بهترین دفاع است : اگر چیزی عجیب و غریب، مشکوک و یا بیش از حد خوب به نظر می رسد ، به احتمال زیاد یک حمله هست .

- به روزرسانی: حتما هر کامپیوتر و یا دستگاه تلفن همراه خود را به طور کامل به روز کرده و مطمئن باشید آخرین وصله ها را دارد . این نه تنها برای سیستم عامل شما، بلکه برای هر برنامه و یا افزونه ای که استفاده میکنید مهم هست. با به روزرسانی مداوم سیستم ها و برنامه های کاربردی به حفاظت از خود در برابر حملات رایج کمک میکنید.

- رمز عبور: از یک رمز عبور منحصر به فرد قوی برای هر یک از حساب های خود استفاده کنید. به این ترتیب اگریکی از وب سایتهای که استفاده می کنید هک شد و تمام کلمات عبور سایت در معرض خطر هستند (از جمله رمز عبور شما) حساب های دیگر شما امن می ماند. همچنین اطمینان حاصل شود که تمام دستگاه های مختلف شما توسط ، رمز عبور منحصر به فرد، NIP و یا برخی از انواع دیگر از مکانیزم قفل قوی محافظت می شود. برای نگهداری و ردیابی امن تمامی رمزهای عبور مختلف خود توصیه می کنیم از یک مدیر رمز عبور استفاده کنید.

بله، شما هدف هستید!

- کارت های اعتباری : صورتهای مالی خود را اغلب بررسی کنید، توصیه می کنیم حداقل هر هفته (ماهیانه کافی نیست). به محض این که شما هر گونه معامله مشکوک در کارت اعتباری خود دیدید، آن را بلافاصله به صادر کننده کارت خود گزارش دهید . اگر بانک شما اجازه می دهد تا از پست الکترونیک و یا پیام متنی هشدار برای اعلام معامله غیر منتظره بزرگ و عجیب و غریب استفاده کنید، از آنها برای اطلاع رسانی هرچه سریع تر فعالیت های مشکوک استفاده کنید.

- شبکه شما: شبکه خانگی بی سیم iF -iW خود را با رمز عبور مدیر قوی امن کنید و مطمئن باشید که هر کس میخواهد از شبکه iF-iW شما استفاده کند نیاز به یک رمز عبور دارد. همچنین اطمینان حاصل شود که می دانید کدام دستگاه های شما به شبکه خانگی شما متصل شده و تمام دستگاه ها به روز شده است.

- رسانه های اجتماعی: هر چه اطلاعات بیشتری شما در شبکه های آنلاین به اشتراک بگذارید، بیشتر احتمال دارد خود را در معرض خطر قرار بدهید. هر گونه اطلاعات شما در نوشته ها برای مجرمان اینترنتی به هدف قرار دادن و فریب شما را آسان تر میکند، همچنین هر گونه اطلاعات شما در نوشته ها ممکن است در واقع شما را به عنوان یک هدف با ارزش تر نشان دهد.

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

اعلان خبر پایان حیات ایکس پی توسط مایکروسافت:
http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx
:OpenDNS
www.opendns.org
راهنمای تغییر سیستم عامل از ویندوز اکس پی:
/http://www.zdnet.com/windows-xp-end-of-life-migration-guide-7000023800
ذاهنمای پشتیبان گیری و بازیابی:
http://www.securingthehuman.org/ouch/2013#september2013

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی