ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

چهار قدم برای امن ماندن

مقدمه

همچنانکه تکنولوژی نقش مهمتری در زندگی ما بدست می آورد، پیچیده تر هم می شود. با سرعتی که تکنولوژی عوض می شود، رعایت نکات امنیتی هم گیج کننده می شود. بنظر می رسد در مورد کارهایی که باید انجام شود یا نشود همیشه راهکارهای جدیدی وجود دارد. اما، در حالیکه جزئیات چگونه امن ماندن به مرور زمان عوض می شود، کارهای اساسی وجود دارند که همیشه باید انجام دهید تا از خود محافظت کنید. صرفنظر از اینکه از چه تکنولوژی ای استفاده می کنید یا کجا از آن استفاده می کنید ما این چهار قدم کلیدی را توصیه می کنیم. برای اطلاعات بیشتر از هر کدام از این مراحل زیر، به قسمت منابع در انتهای همین خبرنامه مراجعه کنید.

سردبیر مهمان

رایان جانسون بر حصول اطمینان از اینکه سازمان ها آماده پاسخگویی به رخنه های اجتناب ناپذیر هستند کار می کند. و شبکه کشف جرایم پیشرفته در SANS تدریس می کند. رایان در توییتر با **@forensicRJ** فعال است.

1. **شما**:اول و در درجه نخست، در ذهن داشته باشید که تکنولوژی به تنهایی هرگز شما را کاملا محافظت نخواهد کرد. حمله کنندگان دریافته اند که آسانترین راه برای دور زدن پیشرفته ترین تکنولوژی امنیتی حمله به شماست. اگر رمز عبور، کردیت کارت یا اطلاعات شخصی تان را بخواهند آسانترین راه فریب شما به نحوی که اطلاعات را به ایشان بدهید است. مثلا، با شما تماس می گیرند و وانمود می کنند از قسمت پشتیبانی تکنولوژی مایکروسافت هستند و ادعا می کنند کامپیوترتان آلوده شده است. در حالیکه در واقعیت آنها فقط مجرمان سایبری هستند که می خواهند شما دسترسی به کامپیوترتان پیدا کنند. یا شاید به شما ایمیلی خواهند فرستاد و توضیح خواهند داد که بسته پستی إرسال نمی شود و از شما می خواهند بر روی لینکی کلیك کنید تا آدرس پستی تان تایید شود، در حالیکه در واقعیت دارند شما را به بازدید از سایتی مخرب که کامپیوترتان را هك خواهد کرد می فریبند. حملاتی مانند باج افزار یا کلاهبرداری مدیر عامل آغاز می شود. در نهایت، مهمترین دفاع در برابر حمله کنند خود شما هستید. مشکوك باشید. با استفاده از عقل سلیم می توانید بیشتر حمله ها را شناسایی و متوقف کنید.

2. **رمز عبور**:مرحله بعد برای حفاظت از خودتان شامل استفاده از یك رمز عبور قوی و منحصر بفرد برای هر کدام از دستگاهها و حساب های آنلاین است. کلمات کلیدی قوی و منحصر بفرد هستند. رمز عبور قوی یعنی رمز عبوری که به آسانی توسط هکر ها یا

چهار قدم برای امن ماندن

برنامه های خودکارشان حدس زده نمی شود. آیا از رمز عبور های پیچیده که هم به خاطر سپری و تایپشان سخت است خسته هستید؟ بجایش از جمله عبور استفاده کنید. بجای یك کلمه، از سری کلمات که بخاطر سپردنشان ساده است استفاده کنید، مثلا، « قهوه من کجاست؟». هر چه جمله عبور طولانی تری داشته باشید، قوی تر است. رمز عبور منحصر بفرد یعنی استفاده از رمز عبوری جداگانه برای هر دستگاه و حساب آنلاین. از این راه اگر یك رمز عبور در معرض خطر قرار گیرد، دیگر حساب های آنلاین و و دستگاهها هنوز محفوظ هستند. نمی توانید همه این رمز عبور های قوی و منحصر بفرد را به خاطر بسپارید؟ نگران نباشید! ما هم نمی توانیم. بهمین دلیل ما توصیه می کنیم از نرم افزار مدیریت رمز عبور که اپلیکیشن تخصصی در رایان یا تلفن هوشمند برای ذخیره امن همه رمز عبورها به شکل رمزگذاری شده است استفاده کنید.

با انجام این چهار قدم ، همزمان که از آخرین تکنولوژی بهره می برید، گام بزرگی هم در حفاظت از خود برداشته اید.

در نهایت، یکی از مهمترین قدم ها که برای حفاظت از هر حسابی می توانید بردارید، فعال نمودن تایید دو مرحله ای است. رمز عبور ها دیگر به تنهایی برای حفاظت از حساب ها کافی نیستند. ما همه به چیزی قوی تر نیاز داریم. تایید دو مرحله ای بسیار قوی تر است. از رمز عبور استفاده می کند اما قدم دومی هم اضافه می کند. یا چیزی که شما هستید (بیومتریك) یا چیزی که شما دارید(مثل کدی که به تلفن هوشمند فرستاده می شود یا اپلیکیشنی در تلفن هوشمند که این کد را برای شما تولید می کند). این گزینه را در همه حساب ها فعال کنید، شامل نوم إفراز مدیریت رمز عبور اگر ممکن باشد. تایید دو مرحله ای شاید تنها و مهمترین قدمی است که می توانید برای محافظت از خودتان بردارید و آسانتر از چیزی است که فکرش را بکنید.

۳. **بروز رسانی** :از اینکه کامپیوتر ها، دستگاههای موبایل، اپلیکیشن و هر چیز دیگری که به اینترنت وصل است با آخرین نسخه نرم افزار کار می کند اطمینان حاصل کنید. مجرمان سایبری دائما بدنبال پیدا کردن نقاط آسیب پذیر نرم افزاری که دستگاهتان استفاده می کند هستند. وقتی نقاط آسیب پذیر را پیدا کردند از برنامه های خاصی برای بهره برداری از آن نقاط ضعف برای هك دستگاه استفاده می کنند. در همین حال، شرکت های سازنده این نرم افزار ها با انتشار بروز رسانی ها به سختی برای درست کردن این نقاط آسیب پذیر کار می کنند. با حصول اطمینان از اینکه موبایل ها و کامپیوتر ها این بروز رسانی ها را نصب می کنند، هك شدن سیستم را برای هکر ها سخت تر می کنید. برای بروز ماندن، همیشه به سادگی گزینه بروز رسانی خودکار را فعال کنید. این قانون

چهار قدم برای امن ماندن

تقریبا شامل هر تکنولوژی ای که وصل به شبکه است، تلویزیون های متصل به اینترنت، مانیتور کودک، روتر خانه، کنسول بازی یا شاید یک روزی ماشین خودتان می شود. اگر سیستم عامل یا دستگاه قدیمی دارید که دیگر بروز رسانی امنیتی نمی شوند، ما توصیه می کنیم آنها را با دستگاهها و سیستم عامل جدیدتر که بروز رسانی می شوند جایگزین کنید.

۴. **پشتیبان ها** :گاهی اوقات صرفنظر از اینکه چقدر مراقب هستید، ممکن است هک شوید. اگر این اتفاق افتاد اغلب تنها انتخاب برای اینکه موبایل یا کامپیوترتان عاری از باج افزار است اینست که بطور کامل آنها را پاک کنید و از اول دوباره بسازید. حمله کننده ممکن است از دسترسی تان به فایل های شخصی، عکسها، و سایر اطلاعات ذخیره شده بر سیستم هک شده هم جلوگیری کند. اغلب تنها راه ذخیره دوباره همه اطلاعات شخصی استفاده از پشتیبان هاست. حتما بطور منظم از هر گونه اطلاعات مهم پشتیبان گیری کنید و بررسی کنید که بتوانید آنها دوباره باز گردانید. بیشتر سیستم عامل ها و دستگاههای موبایل پشتیبان گیری خودکار انجام می دهند. بعلاوه، توصیه می کنیم پشتیبان ها را در سیستم ابری یا آفلاین ذخیره کنید تا از حمله کنندگان سایبری در امان باشند.

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

منابع

فیشینگ: https://securingthehuman.sans.org/ouch/2015#december2015

نرم افزار مدیریت رمز عبور: https://securingthehuman.sans.org/ouch/2015#october2015

تایید دو مرحله ای: https://securingthehuman.sans.org/ouch/2015#september2015

جمله عبور: https://securingthehuman.sans.org/ouch/2015#april2015

پشتیبان ها: https://securingthehuman.sans.org/ouch/2015#august2015

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

ترجمه شده توسط : سعید میرجلیلی