ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- مهندسی اجتماعی
- تشخیص / توقف حملات مهندسی اجتماعی
- جلوگیری از حملات آینده

مهندسی اجتماعی

مقدمه

یکی از اشتباهات رایجی که مردم در مورد هکرهای سایبری میکنند این است که هکرها فقط با استفاده از ابزارها و فن آوری های هک پیشرفته به رایانه مردم، حساب و دستگاه های تلفن همراه نفوذ میکنند. این اصلا درست نیست. هکرها آموخته اند که یکی از ساده ترین راه ها برای سرقت اطلاعات شما یا هک رایانه شما برای رسیدن به نیات شومشان، صحبت ساده با شما و گمراه کردن شما است. در این خبرنامه خواهیم آموخت که چگونه این نوع از حملات انسانی، معروف به حملات مهندسی اجتماعی کار میکنند و برای محافظت از خودتان چه می توانید انجام دهید.

سردبیر مهمان

Alissa Torres مربی مورد تایید SANS و متخصص در بازرسی قانونی پیشرفته رایانه و پاسخ سریع است. تجربه کاری او شامل خدمت در شغل هایی مانند کنترل کننده حادثه و کار با یک تیم امنیت به عنوان بازرس قانونی دیجیتال است. او را می توانید در توییتر با آدرس **@sibertor** دنبال کنید.

مهندسی اجتماعی

مهندسی اجتماعی نوعی حمله غیر فنی و بیشتر روانی است که در آن یک مهاجم شما را به انجام کاری که آنها می خواهند فریب میدهند تا شما آن کار را برای آنها انجام دهید. مهندسی اجتماعی از هزاران سال پیش وجود داشته است، این ایده کلاه برداری و یا فریب جدید نیست. با این حال، هکرهای سایبری آموخته اند که استفاده از این روش در اینترنت بسیار موثر است و می توانند با این روش میلیون ها نفر را فریب دهند. ساده ترین راه برای درک چگونگی کارکرد مهندسی اجتماعی نگاه به یک مثال واقعی و متداول است.

فردی با شما تماس تلفنی برقرار میکند و ادعا می کند از یک شرکت پشتیبانی رایانه، از شرکت خدمات اینترنتی شما (ISP) یا حتی بخش پشتیبانی فنی مایکروسافت است. تماس گیرنده توضیح می دهد که آنها متوجه شده اند که رایانه شما رفتار عجیب و غریبی، مانند اسکن اینترنت و یا ارسال هرزنامه انجام میدهد، و آنها بر این باورند که رایانه شما آلوده شده است و از آنها خواسته شده که این موضوع را بررسی کرده و به شما کمک کنند رایانه خود را امن کنید. سپس انواع و اقسام اصطلاحات فنی بکار میبرند و شما را با ترفندهای گیج کننده متقاعد میکنند که رایانه شما آلوده شده است.

به عنوان مثال، ممکن است از شما بخواهند که چک کنید آیا فایل های خاصی بر روی رایانه شما وجود دارد و قدم به قدم شما را راهنمایی کنند که چگونه آن فایل ها را پیدا کنید. هنگامی که شما این فایلها را پیدا کردید، تماس گیرنده شما را متقاعد میکند که این فایل ها نشانه این است که رایانه شما آلوده شده است، در حالیکه این فایل ها، فقط فایل های رایج سیستم هستند که بر روی هر رایانه ای وجود دارند. هنگامی که آنها شما را به این باور که رایانه شما آلوده شده است فریب دادند، آنها شما را به رفتن به وب سایتی و خرید نرم افزار امنیتی خودشان تحت فشار قرار داده و یا از شما می خواهند به آنها دسترسی از راه دور به رایانه تان را بدهید تا آنها بتوانند مشکل را حل کنند. اما نرم افزاری که آنها به شما میفروشند در واقع یک برنامه مخرب است. در صورت خرید و نصب آن نرم افزار نه تنها آنها شما را به آلوده

مهنـدسی اجتماعـی

کـردن رایانـه تـان فریـب داده انـد، حـتی شـما دسـتمزد اینکارشـان را هـم پرداخـت کـرده ایـد. اگـر شـما بـه آنهـا دسـترسی از راه دور بـه رایانـه تـان را بدهیـد تـا آن را تعمـیر کننـد، در واقعیـت آنهـا مـی خواهنـد کنـترل رایانـه شـما را بدسـت بگیرنـد و آن را آلـوده کننـد.

بـه خاطـر داشـته باشـید، حمـلات مهنـدسی اجتماعـی از ایـن دسـت بـه تمـاس هـای تلفـنی محـدود نیسـت؛ آنهـا مـی تواننـد تقریبـا بـا کمـک هـر فـن آوری اینـکار را بکننـد، از جملـه حمـلات فیشـینگ از طریـق ایمیـل، پیـام هـای متـنی، پیـام هـای فیـس بـوک، نوشـته هـای توییـتر و یـا چـت آنلایـن. مهـم درک مفهـوم مهنـدسی اجتماعـی اسـت.

یادگیری نحوه جلوگیری، تشخیص و توقف حملات مهندسی اجتماعی یکی از موثر ترین قدمهایی است که شما می توانید برای حفاظت از خود بردارید.

تشخیص / توقف حملات مهندسی اجتماعی

سـاده تریـن راه بـرای دفـاع در برابـر حمـلات مهنـدسی اجتماعـی دقـت و هوشـیاری بیشـتر اسـت. اگـر چـیزی مشـکوک بـه نظـر مـی رسـد و یـا درسـت بـه نظـر نمـی آیـد، ممکـن اسـت حملـه باشـد. برخـی از شـاخص هـای معمـول حملـه مهنـدسی اجتماعـی عبارتنـد از:

- بـرای شـما ایجـاد حـس فـوق العـاده اضطـراری میکننـد. اگـر شـما احسـاس مـی کنیـد تحـت فشـار بـرای اتخـاذ یـک تصمیـم بسـیار سریـع هسـتید، مشـکوک باشـید.
- کـسی درخواسـت اطلاعـاتی دارد کـه یـا نبایـد بـه آن دسـترسی داشـته باشـد یـا بایـد آن را میدانسـت و سـوال پرسـیدن از شـما بـرای دانسـتن آن اطلاعـات عجیـب اسـت.
- چـیزی بیـش از حـد خـوب بـه نظـر بیایـد. یـک مثـال معمـول ایـن اسـت کـه بـه شـما اطـلاع داده میشـود کـه شـما برنـده قرعـه کـشی شـدید، در حالیکـه شـما هرگـز حـتی وارد آن قرعـه کـشی نشـده ایـد.

در صـورت شـک بـه کـسی کـه در تـلاش اسـت تـا شـما را قربـانی یـک حملـه مهنـدسی اجتماعـی کنـد، بـا فـرد بیشـتر ارتبـاط برقـرار نکنیـد. اگـر کـسی بـه شـما تلفـن زده اسـت، قطـع کنیـد. اگـر کـسی بـا شـما بـه صـورت آنلایـن چـت میکنـد، مکالمـه را پایـان دهیـد. اگـر ایمیـلی اسـت کـه بـه آن اعتمـاد نداریـد، آن را حـذف کنیـد. اگـر ایـن حملـه در محـل کار یـا مرتبـط بـا کار باشـد، لازم اسـت تـا گـزارش آن را بـه مرکـز رایانـه و یـا تیـم امنیـت اطلاعـات اطـلاع دهیـد.

پیشگیری از حملات مهندسی اجتماعی آینده

خوشبختانه اقدامات احتیاطی وجود دارد که می توانید برای جلوگیری از حملات مهندسی اجتماعی در آینده استفاده کنید.

- **هرگـز کلمـه عبـور را بـا کـسی در میـان نگذاریـد:** هیـچ سـازمانی هرگـز بـا شـما تمـاس و درخواسـت رمـز عبـور نخواهـد کـرد. اگـر کـسی از شـما درخواسـت رمـز عبـور کـرد، آن یـک حملـه اسـت.

مهندسی اجتماعی

- **خیلی اطلاعات به دیگران ندهید:** هر چه هکر بیشتر در مورد شما بداند، آسان تر میتواند شما را پیدا و گمراه کند تا کاری که میخواهند را برایشان انجام دهید. حتی به اشتراک گذاری جزئیات کوچک در مورد خودتان به مرور زمان می توان با کنار هم قرار دادن اطلاعات کاملتری از شما بدست آورد و استفاده کرد. هر چه کمتر اطلاعات به اشتراک عمومی بگذارید، مخصوصا در سایت های رسانه های اجتماعی، یا انجمن های عمومی و گروههای ایمیلی، کمتر احتمال دارد که شما مورد حمله قرار بگیرید.

- **بررسی حقیقی بودن تماس:** ممکن است زمانی توسط بانک، شرکت کارت اعتباری، ارائه دهنده خدمات تلفن همراه و یا دیگر سازمانها به دلایل قانونی و موجه با شما تماس گرفته شود. اگر هر گونه شک و تردید دارید که آیا این تماس و درخواست اطلاعات حقیقی است، از فرد نامش و شماره داخلی را بپرسید. سپس شماره تلفن شرکت را از یک منبع قابل اعتماد دیگر پیدا کنید، مانند شماره پشت کارت اعتباری خود، شماره تلفن روی نامه دریافتی از بانک، یا شماره اعلام شده روی سایت بانک (مطمئن شوید که URL را در مرورگر خودتان تایپ میکنید). به این ترتیب هنگامی که با این سازمان تماس گرفتید، شما می دانید که واقعاً با خود آنها صحبت کرده اید. اگر چه این زحمت اضافه به نظر می رسد، ولی محافظت از اطلاعات شخصی و اختصاصی شما ارزش این کارها را دارد.

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

منابع

حملات فیشینگ پست الکترونیک: http://www.securingthehuman.org/ouch/2013#february2013

عضویت در شبکه های اجتماعی با خیال راحت: http://www.securingthehuman.org/ouch/2013#march2013

اجتناب از کلاه برداری: http://www.onguardonline.gov/topics/avoid-scams

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

ترجمه شده توسط : سعید میرجلیلی