ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

کلاهبرداری CEO

کلاهبرداری CEO چیست؟

مجرمان اینترنتی آب زیر کاه هستند. آنها دائما راههای جدیدی برای بدست آوردن چیزی که می خواهند می یابند. یکی از موثر ترین روشها هدف قرار دادن مردمی مثل شماست. حمله کنندگان سایبری یاد گرفته اند که افراد ناآگاه ضعیف ترین پیوند در هر سازمانی هستند اما فراموش کرده اند که افراد دانایی مثل خوانندگان OUCH! می توانند موثرترین دفاع یك سازمان باشند.

سردبیر مهمان

Angela Pappas مدیر بخش آگاهی و آموزش امنیت اطلاعات در موسسه Thomson Reuters است. آنجلا مسؤول برنامه سفیر، یادگیری الکترونیك و آموزش کارکنان در مورد فیشینگ می باشد.

مجرمان سایبری حمله جدیدی بنام کلاهبرداری CEO ایجاد کرده اند که بنام Business Email Compromise (BEC) هم شناخته می شود. در اینگونه حمله ها، حمله کننده ای سایبری وانمود می کند که CEO یا مدیر ارشد دیگری از سازمان است. مجرمان به کارمندانی مثل شما ایمیل می فرستند و بدین وسیله تلاش می کنند شما را به انجام کاری که نباید انجام دهید تشویق می کنند. اینگونه حمله ها بسیار کارا هستند چون مجرمان سایبری تحقیقاتشان را انجام می دهند. آنها وبسایت سازمان را برای کسب اطلاعاتی نظیر مکان سازمان، مدیران ارشد چه کسانی هستند و سازمان های دیگری که با آنها کار می کنید بررسی می کنند. سپس مجرمان سایبری هر چه می توانند اطلاعات در مورد همکارانتان از طریق وبسایت هایی نظیر LinkedIn، Facebook یا Twitter کسب می کنند. وقتی ساختار سازمانتان را دانستند، شروع به تحقیق و هدف گیری کارکنان مشخصی می کنند. آنها طعمه هایشان را بر اساس أهداف مشخصی انتخاب می کنند. اگر مجرم سایبری به دنبال پول باشد، ممکن است افرادی در بخش حسابداری را بعنوان طعمه انتخاب کنند. اگر بدنبال اطلاعات مالیاتی باشند، ممکن است افرادی از اداره استخدام را انتخاب کنند. اگر بخوانند به سرور های بانك اطلاعاتی دسترسی پیدا کنند، می توانند شخصی در بخش IT را مورد هدف قرار دهند.

وقتی که مشخص کردند که چه چیزی می خواهند و چه کسی هدف باشد،شروع به ساخت حمله هایشان می کنند. اغلب از فیشینگ نیزه ای استفاده می کنند. فیشینگ زمانیست که حمله کننده ای ایمیلی را به میلیون ها نفر به مقصود فریب دادن آنها به انجام کاری، مثلا باز کردن پیوست ایمیل آلوده یا بازدید از وب سایت های مخرب إرسال می کند. فیشینگ نیزه ای مشابه فیشینگ است. اما، بجای فرستادن ایمیلی عمومی به میلیونها نفر، آنها ایمیل هایی که بسیار واقعی به نظر می رسند و تشخیص غیر واقعی بودنشان بسیار سخت است می فرستند. این ایمیل

کلاهبرداری CEO

ها اغلب بنظر می رسد از طرف شخصی که شما می شناسید یا با او کار می کنید مثل دوستی همکار یا حتی رئیستان آمده است. ایمیل ها واقعی بنظر می رسند چون مثلا همان اصطلاحاتی که همکارانتان استفاده می کنند را بکار می برند، ممکن است از لوگوی سازمان یا حتی از امضای رسمی یکی از مدیران استفاده کنند. این ایمیل ها حس فوریت شگرفی ایجاد می کنند، خواستار عمل فوری شما بدون صحبت با کسی می شوند. هدف مجرم سایبری فشار بر شما به انجام کاری اشتباه با سرعت است. اینجا ۳ سناریو رایج را می آوریم:

کلاهبرداری CEO حمله ای قوی است که می تواند اکثر حفاظتهای امنیتی را کنار بزند. در نهایت شما بهترین دفاع خود هستید.

- **انتقال پول:** مجرم سایبری بدنبال پول است. یعنی آنها تحقیق می کنند و می دانند چه کسی در حساب های پرداختنی یا تیمی که امور مالی سازمان را مدیریت می کند کار می کند. مجرمان سپس ایمیلی تهیه می کنند و وانمود می کنند که رییس این افراد هستند. ایمیل به آنها می گوید موردی اضطراری است و پول باید سریعا به حساب مشخصی انتقال پیدا کند.

- **کلاهبرداری مالیاتی:** مجرمان سایبری می خواهند اطلاعاتی در مورد همکارانتان بدزدند و بدین ترتیب با جعل هویت کارکنان کلاهبرداری مالیاتی انجام دهند. آنها در مورد سازمان تحقیقات انجام می دهند و کسی که مسوول اطلاعات کارکنان است را شناسایی می کنند، مثلا فردی در قسمت استخدام. از آنجا مجرم سایبری ایمیل جعلی می فرستد و وانمود می کند مدیر ارشد است یا شخصی مشروع است ، و درخواست دریافت سریع اسنادی مشخص می کند.

- **جعل هویت وکالت:** همه کلاهبرداری های CEO شامل تنها ایمیل نیست. روشهای دیگر مثل تلفن ممکن استفاده شود. در این سناریو، مجرمان شروع به ایمیل زدن می کنند و وانمود می کنند مدیر ارشد هستند. توصیه می کنند که وکیلی بخاطر موضوعی اضطراری با شما تماس خواهد گرفت. سپس مجرم با شما تماس می گیرد و وانمود می کند همان وکیل است. این مجرم با صحبت از موضوعات محرمانه و حساس به زمان حس فوریت شگرفی در شما ایجاد می کند. این حس فوریت شما را به انجام بلافاصله عملی می فریبد.

کلاهبرداری CEO

محافظت از خود

پس چکار می توانید برای محافظت از خود و سازمانتان انجام دهید؟ هوشیاری بهترین دفاع است. اگر پیامی از رئیستان یا همکار دریافت می کنید و این ایمیل درست بنظر نمی رسد، ممکن است حمله باشه. سرنخ ها شامل حس اضطرار عجیب امضایی که درست بنظر نمی رسد، لحنی که هیچوقت انتظار نداشتید، یا اسمی در ایمیل که با اسمی که آن شخص واقعا شما را آنگونه می نامد متفاوت است. سرنخ دیگر حمله کننده از آدرس ایمیل یا شماره تلفنی که شما هرگز قبلا ندیده اید، یا از آدرس ایمیلی بسیار مشابه اما نه کاملا همان ایمیل رییس یا همکارتان استفاده می کند. وقتی مشکوک هستید، به آن شخص با شماره تلفن امن تماس بگیرید یا حضوری با او صحبت کنید (به ایمیل جواب ندهید) تا مطمئن شوید این ایمیل از طرف همان شخص است. هرگز خط مشی ها و روند های امنیتی را کنار نگذارید. سازمان ممکن است خط مشی هایی که روند مناسب برای اجازه دادن به انتقال وجه یا افشای اطلاعات محرمانه را بیان می کنند داشته باشد. درخواست هایی که تلاش می کنند این خ مشی ها را کنار بزنند صرفنظر از منبع شان باید مشکوک در نظر گرفته شوند و قبل از هرگونه اقدامی بررسی شوند. اگر چنین درخواستی دریافت می کنید و نمی دانید چکار انجام دهید فورا با مافوق تان، بخش پشتیبانی IT یا تیم امنیت تماس بگیرید.

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

مهندسی اجتماعی:	https://securingthehuman.sans.org/ouch/2014#november2014
فیشینگ:	https://securingthehuman.sans.org//ouch/2015#december2015
بدافزار چیست:	https://securingthehuman.sans.org/ouch/2016#march2016
تایید دو مرحله ای:	https://securingthehuman.sans.org/ouch/2015#september2015
نکته روز:	https://www.sans.org/tip-of-the-day

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