کلاهبرداری CEO

مجرمان سایبری حمله جدیدی بنام کلاهبرداری CEOایجاد کرده اند که بنام (BES) هم شناخته می شوند. 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 ها، 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 اطلاعاتی در مورد همکارانتان از طریق وبسایت هایی نظیر linkedIn , Facebookو..کسب می کنند. وقتی ساختار سازمانتان را دانستند، شروع به تحقیق و هدف گیری کارکنان مشخصی می کنند. آنها طعمه هایشان را براساس اهداف 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 را از اداره استخدام را انتخاب کنند. اگر بخواهند به سرور های بانک اطلاعاتی دسترسی پیدا کنند، می توانند شخصی در بخش IT را مورد هدف قرار دهند.

وقتی 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 زمانی است که حمله کننده ای ایمیلی را به میلیون ها نفر به مقصود فریب دادن آنها به انجام کاری، مثل باز کردن پیوست ایمیل آلوده یا بازدید از وب سایت های مخرب ارسال می کند.فیشینگ نیزه ای مشابه فیشینگ است. اما، بجای فرستادن ایمیل عمومی به میلیون ها نفر، آنها ایمیل هایی که بسیار واقعی به نظر می رسند را می فرستند. این ایمیل ها اغلب به نظر می رسد از طرف شخصی که میشناسید یا با او کار می کنید مثل دوست،همکار یا حتی رئیستان آمده است.ایمیل ها واقعی به نظر 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 خواستار عمل فوری شما بدون صحبت با کسی می شوند. هدف مجرم سایبری فشار بر شما به انجام کاری اشتباه با سرعت است. اینجا 3 سناریو رایج را می آوریم:

- 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 میکند. 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 بایدسریعا به حساب مشخصی انتقال پیدا کند.

- کلاهبرداری مالیاتی: مجرمان سایبری می خواهند اطلاعایت 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 فرستند و وانمود می کند مدیر ارشد است یا شخصی مشروع است،و درخواست دریافت سریع اسنادی مشخص می کند.

■ جعل هویت وکالت:همه کلاهبرداری هایCEO شامل تنها ایمیل نیست. روشهای دیگر مثل تلفن ممکن است 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 وبا صحبت از موضوعات محرمانه و حساس،حس فوریت شگرفی در شما ایجاد می کند.این حس فوریت شما را به انجام بلافاصله عملی می فریبد.

پس چه کاری می توانید برای حفاظت 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 باشد. سر نخ ها شامل حس اضطرار عجیب، امضایی که درست بنظر نمی رسد وغیره..

سرنخ دیگر حمله کننده از آدرس ایمیل یا شماره تلفنی که شما هرگز ندیده اید، یا از آدرس ایمیلی بسیار مشابه اما نه کاملا همان ایمیلی که 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 ایمل از طرف همان شخص است. هرگز خط مشی ها و روندهای 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 خط مشی ها را کنار بزنند صرف نظر از منبع شان باید مشکوک در نظر گرفته شوند. اگر چنین درخواستی دریافت کردید فورا با مافوق تان،بخشITیا تیم امنیت تماس بگیرید.