جنگ میان تروجان‌ها و یونانی‌ها به‌شدت گره‌خورده بود. پس از یک محاصره بی‌ثمر ۱۰ساله، یونانی‌ها به دستور ادیسه اسب چوبی عظیمی ساختند که به اسب تروا مشهور است. گروهی از مردان از جمله خود ادیسه در داخل آن اسب پنهان شدند. آنها با نقشه‌ای که ادیسه طراحی کرده بود، تروجان‌ها را فریب دادند تا اسب را به‌عنوان غنائم حاصل از نبرد وارد شهر کنند. تروجان‌ها اسب را به‌عنوان غنائم پیروزی به داخل شهر خود کشیدند. سرانجام در آن شب، نیروهای یونانی از اسب بیرون آمدند و دروازه‌ها را برای بقیه لشکر یونان باز کردند. یونانی‌ها وارد شهر شدند و شهر را ویران کردند و به جنگ پایان دادند.

سید علی فقیه موسوی
دانشجو مهندسی کامپیوتر
دانشکدگان فارابی دانشگاه تهران
faghih.mousavi@ut.ac.ir

مهندسی اجتماعی
Social Engineering

مهندسی اجتماعی چیست؟

مهندسی اجتماعی اصطلاحی است که برای طیف گسترده‌ای از فعالیت های مخرب بکار برده می‌شود که از طریق تعاملات انسانی انجام می‌شوند. حملات مهندسی اجتماعی به‌طورکلی در چند مرحله اتفاق می‌افتد. ابتدا قربانی موردنظر مورد بررسی قرار می‌گیرد تا اطلاعات موردنیاز برای نفوذ، مانند نقاط ورود احتمالی و یا پروتکل‌های امنیتی ضعیف، شناسایی شوند. سپس، مهاجم برای جلب‌اعتماد قربانی حرکت می‌کند و محرک هایی را برای اقدامات بعدی خود فراهم می‌کند. تا رویه‌های امنیتی را نقض کنند.

چیزی که مهندسی اجتماعی را خطرناک‌تر می‌کند این است که به‌جای تمرکز بر آسیب‌پذیری زیرساخت‌ها و سپرهای امنیتی، بر خطای انسانی متکی است. اشتباهات مرتکب شده توسط انسان‌ها خیلی کمتر قابل‌پیش بینی هستند و شناسایی و خنثی‌کردن آنها برای قربانی سخت‌تر از انواع دیگر نفوذ است.

در داستان اسب تروا ادیسه توانسته بود با ایده‌ای ناب راه نفوذ به داخل شهر تروجان‌ها را پیدا کند. ادیسه در واقع برای ورود به قلمرو شهر تروجان‌ها از نقاط ضعف خود آنها استفاده کرده بود. ساخت اسب تروا و در معرض دید تروجان‌ها قراردادن آن در واقع آنها را وادار کرده بود تا این اسب را به داخل شهر خود ببرند او پیش‌بینی کرده بود که تروجان ها با دیدن اسب تروا آن را غنیمت به شمار آورده و آن را به داخل شهر خود می‌برند این موضوع فارغ از اینکه یک داستان واقعی بوده و یا یک افسانه است می‌تواند به‌عنوان نمونه‌ای بسیار بسیار قدیمی از مهندسی اجتماعی شمرده شود.

سست ترین بخش هر سیستم برای نفوذ، کاربر انسانی است که با ان سیستم کار می کند.

مسیری که در ابتدا برای نفوذ به یک سیستم قابل‌تصور است، شکاندن سپر امنیتی آن سیستم می‌باشد در مهندسی اجتماعی اما به سراغ کاربر انسانی که با سیستم کار می‌کند می‌رویم. کاربر انسانی به‌مراتب خطای بیشتری از سپرهای امنیتی سیستم موردنظر دارد. به‌تبع انسان بودن همراه با یک سری ویژگی‌هایی است که برخی اوقات می‌تواند به ضرر امنیت سیستم تمام شود. برای نمونه عواطف و احساسات انسانی، تصمیمات لحظه‌ای و... از جمله مواردی هستند که می‌توانند آغازی برای تحت‌تأثیر قراردادن کاربر انسانی و نفوذ به یک سیستم باشند. می توان گفت ساده‌ترین راه نفوذ به هر سیستم کاربر انسانی است که با آن سیستم کار می‌کند. برای نمونه در داستان اسب تروا، ادیسه با صرف نیروی بسیار کمتر نسبت به آن که بخواهد سپرهای امنیتی شهر تروجان‌ها را بشکند و با استفاده از مهندسی اجتماعی در مقابل کاربرانی که در آن شهر وجود داشتند، توانست آنها را وادار کند که اسب را به داخل شهر خود ببرند.

مهندسی اجتماعی در فناوری اطلاعات

اگرچه چنین شکلی از حیله همیشه وجود داشته است، اما به طور قابل توجهی با فناوری‌های IT تکامل‌یافته است. استفاده روزافزون از فناوری های IT طبیعتاً منجر به افزایش استفاده از چنین تکنیک‌هایی و همچنین ترکیب آنها شده است تا جایی که اکثر حملات سایبری

امروزه شامل نوعی مهندسی اجتماعی می‌شوند. به‌طورکلی، تکنیک‌های مهندسی اجتماعی در زمینه فناوری اطلاعات را می‌توان از دو زاویه بررسی کرد:

استفاده از دست‌کاری روان‌شناختی

برای دسترسی بیشتر به سیستم هدف، مهاجم به سراغ دست‌کاری روان شناختی فرد مورد تهاجم می‌رود. به‌گونه‌ای که ابتدا خود فرد، نقاط حساس وی و مواردی که فرد را درگیر احساسات می‌کند را شناسایی کرده، سپس آنها رو مورد هدف قرار می‌دهد و نفوذ را از طریق آن‌ها صورت می‌دهد به‌عنوان‌مثال: مهاجم از طریق تماس تلفن و با جعل هویت، یک مشتری فریب می‌دهد و او را وادار به ورود به یک وب‌سایت مخرب می‌کند.

استفاده از تکنیک‌های فناوری اطلاعات

کاربر مهاجم به عنوان پشتیبانی از تکنیک‌های دست‌کاری روان‌شناختی برای دستیابی به هدفی خارج از حوزه فناوری اطلاعات، از خود این فناوری کمک می‌گیرد. به‌گونه‌ای که با استفاده از ابزارهای حوزه فناوری اطلاعات به سراغ فرد مورد تهاجم می‌رود. به‌عنوان‌مثال: مهاجم برای به دست‌آوردن اعتبار بانکی فرد، از طریق یک حمله فیشینگ (در ادامه به آن می‌پردازیم) اقدام می‌کند.

تکنیک‌های حمله مهندسی اجتماعی

حملات مهندسی اجتماعی اشکال متفاوتی دارند و می‌توانند در هر جایی که تعامل انسانی وجود دارد انجام شوند. چند مورد از رایج‌ترین شکل‌های حملات مهندسی اجتماعی در حوزه IT را بررسی می‌کنیم.

حملات Baiting (طعمه‌گذاری)

همان‌طور که از نامش پیداست، این حملات از یک وعده دروغین برای تحریک حرص و طمع یا کنجکاوی قربانی استفاده می‌کنند. آنها کاربران را به دامی می‌کشانند و اطلاعات شخصی آنها را می‌دزدند یا بدافزارها را وارد سیستم‌های آنها می‌کنند.

معمولاً در طعمه‌گذاری از رسانه‌های فیزیکی برای واردکردن بدافزارها به سیستم‌های هدف استفاده می‌شود. به‌عنوان‌مثال، مهاجم فلش آلوده به بدافزار را در مناطقی که قربانیان احتمالی آنها را می‌بینند (مانند آسانسور یا پارکینگ) رها می‌کنند. به‌گونه‌ای که در معرض دید قربانی قرار گیرد. طعمه ظاهری طبیعی دارد، یعنی ظاهر آن به‌گونه‌ای می‌باشد که قربانی آن را مورداستفاده قرار دهد. مثلاً: دارای برچسبی است که آن را به‌عنوان لیست اموال شرکت هدف نشان دهد. قربانیان از روی کنجکاوی طعمه را برمی‌دارند و آن را در رایانه محل کار یا خانه خود قرار می‌دهند و بدافزارها به طور خودکار روی سیستم آن‌ها نصب می‌شوند.

نکته قابل‌توجه این است که نفوذ با طعمه‌گذاری لزوماً نباید در دنیای فیزیکی انجام شود. شکل‌های مجازی از طعمه‌گذاری نیز وجود دارند. مانند: تبلیغاتی که به سایت‌های مخرب منتهی می‌شود و کاربران را به دانلود برنامه‌های آلوده تشویق می‌کند.

حملات Scareware

این حملات شامل بمباران قربانیان با هشدارهای نادرست و تهدیدهای ساختگی است. در این روش انبوهی از هشدارها و اخطارها برای قربانی ارسال می‌شود و احساسات وی را تحت‌تأثیر قرار می‌دهد. معمولاً افرادی که سست‌تر هستند هدف این‌گونه حملات قرار می گرند. به‌وسیله این هشدارها کاربران فریب می‌خورند و تصور می‌کنند سیستمشان به بدافزار آلوده شده است. کاربر به دلیل احساس ترسی که با آن درگیر شده نمی تواند خود را مدیریت کند. برای مثال: مجبور می‌شود که نرم‌افزاری را نصب کند که نه‌تنها هیچ سودی برایش ندارد؛ بلکه خود بدافزار است.

یک مثال رایج، بنرهایی است که با ظاهری قانونی هنگام گشت‌وگذار در وب در مرورگر شما ظاهر می‌شوند و متنی مانند "رایانه شما ممکن است به برنامه‌های مضر آلوده شده باشد" را نمایش می‌دهند. سپس پیشنهاد می‌کنند که ابزاری را برای شما نصب کند (که آلوده به بدافزار است)، یا شما را به یک سایت مخرب هدایت می‌کنند که از طریق آن رایانه شما آلوده می‌شود.

حملات Phishing

به‌عنوان یکی از محبوب‌ترین انواع حملات مهندسی اجتماعی به شمار می‌روند. کلاهبرداری‌های فیشینگ، کمپین‌های ایمیل یا پیام‌های متنی هستند که باهدف ایجاد حس فوریت، کنجکاوی یا ترس در قربانیان انجام می‌شوند. سپس آنها را وادار می‌کنند تا اطلاعات حساس خود را فاش کنند، روی پیوندهای وب‌سایت‌های مخرب کلیک کنند یا پیوست های حاوی بدافزار را باز کنند.

یک مثال ایمیلی است که برای کاربران یک سرویس آنلاین ارسال می شود و به آنها از مشکلی هشدار می‌دهد که نیاز به اقدام فوری از سوی آنها دارد، مانند تغییر رمز عبور. این پیام شامل پیوندی به یک وب‌سایت غیرقانونی می‌باشد. (تقریباً از نظر ظاهری شبیه به نسخه قانونی آن است) که کاربر ناآگاه را وادار می‌کند تا اطلاعات فردی و رمز عبور جدید خود را وارد کند. پس از ارسال فرم، اطلاعات برای مهاجم ارسال می‌شود. مهاجم به‌این‌ترتیب به صفحه شخصی قربانی در آن سرویس آنلاین دسترسی پیدا می‌کند.

حملات Peretexing

در این نوع از حملات مهاجم اطلاعاتی را از طریق یک سری دروغ‌های هوشمندانه به دست می‌آورد. این کلاهبرداری اغلب توسط فردی آغاز می‌شود که وانمود می‌کند به اطلاعات حساس قربانی نیاز دارد تا یک وظیفه مهم را انجام دهد. افرادی که دانش بالایی ندارند بیشتر درگیر این نوع حملات می‌شوند. مهاجم ابتدا با جلب‌اعتماد قربانی خود به‌وسیله دزدیدن هویت افرادی که دارای اختیارات حق شناخت هستند (مانند پلیس، مقامات بانکی) شروع می‌کند. وی سؤالاتی را می‌پرسد که ظاهراً برای تأیید هویت قربانی موردنیاز است و از طریق آنها اطلاعات شخصی مهمی را جمع‌آوری می‌کند. انواع اطلاعات و سوابق لازم با استفاده از این کلاهبرداری جمع‌آوری می‌شوند. مانند: شماره ملی، آدرس، شماره‌تلفن های شخصی، شماره‌حساب و سوابق بانکی.

پیشگیری از حملات مهندسی اجتماعی

مهندسان اجتماعی احساسات انسانی مانند کنجکاوی یا ترس را دست کاری می‌کنند تا نقشه‌ها خود را اجرا کنند و قربانیان را به دام خود بکشانند؛ بنابراین، هر زمان که احساس خطر می‌کنید، از یک ایمیل نگران می‌شوید یا به پیشنهادی که در یک وب‌سایت نمایش داده می‌شود جذب می‌شوید هوشیار باشید. هوشیار بودن می‌تواند به شما کمک کند از خود در برابر اکثر حملات مهندسی اجتماعی که در حوزه دیجیتال رخ می‌دهند محافظت کنید.

پیشگیری‌های فردی:

ایمیل‌ها و پیوست‌های منابع مشکوک را باز نکنید

اگر فرستنده موردنظر را نمی‌شناسید، نیازی به پاسخ‌دادن به ایمیل ندارید. حتی اگر آنها را می‌شناسید و به پیام آنها مشکوک هستید، اخبار را از منابع دیگر، مانند تلفن یا مستقیماً از سایت ارائه‌دهنده خدمات، بررسی و تأیید کنید. به یاد داشته باشید که آدرس‌های ایمیل در حملات همیشه جعلی هستند. حتی ایمیلی که ظاهراً از یک منبع قابل‌اعتماد می آید ممکن است در واقع توسط یک مهاجم آغاز شده باشد.

از احراز هویت چندعاملی استفاده کنید

یکی از ارزشمندترین اطلاعاتی که مهاجمان به دنبال آن هستند، اطلاعات کاربری حساب شما است. استفاده از احراز هویت چندعاملی به محافظت از حساب شما در صورت به‌خطرافتادن سیستم کمک می‌کند.

مراقب پیشنهادات وسوسه‌انگیز باشید

اگر پیشنهادی خیلی غیرطبیعی به نظر می‌رسد، قبل از پذیرش آن به عنوان واقعیت، دو بار فکر کنید. جستجوی موضوع در گوگل حتی به شما کمک می‌کند تا به‌سرعت تشخیص دهید که با یک پیشنهاد قانونی یا یک دام سروکار دارید.

نرم‌افزارهای ضد بدافزار خود را به‌روز نگه دارید

مطمئن شوید که به‌روزرسانی‌های خودکار انجام شده است. به‌صورت دوره‌ای بررسی کنید تا مطمئن شوید که تمامی به‌روزرسانی‌ها اعمال شده‌اند و سیستم خود را برای تهدیدهای احتمالی اسکن کنید.

پیشگیری‌های سازمانی :

ایمن‌سازی

در ابتدا هر سازمانی باید دارایی‌های حیاتی خود را شناسایی کرده و سیاست‌ها و پروتکل‌های امنیتی مناسب با آن را اجرا کند. در صورت لزوم، این موارد باید با استفاده از فناوری‌های بروز تقویت شوند. ایجاد سپر امنیتی قوی اولین مرحله برای جلوگیری از نفوذ می‌باشد.

آموزش کارکنان

همان‌طور که پیش‌تر به آن پرداختیم حملات مهندسی اجتماعی از طریق نفوذ به کاربران زیر مجموعه سازمان هدف صورت می‌گیرد. سازمان‌ها موظف‌اند کارکنان خود را آموزش دهند و آنها را از خطرات احتمالی آگاه کنند. کاربران در واقع می‌بایست با روش‌های پیشگیری فردی حملات مهندسی اجتماعی آشنایی کامل داشته باشند.

تست نفوذ

در نهایت روشی که برای سنجش میزان امنیت یک سازمان وجود دارد تست نفوذ است. به‌وسیله آن شرکت هایی که این تست را ارائه می‌دهند اقدام به نفوذ به سازمان شما می‌کنند و نتایج حاصل از این حملات را در اختیار شماقرار می‌دهند تا نقاط ضعف سیستم امنیتی خود را تقویت کنید.

منابع

/https://www.enisa.europa.eu
/https://www.imperva.com