مهندسی اجتماعی

Social Engineering

مهندسی اجتماعی چیست؟

مهندسی اجتماعی لزوماً فنی نیست

بسیاری از حملات مهندسی اجتماعی نیازی به اطلاعات فنی تخصصی ندارند و لازم نیست تا یک متخصص رایانه و یک هکر حرفه‌ای به شما حمله کند. باید نسبت به محیط اطراف آگاه بود؛ چرا که هریک از افراد جامعه می‌تواند نقش یک مهاجم را ایفا کند.

مهاجم شما را در حالت‌های خاص روانی قرار می‌دهد

حملات مهندسی اجتماعی شما را در حالت‌هایی نظیر اضطراب، هیجان، ترس و به صورت کلی حالات خاص روانی قرار می‌دهند تا تمرکز و توان تصمیم‌گیری شما را کاهش دهند. لذا باید از تصمیم‌گیری‌های شتاب‌زده پرهیز کنید.

حملات مهندسی اجتماعی فریبنده هستند

در اکثر حملات مهندسی اجتماعی، پیشنهاداتی به شما ارائه می‌شود که در نگاه اول، بسیار پرسود و جذاب به نظر می‌آیند. باید تلاش کرد تا بر وسوسه پاسخگویی به این دسته از پیشنهادات غلبه کرد؛ چراکه برخی از آنها، طعمه‌هایی برای حملات مهندسی اجتماعی هستند.

حملات صیادی و هرزنامه

- در یک حمله صیادی، ابتدا مهاجم طعمه خود را که معمولا پیامی جعلی با ظاهری مشابه پیامهای یک نهاد معتبر (نظیر بانک) است را برای تعداد زیادی از کاربران ارسال می‌نماید.
- در گام بعد مهاجم منتظر می‌ماند، به این امید که افراد هدف حمله، فریب خورده و خود را در دام وی گرفتار نمایند. حال ممکن است این کار با کلیک بر روی یک پیوند باشد یا ارسال مشخصات فردی.

طعمه‌گذاری

- طعمه‌گذاری با استفاده از ابزارهای فیزیکی انجام می‌شود. مهاجم وسایلی نظیر لوح فشرده و فلش دیسک که حاوی بدافزار هستند را به عناوین مختلفی نظیر هدایای تبلیغاتی و مطالب مفید و جذاب در اختیار قربانیان قرار می‌دهد.
- در مرحله بعد، قربانیان این وسایل را به رایانه‌های خود متصل کرده و با این کار، بدافزارهای مهاجم را اجرا می‌نمایند. به این ترتیب، مسیر دسترسی مهاجم به اطلاعات موجود بر روی این رایانه ها فراهم می‌شود.

دستاویزسازی

- در حملات دستاویزسازی، اولین گام مهاجم، هدف قرار دادن افراد خاص و کسب اطلاعات در مورد آن‌هاست.
- گام بعد، ارتباط با قربانی است. مهاجم با بازگوی اطلاعاتی که از قربانی به دست آورده است، اعتماد وی را جلب کرده و به او تلقین می‌نماید که دارای اشتراکات زیادی با یکدیگر هستند. در نهایت، اعتماد جلب‌شده از قربانی سبب می‌شود تا وی، اطلاعاتی که در اختیار افراد غریبه قرار نمی‌دهد را در به سادگی در اختیار مهاجم بگذارد.

چطور از حملات مصون بمانیم؟!

آموزش مهمترین اصل است

ساده‌ترین و کارآمدترین راه‌کار برای مقابله با حملات مهندسی اجتماعی، آموزش افراد و افزایش آگاهی آن‌ها است. در صورتی که تک‌تک افراد، آگاهی کافی نسبت به محیط خود داشته باشند، در لحظات حساس به درستی و بر اساس اصول تصمیم‌گیری کنند و فریب وسوسه‌های مهاجمان را نخورند، دیگر هیچ حمله مهندسی اجتماعی موفقی رخ نخواهد داد!

آگاه باشید چه چیزی را منتشر می‌کنید

مهمترین منبع اطلاعاتی مهاجمان در حملات مهندسی اجتماعی، مطالبی است که در مورد افراد در منابعی نظیر اینترنت قرار دارد و به سادگی قابل دسترس است؛ به‌ویژه اطلاعاتی که خود فرد در شبکه‌های اجتماعی منتشر می‌کند. در صورتی که افراد با مطالب شخصی خود آگاهانه رفتار کرده و آنها را در معرض دید عموم قرار ندهند، امکان استفاده از این اطلاعات در حملات مهندسی اجتماعی نیز کاهش خواهد یافت.

داشته‌های خود را بشناسید

نکته مهمی که برای مقابله با حملات مهندسی اجتماعی باید به آن توجه داشت، شناخت اطلاعات ارزشمند و داشته‌های فردی و سازمانی است. در صورتی که هر فرد بداند کدامیک از اطلاعات وی می‌تواند چه ارزشی برای مهاجمان داشته باشد، در زمان ارائه این اطلاعات به دیگران با احتیاط بیشتری عمل کرده و در نتیجه، احتمال موفقیت حملات مهندسی اجتماعی کاهش می‌یابد.

سیاست‌های امنیتی تعیین کنید

یکی از راهکارهای مؤثر که برای افزایش قدرت و دقت تصمیم‌گیری افراد وجود دارد، آن است که اعضای یک مجموعه همگی از سیاست‌های مشخص و مدونی پیروی نمایند. برای مثال، اگر یک سازمان سیاست‌های امنیتی مشخصی را به کارمندان خود ارائه نماید و آنان نیز از سیاست‌های مذکور پیروی نمایند، اشتباهات فردی کاهش یافته و کل مجموعه در برابر حملات مهندسی اجتماعی امن‌تر می‌شود.

سازمان فناوری اطلاعات ایران
مرکز ماهر
مرکز راه کارهای اطلاعاتی هوشمند