به نام خدا

نقش مهندسی اجتماعی در حملات باج افزاری و تهدیدات نوین و روش های پیشگیرانه

مولف:

مهدی حقدادی

انتشارات ارسطو

(سازمان چاپ و نشر ایران – ۱۴۰۳)

نسخه الکترونیکی این اثر در سایت سازمان چاپ و نشر ایران و اپلیکیشن کتاب رسان موجود می باشد

chaponashr.ir

سرشناسه : حقدادی، مهدی، ۱۳۶۸-
عنوان و نام پدیدآور : نقش مهندسی اجتماعی در حملات باج افزاری و تهدیدات نوین و روش های پیشگیرانه/ مولف مهدی حقدادی.
مشخصات نشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)، ۱۴۰۳.
مشخصات ظاهری : ۱۲۰ ص.
شابک : ۴-۰۹۳-۴۵۵-۶۲۲-۹۷۸
وضعیت فهرست نویسی : فیپا
موضوع : مهندسی اجتماعی - حملات باج افزاری - تهدیدات نوین - روش های پیشگیرانه
رده بندی کنگره : HV۶۲۵۷
رده بندی دیویی : ۳۶۴/۱۱۱
شماره کتابشناسی ملی : ۹۹۳۳۳۹۵
اطلاعات رکورد کتابشناسی : فیپا

نام کتاب : نقش مهندسی اجتماعی در حملات باج افزاری و تهدیدات نوین و روش های پیشگیرانه
مولف : مهدی حقدادی
ناشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)
صفحه آرایی، تنظیم و طرح جلد: پروانه مهاجر
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : اول - ۱۴۰۳
چاپ : زبرجد
قیمت : ۱۲۰۰۰۰ تومان
فروش نسخه الکترونیکی - کتاب‌رسان :
https://chaponashr.ir/ketabresan
شابک : ۴-۰۹۳-۴۵۵-۶۲۲-۹۷۸
تلفن مرکز پخش : ۰۹۱۲۰۲۳۹۲۵۵
www. chaponashr. ir

فهرست

فصل اول

مقدمه‌ای بر مهندسی اجتماعی و جرایم سایبری

مهندسی اجتماعی یکی از روش‌های پرکاربرد در دنیای جرایم سایبری است که از طریق دستکاری روان‌شناختی افراد، اطلاعات حساس آن‌ها را به دست می‌آورد. برخلاف حملات فنی که بر نقاط ضعف نرم‌افزاری یا سخت‌افزاری تمرکز دارند، مهندسی اجتماعی بر نقاط ضعف انسانی تأکید دارد و تلاش می‌کند با فریب، متقاعدسازی یا ایجاد اعتماد، فرد را وادار به افشای اطلاعات مهم کند. این روش در بسیاری از حملات سایبری، از جمله فیشینگ، جعل هویت و کلاهبرداری‌های اینترنتی به کار می‌رود. شناخت این تهدیدات و آگاهی‌بخشی به کاربران یکی از مهم‌ترین راهکارهای مقابله با این نوع حملات است. همتی، ع. (۱۳۹۵).

مهاجمان سایبری از تکنیک‌های مهندسی اجتماعی برای سوءاستفاده از اعتماد و اطلاعات افراد استفاده می‌کنند. این روش‌ها به دلیل سادگی و اثربخشی، در بسیاری از حملات سایبری به کار می‌روند. در این نوع حملات، به جای نفوذ به سیستم‌ها از طریق آسیب‌پذیری‌های فنی، مهاجم تلاش می‌کند تا از طریق فریب یا متقاعدسازی، فرد را وادار به افشای اطلاعات حساس کند. از جمله رایج‌ترین روش‌های مورد استفاده در مهندسی اجتماعی می‌توان به تماس‌های تلفنی جعلی، پیام‌های ایمیلی فریبنده، لینک‌های مخرب و استفاده از هویت‌های جعلی اشاره کرد.یکی از تکنیک‌های رایج، جعل هویت است که در آن مهاجم خود را به‌عنوان یک فرد قابل اعتماد معرفی می‌کند. برای مثال، یک کلاهبردار ممکن است با تقلید از یک مقام اجرایی در سازمان، از کارکنان بخواهد که اطلاعات ورود به سیستم را ارائه دهند یا پرداخت مالی انجام دهند. این نوع حملات معمولاً در قالب ایمیل‌های جعلی یا تماس‌های تلفنی انجام می‌شود. مهاجم ممکن است با بیان یک سناریوی اضطراری، قربانی را تحت فشار قرار دهد تا سریعاً اطلاعات موردنظر را فاش کند.روش دیگر، ارسال لینک‌های فریبنده در ایمیل‌ها یا پیام‌های متنی است. این لینک‌ها معمولاً به سایت‌های جعلی هدایت می‌شوند که ظاهری مشابه وب‌سایت‌های معتبر دارند. هنگامی که کاربر اطلاعات ورود خود را در این سایت‌ها وارد می‌کند، مهاجم به‌راحتی به این اطلاعات

دسترسی پیدا می‌کند. در برخی موارد، این لینک‌ها حاوی بدافزارهایی هستند که پس از کلیک کاربر، روی دستگاه او نصب شده و اطلاعات او را سرقت می‌کنند. آقابابایی، ح. (۱۳۹۷).

در برخی حملات مهندسی اجتماعی، مهاجم تلاش می‌کند تا قربانی را به دانلود و نصب نرم‌افزارهای آلوده ترغیب کند. برای مثال، ممکن است فردی ایمیلی دریافت کند که حاوی یک پیوست به ظاهر بی‌ضرر است، اما در واقع این فایل حاوی بدافزار است. بدافزارها می‌توانند برای سرقت اطلاعات، ثبت فعالیت‌های کاربر، یا ایجاد دسترسی غیرمجاز به سیستم قربانی مورد استفاده قرار گیرند.یکی دیگر از روش‌های حمله، نفوذ فیزیکی به محیط‌های کاری یا سازمانی است. در این روش، مهاجم ممکن است با پوشیدن لباس کارمندان، نیروهای خدماتی یا حتی مأموران امنیتی، وارد محیط سازمان شود و به اطلاعات حساس دسترسی پیدا کند. برخی از مهاجمان حتی از طریق تعاملات اجتماعی و ایجاد روابط دوستی با کارمندان، اطلاعات محرمانه را استخراج می‌کنند.

یکی از راه‌های مؤثر برای مقابله با این نوع حملات، آموزش و افزایش آگاهی کارکنان و کاربران است. سازمان‌ها باید به‌طور منظم دوره‌های آموزشی در زمینه امنیت سایبری برگزار کنند و به کارمندان بیاموزند که چگونه علائم یک حمله مهندسی اجتماعی را تشخیص دهند. یکی از روش‌های پیشنهادی، اجرای تست‌های امنیتی داخلی است که در آن، سازمان‌ها خود به‌طور آزمایشی حملات مهندسی اجتماعی را شبیه‌سازی کرده و آگاهی کارکنان را ارزیابی می‌کنند.علاوه بر آموزش، استفاده از فناوری‌های امنیتی نیز می‌تواند به کاهش خطرات ناشی از مهندسی اجتماعی کمک کند. به‌کارگیری احراز هویت چندمرحله‌ای (MFA) یکی از مؤثرترین روش‌ها برای جلوگیری از دسترسی غیرمجاز به حساب‌های کاربری است. در این روش، علاوه بر رمز عبور، از یک لایه امنیتی اضافی مانند پیامک تأیید، اثر انگشت یا کدهای یک‌بارمصرف استفاده می‌شود.

همچنین، فیلترهای پیشرفته ایمیل و نرم‌افزارهای ضد فیشینگ می‌توانند پیام‌های مخرب را شناسایی و مسدود کنند. سازمان‌ها باید از سیاست‌های امنیتی سخت‌گیرانه برای کنترل دسترسی به اطلاعات حساس استفاده کنند و دسترسی کارکنان را بر اساس نیازهای واقعی آن‌ها تنظیم نمایند. ایزدی، م. (۱۳۹۵).

فرهنگ امنیتی در سازمان‌ها باید تقویت شود و کارکنان تشویق شوند که هرگونه فعالیت مشکوک را گزارش دهند. بسیاری از حملات مهندسی اجتماعی به دلیل ترس یا ناآگاهی کاربران از

پیامدهای امنیتی موفقیت‌آمیز هستند. ایجاد یک محیط کاری که در آن کارکنان بتوانند بدون نگرانی، تهدیدهای امنیتی را گزارش دهند، می‌تواند به جلوگیری از وقوع حملات کمک کند.
یکی دیگر از اقدامات پیشگیرانه، استفاده از تست‌های امنیتی و ارزیابی‌های دوره‌ای است. سازمان‌ها می‌توانند از شرکت‌های متخصص در حوزه امنیت سایبری برای انجام تست‌های نفوذپذیری استفاده کنند تا نقاط ضعف احتمالی شناسایی شده و اقدامات اصلاحی انجام شود.همچنین، سازمان‌ها باید به‌روزرسانی‌های امنیتی را به‌طور مداوم انجام دهند و از ابزارهای پیشرفته برای شناسایی و مقابله با تهدیدات استفاده کنند. به‌روزرسانی نرم‌افزارها و سیستم‌های امنیتی می‌تواند به جلوگیری از سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده کمک کند.در کنار همه این تدابیر، کاربران نیز باید مسئولیت‌پذیر باشند و در استفاده از اطلاعات شخصی خود احتیاط کنند. نباید روی لینک‌های مشکوک کلیک کرد یا اطلاعات حساس را در اختیار افراد ناشناس قرار داد. همچنین، استفاده از رمزهای عبور قوی و عدم استفاده از رمزهای تکراری در حساب‌های مختلف، می‌تواند احتمال دسترسی غیرمجاز به اطلاعات را کاهش دهد. همتی، ع. (۱۳۹۵).

در مجموع، مهندسی اجتماعی یکی از خطرناک‌ترین روش‌های حمله در دنیای دیجیتال است که بر ضعف‌های انسانی تکیه دارد. مقابله با این نوع تهدیدات نیازمند ترکیبی از آموزش، فناوری‌های امنیتی و سیاست‌های سازمانی مناسب است. هر فرد و سازمانی باید آگاه باشد که امنیت اطلاعات به رعایت نکات ایمنی و افزایش آگاهی بستگی دارد. با اتخاذ رویکردی جامع در زمینه امنیت سایبری، می‌توان از بسیاری از حملات مهندسی اجتماعی جلوگیری کرد و از اطلاعات حساس محافظت نمود. جعفری، ج. (۱۳۹۶).

تعریف و اهمیت مهندسی اجتماعی

مهندسی اجتماعی به مجموعه‌ای از روش‌ها و تکنیک‌هایی گفته می‌شود که مهاجمان از آن‌ها برای فریب افراد و دسترسی غیرمجاز به اطلاعات یا سیستم‌های امنیتی استفاده می‌کنند. این روش‌ها مبتنی بر فریب و سوءاستفاده از اعتماد انسان‌ها است، به‌جای آن‌که بر نقاط ضعف فنی سیستم‌های کامپیوتری تمرکز داشته باشد. در واقع، مهندسی اجتماعی نوعی دستکاری روان‌شناختی است که باعث می‌شود افراد بدون آنکه متوجه شوند، اطلاعات حساس خود را در اختیار افراد غیرمجاز قرار دهند.

اهمیت مهندسی اجتماعی در دنیای امروز بسیار زیاد است، زیرا اکثر حملات سایبری موفق از طریق این روش انجام می‌شوند. برخلاف هک‌های سنتی که نیاز به دانش عمیق فنی دارند، مهندسی اجتماعی به مهارت‌های ارتباطی و روان‌شناختی متکی است. حملات مبتنی بر مهندسی اجتماعی معمولاً هزینه‌ی کمتری دارند و احتمال موفقیت آن‌ها بیشتر است، زیرا کاربران اغلب از خطرات احتمالی آگاهی ندارند.یکی از دلایل اهمیت مهندسی اجتماعی این است که سیستم‌های امنیتی امروزی به‌شدت تقویت شده‌اند و نفوذ به آن‌ها دشوارتر شده است. بنابراین، مهاجمان به‌جای تلاش برای شکستن دیوارهای امنیتی، به فریب و اغوای کاربران متوسل می‌شوند. به‌عنوان مثال، ارسال ایمیل‌های فیشینگ که حاوی لینک‌های جعلی هستند، یکی از رایج‌ترین روش‌های مورد استفاده در مهندسی اجتماعی است. همتی، ع. (۱۳۹۵).از دیگر عوامل اهمیت مهندسی اجتماعی می‌توان به نقش آن در حملات هدفمند اشاره کرد. در این نوع حملات، مهاجمان اطلاعات دقیقی از قربانیان جمع‌آوری کرده و با استفاده از اطلاعات شخصی، اعتماد آن‌ها را جلب می‌کنند. برای مثال، یک مهاجم ممکن است خود را به‌عنوان همکار یا مدیر شرکت معرفی کرده و از طریق تماس تلفنی، اطلاعات محرمانه را دریافت کند.

تأثیر مهندسی اجتماعی فراتر از حوزه‌های فناوری اطلاعات است. این تکنیک‌ها در حوزه‌های مالی، سیاسی و حتی روابط شخصی نیز کاربرد دارند. برای مثال، کلاهبرداران ممکن است با استفاده از روش‌های مهندسی اجتماعی، مردم را متقاعد کنند که در یک طرح سرمایه‌گذاری تقلبی شرکت کنند یا اطلاعات بانکی خود را ارائه دهند.یکی از مهم‌ترین چالش‌های مهندسی اجتماعی این است که هیچ ابزار امنیتی کاملاً قادر به جلوگیری از آن نیست. حتی پیشرفته‌ترین نرم‌افزارهای امنیتی نیز نمی‌توانند مانع از فریب کاربران شوند. به همین دلیل، آگاهی و آموزش کاربران در این زمینه ضروری است.

برای مقابله با مهندسی اجتماعی، سازمان‌ها باید برنامه‌های آموزشی جامعی اجرا کنند و به کارکنان خود روش‌های شناسایی حملات را بیاموزند. علاوه بر این، استفاده از پروتکل‌های امنیتی مانند احراز هویت چندمرحله‌ای، محدود کردن دسترسی به اطلاعات حساس و ایجاد فرآیندهای تأیید هویت می‌تواند به کاهش ریسک حملات کمک کند.مهندسی اجتماعی یکی از مهم‌ترین تهدیدات امنیتی در دنیای دیجیتال است که می‌تواند خسارات سنگینی به افراد و سازمان‌ها وارد کند. آگاهی از روش‌های این نوع حملات و اتخاذ راهکارهای پیشگیرانه می‌تواند از بسیاری از تهدیدات جلوگیری کند و امنیت اطلاعات را افزایش دهد.

تاریخچه و تحول حملات مبتنی بر مهندسی اجتماعی

حملات مبتنی بر مهندسی اجتماعی قدمتی به اندازه‌ی تاریخ تعاملات انسانی دارند، اما با پیشرفت تکنولوژی و دیجیتالی شدن ارتباطات، این حملات نیز پیچیده‌تر و گسترده‌تر شده‌اند. در دوران باستان، کلاهبرداری و فریب افراد برای کسب اطلاعات یا منابع رایج بود. به عنوان مثال، داستان اسب تروا نمونه‌ای کلاسیک از یک حمله‌ی مهندسی اجتماعی است که در آن، یونانیان با استفاده از یک حیله‌ی فریبنده، به شهر تروا نفوذ کردند. کاظمی، ت. (۱۳۹۶).با گذر زمان و شکل‌گیری سازمان‌ها و حکومت‌ها، جاسوسی و فریب‌کاری به‌عنوان ابزارهایی برای دسترسی به اطلاعات محرمانه به کار گرفته شد. در قرون وسطی، فرستادن پیام‌های جعلی، جعل هویت و سوءاستفاده از اعتماد مردم روش‌هایی بود که برای جمع‌آوری اطلاعات یا فریب مقامات استفاده می‌شد. در دوره‌ی جنگ‌های جهانی اول و دوم، مهندسی اجتماعی به شکلی گسترده برای فریب دشمنان و کسب اطلاعات نظامی مورد استفاده قرار گرفت. یکی از معروف‌ترین نمونه‌ها، عملیات "دختر فریبکار" بود که در آن نیروهای متفقین از روش‌های فریب روان‌شناختی برای گمراه کردن نیروهای آلمانی استفاده کردند.

با ظهور فناوری‌های ارتباطی مانند تلفن و تلگراف، روش‌های مهندسی اجتماعی نیز تغییر یافتند. در دهه‌های ۱۹۶۰ و ۱۹۷۰، مجرمان و هکرها از طریق تماس‌های تلفنی به کارکنان شرکت‌ها نزدیک شده و با فریب آن‌ها، اطلاعات حساس مانند رمزهای عبور و اطلاعات حساب‌ها را به دست می‌آوردند. در آن دوران، اصطلاح "فریکینگ (Phreaking) "برای اشاره به تکنیک‌های فریب‌کاری در شبکه‌های مخابراتی رواج یافت و افراد مشهوری مانند کوین میتنیک از این روش‌ها برای نفوذ به سیستم‌های تلفنی و کامپیوتری استفاده می‌کردند. جعفری، ج. (۱۳۹۶).

در دهه‌ی ۱۹۹۰ و اوایل ۲۰۰۰، با گسترش اینترنت و ایمیل، روش‌های مهندسی اجتماعی پیچیده‌تر شدند. حملاتی مانند فیشینگ (Phishing) برای اولین بار ظاهر شدند که در آن، مهاجمان از ایمیل‌های جعلی برای فریب کاربران و سرقت اطلاعات ورود به حساب‌های کاربری آن‌ها استفاده می‌کردند. یکی از اولین حملات فیشینگ بزرگ، در اوایل دهه‌ی ۲۰۰۰ اتفاق افتاد که در آن، مهاجمان با ارسال ایمیل‌هایی که خود را به‌عنوان بانک‌های معتبر معرفی می‌کردند، اطلاعات مالی کاربران را سرقت کردند.

در سال‌های بعد، با پیشرفت شبکه‌های اجتماعی، حملات مهندسی اجتماعی وارد فاز جدیدی شدند. مهاجمان از اطلاعاتی که کاربران به‌صورت عمومی در پلتفرم‌هایی مانند فیس‌بوک، توییتر

و لینکدین منتشر می‌کردند، برای ایجاد حملات هدفمند استفاده کردند. به‌عنوان مثال، در حملات "فیشینگ هدفمند(Spear Phishing) "، مهاجمان ایمیل‌های جعلی را برای قربانیان ارسال می‌کردند که به‌شدت با اطلاعات شخصی آن‌ها تطابق داشت و باعث می‌شد احتمال فریب خوردن افراد افزایش یابد.

در سال‌های اخیر، با گسترش اینترنت اشیا (IoT) و هوش مصنوعی، مهندسی اجتماعی نیز تحول چشمگیری پیدا کرده است. امروزه، مهاجمان از ربات‌های هوشمند برای ارسال پیام‌های جعلی در پیام‌رسان‌ها و شبکه‌های اجتماعی استفاده می‌کنند. همچنین،) Deepfakeتکنولوژی جعل عمیق) به‌عنوان یک تهدید جدید مطرح شده است که می‌تواند صدای افراد را شبیه‌سازی کرده و تماس‌های تلفنی جعلی ایجاد کند.در مجموع، تاریخچه‌ی مهندسی اجتماعی نشان می‌دهد که این روش‌ها همواره در حال تکامل بوده‌اند و با تغییر فناوری‌های ارتباطی، تاکتیک‌های جدیدی برای فریب افراد به کار گرفته شده‌اند. با پیشرفت تکنولوژی و افزایش وابستگی به فضای دیجیتال، پیش‌بینی می‌شود که حملات مبتنی بر مهندسی اجتماعی در آینده حتی پیچیده‌تر و خطرناک‌تر شوند. آقابابایی، ح. (۱۳۹۷).

در سال‌های اخیر، ظهور فناوری‌های نوین مانند یادگیری ماشینی و هوش مصنوعی، مهندسی اجتماعی را وارد مرحله‌ای جدید کرده است. امروزه مهاجمان قادرند با استفاده از تحلیل داده‌های کلان (Big Data) و الگوریتم‌های پیشرفته، اطلاعات دقیقی از رفتار کاربران به دست آورند و حملات خود را به شکل شخصی‌سازی‌شده اجرا کنند. برای مثال، آن‌ها از ابزارهای هوش مصنوعی برای تقلید سبک نوشتاری افراد در ایمیل‌ها یا پیام‌های متنی استفاده می‌کنند تا قربانیان را به پاسخ‌گویی و ارائه اطلاعات حساس ترغیب کنند.یکی از جدیدترین روش‌های مهندسی اجتماعی، استفاده از "هوش مصنوعی تعاملی" در تماس‌های تلفنی جعلی است. در این نوع حملات، مهاجمان از نرم‌افزارهایی بهره می‌برند که می‌توانند صدای افراد واقعی را تقلید کنند. این فناوری باعث شده است که تأیید هویت از طریق صدا دیگر به‌عنوان یک روش امنیتی مطمئن در نظر گرفته نشود. به‌عنوان مثال، در برخی حملات اخیر، مهاجمان توانسته‌اند با تقلید صدای مدیران شرکت‌ها، کارکنان مالی را متقاعد کنند که مبلغی کلان را به حساب‌های جعلی منتقل کنند. همتی، ع. (۱۳۹۵).

از سوی دیگر، رسانه‌های اجتماعی بستری مناسب برای حملات مهندسی اجتماعی فراهم کرده‌اند. امروزه، مهاجمان از اطلاعاتی که افراد به‌صورت عمومی در شبکه‌هایی مانند اینستاگرام، لینکدین

و توییتر منتشر می‌کنند، برای طراحی حملات دقیق‌تر استفاده می‌کنند. آن‌ها می‌توانند از عکس‌ها، علایق، محل کار و سایر اطلاعات شخصی کاربران برای ایجاد سناریوهای فریبنده بهره ببرند. برای مثال، مهاجمان ممکن است با ایجاد حساب‌های جعلی در لینکدین، خود را به‌عنوان یک کارفرمای معتبر معرفی کرده و افراد را به ارائه اطلاعات حساس ترغیب کنند.علاوه بر این، رشد پلتفرم‌های پیام‌رسان مانند واتساپ و تلگرام، روش‌های جدیدی را برای مهندسی اجتماعی به وجود آورده است. در حملات "مهندسی اجتماعی پیام‌رسانی"، مهاجمان با استفاده از پیام‌های جعلی، قربانیان را به کلیک بر روی لینک‌های مخرب یا دانلود فایل‌های آلوده ترغیب می‌کنند. یکی از رایج‌ترین این حملات، ارسال پیام‌هایی است که ادعا می‌کنند کاربر در یک قرعه‌کشی برنده شده است یا باید فوراً اطلاعات حساب خود را برای جلوگیری از مسدود شدن آن تأیید کند. ایزدی، م. (۱۳۹۵).

در سطح سازمانی، حملات مهندسی اجتماعی از اهمیت بیشتری برخوردارند. مجرمان سایبری اغلب سازمان‌های بزرگ را هدف قرار می‌دهند و از طریق کارکنان آن‌ها به سیستم‌های حیاتی نفوذ می‌کنند. روش‌هایی مانند "طعمه‌گذاری (Baiting) "که در آن مهاجمان یک حافظه‌ی USBآلوده را در نزدیکی محل کار کارکنان قرار می‌دهند، همچنان از جمله روش‌های مؤثر برای دسترسی غیرمجاز به اطلاعات سازمانی محسوب می‌شود.

یکی از جدیدترین تهدیدات در حوزه‌ی مهندسی اجتماعی، ترکیب این حملات با بدافزارهای مبتنی بر هوش مصنوعی است. در این روش، بدافزارها به‌طور خودکار اطلاعات کاربران را جمع‌آوری کرده و پیام‌های فریبنده‌ای تولید می‌کنند که به‌شدت با عادات و رفتارهای آن‌ها همخوانی دارد. برای مثال، یک بدافزار ممکن است پس از دسترسی به ایمیل‌های یک کاربر، پیام‌های جعلی‌ای ایجاد کند که از نظر زبانی و محتوایی کاملاً مشابه ایمیل‌های واقعی او باشد.در آینده، انتظار می‌رود که مهندسی اجتماعی حتی پیچیده‌تر شده و تهدیدات جدیدی را به همراه داشته باشد. فناوری‌هایی مانند واقعیت مجازی و واقعیت افزوده می‌توانند بسترهای جدیدی برای فریب کاربران ایجاد کنند. همچنین، با گسترش استفاده از چت‌بات‌های هوشمند، امکان دارد مهاجمان از این ابزارها برای ایجاد مکالمات جعلی و فریب کاربران استفاده کنند.در مجموع، تحول حملات مهندسی اجتماعی نشان می‌دهد که این تهدید همواره در حال تغییر و سازگاری با فناوری‌های جدید است. از این‌رو، آگاهی‌بخشی مداوم و توسعه‌ی روش‌های پیشگیری از جمله

آموزش امنیت سایبری، به‌کارگیری احراز هویت چندمرحله‌ای، و تقویت سیاست‌های امنیت اطلاعات، می‌تواند نقش مهمی در کاهش اثرات این حملات داشته باشد.

نقش روانشناسی در فریب کاربران

مهاجمان سایبری از اصول روانشناسی برای فریب کاربران و متقاعد کردن آن‌ها به افشای اطلاعات حساس یا انجام اقدامات ناخواسته استفاده می‌کنند. این تکنیک‌ها بر اساس درک عمیق از نحوه‌ی تصمیم‌گیری انسان، هیجانات، و رفتارهای اجتماعی طراحی شده‌اند. جعفری، ج. (۱۳۹۶).یکی از رایج‌ترین اصول روانشناختی که در مهندسی اجتماعی به کار گرفته می‌شود، اعتمادسازی است. انسان‌ها به‌طور طبیعی تمایل دارند به افرادی که دوستانه و معتبر به نظر می‌رسند اعتماد کنند. مهاجمان از این ویژگی سوءاستفاده کرده و خود را به‌عنوان یک شخص قابل‌اعتماد، مانند همکار، مدیر، یا نماینده‌ی یک شرکت معتبر معرفی می‌کنند. برای مثال، در حملات فیشینگ، ایمیل‌هایی که با زبان رسمی و حرفه‌ای نوشته شده‌اند و به نظر می‌رسد از یک منبع قانونی ارسال شده‌اند، احتمال بیشتری برای فریب کاربران دارند.

یکی دیگر از تکنیک‌های روانشناسی، ایجاد حس اضطرار است. انسان‌ها هنگام مواجهه با شرایط فوری، کمتر به تحلیل و بررسی دقیق اطلاعات می‌پردازند و تصمیم‌های عجولانه می‌گیرند. مهاجمان از این ویژگی برای تحت‌فشار قرار دادن قربانیان استفاده می‌کنند. برای مثال، پیام‌هایی که ادعا می‌کنند حساب بانکی کاربر در معرض خطر است و باید فوراً اقدام کند، از این اصل بهره می‌برند.اثر هاله‌ای یکی دیگر از اصول روانشناسی مورد استفاده در حملات مهندسی اجتماعی است. در این روش، مهاجمان با استفاده از ظاهر، نام یا موقعیت اجتماعی خاصی، خود را معتبر جلوه می‌دهند. برای مثال، فردی که از آدرس ایمیل سازمانی جعلی استفاده می‌کند، بیشتر احتمال دارد که قربانیان را متقاعد کند که واقعاً یک مقام رسمی است.

ترس و اضطراب از دیگر عوامل روانشناسی مؤثر در فریب کاربران هستند. مهاجمان از تهدیدها و هشدارهای جعلی برای ترساندن افراد و ترغیب آن‌ها به انجام اقدامات خاص استفاده می‌کنند. برای مثال، پیام‌هایی که اعلام می‌کنند یک بدافزار خطرناک روی دستگاه کاربر شناسایی شده است و او باید فوراً یک نرم‌افزار امنیتی خاص را نصب کند، نمونه‌ای از این روش هستند.

اصل کمیابی و فرصت محدود نیز در حملات مهندسی اجتماعی نقش مهمی ایفا می‌کند. انسان‌ها تمایل دارند به سرعت از فرصت‌های نادر و محدود استفاده کنند. مهاجمان با ارسال پیام‌هایی که

پیشنهادهای ویژه و زمان‌دار ارائه می‌دهند، کاربران را به کلیک بر روی لینک‌های مخرب یا افشای اطلاعات ترغیب می‌کنند.

تمایل به پیروی از جمع نیز یک عامل مهم دیگر است. وقتی کاربران مشاهده می‌کنند که افراد زیادی در حال انجام یک عمل خاص هستند، احتمال بیشتری دارد که آن‌ها نیز همان رفتار را تکرار کنند. مهاجمان از این ویژگی برای انتشار بدافزارها و حملات فیشینگ در شبکه‌های اجتماعی استفاده می‌کنند. برای مثال، ممکن است کاربران پیام‌هایی دریافت کنند که دوستانشان نیز آن را به اشتراک گذاشته‌اند، در نتیجه بیشتر احتمال دارد که روی لینک کلیک کنند.

ایجاد حس کنجکاوی یکی دیگر از روش‌های روانشناسی در مهندسی اجتماعی است. مهاجمان با ارسال پیام‌هایی که اطلاعات جذاب یا محرمانه‌ای را وعده می‌دهند، کاربران را به کلیک بر روی لینک‌های آلوده یا دانلود فایل‌های مخرب تشویق می‌کنند. به عنوان مثال، پیام‌هایی با مضمون «ببینید چه کسی پروفایل شما را دیده است!» یا «یک خبر فوری که شما را شگفت‌زده خواهد کرد» از این اصل بهره می‌برند. کاظمی، ت. (۱۳۹۶).

اصل بده‌بستان نیز از دیگر تکنیک‌های روانشناسی مورد استفاده در فریب کاربران است. مهاجمان ابتدا یک خدمت کوچک یا اطلاعات مفید در اختیار کاربران قرار می‌دهند و سپس از آن‌ها درخواست اطلاعات حساس می‌کنند. برای مثال، ممکن است یک وب‌سایت جعلی یک فایل رایگان به کاربران ارائه دهد و در عوض از آن‌ها بخواهد که اطلاعات ورود خود را وارد کنند.

شرایط احساسی و هیجانی نیز در فریب کاربران نقش مهمی دارند. وقتی افراد تحت تأثیر احساسات شدید مانند شادی، خشم، یا استرس قرار دارند، قدرت تحلیل آن‌ها کاهش یافته و بیشتر در معرض فریب قرار می‌گیرند. مهاجمان از این موقعیت‌ها برای ارسال پیام‌های هیجانی و فریبنده استفاده می‌کنند.در مجموع، روانشناسی نقشی اساسی در حملات مهندسی اجتماعی دارد و آگاهی از این تکنیک‌ها می‌تواند کاربران را در برابر فریب‌های سایبری مقاوم‌تر کند. آموزش و تمرین مهارت‌های تفکر انتقادی، توجه به جزئیات پیام‌ها، و پرهیز از تصمیم‌گیری عجولانه، از راهکارهای مهم برای مقابله با این تهدیدات است.

باج‌افزارها مفاهیم و انواع

باج‌افزارها نوعی از بدافزارهای مخرب هستند که دسترسی کاربر به داده‌هایش را محدود کرده و در ازای بازیابی آن‌ها، از قربانی درخواست باج می‌کنند. این نوع حملات سایبری از مهم‌ترین