سازمان پدافند غیرعامل کشور

مهندسی اجتماعی (بخش دوم)

شماره ۹۰

اداره کل پدافند غیرعامل استانداری فارس

تابستان ۱۴۰۲

پدافند غیرعامل

مهندسی اجتماعی (بخش دوم)

همان‌طور که در بخش قبلی مقاله بیان گردید، مهندسی اجتماعی در حوزه امنیت سایبری و امنیت اطلاعات، به فرآیند استفاده از تکنیک‌های روانشناسی به منظور برقراری ارتباط با افراد و اعتمادسازی و سپس کسب و استخراج اطلاعات مورد نیاز از ایشان، یا متقاعدسازی افراد برای انجام کاری خاص گفته می‌شود. در مهندسی امنیت اطلاعات، این فرآیند در حقیقت نوعی حمله محسوب می‌شود و می تواند تهدیدات جدی برای افراد داشته باشد.

مکانیزم‌های مهندسی اجتماعی

حملات و ترفندهای مهندسی اجتماعی در حال به روز شدن هستند. به طور کلی مهندسی اجتماعی به دو شکل **انسان محور** و **رایانه محور** انجام می‌شود.

مهندسی اجتماعی انسان محور

مهندسی اجتماعی انسان محور به معنی استفاده از تعامل مستقیم با اشخاص کلیدی در سازمان برای فراهم کردن اطلاعات حساس است. این حمله‌ها به طور عمده برای جعل هویت استفاده می‌شوند. روش‌های مهندسی اجتماعی انسان محور عبارتند از:

* **شنود:** به معنی گوش کردن غیرمجاز به گفتگو و یا خواندن پیام‌ها است. شنود می تواند در مورد هر شکلی از ارتباط از قبیل صدا ویدئو و یا متن اتفاق بیفتد.
* **سرک کشیدن:** مهاجم از این طریق می تواند به اطلاعات مهمی همچون گذر واژه، شماره شناسه فردی، شماره حساب، اطلاعات کارت اعتباری و ... دست یابد.

زباله‌گردی: شامل جستوجو برای اطلاعات حساس در سطل‌های زباله سازمان هدف است. مهاجم با این

کار می‌تواند اطلاعاتی از قبیل صورت حساب، اطلاعات تماس، مالی، گزارشات مربوط به عملیات‌های سازمانی را به دست آورد.

مهندسی اجتماعی رایانه محور

به طور کلی مهندسی اجتماعی رایانه محور به روش‌های زیر انجام می‌شود:

* **فیشینگ:** فیشینگ یکی از رایج‌ترین حملات مهندسی اجتماعی است و حدود ۴۰ سال از ظهور آن می‌گذرد. فیشینگ به تلاش برای به دست آوردن اطلاعات احراز هویتی و بانکی شما از طریق ایمیل و درگاه‌های جعلی و وب‌سایت‌های جعلی گفته می‌شود. بیشترین هدف حملات فیشینگ به دست آوردن مشخصات کاربری، حساب‌های بانکی، جزئیات کارت‌های بانکی، جزئیات کارت‌های اعتباری و حساب‌ها است.

* **فیشینگ هدفمند:** این نوع حمله نیز مکانیزمی مشابه حملات فیشینگ دارد. تفاوت این دو نوع حمله در انتخاب جامعه هدف است. در فیشینگ ساده جامعه هدف انبوهی از کاربران در فضای مجازی هستند، گاهی یک حمله کننده میلیون‌ها ایمیل به طعمه‌های متفاوت ارسال می‌نماید و از تعداد انبوه همیشه عده‌ای ساده فریب او را خواهند خورد. در فیشینگ هدفمند جامعه هدف انبوه نیست؛ بلکه شامل کارمندان یک ارگان خاص هستند، یا یک شخص به خصوص نیز می‌تواند هدف باشد. به عبارت دیگر فیشینگ هدفمند نیاز به اطلاعات دقیق‌تر از شخص دارد و کمی تخصصی‌تر است.

وب‌سایت‌های شبکه اجتماعی: مهندسی

اجتماعی رایانه محور می‌تواند در بستر سایت‌های شبکه اجتماعی همانند اینستاگرام، یوتیوب، فیسبوک، لینکدین، توئیتر، تلگرام، واتساپ و ... رخ دهد. حمله‌کنندگان از وب‌سایت‌های این شبکه‌های اجتماعی برای به‌دست آوردن اطلاعات کاربران استفاده می‌کنند.

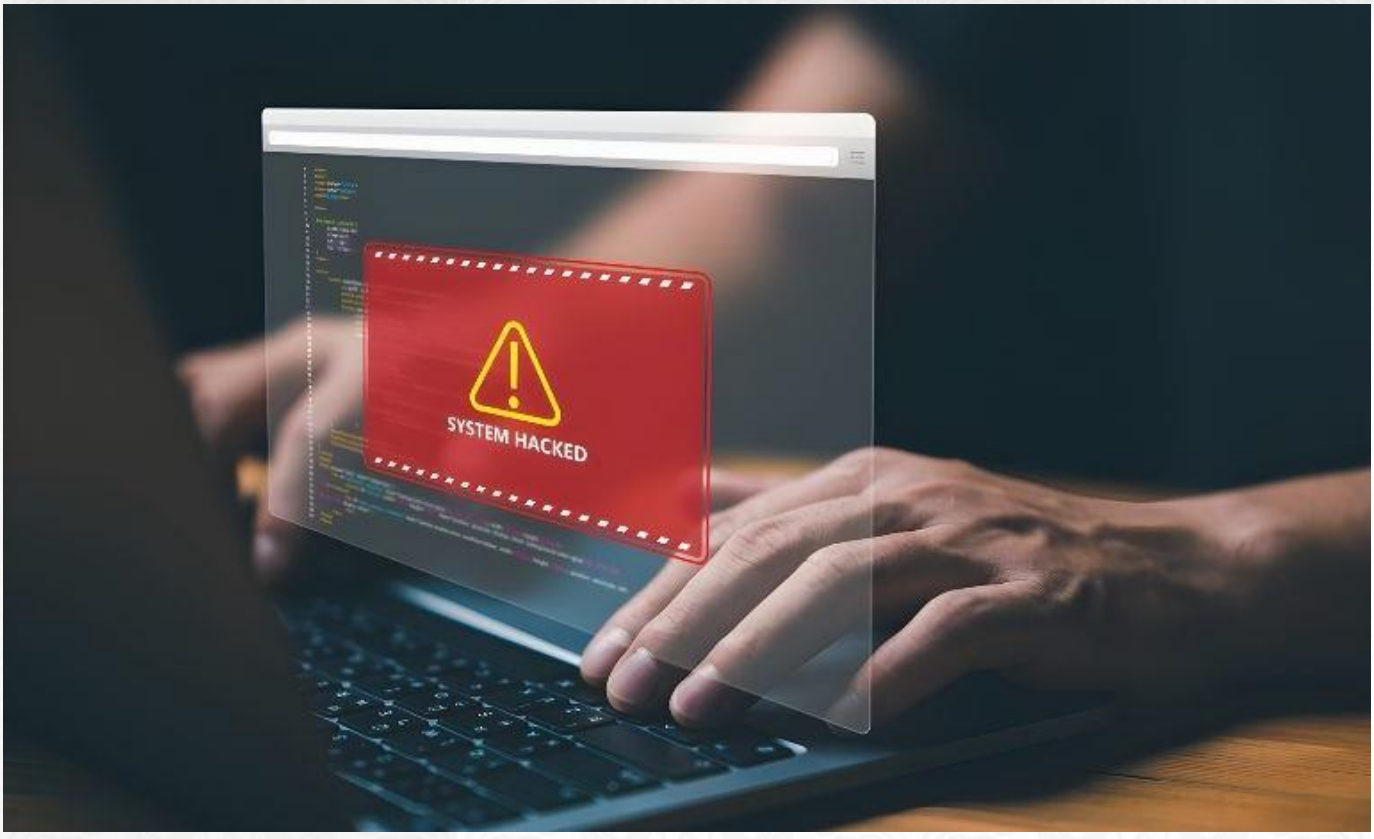
پنجره‌های پاپ‌آپ: مهندسی اجتماعی می‌تواند از طریق پنجره‌های پاپ‌آپ انجام شود. پنجره‌های پاپ‌آپ به طور ناگهانی هنگام کار با اینترنت ظاهر می‌شوند و در این پنجره از کاربر درخواست ورود اطلاعات از قبیل نام کاربری و رمز عبور می‌شود.

نامه‌های غلط: در واقع ایمیل‌هایی هستند که در آن به کاربر در مورد ویروس‌های جدید و کرم‌هایی که ممکن است به سیستم او صدمه وارد کنند، هشدار می‌دهند و از کاربران درخواست می‌شود برای در امان ماندن از این آسیب‌ها وارد وب سایت خاص شوند. در واقع این وبسایت‌ها جهت نفوذ هکر به سیستم طراحی شده اند.

پیشگیری از مهندسی اجتماعی

مهندسی اجتماعی و فیشینگ تهدیدی جدی برای امنیت سایبری سازمان‌هاست. بهترین روش‌ها برای مقابله با این نوع حملات عبارت‌اند از:

* **آموزش کارکنان:** بهتر است که کارکنان در خصوص تهدیدات مهندسی اجتماعی بدانند تا به بهترین نحو آن‌ها را شناسایی و به آن‌ها پاسخ دهند. بخش مهم این آموزش، نحوه شناسایی انواع مختلف حملات فیشینگ و این واقعیت است که فیشینگ به ایمیل محدود نمی‌شود.
* **احراز هویت چند مرحله‌ای:** حملات مهندسی اجتماعی معمولا به



دنبال اطلاعات کاربری افرادی هستند که می‌تواند برای دسترسی به منابع شرکت مورد استفاده قرار گیرد. استفاده از احراز هویت چند مرحله‌ای می‌تواند این کار را برای آن‌ها سخت‌تر نماید.

* **تفکیک وظایف:** حملات مهندسی اجتماعی برای فریب اهداف به منظور دریافت اطلاعات و پول از سوی قربانیان طراحی می‌شوند. برای توقف این حملات می‌بایست که تمامی پرداخت‌ها و سایر اقدامات پرخطر چندین وقفه در مسیر خود داشته باشد تا احتمال فریب خوردن به وسیله هرگونه کلاهبرداری را کاهش دهد.

* **ضد بدافزار و ضد ویروس:** حملات فیشینگی معمولا برای ارسال بدافزار طراحی می‌شوند. راهکارهای امنیتی چون ضد بدافزارها می‌توانند عامل بازدارنده و شناساگر ضروری برای این قبیل حملات باشند.

* **راهکارهای حفظ امنیت ایمیلی:** عاملان فیشینگ از تکنیک‌های مختلفی برای واقعی جلوه دادن پیام‌های خود و فریب قربانی استفاده می‌کنند. راهکارهای حفظ امنیت ایمیلی، ایمیل‌ها را برای محتوای مشکوک اسکن می‌کنند و محتوای مخرب احتمالی را از پیام‌ها و پیوست‌ها پیش از تحویل به گیرنده پاک می‌کنند.

متاسفانه هیچ تکنولوژی‌ای در دنیا قادر نیست که از حمله مهندسی اجتماعی جلوگیری کند. تنها راه این است که تمام افراد سازمان از وجود چنین مهاجمانی که قصد دارند با فریب و ترفند، آن‌ها را مورد دستکاری روانشناختی قرار دهند، باخبر باشند و درباره اینکه چه اطلاعاتی و چگونه باید از آن‌ها محافظت شود، آموزش ببینند.