مهندسین مشاور سازه پردازی ایران (سهامی خاص)

SAZEH PARDAZI IRAN
Consulting Eng. Co

جلوگیری از حملات مهندسی اجتماعی

- مهندسی اجتماعی اصطلاحی است که برای طیف وسیعی از فعالیتهای مخرب حاصل از تعاملات انسانی به کار می رود. این روش از فریب دادن کاربران در جهت انجام اشتباهات امنیتی یا دادن اطلاعات حساس استفاده می‌کند.
- حملات مهندسی اجتماعی در یک یا چند مرحله اتفاق می افتد. یک مهاجم در ابتدا قربانی مورد نظر را زیر نظر می گیرد تا اطلاعات زمینه ای لازم، مانند نکات احتمالی ورود و پروتکل‌های امنیتی ضعیف را برای ادامه حمله جمع آوری کند. سپس ، مهاجم در جهت جلب اعتماد قربانی حرکت کرده و محرک هایی را برای اقدامات بعدی برای نقض اقدامات امنیتی مانند افشای اطلاعات حساس یا اعطای دسترسی به منابع مهم ایجاد می کند.
- آنچه مهندسی اجتماعی را به طور خاصی خطرناک می سازد این است که به جای آسیب پذیری در نرم افزار و سیستم عامل ، متکی به خطای انسانی است. در واقع اشتباهات انجام شده توسط کاربران قانونی بسیار کمتر قابل پیش بینی هستند و شناسایی و خنثی کردن آنها دشوارتر از یک نفوذ مبتنی بر بدافزار است.

تکنیک های حمله مهندسی اجتماعی

- حملات مهندسی اجتماعی اشکال مختلفی دارد و می توانند در هر جایی که با تعاملات انسانی دخیل است انجام شود. در ادامه پنج شکل متداول از حملات مهندسی اجتماعی دیجیتال آورده شده است.

طعمه گذاری(Baiting)

- حملات طعمه گذاری همانطور که از نام آن نیز پیداست ، از یک وعده دروغین برای تحریک طمع یا کنجکاوی قربانی استفاده می کنند. آنها کاربران را به دامی سوق می دهند که اطلاعات شخصی آنها را دزدیده یا سیستم های آنها را به بدافزار آلوده می کند.
- رایج ترین شکل طعمه گذاری از رسانه های فیزیکی برای پراکنده کردن بدافزار استفاده می کند. به عنوان مثال ، مهاجمان طعمه را به صورت درایوهای فلش آلوده به بدافزار در مناطق قابل توجهی که قربانیان بالقوه مطمئناً آنها را می بینند قرار می دهند. طعمه ظاهری معتبر دارد ، مانند برچسبی که آن را به عنوان لیست حقوق و دستمزد شرکت نشان می دهد. قربانیان از روی کنجکاوی طعمه را برمی دارند و آن را وارد رایانه محل کار یا خانه می کنند و در نتیجه بدافزار خودکار روی سیستم نصب می شود.
- کلاهبرداری طعمه گذاری لزوماً نباید در دنیای فیزیکی انجام شوند. انواع آنلاین طعمه گذاری شامل تبلیغات فریبنده ای است که منجر به ایجاد سایت های مخرب می شود یا کاربران را به بارگیری یک برنامه آلوده به بدافزار ترغیب می کند.

ترس افزار(Scareware)

- ترس افزار شامل بمباران قربانیان با هشدارهای دروغین و تهدیدات ساختگی است. در واقع کاربران را فریب می دهند که سیستمشان به بدافزار آلوده است ، و باعث می شود نرم افزاری نصب کنند که هیچ منفعتی (به جز برای مجرم) ندارد یا خود یک بدافزار است. از ترس افزار به عنوان نرم افزار فریب ، نرم افزار اسکنر سرکش و کلاهبرداری نیز یاد می شود.
- ترس افزار همچنین از طریق ایمیل اسپم توزیع می‌شود که هشدارهای جعلی را تایید می‌کند، و یا پیشنهاداتی برای کاربران برای خرید خدمات بی‌ارزش و مضر ارائه می‌دهد.

نرم افزار تبلیغاتی(Adware)

- بدافزاری است که مرورگر شما را مجبور می کند به سمت تبلیغات وب هدایت شود ، که اغلب خود به دنبال دانلود بیشتر نرم افزارهای مخرب هستند. همانطور که نیویورک تایمز متذکر می شود ، نرم افزارهای تبلیغاتی مزاحم اغلب به برنامه های "رایگان" وسوسه انگیز مانند بازی ها یا افزونه های مرورگر منتقل می شوند.
- یک مثال متداول برای ترسناک بودن ، بنرهای پنجره ای با ظاهر قانونی است که هنگام مرور وب در مرورگر شما ظاهر می شوند و متن هایی از جمله "کامپیوتر شما ممکن است به برنامه های جاسوسی مضر آلوده شود" را نشان می دهد. این برنامه یا نصب این ابزار (که اغلب به بدافزار آلوده است) را برای شما پیشنهاد می کند ، یا شما را به یک سایت مخرب هدایت می کند که رایانه شما آلوده می شود.

بهانه سازی(Pretexting)

- در اینجا یک مهاجم اطلاعات را از طریق یک سری دروغ های هوشمندانه بدست می‌آورد. این کلاهبرداری اغلب توسط مجرمی شروع می‌شود که وانمود می‌کند به اطلاعات حساس یک قربانی نیاز دارد تا یک کار مهم و ضروری را انجام دهد.
- مهاجم معمولاً با اعتماد به نفس در مقابل قربانی خود با جعل هویت از همکاران ، پلیس ، مقامات بانکی و مالیاتی یا سایر اشخاصی که دارای قدرت شناخت درست هستند ، شروع می کند. بهانه گیر سوالاتی را مطرح می کند که ظاهراً برای تأیید هویت قربانی لازم است ، و از طریق آنها اطلاعات شخصی مهم را جمع آوری می کند.
- انواع اطلاعات و سوابق مربوطه با استفاده از این کلاهبرداری مانند شماره های تأمین اجتماعی ، آدرس های شخصی و شماره تلفن ها ، سوابق تلفن ، تاریخ تعطیلات کارکنان ، سوابق بانکی و حتی اطلاعات امنیتی مربوط به گیاه فیزیکی جمع آوری می شود.

پیشگیری از مهندسی اجتماعی

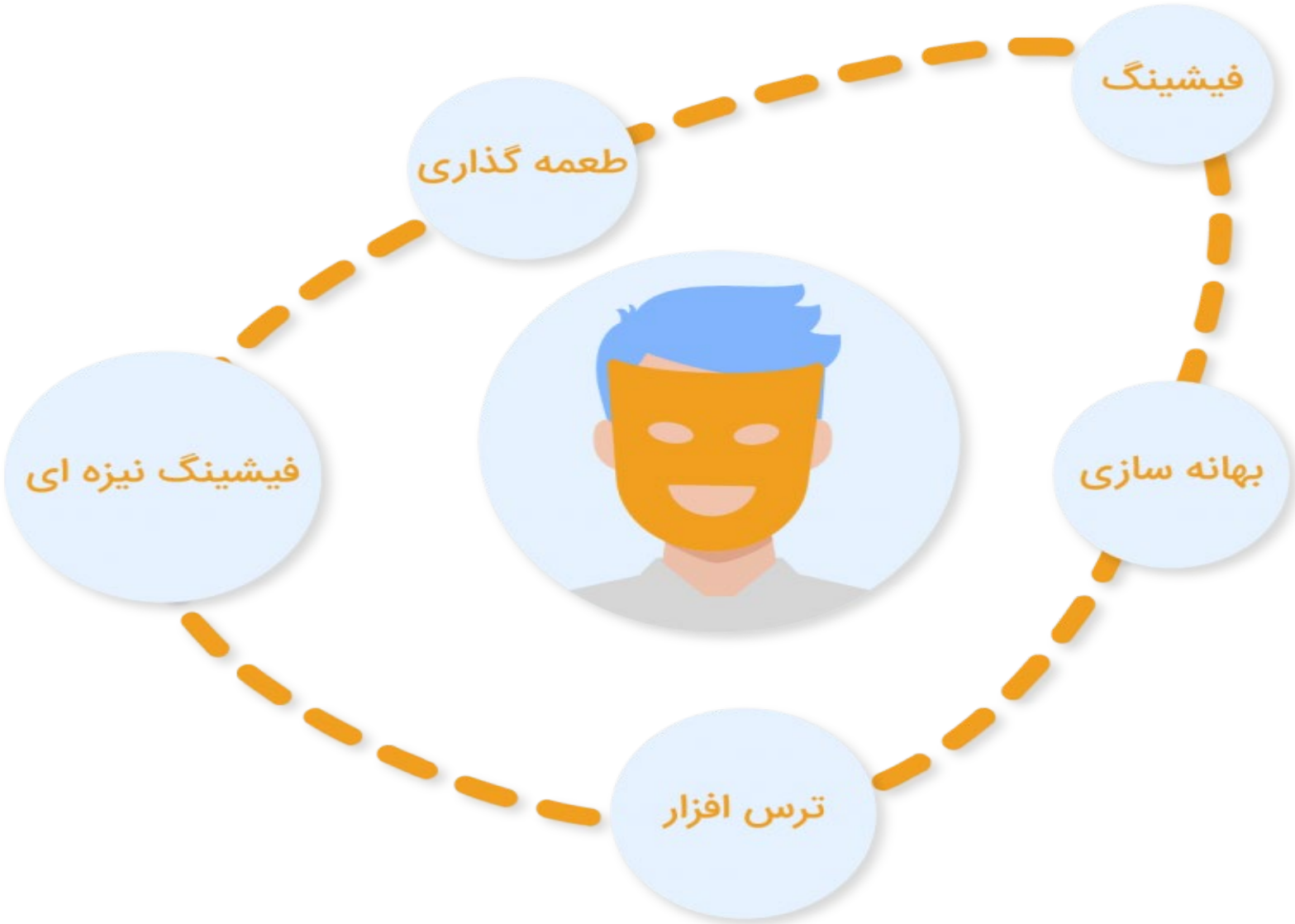
- مهندسان اجتماعی با استفاده از احساسات انسانی ، مانند کنجکاوی یا ترس ، طرح هایی را اجرا کرده و قربانیان را به دام خود می کشانند. بنابراین بهتر است هنگام مواجه شدن با ایمیل های مشکوک یا پیشنهادات تبلیغاتی در وب سایت ها محتاط باشید. هوشیاری می تواند به شما کمک کند در برابر بیشتر حملات مهندسی اجتماعی که در حوزه دیجیتال اتفاق می افتد ، از خود محافظت کنید .علاوه بر این ، نکات زیر می تواند به بهبود هوشیاری شما در رابطه با هک های مهندسی اجتماعی کمک کند.

فیشینگ(Phishing)

- کلاهبرداری فیشینگ به عنوان یکی از محبوب ترین انواع حمله های مهندسی اجتماعی، عبارتند از برنامه های ایمیل و پیام کوتاه با هدف ایجاد احساس اضطرار ، کنجکاوی یا ترس در قربانیان است. سپس آنها را ترغیب کرده تا اطلاعات حساس را فاش کنند ، روی پیوندها به وب سایتهای مخرب کلیک کنند یا پیوستهایی را که حاوی بدافزار هستند باز کنند.
- به عنوان مثال ایمیلی برای کاربران یک سرویس آنلاین ارسال شده است که به آنها در مورد نقض خط مشی هشدار می دهد که نیاز به اقدام فوری از طرف آنها مانند تغییر گذرواژه دارد. این شامل لینک به یک وب سایت غیرقانونی است که تقریباً از نظر ظاهری با نسخه قانونی آن تقریباً یکسان است و باعث می شود کاربر اعتبار فعلی و رمز ورود جدید خود را وارد کند. پس از ارسال فرم ، اطلاعات برای مهاجم ارسال می شود.
- با توجه به اینکه پیامهای یکسان یا تقریباً یکسان در کمپین های فیشینگ برای همه کاربران ارسال می شود ، شناسایی و مسدود کردن آنها برای سرورهای نامه ای که به سیستم عامل های اشتراک تهدید دسترسی دارند بسیار آسان تر است.

فیشینگ نیزه ای(Spear phishing)

- فیشینگ نیزه ای یک نسخه هدفمندتر از حمله فیشینگ است که به موجب آن مهاجم، افراد یا شرکت های خاصی را انتخاب می کند. آنها سپس پیام های خود را بر اساس ویژگی ها ، موقعیت های شغلی و ارتباطات متعلق به قربانیان خود تنظیم می کنند تا حمله آنها کمتر مشهود شود. فیشینگ نیزه ای به تلاش بیشتری از سوی مجرم احتیاج دارد و ممکن است هفته ها و یا ماه ها طول بکشد تا متوقف شود. اگر با مهارت انجام شوند ، تشخیص آنها بسیار دشوارتر و میزان موفقیت آن ها بالاتر است.
- یک سناریوی فیشینگ نیزه ای ممکن است شامل یک مهاجم باشد که به عنوان مشاور IT سازمان، یک ایمیل برای یک یا چند کارمند ارسال می‌کند. این نامه دقیقا همان طور که مشاور به طور معمول انجام می‌دهد، نوشته شده و امضا شده‌است، در نتیجه دریافت کنندگان را طوری فریب می‌دهد که فکر می‌کنند این یک پیام معتبر است. این پیام باعث می‌شود که گیرنده رمز عبور خود را تغییر داده و آن‌ها را با یک لینک هدایت کند که آن‌ها را به صفحه مخربی که در آن مهاجم اعتبار آن‌ها را ثبت می‌کند، هدایت می‌کند.


فیشینگ
طعمه گذاری
بهانه سازی
فیشینگ نیزه ای
ترس افزار

ایمیل و پیوست ها را از منابع مشکوک باز نکنید

- اگر فرستنده ایمیل را نمی شناسید ، نیازی به پاسخ دادن به ایمیل نیست. حتی اگر فرستنده را می شناسید ولی در مورد پیام مشکوک هستید ، اخبار را از منابع دیگر مانند تلفن یا مستقیماً از سایت ارائه دهنده خدمات بررسی کرده و تأیید کنید. به یاد داشته باشید که آدرس های ایمیل همیشه جعل می شوند. حتی ایمیلی که گویا از یک منبع معتبر می آید ممکن است در واقع توسط یک مهاجم ایجاد شده باشد.

از احراز هویت چند عاملی استفاده کنید.

- یکی از با ارزش ترین اطلاعاتی که مهاجمان به دنبال آن هستند اعتبار کاربر است. استفاده از احراز هویت چند عاملی به شما کمک می کند تا در صورت به خطر افتادن سیستم از محافظت از حساب خود اطمینان حاصل کنید. آتین یک راه حل آسان برای احراز هویت چند عاملی است که می تواند امنیت حساب برنامه های شما را افزایش دهد.

از رمزهای عبور قوی و یک برنامه مدیریت رمز عبور استفاده کنید.

- هر یک از رمزهای عبور شما باید منحصر به فرد و پیچیده باشد. هدف باید استفاده از انواع کاراکتر های متنوع ، از جمله حروف بزرگ ، اعداد و نمادها باشد. همچنین در صورت امکان رمزهای عبور طولانی تری را انتخاب کنید. برای کمک به مدیریت همه گذرواژه های خود می توانید از یک برنامه مدیریت گذرواژه برای ذخیره و به خاطر سپردن امن آنها استفاده کنید.

از به اشتراک گذاری نام مدارس ، حیوانات خانگی ، محل تولد یا سایر مشخصات شخصی خود خودداری کنید.

- شما ممکن است به طور ناآگاهانه پاسخ سوالات امنیتی یا بخشهایی از رمز ورود خود را در معرض دید قرار دهید. اگر سوالات امنیتی خود را طوری تنظیم کنید که به یادماندنی اما نادرست باشند ، شکستن حساب شما برای یک هکر سخت تر می شود. مثلا اگر اولین اتومبیل شما "تویوتا" بود ، نوشتن نام دروغینی مانند "ماشین دلقک" می تواند هکرهای کنجکاو را کاملاً دور بیندازد.

مراقب پیشنهادهای وسوسه انگیز باشید.

- اگر پیشنهادی بیش از حد فریبنده به نظر می رسد ، قبل از پذیرفتن آن خوب فکر کنید. جستجو در مورد موضوع می تواند به شما کمک کند تا به سرعت تشخیص دهید که با یک پیشنهاد قانونی روبرو هستید یا یک دام.

نرم افزار آنتی ویروس / آنتی بدافزار خود را به روز نگه دارید.

- اطمینان حاصل کنید که گزینه به روزرسانی خودکار فعال است. همچنین بارگیری روزانه جدیدترین نسخه ها را برای خود تبدیل به عادت کنید. برای اطمینان از اینکه به روزرسانی ها اعمال شده اند ، به صورت دوره ای نرم افزار را بررسی کرده و سیستم خود را برای جلوگیری از عفونت های احتمالی اسکن کنید.