موضوع

مهندسی اجتماعی

(Social Engineering)

استاد: دکتر پورابراهیمی

دانشجو: علی ثاقب موفق – 98571100104

خرداد 1399

تعریف مهندسی اجتماعی:

مهندسی اجتماعی، همانگونه که از نام آن پیدا است، اندازه گیری و برآورد رفتارهای اجتماعی است که می تواند به منظور و اهداف مختلفی مورد بهره برداری قرار گیرد. مهندسی اجتماعی در زمینه امنیت اطلاعات به دستکاری روانشناسی مردم برای انجام اقدام و یا کسب اطلاعات محرمانه می باشد و به عبارتی نوعی فریب انسانها برای بدست آوردن اطلاعات، تغلب یا دسترسی به سیستم است. در رابطه با موضوع امنیت اطلاعات، مهندسی اجتماعی، هنر بهره برداری از رفتارهای ناآگاهانه انسان ها برای ایجاد شکاف امنیتی بدون هیچ شک و گمانی از سوی قربانی است. اصطلاح مهندسی اجتماعی، به نفوذهایی اشاره دارد که به جای استفاده از ضعفهای تکنیکی بر استفاده از ارتباطات انسانی و فریب افراد متکی است.

به طور کلی امنیت اطلاعات یا بر پایه اطلاعات فنی هکر مورد خدشه واقع میشود که شامل دزدیدن نامهای کاربری و رمزهای عبور به شیوه های هک کردن و نفوذ به شبکه است که مستلزم داشتن دانش فنی در زمینه شبکه و رایانه می باشد و یا بر پایه ارتباطات انسانی است که در این حالت، مجرم، اهداف خود را با ایجاد ارتباط با اشخاص بوسیله تلفن و یا تماس فیزیکی انجام میدهند و اینگونه افراد معمولاْ دارای اطلاعات فنی زیادی نبوده و صرفا دارای روابط اجتماعی و قدرت نفوذ در دیگران هستند .

مهندسی اجتماعی در سازمان ها:

در اینجا مهندسی اجتماعی شامل هر عملی که باعث نفوذ در کارمند یک سازمان و مجاب ساختن او برای انجام عمل و اقدامی برای شخص نفوذ کننده باشد. رفتار کارکنان ممکن است بیشترین تاثیر در امنیت اطلاعات سازمان داشته باشد. مفاهیم فرهنگی می تواند در امنیت اطلاعات سازمان موثر باشد و کشف رابطه بین فرهنگ سازمانی و فرهنگ امنیت اطلاعات مهم است.

کارکنانی که خودشان را بخشی از امنیت اطلاعات سازمان نمی بینند، از موضوعات امنیت اطلاعات چشم پوشی می کنند. تحقیقات نشان داده است که فرهنگ امنیت به بهبود مداوم نیاز دارد.

به عبارتی مهندسی اجتماعی سوء استفاده از اطمینان و یا فریب کارکنان جهت دسترسی به اطلاعات محرمانه سازمان و در مرحله بعد سوء استفاده از این اطلاعات است. مهندسی اجتماعی شامل جمع آوری تدریجی اطلاعات و استفاده از اطلاعات قبلی برای بدست آوردن اطلاعات جدید است و هدف آن دسترسی غیرمجاز به سیستم به منظور سرقت اطلاعات وکلاهبرداری، نفوذ غیر مجاز به شبکه، جاسوسی صنعتی، سرقت هویت، یا مختل کردن شبکه است. کارکنان ناراضی، کارگران خدماتی، پرسنل تعمیرات، کارکنان موقتی، مشاورین و شرکای سازمان ، اشخاص مورد اعتماد مثل پیمانکاران از اسیب پذیری های نیروی انسانی سازمان است

پنج گام برای مدیریت فرهنگ امنیت اطلاعات در سازمان ها:

پیش ارزیابی: شناسایی آگاهی امنیت اطلاعات کارکنان و تحلیل سیاست امنیتی فعلی

برنامه ریزی استراتژیک: تدوین یک برنامه آگاهی بخشی بهتر، شفاف سازی اهداف، تقسیم بندی کارکنان برای این منظور.

برنامه ریزی عملیاتی:تنظیم یک فرهنگ امنیتی مناسب مبتنی بر ارتباطات داخلی، مدیریت و آگاهی رسانی امنیتی و برنامه های آموزشی

پیاده سازی: چهار مرحله برای پیاده سازی فرهنگ امنیت اطلاعات بایستی طی شود که شامل تعهد مدیریت، ارتباطات با اعضاء سازمانی، دوره هایی برای اعضاء سازمان و تعهد کارکنان می باشد.

اصول اساسی مهندسی اجتماعی:

- محبت و لطف: مردم دوست دارن که لطف داشته باشند، به طوریکه در بازاریابی این موضوع فراگیر است.مثل کمک های مردمی در شرایط خاص مثل زلزله.
- تعهد، اگر مردم شفاها یا کتبی برای یک هدف یا ایده متعهد شوند، آنها به احتمال زیاد به آنچه برای آن ایده است متعهد خواهند بود.
- ثبات اجتماعی: مردم دوست دارند کاری را انجام دهند که سایرین هم انجام داده اند. به طور مثال کسی که به آسمان نگاه می کند، سایرین نیز به آسمان نگاه می کنند تا چیزی ببینند.
- اقتدار: مردم دوست دارند از ژست های اعتبار واقتدار طبعیت کنند، حتی اگر از آنها بخواهند که اقدام قابل اعتراضی را انجام دهند.
- لایک کردن، مردم به آسانی توسط کسانی که آنها را دوست دارند، مجاب می شوند. مردم اغلب دوست دارند که بخرند، اگر آنها فروشنده آن چیزی را که می خواهد به آنها بفروشد را دوست داشته باشند.
- کمبود: کمبود درک شده تقاضا ایجاد خواهد کرد. برای مثال ارائه پیشنهاد "تنها برای یک زمان محدود" ، فروش را تشویق می کند.

چرخه حملات مهندسی اجتماعی : این چرخه شامل چهار مرحله، جمع آوری اطلاعات، برقراری ارتباطات، بهره کشی و عمل و اجرا است.

برخی روش های مهندسی اجتماعی در سازمان ها:

بسیاری از انواع رایج مهندسی اجتماعی، تلفنی است و یا اینکه مجرمانی بعنوان خرابکار جهت دزدی رمزهای مهم شرکت در محل شرکت به نحو موثری مستقر می شوند.در این حالت افراد ممکن است از طریق helpdesk و

ایجاد یک درخواست در آن سامانه، باعث مراجعه کارمند ذیربط به آنها شده و کلمه عبور و پسورد را کشف کنند و یا اینکه با تماس تلفنی و جلب اعتماد در کارکنان یک شرکت، امکان دسترسی به شبکه را پیدا نمایند.

در روش تلفنی هکر با بخشی از سازمان تماس میگیرد و به شیوه های متنوع حرفه ای نسبت به اخذ اطلاعات اقدام می کند مثلا، وانمود میکند از درون سازمان تماس می گیرد و خود را به جای یکی از اشخاص رده بالای سازمان معرفی میکند و بتدریج اطلاعات را از کاربر می گیرد یا خود را مسئول شبکه یک سازمان دیگر معرفی می کند و برای حل بعضی از مشکلات بخش شبکه، اعلام نیاز به نام کاربری و کلمه رمز دارد و یا اینکه با یکی از کارمندان واحد شبکه سازمان طرح دوستی ایجاد می کند و در یک مکالمه از او اطلاعات امنیتی شرکت را دریافت می کند.

من الله التوفیق

علی ثاقب موفق