فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱۴ (تابستان ۱۳۹۴): صص ۶۵ – ۸۴

حفاظت و امنیت اطلاعات
با ارائه الگوی مفهومی مهندسی اجتماعی

محمدمهدی قوچانی[۱]
امیر موسوی[۲]
داود حسین پور[۳]

چکیده

موضوع مهندسی اجتماعی که به عنوان هنر بهره‌برداری از رفتارهای آسیب‌پذیر انسان‌ها برای ایجاد شکاف امنیتی بدون هیچ ظن و گمانی از سوی فرد شناخته می‌شود، امروزه به عنوان یکی از مباحث مهم در حوزه امنیت سازمان‌ها مطرح‌شده است. رشد و توسعه فناوری اطلاعات و تکنولوژی‌های سازمان باعث شده تا فرصت‌های بسیاری برای سوءاستفاده از اطلاعات و افراد در سازمان‌ها ایجاد شود. سؤال اصلی تحقیق این است که امنیت اطلاعات در برابر حملات مهندسی اجتماعی چگونه قابل محافظت است. تحقیقات گذشته می‌تواند بیانگر مسیر طی شده در فرآیند رشد مهندسی اجتماعی باشد. از همین رو ضمن اشاره به برخی از مهم‌ترین تحقیقات انجام‌شده در این حوزه، مبانی نظری تحقیق بیان شدند تا بتوانند آشنایی بیشتری نسبت به موضوع برای مخاطبان ایجاد نمایند. روش تحقیق توصیفی ـ کیفی است و رویکرد شبه آماری و فن تحلیل محتوا برای بررسی داده‌ها مورداستفاده قرارگرفته است، هم‌چنین از مدل تحقیق به عنوان ساختار مصاحبه استفاده‌شده ولی پاسخ‌های مصاحبه شوندگان باز در نظر گرفته شد تا ابعاد جدیدی از موضوع شناسایی و کشف شود. نتیجه گرفته شد که افراد، مهم‌ترین عنصر آسیب‌پذیر در سازمان در برابر حملات مهندسی اجتماعی هستند. پیوست‌های ایمیل را می‌توان به عنوان مهم‌ترین روش حمله در داخل کشور قلمداد کرد. از سوی دیگر آموزش به عنوان مهم‌ترین راهبرد دفاعی باید موردتوجه سازمان‌ها قرار گیرد. خسارت‌های مالی نیز مهم‌ترین آسیبی هستند که حملات به سازمان‌ها وارد می‌کنند.

کلیدواژه‌ها: *مهندسی اجتماعی، اینترنت، امنیت اطلاعات، فناوری*

۱- دانشجوی دکترا، مدیریت دولتی، دانشگاه علامه طباطبایی، ghochany@yahoo.com
۲- دانشجوی دکترا، مدیریت رفتاری، دانشگاه سمنان، amirmoosavi1986@yahoo.com
۳- استادیار دانشکده مدیریت و حسابداری دانشگاه علامه طباطبایی(ره)، dhp748@gmail.com

مقدمه

امروزه استفاده از ابزارهای تکنولوژی برای تسهیل زندگی بشر در سراسر جهان به عنوان یک استراتژی مهم و پیشرو موردتوجه قرارگرفته است. کامپیوترها، تبلت ها، تلفن‌های همراه هوشمند، شبکه جهانی اینترنت، شبکه‌های گسترده اجتماعی همگی زندگی انسان را تحت تأثیر قرار داده‌اند. این فضای جدید هم می‌تواند به عنوان یک فرصت بزرگ مورداستفاده قرار گیرد و هم می‌تواند تهدیدی جدی برای ادامه حیات باشد. از سال‌های ابتدایی فراگیر شدن کامپیوترهای شخصی و پس‌ازآن شبکه اینترنت موضوع امنیت شبکه‌ها و اطلاعات کاربران یکی از مباحث مهم بوده است. مهندسی اجتماعی در شبکه‌های جهانی یکی از موضوعاتی است که در سالیان اخیر موردتوجه قرارگرفته است و به عنوان یکی از مخاطرات استفاده از ابزارهای تکنولوژیک معرفی می‌شود. سؤال اصلی تحقیق این است که: «**امنیت اطلاعات در برابر حملات مهندسی اجتماعی چگونه قابل محافظت است**». هم‌چنین سؤالات فرعی تحقیق عبارت‌اند از: کدام‌یک از عناصر سازمانی به عنوان آسیب‌پذیرترین عنصر مطرح می‌شوند، کدام روش‌های حمله بیش‌ترین کاربرد را دارند، کدام روش دفاعی به عنوان ارزشمندترین روش مورداستفاده قرار می‌گیرد و پیامد اصلی حملات مهندسی اجتماعی در سازمان چیست. در این مقاله تلاش شده است تا با معرفی این پدیده به بیان مؤلفه‌های اصلی آن پرداخته و با بهره‌گیری از نظر متخصصان، عوامل مؤثر بر متغیرهای مدل مفهومی تحقیق را رتبه‌بندی نمود. تحقیقاتی که در گذشته در این زمینه صورت گرفته‌اند بیشتر متمرکز بر آن بودند که میزان قابلیت کاربران برای قرار گرفتن در معرض حملات مهندسی اجتماعی را بسنجند. برای مثال اورجیل[1] و دیگران در سال ۲۰۰۴ دریافتند که اگر از کارکنان ناآگاه بخواهیم که اطلاعات حساس خود را در اختیار کسی که ادعا می‌کند در حال انجام تحقیق در مورد امنیت سیستم‌هایشان هست، قرار دهند، تقریباً ۸۰٪ آن‌ها نام کاربری و ۶۰٪ آن‌ها رمز عبورشان را در اختیار وی قرار خواهند داد. بر طبق آخرین یافته‌ها در دو سال گذشته ۴۸٪ از کسب‌وکارهای بزرگ حداقل ۲۵ بار از حملات مهندسی اجتماعی در فضای سازمان‌های خود آسیب‌دیده‌اند که در هر حمله بین ۲۵ تا ۱۰۰ هزار دلار خسارت ایجادشده است. با توجه به گسترش روزافزون اینترنت در کشور و رواج بهره‌گیری از شبکه‌های مختلفی چون فیس بوک، ایمیل و موتورهای جستجوگر باید مهندسی اجتماعی آنلاین را جدی گرفته و نسبت به آگاه‌سازی کاربران اقدام نمود. در این مقاله با بررسی سیر تحقیقاتی گذشته، هستی‌شناسی مفهوم مهندسی اجتماعی تبیین

1.Orgill

می‌گردد و مبانی نظری تحقیق بیان می‌شود. ارائه مدل تحقیق و روش بررسی آن در روش‌شناسی تحقیق مطرح می‌شود سپس داده‌های تحقیق مورد تجزیه و تحلیل قرار می‌گیرد و در انتها جمع‌بندی و نتیجه‌گیری موضوع بیان می‌شود. در انتها نیز پیشنهادهای عملیاتی تحقیق برای سازمان‌ها و توسعه علمی این مفهوم در کشور و تحقیقات آینده ارائه می‌گردد.

۱- مبانی نظری

ضرورت‌های شناخت مهندسی اجتماعی

در سال‌های اخیر میزان خسارت‌های ناشی از مهندسی اجتماعی، باعث شده تا ضرورت بیشتری برای تحقیق در این حوزه ایجاد شود. در سال ۲۰۰۵ مؤسسه مدیریت و سرپرستی (IOMA) مهندسی اجتماعی را به عنوان مهم‌ترین خطر و تهدید امنیتی معرفی نمود (Thompson.2006:10). از سوی دیگر در سال ۲۰۰۶ اف بی ای طی تحقیقاتی اعلام کرد که هر سال بیش از ۶۷ میلیارد دلار هزینه حملات امنیتی می‌شود. تورنبرگ در سال ۲۰۰۴ بیان کرد که مهندسی اجتماعی پذیرش بالایی را در جامعه تکنولوژی اطلاعات به عنوان یک ابزار اجتماعی و روان‌شناختی مؤثر جهت بهره‌برداری از مکانیسم امنیت سازمان هدف، به دست آورده است (bakhshi et al,2008:9). این آمارها نشان می‌دهد که مهندسی اجتماعی یکی از ضرورت‌های تحقیقی در فضای امنیت سایبری است. سابقه تحقیقات انجام‌شده درباره مهندسی اجتماعی به دو دهه اخیر برمی‌گردد. برخی از مهم‌ترین تحقیقاتی که در سال‌های اخیر انجام‌شده‌اند، در جدول ذیل ارائه می‌شوند.

جدول ۱: تحقیقات گذشته

محقق	موضوع تحقیق	سال	منبع
اورجیل و دیگران	میزان قابلیت کاربران برای واکنش به مهندسی اجتماعی	۲۰۰۴	برودی و دیگران
هاگن و دیگران	میزان آگاهی کارمندان در مورد مهندسی اجتماعی	۲۰۱۱	برودی و دیگران
بخشی و دیگران	سنجش میزان آگاهی در خصوص امنیت شبکه	۲۰۰۸	بخشی و دیگران
کاراکاسیلوتیس و دیگران	بررسی سطح قابلیت کاربران برای مقابله با حملات	۲۰۰۷	بخشی و دیگران
نهاد دولتی در ترکیه	اجرای آزمایشی حملات در ترکیه برای سنجش میزان آگاهی	۲۰۱۰	آزکان و دیگران
ادارو و دیگران	مهندسی اجتماعی	۲۰۱۰	ادارو و دیگران

تحقیقاتی که در گذشته در این زمینه صورت گرفته است بیشتر متمرکز بر آن بودند کـه میـزان قابلیـت کاربران برای واکنش به حملات مهندسی اجتماعی را بسنجند. در آینده تحقیقات باید به سـمتی بـرود کـه معلوم شود چرا و چگونه افراد مستعد پذیرش حملات هستند. هم‌چنین یکی از مواردی که باید در تحقیقـات آینده موردنظر قرار داد این است که نسبت به یک حمله یکسان در نقاط مختلف جهان چه واکنشـی نشـان داده می‌شود.

مهندسی اجتماعی: مهندسی اجتماعی هنر بهره‌برداری از رفتارهای آسیب‌پذیر انسان‌ها بـرای ایجـاد شکاف امنیتی بدون هیچ ظن و گمانی از سوی قربانی است. مهندسی اجتماعی انسـان‌هـا را بـا روش‌هـای مختلف فریب داده و با متقاعد کردنشان از آن‌ها برای دست‌یابی به اطلاعات سوءاستفاده می‌کند. مهندسـی اجتماعی برای تغییر رفتار افراد استفاده می‌شود (heikkinen.2007:5) درواقع به صورت ساده می‌تـوان گفـت که مهندسی اجتماعی هنـر بهـره‌بـرداری از ویژگـی‌هـای انسـانی بـرای دسـت‌یـابی بـه اطلاعـات اسـت (pavkovic.2011:8).

پیشینه مهندسی اجتماعی: مهندسی اجتماعی سیر تکامل‌یافتـه هکرهاسـت. بـا ظهـور کـامپیوتر در دروان جدید و فراگیر شدن آن از دهه ۷۰ میلادی مانند هر پدیده دیگری انحراف در کاربرد این ماشین نیـز با ظهور هکرها به وجود آمد. هکرها با استفاده از حملات تکنولوژی محور، آسیب‌هـای جبـران‌ناپـذیری بـه افراد و سازمان‌ها وارد می‌کردند و یا اطلاعات موردنیاز خود را به دست می‌آوردند. اما بـا افـزایش آگـاهی و پیشرفت سیستم‌های امنیتی و کاربرد مداوم آن توسـط کـاربران، مهندسـی اجتمـاعی را بـه عنـوان روشـی جایگزین انتخاب نمودند تا هم از تکنولوژی و هم از افراد برای دست‌یابی به اهـداف خـود اسـتفاده نماینـد (Janczewski et al.2010:11).

انگیزه‌های مهندسی اجتماعی: مهندسی اجتمـاعی دو بعـد فیزیکـی و اجتمـاعی روان‌شـناختی دارد. اشتباهی که بسیاری از سازمان‌ها مرتکب می‌شوند این است که روی بعد فیزیکی تمرکز می‌کنند. مهم‌ترین انگیزه‌های مهندسان اجتماعی را می‌توان، منفعت مالی، علاقه شخصی، فشار خارجی، چالش ذهنی، محدود کردن آسیب‌هـا، غـرض شخصـی (ناشـی از بـی‌عـدالتی، انتقـام‌جـویی) و سیاسـت دانسـت (Asterloo et al.2008:14). از سوی دیگر می‌توان یکی دیگـر از انگیـزه‌هـای مهاجمـان را قـدرت‌طلبـی و یـا برانـدازی سازمان‌ها و نظام‌ها دانست.

آسیب‌پذیرها: در هر سازمانی که مورد هجوم حملات مهندسی اجتماعی قرار می‌گیرد، بخش‌هـایی از سازمان آسیب می‌بینند. با توجه به نوع حملات، شدت؛ مدت زمان و دیگر متغیرهای مؤثر در حملات، نقـاط

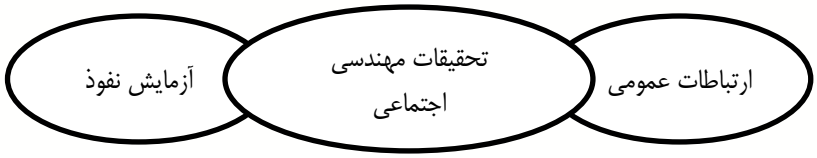
مختلفی با خسارت‌های جدی مواجه می‌شوند. گاهی اوقات این افراد هستند که در سازمان بیشتر خسارت را می‌بینند. در برخی دیگر از حملات سیستم‌های امنیتی سازمان با چالش مواجه می‌شوند. گاهی نیز تکنولوژی سازمان به عنوان هدف اصلی مهاجمان موردحمله قرار می‌گیرد (Janczewski et al.2010:13).

محیط‌های شکل‌گیری مهندسی اجتماعی: می‌توان سه محیط برای انجام حملات مهندسی اجتماعی در نظر گرفت:

۱) ارتباطات عمومی: محیطی است که ارتباطات بین عموم از طریق ابزاری مانند رادیو و تلویزیون ایجاد می‌شوند. حملات مهندسی اجتماعی در این محیط معمولاً به قصد جلب بیننده و شنونده انجام می‌شوند. محتوای این حملات معمولاً به قصد آسیب به قربانی نیست و کسی که این کار را انجام می‌دهد از آن آگاهی ندارد.

۲) آزمایش نفوذ: محیطی که در آن تلاش می‌کنند تا میزان آسیب‌پذیری برای نفوذ به یک سیستم را بیابند. قصد آن آسیب نیست بلکه سنجش میزان نفوذپذیری است. معمولاً از طریق تلفن، اینترنت یا حملات فیزیکی صورت می‌گیرد.

۳) تحقیقات مهندسی اجتماعی: این محیط می‌تواند هر دو محیط دیگر را نیز تحت پوشش خود قرار دهد. هدف آن آسیب به مشارکت‌کنندگان نیست اگرچه بهتر است که آن‌ها ندانند تحت حمله قرارگرفته‌اند چون ممکن است رفتارشان تغییر کند.



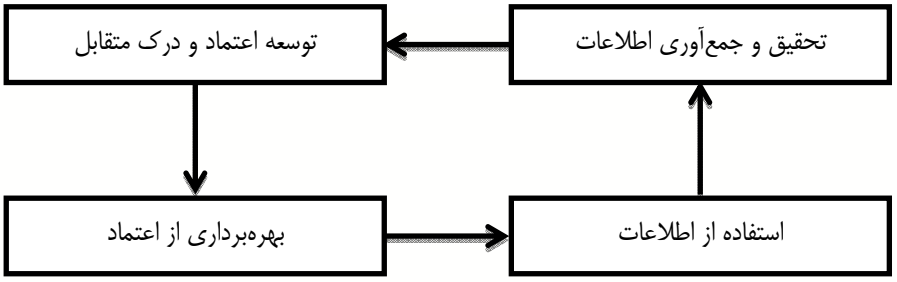
شکل ۱: محیط‌های انجام حملات مهندسی اجتماعی (Moton et al.2010:7)

حملات مهندسی اجتماعی: با توجه به ذات حملات مهندسی اجتماعی که در آن قربانی به صورت ناخودآگاه موردحمله قرار می‌گیرد و اطلاعات را افشاء می‌کند، باید بتوان ابتدا کسانی که در معرض خطر هستند را با حملات آشنا کرد تا در صورت مواجهه با نشانه‌ها بتوانند برای مقابله اقدام کنند. برای درک مهندسی اجتماعی افراد ابتدا باید بفهمند که آن‌ها به راحتی می‌توانند یک قربانی باشند (Brody et al.2012:9). حملات مهندسی اجتماعی در سال‌های اخیر شیوع بیشتری پیداکرده‌اند. برخی آمارها

نشان‌دهنده ضرورت بررسی عمیق حملات اجتماعی هستند. ۳۳٪ شرکت‌هایی کـه بـیش از ۵۰۰۰ کارمنـد دارند بیش از ۵۰ بار در بین سال‌های ۲۰۱۰ تا ۲۰۱۲ موردحمله قرارگرفته‌اند. ۷۲٪ شرکت‌ها باور دارنـد کـه رفتار کارکنان آن‌ها در شبکه‌های اجتماعی امنیت کسب‌وکارشان را به خطر می‌انـدازد (Gulenco.2013:11). تا فرد یا سازمانی خود را در معرض خطر مشاهده نکند، نمی‌تواند ریسک‌های موجود را درک کند. به همـین دلیل به راحتی مورد هجوم قرار می‌گیرد. اگر بخواهید چهارچوبی کلی و عمـومی بـرای حمـلات مهندسـی اجتماعی بیابید، می‌توان آن را به صورت ذیل بیان کرد:

"سلام، من کسی هستم که شما باید به او اعتماد کنید و طوری صحبت می‌کنم که گویی مـی‌دانـم در مورد چه صحبت می‌کنم و روی چیزی کار می‌کنم که احتمالاً شما نمی‌فهمید. به همین علت نیاز دارم کـه شما اطلاعاتی به من دهید کـه در حالـت طبیعـی بـه غریبـه‌هـا نمـی‌دهیـد، مـن قابـل‌پـذیرش هسـتم." (Thornburgh.2005:4)

می‌توان چرخه شکل‌گیری حملات را به صورت ذیل نشان داد:



شکل ۲: فرآیند حمله مهندسی اجتماعی (bakhshi et al, 2008:9)

دفاع در برابر مهندسی اجتماعی: دفاع در برابر مهندسی اجتماعی به عنوان بخشی از امنیت فضـای سایبری موردتوجه قرار می‌گیرد. برخلاف باور عموم که بیش‌ترین آسیب‌پذیری در سیستم‌های اطلاعـاتی را در حوزه نرم‌افزار می‌دانند، این عامل انسانی است که بیش‌ترین میـزان ریسـک را دارد (pavkovic.2011:8). البته در مورد تکنولوژی‌های نوین، دیگر انسان به عنوان ضعیف‌ترین رابط در حمـلات مهندسـی اجتمـاعی نیست بلکه نحوه استفاده او از سیستم‌های جدیـد اسـت (podhradski et al.2013:12). روش‌هـای متفـاوتی

برای مقابله با این حملات وجود دارد. درواقع همان‌طور که راه‌های حمله مختلف هستند، راه‌های مقابله نیز متنوع هستند. راه‌های مقابله بر اساس دو دیدگاه شکل می‌گیرند:

۱) دیدگاه روان‌شناختی: به وضعیت احساسی و توانایی‌های شناختی فرد تکیه می‌کند. درواقع فرد را از نظر پتانسیل احساسی برای مغلوب شدن در برابر حملات موردبررسی قرار می‌دهند. هر فردی با توجه به خصوصیات رفتاری و شخصیتی‌اش، پتانسیل خاصی برای تحت تأثیر قرار گرفتن دارد.

۲) دیدگاه علوم کامپیوتری: به حساسیت اطلاعات تأکید می‌کند. درواقع گفته می‌شود که فرد به چه میزان آمادگی اطلاعاتی برای مقابله با حملات را دارد. میزان دانش و آگاهی وی برای این‌که تحت تأثیر حملات قرار نگیرد به چه میزان است (Moton et al.2010:7).

پیامدهای حملات: مطمئناً قرار گرفتن در معرض حملات مهندسی اجتماعی باعث ایجاد پیامدهایی در سازمان می‌شود. یکی از نقاط قوت یک مدل خوب آن است که بتواند پیامدهای متغیرهای مستقل را بر متغیر وابسته نشان دهد. به‌طورکلی می‌توان پیامدها را به دو گروه اولیه و ثانویه تقسیم نمود که از نظر اولویت زمانی با یکدیگر متمایز می‌شوند. در مرحله اول پس از حمله ابتدا آمادگی یا امانت‌داری سازمان مخدوش می‌شود و در ادامه آسیب‌های مالی یا اعتباری به سازمان وارد می‌گردد (podhradski et al.2013:12).

مدل تحقیق:

مدلی که به عنوان مدل مبنا انتخاب‌شده است، در سال ۲۰۱۰ توسط جانزوفسکی و همکارانش در مجله علوم کامپیوتر و تکنولوژی اطلاعات[1] به چاپ رسیده است. آن‌ها برای بررسی مدل ارائه‌شده با ۲۵ متخصص از ۱۷ سازمان مصاحبه نموده‌اند که ۷ سازمان محلی و ۱۰ سازمان بین‌المللی در میان آن‌ها بوده است. در مدل مبنا پارامترهای مهمی بیان‌شده‌اند ولی کامل نبودند، به همین علت این مدل با استفاده از متغیرهایی که در طی فرآیند تحقیق به دست آمدند، تکمیل شد.

1. Computer science & information technology

آسیب‌پذیرها	روش‌های دفاعی	روش‌های حمله		پیامدها	
		تکنولوژی محور	فرد محور	آسیب‌های اولیه	آسیب‌های ثانویه
ـ افراد ـ استراتژی امنیتی ـ تکنولوژی	ـ خط‌مشی گذاری ـ آموزش ـ تربیت آگاهی‌دهنده ـ محصولات ایمن شده ـ برقراری امنیت فیزیکی ـ کنترل‌های تکنیکی	ـ پنجره‌های POP-UP ـ پیوست‌های ایمیل ـ مهندسی اجتماعی آنلاین ـ نقاب زدن برای فریب	ـ جعل هویت ـ دست‌یابی به زباله‌ها ـ جاسوسی فیزیکی افراد ـ مهندسی اجتماعی معکوس	ـ محرمانه ـ امانت‌داری ـ آمادگی	ـ مالی ـ اعتباری

شکل ۳: مدل نظری تحقیق

۲- روش‌شناسی

در زمانی که مطالعه بر معنای پدیده خاصی از دیدگاه مشارکت‌کنندگان متمرکز است و قبل از این‌که یک مطالعه کمی بتواند انجام شود، بررسی اکتشافی ضروری است می‌توان از مصاحبه پژوهش کیفی استفاده کرد. تعریف مصاحبه پژوهش کیفی بدین شرح است: « شیوه ایست که هدف آن گردآوری توصیف‌هایی در مورد جهان واقعی زندگی مصاحبه شونده با توجه به تفسیر معنای پدیده توصیفی است». هدف هر نوع مصاحبه پژوهش کیفی نگاه به موضوع پژوهش از منظر مصاحبه شونده و درک چگونگی و چرایی این منظر یا دیدگاه است (دانایی‌فر و دیگران،۱۳۹۲:۱۲۷)

روش تحقیق کیفی بر اساس چهارچوب تفسیرگرایی انجام می‌شود. در اینجا تأکید بر توضیح و تفسیر کلمات و جملات است (دهدشتی و دیگران، ۱۳۸۹:۲۵۳) انجام دادن تحقیق کیفی در موقعیت‌هایی که عدم اطمینان مسئله بسیار بالاست، مناسب است. با توجه به این‌که موضوع مهندسی اجتماعی در کشور ما موضوع جدیدی است و نیاز به بهره‌گیری از نظرات متخصصان و اندیشمندان در این حوزه داده، بنابراین تحقیق حاضر اکتشافی و از نوع کیفی است. درجایی که شرح توصیفی و صریح از یک موضوع، بدون آزمون فرضیه رسمی ضروری است و ماهیت و دامنه افکار و دیدگاه‌های احتمالی مشارکت‌کنندگان در مورد موضوع پژوهش پیشاپیش شناخته‌شده نیست از مصاحبه ساختارمند دارای پاسخ باز استفاده می‌شود. در این

تحقیق از مدل تحقیق به عنوان ساختار مصاحبه استفاده‌شده ولی پاسخ‌های مصاحبه شوندگان باز در نظر گرفته شد تا ابعاد جدیدی از موضوع شناسایی و کشف شود. (دانایی‌فر و دیگران،۱۳۹۲:۱۲۸)

تعیین مشارکت‌کنندگان در مصاحبه کیفی بستگی به اهداف مطالعه یا بررسی دارد. جامعه آماری این تحقیق مدیران واحدهای برنامه‌ریزی، فناوری اطلاعات و مدیریت پروژه در سازمان‌ها هستند که اینترنت یکی از ابزارهای در دسترس کارکنان آن سازمان‌هاست. با استفاده از ۳ عامل تحصیلات مرتبط، تجربه کاری در حوزه فناوری اطلاعات و در دسترس بودن نمونه‌ها از میان جامعه آماری به صورت تصادفی انتخاب‌شده‌اند. با تعداد ۱۰ نفر از متخصصان این حوزه و افرادی که در جامعه آماری تحقیق قرار می‌گرفتند، مصاحبه انجام گرفت. پس‌ازآن جام مصاحبه‌ها برای بار دوم پرسشنامه‌هایی برای آن‌ها ارسال شد و از آن‌ها خواسته شد تا به شاخص‌های هر بخش امتیازدهی نمایند. این عمل که به عنوان طوفان نوشتاری[1] شناخته می‌شود، باعث تثبیت پایایی تحقیق و بالا رفتن اعتبار تحقیق کیفی به عنوان یک روش ساختاریافته علمی می‌شود.

برای تحلیل داده‌های مصاحبه شوندگان از رویکرد شبه آماری استفاده‌شده است. این رویکرد در فن تحلیل محتوا به بهترین وجه متجلی می‌شود. واحد مناسبی برای اندازه‌گیری انتخاب‌شده است و آنگاه هر واحد طبقه‌بندی می‌شود. در این تحقیق جداول رتبه‌بندی امتیازی برای شاخص‌های مختلف طراحی‌شده است. در این سیستم امتیازدهی از پاسخ‌دهندگان خواسته شد که به هر کدام از معیارهای ذکرشده از ۱ تا ۵ امتیاز دهند. مجموع امتیازات آن‌ها برای رتبه‌بندی شاخص‌ها مورداستفاده قرارگرفته است. این مقایسه نمی‌تواند متضمن آزمون معنی‌داری آماری باشد و فقط می‌تواند به عنوان راهی که بدان طریق به تمرکز تحلیل‌های کیفی محض روی موضوعات کلیدی بینجامد، کمک کند.

برای اثبات پایایی در پژوهش کیفی می‌توان از دو روش شناخت پیش داشته‌ها و یا کدگذاری موضوعات استفاده کرد که در این پژوهش از روش اول استفاده شده است. در این روش پژوهشگر باید به‌طور صریح پیش داشته‌های مفهومی خود را بشناسد و در تحلیل داده‌ها هوشیارانه عمل کند و اجازه دهد که یافته‌ها او را شگفت‌زده کند. در پژوهش‌های کیفی ابزاری دارای روایی است که به‌طور واقعی آنچه را که ادعا می‌شود بررسی‌شده است، بررسی کند. در پژوهش‌های کیفی توجه به روایی تفاسیر است. تنها معیار صحت یک تفسیر بین الاذهانی بودن آن است. یعنی گروهی از افراد که دارای جهان مشابهی شوند (دانایی‌فر و دیگران،۱۳۹۲:۲۴۰) در این پژوهش با استفاده از حلقه‌های بازخور و جست و جوی فعالانه تناقضات در داده‌ها، روایی تحقیق اثبات شد. پس از مصاحبه اولیه با نخبگان، داده‌ها جمع‌آوری شد و موردبررسی قرار گرفت. با توجه به نتایجی که از داده‌ها به دست آمد سؤالاتی طراحی شد و دوباره برای نخبگان ارسال شد.

1. Brain writing

جواب‌های آن‌ها با مصاحبه‌های اولیه انطباق داده شد تا میزان روایی پاسخ‌ها به دست آید. طبق نتایج گرفته‌شده روایی تحقیق مورد تأیید قرار گرفت.

۳- تجزیه و تحلیل داده‌ها و یافته‌ها

در این بخش دو نوع نتیجه‌گیری بیان می‌شود. در نوع اول با توجه به سؤالات مصاحبه که از ساختار مدل تحقیق به‌دست‌آمده ، پاسخ‌های مصاحبه شوندگان مورد تجزیه و تحلیل محقق قرارگرفته و نکات مورداشاره آن‌ها به صورت توصیفی بیان‌شده است. در انتهای هر کدام از سرفصل‌ها نیز جداول رتبه‌بندی امتیازی برای شاخص‌های مختلف طراحی‌شده است. در این سیستم امتیازدهی از پاسخ‌دهندگان خواسته شد که به هر کدام از معیارهای ذکرشده از ۱ تا ۵ امتیاز دهند. مجموع امتیازات آن‌ها برای رتبه‌بندی شاخص‌ها مورداستفاده قرارگرفته است.

آسیب‌پذیرها: کلیه افراد سازمان در معرض حملات هستند. افراد را از طریق ارتباطات غیرمجاز مورد تخلیه اطلاعاتی قرار می‌دهند و با فریب آن‌ها و راضی کردنشان از آن‌ها برای دست‌یابی به اطلاعات سوءاستفاده می‌کنند. از دیدگاه مصاحبه شوندگان افراد مهم‌ترین بخش آسیب‌پذیر در حملات مهندسی اجتماعی هستند زیرا تمام عناصر دیگر فقط با وجود افراد تشکیل می‌گردند و هویت اصلی خود را پیدا می‌کنند. هر سازمانی با توجه به نوع فعالیت و تکنولوژی خود از سیستم‌های امنیتی متناسب بهره می‌گیرد. پاسخ‌دهندگان مواردی را به عنوان اصول تدوین یک سیستم امنیتی اثربخش مطرح نمودند که باعث می‌شود مقاومت سیستم در برابر حملات افزایش یابد. اولویت‌بندی این موارد در نمودار ذیل نشان داده‌شده است:

نمودار ۱: اصول طراحی سیستم امنیتی سازمان

سیستم‌های کامپیوتری، شبکه‌های سخت‌افزاری و نرم‌افزاری، سیستم‌های اطلاعات یکپارچه، اینترنت و اینترانت همگی ابزارهایی هستند که به عنوان تکنولوژی در سازمان‌ها مورداستفاده قرار می‌گیرند. یکی از اهداف اصلی مهندسان اجتماعی آسیب رساندن به زیرساخت‌های تکنولوژیک سازمان‌هاست تا بتوانند با بهره‌گیری از این نقطه‌ضعف، منافع خود را تأمین نمایند. با توجه به این‌که بحث مهندسی اجتماعی نیز در فضای اینترنت روی می‌دهد، حداکثر آسیب حملات مهندسی اجتماعی در فضای اینترنت رخ می‌دهد. پاسخ‌دهندگان اذعان داشتند که نظارت بر اینترنت در سازمان‌ها و مراکز داخل کشور با مشکلات بسیاری مواجه است. اولویت‌بندی این مشکلات به شکل ذیل نشان داده‌شده است:

نمودار ۲: موانع نظارت کارآمد بر فضای مجازی سازمان

در ادامه در نمودار ذیل نشان داده‌شده که از دیدگاه پاسخ‌دهندگان، افراد بیش‌ترین آسیب را در اثر حملات مهندسی اجتماعی می‌بینند.

نمودار ۳: اولویت‌بندی آسیب‌پذیرها در سازمان

روش‌های حمله: روش‌های حمله به دو گروه تکنولوژی محور و فرد محور تقسیم می‌شود. با توجه به این‌که دسترسی به ایمیل برای بسیاری از کارمندان سازمان‌ها به یک ضرورت تبدیل‌شده، این امکان در بسیاری از سازمان‌ها فراهم گردیده که بتوانند در محل کار به ایمیل دسترسی داشته باشند. یکی از مشکلات امنیتی در سازمان‌ها استفاده از ایمیل‌های شخصی برای انجام امور اداری است. بسیاری اوقات نامه‌های مخرب یا لینک‌های جعلی که در ایمیل‌های افراد وجود دارد، باعث اختلال در شبکه‌های داخلی سازمان‌ها می‌شود. امروزه عضویت در وب‌سایت‌های مختلف برای کاربران یک امر طبیعی است. بسیاری از سایت‌ها برای ارائه خدمات مختلف خود پرسشنامه‌هایی را برای متقاضیان ارسال می‌کنند و از آن‌ها اطلاعاتی درخواست می‌نمایند. باید یک سری آموزش‌های لازم برای کارمندان در نظر گرفت تا هرگونه اطلاعاتی که از آن‌ها خواسته شد را به راحتی در اختیار متقاضی قرار ندهند. هم‌چنین نحوه شناسایی وب‌سایت‌های معتبر نیز جزء مواردی بود که تأکید داشتند باید به کارکنان آموزش داده شود. یکی از شایع‌ترین روش‌های حملات صفحات جعلی هستند. دانش کافی در مورد شناسایی صفحات جعلی در میان کاربران وجود ندارد. محدودیت در دسترسی به سایت‌هایی که با حوزه کاری کارمندان تناسبی ندارد یکی از روش‌های پیشنهادی برای مقابله با این وب‌سایت‌هاست. برخی سازمان‌ها برای دست‌یابی به اطلاعات رقبا، فردی را در سطوح پایین سازمانی برای استخدام در سازمان رقیب می‌فرستند. آن فرد پس از وارد شدن به سیستم و جاسوسی در دفاتر، پایگاه داده‌ها و مدیران سطوح بالاتر، اطلاعات موردنظر خود را جمع‌آوری می‌کند. پس از دست‌یابی به اطلاعات فرد با ترفند خاصی از سازمان خارج می‌شود به طوری که شک‌برانگیز نباشد. این روش یکی از مصداق‌های جاسوسی فیزیکی افراد است. برخی مهاجمان با شناسایی افراد هدف و بررسی رفتار آن‌ها در فضای مجازی، نیازهای آن‌ها را درک می‌کنند و پس‌ازآن با معرفی خود به عنوان فرد یا گروهی که می‌تواند نیازها را برطرف نماید، فعالیت خود شروع می‌کنند. حضور کاربران در سایت‌های مختلف و ثبت‌نام در آن‌ها بخشی از این فرآیند است که مهندسی اجتماعی معکوس نام دارد.

اثرگذاری روش‌های مختلف حمله به ترتیب ذیل می‌باشد:

نمودار ٤: اثرگذاری روش‌های مختلف حمله

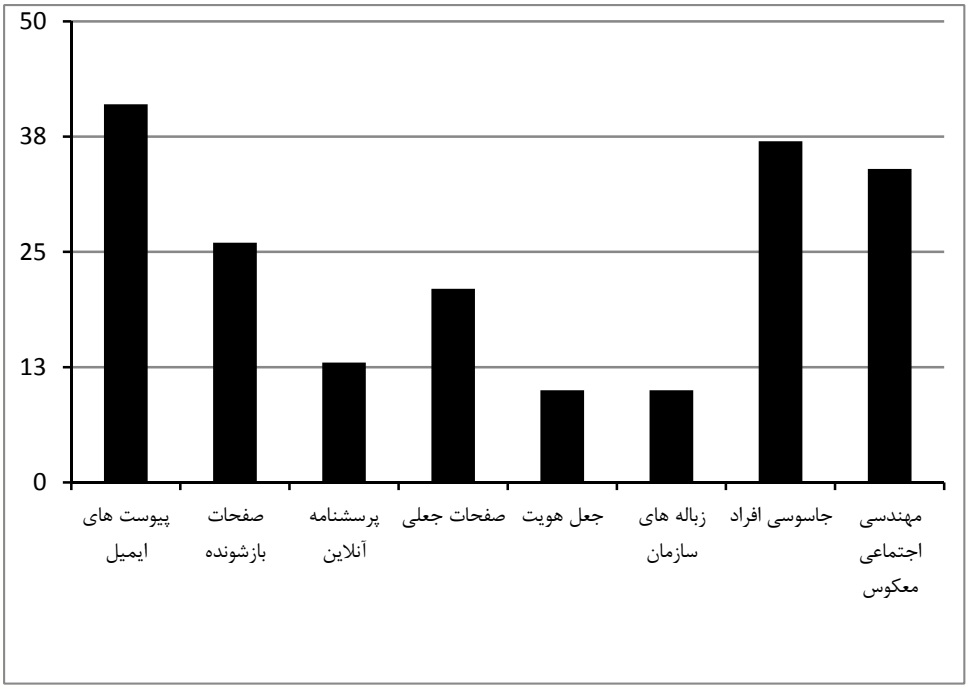
در ادامه از پاسخ‌دهندگان درخواست شد تا با توجه به تجربیات کاری خود در سازمان‌های مختلف و برخوردهایی که با روش‌های مختلف حملات مهندسی اجتماعی داشته‌اند، میزان مواجه بودن سازمان خود با حملات مهندسی اجتماعی را موردتوجه قرار داده و امتیازدهی نمایند تا شیوع روش‌های مختلف در سازمان‌های کشور نشان داده شود. بدیهی است که امتیاز ۱ نشانگر برخورد بسیار کم پاسخ‌دهندگان با روش مربوطه و امتیاز ۵ نشانگر برخوردهای بسیار زیاد با روش مربوطه می‌باشد.

جدول ۲: امتیاز بندی شیوع روش‌های حمله در کشور

	پیوست‌های ایمیل	صفحات باز شونده	پرسشنامه آنلاین	صفحات جعلی	جعل هویت	زباله‌های سازمان	جاسوسی افراد	مهندسی اجتماعی معکوس
فرد ۱	۴	۴	۱	۱	۱	۱	۱	۱
فرد ۲	۵	۲	۱	۲	۱	۱	۴	۵
فرد ۳	۵	۳	۲	۲	۱	۱	۵	۳
فرد ٤	۳	۲	۱	۳	۱	۱	۳	۳
فرد ٥	۴	۳	۱	۳	۱	۱	۵	۴
فرد ٦	۵	۱	۲	۱	۱	۱	۴	۲
فرد ۷	۳	۳	۲	۲	۱	۱	۴	۵
فرد ۸	۳	۲	۱	۳	۱	۱	۵	۴

فرد ۹	۵	۴	۱	۲	۱	۱	۳	۳
فرد ۱۰	۴	۲	۱	۲	۱	۱	۱	۳	۴
مجموع	**٤١**	**٢٦**	**١٣**	**٢١**	**١٠**	**١٠**	**٣٧**	**٣٤**

با توجه به جدول فوق در ادامه نمودار شیوع روش‌های مختلف حمله در کشور ارائه می‌گردد:

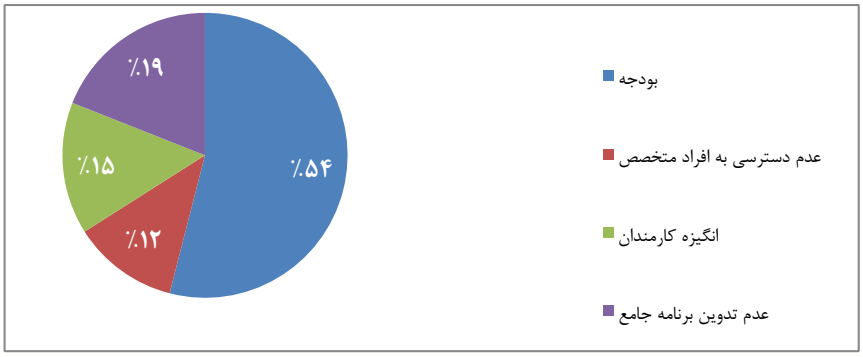


نمودار ۵: رتبه‌بندی روش‌های حمله در سازمان

روش‌های دفاعی: یکی از راه‌های مقابله با جاسوسی در سازمان برقراری امنیت فیزیکی است. تقریباً در تمامی سازمان‌های بزرگ واحدی برای برقراری امنیت فیزیکی در نظر گرفته‌شده است. هم‌چنین آیین‌نامه‌ها و دستورالعمل‌های ویژه‌ای نیز در نظر گرفته‌شده که باید اجرا شود. تجهیزاتی چون دوربین‌های مداربسته، کارت‌های الکترونیکی عبور و مرور، درب‌های هوشمند، حسگرهای دیجیتالی جزء مواردی هستند

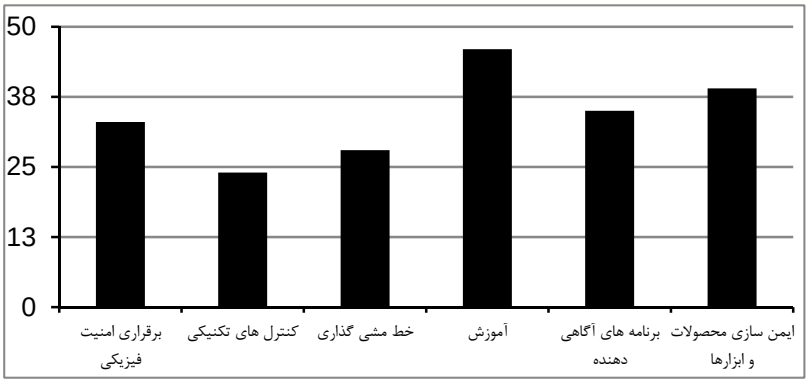
که سازمان‌ها از آن‌ها بهره می‌گیرند تا بتوانند ضریب امنیت فضای کاری خود را افزایش دهند. بسیاری از سازمان‌ها خط‌مشی مشخصی برای مقابله با حملات ندارند.

فعالیت‌هایی به صورت جداگانه و غیرمتمرکز در واحدهای مختلف سازمان صورت می‌پذیرد اما هیچ رویکرد مشترکی وجود ندارد. بدون داشتن رویکرد مشترک هزینه‌هایی که در واحدهای مختلف سازمان صورت می‌پذیرد، عملاً بهره‌وری ندارند. برای ایجاد یک رویکرد مشترک نیاز به یک خط‌مشی سازمانی است. تدوین یک خط‌مشی امنیتی مناسب و نظارت بر اجرای صحیح آن، می‌تواند سازمان‌ها را در برابر حملات تقویت نماید و ریسک را پایین بیاورد. مهم‌ترین روشی که پاسخ‌دهندگان برای مقابله با مهندسی اجتماعی به آن تأکید داشتند، آموزش کارمندان است. با توجه به هویت مهندسی اجتماعی که حملات بر اساس ضعف افراد در استفاده از ابزارهای تکنولوژیک طراحی‌شده است، مهم‌ترین راه مقابله با حملات، بالا بردن سطح دانش و آگاهی کارمندان است. البته مشکلاتی برای بخش آموزش در سازمان وجود دارد که اولویت آن‌ها به شرح ذیل می‌باشد:



شکل ۵: مشکلات آموزش

در این نمودار نشان داده‌شده که از نظر مصاحبه شوندگان آموزش مهم‌ترین روش مقابله با حملات مهندسی اجتماعی است که بیش‌ترین سرمایه‌گذاری در سازمان باید برای آن صورت گیرد. هم‌چنین روش کنترل تکنیکی نسبت به دیگر روش‌ها امتیاز کم‌تری دارد. البته مصاحبه شوندگان تأکید داشتند که برای داشتن یک برنامه دفاعی مؤثر باید از همه این روش‌ها در کنار یکدیگر استفاده نمود تا بتوان حداکثر امنیت را ایجاد کرد.



نمودار ٦: رتبه‌بندی روش‌های دفاعی

پیامدهای حملات مهندسی اجتماعی: مهم‌ترین پیامدی که پاسخ‌دهندگان به آن اشاره داشتند، پیامدهای مالی است که سازمان را تحت تأثیر قرار می‌دهد. دسترسی به اطلاعات غیرمجاز کاربران و یا برنامه‌ها و اهداف سازمان می‌تواند برای رقبا مورداستفاده قرار گیرد و ضرر آفرین باشد. در بسیاری از سازمان‌های خدمت رسان ممکن است بحث مالی خیلی اهمیت نداشته باشد و وجهه سازمان برای مخاطبانش ارزش و اهمیت بیشتری داشته باشد. یکی از مواردی که در کشور ما کم‌تر موردتوجه قرار می‌گیرد، بحث رعایت حقوق کاربران در فضای مجازی است. انتشار اطلاعات یکی دیگر از پیامدهای مهندسی اجتماعی است. بسیاری از اطلاعاتی که کاربران در فضای مجازی برای یک وب‌سایت خاص منتشر می‌کنند، به راحتی در اختیار دیگر پایگاه‌های داده‌ها قرارگرفته و مورد بهره‌برداری آن‌ها قرار می‌گیرد. این در حالی است که هیچ مجوزی از سوی کاربران برای این کار در اختیار آن‌ها قرار نگرفته است. موضوع حریم شخصی و حفظ اطلاعات کاربران امروزه یکی از مهم‌ترین دغدغه‌های استراتژیست‌های سازمانی است. خصوصاً در بحث شبکه‌های اجتماعی، ایمیل و موتورهای جست‌وجوگر ضعف سازمان در برابر حملات می‌تواند حجم زیادی از اطلاعات را در اختیار مهاجمان قرار دهد. در این نمودار نشان داده شد که از نظر مصاحبه شوندگان مهم‌ترین پیامد حملات، زیان مالی است که می‌تواند خسارات جبران‌ناپذیری به سازمان وارد کند. تقریباً تمامی پیامدهای حملات مهم هستند و باید موردتوجه کارشناسان و مدیران قرار گیرند.

نمودار ۷: رتبه‌بندی روش‌های حمله در سازمان

٤- نتیجه‌گیری و پیشنهادهای

نتیجه‌گیری: سعی محقق بر این بوده است که بتواند آگاهی مختصر اما جامعی در خصوص مؤلفه‌های مؤثر بر پدیده مهندسی اجتماعی ایجاد نماید و بتواند به سؤال اصلی تحقیق که چگونگی محافظت از اطلاعات سازمان در برابر این حملات است، پاسخ دهد. با توجه به مدل تحقیق چهار مؤلفه آسیب‌پذیرها، روش‌های حمله، روش‌های دفاعی و پیامدها موردبررسی قرار گرفتند و از تحلیل داده‌ها نتیجه گرفته شد که افراد، مهم‌ترین عنصر آسیب‌پذیر در سازمان در برابر حملات مهندسی اجتماعی هستند. از میان روش‌های حمله می‌توان پیوست‌های ایمیل را به عنوان مهم‌ترین روش حمله در داخل کشور قلمداد کرد، از سوی دیگر آموزش به عنوان مهم‌ترین راهبرد دفاعی باید موردتوجه سازمان‌ها قرار گیرد. مهندسی اجتماعی پیامدهای متعددی برای سازمان‌ها در پی دارد که خسارت‌های مالی مهم‌ترین آسیبی هستند که این حملات به سازمان‌ها وارد می‌کنند.

مهم‌ترین تهدیداتی که در آینده در حوزه مهندسی اجتماعی قابل‌ذکر هستند، استفاده گسترده از شبکه‌های اجتماعی و تلفن‌های همراه هوشمند است. توسعه روزافزون این ابزارها و حضور فعال آن‌ها در زندگی روزمره بشر، فضای وسیعی برای سوءاستفاده مهاجمان به وجود آورده است. در مقابله با این سیل حملات و خطراتی که سازمان‌ها با آن‌ها مواجه هستند، روند ایجاد همکاری میان کشورها باعث تسریع در مقابله با این پدیده شده است. امروزه کشورها درک کرده‌اند که به‌تنهایی نمی‌توانند با مهندسی اجتماعی

مقابله کنند و برای برخورد مؤثر و کاهش خسارات، باید بتوانند تعامل مثبت با یکدیگر داشته باشند و از هم پشتیبانی کنند. در سطح بین‌الملل همکاری میان دولت‌های مختلف توسعه می‌یابد تا بتوانند استراتژی‌های انعطاف‌پذیر و مشترک برای مقابله اجرا نمایند. از سوی دیگر در داخل کشورها نیز تقویت همکاری بین سطوح تصمیم‌گیری و عملیاتی در سازمان‌ها و تقویت همکاری بین بخش خصوصی و دولتی یکی از روندهای مؤثر برای کاهش اثرات این پدیده است.

در این مقاله تلاش شده است تا شناخت نسبی از این پدیده به خوانندگان داده شود. هم‌چنین با رویکردی کاربردی و مصاحبه با متخصصان حوزه فناوری اطلاعات و استراتژی‌های سازمان، مؤلفه‌های مهم این موضوع شناسایی و اولویت‌بندی شوند.

پیشنهادهای: با توجه به کاربردی بودن پژوهش، مهم‌ترین پیشنهادهایی که می‌توان بیان کرد به ترتیب ذیل می‌باشد: . ایجاد یک تیم متخصص و توانمند در حوزه مهندسی اجتماعی توسط سازمان‌های مسئول. این تیم می‌تواند با برگزاری کارگاه‌های تخصصی در سازمان‌ها اهمیت این موضوع را برای مدیران نهادینه سازد و آموزش‌های اولیه مقابله با حملات مهندسی اجتماعی را برایشان ارائه نماید.

- با توجه به این‌که پیوست‌های ایمیل به عنوان مهم‌ترین روش حمله در داخل کشور شناخته می‌شوند، محدودیت دسترسی به برخی از شبکه‌های ایمیل می‌تواند مانع آسیب به سیستم‌های امنیتی شود. می‌توان با ایجاد سیستم‌های ایمیل داخلی در سازمان‌ها از نفوذ بد افزارها از خارج از سازمان جلوگیری نمود.
- چون آموزش به عنوان مهم‌ترین راهبرد دفاعی در برابر حملات مطرح است، تعیین برنامه‌های آموزشی، سمینارها و کارگاه‌های تخصصی، چاپ و تهیه بروشورها، کتابچه‌ها و مجلات آموزشی برای ارتقاء دانش کارکنان درزمینه مهندسی اجتماعی می‌تواند گام مؤثری برای کاهش صدمات ناشی از این حملات باشد.
- پیگیری رفتار افراد در فضای مجازی در سازمان می‌تواند باعث ارتقاء ضریب امنیت سیستم‌های سازمان شود. با در نظر گرفتن این موضوع که افراد مهم‌ترین عنصر آسیب‌پذیر در سازمان هستند، باید توجه ویژه‌ای به اعمال آن‌ها در فضای مجازی سازمان نمود تا بتوان مانع دسترسی مهاجمان به اطلاعات حیاتی کاربران شد.
- بررسی احتمال حملات مختلف در سازمان و برآورد خسارت مالی هر کدام از آن‌ها می‌تواند در تدوین برنامه‌های مقابله با مهندسی اجتماعی کمک بسیاری نماید. چون خسارت‌های مالی مهم‌ترین آسیب این حملات هستند، بنابراین در تدوین برنامه‌ها باید توجه زیادی به این موضوع نمود و آن را در دستور کار قرار داد.

منابع:

دانایی‌فر، حسن، و دیگـران، ۱۳۹۲، ***روش‌شناسی پژوهش کیفی در مدیریت: رویکردی جامع***، تهـران، انتشارات صفار.

دهدشتی شاهرخ، زهره، منیژه بحرینی‌زاده ، ۱۳۸۹، ***تحقیقات بازاریابی***، تهران، انتشارات سمت.

Social engineering:A means to violate a computer system. SANS Insitutte. (2006).

The risk of social engineering on information security. Dimensional research. (2011).

Capabilities for syber security resilience. Homeland Security (2012).

A.Cazier, J. (2007). Social enginerring's threat to public privacy. Appalachian State university.

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering:assessing vulnerabilities in practice. Information management & computer security.

Bezuidenhout, M., & Mouton, F. (2011). Social engineering attack detection model:SEADM. University of petoria.

Conheady, S. (2012). The future of social engineering.

G.Brody, R., B.Brizzee, W., & Cano, L. (2012). Flying under the radar:social engineering. International journal of accounting & information management.

Granger, S. (2001). Social engineering fundamentals.

Gulenco, I. (2013). Social against social engineering. Information management and computer security.

Harley, D. (1998). Re-Floating the Titanic:Dealing with social engineering attacks. Imperical canser research fund.

Heikkinen, S. (2007). Social engineering in the world of emerging communiaction technologies. Tampere university of technology.

J.Janczewski, L. (2010). Social engineering based-attacks:Model & New Zealand perspective. Computer science & information technology.

M.Kluchin, R. (2004). Social engineering in the united states:eugenics and euthanasis.

Maamar, Z., Yahyaoui, H., Lim, E., & Thairan, P. (2011). Social engineernig of communities of web services. IEEE computer society.

Mataracioglu, T., & Ozkan, S. (2011). User awareness measurement through social engineering. TUBITAK Inc.

Mouton, F., Malan, M. M., & Venter, H. S. (2013). Social engineering from a normative ethics perspective. University of petroria.

Oosterloo, B. (2008). Managing social engineering risk. Atos consulting.

pavkovic, N., & Perkov, L. (2010). Social engineering toolkit- A systematic approach to social engineering. Ruder boskovic institute.

Podhradsky, A., & Casy, C. (2013). Xbox 360 hoaxes,social engineering and gamertag exploits.

S.Winkler, I. (1998). Case study of industrial espionage thruogh social engineering. National computer security association.

Thornburgh, T. (2005). Social engineering: The Dark Art. Kennesaw state university.