

الگوی شناسایی حملات مبتنی بر مهندسی اجتماعی در سازمان‌های نظامی

مهدی بصیری^۱، حسین فتح آبادی^۲

تاریخ دریافت: ۱۴۰۱/۱۰/۱۶

تاریخ پذیرش: ۱۴۰۱/۰۱/۲۲

چکیده

مهندسی اجتماعی، هنر متقاعد کردن کاربران برای نفوذ به سیستم‌های اطلاعاتی است. مهندسين اجتماعي به جای استفاده از حملات فنی علیه سیستم‌ها، انسان‌هایی را که به اطلاعاتی خاص دسترسی دارند، مورد هدف قرار داده و آنها را تشویق به افشای اطلاعات حساس نموده و یا حتی حملات مخربشان را از طریق نفوذ به افراد و متقاعد کردن آنها اجرا می‌کنند. هدف پژوهش حاضر ارائه الگوی شناسایی حملات مهندسی اجتماعی و ارائه راهکارهای افزایش ضریب امنیت سازمان‌های نظامی در برابر حملات مهندسی اجتماعی به ویژه باج‌افزارها در قالب الگوی شناسایی حملات مبتنی بر مهندسی اجتماعی می‌باشد. در این پژوهش اطلاعات و داده‌ها به دو روش کتابخانه‌ای و میدانی گردآوری گردید. ابزار پژوهش حاضر مصاحبه با کارشناسان و پرسشنامه حاوی تعدادی پرسش درباره‌ی متغیرهای مورد سنجش از جامعه‌ی مورد مطالعه است که روایی و پایایی آن نیز در حد مطلوب ارزیابی گردید. جامعه آماری این پژوهش شامل کلیه کارشناسان و کارکنان سازمان نظامی مورد مطالعه در شهر تهران می‌باشد. تعداد نمونه آماری تحقیق بر اساس جدول ابداعی مورگان محاسبه گردید و روش نمونه‌گیری تصادفی طبقه‌ای ساده می‌باشد. تجزیه و تحلیل داده‌ها نیز در دو بخش توصیفی و استنباطی انجام شده است. در پایان الگوی شناسایی حملات مبتنی بر مهندسی اجتماعی در سازمان‌های نظامی شامل ۶ بعد شامل: تدوین خط و مشی‌های امنیتی مناسب، آموزش همگانی کارکنان، آموزش تخصصی کارکنان، تثبیت و یادآوری، مین گذاری برای آشکارسازی حملات، سطح تهاجمی و ۲۰ مولفه تدوین و ابزاری مناسب برای استانداردسازی و ارزیابی سازمان برای جلوگیری و مقابله با حملات مهندسی اجتماعی ارائه گردید.

واژگان کلیدی: الگو، حملات سایبری، مهندسی اجتماعی، سازمان‌های نظامی.

^۱ نویسنده مسئول، دکتری مدیریت فناوری اطلاعات و استادیار دانشگاه فرماندهی و ستاد آجا (basiri60@gmail.com)

^۲ - استادیار دانشگاه پدافند هوایی خاتم الانبیاء(ص) (Fh_ie@yahoo.com)

۱- مقدمه:

امروزه استفاده از ابزارهای فناوری اطلاعات و ارتباطات برای تسهیل زندگی بشر در سراسر جهان به عنوان یک راهبرد مهم و پیشرفته مورد توجه قرار گرفته است. رایانه‌ها، تلفن‌های همراه هوشمند، اینترنت و شبکه‌های گسترده اجتماعی مجازی همگی زندگی انسان را تحت تأثیر قرار داده‌اند. این فضای جدید هم می‌تواند به عنوان یک فرصت بزرگ مورد استفاده قرار گیرد و هم می‌تواند تهدیدی جدی برای ادامه حیات باشد. مهندسی اجتماعی یکی از موضوعاتی است که در سالیان اخیر مورد توجه قرار گرفته است [۲].

مهندسی اجتماعی اصطلاحی است که برای طیف گسترده‌ای از فعالیت‌های مخرب انجام می‌شود که از طریق تعامل انسان انجام می‌شود [6].

حملات مهندسی اجتماعی در یک یا چند مرحله اتفاق می‌افتد. یک نفوذگر ابتدا برای قربانی در نظر گرفته شده برای جمع‌آوری اطلاعات لازم، از جمله نقاط احتمالی ورود و پروتکل‌های امنیتی ضعیف، برای انجام حمله، تحقیق می‌کند. سپس، مهاجم برای جلب اعتماد قربانی و ایجاد انگیزه برای اقدامات بعدی که باعث نقض اقدامات امنیتی می‌شود، مانند افشای اطلاعات حساس یا دسترسی به منابع مهم، تلاش می‌کند [8].

سازمان‌های نظامی به جهت نوع مأموریت و فعالیت‌های نظامی همواره با اطلاعات حساس و طبقه‌بندی شده سروکار دارند. و این امر موجب می‌گردد تا همواره سیستم‌ها و کارکنان این سازمان‌ها در معرض تهدید حملات رایانه‌ای از نوع مهندسی اجتماعی قرار گیرند. لذا آگاهی کارکنان از چگونگی تشخیص و مقابله با این نوع حملات ضرورتی اجتناب‌ناپذیر خواهد بود. به ویژه که ماهیت اطلاعاتی که کارکنان این نوع از سازمان‌ها با آن سروکار دارند همواره برای کشور حیاتی و مهم بوده و سرقت و یا دسترسی غیر مجاز به این نوع از اطلاعات می‌تواند صدمات و آسیب‌های جبران‌ناپذیری را برای امنیت ملی کشور فراهم سازد. بر این اساس مقاله پیش رو به دنبال پاسخ به این مسأله اساسی است که الگوی مناسب شناسایی حملات مبتنی بر مهندسی اجتماعی در سازمان‌های نظامی کدام می‌باشد؟

۲- مبانی نظری و پیشینه شناسایی تحقیق:

۱-۲- مبانی نظری:

مهندسی اجتماعی بیشتر هنر بهره‌گیری از روانشناسی رفتار افراد است تا مجموعه‌ای از تکنیک‌های فنی هک کردن. مجرمان از این هنر برای دسترسی به ساختمان‌ها، سیستم‌ها یا داده‌ها استفاده می‌کنند. با تمرین می‌توان نشانه‌های به‌کارگیری مهندسی اجتماعی را تشخیص داد. در ادامه‌ی این مطلب متداول‌ترین تکنیک‌های مهندسی اجتماعی، شناخته شده‌ترین حملات مبتنی بر مهندسی اجتماعی و راهکارهای مقابله با این تکنیک‌ها را بیان خواهیم کرد.

ایده مهندسی اجتماعی و بسیاری از تکنیک‌های موجود در این زمینه قدمتی برابر با وجود کلاهبرداران و کلاهبرداری دارد، اما اصطلاح **مهندسی اجتماعی** در دهه آخر قرن بیستم میلادی عمومیت یافته که هکر مشهور کوین مینتیک (Kevin Mitnick) نقشی اساسی در این موضوع داشته است. [4].

حتی به‌کارگیری تمام تجهیزات امنیتی مورد نیاز برای تامین امنیت مراکز داده، فضای ابری و محیط فیزیکی ساختمان شرکت، سرمایه‌گذاری بر روی فناوری‌های دفاعی، استفاده از سیاست‌ها و فرایندهای امنیتی مناسب و بررسی و بهبود مداوم اثرگذاری این سیاست‌ها و فرایندها نیز ممکن است برای جلوگیری از ورود یک مهندس اجتماعی ماهر کافی نباشد [16].

۲-۱-۱- تعریف مهندسی اجتماعی:

مهندسی اجتماعی، هنر متقاعد کردن کاربران برای نفوذ به سیستم‌های اطلاعاتی است. مهندسین اجتماعی به جای استفاده از حملات فنی علیه سیستم‌ها، انسان‌هایی را که به اطلاعاتی خاص دسترسی دارند، مورد هدف قرار داده و آنها را تشویق به افشای اطلاعات حساس می‌کنند و یا حتی حملات مخربشان را از طریق نفوذ به افراد و متقاعد کردن آنها اجرا می‌کنند. در حالی که مردم تصور می‌کنند که در شناسایی چنین حملاتی مهارت دارند، تحقیقات نشان می‌دهند که مردم در شناسایی دروغ و فریب عملکرد ضعیفی دارند [11].

۲-۱-۲- طبقه‌بندی حملات مهندسی اجتماعی:

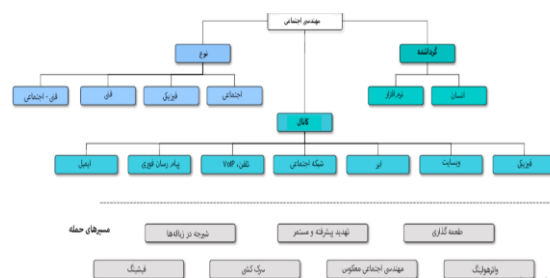
به‌طور کلی حملات مهندسی اجتماعی را بر اساس سه معیار کانال، گرداننده و نوع می‌توان دسته‌بندی کرد [16]. (شکل

(۱)

ب- استفاده از رویه‌های احسن برای کاهش

ریسک

- برای سنجش وضعیت کارمندان و پیمانکاران، رویه‌های صحت‌گذاری باید مد نظر قرار گیرد.
- سیستم‌های طبقه‌بندی داده با چارچوب‌هایی برای آزادسازی اطلاعات در هر سطح، تدوین شود.
- برای پیامدهای امنیتی تمامی کارمندان، برنامه آموزشی گذاشته شود.
- پرسنل کلیدی باید آموزش‌هایی برای مقاومت در برابر حملات مهندسی اجتماعی ببینند.
- تست‌های نفوذ پذیری و اطمینان از اطلاعات بطور مستمر، برای توسعه آگاهی و بازخورد سریع از کارمندان گرفته شود.
- بطور مستمر و اتفاقی، مانورهای مهندسی اجتماعی در سازمان انجام شود.
- تمام کارمندان باید از حملات مهندسی اجتماعی آگاه باشند. تا خود قاضی خود باشند و مثلاً اگر فکر می‌کنند نامه‌ای مشکوک است، آن را باز نکنند.
- باید به تمام کارمندان فنی مفاهیم اسب تراوا و نامه‌های زنجیره‌ای توضیح داده شود.
- به تمام کاربران سیستم اطلاعاتی باید آموزش داده شود که چگونه از نرم‌افزارهای ضد ویروس استفاده کنند و آن را بروز رسانی کنند. نیز آگاه باشند که پیوست نامه‌های الکترونیکی و پیوندهای ناشناخته را باز نکنند.
- آگاهی باید همواره در سطح بالایی قرار گیرد. به همین دلیل باید دوره‌های روزرسانی وجود داشته باشد و بعنوان مثال در آن‌ها نمونه‌های جدید حملات مهندسی اجتماعی بیان شود.
- عمق دفاع در سیستم جزء مهمی در امنیت است و از حمله‌های چندگانه جلوگیری می‌کند. باید از چک کردن‌های دولایه یا سه لایه استفاده شود.
- باید ممیزی‌های مستمری وجود داشته باشد و رویه‌های امنیتی با استفاده از کارمندان همواره تست شود. مثلاً چک شود که دستگاه‌های غیرمجاز به سیستم اطلاعاتی سازمان، متصل نشده باشند.



شکل ۱: طبقه بندی حملات مهندسی اجتماعی

۲-۱-۳- استراتژی‌های رویارویی با حملات مهندسی

اجتماعی

استراتژی‌های مستند شده پاسخگویی، این اطمینان را به وجود می‌آورند که کارمند در شرایطی که تحت فشار است، دقیقاً بداند که باید از چه رویه‌هایی پیروی کند. بعنوان مثال، اگر کارمند درخواستی را دریافت کرد، صحت آن را قبل از عمل به آن دستورالعمل، بررسی کند و اگر قبلاً به آن درخواست عمل کرده بود، باید رئیس را از این موضوع مطلع کند. از این به بعد، این مسئولیت رئیس است که مطمئن شود هیچ کارمند دیگری به درخواست‌های مشکوک پاسخ نمی‌گوید.

الف- استراتژی‌های محافظت از پسرود و روش‌های صحت

گذاری

متداول‌ترین اطلاعاتی که مهاجم مهندسی اجتماعی سعی در آگاهی از آن دارد، دانستن رویه‌های اعتبار سنجی می‌باشد. به محض اینکه پسرود کارمندی لو برود، هکر کنترل اوضاع را در دست خواهد گرفت و به سازمان ضرر خواهد رساند. سیاست پسرود بسیار ساده است. درباره پسرود هرگز، نه تنها در تلفن بلکه هر زمان دیگر صحبت نکنید. کاربران باید بطور کامل از اهمیت پسرودشان آگاه باشند و اگر به آنها آموزش لازم داده نشود آن را بدون هیچ فکر و واهمه‌ای در اختیار دیگران قرار می‌دهند. پسرودها باید در زمانهای متوالی تعویض شوند و قوانین پسرود توسط مدیران ارشد به کارمندان القاء شود. البته راه حل‌های تکمیلی دیگری چون PIN و ID کارت‌ها نیز برای حفظ دسترسی به سیستم‌های مهم وجود دارد. البته باید توجه کرد که اولین اقدام هر هکر آن خواهد بود که در اولین فرصت PINها را عوض کند.

ه- ممیزی پذیرش و کاربری سیاست‌ها

تدوین استراتژی‌ها، سیاست‌ها و کارمندان آموزش دیده در صورتیکه موافقتی با آن وجود نداشته باشد، کاملاً بی‌ارزش خواهد بود؛ بنابراین نیاز به ممیزی کاربری سیاست‌ها در سازمان می‌باشد. برای مثال، هنگامیکه تضمین کیفیت برای پروژه‌ای اجرا می‌شود، یکی از گام‌ها، ارزیابی پذیرش سیاست‌های امنیتی در سازمان می‌باشد. برای مثال رویه‌های ممیزی خاصی باید وجود داشته باشد تا مطمئن شویم کارمند Helpdesk، درباره پسورد، پشت تلفن یا از طریق نامه‌های رمزنگاری نشده، صحبت نمی‌کند. مدیران نیز باید بطور دوره‌ای دسترسی‌های کارمندان را بازنگری کنند. ممیزی امنیتی نیز باید اطمینان حاصل کند که افراد دیگر دسترسی‌های غیرلازم را ندارد. نقاط دسترسی نیز مانند درب‌ها و... باید همواره مانیتور شوند. بدین ترتیب اطمینان حاصل می‌شود که کارمندان سیاست‌های امنیتی را برای دسترسی به نقاط امن، رعایت می‌کنند. محل کار کارمندان نیز باید بطور تصادفی مورد بازرسی قرار گیرد تا مطمئن شویم اسناد محرمانه در کمد‌های امن قرار گرفته‌اند. محل‌های کار نیز خارج از زمان‌های کاری، باید همواره قفل باشند. [3]

۲-۲- پیشینه تحقیق:

فرانکو موتون (۲۰۱۸) در تحقیقی با عنوان «مدل شناسایی حملات مهندسی اجتماعی» به دنبال بازنگری در مدل‌های موجود در زمینه شناسایی حملات مبتنی بر مهندسی اجتماعی بوده است. وی در مطالعه خود نسبت به معرفی سه مدل جهت شناسایی حملات مهندسی اجتماعی اقدام نمود. در مدل اول که برای یک مرکز تلفن طراحی شده بود جهت منع حملات در ارتباطات دو طرفه مورد استفاده قرار گرفت. مدل دوم وی برای جلوگیری از حملات مهندسی اجتماعی در ارتباطات یک طرفه طراحی گردید. مدل سوم وی برای ممانعت از حملات در ارتباطات خودکار محدود طراحی گردید. [5]

کایل تورنتن (۲۰۱۷) در تحقیقی با عنوان «شناسایی انواع حملات مهندسی اجتماعی و راه کارهای مقابله با آن» ضمن تشریح تفصیلی حملات مهندسی اجتماعی به شناسایی و طبقه

- تهدیدهای درونی شناسایی شوند. پیمانکاران و دانشی را که کارمندان هنگام ترک سازمان با خود می‌برند. کنترل شود.
- برای رسانه‌های مشکوک، مدیریت و برنامه‌ریزی وجود داشته باشد.

ج- فرهنگ امنیت

ایجاد فرهنگ امنیت اطلاعات در سازمان، فرایندی است اثر بخش که گام‌های زیر را در بر خواهد داشت:

- ایجاد آگاهی از حملات امنیتی در کارمندان
- فراهم سازی ابزارهای مقابله
- برقراری ارتباطات دو طرفه میان پرسنل امنیت، مدیران و کارمندان

ایجاد فرهنگ امنیت، امری زمان بر بوده و به آن با عنوان سرمایه‌گذاری بلند مدت باید نگاه کرد که نیاز به تلاش مستمر، بهبود و نگه داری دارد.

د- بررسی اعتبار

اعتبارسنجی مدارک و احراز هویت باید در سازمان نهادینه شود و برای تمام کسانی که به ادعا یا سمتشان شک می‌رود مورد استفاده قرار گیرد؛ چه یونیفرم سازمان را پوشیده باشد و چه ادعا کند که در حالت اضطراری هستند. بررسی اعتبار سه مرحله دارد:

- اعتبار سنجی مشخصات
- اعتبار سنجی رتبه کارمندی
- اعتبار سنجی «نیاز به دانستن»

چنین استراتژی‌های اعتبار سنجی فقط زمانی مؤثر خواهد بود که بعنوان سیاست‌های امنیتی توسط مدیر ارشد پشتیبانی شوند. از آنجایی که مهندس اجتماعی از توانایی دسترسی افراد به اطلاعات، سوء استفاده می‌کند؛ بنابراین اگر کسی مدیر ارشد را برای احراز هویتش به چالش بیندازد، نباید او را سرزنش کرد. اگر با کارمندان بطور مسالمت آمیزی رفتار نشود، آنها توانایی و دلگرمی خود را در چالش کشیدن هر کسی که ادعای ارشد بودن می‌کند را از دست خواهند داد؛ بنابراین باید به آنها آموزش داد تا به گونه‌ای دوستانه از دیگران بخواهند که خودشان را به سازمان بشناسانند.

پیش آزمون و همچنین مقدار آلفای نهایی در جدول زیر آورده شده است.

$$\alpha = \left(\frac{j}{j-1} \right) \left(1 - \frac{\sum S^2 j}{S^2} \right)$$

در این فرمول α برآورد اعتبار آزمون، j تعداد سوال های آزمون، $S^2 j$ واریانس زیر مجموعه j ام و S^2 واریانس است.

جدول ۱: پایایی متغیرهای تحقیق

متغیر	آلفای کرونباخ
استفاده از تلفن همراه	۰.۸۱۱
آگاهی از مد	۰.۷۴۳
رهبری	۰.۸۳۴
آگاهی از سلامت	۰.۸۱۴
آسوده خاطر بودن	۰.۷۲۵
آگاهی از جامعه	۰.۷۱۱
آگاهی از هزینه	۰.۸۶۴
کاربردی بودن	۰.۹۱۲

جامعه آماری این پژوهش شامل کارکنان سازمان نظامی هدف در شهر تهران می باشد. روش نمونه گیری تحقیق حاضر تصادفی ساده می باشد.

از آنجائی که جامعه آماری تحقیق حاضر شامل کارکنان سازمان نظامی در شهر تهران بوده و تعداد آنها نامشخص می باشد، جهت تعیین حداقل حجم نمونه لازم، از فرمول کوکران برای جامعه نامحدود استفاده گردید:

$$n = \frac{z^2 pq}{d^2}$$

$$n = \frac{(1/96)^2 (0/5)(1-0/5)}{(0/5)(1-0/5)} \approx 384$$

که در آن:

n = حداقل حجم نمونه لازم

p = نسبت توزیع صفت در جامعه

بندی انواع این حملات پرداخته است. وی ضمن بر شمردن تعدادی از حملات به راهبردهای مقابله با این حملات از جمله مدیریت آگاهانه، حفاظت فیزیکی، آموزش کارکنان، خط و مشی های امنیتی شفاف اشاره می نماید.

کوته اشمیت (۲۰۱۶) در تحقیقی با عنوان « امنیت سایبری، ریسک، و آسیب پذیری ها و شاخص های جلوگیری از حملات مهندسی اجتماعی » به بررسی تهدیدات این نوع از حملات در فضای سایبری اقدام نموده است. وی در تحقیق خود بر تدوین استانداردها و خط و مشی های امنیتی برای دارایی های سخت افزاری و نرم افزاری شرکت ها و نیز آموزش قوانین و مقررات به کارکنان را در جلوگیری از حملات مهندسی اجتماعی موثر دانسته است.

مارتین لیختنشتاین (۲۰۱۵) در تحقیقی با عنوان «مهندسی اجتماعی و کاهش ریسک های انسانی» به بررسی عوامل موثر بر کاهش ریسک ناشی از حملات مهندس اجتماعی در اثر خطاهای نیروی انسانی سازمان ها پرداخته است. وی در این تحقیق با تمرکز بر عوامل انسانی به شناسایی هشت مولفه موثر در این زمینه پرداخته است. مهمترین این مولفه ها شامل آموزش منابع انسانی، تدوین خط و مشی های امنیتی شفاف، جلب اعتماد کارکنان و مدیریت دسترسی می باشد.

فرانکو موتون (۲۰۱۴) در تحقیقی با عنوان « چارچوب حملات مهندسی اجتماعی » ضمن بررسی الزامات امنیتی در زمینه مقابله با حمله نوع مهندسی اجتماعی به ارائه مولفه ها و عناصر دخیل در این امر پرداخته است. نتایج پژوهش وی بیانگر آن است که افزایش سطح آگاهی کارکنان سازمان به همراه کنترل موثر دسترسی ها از مهم ترین مولفه های چارچوب ارائه شده می باشد.

۳- روش شناسی تحقیق

تحقیق حاضر از نظر هدف کاربردی می باشد. همچنین تحقیق حاضر از نظر گردآوری داده ها و اطلاعات و روش تجزیه و تحلیل یک تحقیق توصیفی و غیر آزمایشی می باشد. برای کسب اطمینان از اعتبار ابزار از ضریب آلفای کرونباخ استفاده می شود که بعد از توزیع ۲۰ پرسشنامه، پایایی متغیرهای پرسشنامه بصورت

	Total	90	100.0	100.0
--	-------	----	-------	-------

با توجه به جدول شماره ۳ می‌توان بیان نمود که ۱۱.۱ درصد افراد نمونه آماری ما دارای سابقه کاری بین ۱۵ الی ۲۰ سال، ۴.۴ درصد دارای سابقه کاری بین ۱۰ الی ۱۵ سال، ۲.۲ درصد دارای سابقه کاری ۲۰ سال به بالا، ۳۶.۷ درصد دارای سابقه کاری بین ۵ الی ۱۰ سال و ۴۵.۶ درصد دارای سابقه زیر ۵ سال بوده‌اند. لازم به ذکر است ۶۵ نفر از شعبه و ۲۵ نفر از ستاد پاسخگوی پرسشنامه‌ها بوده‌اند.

ب) یافته‌های استنباطی:

در این بخش از تحقیق به بررسی الگوی تحقیق و همچنین تحلیل روابط بین متغیرهای تحقیق پرداخته می‌شود.

هر ۳ سوال یک عامل را بررسی می‌کند و هر سوال با ۵ گزینه ارزیابی می‌شود. در بررسی‌های انجام شده در نرم افزار SPSS دو گزینه‌ای که به عنوان ریسک‌پذیری بالا مورد نظر بود یک، و سه گزینه‌ای دیگر صفر در نظر گرفته شده‌اند.

در ادامه به بررسی رابطه بین هر یک از عوامل با سن، جنسیت، سابقه کاری، تاهل، تحصیلات و واحد سازمانی (ستاد یا شعبه) از طریق انجام آزمون مربع کای ۳ در نرم افزار SPSS پرداخته شده است.

آزمون خی‌دوی یا آزمون کی دو یا خی دو یا مربع کای از آزمون‌های آماری و از نوع ناپارامتری است و برای ارزیابی هم-قواری متغیرهای اسمی به کار می‌رود. [1]

$$\chi^2 = \sum_{t=1}^m \frac{(O_t - E_t)^2}{E_t}$$

O = فراوانی‌های مشاهده شده

E = فراوانی‌های مورد انتظار

اگر میزان بدست آمده برای این آزمون کمتر از ۰.۱ باشد، نشان دهنده میزان اختلاف معنی دار بین متغیرها است.

این آزمون تنها راه حل موجود برای آزمون همگنی در مورد متغیرهای مقیاس اسمی با بیش از دو مقوله‌است، بنابراین

$z\alpha/2$ = مقدار به دست آمده از جدول توزیع نرمال استاندارد (در این تحقیق و با در نظر گرفتن مقدار خطای ۰/۰۵، مقدار به دست آمده از جدول توزیع نرمال استاندارد ۱/۹۶ می‌باشد).

d = خطای پذیرفته شده توسط محقق یا بازه قابل تحمل از برآورد پارامتر مورد نظر (معمولاً در علوم اجتماعی برابر ۰/۰۵ در نظر گرفته می‌شود).

نکته‌ای که لازم است در خصوص این فرمول، گفته شود آن است که چنانچه مقدار p در دسترس نباشد، می‌توان مقدار ۰/۵ را برای آن در نظر گرفت، که در این حالت، این فرمول بزرگترین و محافظه کارانه‌ترین عدد ممکن را به دست خواهد داد، که در این تحقیق نیز عدد ۰/۵ برای آن در نظر گرفته شد. با جایگذاری پارامترها در فرمول مذکور حجم نمونه لازم با اعمال ظریب امنیتی ۴۸۴ نفر خواهد بود.

۴- یافته‌ها و تجزیه و تحلیل داده‌ها:

الف: یافته‌های جمعیت‌شناسی تحقیق

بررسی وضعیت تحصیلات در نمونه آماری

جدول ۲: بررسی وضعیت تحصیلات در نمونه آماری

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	8.9	8.9	8.9
	2	64	71.1	71.1	80.0
	3	14	15.6	15.6	95.6
	4	4	4.4	4.4	100.0
	Total	90	100.0	100.0	

با توجه به جدول شماره ۲ می‌توان بیان نمود که فوق‌دیپلم ۸.۹ درصد، افراد لیسانس ۷۱.۱ درصد، فوق‌لیسانس ۱۵.۶ درصد، و دکتری ۴.۴ درصد از کل نمونه تحقیق را تشکیل می‌دهند.

بررسی وضعیت سابقه کاری

جدول ۳: بررسی وضعیت سابقه کاری در نمونه آماری

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	41	45.6	45.6	45.6
	2	33	36.7	36.7	82.2
	3	4	4.4	4.4	86.7
	4	10	11.1	11.1	97.8
	5	2	2.2	2.2	100.0

3 Chi-squared test

N of Valid Cases	90		
------------------	----	--	--

با توجه به مقدار به دست آمده از جدول ۶ برای Pearson Chi-Square که برابر است با ۰.۶۳۴ اختلاف معنا داری از لحاظ ترس در رده های سنی مختلف وجود ندارد.

بررسی رابطه بین تحصیلات و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۷: بررسی رابطه بین تحصیلات و ترس

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.149a	3	.027
Likelihood Ratio	14.031	3	.003
Linear-by-Linear Association	6.668	1	.010
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۷ برای Pearson Chi-Square که برابر است با ۰.۰۲۷ اختلاف معنا داری از لحاظ ترس در رده های تحصیلی مختلف وجود دارد.

بررسی رابطه بین سابقه کاری و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۸: بررسی رابطه بین سابقه کاری و ترس

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.973a	4	.410
Likelihood Ratio	5.585	4	.232
Linear-by-Linear Association	1.605	1	.205
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۸ برای Pearson Chi-Square که برابر است با ۰.۴۱۰ اختلاف معنا داری از لحاظ ترس با سابقه کاری وجود ندارد.

بررسی رابطه بین واحد سازمانی و عامل ترس

کاربرد خیلی زیادتری نسبت به آزمون های دیگر دارد. این آزمون نسبت به حجم نمونه حساس است. آزمون کای اسکوئر برای تعیین تفاوت ها میان چند چیز هم بکار می رود.

بررسی رابطه بین متغیرهای دموگرافی با عامل ترس

بررسی رابطه بین جنسیت و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۵: بررسی رابطه بین جنسیت و ترس

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.992a	1	.084		
Continuity Correction ^b	2.052	1	.152		
Likelihood Ratio	3.430	1	.064		
Fisher's Exact Test				.136	.071
Linear-by-Linear Association	2.958	1	.085		
N of Valid Cases ^b	90				

با توجه به مقدار به دست آمده از جدول ۵ برای Pearson Chi-Square که برابر است با ۰.۰۸۴ اختلاف معنا داری از لحاظ ترس در میان مردان و زنان وجود دارد.

بررسی رابطه بین سن و عامل ترس

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۶: بررسی رابطه بین سن و ترس

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.911a	2	.634
Likelihood Ratio	.920	2	.631
Linear-by-Linear Association	.535	1	.465

با توجه به مقدار به دست آمده از جدول ۱۰ برای Pearson Chi-Square که برابر است با ۰.۰۰۴ اختلاف معنا داری از لحاظ طمع در بین مردان و زنان وجود دارد.

بررسی رابطه بین سن و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۱: بررسی رابطه بین سن و طمع

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.297a	2	.192
Likelihood Ratio	5.330	2	.070
Linear-by-Linear Association	2.527	1	.112
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۱۰ برای Pearson Chi-Square که برابر است با ۰.۱۹۲ اختلاف معنا داری از لحاظ طمع در رده های سنی مختلف وجود ندارد.

بررسی رابطه بین ازدواج و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۲: بررسی رابطه بین ازدواج و طمع

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.150a	1	.699		
Continuity Correction ^b	.008	1	.931		
Likelihood Ratio	.154	1	.695		
Fisher's Exact Test				1.000	.478
Linear-by-Linear Association	.148	1	.700		
N of Valid Cases ^b	90				

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۹: بررسی رابطه بین واحد سازمانی و ترس

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.013a	1	.908		
Continuity Correction ^b	.000	1	1.000		
Likelihood Ratio	.013	1	.908		
Fisher's Exact Test				1.000	.564
Linear-by-Linear Association	.013	1	.909		
N of Valid Cases ^b	90				

با توجه به مقدار به دست آمده از جدول ۹ برای Pearson Chi-Square که برابر است با ۰.۹۰۸ اختلاف معنا داری از لحاظ ترس در واحدهای سازمانی مختلف وجود ندارد.

بررسی رابطه بین متغیرهای دموگرافی با عامل طمع

بررسی رابطه بین جنسیت و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۰: بررسی رابطه بین جنسیت و طمع

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	8.473a	1	.004		
Continuity Correction ^b	6.661	1	.010		
Likelihood Ratio	7.380	1	.007		
Fisher's Exact Test				.007	.007
Linear-by-Linear Association	8.379	1	.004		
N of Valid Cases ^b	90				

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۴: بررسی رابطه بین واحدسازمانی و طمع

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.986a	1	.321		
Continuity Correction ^b	.497	1	.481		
Likelihood Ratio	.947	1	.330		
Fisher's Exact Test				.389	.237
Linear-by-Linear Association	.975	1	.323		
N of Valid Cases ^b	90				

با توجه به مقدار به دست آمده از جدول ۱۴ برای Pearson Chi-Square که برابر است با ۰.۳۲۱ اختلاف معنا داری از لحاظ طمع در واحدهای سازمانی مختلف وجود ندارد.

بررسی رابطه بین متغیرهای دموگرافی با عامل اطاعت

بررسی رابطه بین جنسیت و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۵: بررسی رابطه بین جنسیت و اطاعت

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.532a	1	.112		
Continuity Correction ^b	1.590	1	.207		
Likelihood Ratio	2.305	1	.129		
Fisher's Exact Test				.183	.106
Linear-by-Linear Association	2.503	1	.114		
N of Valid Cases ^b	90				

با توجه به مقدار به دست آمده از جدول ۱۱ برای Pearson Chi-Square که برابر است با ۰.۶۹۹ اختلاف معنا داری از لحاظ طمع با ازدواج وجود ندارد.

بررسی رابطه بین تحصیلات و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۲: بررسی رابطه بین تحصیلات و طمع

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.745a	3	.191
Likelihood Ratio	7.199	3	.066
Linear-by-Linear Association	.151	1	.697
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۱۲ برای Pearson Chi-Square که برابر است با ۰.۱۹۱ اختلاف معنا داری از لحاظ طمع در رده های تحصیلی مختلف وجود دارد.

بررسی رابطه بین سابقه کاری و عامل طمع

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۳: بررسی رابطه بین سابقه کاری و طمع

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.053a	4	.399
Likelihood Ratio	6.485	4	.166
Linear-by-Linear Association	3.443	1	.064
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۱۳ برای Pearson Chi-Square که برابر است با ۰.۳۹۹ اختلاف معنا داری از لحاظ طمع با سابقه کاری وجود ندارد.

بررسی رابطه بین واحد سازمانی و عامل طمع

با توجه به مقدار به دست آمده از جدول ۱۷ برای Pearson Chi-Square که برابر است با ۰.۰۰۵ اختلاف معنا داری از لحاظ اطاعت با ازدواج وجود دارد.

بررسی رابطه بین تحصیلات و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۸: بررسی رابطه بین تحصیلات و اطاعت

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.868a	3	.049
Likelihood Ratio	7.166	3	.067
Linear-by-Linear Association	.634	1	.426
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۱۸ برای Pearson Chi-Square که برابر است با ۰.۰۴۹ اختلاف معنا داری از لحاظ اطاعت در رده های تحصیلی مختلف وجود دارد.

بررسی رابطه بین سابقه کاری و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۹: بررسی رابطه بین سابقه کاری و اطاعت

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.515a	4	.642
Likelihood Ratio	3.149	4	.533
Linear-by-Linear Association	.027	1	.870
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۱۹ برای Pearson Chi-Square که برابر است با ۰.۶۴۲ اختلاف معنا داری از لحاظ اطاعت با سابقه کاری وجود ندارد.

بررسی رابطه بین واحد سازمانی و عامل اطاعت

با توجه به مقدار به دست آمده از جدول ۱۵ برای Pearson Chi-Square که برابر است با ۰.۱۱۲ اختلاف معنا داری از لحاظ اطاعت در بین مردان و زنان وجود دارد.

بررسی رابطه بین سن و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۶: بررسی رابطه بین سن و اطاعت

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	16.293a	2	.000
Likelihood Ratio	13.119	2	.001
Linear-by-Linear Association	9.459	1	.002
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۱۶ برای Pearson Chi-Square که برابر است با ۰.۰۰۱ اختلاف معنا داری از لحاظ اطاعت در رده های سنی مختلف وجود دارد.

بررسی رابطه بین ازدواج و عامل اطاعت

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۱۷: بررسی رابطه بین ازدواج و اطاعت

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	7.792a	1	.005		
Continuity Correction ^b	6.205	1	.013		
Likelihood Ratio	12.211	1	.000		
Fisher's Exact Test				.005	.002
Linear-by-Linear Association	7.705	1	.006		
N of Valid Cases ^b	90				

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۲۰: بررسی رابطه بین واحدسازمانی و اطاعت

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.026a	1	.873		
Continuity Correction ^b	.000	1	1.000		
Likelihood Ratio	.026	1	.872		
Fisher's Exact Test				1.000	.561
Linear-by-Linear Association	.025	1	.873		
N of Valid Cases ^b	90				

با توجه به مقدار به دست آمده از جدول ۲۰ برای Pearson Chi-Square که برابر است با ۰.۸۷۳ اختلاف معنا داری از لحاظ اطاعت در واحدهای سازمانی مختلف وجود ندارد.

بررسی رابطه بین متغیرهای دموگرافی با عامل خیرخواهی

بررسی رابطه بین جنسیت و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۲۱: بررسی رابطه بین جنسیت و خیرخواهی

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.366a	1	.545		
Continuity Correction ^b	.113	1	.737		
Likelihood Ratio	.368	1	.544		
Fisher's Exact Test				.599	.370
Linear-by-Linear Association	.362	1	.547		
N of Valid Cases ^b	90				

با توجه به مقدار به دست آمده از جدول ۲۱ برای Pearson Chi-Square که برابر است با ۰.۵۴۵ اختلاف معنا داری از لحاظ خیرخواهی در بین مردان و زنان وجود ندارد.

بررسی رابطه بین سن و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۲۲: بررسی رابطه بین سن و خیرخواهی

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.405a	2	.041
Likelihood Ratio	6.484	2	.039
Linear-by-Linear Association	1.933	1	.164
N of Valid Cases	90		

با توجه به مقدار به دست آمده از جدول ۲۲ برای Pearson Chi-Square که برابر است با ۰.۰۴۱ اختلاف معنا داری از لحاظ خیرخواهی در رده های سنی مختلف وجود دارد.

بررسی رابطه بین ازدواج و عامل خیرخواهی

زمانی اختلاف معنا داری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۲۳: بررسی رابطه بین ازدواج و خیرخواهی

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.063a	1	.802		
Continuity Correction ^b	.000	1	.996		
Likelihood Ratio	.063	1	.802		
Fisher's Exact Test				1.000	.499
Linear-by-Linear Association	.062	1	.803		
N of Valid Cases ^b	90				

با توجه به مقدار به دست آمده از جدول ۲۳ برای Pearson Chi-Square که برابر است با ۰.۸۰۲ اختلاف معنا داری از لحاظ خیرخواهی با ازدواج وجود ندارد.

۵- نتیجه گیری:

بررسی رابطه بین تحصیلات و عامل خیرخواهی

زمانی اختلاف معناداری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۲۴: بررسی رابطه بین تحصیلات و خیرخواهی

با توجه به مقدار به دست آمده از جدول ۲۴ برای Pearson Chi-Square که برابر است با ۰.۰۵ اختلاف معناداری از لحاظ خیرخواهی در رده های تحصیلی مختلف وجود دارد.

بررسی رابطه بین سابقه کاری و عامل خیرخواهی

زمانی اختلاف معناداری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۲۵: بررسی رابطه بین سابقه کاری و اطاعت

Pearson با توجه به مقدار به دست آمده از جدول ۲۵ برای Chi-Square که برابر است با ۰.۰۰۱ اختلاف معنا داری از لحاظ خیرخواهی، با سابقه کاری وجود دارد.

بررسی رابطه بین واحد سازمانی و عامل خیرخواهی

زمانی اختلاف معناداری بین دو عامل وجود دارد که مقدار Pearson Chi-Square کمتر از ۰.۱ است.

جدول ۲۶: بررسی رابطه بین واحدسازمانی و خیرخواهی

شکل ۳: الگوی شناسایی حملات مهندسی اجتماعی در سازمان های نظامی

سطح ۱: تدوین خط و مشی های امنیتی مناسب:

هیچ دژی بدون پایه‌های مستحکم و پایدار، دوام پیدا نخواهد کرد. اساس امنیت اطلاعات سیاست‌های آن است. سیاست‌های امنیتی، استانداردها و سطوح امنیتی شبکه را تعیین می‌کند. این بنیان زمانی حیاتی تر می‌گردد که سیاست‌های امنیتی بخواند شبکه را از حملات مهندسی اجتماعی مصون بدارد. سیاست‌های

پسوردش را به من بدهد.» نکته در اینجا است که هدف هر یک پیچیده تر بوده و سعی در ایجاد اطمینان در فرد و سوء استفاده از آن می باشد. کارمندان باید آگاه باشند که مهاجم مهندسی اجتماعی به چه اطلاعات اولیه ای نیاز خواهد داشت و از چه گفتگو هایی در راه رسیدن به آن استفاده خواهد کرد. همچنین کارمندان باید بدانند چگونه اطلاعات محرمانه را تشخیص دهند و مسئولیتشان را در قبال محافظت از آن بدانند. آنها باید بدانند که چگونه در مقابل خواسته های غیرمجاز «نه» بگویند و چه زمانی برای گفتن این کلمه مناسب است! برنامه های آموزشی نیز باید از سیاست های امنیتی پیروی کند. این بخش از نتایج با یافته های لیختنشتاین (۲۰۱۵) مه بر امر آموزش کارکنان تاکید داشت در انطباق می باشد.

سطح ۳: آموزش پرسنل کلیدی سازمان

نه تنها تمام کارمندان باید آگاهی های امنیتی را آموزش ببینند، بلکه در دفاع چند لایه، باید آموزش مقاومت برای پرسنل کلیدی نیز وجود داشته باشد. پرسنل کلیدی پرسنل راهنمایی، خدمات به مشتریان، منشی ها، تحویل داران و مهندسان و ناظران سیستم را شامل می شود یا بطور کلی هر کسی که کار یاری رسانی و رویارویی با دیگران را در سازمان ایفا می کند. آموزش مقاومت منجر می شود که کارمندان از متقاعد شدن و افشای اطلاعات مورد نیاز هکر، دوری جویند. روش های آموزش مقاومت در ادبیات روانشناسی اجتماعی وجود دارد و کاربران را در برابر تکنیک های هک، قوی می کند.

- واکسیناسیون: این روش منطبق با ایده واکسیناسیون بوده، بطوریکه ضعیف شده آن چیزی که هکرها از کارمندان می خواهند را، به کارمندان آموزش می دهیم. هکر نیز از روش های مشابه پیروی خواهد کرد؛ بنابراین واکسن از توسعه یک روش جلوگیری می کند.
- پیش آگاهی: قبل از آنکه اتفاقی رخ دهد در مورد آن اخطار داده و بصورت پیام بگوش همه می رسانی، در اخطار نه تنها از امکان حمله مهاجم اجتماعی خبر می دهیم بلکه روش ها و چگونگی حمله را نیز بیان می کنیم.
- سنجش واقعیت: یکی از دلایل آموزش آگاهی امنیتی به این خاطر است که همگان نسبت به آسیب پذیریشان بطور غیر واقعی خوش بین هستند. این برداشت خیلی ها را از دیدن ریسک های به حق، دور

مهندسی اجتماعی به کارمندان چگونگی پاسخ دهی به درخواست های مشکوک را می آموزد. سیاست های تثبیت شده، کمک می کند که کاربر نهایی حس کند، چاره ای جز مقاومت در برابر خواست هکران ندارد. کاربران نهایی نیز نباید نقش تصمیم گیرنده برای در اختیار گذاری اطلاعات، را داشته باشند. نکته جالب دیگری که در تئوری تحریک و تشویق وجود دارد، فرا شناخت می باشد. فراشناخت، توانمندی است که با آن از اندیشه و فرایند فکر کردن دیگران می توان آگاه شد. با توجه به مطالعات انجام شده درباره فراشناخت در تئوری تحریک، محققان به این نتیجه رسیده اند که یکی از راه های مقاومت سازی در برابر حملات، توسعه اعتماد به فکر، در کارمندان می باشد. نتایج این بخش با یافته های اشمیت (۲۰۱۶) در مورد اولیت تدوین سیاست ها و خط و مشی های امنیتی در برابر حملات مهندسی اجتماعی تطابق دارد. سیاست های امنیتی واضح و روشن، خطر تأثیر گذاری متجاوزان بر روی کارمندان را کاهش می دهد. سیاست امنیتی باید حوزه های خاصی را مد نظر قرار دهند تا بتوانند بعنوان پایه های مقاومت مهندسی اجتماعی بحساب آیند. کنترل دسترسی به اطلاعات، راه اندازی حساب ها، تأیید دسترسی و تغییر در کلمات عبور باید در نظر گرفته شود. سیاست ها باید نظم و دیسیپلین داشته باشند و به همگان ابلاغ شوند. سطح سیاست امنیت در دفاع، به دفاع کارمندان در برابر تحریکات روانشناسانه ای مانند قدرت، حس مسئولیت و... کمک می کند. همچنین در سیاست ها باید سطوح مسئولیت، برای اطلاعات یا دسترسی تعیین شوند. بطوریکه اگر فرد اطلاعات در دسترسش را در اختیار دیگران قرار دهد، دیگر هیچ نقطه سؤال برانگیزی باقی نماند.

سطح ۲: آموزش همگانی کارکنان

پس از تثبیت سیاست های امنیتی، تمام کارمندان باید برای آگاهی های امنیتی آموزش ببینند. سیاست امنیتی همانگونه که انگیزه های امنیتی را بوجود می آورند، چارچوب آموزش را نیز تعیین خواهند کرد. سیاست هایی که با تفکر تدوین شده باشند و به کارمندان آموزش داده شده باشند در پاسخگویی کارمندان به درخواست های مختلف، متجاوزان تمایز ایجاد خواهند کرد. آگاهی های امنیتی خیلی پیچیده تر از آنست که به کارمندان بگوییم که پسوردشان را به کسی ندهند. بطوریکه هکر معروف کوین میتنیک گفته است: «من هرگز از کسی نخواسته ام که

[۲] قوچانی، محمد مهدی، موسوی، امیر، حسین پور، داود (۱۳۹۴). حفاظت و امنیت اطلاعات با ارائه الگوی مفهومی مهندسی اجتماعی. فصلنامه پژوهش‌های حفاظتی-امنیتی. دانشگاه جامع امام حسین (ع) سال سوم. شماره ۱۴. صص. ۸۴.

ب- منابع انگلیسی:

- [۳] Allen, M. (June 2006). The use of "Social Engineering" as a means of violating compute systems. <http://www.sans.org/rr/paper.php?id=529>.
- [4] BilgeKarabacak, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers & Security*, 413-419.
- [۵] Francois Mouton, M. M. (2018). Social Engineering Attack Model. *Defence Peace Safety & Security, Council for Industrial and Scientific Research, South Africa*: 9.
- [۶] Fan, Wenjun, Lwakatare, Kevin. Rong, Rong. (2017) Social Engineering: I-E based model of Human Weakness for Attack and Defense Investigations. *Computer Network and Information Security*. Vol 5.no 12.
- [۷] Gartner. (2002). There Are No Secrets: Social Engineering and Privacy. *Social Engineering: Exposing the Danger Within*.
- [۸] Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. the United States of America: Wiley Publishing, Inc.
- [۹] Hanan Sandouka, D. C. (2009). Social Engineering Detection using Neural Networks. *International Conference on CyberWorlds, UK*: 6.
- [10] Lichtenstein, M. (2015). Social Engineering Mitigating Human Risk in Mitigating Human Risk in. *VASCO Data Security*.
- [11] Krombholz, Kathrina, Hobel, Heidelinde. Huber, Markuse. (2015). Advanced social engineering attacks. *Journal of information Security and Applications*, Vol 22.no 3.
- [12] M. Junger, L. M.-J. (January 2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, Volume 66, Pages 75-87.
- [13] MITNICK, K. D. (2004). *THE ART OF DECEPTION Controlling the Human Element of Security*.
- [14] Ram Bhakta, I. G. (2015). Semantic Analysis of Dialogs to Detect Social Engineering Attacks. *International Conference on Semantic Computing, USA*: 4.

می‌کند. اگر یکبار بتوانیم طی آموزش آنها را فریب دهیم و سپس نشان دهیم که چقدر آسیب پذیرند، آموزش بسیار مؤثر خواهد بود.

سطح ۴: تثبیت و یادآوری

دفاع چند لایه نیاز به یادآوری‌های متمادی از اهمیتی آگاهی دارد. تلنگری کوتاه مدت برای مقابله با نفوذگر، فقط در زمان کوتاهی مؤثر خواهد بود. یادآوری‌های متوالی و خلاقانه، برای هشجاری افراد از خطرهای موجود، مورد نیاز است. یکی از بهترین سیاست‌ها در نیروی پلیس اجرا می‌شود، بطوریکه آنها همواره به انسان‌ها یادآوری می‌کنند که چگونه همکارانشان طی عملیات مختلف کشته شده‌اند.

سطح ۵: مین گذاری برای آشکارسازی حملات

SELM ها، تله‌هایی در سیستم هستند که حمله‌ها را آشکار کرده و از وقوع آن جلوگیری می‌کنند. درست مثل میدان مین در صحنه نبرد. همانگونه که مین در صورت مقابله با متجاوز منفجر می‌شود، مهاجم را زمین گیر کرده و حمله را متوقف می‌سازد. SELM به قربانی هشدار می‌دهد که حمله‌ای در حال صورت گرفتن است و وضعیت امنیتی جدیدی را باید در پی گرفت.

سطح ۶: سطح تهاجمی

آخرین سطح دفاعی، پاسخ دهی به رویدادها می‌باشد. بدین ترتیب شبکه دیگر اجازه نمی‌دهد که مهاجم اجتماعی بتواند با کارمندان بی‌توجه به امنیت در سازمان، صحبت کند؛ بنابراین نیاز است که فرایندهای پاسخ دهی کاملاً معین باشند تا کارمندان به محض آنکه به فرد یا رفتاری مشکوک شدند، بتوانند آن را به گوش همگان برسانند. برای اثر بخشی بیشتر، باید فرد یا بخشی را برای رهگیری دقیق این رویدادها داشته باشیم، بطوریکه حملات بتوانند سریع و موثرتر شناسایی شوند. این فرد همان شخصی خواهد بود که لاگ‌های رسیده از افرادی که درخواست‌های مشکوک داشته‌اند را شناسایی می‌کند.

۶- فهرست منابع:

الف- منابع فارسی:

- [۱] رائگرز. جورج. (۱۳۹۷) / آمار و احتمال کاربردی مهندسی. مترجم کریم آتشگر. انتشارات دانشگاه علم و صنعت.

- [15] Ravne, M. H. (2005). Fighting Social Engineering. URL: www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-۲۸۱.pdf.
- [16] Peng, T., Harris, I., Sawa, Y. (2018) "Detecting phishing attacks using natural language processing and machine learning." 2018 IEEE 12th International Conference on Semantic Computing (ICSC). IEEE, 2018.
- [17] Sungho, K. J. (۲۰۰۷). Common defects in information security management system of Korean companies. *The Journal of Systems and Software*. 80.۱۶۳۸-۱۶۳۱, (۱۰)
- [18] Thornton, K. (Apr 14, 2017). 5 Types of Social Engineering Attacks. *datto*. Francois Mouton, Louise Leenen, Mercia M. Malan, and H.S. Venter; " Towards an Ontological Model Defining the Social Engineering Domain ", Defence Peace Safety & Security, Council for Industrial and Scientific Research, Pretoria, South Africa, ۱۵, ۲۰۱۴