مطالعه تطبیقی عوامل موثر بر وقوع تهدیدات امنیتی سهوی توسط کارمندان

بهرام علیشیری طالقانی[۱] ، کبری دهبسته[۲]

چکیده

کارکنان سازمان سازمان به دلیل دسترسی خود به اطلاعات، سیستم‌ها و شبکه سازمان، به عنوان یک منبع ریسک شناسایی می‌شوند و می‌توانند از منابع سازمان به منظور انجام جرایم و افشای اطلاعات محرمانه سازمان بصورت عمدی یا سهوی استفاده نمایند. بر اساس گزارش ، وقوع تهدیدات امنیتی در سازمانها در نتیجه اشتباهات و اقدامات سهوی کارکنان نتایج وخیمی را داشته است. لذا از آنجاییکه بسیاری از این نوع از تهدیدات سهوی متاثر از تکنیک ها و حملات مبتنی بر مهندسی اجتماعی بوده که از محدودیت عقلایی افراد بهره می برد و با توجه به اثرات و پیامدهای سنگین این

۱- هیات علمی و استادیار دانشکده مدیریت و حسابداری دانشگاه آزاد اسلامی واحد تهران جنوب
Bahramalishiri1350@yahoo.com
۲- دانشجوی مدیریت فناوری اطلاعات مقطع دکتری دانشگاه آزاد اسلامی واحد تهران جنوب rdehbasteh@gmail.com

نوع از تهدیدات، در این پژوهش سعی شده است تا با روش پیمایشی به بررسی و تطبیق عوامل موثر بر افزایش احتمال بروز حملات مبتنی بر مهندسی اجتماعی در کارکنان صنعت فناوری اطلاعات پرداخته شود. بنابر تحلیل صورت گرفته دو عامل سازمانی و انسانی بر روی افزایش خطای تصمیم گیری افراد و در نتیجه وقوع این نوع از تهدیدات موثر می باشد.

کلمات کلیدی: مهندسی اجتماعی، محدودیت عقلایی، تهدید امنیتی سهوی کارکنان

مقدمه

کارکنان سازمان به دلیل دسترسی خود به اطلاعات، سیستم‌ها و شبکه سازمان، به عنوان یک منبع ریسک شناسایی می‌شوند. کارکنانی که مشکلات مالی دارند و یا توسط ورود کارکنان جدید تحت تاثیر قرار می‌گیرند می‌توانند از منابع سازمان به منظور انجام جرایم و سرقت اطلاعات سازمان استفاده نمایند.

تهدید مربوط به حملات کارکنان سازمان جدی و واقعی است، بر اساس گزارش ارزیابی امنیتی فضای مجازی در سال ۲۰۱۱ که توسط مجله CSI (Computer Security Institute) منتشر شده است، در شرایطی که سازمان‌ها موفق به شناسایی منبع حمله خود شده‌اند، ۲۱٪ از حوادث توسط کارکنان سازمان صورت گرفته است و ۴۶٪ از سازمان‌های مورد بررسی حجم تخریب تهدیدهای کارکنان سازمان را بسیار بیشتر از تهدیدهای صورت گرفته از خارج از سازمان می‌دانند. بر اساس این بررسی جرایم الکترونیکی انجام شده توسط کارکنان سازمان شامل مواردی همچون دسترسی غیر مجاز و یا استفاده از اطلاعات سازمانی، انتشار سهوی اطلاعات حساس و یا محرمانه سازمان، انتشار ویروس، کرم و یا بدافزارهای دیگر و سرقت اطلاعات دارای مالکیت معنوی سازمان بوده است. همچنین بر

اساس گزارش شرکت مخابراتی Verizon در سال ۲۰۱۳، وقوع تهدیدات داخلی از قبیل ارسال اطلاعات محرمانه به مقصد نادرست و خطاهای مسئولین شبکه دارای تاثیرات سنگینی بوده و این شرکت متاثر از وقوع اشتباهات سهوی کارمندان خود بوده است.(Verizon RISK Team. 2013)

مقابله با تهدیدهای کارکنان سازمان امکانپذیر است ولی مقابله با این نوع از تهدیدات در حوزه مشکلات پیچیده طبقه بندی شده است. (Dawn Cappelli , Andrew Moore , Marisa Reddy Randazzo, Ph.D., 2004).

گردآوری اطلاعات مرتبط با تهدیدهای رایانه‌ای داخلی در سازمانها از اهمیت بالایی برخوردار می باشد ولی وجود دلایلی همچون عدم امکان تخمین و مشاهده دقیق خسارت وارده به سازمان، عدم امکان دریافت شواهد به منظور پیگیری‌های بعدی و وجود نگرانی‌های مسئولین سازمانها از ایجاد خسارت به شهرت و اعتبار سازمان در کسب اطلاعات این نوع از رخدادهای رایانه ای در سازمانها خدشه واردمی نماید (Eileen Kowalski, Dawn Cappelli , Bradford Willke, 2008) .

از سوی دیگر همانطور که گفته شد، سازمانها در معرض ریسک حاصل از اقدامات بسیاری از کارکنان خود بوده که به صورت سهوی و غیرعمد مواردی را انجام داده که در نهایت منجربه به تهدید سازمان می گردد. بر اساس گزارش شرکت AlgoSec در سال ۲۰۱۳، شرکتهای مورد مطالعه، حجم بالایی از تهدیدات سایبری سازمانها مرتبط با تهدیدات کارکنان سازمان دانسته و همچنین بیش از ۴۰ در صد از آنها بیان نموده اند که کارکنان سازمان بصورت تصادفی یا در اثر خطاهای مختلف منجربه نشت اطلاعات سازمان می گردند که یکی از منابع مهم نگرانی برای آنها محسوب می گردد. (. AlgoSec, Inc., 2013)

به منظور شناخت بهتر تهدیدات سهوی کارکنان سازمان، تعریف ارایه شده از سوی دانشگاه کارنگملون در این رابطه ارایه شده است، این نوع از تهدید یا UIT به کارکنان فعلی یا پیشین، پیمانکاران، شرکا و هر فردی که به نحوی دارای حقوق دسترسی مجاز به شبکه، سیستم و یا دیتای سازمان بوده و همچنین کسی که با انجام اقدامی بدون اهداف مخرب و خرابکارانه، منجربه صدمه و یا افزایش احتمال صدمات و تخریب و نقض محرمانگی، یکپارچگی و در دسترس پذیری اطلاعات و یا سیستم های اطلاعاتی سازمان گردد. بر اساس پژوهش دانشگاه مذکور، تهدیدات UIT از چهار منبع اصلی آغاز می گردند که شامل افشا و یا ارسال تصادفی اطلاعات، ورود بدافزارها به سازمان و اجرای آنها، امحای نادرست یا تصادفی اطلاعات غیرالکترونیکی و در نهایت به سرقت رفتن و یا مفقود شدن تجهیزات اطلاعاتی قابل حمل می باشد.

بسیاری از تهدیدات UIT موفق که در سازمانها اجرا شده و منجربه سرقت اطلاعات محرمانه گردیده است در نتیجه موفقیت مهاجم در تحریک و یا الزام کارکنان آن سازمان به اجرای موارد مورد نیاز او از طریق روشهای مهندسی اجتماعی صورت پذیرفته است. به همین دلیل در این مرحله نیاز به تعریف مفهوم مهندسی اجتماعی در رابطه با تهدیدات UIT در پژوهش می باشد. مهندسی اجتماعی در حوزه امنیت اطلاعات، به مفهومی گفته می شود که با تحت تاثیر قراردادن افراد، آنها ناآگاهانه مرتکب اعمالی شوند که به محرمانگی، یکپارچگی و در دسترس بودن منابع سازمان و یا دارایی های آن مانند اطلاعات، سیستم های اطلاعاتی و سیستم های مالی صدمه وارد گردد. مهندسی اجتماعی با تکیه بر محدودیتهای انسانی بر روانشناسی انسانها و متقاعد نمودن آنها تمرکز دارد.

به همین دلیل در این پژوهش سعی شده است تا پارامترهای موثر بر افزایش موفقیت حملات مهندسی اجتماعی و در نتیجه وقوع تهدیدات داخلی سهوی از سوی کارکنان مورد بررسی قرار گرفته و با شناسایی و بومی سازی این عوامل، منجربه یاری رساندن در خصوص شناسایی زودهنگام نشانه های وجود این تهدید در سازمان و در نتیجه کمک به پیاده سازی راهکارهای کاهش موارد مذکور به مدیران امنیت اطلاعات سازمانها گردد.

چارچوب نظری

بر اساس استاندارد امنیت اطلاعات، ISO 27001:2013، امنیت فناوری اطلاعات در سه حوزه افراد، تکنولوژی و فرآیندها تعریف می گردد. هر سازمان تهدیدات مرتبط با دارایی های اطلاعاتی خود را در هریک از سه حوزه مشخص نموده و سعی در شناسایی راهکارهای مقابله و کاهش سطح ریسک می نماید (Danijel Milicevic, Matthias Goeken,2013). اجرای سهوی تهدیدات رایانه ای از سوی کارکنان، مبتنی بر تکنیک های مهندسی اجتماعی می باشد و همچنین تکنیک های مورد استفاده در مهندسی اجتماعی مبتنی بر محدودیتهای تصمیم گیری توسط انسان معنا یافته که به آن محدودیت های شناختی (cognitive biases) شناخته می شود (Jaco, K ,2004). از جمله نظریه های مطرح در این حوزه می توان به نظریه محدودیت عقلایی هربرت سایمون اشاره داشت که بیان کننده تاثیر محدودیت های اطلاعات، زمان و همچنین محدودیت درک یا شناخت انسان در تصمیم گیری بوده و فرد تصمیم گیرنده با توجه به محدودیت های مذکور به دنبال اتخاذ تصمیم راضی کننده به جای تصمیم بهینه می باشد(Elster, Jon,1983).

همچنین بر اساس تئوری انتظارات کاهنمن در ۱۹۷۰، افراد در هنگام انتخاب و تصمیم گیری در شرایط ریسک و عدم اطمینان، به جای تمرکز بر خروجی نهایی بر روی ارزش پتانسیل سود و زیانی که

بدست می آورند متمرکز شده و این تصمیم گیری وابسته به محدودیتهای استنباطی آنها از شرایط خواهد بود. قبل از مطرح شدن تئوری انتظار، تئوری مسلط در تصمیم گیری تئوری مطلوبیت مورد انتظار بود، که فرض می کرد افراد در شرایط ریسک انتخاب های عقلانی انجام می دهند. تئوری مطلوبیت دو اصل اساسی داشت: حداکثر سازی مطلوبیت و عدم پراکندگی انتخاب ها. اولین اصل بیان می کند که افراد برای حداکثرسازی مطلوبیت نهایی خود انتخاب هایشان را انجام می دهند و اصل دیگر بدین معناست که ترجیحات بین انتخاب ها مستقل از نمایشات متفاوت همان مسئله است. کاهنمن و تورسکی اظهار کردند که این دو اصل به خاطر کامل نبودن ادراک انسان نقض می شوند(Kahneman, Daniel; Tversky, Amos ,1979).

از سوی دیگر، هافستد در سال ۱۹۹۱، فرهنگ سازمانی را برنامه‌ریزی جمعی ذهن بیان می‌کند که افراد یک سازمان را از سازمانهای دیگر متمایز کند. بر اساس نتایج تحقیقات هافستد وی پنج جنبه فرهنگ را مشخص کرده که عبارتند از: فردگرایی در برابر جمع گرایی، فاصله قدرت، اجتناب از عدم اطمینان، مردخویی در مقابل زن خویی و دید بلندمدت در برابر دید کوتاه مدت. شاخص سوم که هافستد مطرح می کند یعنی اجتناب از عدم اطمینان، با مفهوم ریسک در رابطه است (Hofstede, geert ,2001).

تئوری طبقه بندی اسمیت و مدین در سال ۱۹۸۱ و پارسونز در سال ۱۹۹۶، بیان می کند که فرضیات طبقه بندی در رابطه با عوامل مرتبط با نیروی انسانی ضروری بوده و مفاهیمی همچون کلاس و دسته بندی را معرفی نموده و اینکه به چه دلیل انسانها مسائل را طبقه بندی می نمایند. بنابراین این نظریه با طبقه بندی مسائل، امکان بررسی سیستمی و الویت بندی آنها می تواند کمک مناسبی در رابطه با تشخیص دلایل رفتاری کارکنان در امنیت اطلاعات داشته باشد و بر اساس نظریه خودکنترلی تیلر، افراد با توجه به تمایلات ذاتی خود به تشخیص قوانین و دنبال نمودن مقررات سازمانی می پردازند(Tyler et al.,2007).

مرور ادبیات موضوعی

پژوهش‌ها در حوزه تهدیدهای داخلی سازمانی از سال ۱۹۹۹ آغاز شده‌است (Sang-Chin Yang, Yi-Lu Wang, 2011). در این پژوهش ها، بر روی جنبه‌هایی همچون بررسی سه نقش کارکنان، فرایندهای سازمانی و تکنولوژی در شناسایی تهدیدهای رایانه ای داخلی تاکید شده است. پروژه MERIT دانشگاه کارنگملون نخستین پژوهشی است که به هر سه جنبه فرآیند، تکنولوژی و کارکنان تاکید داشته و آنها را مورد بررسی قرار داده است. در سال ۲۰۰۲، موسسه تحقیقاتی

CERT[1] در دانشگاه کارنگملون[2] به همراهی موسسه انتک[3] وزارت اطلاعات آمریکا پروژه تحقیقاتی در خصوص تهدیدهای مربوط به کارکنان سازمان سازمان را آغاز نمودند. این پروژه تحقیقاتی بر اساس اطلاعات انتک از روانشناسی رفتار کارکنان و تجربیات تخصصی و فنی کارشناسان CERT در خصوص بیش از ۱۵۰ رخداد که در زیرساخت حیاتی آمریکا از سال ۱۹۹۶ تا ۲۰۰۲ به وقوع پیوسته بود انجام گردید این پژوهش بر اساس اطلاعات مستندات باقی مانده از رخدادها و مصاحبه با افرادی که در رخداد شرکت داشتند انجام شده است (Andrew P. Moore , Dawn M. Cappelli, 2008).

گزارشاتی مبنی بر تحلیل رخدادهای مربوط به کارکنان سازمان در زیرساخت‌های بانکی در سال ۲۰۰۴ (Dawn Cappelli , Andrew Moore , Marisa Reddy Randazzo, Ph.D., 2004) و گزارشی دیگر در خصوص تحلیل تهدیدهای کارکنان سازمان سازمان در تمامی زیرساخت‌های حیاتی آمریکا (Michelle Keeney , Dawn Cappelli, 2005) و گزارشی در خصوص زیرساخت‌های فناوری اطلاعات و ارتباطات (Dawn Cappelli, Eileen Kowalski , Andrew Moore, 2008) و زیرساخت‌های دولتی (Eileen Kowalski, Dawn Cappelli , Bradford Willke, 2008) در سال ۲۰۰۷ تدوین گردید.

همانطور که در بخش قبل گفته شد، انتشار اطلاعات محرمانه سازمان و وقوع تهدیدات مختلف به دلیل اجرای اقدامات سهوی کارکنان یکی از دلایل مهم ایجاد رخدادهای امنیتی در سازمانها می باشد. دانشگاه کارنگملون به همین دلیل دو گزارش در رابطه بررسی و تحلیل عوامل موثر بر افزایش احتمال بروز حملات مبتنی بر مهندسی اجتماعی را در سال ۲۰۱۳ و ۲۰۱۴ با بررسی رخدادهای به وقوع پیوسته در کشور امریکا ارایه نموده است (Department of Homeland Security, 2013). بر اساس پژوهش دانشگاه کارنگملون، سه حوزه اصلی از عوامل می توانند در وقوع تهدیدات UIT از طریق مهندسی اجتماعی موثر باشند که آنها شامل عوامل جمعیتی، سازمانی و انسانی می باشند که در ادامه توضیح داده است (Department of Homeland Security, 2014).

عوامل جمعیتی

در پژوهشی که توسط شنگ از دانشگاه کارنگملون در رابطه با بررسی ارتباط عوامل جمعیتی با وقوع حملات فیشینگ که در نتیجه حملات مهندسی اجتماعی رخ می دهد، مشخص گردید زنان

1 .Computer Emergency Response Team
2 .Carnegie Mellon
3 . NTAC (National Threat Assessment Center)

بیشتر از مردان در معرض این نوع از حملات واقع هستند و همچنین در بررسی انجام شده توسط هالوی مشخص گردید زنان در استفاده از ارتباطات دیجیتال احساس راحتی بیشتری دارند. ولی در تحقیق موهبزادا در سال ۲۰۱۲ بر روی دانشجویان، هیچگونه تفاوتی در تاثیر جنسیت بر وقوع حملات مهندسی اجتماعی مشاهده نگردید که البته او این نتیجه را نشان از تاثیر بیشتر عواملی همچون میزان تجربه فرد، رشته تحصیلی یا سمت شغلی او در مواجهه با این نوع از حملات می داند. از سوی دیگر، بصورت کلی پژوهش های زیادی نشان از تاثیر منفی میان سن و احتمال وقوع حملات فیشینگ را بیان نموده اند و افراد در سن ۱۸ تا ۲۵ سال بیشتر تحت تاثیر این نوع از حملات قرار می گیرند. همچنین بسیاری از اندیشمندان معتقدند عادات شخصیتی افراد نقش اساسی در احتمال وقوع حملات مهندسی اجتماعی دارد. تفاوتهای شخصیتی می تواند منجربه تفاوت در رفتار و تعامل با دیگران، تفاوت در تصمیم گیری و عکس العمل در شرایط فشار کاری و یا ریسک و همچنین تفاوت در پاسخ به حملات مهندسی اجتماعی گردد. به عنوان مثال در پژوهشی که در رابطه با بررسی ارتباط مدلهای شخصیتی افراد با وقوع حملات فیشینگ صورت گرفته است، افرادی که بیشتر تمایل به اطاعت داشته و نسبت به دیگران حس مثبتی را دارا هستند، کمتر در برابر حملات مهندسی اجتماعی مقاومت می نمایند. البته، تحقیقات محدودی در رابطه با تاثیر تفاوت های فرهنگی بر وقوع حملات مهندسی اجتماعی انجام شده است. به عنوان مثال در پژوهشی که در این رابطه در عربستان صورت پذیرفته است، ۷ در صد از دانشجویان به حمله نامه الکترونیک دارای حمله فیشینگ پاسخ مثبت داده و همچنین در بررسی مشابه در کشورهای غربی نیز این آمار بین ۳ تا ۱۱ درصد بوده است.

عوامل سازمانی

عوامل سازمانی اشاره به خط مشی های مدیریتی، محیط کار، حجم کار و جنبه های دیگر محیط کار دارد که بتواند بر روی عملکرد افراد تاثیر بگذارد و منجربه ایجاد خطای انسانی گردد و در نتیجه تهدیدات UIT به وقوع بپیوندد. البته شناسایی این عوامل به سختی صورت می گیرد زیرا پارامترهای مذکور مرتبط به نحوه مدیریت تیم، خط مشی های سازمان و الزام آنها بستگی دارد. همچنین شرایط نامناسب محیط کار که منجربه ایجاد خطای انسانی کارکنان شده می تواند در نتیجه ارتباطات ضعیف کاری در خصوص شفاف سازی وظایف سپرده شده و اهداف آنها، مبهم بودن روال ها و دستورات، طراحی نادرست سیستمها که منجربه کاهش کارآیی آنها می گردد، ناکافی بودن منابع برای اجرای وظایف، شرایط نامناسب محیطی مثل دما یا صدا، ایجاد تغییرات در روالهای عادی و فشار کاری به دلیل غیرواقعی بودن مهلت اجرای امور و ضعف در سیستمها و روالهای امنیتی سازمان باشد. البته در

پژوهش دانشگاه کارنگملون بیان شده است که به دلیل غیرقابل سنجش بودن و یا مبهم بودن برخی از عوامل نامبرده شده در سازمانهای مورد بررسی، تفکیک عامتری به منظور تسهیل در اجرای پژوهش انتخاب گردیده که شامل ناکافی بودن سیستم های مدیریتی، اثربخشی سیستم ها و خط مشی های امنیتی و فشار کاری است.

بر اساس پژوهش لکا در سال ۲۰۰۴، مدیریت موثر مشتمل بر اطمینان از در دسترس بودن کارمندان دارای صلاحیت، اختصاص وظایف به آنها و موجود بودن منابع برای اجرای وظایف می باشد و کمبود و نقصان در هریک از آنها، نارضایتی، استرس و ایجاد مشکل برای کارمندان و سپس افزایش احتمال وقوع خطای انسانی را در پی خواهد داشت. بر اساس موارد ذکر شده می توان گفت مطابق با پژوهش انجام شده در سال ۲۰۱۲، کارکنان بصورت مناسب از ماهیت حملات فیشینگ آگاه نشده و دانش مناسبی نسبت به نحوه شناسایی حملات مهندسی اجتماعی ندارند و در واقع در خصوص شفاف سازی نحوه عملکرد آنها، تعامل مناسبی انجام نمی گردد. اگرچه قابل ذکر است دانش عمومی نسبت به خطرات رایانه ای و مفاهیم آنها مانند بدافزارها هیچ کمکی در این رابطه نمی تواند داشته باشد.

ملاحظه دیگری که در این مجموعه قابل بررسی بوده میزان اثربخشی سیستمها و خط مشی های امنیتی در سازمان است. روالهای امنیتی معمولا برای متوسط افراد سازمان دشوار و مبهم به نظر می رسد و خطاهای حاصل از این پیچیدگی می تواند نتایج وخیمی داشته باشد. در واقع سیستمها و روالهی امنیتی که از پیچیدگی بالایی برخوردار هستند از مقبولیت کمتری برخوردار شده و منجربه ترغیب کاربر به یافتن راههای کوتاهتر برای انجام امور خود و در نتیجه احتمال وقوع تهدیدات UIT افزایش می یابد. بر اساس پژوهش انجام شده در سال ۱۹۹۶، کارآیی و امنیت اغلب در سیستمهای رایانه ای بصورت همزمان وجود نداشته و از سوی دیگر خط مشی های امنیتی کارآیی مناسبی در برابر حملات پیچیده و پیشرفته مهندسی اجتماعی از خود نشان نخواهند داد.

محیط نامناسب کاری می تواند یکی از مهمترین دلایل ایجاد استرس و خستگی در کارکنان باشد. بر اساس پژوهش های انجام شده محدودیت و فشار زمانی و حجم کار از منابع ایجاد استرس هستند. محدودیت زمانی حتی می تواند بر روی عملکرد کارکنان آزموده و آموزش دیده نیز تاثیر بگذارد و از سوی دیگر حجم کاری بالا منجربه افزایش خستگی و در نهایت کاهش عملکرد مناسب افراد می گردد. بر اساس پژوهشی دیگر، هنگامیکه خطای انسانی در نتیجه طراحی نادرست سیستم اتفاق می افتد، این خروجی یا خطا نباید در ارتباط با کاربر در نظر گرفته شود. در واقع هنگامیکه گفته می شود رخنه امنیتی در نتیجه خطای کاربر اتفاق افتاده است، نباید مسئولیتی برای سیستم لحاظ

گردد و بالعکس. البته این نظریه یکی از نظریه های جدید و چالش برانگیز در ارتباط با موضوع امنیت کارا بوده که در سال ۲۰۰۵ ارایه شده است.

عوامل انسانی

البته قابل ذکر است که حتی با وجود سیستم ها و خط مشی های مدیریتی و امنیتی مناسب در سازمان، حملات مبتنی بر مهندسی اجتماعی مانند فیشینگ به کار خود ادامه می دهند. در برخی از پژوهشها بر تمرکز بر جنبه های روانشناختی افراد و کارکنان سازمان تکیه نموده و این عوامل را مهم قلمداد می نمایند. به عنوان مثال در پژوهشی که به منظور بررسی قدرت شناسایی وب سایتهای جعلی صورت پذیرفته بود، آنها متوجه شدند که عدم توجه کافی افراد به پیام ها و ویژگی های امنیتی وب سایت و همچنین اعتبار ظاهری وب سایتها می تواند حتی کاربران متخصص در این حوزه را نیز گمراه نماید. از سوی دیگر معمولا افراد در شرایط برخورد با موارد اورژانسی، تناقضات و یا خطاهای امنیتی را نادیده گرفته و یا کمتر توجه می نمایند. همچنین همانطور که گفته شد هنگامیکه افراد با حجم بالایی از پست الکترونیک روبرو هستند به دلیل افزایش حجم کار و در نتیجه کاهش توجه و دقت، با احتمال بالاتری به حملات مهندسی اجتماعی پاسخ مثبت می دهند.

در بررسی که توسط دانز در سال ۲۰۰۷ صورت گرفته است، داشتن تجربه قبلی در افراد در رابطه با حملات مبتنی بر مهندسی اجتماعی می تواند منجربه کاهش احتمال بروز مجدد این نوع از حملات در رابطه با آنها گردد. زیرا افرادی که به مدت طولانی دچار این نوع از حملات نشده اند، به مرور زمان حس اعتماد بیشتری به محیط اینترنت پیدا کرده و در نتیجه در گذر زمان حتی علائم واضح و مشخص حملات و تهدیدات را نادیده می گیرند.

از سوی دیگر، بر اساس نظریه کاهنمن، تصمیمات اتخاذ شده توسط افراد اغلب عقلانی نبوده و جانبدارانه است و در نتیجه افراد یا کارکنان سازمان تصور می کنند که وقوع تهدیدات برای آنها بعید بوده و در مورد قدرت حملات مهندسی اجتماعی به اشتباه نتیجه گیری نموده و این نوع از تهدیدات را نادیده می گیرند. در بررسی انجام شده توسط جاکوبسون گفته شده که افراد معمولا مبنای قضاوت و تصمیمگیری خود در مورد اعتبار یک پیام یا وب سایت را محتوای آن قرار می دهند و کمتر به ویژگی های امنیتی آنها توجه می نمایند.

بر اساس پژوهش دانشگاه کارنگملون، تحلیل رفتار افراد در رابطه با شرایط دارای ریسک نیز یکی دیگر از مواردی است که باید مورد بررسی قرار گیرد. در واقع افرادی که بیشتر تمایل به تجربه شرایط ریسک را دارند، بیشتر در معرض حملات مهندسی اجتماعی قرار خواهند گرفت.

از سوی دیگر انطباق و تعهد افراد از قوانین و هنجارهای سازمان نیز یکی دیگر از پارامترهای انسانی مورد بحث در کاهش احتمال بروز حملات UIT شناخته می شود که البته مواردی همچون پاداش یا تنبیه در ایجاد این تعهد اثرگذار نبوده و تنها در تحکیم آن موثر هستند و اعتقادات درونی فرد منشا بروز این تطابق در سازمان می باشد. البته بالگورکو معتقد است ایجاد فرهنگ امنیت در سازمان می تواند به ارتقا امنیت سازمان کمک کند و سازمانها باید آموزشهای لازم را برای کارکنان خود در نظر داشته باشند تا اطمینان یابند نیازمندیهای کارکنان خود برای مطابقت با هنجارهای امنیتی را شناسایی نموده اند.

فرضیات پژوهش

- عوامل جمعیتی بر روی بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT موثر می باشد.
- عوامل سازمانی بر روی بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT موثر می باشد.
- عوامل انسانی بر روی بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT موثر می باشد.

روش شناسی پژوهش

این پژوهش به لحاظ گردآوری اطلاعات به روش پیمایشی و با تهیه پرسشنامه مرتبط انجام گرفته است و برای بررسی عوامل موثر بر وقوع تهدیدات امنیتی سهوی کارمندان و مبتنی بر مهندسی اجتماعی، پرسشها در ۳ دسته از عوامل مورد بررسی قرار گرفت. با توجه به بررسی اقدامات صورت گرفته در حوزه های مشابه که در بخش تاریخچه موضوعی شرح داده شد، عوامل مختلفی همچون عوامل جمعیتی، سازمانی و انسانی در افزایش احتمال حملات مبتنی بر مهندسی اجتماعی به شرح ذیل مطرح گردید که مطابق با پرسشنامه طراحی شده در این پژوهش، در میان ۴۰ نفر از کارمندان با حوزه کاری تخصصی فناوری اطلاعات مورد بررسی قرار گرفته است.

یافته های پژوهش

یکی از قسمت‌های مهم هر روش تحقیق، تجزیه و تحلیل یافته‌هاست. این قسمت مشتمل بر توضیحات، جداول و همچنین تجزیه و تحلیل اطلاعات است. برای تحلیل یافته‌های پژوهش از روش-های خاص آماری استفاده می‌شود و در این رابطه اطلاعات آماری جمع آوری شده برای مقایسه و تجزیه و تحلیل فرضیه‌های پژوهش آماده می‌گردند. در این پژوهش، استخراج نتایج مربوطه با استفاده از نرم افزار SPSS انجام گرفته است. بنابراین، با توجه به مطالب فوق ابتدا به بیان جداول و سپس به تجزیه و تحلیل داده‌ها پرداخته خواهد شد. پرسشنامه مورد بررسی دارای ۱۸ سوال بوده و میان ۴۰ نفر از کارمندان حوزه فناوری اطلاعات و ارتباطات اشتراک گذاشته شد که با آلفای کرونباخ ۰.۸۷۹ از اعتبار مناسبی برخوردار می باشد.

در این نمونه متغیرهای بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی، عوامل سازمانی، عوامل انسانی، عوامل جمعیتی شامل سن ، جنسیت و تحصیلات مورد مطالعه قرار گرفته است. در جداول زیر شاخص‌ها و آمار توصیفی مربوط به این نمونه ارائه شده است.

	تعداد	میانگین	انحراف استاندارد	میانه
بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی	۴۰	۲/۷۸	۰/۷۶۸	۳/۰۰
عوامل سازمانی	۴۰	۲۳/۰۵	۴/۱۴۵	۲۳/۵۰
عوامل انسانی	۴۰	۲۶/۹۵	۴/۲۰۰	۲۷/۵۰
سن	۴۰	۳۰/۲۵	۳/۱۸۴	۳۰/۰۰

از آنجا که بر اساس نتایج آزمون کولموگروف- اسمیرنف، متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT متغیری رتبه ای بوده و دارای توزیع نرمال نمی باشد، لذا در بررسی ارتباطات بین متغیرهای پژوهش، از آزمون همبستگی اسپیرمن، به عنوان یک آزمون ناپارامتری مناسب، استفاده می شود.

	آماره	درجه آزادی	سطح معناداری	نتیجه
بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی	۰/۲۹۰	۴۰	۰/۰۰۱	توزیع نرمال نیست
عوامل سازمانی	۰/۱۰۶	۴۰	۰/۲۰۰	توزیع نرمال است
عوامل انسانی	۰/۱۱۲	۴۰	۰/۲۰۰	توزیع نرمال است

بررسی فرضیه اول:

عوامل جمعیتی بر روی بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT موثر می باشد.

به منظور بررسی تأثیر عوامل جمعیتی بر بر روی بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT، ارتباط بین متغیرهای سن، جنسیت و تحصیلات با متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT، به وسیله آزمون همبستگی اسپیرمن، مورد ارزیابی قرار گرفته است. این آزمون ارتباط بین متغیرهایی که حداقل یکی از آنها به صورت رتبه ای است، استفاده می‌شود نتایج این آزمون در جدول‌های زیر ارائه شده است

		سن	جنسیت	تحصیلات
بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی	ضریب همبستگی اسپیرمن	-۰/۰۶۴	۰/۱۰۳	-۰/۲۳۵
	سطح معناداری	۰/۶۹۴	۰/۵۲۹	۰/۱۴۴
	تعداد	۴۰	۴۰	۴۰

نتایج آزمون همبستگی اسپیرمن نشان می‌دهد که ارتباط بین متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و متغیر سن، جنسیت و تحصیلات معنادار نمی‌باشد. به عبارت دیگر براساس سطح معناداری محاسبه شده در آزمون اسپیرمن و بزرگ‌تر بودن آن از مقدار عددی ۰/۰۵ می‌توان نتیجه گرفت که در سطح اطمینان ۹۵٪ ارتباط بین این دو متغیر معنادار

نیست لذا فرض صفر مبنی بر عدم ارتباط دو متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و عوامل جمعیتی تأیید شده و فرض پژوهش رد می‌شود. بر این اساس می‌توان نتیجه گرفت که ارتباطی بین بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT دارای سنین، جنسیت و تحصیلات مختلف وجود ندارد.

بررسی فرضیه دوم:

عوامل سازمانی بر روی بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT موثر می باشد.

نتایج آزمون همبستگی اسپیرمن نشان می‌دهد که ارتباط بین متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و متغیر عوامل سازمانی معنادار است. به عبارت دیگر براساس سطح معناداری محاسبه شده در آزمون اسپیرمن (۰/۰۰۱) و کوچک‌تر بودن آن از مقدار عددی ۰/۰۵ می‌توان نتیجه گرفت که در سطح اطمینان ۹۵٪ ارتباط بین این دو متغیر معنادار است لذا فرض صفر مبنی بر عدم ارتباط دو متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و عوامل سازمانی رد شده و فرض پژوهش تایید می‌شود. بر این اساس می‌توان نتیجه گرفت که بین بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و عوامل سازمانی ارتباط معناداری وجود دارد.

		عوامل سازمانی
بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی	ضریب همبستگی اسپیرمن	۰/۵۰۰
	سطح معناداری	۰/۰۰۱
	تعداد	۴۰

بررسی فرضیه سوم:

عوامل انسانی بر روی بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT موثر می باشد.

نتایج آزمون همبستگی اسپیرمن نشان دهنده این است که ارتباط بین متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و متغیر عوامل انسانی معنادار

است. به عبارت دیگر براساس سطح معناداری محاسبه شده در آزمون اسپیرمن (۰/۰۱۰) و کوچک‌تر بودن آن از مقدار عددی ۰/۰۵ می‌توان نتیجه گرفت که در سطح اطمینان ۹۵٪ ارتباط بین این دو متغیر معنادار است لذا فرض صفر مبنی بر عدم ارتباط دو متغیر بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و عوامل انسانی رد شده و فرض پژوهش تایید می‌شود. بر این اساس می‌توان نتیجه گرفت که بین بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی از سوی کارمندان صنعت IT و عوامل انسانی ارتباط معناداری وجود دارد.

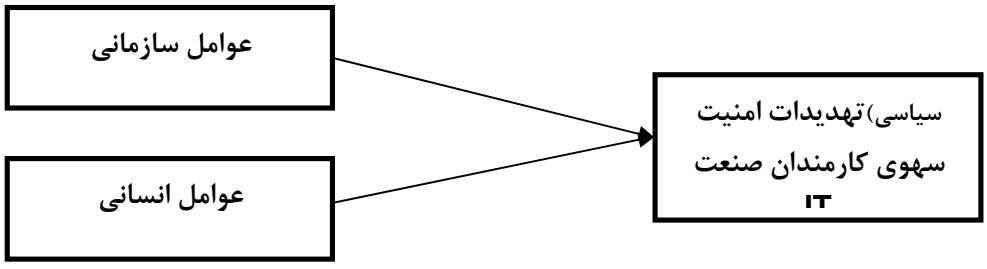
		عوامل انسانی
بروز تهدیدات امنیت سهوی مبتنی بر مهندسی اجتماعی	ضریب همبستگی اسپیرمن	۰/۴۰۲
	سطح معناداری	۰/۰۱۰
	تعداد	۴۰

با توجه به یافته ها و تحلیل آماری صورت گرفته مشاهده می گردد که عامل جمعیتی شامل سن، جنسیت و تحصیلات در نمونه مورد بررسی بر روی وقوع تهدیدات امنیتی سهوی مبتنی بر مهندسی اجتماعی از سوی کارکنان موثر نبوده و این نتیجه می تواند نشان از تاثیر بیشتر عواملی دیگر همچون عوامل سازمانی و انسانی افراد در مواجهه با این نوع از تهدیدات باشد. دو عامل سازمانی به معنای خط مشی های مدیریتی، حجم و جنبه های دیگر محیط کار دارد که بتواند بر روی عملکرد افراد تاثیر بگذارد و منجربه ایجاد خطای انسانی گردد و عامل انسانی به معنای تمرکز بر جنبه های روانشناختی افراد و کارکنان سازمان بر روی وقوع تهدیدات امنیتی سهوی مبتنی بر مهندسی اجتماعی از سوی کارکنان سازمان موثر می باشد.

در زمره عامل سازمانی می توان به ناکافی بودن سیستم های مدیریتی موثر، مبهم بودن روالهای امنیتی، فشار کاری، استرس و نارضایتی کارکنان، نبود دانش مناسب کارکنان نسبت به نحوه شناسایی حملات مهندسی اجتماعی که افزایش احتمال وقوع خطای انسانی را در پی خواهد داشت اشاره نمود. در رابطه با عامل انسانی نیز همانطور که در بخشهای قبل گفته شد، افراد در شرایط برخورد با موارد دارای ریسک یا اورژانسی، تناقضات و یا خطاهای امنیتی را نادیده گرفته و همچنین نداشتن تجربه قبلی در رابطه با این نوع از حملات و یا شبیه سازی آنها می تواند منجربه افزایش اعتماد به محیط اینترنت گردد و در نتیجه در گذر زمان حتی علائم واضح و مشخص حملات و تهدیدات را نادیده می گیرند. تصمیمات اتخاذ شده توسط افراد اغلب عقلانی نبوده و جانبدارانه است و در نتیجه افراد یا

کارکنان سازمان تصور می کنند که وقوع تهدیدات برای آنها بعید می باشند. در نهایت در این بحث افزایش انطباق و تعهد افراد از قوانین و هنجارهای سازمان نیز از اهمیت بالایی برخوردار است.

همانطور که در بخش چارچوب نظری توضیح داده شد، موفقیت آمیز بودن تکنیک های مهندسی اجتماعی به دلیل سو استفاده از محدودیتهای عقلایی افراد در تصمیم گیری به وقوع می پیوندد و افراد در اتخاذ تصمیم خود به محدودیتهای استنباطی دچار می شوند. به علاوه، اجتناب از عدم اطمینان یکی از پارامترهای موثر در ارتقا فرهنگ سازمانی است و افراد با توجه به تمایلات ذاتی خود به تشخیص قوانین و دنبال نمودن مقررات سازمانی می پردازند، بنابراین همانطور که بررسی های پژوهش تایید می نماید، می توان گفت مدیران سازمان می بایست تلاش خود را بر روی کاهش سطح ابهام در محیط کار و در نتیجه کمک به ارتقا تصمیم گیری صحیح توسط کارمندان خود متمرکز نمایند تا در نتیجه از وقوع تهدیدات امنیتی سهوی و انتشار اطلاعات محرمانه سازمان جلوگیری به عمل آید.



متغیرهای مستقل یا پیش بین **متغیر پاسخ یا وابسته**

پیشنهادات و اقدامات آتی

با توجه به حساسیت اطلاعات در دسترس کارکنان هر سازمان از یک سو و تمرکز مهاجمین بر سو استفاده از آسیب پذیری های کارکنان به منظور دسترسی به منابع اطلاعاتی، تمرکز بر ارتقا عوامل سازمانی و انسانی موثر در کاهش خطای تصمیم گیری افراد و در نتیجه وقوع تهدیدات امنیتی سهوی مبتنی بر مهندسی اجتماعی از اهمیت بالایی برخوردار می باشد. لذا برنامه ریزی و ترغیب اجرای اقدامات پژوهشی در قالب راهکارهای عملیاتی نمودن نتایج پژوهش در سازمانهای کشور باید مورد بررسی قرار گیرد.

منابع

1-Verizon RISK Team, Verizon 2013 Data Breach Investigations Report, 2013
2-Dawn Cappelli , Andrew Moore , Marisa Reddy Randazzo, Ph.D., Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, Carnegie Mellon University, 2004
3-Eileen Kowalski, Dawn Cappelli , Bradford Willke, Insider Threat Study: Illicit Cyber Activity in the Government Sector, Carnegie Mellon University, 2008
4-AlgoSec. The State of Network Security: Attitudes and Opinions. AlgoSec, Inc., 2013.
5-Danijel Milicevic, Matthias Goeken, Social Factors in Policy Compliance - Evidence Found in Literature to Assist the Development of Policies in Information Security Management, 2013
6-Jaco, K ,CSEPS Course Workbook, Jaco Security Publishing, 2004
7-Elster, Jon, Sour Grapes: Studies in the Subversion of Rationality ,Cambridge,1983
8-Kahneman, D. & Tversky, A. "Prospect Theory: An Analysis of Decision under Risk." Econometrica, 1979
9-Geert Hofstede, Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations. 2nd Edition, Thousand Oaks CA: Sage Publications, 2001
10-Tyler et al, Measuring Self-Control Problems, The American Economic Review, Vol. 97, No. 3, pp. 966-972, 2007
11-Sang-Chin Yang, Yi-Lu Wang, System Dynamics Based Insider Threat Modeling, International Journal of Network Security & Its Applications, 2011
12-Andrew P. Moore , Dawn M. Cappelli, The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures, Carnegie Mellon University, 2008
13-Michelle Keeney , Dawn Cappelli, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, Carnegie Mellon University, 2005

14-Dawn Cappelli, Eileen Kowalski , Andrew Moore, Insider Threat Study:Illicit Cyber Activity in the Information Technology and Telecommunications Sector, Carnegie Mellon University, 2008
15-Eileen Kowalski, Dawn Cappelli , Bradford Willke, Insider Threat Study: Illicit Cyber Activity in the Government Sector, Carnegie Mellon University, 2008
16-Department of Homeland Security , The CERT Insider Threat Team , Unintentional Insider Threats A Foundational Study, 2013
17-Department of Homeland Security , The CERT Insider Threat Team , Unintentional Insider Threats Social Engineering , 2014