هفتمین کنفرانس ملی مباحث نوین در کامپیوتر و فناوری اطلاعات
7th National Conference on Advanced Topics in Computer and Information Technology
۲ آذر ماه ۱۴۰۲

بررسی عوامل موثر بر آگاهی امنیت فناوری اطلاعات در سازمان‌ها

شکوفه جهان بزرگی مطلق - نسیم حمیدیان

چکیده : در سال‌های اخیر با پیشرفت فناوری اطلاعات و ارتباطات شاهد بکارگیری تجهیزات الکترونیکی و روش‌های مجازی در بخش عمده‌ای از فعالیت‌های روزمره همچون ارائه خدمات مدیریت و نظارت و اطلاع‌رسانی می‌باشیم. یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات ارتقاء آگاهی کاربران از امنیت اطلاعات می‌باشد که افراد آگاهی‌های لازم و مربوط به نقش و مسئولیت خویش را در جهت حفظ امنیت اطلاعات در کار مربوط به خود کسب می‌نمایند. در واقع آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت‌های خوب امنیتی شده و به افراد اجازه می‌دهد تا نسبت به امنیت فناوری اطلاعات نگران و پاسخگو بوده و به تدریج به فرهنگ سازمان‌ها تبدیل شوند. لذا می‌توان گفت آگاهی امنیتی کاربران نقش بسزایی در امنیت اطلاعات سازمان‌ها دارد. با این وجود، بسیاری از نقض‌های امنیت اطلاعات حین کار ناشی از عدم پیروی کارکنان از سیاست‌های امنیت اطلاعات می‌باشد. بنابراین باید به این نکته توجه کرد که پیروی کارکنان حوزه فناوری اطلاعات از سیاست‌های امنیت اطلاعات مهمترین عامل در امنیت سیستم‌های اطلاعاتی بوده و درک میزان پیروی کارکنان از سیاست‌های امنیتی برای سازمان‌ها بسیار حیاتی می‌باشد.

کلمات کلیدی: آگاهی امنیتی، فناوری اطلاعات، رفتار حرفه‌ای، سازمان

۱ - امنیت اطلاعات

اطلاعات در تعریف علمی آن به مجموعه‌ای از داده‌ها که دارای معنی و هدف باشند اطلاق می‌شود از این رو اطلاعات می‌تواند به هر نوع از داده‌های معنی‌دار نظیر اطلاعات چاپی، کاغذی، الکترونیکی، صوتی و تصویری گفته شود و حتی گفته شفاهی ما به یکدیگر را نیز پوشش دهد بنابراین بر اساس تاریخ توافق شده جهانی امنیت اطلاعات به فرآیند حفاظت اطلاعات در برابر انواع کارهای غیرمجاز شامل دسترسی، استفاده، افشا، اختلال، تغییر، مطالعه، بازرسی، ضبط یا تخریب گفته می‌شود. امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز که این فعالیت‌ها شامل دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یا ضبط، خراب کردن، تغییر و دستکاری است؛ واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاه به اشتباه به جای هم به کار برده می‌شود اگرچه این موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آنها وجود دارد که این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله و موضوعاتی که تمرکز کرده‌اند دارد[۱]. امنیت اطلاعات یک مسأله حیاتی است و امروزه سازمان‌ها در سراسر دنیا با آن روبه رو هستند، امنیت سیستم‌های اطلاعاتی هم فناوری و هم افراد (عوامل انسانی) را در بر می‌گیرد در بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی صورت گرفته یک نوع دید و رویکرد فنی وجود داشته است. نقش فناوری اطلاعات در رسیدن به اهداف راهبردی سازمان نشان می‌دهد که سیستم‌هایی که با فناوری اطلاعات تطبیق داده شده‌اند به دستیابی اهداف توسعه راهبردی سازمان کمک خواهند کرد همچنین بیان شده است که موفقیت فناوری اطلاعات در یک سازمان می‌تواند به بعضی فاکتورهای اصلی مثلا پشتیبانی مدیریت ارشد و همچنین مشارکت کاربران که فاز اجرای پروژه را تسهیل می‌کنند بستگی داشته باشد. امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ و یا اشکال دیگر مربوط است. امنیت کامپیوتر در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم

کامپیوتری تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می‌شود؛ دولت‌ها، مراکز نظامی، شرکت‌ها، مؤسسات مالی، بیمارستان‌ها و مشاغل خصوصی مقدار زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصولات، تحقیقات و وضعیت مالی گردآوری می‌کنند بسیاری از اطلاعات در حال حاضر بر روی رایانه‌ها، جمع‌آوری، پردازش و ذخیره و در شبکه به کامپیوترهای دیگر منتقل می‌شود. اگر اطلاعات محرمانه در مورد مشتریان و یا امور مالی یا محصول جدید موسسه‌ای به دست رقیب بیفتد این سرقت اطلاعات ممکن است به خسارات مالی به کسب‌وکار، پیگرد قانونی و یا حتی ورشکستگی منجر شود لذا حفاظت از اطلاعات محرمانه یک نیاز تجاری و در بسیاری از موارد نیز نیاز اخلاقی و قانونی است. برای افراد امنیت اطلاعات تأثیر معناداری بر حریم خصوصی دارد البته در فرهنگ‌های مختلف این مفهوم حریم خصوصی تعبیرهای متفاوتی دارد[۲].

۲- امنیت اطلاعات در سازمان‌ها

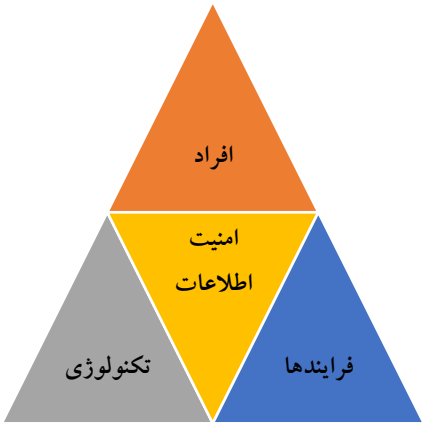
امنیت اطلاعات در سازمان‌ها آشنایی با دانش روز در حوزه فناوری اطلاعات و ارتباطات جهت بهره‌مندی از امکانات و فرصت‌هایی که در سایه این فناوری در اختیار بشر گذاشته شده امری ضروری می‌باشد، امروزه اصطلاح با سواد به کسی اطلاق می‌شود که در این حوزه نیز دارای اطلاعات لازم جهت تعامل و کار و استفاده از فرصت‌های فراهم شده در این عرصه باشد؛ امکان دست‌یابی سریع به اطلاعات مورد نظر از طریق جست وجو در بانک‌های اطلاعاتی در تمامی ساعات بدون محدودیت زمانی و جغرافیایی و امکان دیدن همزمان یک سند توسط کاربران متعدد در نقاط گوناگون، ارسال و دریافت اطلاعات به نقطه مورد نظر، گفتگو و تبادل نظر متنی، صوتی و تصویری فرصت‌هایی است که باید از آن بهره کامل برد. رشد این فناوری آنچنان سریع و عمیق بوده که در جای جای زندگی فردی و اجتماعی انسان‌ها نفوذ کرده و حضور قدرت‌مندانه خود را به رخ می‌کشد به نحوی که بسیاری از مراکز و مؤسسات دولتی و خصوصی، بانک‌ها، شرکت‌ها و ادارات، مراکز آموزشی، پژوهشی، تبلیغی و اطلاع‌رسانی در انجام وظایف و مأموریت‌های خود از این فناوری بهره می‌برند و خدمات خود را نیز از طریق آن عرضه داشته و اطلاع‌رسانی می‌کنند اگر نگاهی به اخبار و اطلاعات مربوط به حوزه فناوری اطلاعات و ارتباطات بیندازیم خبرهای بسیاری در زمینه عملیات خرابکارانه در سرورها، شبکه‌ها و سایت‌های اینترنتی مشاهده خواهیم کرد مثل نفوذ به سیستم‌های بانکی، سرقت حساب‌های بانکی، سرقت اطلاعات مهم، حذف اطلاعات، مخدوش کردن اطلاعات، از سرویس خارج کردن و از کار انداختن سرورها از جمله کارهایی است که در نقاط مختلف جهان رخ داده و می‌دهد؛ در این میان حتی کشورهای مدعی در حوزه فناوری اطلاعات و ارتباطات از عواقب سوء این حملات مصون نبوده‌اند و هریک به تناسب دانش، توانایی و درک موقعیت برای جلوگیری از حملات و نیز رفع آثار در صورت موفقیت حملات و ترمیم خرابی‌ها و تثبیت نقاط آسیب‌پذیر وتوسعه فناوری با توجه به شرایط و تحولات پیش رو هزینه کرده‌اند و موفقیت‌های خوبی نیز بدست آورده‌اند[۳].

۳- سیاست امنیت اطلاعات

اقدام امنیتی مشترکی که بسیار در کانون توجه قرار دارد تدوین و تنظیم سیاست امنیت اطلاعات است، سیاست امنیت اطلاعات مجموعه‌ای از سیاست‌هاست که اهداف، اصول، قوانین و رهنمودهایی را دربردارد که مدیریت انتظار دارد کارکنان به آنها پای‌بند باشند و باید شامل شرح مواردی چون پیامد نقض امنیت اطلاعات، استفاده در چارچوب مقررات از منابع کامپیوتری، مسئولیت‌های امنیت اطلاعات و آموزش کارمندان باشد. سیاست امنیت اطلاعات، کارمندان را در خصوص چگونگی استفاده از اطلاعات و فناوری اطلاعات در سازمان راهنمایی می‌کند. بسیاری از مطالعات گذشته که در زمینه امنیت سیستم‌های اطلاعاتی انجام شده‌اند تأکید کرده‌اند که اثربخشی امنیت سیستم‌های اطلاعاتی با مسائل فنی مرتبط است در صورتی که باید بر هر دو معیارهای فنی و غیرفنی توجه شود به این معنا که پایبندی به سیاست‌های امنیت اطلاعات سازمان شامل پذیرش اقدامات مرتبط با فناوری اطلاعات و موافقت با معیارهای غیرفنی است؛ از جمله اقدامات مرتبط با فناوری اطلاعات استقرار نرم‌افزار آنتی‌ویروس، فایروال‌ها، سیستم‌های تشخیص نفوذ است در حالی که موافقت با مباحث غیر فنی شامل مسائلی چون پذیرش قوانین، رویه‌ها و الزامات امنیت اطلاعات می‌شود[۴].

۴- جنبه‌های مختلف در امنیت اطلاعات

امنیت اطلاعات درای سه جنبه است که عبارتند از[۵]:



شکل ۲-۱: جنبه‌های مختلف در امنیت اطلاعات [۵]

امروزه از تکنولوژی‌های متعددی به منظور ارائه سرویس‌های لازم در رابطه با ایمن‌سازی اطلاعات و تشخیص مزاحمین اطلاعاتی استفاده می‌گردد. سازمان‌ها و مؤسسات می‌بایست سیاست‌ها و فرایندهای لازم به منظور استفاده از یک تکنولوژی را مشخص کنند تا زمینه انتخاب و به کارگیری درست تکنولوژی در سازمان مربوطه فراهم گردد. در این رابطه می‌بایست به مواردی همچون سیاست امنیتی، اصول ایمن‌سازی اطلاعات، استانداردها و معماری ایمن‌سازی اطلاعات، استفاده از محصولات مربوط به ارائه دهندگان شناخته شده و خوشنام، راهنمای پیکربندی، پردازش‌های لازم برای ارزیابی ریسک سیستم‌های مجتمع و بهم مرتبط، توجه گردد.

فرایندها منظور از عملیات مجموعه فعالیت‌های لازم به منظور نگهداری وضعیت امنیتی یک سازمان است. در این رابطه لازم است به موارد زیر توجه شود[۶] :

- ✓ پشتیبانی ملموس و به هنگام‌سازی سیاست‌های امنیتی
- ✓ اعمال تغییرات لازم با توجه به روند تحولات مرتبط با تکنولوژی اطلاعات
- ✓ مدیریت وضعیت امنیتی با توجه به تکنولوژی‌های استفاده شده در رابطه با ایمن‌سازی اطلاعات
- ✓ ارائه سرویس‌های مدیریتی اساسی و حفاظت از زیرساخت‌های مهم
- ✓ ارزیابی سیستم امنیتی
- ✓ هماهنگی و واکنش در مقابل حملات جاری
- ✓ تشخیص حملات و ارائه هشدار و پاسخ مناسب به منظور ایزوله نمودن حملات و پیشگیری از موارد مشابه
- ✓ بازیافت و برگرداندن امور به حالت اولیه

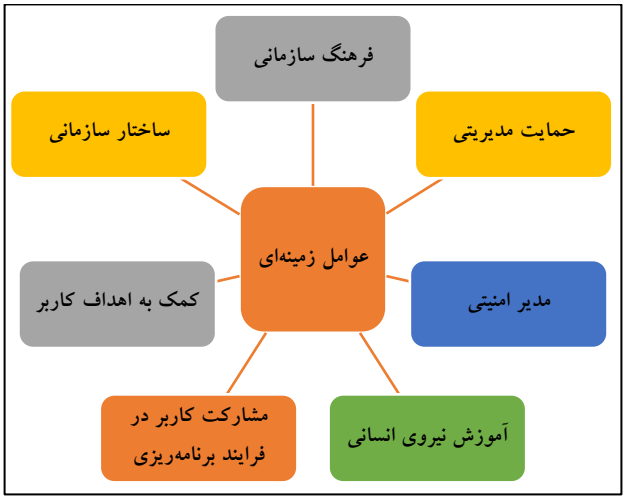
موفقیت در ایمن‌سازی اطلاعات با پذیرش مسئولیت و حمایت مدیریت مالی یک سازمان و براساس شناخت مناسب از تهاجمات حاصل می‌شود، نیل به موفقیت با پیگیری سیاست‌ها و روتین‌های مربوطه و تعیین وظایف و مسئولیت‌های آموزش منابع انسانی حساس و همچنین توجیه مسئولیت‌های شخصی کارکنان حاصل می‌گردد که در این راستا لازم است یک سیستم امنیتی فیزیکی و شخصی به منظور کنترل و هماهنگی در دستیابی به هر یک از عناصر حیاتی در محیط‌های مبتنی بر تکنولوژی اطلاعات نیز ایجاد گردد. ایمن‌سازی اطلاعات از جمله مواردی است که می‌بایست موفقیت خود را در عمل و نه در حرف نشان دهد بنابراین لازم است که پس از تدوین سیاست‌ها و دستورالعمل‌های مربوطه پیگیری مستمر و هدفمند جهت اجرای سیاست‌ها و دستورالعمل‌ها دنبال گردد.

۵– نقش عوامل انسانی در امنیت اطلاعات

برخلاف دید غالب در مورد آسیب‌های اطلاعاتی مبنی بر کامپیوتر امنیت اطلاعات فقط اتخاذ روش‌های قوی رمزنگاری و کلمه رمز عبور قوی نیست؛ این موارد تنها بعد فنی امنیت اطلاعات است حتی در صورتی که شما حداکثر کنترل‌های فنی را در سازمان خود پیاده‌سازی کرده باشید ممکن است به دلیل عدم توجه به مسائل غیر فنی به نتایج دلخواه نرسد لذا امنیت فقط در بعد فنی آن خلاصه نمی‌شود و نیاز به روال‌های اداری و تشکیلات سازمانی و مدیریتی دارد. امنیت یک فرآیند مستمر است و برقراری امنیت در یک برهه زمان به معنای امنیت برای همیشه نیست لازم به ذکر است که در حال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور به ویژه در حوزه سازمان‌های دولتی در سطح نامطلوبی قرار دارد؛ از جمله دلایل اصلی وضعیت موجود می‌توان به فقدان زیرساخت‌های فنی و اجرایی امنیت و عدم انجام اقدامات موثر در خصوص ایمن‌سازی فضای تبادل اطلاعات سازمان‌های دولتی، نبود سیستم‌های مدیریت امنیت اطلاعات، فقدان سیاست‌ها و استراتژی‌های امنیتی و عدم توجه به عوامل انسانی همچون عدم حمایت مدیریتی و بی توجهی به آموزش و ارتقاء سطح آگاهی‌های کاربران از امنیت اطلاعات اشاره نمود. در شکل زیر عوامل غیر فنی تأثیرگذار بر به کارگیری امنیت اطلاعات قابل مشاهده است که بیشتر مربوط به عوامل انسانی و مدیریتی است[۷].

ابزارها و ساز و کارهای امنیتی اثربخشی محدودی دارند زیرا امنیت در وهله اول مسئله‌ای انسانی و به همان میزان مسئله‌ای سازمانی و یا مدیریتی است، تحت این دیدگاه اهمیت مدیریت امنیت سیستم‌های اطلاعاتی به زمینه سازمانی بر می‌گردد که در آنجا وجود دارد که این امر لزوم توجه به منشا تهدیدات سازمانی و شناسایی ویژگی‌های داخلی و

خارجی سازمان را برجسته می‌سازد. نقل قول معروفی این روزها وجود دارد که ۸۰ درصد یا حداقل بخش عظیمی از ریسک‌های سیستم‌های اطلاعاتی از داخل سازمان می‌باشد که این نقل قول راه‌کار پیشنهادی به همراه ندارد و همچنین عنوان نمی‌کند که باید بیشتر یا کمتر به تهدیدات بیرونی بپردازیم. معمولا تهدیدات بیرونی جدی‌تر می‌باشند و می‌توانند منجر به خرابی سیستم‌های اطلاعاتی شرکت یا سرقت اطلاعات محرمانه و غیره شوند هر چند انگیزه این افراد به طور کلی کمتر است و قوانین بازدارنده‌ای وجود دارد ولی تنوع و تعداد زیاد آنها موجب تهدیدات زیادی می‌شود. ویژگی مشترک آنها این است که شانس کمتری برای موفقیت در حملات دارند چون تنها از رخنه‌ها و نقاط ضعف سیستم‌های حفاظتی می‌توانند شانس کمتری برای موفقیت در حمله داشته باشند اما تهدیدات داخلی از دسترسی مجاز بهره‌مند است و موجب آسیب زدن راحت‌تر در مقیاس با تهدیدات خارجی می‌شود همچنین عموم دفاع سازمان در برابر آن ناکافی است و نوع دسترسی که موجبات تخریب را فراهم می‌آورند برای انجام وظایف آنها ضروری است البته نباید فراموش کرد که اکثر کارمندان به سازمان وفادارند و نباید با دید منفی به آنها نگریست.



شکل ۲-۲: فاکتور غیر فنی مؤثر بر امنیت سیستم‌های اطلاعاتی

۶ – آگاهی و آموزش امنیت اطلاعات به کاربران

همان طور که بیان شد یکی از جنبه‌های مهم در مدیریت امنیت اطلاعات در سازمان توجه به امنیت از منظر منابع انسانی است به طوری که بدون در نظر گرفتن عوامل انسانی ،راه‌حل‌های فنی چندان تأثیری در مدیریت امنیت اطلاعات نخواهند داشت. از جمله فاکتورهای مؤثر عوامل انسانی در تأمین امنیت اطلاعات ، موضوع آگاهی و آموزش امنیت اطلاعات کاربران است[۸]. به طور کلی یک ساختار تأثیرگذار امنیتی باید ترکیبی از عناصر تکنیکی و کاربردی باشد تا تأثیری متقابل بر روی خطرات ناشی از اطلاعات قابل حذف داشته باشد، با سریع‌تر شدن آهنگ تغییرات فناوری نیاز به تدابیر منعطف امنیتی نیز بیشتر احساس می‌شود لذا اداره صحیح اطلاعات قابل حذف و آگاه‌سازی تمامی کارکنان از این خط‌مشی چاره‌اندیشی‌ها و روش‌های استفاده از آن باید بخشی از سیاست‌های امنیتی بوده که باید با سیاست‌گذاری‌های مناسب همراه باشد. کارکنانی که با اطلاعات حیاتی سر و کار دارند باید از مفهوم امنیت اطلاعات قابل حذف، آگاهی کامل پیدا کنند، اگر آگاهی و آموزش امنیتی به عنوان بخشی از مشاغل در نظر گرفته شود افراد نسبت به شغل و وظیفه خود احساس مسئولیت می‌کنند. یکی از بهترین راه‌های کاهش ریسک‌های امنیت اطلاعات در سازمان‌ها آگاه سازی هرچه بیشتر کارمندان نسبت به مسائل امنیتی است این آگاهی به این معناست که آنها باید مسئولیت اعمال خود در محیط کاری را به عهده بگیرند.

۷– سطوح امنیت اطلاعات به کاربران

همان طور که در شکل زیر مشاهده می‌کنیم طبق تعریف NIST1 مراحل ارتقای دانش امنیت اطلاعات کاربران به سطوح آگاهی۲، تربیت۳ و تحصیلات و آموزش۴ تقسیم می‌شود[۹].



شکل ۳-۲: مراحل ارتقا دانش امنیت اطلاعات[۹]

همانطور که مشاهده می‌شود یادگیری دانش امنیت اطلاعات در سطح پایین که مربوط به همه کاربران می‌شود از آگاهی شروع می‌شود و با

[1] National Instituteof Standards and Technology
[2] Awareness
[3] Training
[4] Education

آشنایی با مفاهیم و ادبیات امنیت وارد مرحله تربیت می‌شود و سپس با آموزش‌های ویژه که مخصوص افراد متخصص در زمینه امنیت اطلاعات است وارد مرحله آموزش و تخصص می‌شود.

آگاهی صرفا آموزش نیست و هدف از آگاهی تمرکز بر اهمیت امنیت است، توجه به مقوله آگاهی به افراد اجازه می‌دهد تا نگرانی‌ها و مسئولیت‌های امنیت فناوری اطلاعات را تشخیص دهند. آگاهی‌رسانی امنیتی مختص تمامی کارمندان سازمان است به نحوی که هدف آگاهی‌رسانی امنیتی به صورت ساده جلب توجه مخاطبین به اهمیت مقوله امنیت در سطح سازمان و ایجاد هوشیاری امنیتی بیشتر در بین مخاطبین است به طوری که کارمند به سادگی از کنار مسائل به ظاهر جزئی نگذرند و به موقع نگرانی‌های امنیتی را تشخیص داده و عملکرد مناسبی در سطح وظایف و اختیارات خود انجام دهند. ابزارهای مناسب برای این امر شامل پوستر، بولتن، روزنامه، آموزش آنلاین و آموزش‌های مبتنی بر شبکه و غیره می‌باشند.

طبق تعریف NIST تربیت به تولید شایستگی‌ها و مهارت‌های امنیتی مرتبط و لازم می‌پردازد مقوله تربیت نیروی انسانی مختص کارمندی است که با سیستم‌های فناوری اطلاعات در سازمان ارتباط داشته و همچنین عهده‌دار وظایف و مسئولیت‌هایی در این سطح است در واقع هدف تربیت نیروی انسانی تلاش در جهت کسب مهارت و شایستگی برای راهبری هرچه بهتر سیستم‌های فناوری اطلاعات می‌باشد.

طبق تعریف NIST آموزش و تحصیلات، تمام مهارت‌ها و صلاحیت‌های امنیتی را با تخصص‌های کاربردی گوناگون در یک دانش کلی ادغام کرده و تلاش می‌کند تا متخصصین امنیت فناوری اطلاعات را متناسب با اهداف و مسئولیت‌ها پرورش دهد. آموزش متخصص در زمینه امنیت شبکه، مختص متخصصین امنیت شبکه سازمان است. هدف از آموزش کسب دانش و تجربه در امر طراحی، پیاده‌سازی و پشتیبانی سیستم‌های امنیت شبکه می‌باشد؛ فرایند آموزش در سه سطح مقدماتی، متوسطه و پیشرفته صورت می‌پذیرد لذا در این بخش لازم است ضمن تبیین ضرورت‌ها و اهداف آموزش متخصصین امنیت شبکه سازمان، سطوح مختلف آموزش و روش‌های اجرایی برای این منظور انتخاب و اعلام گردد.

۸- آگاهی از امنیت اطلاعات

یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات ارتقاء آگاهی کاربران از امنیت اطلاعات است در این صورت افراد آگاهی‌های لازم و مربوط به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می‌کنند. آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت‌های خوب امنیتی می‌شود و به افراد اجازه می‌دهد تا نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند و به تدریج به فرهنگ سازمان‌ها تبدیل خواهد شد لذا بایستی به موازات تمهیدات فنی اعمال شده جهت امنیت اطلاعات، در قوانین و سیاست‌های جاری نیز متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و اطلاع‌رسانی تجدید نظر شود و آموزش‌های صحیح به کارگیری اطلاعات و تأمین امنیت آنها با اولویت بالاتری در سطح جامعه ترویج شود. آگاهی از امنیت اطلاعات طبق نظر پارک و همکاران شامل سه بعد زیر است [۱۰]:

الف) آگاهی عمومی از امنیت اطلاعات به معنای آگاهی‌رسانی عمومی در زمینهٔ ابعاد امنیت از جمله اهداف یک سیستم مدیریت امنیت اطلاعات است که با هدف افزایش آگاهی عمومی کاربران و جامعهٔ مخاطبان سیستم‌های مدیریت امنیت اطلاعات صورت می‌گیرد.

ب) آگاهی از قوانین امنیت اطلاعات که یک مفهوم ساختاری جدید است که به آگاهی، درک و رعایت کارکنان از سیاست‌ها، قوانین و اطلاعات امنیتی سازمان مرتبط اشاره و بیان می‌کند که آگاهی کارکنان از سیاست امنیت اطلاعات سازمان تأثیر مثبتی بر نگرش کارکنان برای موافقت با سیاست‌های امنیتی شرکت دارد.

ج) آگاهی از شدت مجازات نقض امنیت اطلاعات به دانش و درک درست کارکنان از انواع مجازات و شدت مجازات‌های مرتبط با نقض امنیت اطلاعات سازمان اطلاق می‌شود.

۹- آگاهی کارمندان از امنیت اطلاعات

یکی از جنبه‌ها و راه‌های غیر فنی برای حفاظت و مدیریت امنیت اطلاعات آگاهی کلیه کارمندان از امنیت اطلاعات است که یکی از موضوعات مهم در امنیت اطلاعات است، توجه به مقوله آگاهی از امنیت اطلاعات منجر به این می شود که کلیه افراد آگاه به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود باشند. آگاهی از امنیت اطلاعات در همه افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت‌های خوب امنیتی می‌شود و به افراد اجازه می‌دهد تا نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند و به تدریج به فرهنگ در سازمان‌ها تبدیل خواهد شد. بنا به پیشنهاد OECD به موازات تمهیدات فتی اعمال شده جهت امنیت اطلاعات لازم است در قوانین و سیاست‌های جاری متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و

اطلاع‌رسانی تجدید نظر شده و فرهنگ و آموزش‌های صحیح بکارگیری اطلاعات و تأمین امنیت آنها در اولویتی بالاتر نیز در سطح جامعه ترویج شود لذا آگاه‌سازی امنیتی کارمندان یکی از کلیدی‌ترین فاکتورهای پیاده‌سازی موفق سیاست امنیتی در سطح یک سازمان می‌باشد که هدف اصلی آن تعریف نقش هر یک از کارمندان در کار با اطلاعات سازمان است؛ این برنامه ضمناً سعی دارد که به روش ساده و کارآمد علاقه مضاعفی را در زمینه امنیت اطلاعات ما بین تمامی کارمندان ایجاد نماید[۱۱].

۱۰- سطوح آگاهی از امنیت اطلاعات

رفتار امنیتی ضعیف برخی از کاربران مثلا خطاهای امنیتی کاربران، بی‌دقتی و عدم توجه در بسیاری از رخدادهای امنیتی دخیل بوده است بسیاری از سازمان‌ها به اهمیت برقراری یک برنامه برای آگاهی‌رسانی پیرامون امنیت اطلاعاتی در سازمان‌های خود پی برده‌اند. در موفقیت این نوع برنامه‌ها حصول اطمینان از اینکه کارمندان به سه سطح از آگاهی از خطرات امنیتی می‌رسند بسیار دخیل است که این سه سطح شامل دانش، درک و نگرش و رفتار و برون‌دهی هستند. با پیشرفت کارمندان یک سازمان در راستای این سه سطح امنیت از سوی افراد بالاتر می‌رود که بالا رفتن آگاهی امنیتی افراد و کاربران نهایی می‌تواند به تغییر فرهنگ‌ها و ارزش‌های امنیتی کمک کند و از این طریق صلاحیت امنیتی بهتری ایجاد می‌شود. اگرچه روشی واحد برای برنامه‌های مربوط به آگاهی امنیتی که با تمامی موقعیت‌ها در سطح سازمانی و انسانی در عملکردهای مختلف وجود ندارد اما داشتن یک روش ثابت برای برقراری یک برنامه آگاهی امنیتی براساس سطوح آگاهی امنیتی بسیار ضروری است[۱۲].

- سطح اول دانش

اولین گام در تأمین امنیت یک سازمان آگاهی یافتن و کسب دانش و اطلاعات لازم جهت درک خطرات امنیتی محیط شغلی است؛ دانش شناسایی حضور یک تهدید و آگاه شدن از آن با توجه به اطلاعات قبلی است، از مزایای تشکیل یک تصویر صحیح از تهدیدات امنیتی محیط اطراف تا حد زیادی می‌تواند با ارتقای مشاهده و درک آگاهی امنیتی تقویت شود.

- سطح دوم نگرش

داشتن دانش و اطلاعات کافی از نحوه رخداد حوادث امنیتی و تأثیرات آن به تنهایی کارساز نیست بلکه کاربران باید به این حد از فهم برسند که امنیت اطلاعات و رعایت نکات ایمنی به هنگام استفاده از اطلاعات و فناوری اطلاعات در مرحله اول به نفع خود آنها و سپس سازمان آنهاست لذا با داشتن یک نگرش مثبت می‌توانند از دانش خود به بهترین شکل استفاده کرده و حتی آن را بنا به نیاز ارتقا دهد.

- سطح سوم رفتار و برون‌دهی

پیشگیری بهتر از درمان است، برای اجتناب از بروز خطرات امنیتی کاربران نهایی باید توانایی برون‌دهی یا پیش‌بینی دوره‌های بعدی حملات امنیتی را داشته باشند. برون‌دهی سومین سطح از ارتقای آگاهی امنیتی است؛ در این سطح رفتارها و عادت‌های خوب امنیتی در فرد ایجاد می‌شود و به ساختن فرهنگ امنیت اطلاعاتی منجر می‌شود و تصمیمات به موقع را می‌توان با آمادگی در توانایی برون‌دهی و رفتار گرفت.

۱۱- نقش آگاهی‌رسانی در امنیت اطلاعات

در سال‌های اخیر با پیشرفت فناوری اطلاعات و ارتباطات شاهد به کارگیری تجهیزات الکترونیکی و روش‌های مجازی در بخش عمده‌ای از فعالیت‌های روزمره همچون ارائه خدمات مدیریت و نظارت و اطلاع‌رسانی هستیم. فضایی که چنین فعالیت‌هایی در آن صورت می‌پذیرد با عنوان فضای تبادل اطلاعات شناخته می‌شود؛ فضای مذکور همواره در معرض تهدیدهای الکترونیکی یا آسیب‌های فیزیکی از قبیل جرایم سازمان یافته به منظور ایجاد تغییر در محتوا یا جریان انتقال اطلاعات، تخریب بانک‌های اطلاعاتی، اختلال در ارائه خدمات اطلاع‌رسانی یا نظارتی و نقض حقوق مالکیت معنوی است از طرف دیگر با رشد و توسعه فزاینده فناوری اطلاعات و گسترش شبکه‌های ارتباطی آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای یاد شده گسترده‌تر و پیچیده‌تر می‌شود. از این رو حفظ ایمنی فضای تبادل اطلاعات از جمله مهمترین اهداف توسعه فناوری اطلاعاتی و ارتباطی محسوب می‌شود. امروزه موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش افرادی که در به کارگیری آن درگیرند وابسته است؛ تحقیقات گذشته نشان می‌دهد یکی از فاکتورهای موثر در عوامل انسانی موضوع آگاهی و اطلاع‌رسانی به کاربران از امنیت اطلاعات است آموزش و آگاهی‌رسانی بایستی یکی از پایه‌ها و سرفصل‌های برنامه‌های امنیتی هر سازمان قرار گیرد که فقدان این مسئله در سازمان‌های دولتی به شدت مشهود است. همین طور در سطح اجتماع در حالی که نفوذ کامپیوتر به سرعت ادامه دارد روند برنامه‌های آموزشی و اطلاع‌رسانی به کندی پیش می‌رود این امر باعث شده که کارکنان سازمان‌ها از حداقل آگاهی‌ها و تدابیر دفاعی لازم آگاه نباشند[۱۳].

۱۲- نتیجه‌گیری

در سال‌های اخیر با رشد و توسعه فزاینده فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته و روش‌های اعمال تهدیدهای یاد شده گسترده‌تر و پیچیده‌تر شده است که در این راستا حفظ ایمنی فضای تبادل اطلاعات از جمله مهمترین اهداف توسعه فناوری اطلاعاتی و ارتباطی محسوب می‌شود. یکی از جنبه‌ها و راه‌های مهم جهت حفاظت و مدیریت امنیت اطلاعات، ارتقاء آگاهی کاربران از امنیت اطلاعات می‌باشد که افراد آگاهی‌های لازم و مربوط به نقش و مسئولیت خویش را در جهت حفظ امنیت اطلاعات در کار مربوط به خود کسب می‌نمایند. بنابراین جهت پیشگیری از حوادث ناشی از خطای انسانی متأثر از رفتار حرفه‌ای نسبت به رعایت الزامات امنیتی از سوی کارکنان و ضرورت توجه به آگاهی امنیتی با آموزش‌های لازم در راستای به حداقل رساندن مخاطرات پیرامون امنیت اطلاعات برای بسیاری از سازمان‌ها به چالش بزرگی تبدیل شده است. لذا می‌توان گفت آگاهی امنیتی کاربران نقش بسزایی در امنیت اطلاعات سازمان‌ها دارد. بر این اساس در این تحقیق بر آن شدیم تا موضوع آگاهی امنیتی و پیروی از مقررات امنیتی توسط کارکنان حوزه فناوری اطلاعات اداره کل بنادر و دریانوردی استان خوزستان را مورد بررسی قرار دهیم. بنابراین در فرآیند اجرایی تحقیق ابتدا پرسشنامه‌هایی که توسط پاسخ دهندگان که ۸۶۴ نفر از کارکنان اداره کل بنادر و دریانوردی بندرامام خمینی بودند تکمیل گردیده است را جمع‌آوری و داده‌های خام مورد نیاز جهت توصیف و آزمون فرضیه‌ها به کمک رایانه و نرم‌افزار استخراج نمودیم و سپس این داده‌ها از طریق نرم‌افزار SPSS تجزیه و تحلیل شده و در دو مرحله به اطلاعات مورد استفاده در این تحقیق تبدیل شدند. در مرحله اول که تجزیه و تحلیل توصیفی می‌باشد داده‌های جمع‌آوری شده به صورت جدول آمار توصیفی ارائه گردیدند و در مرحله دوم که تجزیه و تحلیل استنباطی می‌باشد با استفاده از معادلات ساختاری مورد بررسی قرار گرفتند. نتایج بدست آمده از این تحقیق نشان دهنده این موضوع است که نگرش کارکنان نسبت به پیروی از سیاست‌های امنیتی سیستم‌های اطلاعاتی بیشترین تأثیر را بر پیروی کارکنان دارد اما از آنجایی که نگرش افراد در طول زمان تکامل فرد شکل می‌گیرد و عوامل متعددی از جمله ارزش‌ها، تجربه مستقیم، جامعه‌پذیری، خودخدمتی و غیره در شکل‌گیری آن نقش دارند لذا به نظر می‌رسد تغییر نگرش امری پیچیده و سخت باشد چرا که نگرش‌ها در طی زمان کمتر دچار تغییر می‌شوند اما توجه به این نکته لازم است که هرچند تغییر نگرش سخت است اما در هر حال نگرش‌ها قابل تغییر هستند و این امر می‌تواند به نفع سازمان مربوطه باشد.

مراجع

[1] Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282-293.

[2] Xue, B., Xu, F., Luo, X., & Warkentin, M. (2021). Ethical leadership and employee information security policy (ISP) violation: exploring dual-mediation paths. *Organizational Cybersecurity Journal: Practice, Process and People*.

[3] Alzahrani, L., & Seth, K. P. (2021). The Impact of Organizational Practices on the Information Security Management Performance. *Information*, *12*(10), 398.

[4] Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability*, *12*(20), 8576.

[5] Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems*, *21*(1), 5.

[6] Arhin, K., & Wiredu, G. O. (2018). An organizational communication approach to information security. *The African Journal of Information Systems*, *10*(4), 1.

[7] Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)* (pp. 62-68). IEEE.

[8] Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*,

282-293.

[9] Hong, Y., & Furnell, S. (2022). Motivating information security policy compliance: Insights from perceived organizational formalization. *Journal of Computer Information Systems*, *62*(1), 19-28.

[10] Park, E. Kim, J. & Park, Y. S. (2017) "The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information." *Computers & Security*, 65: 64-76

[11] dos Santos Vieira, P., DIAS, M. D. O., Pereira, L. J. D., & da Silv, G. D. B. P. (2022). Brazilian Organizational Culture on Information Security: A Literature Review. *GPH-International Journal of Business Management (IJBM)*, *5*(01), 56-67.

[12] Jafari, M. S., Hamidizadeh, A., & Montazeri Najafabadi, R. (2016). Investigating the effective factors on employees' compliance with information systems security policies in the organization. Scientific Journal of Information Management, 2(2), 102-131.

[13] Kumah, P. (2022). The role of human resource management in enhancing organizational information systems security. In *Research Anthology on Human Resource Practices for the Modern Workforce* (pp. 1251-1277). IGI Global.