امنیت اطلاعات در حوزه‌ی منابع انسانی

مصطفی فرازی*

چکیده:

امنیت اطلاعات مقوله‌ای است که در دهه‌ی جدید به شدت مورد توجه قرار گرفته است. وجود تهدیدهای بی‌شمار در فضای کسب و کار کنونی با توجه به ماهیت متغیر آنها نیاز به سیستم مدیریت امنیت اطلاعات را بیش از پیش توجیه می‌نماید.

هدف از این مقاله لزوم توجه به امنیت منابع انسانی سازمان‌ها به عنوان آسیب‌پذیرترین دارایی هر سازمان است.

در این مقاله ابتدا با عناوینی چون امنیت اطلاعات آشنا می‌شویم و سپس به بررسی راهکارهای مناسب جهت ایجاد امنیت نیروی انسانی می‌پردازیم.

کلید واژه:

امنیت اطلاعات، آگاهی از امنیت اطلاعات، مدیریت امنیت اطلاعات، استانداردهای امنیت اطلاعات، ISO27001، ISO27002، ISMS

مقدمه:

از فناوری اطلاعات می توان به عنوان بزرگترین فناوری در طول تاریخ یاد کرد که توانسته بین رشته‌های مختلف علوم، ارتباط برقرار کند. این فناوری با بکارگیری تمام علوم توانسته است اطلاعات مورد نیاز پژوهشگران، صنعتگران، بازرگانان و همچنین قشرهای مختلف جامعه را در کمترین زمان و بهترین وجه فراهم کند به طوری که می توان ادعا کرد امروزه فناوری اطلاعات، مرزهای کشورهای مختلف را در نوردیده و ملتها را در یک جامعه جهانی گردهم آورده است.

گفتن و شنیدن از مزایای فناوری اطلاعات و امکاناتی که برای بشر به ارمغان آورده همواره لذتبخش است. اما این فناوری همانند سایر فناوری ها همچون سکه دو رو دارد: فرصت و تهدید. اگر به همان اندازه که به توسعه و فراگیری آن توجه می‌کنیم به امنیت آن توجه نکنیم می تواند به یک تهدید و مصیبت بزرگ تبدیل شود.

* کارشناسی ارشد مهندسی صنایع دانشگاه آزاد اسلامی واحد تهران جنوب

Email:MostafaFarazi@gmail.com

حجم بالای اطلاعات در هر سازمان در قالب طرح ها، نقشه ها، سیاستها، بخشنامه ها، مکاتبات بازرگـانی، مستندات پروژه‌های پژوهشی و سایر اطلاعاتی که ما برای ذخیره‌سازی و پردازش در اختیار این فناوری قـرار می‌دهیم، ما را برآن می‌دارد تا به فکر حفاظت از آن نیز باشیم.

اطلاعات یاد شده مهمترین دارایی و کلید رشد و موفقیت هر سازمان است. اگر نتوانیم این دارایی مهم را از دسترس نامحرمان و سایر تهدیدها حفظ کنیم به شدت آسیب می بینیم.

بنابراین هر سازمان برای ادامه‌ی حیات و زنـدگی خـود نیازمنـد کسـب اطلاعـات گونـاگون و همچنـین حفاظت از اطلاعات و اسرار خود می‌باشد.

امنیت اطلاعات

اطلاعات، دارایی است همانند سایر دارایی‌های مهم کسب و کار کـه بـرای کسـب و کـار سـازمان دارای اهمیت است، و در نتیجه باید به گونه‌ای مناسب محافظـت شـود. ایـن موضـوع مخصوصـاً در محیطـی کـه تعاملات کسب و کار رو به رشد است، از اهمیت بیشـتری برخـوردار اسـت. در نتیجـه ایـن افـزایش تعامـل، اطلاعات در معرض تعداد بیشتر و انواع گوناگون‌تری از تهدیدات و آسیب‌پذیری‌ها قرار گرفته است.

امنیت اطلاعات، محافظت از اطلاعات در برابر طیف گسترده‌ای از تهدیدات است که به منظور اطمینان از استمرار کسب و کار، کمینه کردن ریسک کسب و کار، حداکثر کردن آورده و فرصتهای کسب و کار است.

نیازهای امنیتی از طریق برآورد روش‌مند ریسک‌های امنیت برای دارایی‌های مختلف، شناسایی می‌شـود. پس از اینکه نیازهای امنیتی و ریسک‌ها، شناسایی شدند کنترل های مناسب جهت برطرف‌سازی تهدیـدهـا انتخاب می‌گردد.

تعدادی از این کنترل‌ها در استانداردهای ISO27001و ISO27002 بعنوان اصول راهنمـا بـرای مـدیریت امنیت اطلاعات، در نظر گرفته شده که در بیشتر سازمان‌ها قابل به کارگیری هستند.

امنیت نیروی انسانی

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 امنیـت اطلاعـات نخواهند داشت.

ولد(۲۰۰۴) در قسمتی از پژوهش خود به یک واقعه تاریخی اشاره می کند: دراواخر سال ۱۲۰۰مـیلادی کوبلای خان و ایل وتبار مغولی او سعی در عبور از دیوار چین داشتند، اما دیوار بسیار محکم و طـولانی بـود. عاقبت به صورت آرام و ساکت، با تطمیع دروازه‌بان، ترتیبی اتخاذ کردند تا با پیروزی بر آن موانـع، توانسـتند بخش بزرگی از کشور چین را فتح کنند. مفهوم این گفته این است که مهم نیست کنترلهای فنی چقدر قوی

باشند، بلکه امنیت همیشه به افراد داخل سازمان بستگی دارد. همچنین در کتاب «راهنمای امنیت اطلاعات» آمده که بسیاری ازپژوهشها نشان می دهند بیش از ۸۰ درصد مشکلات امنیتی پیش آمده در سازمانها ناشی از خطاهای سهوی و عمدی کارکنان بوده است. (Sadowsky et al,2003)

دو نقل بالا بر این نکته تاکید دارند که انسان آسیب پذیرترین عنصر در حلقه امنیت اطلاعات می باشد، از این رو توجه به آن در رسیدن به حداکثر ایمنی کمک می‌کند. شاخصهای موثر در امنیت نیروی انسانی که می‌توانند سبب بروز اختلال در فعالیتهای نیروی انسانی شوند، عبارتند از:

- کار زیاد
- نداشتن مهارت کافی و لازم
- تداخل مسئولیتها
- عدم اطلاع از میزان ارزش اطلاعات
- نداشتن انگیزه
- کوتاهی و بی مسئولیتی
- فراموش کاری

یکی از جنبه‌ها و راههای مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقاء آگاهی کاربران از امنیت اطلاعات است. در این صورت، افراد آگاهی های لازم و مربوط به نقش و مسؤولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می کنند (Von Solms, 2004). آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت های خوب امنیتی می شود و به افراد اجازه می‌دهد تا نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند (Wilson & Hash, 2003). و به تدریج به فرهنگ سازمان ها تبدیل خواهد شد (Kruger & Kearrney,2006؛ Niekerk &Solms, 2009)

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 سازمان ترویج شود.

در یکی از تحقیقات مهم در این زمینه که توسط چو ، کیم و جو(Choi et al.,2008) انجام شد، یافته‌ها حاکی از آن بود که افزایش میزان آگاهی و دانش کاربران از امنیت اطلاعات تأثیری مستقیم بر نحوه عمل و رفتار امنیتی کارکنان خواهد گذاشت و در نتیجه، عملکرد سازمان بهبود خواهد یافت.

در تحقیقی دیگر، که توسط ویگا و الوف (Veiga & Eloff,2010) انجام گرفت، چارچوبی برای ایجاد فرهنگ امنیت اطلاعات ارائه شد. وی تبیین مدل خود را بدین صورت بیان نمود که برخی از مؤلفه‌ها مانند رهبری و حاکمیت در سازمان، تغییر، سیاست‌های امنیتی، رویه‌ها و دستورالعمل‌ها با تأثیرگذاری بر رفتار، چه به صورت فردی، گروهی و سازمانی منجر به ایجاد فرهنگ امنیت اطلاعات در سازمان خواهند شد.

آگاهی و آموزش امنیت اطلاعات به کاربران

از جمله فاکتورهای مؤثر عوامل انسانی در تأمین امنیت اطلاعات، موضوع آگاهی و آموزش امنیت اطلاعات کاربران است.

با سریع تر شدن آهنگ تغییرات فناوری، نیاز به تدابیر منعطف امنیتی نیز بیشتر احساس می شود؛ لذا اداره صحیح اطلاعات و آگاه‌سازی تمامی کارکنان از خط‌مشی‌ها، چاره‌اندیشیها و روشهای استفاده از آن، باید بخشی از سیاست‌های امنیتی باشد و با سیاستگذاری‌های مناسب همراه باشد. کارکنانی که با اطلاعات حیاتی سر و کار دارند باید از مفهوم امنیت اطلاعات 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 مسؤولیت می‌کنند. درباره بحث آموزش، تربیت و آگاهی نیروی انسانی بحثهای زیادی انجام شده است. دلیل آن این است که آنها اساساً یک مسأله مرتبط با عوامل انسانی هستند. این مهم است که تشخیص دهیم که مسائل انسانی در بیشتر مواقع علت اصلی نواقص امنیتی است. یکی از بهترین راههای کاهش ریسکهای امنیت اطلاعات در سازمانها، آگاهسازی هر چه بیشتر کارمندان نسبت به مسائل امنیتی است. این آگاهی به این معناست که آنها باید مسؤولیت اعمال خود در محیط کاری را به عهده بگیرند.

در یک بررسی که در سال ۲۰۰۲ درباره استفاده نادرست از فناوری اطلاعات، توسط کمیسیون نظارت انگلستان انجام شد، بیان شد که اکثر دلایل این استفاده‌های نادرست به افراد مربوط می‌شود. از این میان یک سوم موارد گزارش شده مربوط به فقدان آگاهی امنیتی و ۲۳٪ هم ناشی از عدم آموزش کافی یا نادرست بود. این نشان می‌دهد اگر افراد می‌خواهند امنیت اطلاعات را به صورت اثربخشی تأمین کنند، نیاز است آنچه را که از آنها انتظار می‌رود، بهتر بدانند. همچنین بنا بر نتایج گزارش، موضوع آگاهی‌رسانی و آموزش کاربران از مسائل امنیتی بعد از مسأله حمایت توسط مدیریت، از مهم ترین مباحث امنیتی است.

راه‌کارها و اقدامات موثر بر امنیت منابع انسانی

- نقش‌ها و مسئولیت‌های امنیتی کارکنان با توجه به خط‌مشی امنیت اطلاعات سازمان، تعریف و مستندسازی شوند.
- کارکنان تعهدنامه‌ای درباره نقش‌ها و مسئولیت‌های امنیتی خود امضا کنند.
- یک فرآیند انظباطی رسمی برای کارکنانی که مرتکب یک نقض پیمان رخنه امنیتی می‌شوند، وجود داشته باشد.
- تمامی کارکنان سازمان آموزش آگاه‌سازی مناسب و به روزرسانی قاعده‌مند خط‌مشی‌ها و رویه-های سازمانی را آنگونه که به وظایف شغلی آنها مربوط است، دریافت کنند.

- بالا بردن مهارتهای فنی گروه امنیت: تعلیم و تربیت کارکنان گروه مدیریت امنیت اطلاعات با سایر کارکنان تفاوت دارد، زیرا این حوزه به طوردائم در حال تغییر و دگرگونی است. کارکنان این گروه باید به طور مستمر با سازمان در کنفرانسهای فنی و تکنیکی و دوره‌های تخصصی با موضوعات امنیت نرم افزار و شبکه و مطالعه مجله‌ها و سایر مستندات منتشر شده، اطلاعات خود را به روز نگه دارند.
- مدیریت سازمان باید اطمینان حاصل کند که کلیه کارمندان در مورد اهمیت اقدامات مرتبط با امنیت اطلاعات آگاهی لازم را دارند و می‌دانند که چگونه باید با همکاری یکدیگر اهداف امنیتی را برآورده نمایند.

نتیجه‌گیری

سازمانها بایستی علاوه بر سرمایه‌گذاری بر راه‌حل‌های فنی برای حفظ امنیت اطلاعات، به عوامل غیر فنی و انسانی از جمله ارتقاء سطح آگاهی کلیه کارمندان از مؤلفه های امنیت اطلاعات، توجه بیشتری داشته باشند. برای این منظور لازم است مسؤولین ذیربط در حیطه فناوری اطلاعات، یک چارچوب مناسب در جهت ارزیابی میزان آگاهی کارمندان و آموزش امنیت اطلاعات پیشرو داشته باشند و با استفاده از این چارچوب و با در نظر گرفتن اولویت مؤلفه ها، اولویت سطوح (دانش، نگرش و رفتار) هر مؤلفه و عوامل مؤثر در آن قادر خواهند بود برنامه های آموزشی آگاهی از امنیت اطلاعات را به نحوی مؤثرتر و مفیدتر ارائه دهند.

منابع و ماخذ

محمودزاده، ابراهیم.(۱۳۸۵) مدیریت امنیت در سیستم‌های اطلاعاتی: فصلنامه علـوم مـدیریت ایـران، دوره اول، شماره ۴،ص ۷۸-۱۱۲

حسن‌زاده، محمود.(۱۳۹۰) ارائه یک چارچوب مفهومی برای ارزیـابی پرمـایگی و آمـوزش آگـاهی از امنیـت اطلاعات کاربران: فصلنامه نظام‌ها و خدمات اطلاعاتی، سال اول، شماره ۲،ص۱-۱۶

استاندارد ملی ایران ایزو ۲۷۰۰۲. (۱۳۸۷) فن‌آوری اطلاعـات-فنـون امنیتـی- آیـین کـار مـدیریت امنیـت اطلاعات

استاندارد ملی ایران ایزو ۲۷۰۰۱. (۱۳۸۷) فن‌آوری اطلاعات-فنون امنیتی- سیسـتم‌هـای مـدیریت امنیـت اطلاعات – الزامات

Choi, Namjoo, Kim, Dan, Jahyun (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. Information Management & Computer Security, 16, 484-485

Von Solms R, Von Solms B. (2004) Information security management (1): why information security is so important. Information Management and Computer Security, Vol 6, PP. 174-77

Wilson, Mark, and Hash, Joan (2003). Building an information technology security awareness and training program National Institute of Standards and Technology, sp 800-50, 20-79

Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information Security awareness. Computer & security, 25, 289-296.

Nikrerk J.F. and Solms, Van (2009). Information security culture: a management perspective. Computer & security, 5, 142-144.

Veiga, A. Da., and Eloff, J.H.P (2010). A Framework and Assessment Instrument For Information Security Culture. Computer & Security, 29(2), 196-200.