3rd National Conference on Interdisciplinary Research in Management & Humanistic Science
25 February 2022-Tehran
سومین همایش ملی تحقیقات میان رشته ای در مدیریت و علوم انسانی
۶ اسفند ۱۴۰۰ محل برگزاری: تهران

بررسی مدیریت امنیت اطلاعات و کامپیوتر

زهرا بیات
دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه پیام نور البرز، واحد کرج
www.bayat7104@yahoo.com

چکیده

تکنولوژی و اینترنت بخش جدایی ناپذیر زندگی امروز است؛ به طوریکه که عموم افراد از تلفن های هوشمند و اینترنت استفاده می کنند و همه ی سازمان ها و شرکت ها حجم زیادی از اطلاعات خود را در کامپیوترها ذخیره می کنند. این موضوع ضمن ایجاد سرعت در انجام کارها، مشکلاتی را نیز به همراه دارد. سرقت اطلاعات یک سازمان، دسترسی به داده های شرکت ها، سوء استفاده از اطلاعات شخصی افراد، سودجویی از اطلاعات حساب بانکی از جمله مواردی هستند که در صورت عدم رعایت امنیت اطلاعات رخ خواهد داد؛ بنابراین موضوع امنیت اطلاعات جزئی جدایی ناپذیر از زندگی امروز است. سازمان ها و دولت ها برای حفظ اطلاعات خود، نیازمند متخصصانی هستند که امنیت لازم را برای آنها فراهم کنند و به طور پیوسته سیستم های امنیت اطلاعاتشان را به روز کنند. متاسفانه در حال حاضر سیستم یا روش خاصی وجود ندارد که امنیت اطلاعات را به طور قطع فراهم کند و از این رو لازم است تا مجموعه ای از نکات، معیارها و استانداردها در نظر گرفته شود تا از این طریق قادر به ایجاد امنیت حداکثری برای حفاظت داده ها باشیم. طی این پژوهش ابتدا به توضیح مختصری از پیشنه ی امنیت اطلاعات می پردازیم و در ادامه با مفهوم امنیت اطلاعات آشنا می شویم؛ سپس ضمن بررسی اهمیت سرمایه گذاری در این حیطه، به طور خلاصه به توضیح در خصوص چرخه ی ایجاد امنیت اطلاعات خواهیم پرداخت.

واژگان کلیدی: مدیریت امنیت اطلاعات، حفاظت اطلاعات کامپیوتری، سرمایه گذاری امنیت اطلاعات

مقدمه

امنیت اطلاعات موضوعی است که بشر از همان روزهای آغازین ارتباط خود نگران آن بوده است. دیپلمات ها و فرماندهان نظامی از زمان های بسیار دور همواره در تلاش بودند تا مکانیزمی برای محافظت از اطلاعات محرمانه ی خود بیابند. جولیوس سزار ۵۰ سال قبل از میلاد، برای جلوگیری از خوانده شدن پیام های مخفی خود، رمز سزار را اختراع کرد. یکی از مشخصات رمز سزار به این ترتیب بود که اطلاعات مهم و حساس علامت گذاری می شدند تا از این طریق مشخص شود که تنها افراد مورد اعتماد میتوانند آن

را حمل کنند، البته پیش از حمل نیز، نامه ها در جعبه ای امن قرار می گرفتند. به مرور و با گسترش خدمات پستی، دولت ها و سازمان های رسمی در راستای حفاظت اطلاعات خود از رمزهای خاص و مهر و موم کردن نامه ها استفاده می کردند. روش هایی که ذکر شد امنیت بالایی نداشتند و در صورت خیانت یکی از افراد حمل کننده نامه، به راحتی آن اطلاعات قابل دسترسی بودند؛ از این رو در اواسط قرن نوزدهم میلادی سیستم های حفاظت اطلاعات، طبقه بندی پیچیده تری پیدا کردند تا از این طریق به دولت ها کمک کنند تا اطلاعات خود را بر اساس میزان حساسیت محافظت کنند. در زمان جنگ جهانی اول محافظت از اطلاعات اهمیت بیشتری پیدا کرد و از این رو سازمان های نظامی از کدسازی اطلاعات استفاده می کردند و به این ترتیب در زمان جنگ، رمزگذاری پیچیده تر از قبل شد؛ چراکه افشای هر نوع اطلاعاتی در شرایط جنگی برابر با شکست خواهد بود و حفاظت از اطلاعات در این شرایط با حفاظت از کشور برابری می کند. مطابق با آنچه ذکر شد، روشن است که محافظت اطلاعات و امنیت آنها همواره موضوعی مهم بوده است.

ایجاد امنیت برای اطلاعات کامپیوتری، موضوعی بود که طی جنگ جهانی دوم اهمیت پیدا کرد. حجم اطلاعات به اشتراک گذاشته شده توسط کشورهای متفین در طی جنگ جهانی دوم، همسویی سیستم های طبقه بندی را ضروری کرد. یکی از تجهیزات استفاده شده؛ ماشین انیگما (Enigma Machine) بود که توسط آلمانی ها برای رمزگذاری اطلاعات جنگ استفاده شده بود و تا ۱۳ سال بعد از ساخت، رمز آن غیر قابل کشف تصور می شد؛ در نهایت آلن تورینگ با موفقیت آن را رمز گشایی کرد، این رمز گشایی میتواند به عنوان نمونه ای بارز برای توجه به اهمیت امنیت اطلاعات و مراقبت از آنها درنظر گرفته شود. بدون شک ضمن درنظر گرفتن مجموعه عوامل موثر در تغییر مسیر جنگ جهانی دوم و شکست آلمان ها، شکست ماشین انیگما و کشف رمز آن نیز تاثیر به سزایی در این مسیر داشت. تلاش های انجام شده در حوزه ی امنیت اطلاعات در طول جنگ جهانی دوم هم از منظر ایجاد امنیت و همینطور از حیث روش ها و تکنیک های شکست ساختارهای امنیتی بسیار قابل توجه هستند.

سال ها بعد از جنگ جهانی دوم، وزارت دفاع ایالات متحده پروژه ای تحقیقاتی را در خصوص امکان سنجی یک سیستم شبکه ای ارتباطی برای تجارت اطلاعات در داخل نیروهای مسلح ایالات متحده آغاز کرد؛ این پروژه در سال ۱۹۶۸ میلادی توسط دکتر لری رابرتز فرموله شد که به مرور تکمیل و تبدیل به آنچه به عنوان اینترنت شناخته می شود، شد.

با توجه به رشد تکنولوژی و گسترش استفاده از کامپیوترها و گوشی های هوشمند، تاثیر فناوری اطلاعات بر زندگی امروزه قابل انکار نیست. اغلب افراد، اطلاعاتی از قبیل عکس های خانوادگی، فیلم های محرمانه یا مجموعه ای از رمزها را در تلفن های همراه یا کامپیوترهای خود دارند که تمایلی به انتشار آنها ندارند. موضوعی که امروزه شاهد سرقت این اطلاعات و در نهایت سوء استفاده از آنها هستیم؛ علاوه بر این دسترسی به اطلاعات حساب افراد و سرقت موجودی بانکی هم از مشکلات رایج عدم توجه به موضوع

امنیت اطلاعات است. البته لازم به ذکر است که موارد عنوان شده، در دسته ی موارد ساده و پیش پا افتاده در خصوص امنیت اطلاعات قرار می گیرند. در برخی موارد سرقت اطلاعات یک سازمان منجر به نابودی آن سازمان یا شرکت خواهد شد؛ از این رو موضوع امنیت اطلاعات یکی از نگرانی های مهم برای کاربران و صاحبان سازمان ها است. حوزه ی امنیت اطلاعات در سال های اخیر رشد و تکامل چشمگیری داشته است به گونه ای که روش های مختلفی را برای ایجاد امنیت بسیاری از حیطه ها ارائه می دهد. تامین امنیت شبکه ها و زیرساخت های وابسته، ایمن سازی برنامه ها و پایگاه های داده، ممیزی سیستم های اطلاعاتی، برنامه ریزی تدام کسب و کار، پزشکی قانونی دیجیتال تعدادی از مواردی هستند که در حیطه ی امنیت آنها رشد قابل توجهی اتفاق افتاده است. موضوعی که باید به آن توجه کرد این نکته است که با توجه به سرعت رشد تکنولوژی برای حفاظت کامل از اطلاعات، باید به طور پیوسته روش های امنیتی را به روز کرد تا احتمال نفوذ به سازمان را به حداقل رساند. برای درک بهتر سرعت رشد تکنولوژی کافیست تلفن همراه خود را به اینترنت متصل کنید، مشاهده خواهید کرد؛ نرم افزارهایی که در حال استفاده از آنها هستید، به طور پیوسته نیازمند به روز رسانی هستند. موضوع در خصوص ویندوز کامپیوتر نیز به همین ترتیب، نیازمند به روز رسانی است و این یعنی همه روزه حملات متعددی در سراسر دنیا به سیستم ها و نرم افزارها اتفاق می افتد که باعث می شود شرکت های ارائه دهنده ی نرم افزارها برای جلوگیری از نفوذ مجدد، تغییراتی در سیستم های امنیتی خود بدهند و مجدد آنها را با اصلاحاتی به بازار ارائه دهند. به طور کلی موضوع امنیت اطلاعات فرایند پیچیده ای است که طی آن کشورها یا سازمان ها با کمک استفاده از فناوری سخت افزار و تکنولوژی نرم افزارها سعی در کنترل و حفاظت اطلاعات دارند. این کنترل ها می تواند به شکل های مختلفی صورت گیرند، از این رو رشته های مختلف دانشگاهی مانند امنیت کامپیوتری، امنیت اطلاعات و شبکه ایجاد شد تا متخصصانی در این حیطه تربیت شوند که بتوانند تسلط کافی بر سیستم های اطلاعاتی داشته باشند و میزان سرقت اطلاعات سازمان ها را به حداقل برسانند.

همه ی سازمان ها باید ارزش اطلاعات خود را ارزیابی کرده و روشی مشخص را برای حفاظت اطلاعات خود در نظر گیرند. برخی از مدیران اعتقاد دارند که سیستم امنیت اطلاعات موضوعی پر هزینه و وقت گیر است اما باید این نکته را در نظر بگیرند که در صورت از دست رفتن اطلاعات و داده های سازمان، هزینه های تحمیل شده بر آنها چقدر خواهد بود. اعمال سیستم های امنیت اطلاعات برای هر سازمانی ضروری است و با توجه به نوع فعالیت سازمان، ارزش و گستردگی اطلاعات سازمان ها، روش های متفاوتی ارائه می شود اما هیچگاه محو نخواهد شد. رشد اطلاعات در دنیای مدرن دیجیتال امروزی، امنیت آن را به موضوعی جدی تبدیل کرده است. در اصل تاثیر رویدادهای امنیتی کسب و کارها و سازمان ها به حدی جدی است که خطر افتادن امنیت اطلاعات

می تواند به سادگی زندگی روزمره مردم جهان را تحت تاثیر قرار دهد، به گونه ای که سرمایه گذاری جهانی بر توسعه ی راهکارهای حفظ امنیت اطلاعات هر ساله روبه افزایش است.

امنیت اطلاعات چیست؟

امنیت اطلاعات، عمل حفاظت از اطلاعات با کاهش خطرات اطلاعاتی است و معمولا شامل جلوگیری یا کاهش احتمال دسترسی غیرمجاز به داده ها یا استفاده ی غیرقانونی، افشاء، اختلال، حذف، فساد، بازرسی، ثبت یا کاهش ارزش اطلاعات است. علاوه براین مجموعه اقداماتی که به منظور کاهش اثرات نامطلوب این حوادث انجام می شوند هم در دسته ی امنیت اطلاعات قرار می گیرند. موضوع قابل توجه در این است که این اطلاعات می توانند به هرشکلی باشند؛ به عنوان مثال اطلاعات الکترونیکی یا اطلاعات فیزیکی (کاغذی) یا حتی اطلاعات نامشهود مانند دانش. تمرکز اصلی امنیت اطلاعات بر حفاظت متوازن از سه مشخصه ی محرمانگی، یکپارچگی و دردسترس بودن داده ها است که به آن مدل سه گانه امنیت اطلاعات (CIA Triad) گفته می شود.

مدل سه گانه امنیت اطلاعات

بر اساس این مدل، برای تامین امنیت اطلاعات باید سه پارامتر محرمانگی، یکپارچگی و در دسترس بودن اطلاعات را درنظر گرفت. در ادامه به تعریف مفاهیم این سه پارامتر می پردازیم.

محرمانگی اطلاعات

موضوع محرمانگی به معنای پیشگیری از افشاء اطلاعات برای افراد فاقد صلاحیت است. موضوع محرمانگی اطلاعات را میتوان در دو حیطه ی محرمانگی داده و حریم خصوصی طبقه بندی کرد. محرمانگی داده در یک سازمان مجموعه ای از اطلاعات هستند که آن سازمان تمایلی به افشاء آنها ندارد و از این رو باید به کمک مجموعه ای از روش ها و نرم افزارها، محیطی ایمن را برای اطلاعات خود فراهم آورد. در زمینه ی حریم خصوصی نیز این افراد هستند که مشخص می کنند چه اطلاعاتی اهمیت دارد و چه افرادی میتوانند در حریم خصوصی آنها حضور داشته باشند و همینطور چه افرادی هستند که احتمال افشاء اطلاعات توسط آنها وجود دارد.

یکپارچگی

یکپارچگی به این معناست که هیچ تغییری در اطلاعات ایجاد نشود، به این معنا که هیچ بخشی از اطلاعات حذف یا دچار تغییر نشده باشند. یکپارچگی را میتوان به دو صورت بررسی کرد؛ یکپارچگی داده و یکپارچگی سیستم. در هر دونوع منظور عدم ایجاد تغییر در هرکدام از موارد ذکر شده است و اگر قصد تغییری هم در آن باشد، باید توسط افراد مجاز انجام شود.

در دسترس بودن

مفهوم در دسترس بودن اطلاعات نیز، به این معناست که داده ها برای افراد مجاز و تایید شده به منظور ذخیره سازی، پذیرش یا محافظت در دسترس و قابل استفاده باشند.

به طور کلی با بررسی منابع مختلف، با مفاهیم مختلفی از امنیت اطلاعات رو به رو می شویم که در ادامه تعدادی از پرتکرارترین مفاهیم آن ذکر شده است.

۱) حفظ محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات. علاوه بر این موارد مشخصه های دیگری مانند اصالت، پاسخگویی، عدم انکار و قابلیت اطمینان نیز از پارامترهای دیگر هستند.

۲) محافظت از اطلاعات و سیستم های اطلاعاتی در برابر دسترسی، استفاده، افشاء، اختلال، اصلاح یا تخریب غیر مجاز به منظور تامین محرمانه بودن، یکپارچگی و در دسترس بودن.

۳) تضمین اینکه فقط کاربران مجاز و محرمانه، به اطلاعات دقیق و یکپارچه دسترسی دارند.

۴) امینت اطلاعات فرایند حفاظت از مالکیت معنوی سازمان است.

۵) امنیت اطلاعات، احساس اطمینان آگاهانه از اینکه ریسک های اطلاعاتی و کنترل ها در تعادل هستند.

آنچه از بررسی تعاریف مختلف بر می آید این است که همه ی آنها تا حدودی تعریف خود را بر اساس مدل سه گانه امنیت اطلاعات ارائه کرده اند، با این حال هنوز بحث در این خصوص که آیا مدل سه گانه برای رسیدگی به الزامات امنیت فناوری که امروزه به سرعت در حال تغییر است، کافیست یا خیر ادامه دارد و از این رو ضمن در نظر گرفتن هر سه پارامتر، محرمانگی، یکپارچگی و امنیت اطلاعات، اصول دیگری نیز مانند پاسخگویی نیز مطرح شده اند. در سال ۱۹۹۸ دان پارکر یک مدل جایگزین برای سه گانه ی کلاسیک پیشنهاد کرد و آن را شش عنصر اتمی اطلاعات نامید که عبارت است از: در اختیار داشتن، محرمانه بودن، یکپارچگی، اصالت، در دسترس بودن و مفید بودن. در سال ۲۰۰۹ میلادی نیز طرح حفاظت از نرم افزار وزارت دفاع آمریکا سه اصل امنیت سایبری را منتشر کرد که عبارت است از: حساسیت سیستم، دسترسی به نقص و قابلیت بهره برداری از نقص. نکته ی قابل توجه این است که ضمن در نظر گرفتن سرعت پیشرفت تکنولوژی هیچکدام از این مدل ها به طور گسترده پذیرفته نشده اند و این مدل ها و نظریه ها همه روزه در حال تکامل و بهبود هستند

به طور کلی و به بیانی ساده میتوان بیان کرد که امنیت اطلاعات یک حوزه ی مطالعاتی و حرفه ای چند رشته ای است که با رشد و توسعه و نیز پیاده سازی مکانیزم های امنیتی به روش های مختلف در راستای محافظت و نگهداری از اطلاعات در همه ی مکان ها رفتار می کند که در نتیجه ی آن، اطلاعات بدون هیچ تهدیدی ایجاد، پردازش، ذخیره و انتقال داده می شوند. مجموعه ای از اهداف امنیتی که در نتیجه ی تجزیه و تحلیل تهدیدها شناسایی می شوند باید به طور مرتب بازنگری شوند تا از همواره از کفایت و انطباق این اهداف با محیطی که پیوسته در حال تحول است، اطمینان حاصل شود. اهداف امنیتی شامل محرمانه بودن، یکپارچگی، در دسترس بودن، حریم خصوصی، اصالت، قابل اعتماد بودن، عدم انکار، پاسخگویی و حسابرسی است.

اهمیت سرمایه گذاری برای امنیت اطلاعات

با درک مفهوم امنیت اطلاعات، متوجه می شویم که برای حفظ سازمان ها، شرکت ها و حتی دولت ها، نیازمند سرمایه گذاری برای حفاظت از داده های محرمانه ی آنها هستیم. منظور از سرمایه گذاری اختصاص دادن پول برای چیزی است با این انتظار که در آینده منافع یا سودی از آن بدست آوریم. به طور کلی میتوان هدف از سرمایه گذاری را ایجاد بازده نامید. در خصوص موضوع مورد بررسی این بازده می تواند در قالب سرمایه، زمان و مزایا مشاهده شود. لازم به یادآوری است که مزایای حاصل از این سرمایه گذاری می توانند به صورت ملموس و ناملموس باشند و با توجه به اینکه محاسبه دارایی های ناملموس دشوار است برای محاسبه ی آنها نیاز است که معادل پولی آن را در نظر گرفت. یک سازمان در راستای استفاده از اقدامات متقابل امنیتی به منظور بهبود و

افزایش سطح امنیت اطلاعات خود، باید هزینه هایی را بپردازد و با توجه به اینکه این هزینه ها مزایای ملموس و ناملموسی را برای سازمان فراهم می کنند، به آن سرمایه گذاری در امنیت اطلاعات گفته می شود. در بسیاری از پژوهش های انجام شده، سرمایه گذاری به عنوان عاملی برای افزایش امنیت به شمار می رود و از این رو برای رسیدن به امنیت صد در صدی، هزینه ها نیز به صورت نمایی افزایش خواهند یافت.

هر سازمانی با توجه به اهمیت اطلاعات خود، نیاز به سطح مشخصی از امنیت دارد و مدیران آن سازمان باید برای دستیابی به اهداف تعیین شده بر سیاست های امنیت اطلاعات توجه ویژه ای داشته باشند و همچنین درک هزینه های پیاده سازی سیاست های امنیتی کارآمد، از اهمیت بالایی برخوردار است. پیش از این سازمان ها در مواجه با تهدیدات امنیتی، تنها با خرید نرم افزارهای امنیتی و برنامه ی های ضد ویروس سعی در ایجاد امنیت داشتند اما طی سال های اخیر بر همگان روشن شد که استفاده از گران ترین محصولات امنیتی بدون در نظر گرفتن نیازهای امنیتی سازمان و تحلیل دقیق آن کار ساز نیست. علاوه بر این این سیستم ها به طور مرتب نیازمند به روز رسانی هستند که طبیعتا این به روز رسانی برای سازمان ها هزینه خواهد داشت. آنچه امروزه برای اکثر سازمان ها و دولت ها روشن شده است، توجه به این نکته است که علی رغم هزینه هایی که برای موضوع امنیت اطلاعات ایجاد می شود، این هزینه های برای بقا امری اجتناب ناپذیر هستند.

تهدیدات پیش روی سیستم های امنیت اطلاعات را مطابق با مدل سه گانه امنیت اطلاعات، میتوان به سه گروه اصلی تقسیم کرد که عبارت است از: افشای اطلاعات محرمانه، صدمه به یکپارچگی اطلاعات و موجود نبودن اطلاعات. البته علاوه بر این سه مورد، مواردی دیگر نیز هستند که می توانند عاملی برای افشای اطلاعات محسوب شوند. تعدادی از پر تکرارترین تهدیدها عبارت است از:

۱) خطاهای انسانی
۲) ایرادات سیستمی
۳) فعالیت های خرابکارانه
۴) سیاست های امنیتی

با درنظر گرفتن مجموعه ی تهدیدات گریز ناپذیری که ذکر شد، مسئولین ارشد سازمان ها به این باور رسیده اند که راهکارهای ضروری برای آنها شامل محاسبه ارزش اطلاعات از منظر اقتصادی، بررسی خطرات و محاسبه های احتمالی و نیز تخمین هزینه سرمایه گذاری، سودمندی استفاده از سیستم های امنیت اطلاعات و بررسی تهدیدات احتمالی و راهکارهای مختلف است.

مدیران سازمان ها برای درک اهمیت سرمایه گذاری برای امنیت اطلاعات کافیست این نکته را درنظر بگیرند که همواره هزینه ی پیشگیری از یک مشکل امنیتی، کمتر از هزینه های بازسازی خرابی های متاثر از آن است؛ البته این در حالتی است که خرابی و

مشکل ایجاد شده، قابل جبران باشد. از دیگر مزایای حاصل از ایجاد امنیت اطلاعات که توجیح پذیری سرمایه گذاری بر آن را بیشتر می کند میتوان به موارد زیر اشاره کرد:

۱) کاهش احتمال غیر فعال شدن سیستم ها و برنامه ها که به این ترتیب احتمال از دست دادن فرصت ها کمتر می شود.
۲) استفاده ی موثر از منابع انسانی و غیر انسانی سازمان که در نهایت منجر به افزایش بهره وری خواهد شد.
۳) کاهش هزینه ی از دست دادن داده ها و اطلاعات توسط ویروس ها یا حفره های امنیتی (مجموعه ای از نقاط ضعف موجود در سیستم از لحاظ سخت افزاری یا نرم افزاری) که به این ترتیب داده های ارزشمند حفظ و نگه داری می شوند.
۴) ارتقای حفاظت از مالکیت معنوی

با درنظر گرفتن مواردی که ذکر شد، مشخص است که سرمایه گذاری بر امنیت اطلاعات از گام های حیاتی برای بقا و رشد هر سازمانی است که البته با توجه به میزان اهمیت اطلاعات خود، میتواند برای حفاظت از آنها اقدام کند.

ایجاد امنیت اطلاعات(ISMS)

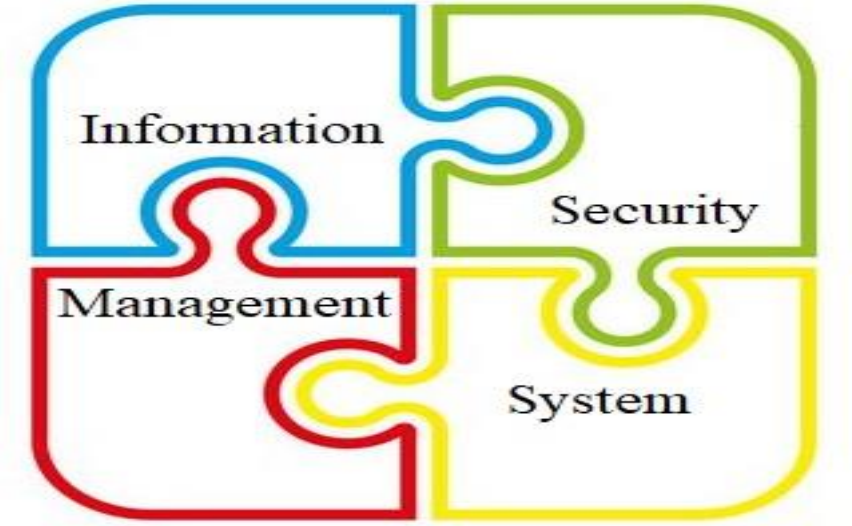
حال که اهمیت موضوع امنیت اطلاعات را درک کردیم، باید این نکته را نیز در نظر بگیریم که سرقت اطلاعات میتواند به روش ها و دلایل مختلفی صورت گیرد که میتوان آنها را در دو دسته ی کلی جای داد؛ انسانی و فناورانه. جنبه ی انسانی امنیت اطلاعات شامل مجموعه اشتباهات و سهل انگاری است که ریشه در بی دقتی کاربران دارد. عدم انتخاب گذرواژه مناسب برای کامپیوتر یا به اشتراک گذاشتن آن رمز با سایر همکاران، یادداشت کردن رمز بر روی کاغذ، باز کردن ایمیل های ناشناخته و مواردی از این دست از جمله اشتباهات کاربران است که منجر به سرقت اطلاعات آنها می شود. راهکار مناسب برای رفع مشکلات ناشی از اشتباهات انسانی، برنامه ریزی جهت آموزش های دوره ای به کارمندان سازمان است تا از این طریق میزان اشتباهات به حداقل برسد. در خصوص موضوع فناورانه نیز میتوان نرم افزارهایی مانند آنتی ویروس ها و آنتی اسپم ها را نام برد که اولین قدم برای حفظ امنیت اطلاعات هستند ولی نمی توانند امنیت صد در صد اطلاعات را تضمین کنند. با در نظر گرفتن اینکه هیچ فرمولی نمیتواند امنیت سیستم های اطلاعاتی را به طور کامل تامین کند؛ به هر حال نیازمند مجموعه ای از استانداردها و معیارها هستیم تا منابع سازمان به طور موثری از آن بهره گرفته و بهترین شیوه ی امنیتی انتخاب شود. در خصوص استفاده از استانداردهای امنیت اطلاعات، الزاما باید به مطابقت آن با استاندارد اصلی توجه کنیم چراکه بومی سازی یا متناسب سازی آن ممکن است مشکلاتی را ایجاد کند.

طی دو دهه ی اخیر با ایجاد نگرش استانداردی به موضوع امنیت اطلاعات، استانداردهای مفیدی تهیه و تدوین شده است. رویکرد ISMS را میتوان رویکرد ساختار یافته ای دانست که چگونگی پیاده سازی امنیت اطلاعات را در یک سازمان مشخص می کند.

این استاندارد در سراسر جهان توسط همه ی سازمان ها به عنوان پایه ای برای مدیریت سیاست سازمان و اجرای امنیت اطلاعات مورد استفاده قرار می گیرد.

ایجاد سیستم مدیریت امنیت اطلاعات ISMS

سیستم های جامع امنیت اطلاعات بر سه اصل اساسی وابسته هستند که شامل سیاست ها و دستورالعمل های امنیتی، تکنولوژی و محصولات امنیتی و عوامل اجرایی است. در خصوص قسمت سیاست ها و دستورالعمل ها، طرح های مرتبط با چگونگی محافظت از سیستم های اطلاعاتی و داده های آنها مورد بررسی قرار می گیرد. در اصل بعدی مجموعه ی ابزارهای مورد استفاده در بخش های مختلف امنیتی به منظور اعمال کنترل ها و نظارت ها را شامل می شود که موظف به نظارت بر شبکه یا کنترل دسترسی های ضد ویروسی هستند. در خصوص بخش اجرایی نیز شامل همه ی پرسنل اعم از مدیران و کاربران شبکه ها هستند که در راستای اجرای رویه ها و دستورالعمل ها به منظور بهبود مستمر امنیت شبکه مشغول هستند. امروزه همانطور که شرکت ها برای بخش های مختلف خود از کارشناسان و مشاوران مخصوص آن حیطه بهره می گیرند، لازم است که مشاور و پیمانکار اختصاصی برای بررسی امنیت اطلاعات و ارائه راه حل های مناسب در راستای پیشگیری از ضرر و زیان های احتمای داشته باشند.



سیستم مدیریت امنیت اطلاعات

گام های ایجاد سیستم ISMS

برای ایجاد سیستم مدیریت امنیت اطلاعات لازم است تا ۵ مرحله ی زیر پیموده شود تا سیستمی یکپارچه و هدفمند ایجاد شود.

۱) ایجاد و تعریف سیاست ها: در این گام مدیران ارشد سیاست های کلی سازمان را با توجه به قواعد و فعالیت های شرکت، در قالب سند تهیه و تدوین می کنند تا به این ترتیب تعریف مشخصی از سیاست های شرکت بدست آید.

۲) تعیین محدوده ی عملیاتی: با در نظر گرفتن این نکته که امکان دارد برخی از شرکت ها، دارای چندین شعبه و زیر مجموعه باشند، لازم است تا برای الویت اجرای استاندارد امنیت اطلاعات مشخص شود تا در ابتدا امنیت در شعبه ی اصلی که مد نظر مدیران است اجرا شود و در گام های بعدی، با توجه به الویت ها در سایر شعبات نیز انجام شود.

۳) ارزیابی تهدیدها: به منظور سهولت ایجاد امنیت و کنترل قسمت های مختلف سازمان، لازم است تا لیستی از دارایی ها ایجاد شود و با توجه به میزان اهمیتشان طبقه شود؛ به این ترتیب با داشتن لیست دارایی ها و در نظر گرفتن اهمیت آنها برای سازمان، تهدیدها قابل شناسایی خواهند بود. به این ترتیب با بررسی هر دارایی و تهدید مربوط به آن نقاط ضعف امنیتی دارایی قابل تشخیص خواهد بود. در نهایت نقاط ضعف یافته شده مستند می شوند تا در گام های بعدی برطرف شوند.

۴) برنامه ریزی برای کنترل تهدیدها: با توجه به اینکه نقاط ضعف امنیتی شناسایی شدند، امکان تصمیم گیری و برای ریزی برای رفع آنها فراهم است و مدیران می توانند با درنظر گرفتن اولویت ها برای رفع نقاط ضعف و حفره های امنیتی اقدام کنند.

۵) قابلیت اجرا: مجموعه ی اطلاعات بدست آمده که شامل دارایی ها، اولویت ها و حفره های امنیتی هستند منجر به اتخاذ تصمیمی برای رفع تهدیدها خواهد شد که در نهایت در خصوص قابلیت اجرایی بودن آن طرح یا روش باید بررسی هایی به عمل آید.

چرخه امنیت اطلاعات

مبحث امنیت اطلاعات فرآیندی دائمی است که به طور پیوسته نیازمند فعالیت و تحرک مداوم دارد که به آن چرخه ی امنیت گفته می شود. با توجه به چهار گام اصلی، به آن چرخه ی PDCA نیز گفته می شود.

چرخه ی اجرای امنیت اطلاعات

همانطور که از تصویر بالا مشخص است، گام های اصلی این چرخه عبارت است از:

۱) برنامه ریزی (Plan) : در این مرحله به تعریف چشم انداز ها و سیاست های امنیتی سازمان پرداخته می شود، مشکلات احتمالی تعیین و ارزیابی می شود، اهداف کنترل مشخص شده و در نهایت شرایط اجرایی آماده سازی می شود.

۲) انجام (Do) : در این مرحله ضمن تدوین طرح، برای رسیدن به اهداف کنترلی طرح اجرا خواهد شد.

۳) ارزیابی (Check) : استقرار روش های نظارت و پایش، بازنگری های پیوسته به منظور ارزیابی اثر بخشی طرح، پیشبرد و هدایت ممیزی های داخلی در راستای ارزیابی تحقیق.

۴) بازانجام (Act) :در این مرحله نیز به اجرای توصیه های ارائه شده برای بهبود برنامه امنیتی، انجام اقدامات اصلاحی و پیشگیرانه و در نهایت ارزیابی مجموعه اقدامات صورت پذیرفته به منظور بهبود طرح امنیتی پرداخته می شود.

نتیجه‌گیری

پیش از این عموم اطلاعات به صورت کاغذی بودند و محافظت و نگه داری از آنها به سادگی ممکن بود اما با توجه به رشد تکنولوژی و ورود اینترنت و کامپیوتر، اطلاعات سازمان ها و دولت ها عموما به صورت داده های مجازی ثبت و نگه داری می شود و ضمن داشتن مزایای بسیار زیاد، حساسیت بالایی هم برای نگه داری آنها وجود دارد. در حال حاضر تعریف واحدی از امنیت که پوشش دهنده ی نیاز همه ی سازمان ها باشد، وجود ندارد. سازمان ها باید اطلاعات خود را ارزیابی کرده و با توجه به اهمیت اطلاعات، روشی را به منظور حفاظت آنها در پیش گیرند. با توجه به اینکه تکنولوژی همه روزه در حال پیشرفت است و روش های مختلفی برای حملات سایبری وجود دارد،اجرای چرخه ی امنیت اطلاعات به عنوان بخش جدایی ناپذیر سازمان هایی تلقی می شود که اطلاعات برایشان حائز اهمیت است.

با در نظر گرفتن اهمیت موضوع، پیشنهاد می شود که مدیران ارشد شرکت ها این را نکته را به خاطر داشته باشند که ایمیل روش ارتباطی امنی برای ارسال قردادهای مهم یا گفت و گو در خصوص امور مالی شرکت نیست، از این رو بهتر است با یک پرتال خصوصی یا دیداری رو در رو امور مهم را انجام داد، همچنین مدیران سازمان ها نباید پروسه ی امنیت اطلاعات را محدود به یک دوره ی زمانی بدانند و نقطه ی شروع و پایان برای آن در نظر بگیرند، بلکه این موضوع باید پویا بوده و به طور پیوسته انجام شود. علاوه بر موارد ذکر شده آموزش مرتب و دوره ای کارمندان به منظور پیشگیری از اشتباهات احتمالی از بهترین راهکار برای به حداقل رساندن خطرات حملات سایبری به یک سازمان است چراکه کارمندان هر سازمان مانند سربازان امنیتی هستند و هرچه مهارت آنها افزایش یابد احتمال سرقت اطلاعات کمتر خواهد شد؛ از این رو لازم است مدیران به این نکته توجه ویژه ای داشته باشند.

منابع

https://fa.wikipedia.org
https://kaliboys.com/cia/
https://referenceworks.brillonline.com/
https://sites.dartmouth.edu/cybenko/
https://blog.isc2.org/isc2_blog/2008/12/cia-triad-versus-parkerian-hexad.html
https://www.connectwise.com/
www.researchgate.net
https://www.iso.org/standard/41933.html

موسوی پریسا، لگزیان محمد، ۱۳۹۷، **مروری سیستماتیک بر رویکردهای سرمایه گذاری در امنیت اطلاعات**، فصلنامه علمی-پژوهشی مطالعات مدیریت کسب و کار هوشمند- سال هفتم – شماره ۲۵.

اخوان فاطمه، رادفر رضا، ۱۳۹۹، **ارائه مدلی برای پایش بلوغ امنیت اطلاعات، فصلنامه رشد فناوری**، سال شانزدهم، شماره۶۴.

حسن زاده و همکاران، ۱۳۹۱، **ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران**، فصلنامه نظام ها و خدمات اطلاعاتی، سال اول، شماره ۲.

مختاری و همکاران، ۱۳۸۶، **امنیت و تجارت الکترونیکی**، چهارمین همایش ملی تجارت الکترونیکی.

احمدی و همکاران، ۱۳۹۱، **سیستم مدیریت امنیت اطلاعات (ISMS)**، پانزدهمین کنفرانس دانشجویی مهندسی برق ایران، کاشان.

Miryna Dimitrova**. Julius Caesar's Self-Created Image and Its Dramatic Afterlife**,Bloomsbury Academic, 14 Dec2017.

Willison Matthew. **"Were Banks Special? Contrasting Viewpoints in Mid-Nineteenth Century Britain"**. SSRN Electronic Journal. 2018.

Matthew Evenden. Allied Power : **Mobilizing Hydro-electricity during canada's second world war**. 24 June 2015.

Hugh Sebag-Montefiore. **Enigma : The Battle for the code**. p576. 1 February 2004.

Jeff Hughes, George Cybenko**. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cvbersecurity**. August 2013.

James M. Anderson**. Why do we need a new definition of information security**. **computers and security**. 17 June 2003.

Laura Madsen. **How the Lack of Data Standardization Impedes Data-Driven Healthcare**. P29. 2 January 2012.