مطالعات مدیریت و کارآفرینی

دوره ۱، شماره ۱، زمستان ۱۳۹۴

صفحات ۴۸- ۶۱

ISSN: ۲۴۷۶-۴۳۷X

www.irijournals.com

نقش استانداردها در مدیریت امنیت اطلاعات

نفیسه قدمی گلشیخ

دانشجوی کارشناسی ارشد مدیریت بازرگانی، گروه مدیریت، دانشگاه پیام نور، تهران، ایران

چکیده

نیاز روز افزون به استفاده از فناوری های نوین در عرصه ارتباطات، ضرورت استقرار سیستم مدیریت امنیت اطلاعات را بیش از پیش آشکار نموده است. در این تحقیق ضمن معرفی سیستم مدیریت امنیت اطلاعات و همچنین درک و شناخت ضرورت پرداختن به موضوع، به بررسی و تحلیل ارزیابی ریسکهای سیستم مدیریت امنیت اطلاعات پرداخته می‌شود و سپس راهکار کاهش ریسک در این زمینه ارایه می‌شود. در پایان می‌توان نتیجه گرفت که سیستم مدیریت امنیت اطلاعات، یک رویکرد نظام مند مدیریت اطلاعات حساس به منظور محافظت از آنهاست.

واژه‌های کلیدی: سیستم مدیریت امنیت اطلاعات امنیت اطلاعات،ارزیابی ریسک، دیواره آتش، تهدید.

مقدمه

یکی از زیرساختهای لازم برای بهبود امنیت فضای اطلاعات و ارتباطات، سیستم مدیریت امنیت اطلاعات (ISMS)[1]می باشد. این سیستم در واقع مجموعه ای از نیروی انسانی، مستندات سیاستها و روشهای امنیتی، مستندات شناسایی و ارزیابی مخاطرات و کنترلهای امنیت شبکه و اطلاعات (اعم از سخت افزار، نرم افزار و .....) میباشد که وظیفه ایجاد و تداوم امنیت اطلاعات و ارتباطات در سازمان را به عهده دارد. در حال حاضر بیشتر سازمانهای دولتی و غیر دولتی در کشور ما فاقد چنین سیستمی می باشند. ولی به دلیل وابسته شدن روز افزون سازمانها به تکنولوژی اطلاعات و ارتباطات، افزایش حجم اطلاعات و گسترده شدن ارتباطات و شبکه های رایانه ای، نیاز به سیستم مدیریت امنیت اطلاعات در همه سازمانها جدیّت بیشتری پیدا کرده است.در تجارت امروز، اطلاعات نقش سرمایه یک شرکت[۱] را ایفا می کند و حفاظت از اطلاعات سازمان یکی از ارکان مهم بقای آن می باشد. جهانی شدن اقتصاد منجر به ایجاد رقابت در سطح جهانی شده و بسیاری از شرکتها برای ادامه حضور خود در عرصه جهانی، ناچار به همکاری با سایر شرکتها هستند. به این ترتیب، طبقه بندی و ارزش گذاری و حفاظت از منابع اطلاعاتی سازمان (چه در مورد سیستم اطلاعاتی و چه اعضای سازمان) بسیار حیاتی و مهم به شمار می رود. سیستم مدیریت اطلاعات ابزاری است در جهت طراحی پیاده سازی و کنترل امنیت نرم افزار و سخت افزار یک سیستم اطلاعاتی[۲]

در گذشته اکثر سازمانها هزینه نسبتاً کمی را برای ایجاد امنیت منابع اطلاعاتی خود پرداخت می کردند و امنیت نیز غالباً پس از وقوع حادثه مورد توجه قرار می گرفت. بنابراین پیشنهاد طراحی برنامه امنیت فناوری اطلاعات، با بی میلی تصویب می شد و پاسخگویی نیز اغلب در سطح کارکنان فنی رده پایین صورت می گرفت. مدیران در حال درک این مطلب هستند که امنیت اطلاعات (IS) و مدیریت ریسک (RM) صرفاً مشکل فنی نیست که با بکارگیری کنترل های امنیتی مهار شود. لذا مدیریت، به خط مشی همه جانبه در برنامه ریزی امنیتی و مهیا نمودن منابع لازم برای برنامه امنیت فراگیر که کارکنان و فرایندها در آن دخیل هستند و نیز تضمین اعتقاد همه ارکان سازمان به چشم انداز امنیتی، نیازمند می باشد

تعریف موضوع (ISMS)

سیستم مدیریت امنیت اطلاعات (ISMS)در مجموع یک رویکرد نظام‌مند به مدیریت اطلاعات حساس بمنظور محافظت از آنهاست. امنیت اطلاعات چیزی فراتر از نصب یک دیواره آتش ساده یا عقد قرارداد با یک شرکت امنیتی است. در چنین رویکردی بسیار مهم است که فعالیتهای گوناگون امنیتی را با راهبردی مشترک به‌منظور تدارک یک سطح بهینه از حفاظت همراستا کنیم. نظام مدیریتی مذکور باید شامل روشهای ارزیابی، محافظت، مستندسازی و بازنگری باشد، که این مراحل در قالب یک چرخه(PDCA (PLAN-DO-CHECK-ACT تحقق پذیر است. این چرخه نقش محوری در تشریح و تحقق استاندارد ISO9001 دارد.

اهداف تحقیق

در حال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور، بویژه در حوزه دستگاههای دولتی و خصوصی در سطح نامطلوبی قرار دارد. از جمله دلایل اصلی وضعیت موجود، می‌توان به فقدان زیرساخت‌های فنی و اجرائی امنیت و عدم انجام اقدامات مؤثر در خصوص ایمن‌سازی فضای تبادل اطلاعات این دستگاه‌ها اشاره نمود.بخش قابل توجهی از وضعیت نامطلوب امنیت فضای

[1]Information Security Management System

تبادل اطلاعات کشور، بواسطه فقدان زیرساخت‌هائی از قبیل نظام ارزیابی امنیتی فضای تبادل اطلاعات، نظام صدور گواهی و زیرساختار کلید عمومی، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، نظام مقابله با جرائم فضای تبادل اطلاعات و سایر زیرساخت‌های امنیت فضای تبادل اطلاعات در کشور می‌باشد. از سوی دیگروجود زیرساخت‌های فوق، قطعا تأثیر بسزائی در ایمن‌سازی فضای تبادل اطلاعات دستگاههای دولتی خواهد داشت.
در این تحقیق سعی شده ضمن معرفی سیستم مدیریت امنیت اطلاعات، به اهدافاجرای آن نیز اشاره شود، هدف از اجرای سیستم مدیریت امنیت اطلاعات به زبان ساده فراهم کردن امکان استفاده مناسب و سودمند از زیر ساخت و اجزای مختلف امنیتی سازمان می‌باشد و یا شناسایی، مدیریت و محافظت از سرمایه های اطلاعاتی سازمان ، حفظ محرمانگی، تمامیت و دسترس پذیری سرمایه های اطلاعاتی سازمان، بکارگیری روشی مناسب برای مقابله با حوادث امنیت اطلاعات، افزایش رضایتمندی کاربران خدمات فناوری اطلاعات، کاهش سطح حوادث امنیت اطلاعات و یا به حداقل رساندن احتمال وقوع تهدیداتی که امروزه سازمانها بواسطه از دست دادن اطلاعات خود با آنها رودرو می باشند.

امنیت اطلاعات:

امنیت اطلاعات عبارت است از حفاظت اطلاعات و به حداقل رساندن دسترسی غیر مجاز به آنها [۳]همچنین علم مطالعه روشهای حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر تغییرات غیر مجاز است [۴]امنیت اطلاعات حفاظت از محرمانگی ، تمامیت و دسترس پذیری اطلاعات است. علاوه بر این ها سایر ویژگی ها از قبیل اصالت، قابلیت جوابگویی، اعتبار، انکار ناپذیری و قابلیت اطمینان اطلاعات نیز می توانند مشمول این حفاظت باشند.

مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف ، امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد. [۴]

سیستم مدیریت امنیت اطلاعات (ISMS)

مفهوم سیستم مدیریت اطلاعات عبارت است از :بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه ی رویکرد مخاطرات کسب و کار قرار داشته و هدف آن پایه گذاری ، پیاده سازی ، بهره برداری ، نظارت ، بازبینی ، نگهداری و بهبود امنیت اطلاعات است . سیستم مدیریت امنیت اطلاعات در مجموع یک رویکرد نظام مند به مدیریت اطلاعات حساس به منظور محافظت از آن هاست.امنیت اطلاعات چیزی فراتر از نصب یک دیواره ی آتش ساده یا عقد قرارداد با یک شرکت امنیتی است. در چنین رویکردی بسیار مهم است که فعالیت های گوناگون امنیتی را با راهبردی مشترک به منظور تدارک یک سطح بهینه از حفاظت همراستا کنیم. [۳]

مزایا و معایب استقرارISMS

هر چند بکارگیری نظام مدیریت امنیت اطلاعات و اخذ گواهینامهISO 27001به تنهایی نشان دهنده برقراری امنیت کامل در یک سازمان نیست، اما استقرار این سیستم مزایایی دارد که مهمترین آنها چنین است:

- **در سطح سازمانی**: استقرار نظام یادشده تضمینی برای التزام به اثربخشی تلاشهای امنیتی در همه سطوح و نمایشی از تلاشهای مدیران و کارکنان سازمان در این زمینه است .

- **در سطح قانونی**: اخذ گواهینامه به اولیای امور ثابت می‌کند که سازمان تمامی قوانین و قواعد اجرایی در این زمینه را رعایت می‌کند
- **در سطح اجرایی**: استقرار این نظام باعث اطلاع دقیقتر از سیستمهای اطلاعاتی و ضعف و قوت آنها می‌شود . علاوه‌بر این چنین نظامی استفاده مطمئن‌تر از سخت‌افزار و نرم‌افزار را تضمین می‌کند.
- **در سطح تجاری**: تلاشهای مؤثر سازمان به منظور حفاظت از اطلاعات در شرکا و مشتریان اطمینان خاطر بیشتری را فراهم می‌آورد.
- **در سطح مالی**: این اقدام باعث کاهش هزینه‌های مرتبط با مسائل امنیتی و کاهش احتمالی حق بیمه‌های مرتبط می‌شود.
- **در سطح پرسنلی** : افزایش آگاهی ایشان از نتایج برقراری امنیت اطلاعات و مسئولیتهای آنها در مقابل سازمان از مزایای بکارگیری چنین نظامی است[۵] امّا قطعاً هر سیستم در کنار مزایای که برای سازمانها دارد معایب و مشکلاتی نیز به دنبال دارد که میتوان به معایب زیر نام برد :
- بی اطلاعی افراد یک سازمان از خود موضوع ISMS
- درک اشتباه پرسنل از موضوع ISMS
- هزبنه بالای استقرار و پیاده سازی ISMS

مطالعات موضوعی (تحول در فناوری اطلاعات)

فناوری اطلاعات به معنای عام آن به عنوان مجموعه ای از ابزارها و سیستم ها جهت گردآوری، سازماندهی، ذخیره و نشر اطلاعات اعم از صوت، تصویر، متن یا عدد می باشد. سابقه این علم به ۳۵۰۰ سال قبل از میلاد مسیح بر می گردد. یعنی از زمان رم باستان که نامه ها را روی لوح گلی و به صورت تصویر می نوشتند و نامه بر در طی یک هفته تنها مقصد کوتاهی را طی می نمود تا هم اکنون که با استفاده از ابزارهای پیشرفته رایانه ای و سیستم های مجهز مخابراتی در کوتاه ترین زمان ممکن اطلاعات دلخواه در اختیار قرار می گیرد. فناوری نوین اطلاعات یعنی فناوری اطلاعات مبتنی بر الکترونیک را می توان در چند سال پیش از دهه ۱۹۴۰ سراغ گرفت. در طی جنگ جهانی دوم و پس از آن بود که پیشرفت های عمده در فناوری الکترونیک رخ داد. تولید اولین کامپیوتر قابل برنامه ریزی و ترانزیستور که منشاء میکروالکترونیک و هسته حقیقی انقلاب فناوری اطلاعات در قرن بیستم بود.

به عقیده «کاستلز » تنها در دهه ۱۹۷۰ بود که فناوری های جدید اطلاعاتی در سطحی گسترده انتشار یافتند و توسعه توأمان خود را شتاب بخشیدند و در پارادایمی جدید گردهم آمدند. کاستلز می گوید: بی گمان می توانیم بدون اغراق بگوییم که انقلاب فناوری اطلاعات به عنوان یک انقلاب در دهه ۱۹۷۰ متولد شد. به ویژه اگر پیدایش و رواج مهندسی ژنتیک به طور موازی و تقریباً در همان زمان و مکان را به آن اضافه کنیم.

جایگاه فناوری اطلاعات در تکامل و پیشرفت کشورها:

بشرسالیان متمادی بدون داشتن وسیلهٔ محاسباتی زندگی می‌کرد و انگشتان دستانش، تنها وسیله محاسباتی او را تشکیل می‌داد. بالا بودن قدرت تفکر انسان در مقایسه با حیوان، سبب گردیده که هیچگاه به امکانات محدود خود اکتفا نکند و همواره درصدد یافتن راه‌هایی برای توسعه و تکامل این امکانات باشد. با توسعه و پیشرفت فناوری‌های نوین در کشورهای مختلف، به خصوص در کشورهای پیشرفته و به دنبال آن انفجار اطلاعات در تمام بخش‌های مختلف جوامع، پاسخگویی با شیوه‌های سنتی دیگر جوابگوی انسان‌ها در زمینه انتقال سریع اطلاعات نبوده و لذا نیاز به شیوه‌های جدیدتر به شدت احساس می‌شد. با ورود کامپیوتر (رایانه)، دگرگونی عظیمی در امر انتقال و بازیابی اطلاعات به وقوع پیوست. در واقع می‌توان به کارگیری رایانه را سومین تحول عظیم بعد از پیدایش خط - کتابت و اختراع چاپ دانست. در چند سال اخیر، رشد شتابان فناوری اطلاعات و به

دنبال آن توسعه شبکه‌های ارتباطی، افق‌های تازه‌ای در پیشبرد تحقیقات علمی، صنعتی، پزشکی و کشاورزی پدید آورده است. هر چند که شکل نهایی نهادهایی که از این دگرگونی بر خواهند خواست، هنوز نامعلوم است.قدرت سحرآمیز شبکه‌های اطلاعاتی و توزیع آنها در گستره این کره خاکی، دگرگونی‌های بنیادی را در ساختار نظام تحقیقات، توسعه و آموزش ایجاد کرد. این امر در کشورهای پیشرفته صنعتی که از این شبکه‌ها استفاده می‌کنند، به خوبی ملموس است. بر این اساس، می‌توان اظهار داشت که در آستانه قرن دانش و اطلاعات، هر نوع برنامه‌ریزی و تصمیم‌گیری و در مجموع هر نوع فعالیت حیاتی معقول، بدون کاربرد اطلاعات (به روز) و سازماندهی اطلاعاتی بر مبنای فناوری‌های جدید در امر اطلاع‌رسانی، امری به دور از واقعیت‌های جامعه جهانی یا به عبارت دیگر "دهکده جهانی " خواهد بود. در عصر فنون جدید تبادل اطلاعات، هر نوع فعالیت ارتباطی به منزله یک سرمایه ملی و در حکم پشتوانه‌ایی برای نیل به اهداف برنامه‌های توسعه و نهایتاً استقلال و خودکفایی کشورها محسوب می‌شود، بنابراین باید پذیرفت که بزرگراه‌های اطلاعاتی زمینه‌ساز بستری مناسب برای توسعه کشورها هستند و جوامعی که از این امکانات محرومند، عملاً قدرت مانور تجاری و علمی خود را تا حد قابل توجهی محدود می‌بینند.

بنابراین در جهان کنونی، هر حادثه اقتصادی –اجتماعی و هر تحول علمی–فرهنگی بر زندگی همگان موثر است و در دنیایی که ارتباط تنگاتنگ و سرنوشت مشترک اعضا روز به روز به یکدیگر نزدیک می‌شود، دسترسی شبکه‌های اطلاعاتی درهمه زمینه‌ها ضروری است. هیچکس از اطلاعات بی‌نیاز نیست وارتباطات گسترده اعضا جامعه بشری چنان است که بدون اطلاعات نمی‌توان در این جهان گام برداشت. گسترش شبکه‌های اطلاع‌رسانی در حقیقت گامی است برای پیوستن به ارتباطات جهانی و پیش از آن گامی است بلند در راه دستیابی به توسعه.

امنیت اطلاعات

با رشد سریع و استفاده گسترده از پردازش الکترونیکی داده‌ها و کسب و کار الکترونیک از طریق اینترنت، همراه با ظهور بسیاری از خرابکاریهای بین‌المللی، نیاز به روش‌های بهتر حفاظت از رایانه‌ها و اطلاعات آنها ملموس گردید. رشته‌های دانشگاهی از قبیل امنیت کامپیوتری، امنیت اطلاعات و اطلاعات مطمئن همراه با سازمان‌های متعدد حرفه ای پدید آمدند. هدف مشترک این فعالیت‌ها و سازمانها حصول اطمینان از امنیت و قابلیت اطمینان از سیستم‌های اطلاعاتی است.

ایجاد امنیت از نظر فیزیکی: امنیت تجهیزات و امکانات مادی در ایجاد یک کانال امن برای تبادل اطلاعات بسیار موثر است. انتخاب لایه کانال ارتباطی امن، انتخاب توپولوژی مناسب برای شبکه، امنیت فیزیکی، محل‌های امن برای تجهیزات، منابع تغذیه شبکه و حفاظت تجهیزات در مقابل عوامل محیطی مواردی است که در امنیت یک سیستم اطلاعاتی بسیار مؤثرند[۱۰].

سطح بندی صحیح اطلاعات با توجه به ارزش اطلاعات و امکان دسترسی به موقع به اطلاعات برای کاربران هر سطح.آموزش کاربران اطلاعاتی سازمان در چگونگی استفاده از تجهیزات سخت افزاری و نرم افزاری سازمان و نیز آموزش راههایی که نفوذ گران برای کسب اطلاعات سازمان استفاده می کنند[۱۱] و هشدار به کارمندان در حفاظت از اطلاعات سازمان. تغیر مداوم در الگوریتم های استفاده شده برای رمز گذاری در کاهش احتمال کشف رمز توسط نفوذ گران و کلاهبرداران اطلاعاتی بسیار موثر است. استفاده از انواع امکانات امنیتی (البته با توجه نتایج ارزیابی سطح امنیتی مورد نیاز) از جمله استفاده از پراکسی که نقش ایجاد دیواره آتش، فیلتر کردن، ثبت کردو تصدیق هویت را در شبکه بر عهده دارد; نیز استفاده از نرم افزارهای مقابله با ویروسها. استفاده از تست نفوذ پذیری: رویه ای است که در آن میزان امنیت اطلاعات سازمان شما مورد ارزیابی قرار می گیرد. یک تیم مشخص با استفاده از تکنیک های هک یک حمله واقعی را شبیه سازی می کنند تا به این وسیله سطح امنیت یک شبکه یا سیستم را مشخص کنند. تست نفوذپذیری به یک سازمان کمک می کند که ضعف های شبکه و ساختارهای اطلاعاتی خود را بهتر بشناسد و در صدد اصلاح آنها بر آید. این امر به یک سازمان کمک می کند تا در زمینه تشخیص، توانایی پاسخ و تصمیم مناسب در زمان خود، بر روی امنیت نیروها و شبکه خود یک ارزیابی واقعی داشته باشد. نتیجه این تست یک گزارش می باشد که برای اجرایی شدن و بازرسی های تکنیکی مورد استفاده قرار می گیرد[۱۲]. و هشدار به کارمندان در حفاظت از

اطلاعات سازمان. از سوی دیگر ایجاد حس تعهد نسبت به شغل و سازمان در کارمندان از طریق اعمال مدیریت صحیح .رمز گذاری اطلاعات و استفاده از امضا دیجیتال[۱] در ارسال اطلاعات موجب افزایش ضریب اطمینان در تجارت الکترونیک خواهد شد.

با استفاده از یک سیستم پشتیبان گیری اطلاعات، از احتمال از بین رفتن اطلاعات جلوگیری می گردد.

بطور مرتب تجهیزات و سیستم اطلاعاتی سازمان را بازرسی نمایید و هر گونه مشکل را گزارش نموده و سعی در رفع آن نمایید. همچنین بطور مرتب سیستم اطلاعاتی و امنیتی سازمان را به روز رسانی کنید و آموزش کارمندان را به صورت مستمر ادامه دهید[۱۳].

بحث امنیت اطلاعات در سال‌های اخیر به میزان قابل توجهی رشد کرده است و تکامل یافته است. راههای بسیاری برای ورود به این حوزه کاری به عنوان یک حرفه وجود دارد. موضوعات تخصصی گوناگونی وجود دارد از جمله: تأمین امنیت شبکه ها و زیرساخت ها، تامین امنیت برنامه‌های کاربردی و پایگاه داده ها، تست امنیت، حسابرسی و بررسی سیستم‌های اطلاعاتی،برنامه ریزی تداوم تجارت و بررسی جرائم الکترونیکی، و غیره.

از زمانی که مبحث امنیت سرمایه‌های فیزیکی مطرح گردید، موضوع امنیت اطلاعات به وجود آمد (زیرا خود اطلاعات، نوعی سرمایه به حساب می‌آید).این دو موضوع را می‌توان پشتوانه یکدیگر دانست که در کنار هم، استخوان بندی کنترل امنیت شرکت‌ها را به وجود می‌آورند[۱۴].

با توجه به تغییرات به وجود آمده در فرایندها وکسب وکارهای سازمانی، شرکت‌ها برای بقاء و حفظ موقعیت رقابتی خود، نیازمند استفاده از فناوری اطلاعات در تبادل اطلاعات، تبادلات مالی و نظارت[۲] هستند[۱۵].

سازمان‌های کوچک و بزرگ، بیش از پیش، این فناوری را برای کنترل و تسریع در کسب و کارهای خود مورد استفاده قرار داده‌اند. از آنجا که مدیریت سازمان‌ها ، طیف وسیعی از فرایندهای سازمان‌ها از جمله تبادلات مالی، فیزیکی و اطلاعاتی از تأمین‌کنندگان تا مشتریان را در بر می‌گیرد، نیاز به یک سیستم دقیق کنترل صحت و دقت اطلاعات و همچنین کنترل تبادلات فیزیکی وجود دارد. در این راستا، مدیریت امنیت اطلاعات برای ایجاد امنیت در پیدایش و تبادل اطلاعات و همچنین تبادلات فیزیکی، بر اساس یک سیستم مدیریتی مبتنی بر استانداردهایی از قبیلBS7799 ،ISO/IEC 27001 و گزارش فنی ISO/IEC TR 13335، ـ که از برجسته‌ترین استانداردها و راهنماهای فنی در این زمینه محسوب می‌گردند، عمل می‌کند[۱۶].

سیستم مدیریت امنیت اطلاعات

براساس نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات ،تأمین امنیت در سازمان‌ها ، به یکباره مقدور نمی‌باشد و لازم است به صورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی ،پیاده‌سازی ، ارزیابی واصلاح انجام گیرد. برای این منظور ،هر سازمان بر اساس یک روش شناسی مشخص و برنامه‌ریزی شده باید به کنترل و نظارت بر پیدایش، جابجایی و تبادلات اطلاعات در درون مجموعه خود بپردازد [۱۷].مدیریت امنیت اطلاعات ، از طریق استفاده از استانداردها و سیستم‌های مدیریت امنیت اطلاعات در سازمان‌ها صورت می‌گیرد.موسسه استاندارد انگلستان، مجموعه‌ای از استانداردهای مدیریتی (BS 13335) را برای ایمن‌سازی فضای تبادل اطلاعات در سازمان‌ها ارائه کرده است.همچنین استاندارد مدیریتی ISO/IEC TR7799 مؤسسه بین المللی استاندارد وگزارش فنی ISO/IEC17799 این مؤسسه، از برجسته ترین استانداردها وراهنماهای فنی در این زمینه محسوب هستند[۱۷].

1. Monitoring

خوشبختانه قریب به یک دهه از ارائه یک ساختار امنیت اطلاعات، توسط مؤسسه استاندارد انگلیس می‌گذرد. در این مدت استاندارد فوق‌الذکر(BS7799) مورد بازنگری قرار گرفته و در سال ۲۰۰۰ میلادی نیز مؤسسه بین‌المللی ISO اولین بخش آن را در قالب استاندارد ISO17799 ارائه کرده است. در سال ۲۰۰۲ نیز یک بازنگری در بخش دوم استانداردBS7799 به‌منظور ایجاد سازگاری با سایر استانداردهای مدیریتی نظیر ISO9001-2000 و ISO14001-1996 صورت پذیرفت. در حال حاضر نیز بازنگری به منظور انجام بهبود در بخشهای مربوط به پرسنل و خدمات تامین‌کنندگان و راحتی کاربری و مفاهیم مرتبط با امنیت برنامه‌های موبایل بر روی این استاندارد در حال انجام است که پیش‌بینی می‌شود در سال جاری میلادی ارائه شود[۵].

هدف ازسیستم مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه‌های آن (نرم‌افزاری، سخت‌افزاری، اطلاعاتی و ارتباطی، و نیروی انسانی) در مقابل هرگونه تهدید (اعم از دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سیستم، و خطرات ایجاد شده از سوی کاربران) استو برای رسیدن به این هدف، نیاز به یک برنامه منسجم است[۱۸].

فرایند سیستم مدیریت امنیت اطلاعات را نمی‌توان یک باره در یک نظام مدیریتی پیاده کرد بلکه نیازمند یک فرایند مداوم ، شامل این مراحل است :۱) برنامه‌ریزی- برپایی شرایط اولیه سیستم، ۲) اجرا- پیاده‌سازی و اجرای سیستم،۳) ارزیابی و کنترل- فعالیت‌های نظارتی و بررسی فعالیت‌های انجام شده و۴) بهبود و اصلاح- فعالیت‌های نگهداری و بهبود مستمر [۷،۱۹].

متدولوژی ارزیابی ریسک (RAM)[3]

اهداف (Objectives)

هدف از این سند، تعیین رویکرد سازمان برای شناسایی، تحلیل و ارزیابی ریسک های محدوده سیستم مدیریت امنیت اطلاعاتاست که به موجب آن امکان تعیین استراتژی و راه کار های مناسب جهت برطرف سازی ریسک ها و بهبود مستمر سیستم مدیریت امنیت اطلاعات میسر خواهد شد.

تعاریف(Terms and definitions)

دارایی : هر آنچه که برای سازمان دارای ارزش است.

محرمانگی : نشان دهنده اهمیت ویژگی محرمانگی برای اطلاعات، که مشخص می کند این اطلاعات نباید در دسترس افراد یا فرآیندهای غیرمجاز قرارگرفته یا فاش شود.

صحت کارکرد : نشان دهنده اهمیت ویژگی حفظ صحت و تمامیت دارایی‌ها.

دسترس پذیری : نشان دهنده اهمیت ویژگی در دسترس و قابل استفاده بودن یک دارایی، به محض نیاز به آن است.

تهدید : دلیل بالقوه یک حادثه ناخواسته ، که ممکن است نتیجه آن خسارت به سیستم یا سازمان باشد.

[3] Risk Assessment Methodology

آسیب پذیری : وجود ضعف در یک دارایی یا مجموعه ای از دارایی ها که می تواند بوسیله یک یا چند تهدید مورد بهره برداری قرار گیرد.

شدت اثر:تغییر مغایر با سطح اهداف تجاری نایل شده.

ریسک : عامل بالقوه ای است که یک تهدید معین، آسیب پذیری های یک دارایی یا گروهی از دارایی ها را حادث می‌شود که عاملی برای صدمه زدن به دارائی های سازمان می‌باشد.

پذیرش ریسک: پذیرفتن ضرر و زیان حاصله از یک ریسک.

اجتناب از ریسک: تصمیم صرفنظر کردن از ریسک.

انتقال ریسک : سهیم شدن در ضرر و زیان حاصله از یک ریسک با طرف دیگری.

کاهش ریسک : اقدامات بکارگرفته شده برای کاهش احتمال وقوع تهدید و یا کاهش شدت اثر یا هر دو آنها برای کاهش ریسک مربوطه[۵].

شناسایی ریسک (Risk Identification)

شناسایی دارایی ها (Asset Identification)

کلیه دارایی های اطلاعاتی محدوده ISMS با توجه به دسته بندی زیر شناسایی می شوند:

دارایی های فیزیکی، نرم افزارها، سرویس ها، منابع انسانی، مدارک و مستندات و اطلاعات

مکانیزم بروز رسانی دارایی های سازمان در خلال پیاده سازی پروژه :

چنانچه خروجی دستورالعمل مدیریت کنترل تغییرات منجر به اضافه شدن دارایی جدیدی به سازمان شود .

چنانچه سازمان بنا به ضرورت های کسب و کار و یا ایجاد یک فرصت تجاری مبادرت به استفاده از یک دارایی اطلاعاتی جدید نماید[۵].

شناسایی تهدید ها (Threat Identification)

در این مرحله، تهدیدهای بالقوه ای که روی هر یک از دارایی های اطلاعاتی وجود دارد، شناسایی می شوند.

یک تهدید، پتانسیل آسیب رسانی به دارایی های اطلاعاتی محدوده سیستم را دارد. اگر تهدیدی بوقوع بپیوندد، می توان تصورکرد که موجب بوجود آمدن حوادث ناخواسته شده و بنابراین تأثیرات مضری را سبب خواهد شد. بدین جهت، در این مرحله کلیه تهدیدهایی که روی هر یک از دارایی های اطلاعاتی وجود دارد، می بایستی شناسایی شوند.

شناسایی آسیب پذیری ها(Vulnerability Identification)

پس از شناسایی تهدیدهای بالقوه در بند ۳، آسیب پذیری های بالقوه ای که در مورد هر یک از دارایی های اطلاعاتی می تواند وجود داشته باشد، شناسایی می شوند. نکته مهم در مورد نحوه شناسایی این آسیب پذیری ها، رعایت ارتباط بین

تهدید/تهدیدهای شناسایی شده با آسیب پذیری/ آسیب پذیری های شناسایی شده است. بدین مفهوم که آسیب پـذیری هـایی شناسایی شده بایستی به تهدیدهایی مربوط باشند که توسط آن تهدیدها می توانند مورد بهره برداری قرار گیرند.

تحلیل ریسک ها(Risks Analysis)

منظور از تحلیل ریسک تعیین ارزش دارایی اطلاعاتی و با توجه به آن تعیـین شـدت اثـر و احتمـال وقـوع تهدیـد و در نهایـت محاسبه ارزش ریسک می باشد.

برای محاسبه ارزش ریسک (سطح ریسک) می بایست ۲ پارامتر احتمال وقوع و شدت اثر ریسک محاسبه و از حاصـل ضـرب (تلاقی) این ۲ پارامتر بر اساس ماتریس ۱ ، ارزش ریسک محاسبه می گردد .

محاسبه شدت اثر (پیامد)ریسک (Impact Estimation)

پیامد ریسک

عبارت است از خسارت ناشی از بوقوع پیوستن تهدید برروی دارایی اطلاعاتی. از اینرو برای محاسبه پیامـد ریسـک ابتـدا مـی بایست ارزش دارایی اطلاعاتی محاسبه گردد.

تعیین ارزش دارایی اطلاعاتی(Asset valuation)

در این بخش میزان ارزش دارایی های اطلاعاتی بر اساس از دست دادن ویژگی های محرمانگی، صحت و دردسترس پـذیری در ۳ سطح زیاد **(H)** متوسط**(M)** و کم**(L)** محاسبه می گردد.

- زمانی "ارزش دارایی اطلاعاتی " زیاد خواهد بود که بابت از دست رفـتن هـر کـدام از معیارهـای محرمانـه بودن، صحت کارکردو در دسترس بودن خسارت سنگینی به سازمان وارد گردد.

با رخ دادن هر یک از موارد زیر ، خسارت سنگینی به سازمان وارد خواهد آمد. حسب هر یک از موارد ذیل ارزش دارایـی زیـاد (High) تلقی خواهد شد:

۱. به خطر افتادن حسن شهرت و اعتبار سازمان.
۲. نقض الزامات و تعهدات قانونی، مقرراتی و حقوقی.
۳. توقف فرآیندهای اصلی کسب و کار و یا ایجاد وقفه هـایی کـه بیشـتر از آسـتانه تحمـل سـازمان باشد.
۴. هزینه مادی ناشی از حادثه بیش از ۵۰۰ میلیون ریال باشد.

- زمانی "حساسیت امنیتی دارایی اطلاعاتی " متوسط خواهد بـود کـه از بابـت از دسـت رفـتن هـر کـدام از معیارهای محرمانگی، صحت کارکرد و دسترس پذیری یکی از موارد ذیل رخ دهد :
  ۱. فرآیندهای اصلی کسب و کار با اختلال و افت کارایی همراه شوند.
  ۲. هزینه ای بین ۱۵۰ تا ۵۰۰ میلیون ریال به سازمان تحمیل گردد.
  ۳. باعث توقف فرآیندهای پشتیبان و مدیریتی سازمان شود.

- هر زمان که از بابت از دست رفتن معیارهای محرمانگی، صحت کارکرد و دردسترس پذیری اطلاعات هیچ از مصادیق ارزش زیاد و متوسط وجود نداشته باشد، ارزش آن دارایی اطلاعاتی کم (Low) خواهد بود.

محاسبه پیامد ریسک (Consequence Estimation)

ارزش پیامد بر این مبنا شناسایی می شود که تهدید شناسایی شده بر کدام یک از معیارهای امنیتی آن دارایی تاثیر می گذارد (محرمانگی، یکپارچگی و یا دسترس پذیری) ، نتیجتاً "پیامد" ارزش همان معیار را خواهد گرفت (در صورتی که آن تهدید بیش از یک معیار امنیتی را تحت تاثیر قرار دهد، پی آمد برابر با معیار بزرگتر خواهد بود).

محاسبه شدت اثر (Impact estimation)

میزان شدت اثر به صورت پیش فرض برابر با "پیامد" می باشد، فقط در مواردی این میزان کمتر از "پیامد" خواهد گردید که دارایی اطلاعاتی دارای طرح دسترس پذیری / تداوم کسب و کار و یا فرایند مدیریت حوادث اطلاعات (Incident Management)و یا هر اقدام و طرحی که بتواند خسارت و اثر ناشی از به وقوع پیوستن تهدید را کمتر از خسارت ناشی از تخمین ارزش دارایی به سازمان تحمیل نماید.

نکته: کیفیت عواملی که می توانند شدت اثر ریسک را کاهش دهند باید به شکل مؤثری تحلیل شود و نتیجه این تحلیل در ۳ وضعیت ضعیف، متوسط و خوب مقدار دهی شود. چنانچه وضعیت خوب تحلیل شود می تواند شدت اثر را ۲ سطح از پیامد ریسک کمتر نماید. بهطور مثال چنانچه پیامد ریسک High باشد و وضعیت طرح های مربوطه **خوب** (Good) ارزیابی گردد شدت اثر ریسک Low خواهد شد.

چنانچه وضعیت طرح ها متوسط باشد ۱ سطح و چنانچه ضعیف باشد تأثیری برروی پیامد نخواهد داشت و پیامد و شدت اثر یکسان خواهد بود.

ارزشیابی ریسک (Risk Evaluation)

هدف از این فعالیت در فرآیند مدیریت ریسک، قاعده مند کردن اتخاذ تصمیمات برای پذیرش و یا برطرف سازی ریسک و همچنین اولویت گذاری ریسک ها برای برطرف سازی می باشد.

ریسکها در ۲ حالت نیازی به برطرف سازی پیدا نمی کنند این ۲ حالت عبارتند از

اولاً ریسک هایی که در بازه پذیرش ریسک قرار داشته باشند

ثانیاً ریسک هایی که خارج از بازه پذیرش بوده ولیکن امکان تأمین منابع مورد نیاز برای برطرف سازی فراهم نبوده و یا برطرف شدن ریسک به ازای اختصاص منابع بسیار زیاد از توجیه اقتصادی لازم برخوردار نباشد.

برای این منظور می بایست حسب ملاحظات ذیل اولویت ریسک ها تعیین شوند:

عوامل شناسایی	اولویت	مهلت انجام /منابع
ارزش شدت اثر ریسک High باشد ریسک مرتبط با دارایی هایی که مؤثر بر	۱	فوری/ تأمین منابع از محل بودجه مصوب و یا از خارج از بودجه مصوب

فرآیندهای اصلی شرکت باشد موضوع ریسک مرتبط با الزامات بالادستی باشد		
ارزش شدت اثر ریسک Medium باشد ریسک مرتبط با دارایی هایی که مؤثر بر فرآیندهای پشتیبان شرکت باشد	۲	در طول فاز پیاده سازی/ تأمین منابع از محل بودجه مصوب
تمامی ریسک هایی که نیاز به برطرف سازی داشته و از شرایط اولویت های ۱و۲ تبعیت نمی کنند.	۳	در طول فاز پیاده سازی / در صورت وجود اعتبار از محل بودجه مصوب و در صورت عدم وجود اعتبار از محل اولین بودجه ریزی سازمان

برطرف سازی ریسک(Risk Treatment)

تدوین بازه پذیرش ریسک توسط مدیریت

با توجه به تعیین شدت ریسکهای موجود در سازمان، مدیریت و یا نماینده آن باید با توجه به زمان و هزینه (منابع مالی و منابع انسانی) لازم جهت بر طرف سازی ریسک ها، بازه پذیریش ریسک سازمان را مشخص نماید

تدوین استراتژی های مقابله با ریسک

برای هر کدام از ریسک هایی که خارج از بازه پذیرش سازمان قرار می گیرند باید استراتژی برخورد تعیین شود. پنج نوع استراتژی برخورد عبارتند از:

اجتناب از ریسک(Avoidance)

اعمال تغییر در یک یا چند عدد از مؤلفه های ایجاد کننده ریسک به شکلی که ریسک مورد نظر دیگر وجود نداشته باشد ، در حقیقت با اعمال این استراتژی ، احتمال وقوع این ریسک به صفر رسیده و لذا ریسک از دامنه مخاطرات سازمان حذف می گردد .

اشتراک ریسک به سایر طرف ها (Sharing) (شرکت های بیمه، تأمین کنندگان و ...):

منظور ازاشتراک ریسک در حقیقت انتقال شدت اثر ریسک (قسمتی از یا تمام خسارت وارده به سازمان در صورت وقوع آن ریسک) به موجودیتی دیگر مانند شرکت حقوقی یا فردی حقیقی است. در حقیقت با انتقال ریسک تمام و یا بخشی از پیامد ریسک به طرف های بیرونی منتقل می شود . اتخاذ این استراتژی با کاهش شدت اثر ریسک می تواند به کاهش سطح ریسک منتهی شود.

تعدیل ریسک (Modification)

برای آن دسته از ریسک هایی که امکان اتخاذ استراتژی های اجتناب از ریسک و اشتراک ریسک برای آنها وجود نداشته باشد ، استراتژی کاهش ریسک اتخاذ می گردد. بطوریکه پس از اعمال کنترل های امنیتی (خط مشی ها، رویه ها و دستورالعمل های امنیتی) ارزش ریسک از محدوده خارج از بازه پذیرش ریسک به محدوده بازه پذیرش ریسک انتقال داده می شود.

توضیح : برای کاهش یک ریسک، می بایست حداقل یکی از معیارهای "احتمال وقوع تهدید" یا "شدت اثر" کاهش یابد.

حفظ و نگهداشت (Retention)

استراتژی حفظ و نگهداشت ریسک در یکی از سه حالت زیر اتفاق خواهد افتاد:

ریسک هایی که از ابتدا در بازه پذیرش بوده اند

ریسک هایی که در ابتدا خارج از بازه پذیرش بوده اند ، ولیکن با اقدامات و استراتژی های مناسب به اندازه ای کاهش یافته اند که در بازه پذیرش قرار می گیرند. در این مورد برای ریسک های باقی مانده(Residual Risks) استراتژی Risk retention اتخاذ می گردد.

ریسک هایی که در ابتدا خارج از بازه پذیرش بوده اند ، ولیکن امکان کاهش آن ریسک در سازمان وجود نداشته باشد، لذا با صلاحدید و نظر مدیریت و به واسطه اینکه کاهش آن ها امکان پذیر نیست ، استثنائاً این قبیل ریسک ها پذیرفته می شوند.

پیش بینی مقدار ریسک پیش از پیاده سازی

بر اساس آن دسته از کنترل هایی که جهت کاهش ریسک انتخاب شده اند و شمارش تعداد آسیب پذیری هایی که توسط این کنترل ها برطرف می شوند ، می بایست احتمال وقوع هر ریسک پیش بینی شود ، همچنین بر اساس آن دسته از کنترل ها و اقداماتی که از جنس BCP[4] هستند و یا استراتژی انتقال ریسک را به دنبال دارند باید مقدار شدت اثر ریسک پیش بینی شود.

بازبینی و پایش ریسک ها (Risk Review) : تمامی اقدامات تعریف شده جهت برطرف سازی ریسک مورد بررسی و بازبینی قرار می گیرند و چنانچه اقدام تعریف شده در عمل با کیفیت مطلوبی پیاده سازی شده باشد، ریسک مربوطه در این حوزه موفقیت آمیز کاهش یافته است. [۵].

نتیجه گیری

بدیهی توجه نکردن به تأمین امنیت فضای تبادل اطلاعات و برخورد نادرست با این مقوله ، مانع از گسترش فضای یادشده در میان جامعه و جلب اعتماد مدیران در بکارگیری روشهای نوین نظارتی می شود . لذا درک درست نقش امنیت اطلاعات در ارائه خدماتی صحیح ، ایمن و مداوم به کاربران ، نتایج زیر را به دنبال دارد .

- شناسائی، مدیریت و محافظت از سرمایه های اطلاعاتی سازمان

[4] Business continuity policy

- حفظ محرمانگی، تمامیت و دسترس پذیری سرمایه های اطلاعاتی سازمان
- شناسائی مخاطرات امنیت اطلاعات، تعیین و اجرای راهکارهای مقابله با این مخاطرات
- کاهش سطح حوادث امنیت اطلاعات و داشتن امنیتی پایدار و همچنین بکارگیری روشی مناسب برای مقابلـه بـا حـوادث امنیت اطلاعات
- رضایتمندی کاربران خدمات فناوری اطلاعات

که دستیابی به تمامی اهداف فوق منوط به مشارکت و همکاری تمامی کارکنان و کـاربران و دیگـر شـرکای تجـاری مـرتبط بـا موضوع سیستم مدیریت امنیت اطلاعات است.

منابع

۱ احترامی، بابک (۱۳۸۳). " نقطه ضعف اصلی" مجله شبکه، ش ۵۲ : ۱۳۸.

۲ بهاری، مهدی(۱۳۸۴). " امنیت تجهیزات شبکه"

۳ پورمند ، علی ، استانداردی برای امنیت اطلاعات www.imi.ir/tadbir

۴ اسعدی شالی ، عادله ، مدیریت سیستمهای امنیت اطلاعات ، مجله الکترونیکـی مرکـز اطلاعـات و مـدارک علمـی ایـران ، شماره چهارم ، دوره چهارم ، مرداد ۱۳۸۴

۵ شریفی، امیر حسین (۱۳۸۳)."مقدمه ای بر مفاهیم تست نفوذپذیری"

۶ دشتی، افسانه(۱۳۸۴)." استانداردهای امنیت" مجله شبکه، ش ۵۴ : ۱۵۸

7 Broderick, J. S. (2006). ISMS, security standards and security regulations, information security technical report. 11: 26 –31.

8 BS 7799-2, BS ISO/IEC 27001, (2005). Information technology-Security techniques-Information security management systems–Requirements (First edition).

9 D. Brewer and W. LiscaA , Fast track ISMS Certification , 2007

10 http://www.usdoj.gov/criminal/fraud/text/Internet.htm

11 ISO/IEC 27005, 2008. (2008) Information technology - Security techniques-Information security risk management (First edition).

12 International standard ISO/IEC27001,Final draft. 2011

13 ISO/IEC 27001, 2005. (2005). Information technology-Security techniques-Information security management systems–Requirements (First edition)

14 Pipkin, Donald. L. (2000)." Information security" new jersey: Prentice Hall

15 POA. (2003). Asset Protection and Security Management Handbook. Auerbach Publications. POA Publishing LLC.

16 Sungho, K., Jang. S., Lee, J., Kim, S. (2007). Common defects in information security management system of Korean companies, The Journal of Systems and Software. 80(10),1631–1638.

17 Sehanovic, Jusuf and Zugaj, Miroslov, "mathematical modeling of organization and information technology", Library management 1996: pp.25-30, MCB university press.

18 Solms, R.V. (1996). Information Security Management: The second Generation. Computers & Security. 15, 281-288.

19 Tan, K.C., Lyman, S.B., Wisner, J.D. (2002). Supply chain management: a strategic perspective. International Journal of Operations and Production Management.22(6), 614–31.