امنیت فناوری اطلاعات در شرکت گاز استان هرمزگان

محسن رئیسی[۱] ، ندا فکری‌کهن[۲]

[۱] کارشناس شبکه و ارتباطات شرکت گاز استان هرمزگان

Raeisi1988@gmail.com

[۲] کارشناس سیستم‌های کاربردی شرکت گاز استان هرمزگان

Nfk1381@gmail.com

چکیده:

تحولات اساسی دانش در سال‌های اخیر با محوریت استفاده روز افزون از فناوری اطلاعات و ارتباطات، تبعات فراوانی را به همراه آورده است. فناوری، ابزارهای جدیدی را در اختیار ما قرار داده که تاثیر آن‌ها در جنبه‌های مختلف زندگی نمایان است. فراهم شدن این ابزارها تنها باعث پیدایش محصولات نوین و راه‌های بهتر و کارآمدتر برای انجام امور نشده است، بلکه در کنار آن امکان سوء استفاده از فناوری را نیز به نوبه خود افزایش داده است. به همین منظور در بسیاری از سازمان‌ها بخصوص سازمان‌هایی که با تراکنش‌های تجاری سر و کار دارند نیاز به ایجاد روش‌ها و سیتم‌های امنیتی، بیشتر اهمیت پیدا می‌کند. از آنجا که فراهم بودن سطح قابل قبول و مناسبی از امنیت موجب می‌شود که افراد، سازمان‌ها، ارگان‌های دولتی و شرکت‌های خصوصی ضمن اعتقاد و اطمینان بیشتر، نقش مورد انتظار خود را به خوبی ایفا کنند، بر این اساس در این مقاله سعی داریم ضمن بیان تاریخچه راه‌های مقابله با تهدیدات احتمالی سازمانی و بر شمردن مزایای استفاده از امنیت فناوری اطلاعات در آن، به بررسی راه‌های بکارگیری این فناوری در سازمان پرداخته و راهکارهای تحقق آن در سازمان را مورد کنکاش قرار دهیم.

واژگان کلیدی: اطلاعات، امنیت، سازمان، فناوری اطلاعات، امنیت منابع اطلاعات

۱-مقدمه:

در عصر نوین سازمان‌ها در ابعاد و جنبه‌های مختلف به طور چشمگیر بر اطلاعات تاکید دارند. اطلاعات قدرت است و هر کسی از آن برخوردار شود، صاحب قدرت است. شرایط متغیر محیطی نیاز به اطلاعات را بیش از پیش نشان می‌دهد و این امر ضرورت جمع‌آوری، ثبت، پردازش و نیز توزیع اطلاعات را در سطوح مختلف سازمان دو چندان می‌سازد [۱].

چارچوب ساختاری تشکیل‌دهنده این عصر را تولید، پردازش، انتقال و مدیریت اطلاعات و ارتباطات به منظور ایجاد پایگاه‌های دانش و معرفت فردی، گروهی، سازمانی و کشوری جهت ارائه خدمات الکترونیکی تشکیل می‌دهد و لذا فناوری اطلاعات را که شامل فناوری‌های به کار گرفته شده در فرآیند مذکور می‌باشد برای سازمان‌ها و جوامع بشری، به عنوان عامل حیاتی و تعیین کننده مطرح ساخته است. امروزه اکثر کسب و کارها بر پایه فناوری اطلاعات بنا می‌شود. مدیران از فناوری اطلاعات به منظور تسهیل وظایف مدیریتی مانند طراحی سازمان، تدوین استراتژی‌ها و تصمیم‌گیری‌ها استفاده می‌کنند. در واقع نه تنها اطلاعات جز دارایی‌های معنوی و غیرملموس هر سازمانی محسوب می‌شود، بلکه در حکم ابزاری برای مدیریت موثر

سایر منابع و دارایی‌های سازمان از جمله منابع مالی، نیروی انسانی و ... نیز محسوب شده و لذا از اهمیت و ارزش ویژه‌ای در سازمان‌ها برخوردار است [۲].

وقتی یک مجموعه اداری خصوصی یا دولتی، مدل‌ها و سیستم‌های نوین مدیریتی و اطلاعاتی را می‌پذیرد، خودبه‌خود حجم زیادی از کارمندان، شرکای تجاری، اسپانسرهای مالی و مشترکین و مشتریان گسترده را در سطوح مختلف در مجموعه خود پذیرا شده است. هر یک از این افراد اطلاعاتی را در مجموعه مورد نظر ذخیره می‌کنند که به نوبه خود حیاتی بوده و از اهمیت خاصی برخوردار است. مقوله امنیت که یکی از حیاتی‌ترین اجزای چرخه رو به رشد فناوری اطلاعات است، از دیرباز جز یکی از اجزای اصلی زیرساخت‌های فناوری اطلاعات به شمار می‌رفت. تمامی رایانه‌ها از رایانه‌های موجود در منازل تا رایانه‌های موجود در سازمان‌ها و موسسات بزرگ، در معرض آسیب و تهدیدات مختلف امنیتی می‌باشند [۳]. در چنین فضایی سازمان همواره در معرض آسیب‌ها و تهدیدهای جدی قرار دارد و عدم اتخاذ رویکرد مناسب در برابر آن‌ها می‌تواند منجر به بروز چالش‌هایی در این زمینه شود که تخریب بانک‌های اطلاعاتی، افشای اطلاعات محرمانه، نقض حقوق حریم خصوصی و حملات اطلاعاتی نمونه‌ای از آن‌هاست.

۲-اهمیت فناوری اطلاعات در سازمان

رشد رایانه‌ها و شبکه‌ها، باعث تغییر شکل سازمان‌ها و شرکت‌ها به سمت و سوی نهادهای شبکه‌ای شده و موجب جریان دایمی اطلاعات در سازمان و خارج از آن شده است، بطوری که از این توانایی می‌توان برای طراحی و شکل‌دهی مجدد سازمان‌ها، تغییر ساختار آن‌ها، دامنه عملیات، مکانیزم کنترل و گزارش‌دهی، آموزش کاری، جریان کار، فرآورده‌ها و خدمات استفاده نمود. استفاده از فناوری اطلاعات می‌تواند نقش بسیار مهمی در ایجاد و شکل‌گیری ایده‌های نو و در نتیجه خلاقیت و نوآوری در سازمان ایفا کند [۱]. سرعت در تولید و عرضه اطلاعات ارزشمند، یکی از رموز موفقیت در سازمان‌ها، شرکت‌ها و موسسات مختلف در عصر اطلاعات است. پس از سازماندهی اطلاعات باید با بهره‌گیری از شبکه‌های رایانه‌ای، زمینه استفاده قانونمند و هدفمند از اطلاعات را برای دیگران فراهم کرد. به موازات حرکت به سمت یک سازمان پیشرفته و مبتنی بر فناوری اطلاعات، باید تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده شود. مهمترین مزیت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی سریع و آسان به اطلاعات است. به طور کلی وظایف فناوری اطلاعات در سازمان را می‌توان به هشت مورد تقسیم نمود:

نگهداری و پردازش	تقسیم وظایف	مدیریت شبکه	توسعه سیستم‌های
توسعه اطلاعات	مدیریت اطلاعات	توسعه کاربردی	مهندسی فناوری اطلاعات

شکل ۱: وظایف فناوری اطلاعات در سازمان.

فناوری اطلاعات از گستره وسیعی از فنون و فرآیندهای موجود استفاده می‌کند. در زمینه فناوری‌های نرم‌افزاری می‌توان به فرآیند سیستم‌های گسترده بانک‌های اطلاعاتی و سیستم‌های پشتیبان تصمیم‌گیری و در زمینه فناوری‌های سخت‌افزاری می‌توان به سیستم‌های کنفرانس از راه دور و سیستم‌های اطلاعاتی مدیریت اجرایی اشاره کرد. اصولاً نیاز به فناوری اطلاعات ناشی از سه عامل است:

۱- فناوری اطلاعات صنعتی استراتژیک است و در زمره سودآورترین صنایع جهان به شمار می‌آید.
۲- فناوری اطلاعات یک فناوری مادر و کلیدی است و در تمام صنایع و خدمات کاربرد دارد.
۳- فناوری اطلاعات یک زیربنای اساسی است که همه سازمان‌ها را قادر می‌سازد تا هزینه‌های خود را کاهش داده و با بهره‌وری کیفیت محصول و خدمات خود را افزایش دهند [۳].

با توجه به اهمیت اطلاعات، می‌توان گفت دسترسی به اطلاعات و مهمتر از آن امنیت و حفاظت از اطلاعات در هر سطحی برای رهبران و مدیران از مهمترین دغدغه‌ها می باشد. دستیابی رقبا به اطلاعات حتی می‌تواند موجب نابودی سازمان گردد. امکان از بین رفتن اطلاعات در اثر عوامل فیزیکی و عوامل تهدید کننده اطلاعات سازمان نیز وجود دارد. به این ترتیب با توسعه فناوری اطلاعات و استفاده از اطلاعات به عنوان یک ابزار تجاری بحث امنیت اطلاعات بُعد جدیدی به خود می‌گیرد، به طوری که حفاظت از اطلاعات سازمان یکی از ارکان مهم بقای آن می‌باشد. بنابراین طبقه‌بندی و ارزش‌گذاری و حفاظت از منابع اطلاعاتی، بسیار حیاتی و مهم به‌شمار می‌آید، به طوری که بی‌توجهی به امنیت اطلاعات تهدیدی بزرگ برای سازمان‌ها در پی خواهد داشت.

۳-فناوری امنیت اطلاعات

امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است [۴]. در واقع امنیت به مجموعه‌ای از روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود. به این ترتیب فناوری امنیت اطلاعات به بهره‌گیری مناسب از تمام فناوری‌های امنیتی پیشرفته برای حفاظت از تمام اطلاعات اشاره دارد. باید توجه داشت که فناوری امنیت اطلاعات در یک لحظه قابل برقراری نیست. استقرار این فناوری اقدامی مداوم است که به صورت فرآیند چرخشی قابل پیاده‌سازی است. مدیران برای نیل به این هدف باید بر سیاست‌های امنیت اطلاعات توجه ویژه‌ای داشته باشند.

فناوری‌های امنیت اطلاعات بر اساس ویژگی زمانی به دو دسته طبقه‌بندی شده‌اند:

۱- کنشی (Proactive): انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی

به عنوان مثال رمزنگاری (Cryptography) یک فناوری امنیت اطلاعات از نوع کنشی است. زیرا اطلاعات را قبل از آن که یک تهدید بالقوه بتواند اعمال خرابکارانه انجام دهد، از طریق رمزگذاری داده‌ها ایمن می‌سازند. پروتکل‌های امنیتی (Security Protocols) نیز، جز فناوری‌های امنیت اطلاعاتی کنشی هستند. زیرا برای حفاظت از اطلاعات حساس از یک پروتکل خاص امنیتی، قبل از آن که اطلاعات به وسیله خرابکاران بدست آید، استفاده می‌کنند. این فناوری در سطوح مختلف قابل پیاده‌سازی است.

۲- واکنشی (Reactive): انجام عکس‌العمل لازم پس از وقوع یک مشکل خاص امنیتی

به عنوان مثال دیوار آتش (Firewall) یک فناوری امنیت اطلاعات واکنشی است و مهمترین ابزار امنیتی مورد استفاده برای کنترل ارتباطات شبکه‌ای بین دو سازمان که به یکدیگر اعتماد ندارند، می‌باشد. با قرار دادن یک دیوار آتش روی هر ارتباط خارجی شبکه، سازمان می‌تواند یک دایره امنیتی تعریف نماید که از ورود افراد خارجی به رایانه‌های سازمان جلوگیری می‌کند. علاوه بر آن، دیوار آتش می‌تواند مانع نفوذ افراد خارجی به منابع موجود در رایانه‌های سازمان و گسترش نامطلوب روی شبکه سازمان شود. این فناوری در سطوح میزبان و در سطح شبکه قابل پیاده‌سازی است. فناوری کلمه عبور (password) نیز یک فناوری امنیت اطلاعات واکنشی است. زیرا به منظور گرفتن مجوز و دسترسی به سیستم، به محض اینکه یک فرد یا فرآیند بخواهد به یک برنامه کاربردی، میزبان یا شبکه متصل شود، بکار می‌رود [۴].

نبود نظام مناسب امنیتی، ممکن است پیامدهای منفی و دور از انتظاری را به دنبال داشته باشد. توفیق در ایمن‌سازی اطلاعات منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است. بدین منظور از سرویس‌های امنیتی متعددی استفاده می‌شود. سرویس‌هایی که انتخاب می‌شوند باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص به موقع حملات و واکنش سریع را داشته باشند. بنابراین می‌توان

محور راهبردی انتخاب شده را بر سه مؤلفه حفاظت، تشخیص و واکنش استوار نمود. حفاظت مطمئن، تشخیص به موقع و واکنش مناسب، از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت کرد.

رویکرد اغلب سازمان‌ها در مواجه با تهدیدات، خرید محصولات امنیتی و به کارگیری آن‌ها در سیستم‌های رایانه‌ای است. در صورتی که استفاده از محصولات امنیتی با هزینه بالا و بدون شناخت و تحلیل دقیق نیازهای امنیتی، به‌تنهایی کارساز نخواهد بود. مدیریت امنیت اطلاعات و نیز سیستم امنیت اطلاعات از راهکارهای حل چنین مشکلاتی می‌باشد [۴].

۴-مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به اهداف و ارائه راهکارهای لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و درنهایت باید تلاش کند تا سیستم را همیشه بروز نگه دارد. هدف مدیریت امنیت اطلاعات در سازمان، حفظ سرمایه‌های سازمان (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 ایجادشده از سوی کاربران) است و برای رسیدن به این اهداف نیاز به یک برنامه منسجم دارد. سیستم امنیت اطلاعات راهکاری برای رسیدن به این هدف می‌باشد [۵].

۵-سیستم امنیت اطلاعات

یکی از وظایف مدیریت امنیت بررسی و ایجاد یک سیستم امنیت اطلاعات است که متناسب با اهداف سازمان باشد. برای طراحی این سیستم باید عوامل مختلفی را در نظر گرفت. محاسبه ارزش اطلاعات از نظر اقتصادی، بررسی خطرات و محاسبه خسارت‌های احتمالی و تخمین هزینه، سودمندی استفاده از سیستم امنیت اطلاعات، بررسی تهدیدات احتمالی و بررسی راهکارهای مختلف و انتخاب سودمندترین روش برای طراحی نظام‌های امنیت اطلاعات ضروری به نظر می‌رسد [۲].

۶-مراحل تحقق امنیت فناوری اطلاعات

با گسترش شبکه‌های رایانه‌ای، نگرش به امنیت اطلاعات و دیگر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی گردیده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک راهبرد خاص پایبند باشد و بر اساس آن، نظام امنیتی را پیاده‌سازی و اجرا نماید. موارد مختلفی ازجمله وجود ضعف امنیتی در شبکه‌های رایانه‌ای و اطلاعاتی، عدم آموزش و توجیه صحیح کاربران نسبت به اهمیت امنیت اطلاعات صرفنظر از مسئولیت شغلی آن‌ها، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقص‌های امنیتی، عدم وجود سیاست‌های مدرن به منظور برخورد مناسب و به موقع با اشکالات امنیتی، باعث به وجود آمدن مسائلی خواهد شد که ضرر آن متوجه تمامی کاربران سازمان شده و عملاً زیرساخت اطلاعاتی سازمان را در معرض آسیب و تهدید جدی قرار می‌دهد. کنترل دستیابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهترین اهداف یک نظام امنیتی در شبکه است [۶].

بسیاری از شرکت‌ها و سازمان‌ها برای حفظ امنیت اطلاعات خود از راهکارهای مدرن و توسعه‌یافته استفاده می‌کنند. راهکارهای حفظ امنیت اطلاعات، با استفاده از فناوری‌های مختلفی پیاده‌سازی می‌شوند. امنیت شبکه، امنیت سرویس‌دهنده‌ها و امنیت برنامه‌های کاربردی همگی باعث ایجاد زمینه امنیت اطلاعات می‌شوند. اما موضوعی که در مورد امنیت اطلاعات در نظر گرفته نمی‌شود، ضرورت ایجاد ساختار مناسب برای استفاده از مزایای فناوری‌های امنیتی است. با استفاده از ایجاد ساختار مناسب است که امکان مدیریت، کنترل و ایجاد روال‌های امنیتی برای زیرساخت‌های امنیت اطلاعات فراهم خواهد شد. برای نیل به این هدف قبل از هر چیز آشنایی کامل با محیط سازمان ضروری است. آشنایی سطحی منجر به تصمیمات سطحی خواهد بود [۲]. آگاهی از سخت‌افزارها و نرم‌افزارهای به‌کار رفته و جزئیات دسترسی و نوع کارکرد آن‌ها برای تصمیم‌گیری درست هر فرد در سازمان مهم است. پس از آشنایی با محیط، تعیین نقش‌های هر فرد و سطح دسترسی از اهمیت ویژه‌ای برخوردار است. در واقع باید نوع دسترسی برای هر گروه و هر فرد خاص به طور کامل مشخص شود. نکته قابل توجه‌ای که در این مورد باید در نظر داشت این است نقش‌های انسانی در تدوین مدل امنیتی سازمان حیاتی است.

هرچند در سازمان زمان و انرژی زیادی صرف کنترل و بررسی موارد امنیتی و اطلاعاتی می‌شود، اما باید در نظر داشت که اطمینان از صحت اطلاعات، اولین شرط برای شروع اجرای تصمیمات جدید است. برای این کار باید فهرستی از تمام مواردی که برای امنیت اطلاعات سازمان حیاتی است تهیه کرده و با مراجعه به افراد مسئول در هر مورد آخرین بررسی‌ها در مورد صحت اطلاعات را انجام داد. پس از بررسی و کنترل، سندی از اطلاعات مورد توافق تهیه‌کرده و آن را به‌عنوان معیار هر مورد اطلاعاتی قرارداد. آخرین مرحله برای تحقق امنیت فناوی اطلاعات کنترل اطلاعاتی است کهاز ساختار اطلاعاتی کسب شده است [۶]. تمامی اجزای ساختار امنیت اطلاعات در سازمان بایستی به‌صورت مستمر و بدون وقفه تحت کنترل باشد. قسمتی از این کنترل مستمر روال‌های انسانی و قسمت مهم‌تر آن ذخیره‌سازی و پردازش گزارشات امنیتی می‌باشد. به‌طورکلی داشتن برنامه و استراتژی جامع و کاملی که تمامی موارد تهدیدکننده و چگونگی برخورد با هر یک را مشخص می‌کند اولویت‌های برنامه هر سازمان می‌باشد.

۷-نتیجه‌گیری

آنچه که پیداست دست یافتن به سطح امنیت در فناوری اطلاعات و ارتباطات به طور کامل ممکن نیست. برای دست یافتن به سطح مطلوب امنیت فناوری اطلاعات و ارتباطات باید تغییر نگرش اساسی در مدیران سازمانی اتفاق بیاید. ازآنجایی‌که یک فناوری جدید مخاطرات جدیدی نیز به وجود می‌آورد و فناوری‌ها هرروز گسترده‌تر می‌شود، لذا امنیت فناوری اطلاعات شایسته توجه است. بر این اساس امنیت فناوری اطلاعات و ارتباطات باید دغدغه همه افراد یک سازمان باشد.

منابع:

[1] D. Lacey, “Understanding and transforming organizational security culture”, Information Management & Computer Security, Vol. 18, no. 1, pp. 4-13, 2010.

[2] G. Dhillon, R. Chowdhuri, “Organizational transformation and information security culture: a telecom case study”, IFIP Advances in Information and Communication Technology, Vol. 428, no. 1, pp. 431-437, 2014.

[3] W. hui, “Brand, knowledge and false sense of security”, Information Management & Computer Security, Vol. 18, no. 3, pp. 162-173, 2010.

[4] S. Furnell, K. Thomson, “Computer fraud & security”, International Journal Performance Evaluation, Vol. 9, no. 1, pp. 5-10, 2009.

[5] A. Ruigharer, S. Maynard, “Organizational security culture: extending the end-user perspective”, Computer & Security, Vol. 26, no. 1, pp. 26-62, 2007.

[6] N. Cuppens, F. Cuppens, S. Jajodia, “ICT systems security and privacy protection”, IFIP Advances in Information and Communication Technology, Vol. 428, no. 1, pp. 169-184, 2014.