نقش امنیت اطلاعات در سازمان ها

خلاصه : طراحی و پیاده سازی یک محیط ایمن در سازمان های مدرن اطلاعاتی یکی از چالش های اساسی در عصر حاضر محسوب می گردد. برای بسیاری از سازمان ها و موسسات اهمیت و ضرورت توجه جدی به مقوله امنیت اطلاعات هنوز در هاله ای از ابهام قرار دارد و برخی دیگر امنیت را تا سطح یک محصول تنزل داده و فکر می‌کنند که با تهیه یک محصول نرم افزاری خاص و نصب آن در سازمان خود، امنیت را برای سازمان خود به ارمغان می آورند. در این مقاله سعی شده است اهمیت پیاده سازی امنیت اطلاعات بررسی و مضرات مالی ناشی از عدم وجود بسترهای امنیتی لازم در سازمانها مورد اشاره قرار گرفت. همچنین مزایای سرمایه گذاری در خصوص پیاده سازی امنیت اطلاعات در سازمان ها و مزایای بکارگیری آن مورد بررسی قرار گرفت.

شماره : 57

تاریخ : 1393/09/29

موضوع : امنیت

متن : چکیده طراحی و پیاده سازی یک محیط ایمن در سازمان های مدرن اطلاعاتی یکی از چالش های اساسی در عصر حاضر محسوب می گردد. برای بسیاری از سازمان ها و موسسات اهمیت و ضرورت توجه جدی به مقوله امنیت اطلاعات هنوز در هاله ای از ابهام قرار دارد و برخی دیگر امنیت را تا سطح یک محصول تنزل داده و فکر می‌کنند که با تهیه یک محصول نرم افزاری خاص و نصب آن در سازمان خود، امنیت را برای سازمان خود به ارمغان می آورند. در این مقاله سعی شده است اهمیت پیاده سازی امنیت اطلاعات بررسی و مضرات مالی ناشی از عدم وجود بسترهای امنیتی لازم در سازمانها مورد اشاره قرار گرفت. همچنین مزایای سرمایه گذاری در خصوص پیاده سازی امنیت اطلاعات در سازمان ها و مزایای بکارگیری آن مورد بررسی قرار گرفت. 1. مقدمه آشنایی با دانش روز در حوزه فناوری اطلاعات و ارتباطات (ICT)، جهت بهره مندی از امکانات و فرصت هایی که در سایه این فناوری در اختیار بشر گذاشته شده امری ضروری است. امروزه اصطلاح با سواد به کسی اطلاق می شود که در این حوزه نیز دارای اطلاعات لازم جهت تعامل و کار و استفاده از فرصت های فراهم شده در این عرصه باشد. امکان دست یابی سریع به اطلاعات مورد نظر از طریق جست وجو در بانک های 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، گفت و گو و تبادل نظر متنی، صوتی و تصویری، فرصت هایی است که باید از آن بهره کامل برد. رشد این فناوری آن چنان سریع و عمیق بوده که در جای جای زندگی فردی و اجتماعی انسان ها، نفوذ کرده و حضور قدرت مندانه خود را به رخ میکشد. بسیاری از مراکز و مؤسسات دولتی و خصوصی، بانک ها، شرکت ها و ادارات، مراکز آموزشی، پژوهشی، تبلیغی و اطلاع رسانی، در انجام وظایف و مأموریت های خود، از این فناوری بهره می برند 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، شبکه ها و سایت های اینترنتی مشاهده خواهیم کرد. نفوذ به سیستم‌های بانکی، سرقت حساب های بانکی، دست برد زدن به 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 هر یک 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 آسیب پذیر و توسعه فناوری با توجه به شرایط و تحولات پیش رو، هزینه کرده اند و موفقیت های خوبی هم داشته اند. 2. تعریف امنیت اطلاعات امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری. دولت ها، مراکز نظامی، شرکت ها، موسسات مالی، بیمارستان ها و مشاغل خصوصی مقدار زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصولات، تحقیقات و وضعیت مالی گردآوری می‌کنند. بسیاری از این اطلاعات در حال حاضر بر روی کامپیوترهای الکترونیکی جمع آوری، 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 درز اطلاعات ممکن است به خسارات مالی به کسب و کار، پیگرد قانونی و یا حتی ورشکستگی منجر شود. حفاظت از اطلاعات محرمانه یک نیاز تجاری و در بسیاری از موارد نیز نیاز اخلاقی و قانونی است. برای افراد، امنیت اطلاعات تاثیر معناداری بر حریم خصوصی دارد. البته در فرهنگ‌های مختلف این مفهوم حریم خصوصی تعبیرهای متفاوتی دارد. 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: تامین امنیت شبکه (ها) و زیرساخت‌ها، تامین امنیت برنامه‌های کاربردی و پایگاه داده‌ها، تست امنیت، حسابرسی و بررسی سیستم‌های اطلاعاتی، برنامه‌ریزی تداوم تجارت و بررسی جرائم الکترونیکی، و غیره. در جهان امروز شاهد بکارگیری تجهیزات الکترونیک و روش¬های مجازی برای برقراری ارتباطات و تبادل اطلاعات هستیم. اما همراه با گسترش این تکنولوژی¬ها روش¬های مختلف حمله به آن¬ها نیز توسعه یافته و امنیت اطلاعات را در معرض خطر قرار داده است. از این رو، به منظور بهره¬مند شدن سازمان¬ها و مشتریان از این تکنولوژی¬ها نیازمند برقراری ارتباطاتی امن هستیم. لازم است که کنترل¬ها و بررسی¬های متعددی انجام گیرد تا از امنیت اطلاعات در سازمان اطمینان یابیم. این کنترل¬ها محدوده¬ی وسیعی از فعالیت¬ها را در برمی¬گیرد بدون شک مهمترین آن¬ها سیاست امنیت اطلاعات یا سیاست امنیتی خواهد بود. سیاست امنیت اطلاعات تعیین کننده جهت امنیت اطلاعات در سازمان است و می¬بایست به صورت یک سند مکتوب تهیه گردد. این سند بایستی مکمل اهداف تجاری سازمان باشد و مشارکت مدیریت را در برقراری امنیت اطلاعات و پشتیبانی از آن، نظیر نقشی که امنیت اطلاعات در تعریف دیدگاه و مأموریت سازمان ایفا می¬کند، تعریف کند. همچنین، سیاست امنیت اطلاعات باید نیاز به امنیت اطلاعات و مفاهیم آن را برای تمامی کاربران منابع اطلاعاتی سازمان شرح دهد و کارمندان را در مورد مسئولیت¬های خود و نحوه استفاده از منابع سازمان مطلع سازد. لازم است که در این سند استفاده¬های مجاز شرح داده شوند و فعالیت¬های غیرمجاز به صورت لیستی ارائه گردند. به عبارت دیگر این سند بیان می¬کند که یک سازمان چگونه قصد

دارد از سرمایه¬های فیزیکی و اطلاعاتی خود محافظت کند. اهداف اصلی یک سیاست امنیت اطلاعات را می¬توان به سه بخش محرمانگی(اطمینان از اینکه اطلاعات تنها در دستان افراد مجاز قرار می¬گیرند.)، درستی(حفاظت از اطلاعات در مقابل تغییر، تحریف و نابودی)، و دسترس¬پذیری(اطمینان از اینکه اطلاعات و سیستم¬های اطلاعاتی در زمان مورد نیاز در دسترس و قابل استفاده هستند. 3. اهمیت امنیت اطلاعات برای یک سازمان وجود یک حفره و یا مشکل امنیتی، می تواند یک سازمان را به روش‌های متفاوتی تحت تاثیر قرار خواهد داد. آشنائی با عواقب خطرناک یک حفره امنیتی در یک سازمان و شناسائی مهمترین تهدیدات امنیتی که می تواند حیات یک سازمان را با مشکل مواجه نماید، از جمله موارد ضروری به منظور طراحی و پیاده سازی یک مدل امنیتی در یک سازمان می باشد. وجود حفره های امنیتی در یک سازمان ، می تواند پیامدهای منفی متعددی را برای یک سازمان به دنبال داشته باشد : کاهش درآمد و افزایش هزینه خدشه به اعتبار و شهرت یک سازمان از دست دادن داده و اطلاعات مهم اختلال در فرآیندهای جاری یک سازما پیامدهای قانونی به دلیل عدم ایجاد یک سیستم ایمن و تاثیر جانبی منفی بر فعالیت سایر سازمان ها سلب اعتماد مشتریان سلب اعتماد سرمایه گذاران 4. امنیت اطلاعات در سازمان ها طی سالیان اخیر ماحصل بررسی انجام شده توسط موسسات و مراکز تحقیقاتی معتبر در خصوص امنیت اطلاعات، نشاندهنده این واقعیت مهم است که حملات مهاجمان بر روی درآمد و هزینه یک سازمان بطور مستقیم و یا غیرمستقیم تاثیر خواهد داشت (کاهش درآمد، افزایش هزینه) . • در سال 2003 ، ویروس ها و حملات از نوع DoS (برگرفته از Denial of Service) بیشترین تبعات منفی را برای سازمان‌ها به دنبال داشته اند. • در سال 2004 ، سرقت اطلاعات بالاترین جایگاه را داشته و حملات از نوع DoS با اندکی کاهش نسبت به سال 2003 در رتبه دوم قرار گرفته اند . • با این که هزینه پیاده سازی یک سیستم حفاظتی اندک نمی باشد ولی می توان آن را به عنوان بخشی از هزینه هائی در نظر گرفت که یک سازمان به دلیل عدم ایمن سازی ، می بایست پرداخت نماید (برخورد با تبعات منفی) • موثرترین راهکار و یا راه حل امنیتی ، ایجاد یک محیط چندلایه ای است . در یک محیط چند لایه ، مهاجمان در هر لایه شناسائی و با آنان برخورد خواهد شد . موفقیت یک مهاجم نیز به عبور موفقیت آمیز از هر لایه بستگی دارد . راه‌هکار امنیتی چندلایه به "دفاع در عمق " نیز مشهور است . در این مدل، در هر لایه از استراتژی های تدافعی خاصی استفاده می گردد که با توجه به ماهیت پویای امنیت اطلاعات، می بایست به صورت ادواری توسط کارشناسان حرفه ای امنیت اطلاعات، بررسی و بهنگام گردند . • در سال 2004 ، هفتاد درصد سازمان ها حداقل یک مرتبه مورد تهاجم قرار گرفته اند . • در سال 2003 بالغ بر 666 میلیون دلار صرف برخورد با مشکلات امنیتی در سازمان ها شده است . • نیمی از سازمان ها به این موضوع اعتراف نموده اند که نمی دانند چه میزان از اطلاعات سازمان خود را به دلیل حملات از دست داده اند . • چهل و یک درصد سازمان ها اعلام داشته اند که دارای هیچگونه طرح و یا برنامه ای برای گزارش و یا پاسخ به تهدیدات امنیتی نمی باشند . 5. مزایای سرمایه گذاری در امنیت اطلاعات سازمان ها و موسسات تجاری با پیاده سازی یک استراتژی امنیتی از مزایای زیر بهره مند خواهند شد : • کاهش احتمال غیرفعال شدن سیستم ها و برنامه ها (از دست دادن فرصت ها) • استفاده موثر از منابع انسانی و غیرانسانی در یک سازمان (افزایش بهره وری) • کاهش هزینه از دست دادن داده توسط ویروس های مخرب و یا حفره های امنیتی (حفاظت از داده های ارزشمند) • افزایش حفاظت از مالکیت معنوی 6. تاثیر بکارگیری فناوری اطلاعات در سازمان ها در جهان امروز تکنولوژی اطلاعات امکان سودمندی و کارآمدی اطلاعات را ممکن ساخته است. بکارگیری تکنولوژی اطلاعات (فناوری اطلاعات)، تحول گسترده ای را در امور اداری و سیستم‌های اطلاعاتی باعث شده است، طوریکه امکان انتقال الکترونیکی داده‌ها، مدارک، اسناد و مکاتبات مختلف از طریق کامپیوتر و خطوط ارتباطات مخابراتی فراهم‌شده است. مطالعات و تحقیقات نشان می دهد که بین سرمایه گذاری در فناوری اطلاعات و بازده موسسات و بهره‌وری نیروی انسانی ارتباط دو سویه مثبتی وجود دارد. همچنین تکنولوژی اطلاعات توانایی سازمانها را افزایش می‌دهد و این در نتیجهٔ افزایش تنوع محصولات و بهبود کیفیت و جلب رضایت مشتری است و نیز سبب تسهیل روند اداری و افزایش بازده نیروی انسانی و مدیریت می‌شود. یکی از نتایج عمده تکنولوژی اطلاعات (فناوری اطلاعات) تمرکز زدایی در عین تمرکزگرایی است. بدین معنی که می‌توان کارها را از راه دور انجام داد بدون آنکه لازم باشد تا در محل حضور فیزیکی و مستمر داشته باشیم که این ویژگی بر کوتاه شدن فواصل زمانی و مکانی به عنوان یک ابر شاهراه تاکید دارد. امروزه تکنولوژی اطلاعات (فناوری اطلاعات) دیگر سیستمهای اطلاعاتی مدیریت از جمله CIS، MIS، DSS AI، EIS، OA و ... را در اختیار گرفته و بدین ترتیب قطب اطلاعاتی مستقر در مرکز را قادر می سازد تا به افزایش کنترل خود بر مناطق و انجام عملیات تمرکزی اقدام نماید. بنابراین امکان افزایش سرعت و کیفیت تصمیم‌گیری و مدیریت را فراهم می‌نماید. تکنولوژی اطلاعات (فناوری اطلاعات) به عنوان یکی از مهمترین ابزار جهت مشارکت در بازار جهانی است. از ویژگیهای اساسی عصر حاضر، اطلاعات و تبدیل آن به دانش است . چنین ویژگی تاثیر زیادی روی نهادهای اجتماعی و اقتصادی جوامع خواهد گذاشت . نهادهای اجتماعی باید بر اساس آن تجدید بنا و تغییر ساختار دهند. گفته می شود که تکنولوژی اطلاعات (فناوری اطلاعات) توانایی سازمان را افزایش می دهد با این وجود چنین پیشرفتهایی اغلب سبب بهبود عملکرد مالی سازمانها نمی شود. ساز وکار و برنامه‌های استراتژیکی خاصی نیاز است تا به این اهداف اساسی در بکار گیری تکنولوژی اطلاعات (فناوری اطلاعات) در سازمان دست یافت. دکتر رومار استاد دانشگاه برکلی در نظریه خویش « رشدجدید اقتصادی» عنوان می‌کند که در عصرحاضر، عامل رشد اقتصادی سرمایه ، نیروی انسانی و مواد خام نیستند بلکه دانش و افکار جدید سبب شکوفایی اقتصادی می‌شود و سرمایه کشورها تابعی ازعلم و عقاید است. محور های بکارگیری فناوری اطلاعات در شرکتها و ادارات محورهای سه گانه که در بکارگیری فناوری اطلاعات در سازمانها مورد توجه است شامل : مردم ، زیر ساخت و کاربردها است. آموزش ، افزایش مهارت و فرهنگ سازی محور اساسی اولیه است که به عنوان مردم مطرح است. شبکه، تجهیزات فنی، مقررات و قوانین محور زیرساخت و بالاخره آموزش الکترونیک، سیستم بدون کاغذ، کنفرانس راه دور، دولت الکترونیکی، تجارت الکترونیک و ... از محورهای کاربرد فناوری اطلاعات مطرح هستند. پیاده سازی فناوری اطلاعات در سازمانها و ادارات همانطوریکه بیان گردید تکنولوژی اطلاعات (فناوری اطلاعات) به عنوان محور و محرک توسعه جوامع و سازمانها مطرح است. مطالعات در این زمینه نشان می دهد که تکنولوژی اطلاعات (فناوری اطلاعات) باید در دو حوزه تحقیق و اجرا در سازمانها مورد بحث قرار گیرد. بخش تحقیق وظیفه شبیه سازی محیطی، تجربه مجازی و فرضیات با هزینه کم، همراه با برنامه ریزی، مدلهای تصمیم گیری و ایجاد خلاقیت در کارکنان را برعهده دارد. اجرا و بکار گیری فناوری اطلاعات (Information Technology) بکار گیری و اجرای تکنولوژی اطلاعات (فناوری اطلاعات)در سازمانها یک نسخه تجویز شده کلی نیست و نمی توان با یک برنامه جامع تکنولوژی اطلاعات برای کلیه سازمانها و شرکتها، ساختار فناوری اطلاعات را پیاده سازی و اجرا نمود. مهمترین عوامل که در پیاده سازی تکنولوژی اطلاعات (فناوری اطلاعات) در هر سازمان باید مورد نظر و توجه

قرارگیرد ، عبارتند از: 1. فرهنگ سازی: بستر سازی فرهنگی در هر سازمان جهت اجرای موفقیت آمیز فناوری اطلاعات لازم می باشد. 2. اعتقاد و باور مدیران ارشد سازمان: هرچه مدیران ارشد سازمان به فناوری اطلاعات به عنوان یک مقوله لاینفک از سازمان خویش توجه کنند، موفقیت بکارگیری آن سریعتر و بیشتر خواهد بوددر این راه اعتقاد و اطمینان مدیران به آینده مؤثرترین عامل در موفقیت بکارگیری فناوری اطلاعات است. 3. آفت شناسی: مشکلات و موانع بکارگیری و پیاده سازی فناوری اطلاعات در سازمان دقیق و علمی بررسی و برنامه‌ریزی شود. 4. سوق به سمت ساختار فرآیندی : ساختار سازمانهای مرتبط با فناوری اطلاعات باید از ساختار وظایفی خارج و به سمت ساختار فرآیندی سوق داده شود. 5. درگیری کلیه افراد سازمان در امور فناوری اطلاعات: کلیه اعضای سازمان از مدیر ارشد تا کارمندان سطح عملیاتی باید به عنوان کارشناسان فناوری اطلاعات شناخته شوند. 6. بهبود شاخصهای بهره وری: شاخصهای اندازه گیری بهره وری در سازمان باید به سمت بهبود رشد نماید و از اطلاعات جهت تبدیل به دانش استفاده شود. 7. کوچک سازی: خارج کردن فعالیتهای غیر محوری از محیط سازمان که کوچک سازی گفته می‌شود ، از ضروریات ملی بشمار می رود. مراجع: [1] دکتر علیرضا احمدی، دانشیار علم و صنعت، ICT Strategic Planning ، انتشارات تولید دانش، تابستان 1383. [2] استانداردی برای مدیریت امنیت اطلاعات، علی پورمند، پایگاه مقالات مدیریت [3] Web site: dp.co.ir [4] Web site: www. wikipedia.com [5] Web site: www.douran.com

نویسندگان : محمد رامندی