

امنیت اطلاعات

گمان می‌رود که این مقاله ناقض حق تکثیر باشد، اما بدون داشتن منبع امکان تشخیص قطعی این موضوع وجود ندارد. اگر می‌توان نشان داد که این مقاله حق نشر را زیر پا گذاشته است، لطفاً مقاله را در ویکی‌پدیا:مشکلات حق تکثیر فهرست کنید. اگر مطمئنید [بیشتر بدانید](#)

هم‌زمان با گسترش به‌کارگیری رایانه‌های شخصی و مطرح شدن شبکه‌های رایانه‌ای و به دنبال آن اینترنت (بزرگترین شبکه‌ی جهانی)، حیات رایانه‌ها و کاربرانشان دسخوش تغییراتی اساسی شده است. کاربران رایانه به منظور به‌کارگیری دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی ویژه و مورد اهمیت قرار دادن همه‌ی مولفه‌های تاثیر گذار در تداوم ارائه خدمت در یک سامانه‌ی رایانه‌ای می‌باشند

امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای از جمله این مؤلفه‌ها بوده که نمی‌توان آن را مختص یک فرد یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای در هر کشور، مستلزم توجه همه کاربران صرف‌نظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای بوده و می‌بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه‌های رایانه‌ای و اطلاعاتی، عدم آموزش و توجیه صحیح همه کاربران صرف نظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه همه کاربران رایانه در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد.

امنیت اطلاعات یک فرایند پیچیده فیزیکی و رایانه‌ای است که طی آن کشوری خاص با به‌کارگیری تجهیزات و فناوری‌های سخت افزاری و نرم افزاری و کنترل اینترنت با استفاده تشکیل ارگان‌ها مختلف سعی بر کنترل اطلاعات شخصی و مهم امنیتی و کاربری کشور و مردم خود میکند. این کنترل‌ها ممکن است در شکل [فیلترینگ](#) و یا [فیلترینگ هوشمند](#) و مسدود سازی و کنترل پروتکل اینترنت (IP) های مزاحم صورت بگیرد.

اکنون پلیس فتا در ایران عهده دار مسئولیت نظارت بر فعالیت های اینترنتی هستند.

نظارت و کنترل فضای مجازی از واجبات دنیای ارتباطات و زندگی انسان هاست این کنترل ها سد اصلی مقابل دزدیده شدن اطلاعات و یا خرابکاری در دنیای مجازی است.

تعریف امنیت اطلاعات

امنیت اطلاعات یعنی حفاظت اطلاعات و سامانه‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری.

واژه‌های امنیت اطلاعات، امنیت رایانه‌ای و اطلاعات مطمئناً گاهی به اشتباه به جای هم بکار برده می‌شود. اگر چه این‌ها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آن‌ها وجود دارد. این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله، و موضوعاتی که تمرکز کرده‌اند دارد.

امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، یا اشکال دیگر.

امنیت رایانه در حصول اطمینان از در دسترس بودن و عملکرد صحیح سامانه رایانه‌ای تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سامانه رایانه‌ای ذخیره یا پردازش می‌شود.

دولت‌ها، مراکز نظامی، شرکت‌ها، موسسات مالی، بیمارستان‌ها، و مشاغل خصوصی مقدار زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصولات، تحقیقات، و وضعیت مالی گردآوری می‌کنند. بسیاری از این اطلاعات اکنون بر روی رایانه‌های الکترونیکی جمع‌آوری، پردازش و ذخیره و در شبکه به رایانه‌های دیگر منتقل می‌شود. اگر اطلاعات محرمانه در مورد مشتریان 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 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 تأثیر 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: تأمین امنیت شبکه (ها) و زیرساخت‌ها، تأمین امنیت برنامه‌های کاربردی و پایگاه داده‌ها، تست امنیت، حسابرسی و بررسی سامانه‌های اطلاعاتی، برنامه‌ریزی تداوم تجارت و بررسی جرائم الکترونیکی، و غیره.

این مقاله یک دید کلی از امنیت اطلاعات و مفاهیم اصلی آن فراهم می‌کند. ویلیام استالینگز/رمزنگاری و شبکه امن: منبع

تاریخچه

از زمانی که نوشتن و تبادل اطلاعات آغاز شد، همه انسان‌ها به‌ویژه سران حکومت‌ها و فرماندهان نظامی در پی راهکاری برای محافظت از محرمانه بودن مکاتبات و تشخیص دستکاری آن‌ها بودند. **ژولیوس سزار** ۵۰ سال پیش از میلاد یک سامانه رمزنگاری مکاتبات ابداع کرد تا از خوانده شدن پیام‌های سری خود توسط دشمن جلوگیری کند حتی اگر پیام به دست دشمن بیفتد جنگ جهانی دوم باعث پیشرفت چشمگیری در زمینه امنیت اطلاعات گردید و این آغاز کارهای حرفه‌ای در حوزه امنیت اطلاعات شد. پایان قرن بیستم و سال‌های اولیه قرن بیست و یکم شاهد پیشرفتهای سریع در ارتباطات راه دور، **سخت‌افزار، نرم‌افزار** و رمزگذاری داده‌ها بود. در دسترس بودن تجهیزات محاسباتی کوچکتر، قوی‌تر و ارزان‌تر پردازش الکترونیکی داده‌ها باعث شد که شرکت‌های کوچک و کاربران خانگی دسترسی بیشتری به آن‌ها داشته باشند. این تجهیزات به سرعت از طریق شبکه‌های رایانه مثل اینترنت به هم متصل شدند.

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 رایانه‌ای، امنیت اطلاعات و اطلاعات مطمئن همراه با سازمان‌های متعدد حرفه‌ای پدید آمدند. هدف مشترک این فعالیت‌ها و سازمان‌ها حصول اطمینان از امنیت و **قابلیت اطمینان** از سامانه‌های اطلاعاتی است.

مفاهیم پایه

همانگونه که تعریف شد، موارد سه‌گانه حفظ محرمانگی، یکپارچه بودن و دسترسی‌پذیری از مفاهیم اصلی امنیت اطلاعات است. در اینجا مفاهیم سه‌گانه «محرمانگی»، «یکپارچه بودن» و «قابل دسترسی بودن» توضیح داده می‌شود. در بین متخصصان این رشته بحث مداومی وجود دارد مبنی بر اینکه علاوه بر این ۳ مفهوم موارد دیگری هم را باید در نظر گرفت مثل «قابلیت حسابرسی»، «قابلیت عدم انکار انجام عمل» و «اصل بودن».

محرمانگی

محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیرمجاز. به عنوان مثال، برای خرید با کارت‌های اعتباری بر روی اینترنت نیاز به ارسال شماره کارت اعتباری از خریدار به فروشنده و سپس به مرکز پردازش معامله است. در این مورد شماره کارت و دیگر اطلاعات مربوط به خریدار و کارت اعتباری او نباید در اختیار افراد غیرمجاز بیفتد و این اطلاعات باید محرمانه بماند. در این مورد برای محرمانه نگهداشتن اطلاعات، شماره کارت رمزنگاری می‌شود و در طی انتقال یا جاهایی که ممکن است ذخیره شود (در پایگاه‌های داده، فایل‌های ثبت وقایع سامانه، پشتیبان‌گیری، چاپ رسید، و غیره) رمز شده باقی می‌ماند. همچنین دسترسی به اطلاعات و سامانه‌ها نیز محدود می‌شود. اگر فرد غیرمجازی به هر نحو به شماره کارت دست یابد، نقض محرمانگی رخ داده‌است.

نقض محرمانگی ممکن است اشکال مختلف داشته باشد. مثلاً اگر کسی از روی شانه شما اطلاعات محرمانه نمایش داده شده روی صفحه نمایش رایانه شما را بخواند. یا فروش یا سرقت رایانه لپ‌تاپ حاوی اطلاعات حساس. یا دادن اطلاعات محرمانه از طریق تلفن همه موارد نقض محرمانگی است.

یکپارچه بودن

یکپارچه بودن یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات نه فقط در حین انتقال بلکه در حال استفاده یا ذخیره شدن ویا نابودشدن نیز به صورت غیرمجاز تغییر داده شود. سامانه‌های امنیت اطلاعات به‌طور معمول علاوه بر محرمانه بودن اطلاعات، یکپارچگی آن را نیز تضمین می‌کنند.

قابل دسترس بودن

اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کار کردن و جلوگیری از اختلال در سامانه‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سامانه‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار، و ارتقاء سامانه در دسترس باقی می‌ماند. یکی از راه‌های از دسترس خارج کردن اطلاعات و سامانه اطلاعاتی درخواست‌های زیاد از طریق خدمات از سامانه اطلاعاتی است که در این حالت چون سامانه توانایی و ظرفیت چنین حجم انبوه خدمات دهی را ندارد از خدمات دادن به‌طور کامل یا جزئی عاجز می‌ماند.

قابلیت بررسی (کنترل دسترسی)

افراد مجاز در هر مکان و زمان که لازم باشد بتوانند به منابع دسترسی داشته باشند.

قابلیت عدم انکار انجام عمل

در انتقال اطلاعات یا انجام عملی روی اطلاعات، گیرنده یا فرستنده یا عمل‌کننده روی اطلاعات نباید قادر به انکار عمل خود باشد. مثلاً فرستنده یا گیرنده نتواند ارسال یا دریافت پیامی را انکار کند.

اصل بودن

در بسیاری از موارد باید از اصل بودن و درست بودن اطلاعات ارسالی و نیز فرستنده و گیرنده اطلاعات اطمینان حاصل کرد. در برخی موارد ممکن است اطلاعات رمز شده باشد و دستکاری هم نشده باشد و به خوبی به دست گیرنده برسد ولی ممکن است اطلاعات غلط باشد یا از گیرنده اصلی نباشد. در این حالت اگر چه محرمانگی، یکپارچگی و در دسترس بودن رعایت شده ولی اصل بودن اطلاعات مهم است.

کنترل دسترسی

برای حراست از اطلاعات، باید دسترسی به اطلاعات کنترل شود. افراد مجاز باید و افراد غیرمجاز نباید توانایی دسترسی داشته باشند. بدین منظور روش‌ها و تکنیک‌های کنترل دسترسی ایجاد شده‌اند که در اینجا توضیح داده می‌شوند.

دسترسی به اطلاعات حفاظت شده باید محدود باشد به افراد، برنامه‌های رایانه‌ای، فرایندها و سامانه‌هایی که مجاز به دسترسی به اطلاعات هستند. این مستلزم وجود مکانیزم‌های برای کنترل دسترسی به اطلاعات حفاظت شده می‌باشد. پیچیدگی مکانیزم‌های کنترل دسترسی باید مطابق با ارزش اطلاعات مورد حفاظت باشد. اطلاعات حساس تر و با ارزش تر نیاز به مکانیزم کنترل دسترسی قوی تری دارند. اساس مکانیزم‌های کنترل دسترسی بر دو مقوله **احراز هویت و تصدیق هویت** است.

احراز هویت تشخیص هویت کسی یا چیزی است. این هویت ممکن است توسط فرد ادعا شود یا ما خود تشخیص دهیم. اگر یک فرد می‌گوید «سلام، نام من علی است» این یک ادعا است. اما این ادعا ممکن است درست یا غلط باشد. پیش از اینکه به علی اجازه دسترسی به اطلاعات حفاظت شده داده شود ضروری است که هویت این فرد بررسی شود که او چه کسی است و آیا همانی است که ادعا می‌کند.

تصدیق هویت عمل تأیید هویت است. زمانی که «علی» به بانک می‌رود تا پول برداشت کند، او به کارمند بانک می‌گوید که او «علی» است (این ادعای هویت است). کارمند بانک کارت شناسایی عکس دار تقاضا می‌کند، و «علی» ممکن است گواهینامه رانندگی خود را ارائه دهد. کارمند بانک عکس روی کارت شناسایی با چهره «علی» مطابقت می‌دهد تا مطمئن شود که فرد ادعاکننده «علی» است. اگر عکس و نام فرد با آنچه ادعا شده مطابقت دارند تصدیق هویت انجام شده است.

از سه نوع اطلاعات می‌توان برای احراز و تصدیق هویت فردی استفاده کرد: چیزی که فرد می‌داند، چیزی که فرد دارد، یا کسی که فرد هست. نمونه‌هایی از چیزی که می‌داند شامل مواردی از قبیل کد، رمز عبور، یا نام فامیل پیش از ازدواج مادر فرد باشد. نمونه‌هایی از چیزی که دارد شامل گواهینامه رانندگی یا کارت مغناطیسی بانک است. کسی که هست اشاره به تکنیک‌های **بیومتریک** هستند. نمونه‌هایی از بیومتریک شامل اثر انگشت، اثر کف دست، صدا و اسکن عنبیه چشم هستند. احراز و تصدیق هویت قوی نیاز به ارائه دو نوع از این سه نوع مختلف از اطلاعات است. به عنوان مثال، چیزی که فرد می‌داند به علاوه آنچه دارد یعنی مثلاً ورود رمز عبور علاوه بر نشان دادن کارت مخصوص بانک. این تکنیک را احراز و تصدیق هویت دو عامله گویند که قوی تر از یک عامله (فقط کنترل **گذرواژه**) است.

در سامانه‌های رایانه‌ای امروزی، نام کاربری رایج‌ترین شکل احراز و رمز عبور رایج‌ترین شکل تصدیق هویت است. نام کاربری و **گذرواژه** به اندازه کافی به امنیت اطلاعات خدمت کرده‌اند اما در دنیای مدرن با سامانه‌های پیچیده‌تر از گذشته، دیگر کافی نمی‌باشند. نام کاربری و **گذرواژه** به تدریج با روش‌های پیچیده تری جایگزین می‌شوند.

پس از آنکه فرد، برنامه یا رایانه با موفقیت احراز و تصدیق هویت شد سپس باید تعیین کرد که او به چه منابع اطلاعاتی و چه اقداماتی روی آن‌ها مجاز به انجام است (اجرا، نمایش، ایجاد، حذف، یا تغییر). این عمل را **صدور مجوز** گویند.

صدور مجوز برای دسترسی به اطلاعات و خدمات رایانه‌ای با برقراری سیاست و روش‌های مدیریتی آغاز می‌شود. سیاست دسترسی تبیین می‌کند که چه اطلاعات و خدمات رایانه‌ای می‌تواند توسط چه کسی و تحت چه شرایطی دسترسی شود. مکانیزم‌های کنترل دسترسی سپس برای به اجرا درآوردن این سیاست‌ها نصب و تنظیم می‌شوند.

رویکردهای کنترل دسترسی مختلفی وجود دارند. سه رویکرد شناخته شده وجود دارند که عبارتند از: رویکرد صلاحیددی، غیرصلاحیددی و اجباری. در رویکرد صلاحیددی خالق یا صاحب منابع اطلاعات قابلیت دسترسی به این منابع را تعیین

می‌کند. رویکرد غیر صلاح‌حیدی همه کنترل دسترسی متمرکز است و به صلاح‌حید افراد نیست. در روش اجباری، دسترسی به اطلاعات یا محروم کردن بسته به طبقه‌بندی اطلاعات و رتبه فرد خواهان دسترسی دارد.

کنترل امنیت اطلاعات

کنترل امنیت به اقداماتی گفته می‌شود که منجر به حفاظت، پیشگیری، مقابله/واکنش، و به حداقل رساندن دامنه تهدیدات امنیتی در صورت بروز می‌شود. این اقدامات را می‌توان به سه دسته تقسیم کرد.

مدیریتی

کنترل مدیریتی (کنترل رویه‌ها) عبارتند از سیاست‌ها، رویه‌ها، استانداردها و رهنمودهای مکتوب که توسط مراجع مسئول تأیید شده‌است. کنترل‌های مدیریتی چارچوب روند امن کسب و کار و مدیریت افراد را تشکیل می‌دهد. این کنترل‌ها به افراد نحوه امن و مطمئن انجام کسب و کار را می‌گویند و نیز چگونه روال روزانه عملیات‌ها هدایت شود. قوانین و مقررات ایجاد شده توسط نهادهای دولتی یک نوع از کنترل مدیریتی محسوب می‌شوند چون به شرکت‌ها و سازمان‌ها نحوه امن کسب و کار را بیان می‌کنند. برخی از صنایع سیاست‌ها، رویه‌ها، استانداردها و دستورالعمل‌های مختص خود دارند که باید دنبال کنند مثل استاندارد امنیت داده‌های صنعت کارت‌های پرداخت (PCI-DSS) مورد نیاز ویزا و مستر کارت یا سامانه مدیریت امنیت اطلاعات ISMS. نمونه‌های دیگر از کنترل‌ها مدیریتی عبارتند از سیاست امنیتی شرکت‌های بزرگ، سیاست مدیریت رمز عبور، سیاست استخدام، و سیاست‌های انضباطی. کنترل‌های مدیریتی پایه‌ای برای انتخاب و پیاده‌سازی کنترل‌های منطقی و فیزیکی است. کنترل‌های منطقی و فیزیکی پیاده‌سازی و ابزاری برای اعمال کنترل‌های مدیریتی هستند.

منطقی

کنترل منطقی (کنترل فنی) به‌کارگیری نرم‌افزار، سخت‌افزار و داده‌ها است برای نظارت و کنترل دسترسی به اطلاعات و سامانه‌های رایانه‌ای. به عنوان مثال: **گذرواژه، دیوار آتش‌ها** ی شبکه و ایستگاه‌های کاری، سامانه‌های تشخیص نفوذ به شبکه، لیست‌های کنترل دسترسی و رمزنگاری داده‌ها نمونه‌هایی از کنترل منطقی می‌باشند.

فیزیکی

کنترل فیزیکی برای حفاظت و کنترل محیط کار و تجهیزات رایانه‌ای و نحوه دسترسی به آن‌ها است که جنبه فیزیکی دارند. به عنوان مثال: درب، قفل، گرمایش و تهویه مطبوع، آژیر دود و آتش، سامانه دفع آتش‌سوزی، دوربین‌ها مداربسته، موانع، حصارکشی، نیروی‌های محافظ و غیره.

امنیت شبکه و ارتباطات راه دور

امنیت اطلاعات و مدیریت ریسک

امنیت برنامه‌های کاربردی

کنترل تنظیمات (رمزنگاری)

در امنیت اطلاعات از رمزنگاری استفاده می‌شود تا اطلاعات به فرمی تبدیل شود که به غیر از کاربر مجاز کس دیگری نتواند از آن اطلاعات استفاده کند حتی اگر به آن اطلاعات دسترسی داشته باشد. اطلاعاتی که رمزگذاری شده تنها توسط کاربر مجازی که کلید رمزنگاری را دارد می‌تواند دوباره به فرم اولیه تبدیل شود (از طریق فرایند رمزگشایی). رمزنگاری برای حفاظت اطلاعات در حال انتقال (اعم از الکترونیکی یا فیزیکی) یا ذخیره شده‌است. رمزنگاری امکانات خوبی برای امنیت اطلاعات فراهم می‌کند از جمله روش‌های بهبود یافته تصدیق هویت، فشرده‌سازی پیام، امضای دیجیتال، قابلیت عدم انکار و ارتباطات شبکه رمزگذاری شده.

رمزنگاری اگر درست پیاده‌سازی نشود می‌تواند مشکلات امنیتی در پی داشته باشد. راه‌های رمزنگاری باید با به‌کارگیری استانداردهای پذیرفته شده که توسط کارشناسان مستقل و خبره بررسی دقیق شده انجام گیرد. همچنین طول و قدرت کلید استفاده شده در رمزنگاری بسیار مهم است. کلیدی ضعیف یا بسیار کوتاه منجر به رمزگذاری ضعیف خواهد شد. مدیریت کلید رمزنگاری موضوع مهمی است. رمزگذاری داده‌ها و اطلاعات و تبدیل کردن آن‌ها به شکل رمزگذاری شده، روش مؤثر در جلوگیری از انتشار اطلاعات محرمانه شرکت می‌باشد.

معماری و طراحی سامانه‌های امن

مسائل حقوقی مرتبط با امنیت اطلاعات

حراست فیزیکی

حراست فیزیکی دارایی‌ها عنصری است که در هر سامانه حسابداری وجود دارد. رایانه‌ها و اطلاعات و برنامه‌های موجود در این رایانه‌ها در حقیقت دارایی‌های با ارزش سازمان هستند. امنیت فیزیکی می‌تواند با اعمال کنترل‌های زیر به دست آید:

1. در صورت داشتن امکانات مالی به‌کارگیری سامانه امنیتی هشدار دهنده و دوربین مدار بسته

2. نگهداری و حفاظت و انبار کردن ابزارهای حاوی اطلاعات مثل دیسک‌ها و نوارها.

به دنبال روشی برای مدیریت امنیت اطلاعات

به دنبال جستجوی روشی به جز شیوه‌های سنتی امنیت شبکه IT شرکت آی‌بی‌ام و چند شرکت و سازمان IT شورای جدید حفاظت از اطلاعات را احداث کرده‌اند. هدف از این کار ایجاد روش‌هایی برای مقابله با هکرها و دیگر راه‌های دسترسی غیرقانونی به اطلاعات است. شرکت IBM در گزارشی اعلام کرد که این شورا برای تنظیم طرحی نوین برای محافظت و کنترل در اطلاعات شخصی و سازمانی افراد همه تلاش خود را به کار خواهد گرفت. استوارت مک‌آروین، مدیر بخش امنیت اطلاعات مشتری IBM می‌گوید: "بیشتر شرکت‌ها و همین‌طور افراد حقیقی کنترل و امنیت اطلاعات خود را به عنوان مسئله‌ای فرعی در نظر می‌گیرند و در کنار دیگر فعالیت‌های خود به آن می‌پردازند." به عقیده اعضای این شورا کنترل و نظارت بر اطلاعات به این معناست که چگونه یک شرکت در کنار ایجاد امکان بهره‌برداری از اطلاعات مجاز، محدودیت‌هایی را برای دسترسی و محافظت از بخش‌های مخفی تدارک می‌بیند. اعضای این شورا بر آن‌اند تا تعریفی جدید از مدیریت کنترل اطلاعات و سیاست‌های مربوط به آن ارائه دهند. هم‌چنین پیش‌بینی شده‌است که این راهکارها بخش مهمی را در زیربنای سیاست‌های IT داشته باشد. مک‌آروین می‌گوید: "ایده اولیه تشکیل این شورا در جلسات سه ماه یک‌بار و غیررسمی شرکت IBM با مشتریان و برخی شرکا شکل گرفت. ما با افرادی گفتگو می‌کردیم که با مشکلات ناامنی اطلاعات به شکل عینی روبه‌رو بودند. برای شرکت IBM و شرکای تجاری آن مشارکت مشتریان عاملی مؤثر در اصلاح و هماهنگی نرم‌افزارهای امنیتی موجود و طراحی نرم‌افزارهای جدید است. ما سعی می‌کنیم ابزارهای امنیتی IBM را با نیازهای مشتری آشتی دهیم. بسیاری از مشتریان شرکت که اکنون اعضای فعال این شورا را تشکیل داده‌اند، خود طرح پروژه‌های جدید برای کنترل خروج اطلاعات و مدیریت آن را تنظیم کرده‌اند. آن‌ها داوطلب شده‌اند که برای نخستین بار این روش‌ها را در مورد اطلاعات شخصی خود به کار گیرند. بدیهی است شرایط واقعی در مقایسه با وضعیت آزمایشی نتیجه بهتری دارد. رابرت گاریگ، مدیر ارشد بخش امنیتی بانک مونترآل و یکی از اعضای شورا، معتقد است اکنون زمان آن رسیده که شرکت‌ها روش‌های جدیدی را برای کنترل اطلاعات مشتریان خود به کار بگیرند او می‌گوید: "من فکر می‌کنم اکنون زمان مدیریت کنترل اطلاعات فرارسیده‌است." پیش از این بخش IT همه حواس خود را بر حفاظت از شبکه‌ها متمرکز کرده بود، اما اکنون اطلاعات به عنوان بخشی مستقل به محدودیت‌هایی برای دستیابی و هم‌چنین روش‌های مدیریتی نوین نیازمند است. این حوزه به کوششی چشمگیر نیازمند است. شرکت‌ها هر روز بیش از پیش با سرقت اطلاعات روبه‌رو هستند. هدف اصلی شورا ایجاد مدیریتی هوشمند و بی‌واسطه است. مسائل مورد توجه این شورا به ترتیب اهمیت عبارت‌اند از: "امنیت، حریم خصوصی افراد، پذیرش قوانین و برطرف کردن سوء تعبیرهایی که در مورد IT و وظایف آن وجود دارد." به نظر این شورا مشکل اصلی ناهماهنگی برنامه‌های بخش IT با فعالیت‌های شرکت و بی‌توجهی به ادغام این راهکارهاست. شرکت آمریکن اکسپرس و بانک جهانی، دانشگاه ایالتی کارولینای شمالی و ... از اعضای این شورا هستند

برنامه جامع امنیت تجارت الکترونیک

با وجود اینکه همه مزایایی که تجارت الکترونیک به همراه دارد، انجام تراکنش‌ها و ارتباطات آنلاین محملی بزرگتر برای سوء به‌کارگیری فناوری و حتی اعمال مجرمانه فراهم می‌کند. این مشکلات تنها مختص تجارت الکترونیک نیست و بخشی از مشکلات گسترده ایست که در سراسر جهان گریبانگیر سامانه‌های اطلاعاتی و رایانه‌ای هستند. هر ساله سازمان‌های بسیاری هدف جرائم مرتبط با امنیت اطلاعات، از حملات ویروسی گرفته تا کلاهبرداری‌های تجاری از قبیل سرقت اطلاعات حساس تجاری و اطلاعات محرمانه کارت‌های اعتباری، قرار می‌گیرند. چنین حملات امنیتی موجب میلیون‌ها دلار ضرر و اخلاف در فعالیت شرکت‌ها می‌شوند. بسیاری از گزارشگران و مشاوران هزینه خسارات مرتبط با نقائص امنیتی را تا میلیاردها دلار برآورد کرده‌اند. با اینحال آنچه مهم‌تر از صحت میزان این خسارات است، این واقعیت است که با افزایش کاربران سامانه‌های اطلاعاتی، دسترسی آسان به اطلاعات و رشد فزاینده کاربران مطلع (فنی) می‌توان به راحتی فرض کرد

که تعداد این سوء استفاده‌ها از فناوری و تهدیدهای امنیتی نیز به همین نسبت افزایش یابد. متأسفانه، از آنجا که بسیاری از شرکت‌ها دوست ندارند نفوذ به سامانه‌شان را تأیید و اطلاعاتشان در مورد این نفوذها و وسعت آن‌ها را با دیگران به اشتراک بگذارند، میزان دقیق خساراتی که شرکت‌ها از جرائم مرتبط با امنیت متحمل شده‌اند، را نمی‌توان بدست آورد. بی‌میلی به ارائه اطلاعات مربوط به نقائص امنیتی، از این ترس معمول ناشی می‌شود که اطلاع عموم از چنین نقایصی باعث بی‌اعتمادی مشتریان نسبت به توانایی شرکت در حفظ دارائی‌های خود می‌شود و شرکت با این کار مشتریان خود و در نتیجه سوددهی اش را از دست خواهد داد. از آنجایی که مصرف‌کنندگان امروزی نسبت به ارائه آن لاین اطلاعات مالی بی‌اعتماد اند، شرکت‌ها با تأیید داوطلبانه این واقعیت که قربانی جرائم مرتبط با امنیت شده‌اند، چیزی بدست نمی‌آورند. با هیجان‌ات رسانه‌ای که امروزه دور و بر اینترنت و قابلیت‌های آن وجود دارد، حفظ یک تصویر مثبت از امنیت تجارت الکترونیک در اذهان، دغدغه شماره یک بسیاری از شرکت‌ها است و برای بقاء و باقی ماندن در رقابت کاملاً ضروری است. نبود اطلاعات دست اول از موارد واقعی برنامه‌ریزی و مقابله با تهدیدهای امنیتی را بسیار مشکل‌تر کرده‌است اما با این وجود هم فناوری‌ها و روش‌های امنیت اطلاعات و فنون کلی مدیریتی در برنامه‌ریزی و حفاظت از منابع فناوری اطلاعات سازمان، در یک دهه گذشته پیشرفت قابل توجهی داشته‌اند. اکنون خبرگانی هستند که در حوزه امنیت سایبر تخصص پیدا کرده‌اند و راهکارهای زیادی برای حفاظت از فناوری‌های تجارت الکترونیک از مجرمین بالقوه فضای سایبر دارند. بسیاری از شرکت‌ها دریافته‌اند که برای موفقیت در تجارت الکترونیک، علاوه بر روش‌های امنیتی که برای حفاظت از منابع فناوری اطلاعات طراحی شده‌اند، نیازمند سرمایه‌گذاری و برنامه‌ریزی برای ایجاد یک برنامه جامع امنیت هستند تا بدان طریق از دارایی‌هایشان در اینترنت محافظت و از نفوذ مجرمین به سامانه‌هایشان که موجب خسارت دیدن فعالیت‌های تجارت الکترونیک آن‌ها می‌شود جلوگیری کنند. برنامه جامع امنیت تجارت الکترونیک شامل برنامه‌های حفاظتی که از فناوری‌های موجود (نرم‌افزار و سخت‌افزار)، افراد، برنامه‌ریزی راهبردی استفاده می‌کنند و برنامه‌های مدیریتی که برای حفاظت از منابع و عملیات تجارت الکترونیک شرکت طراحی و اجرا می‌شوند، است. چنین برنامه‌ای برای بقاء کلی فعالیت‌های تجارت الکترونیک شرکت حیاتی است و سازمان باید آن را به عنوان مؤلفه‌ای اساسی در راهبرد تجارت الکترونیک موفق به حساب آورد. موفقیت چنین برنامه‌هایی به حمایت کامل مدیران رده بالا و مشارکت کامل بخش فناوری اطلاعات و مدیریت در جهت درک تأثیرگذاری و محدودیت‌های برنامه است. علاوه بر این برای اطمینان از بروز بودن این برنامه و ابزارهای آن و هماهنگی با واپسین فناوری‌ها و فنون مدیریت، باید آن را به‌طور مداوم مورد ارزیابی و سنجش قرار داد.

ارزیابی عملیات تجارت الکترونیک

نخستین گام برای ایجاد یک برنامه جامع امنیت تجارت الکترونیک، انجام یک ارزیابی کامل از ارزش و اهمیت تجارت الکترونیک در موفقیت کلی اهداف و برنامه تجاری شرکت است. گام بعدی باید ارزیابی آسیب‌پذیری سامانه تجارت الکترونیک شرکت از هر دو جنبه تهدیدات داخلی و خطرات موجود خارجی است. شناخت آسیب‌پذیری‌های خارجی بسیار ساده‌تر از دیدن آسیب‌پذیری‌های خارجی است. با این وجود همه تلاش‌ها باید در راستای شناخت حوزه‌هایی باشد که سامانه از داخل مورد سوءاستفاده قرار می‌گیرد. این کار را می‌توان به خوبی با صحبت با کاربران سامانه و توسعه دهندگان انجام داد. علاوه بر این بسته‌های نرم‌افزاری بسیاری هم وجود دارند که می‌توانند توانایی نظارت بر استفاده کلی از سامانه و دسترسی داخلی به آن را دارند و می‌توانند تحلیل کاملی از فعالیت‌های مشکوک احتمالی کاربران داخلی ارائه دهند.

گام بعد ایجاد یک طرح مستمر تجارت الکترونیک است که به طور شفاف همه نقاط ضعف احتمالی، روش‌های جلوگیری و مقابله با آن‌ها و برنامه‌های محتمل برای ترمیم نفوذها و و تهدیدهای امنیتی است. بسیاری از شرکت‌ها تمایل دارند به خود بقبولانند که داشتن برنامه ضد ویروس و دیواره‌های آتش، برای حفاظت از سامانه‌هایشان کافی است. داشتن چنین نرم‌افزارهایی گام نخست خوبی است اما حتی با این وجود نیز سامانه‌های تجارت الکترونیک با نقاط ضعف زیر روبرو هستند:

1. آتش‌سوزی و انفجار،

2. خرابکاری عمدی در سخت‌افزار، نرم‌افزار یا داده‌ها و اطلاعات،

3. دزدیده شدن نرم‌افزار و سخت‌افزار،

4. نبود پرسنل کلیدی امنیت تجارت الکترونیک

5. نبود برنامه‌های کاربردی

6. نبود فناوری

7. نبود ارتباطات

8. نبود فروشندگان.

تهدیدها در هر یک از این حوزه‌ها باید به دقت ارزیابی و طرح‌های محتمل ترمیم باید با جزئیات کامل برای مقابله با هر کدام تهیه شود. علاوه بر این باید در طرح افراد مسئول مدیریت و تصحیح مشکلات به وجود آمده از این نقائص معین گردند. سپس، سازمان باید نرم‌افزارها و سخت‌افزارهایی که حفاظت از سامانه تجارت الکترونیک را بر عهده دارند را، ارزیابی کند. درک اینکه فناوری‌های مورد استفاده باید مناسب نیازهای شرکت بوده و برای همه تهدیدهای امنیتی احتمالی سطحی از محافظت را فراهم کنند از اهمیت بسزایی برخوردار است.

حوزه‌های بحرانی که با مورد توجه قرار گیرند عبارتند از: حساسیت داده‌ها و اطلاعات در دسترس، حجم ترافیک دسترسی و روش‌های دسترسی. امنیت تجارت (SSL (Secure Socket Layer یا SET (Secure Electronic Transaction) الکترونیک مبتنی بر فناوری باید با به‌کارگیری الگوی امنیت شامل لایه‌های مختلف امنیتی باشد. هدف نهایی امنیت مبتنی بر فناوری باید فراهم کردن صحت، یکپارچگی، پنهان کردن و غیرقابل رد بودن مؤثر باشد. بسیاری از شرکت‌ها،

در طول این مرحله ایجاد برنامه جامع امنیت تجارت الکترونیک از تجربه شرکت‌های دیگری که در زمینه ارزیابی سامانه‌های امنیتی مبتنی بر فناوری تخصص دارند، استفاده می‌کنند.

افراد

مهمترین مؤلفه هر برنامه امنیتی مؤثری افرادی هستند که آن را اجرا و مدیریت می‌کنند. نقائص امنیتی بیش از آن که ناشی از سامانه باشند، به وسیله کاربران سامانه و افرادی که مدیریت سامانه را بر عهده دارند، رخ می‌دهند. بیشتر مطالعات گذشته نشان داده‌اند تهدیدهای داخلی سامانه‌های تجارت الکترونیک اغلب بسیار مهم‌تر از تهدیدهای خارجی بوده‌اند. در

بسیاری از موارد مجرمانی که در نفوذ به سامانه موفق بوده‌اند، یا دانش پیشین از سامانه داشته یا دارای شریک جرمی در داخل شرکت بوده‌اند. مهم‌ترین ابزاری که مدیریت برای کاهش تهدید داخلی در اختیار دارد آموزش کاربران داخلی سامانه و پرسنل مدیریت آن در مورد نتیجه اخلاق در یکپارچگی و امنیت سامانه است. بسیاری از کاربران از این واقعیت که نفوذ به سامانه‌های اطلاعاتی جرم است و اخلاطگران تحت پیگرد قانونی قرار می‌گیرند، اطلاع دارند. شرکت، با آگاهی دادن به کاربران و ترساندن آن‌ها از عواقب این اعمال می‌تواند تا حد زیادی مانع آن‌ها گردد.

راهبرد

ایجاد یک برنامه راهبردی مؤثر و بی‌عیب اهمیت بسیاری در امنیت تجارت الکترونیک دارد. چنین راهبردی باید شامل هدف کلی برنامه جامعه امنیت تجارت الکترونیک، اهداف جزئی و محدوده آن باشد. این راهبرد باید در راستای راهبرد تجاری کلی تجارت الکترونیک شرکت باشد. یکی از اهداف جزئی این راهبرد می‌تواند حفاظت کامل از همه منابع تجارت الکترونیک شرکت و فراهم کردن امکان ترمیم هر اخلاق با حداکثر سرعت ممکن باشد. علاوه بر این این برنامه باید شامل منابع مورد نیاز برای پشتیبانی از اهداف جزئی و کلی در کنار قیود و محدودیت‌های برنامه راهبردی و همچنین حاوی منابع انسانی کلیدی، اجرای برنامه‌های امنیتی متفاوت در غالب بخشی از برنامه راهبردی باشد. ساختارهای مدیریتی و تصمیم‌سازان

مدیریت

موفقیت برنامه جامع امنیت تجارت الکترونیک در گروی مدیریت مؤثر چنین برنامه‌ای است. پشتیبانی مدیریت، از مدیران رده بالا آغاز و در همه سطوح ادامه می‌یابد. چنین برنامه‌ای در شرکت‌های بزرگ باید مستقیماً به وسیله یک مدیر ارشد و در شرکت‌های متوسط و کوچکتر به وسیله رئیس یا صاحب آن شرکت اداره و نظارت گردد. مسئولیت اصلی مدیر برنامه به روز نگه داشتن کامل برنامه، اجرای برنامه‌های آن و ارزیابی مجدد برنامه‌های موجود است.

بخشی از فعالیت‌های چنین فردی آموختن راهکارهای عملی مؤثر در برنامه امنیتی سایر سازمان‌هاست که می‌تواند آن را با مطالعه مقالات، کتب و مطالعات موردی منتشر شده بدست آورد.

مدرک CISSP

مدرک (Certified Information Systems Security Professional) مدرکی برای متخصصان امنیت است و کسب این مدرک مراحل دارد. این مدرک مستقل از هر نوع سخت‌افزار و نرم‌افزار خاص یک شرکت است و به عنوان یک عنصر کلیدی در ارزشیابی داوطلبان کار در موسسات بزرگ و سامانه‌های Enterprise شناخته می‌شود. افرادی که صاحب این مدرک باشند می‌توانند برای پست مدیریت شبکه‌های کوچک و بزرگ اطلاعاتی خود را معرفی کنند.

در سال ۱۹۸۹، چند سازمان فعال در زمینه امنیت اطلاعات کنسرسیومی را تحت نام (ISC)۲ بنا نهادند که هدف آن آرایه استانداردهای حفاظت از اطلاعات و آموزش همراه با آرایه مدرک مربوط به افراد آموزش دیده بود.

در سال ۱۹۹۲ کنسرسیوم مذکور اقدام به طرح مدرکی به نام CISSP نمود که هدف آن ایجاد یک سطح مهارت حرفه‌ای و عملی در زمینه امنیت اطلاعات برای افراد علاقه‌مند به آن بود.

اعتبار

این مدرک به دلیل این که بر خلاف سایر مدارک امنیتی، وابسته به محصولات هیچ شرکت خاصی نیست، قادر است به افراد متخصص امنیت، تبحر لازم را در طرح و پیاده‌سازی سیاست‌های کلان امنیتی اعطا نماید. اتخاذ تصمیمات اصلی و حیاتی برای برقراری امنیت، مسئله‌ای نیست که مدیران سطح بالای یک سازمان بزرگ آن را به عهده کارشناسان تازه‌کار یا حتی آن‌هایی که مدرک امنیت در پلتفرم کاری خاصی را دارند، بگذارند بلکه مهم آن است. که این قبیل مسئولیت‌ها به اشخاصی که درک کامل و مستقلی از مسائل مربوط به مهندسی اجتماعی دارند و می‌توانند در جهت برقراری امنیت اطلاعات در یک سازمان به ارائه خط مشی ویژه و سیاست امنیت خاص کمک‌کننده سپرده شود.

مراحل کسب مدرک

برای کسب مدرک CISSP، داوطلبان باید حداقل سه سال سابقه کاری مفید در یکی از زمینه‌های امنیتی اعلام شده توسط (ISC)² را داشته باشند. از ابتدای سال ۲۰۰۳ به بعد شرط مذکور به چهار سال سابقه کاری یا سه سال سابقه کار به علاوه یک مدرک دانشگاهی یا بین‌المللی در این زمینه تغییر یافت. زمینه‌های کاری امنیتی که انجمن (ISC)² داوطلبان را به داشتن تجربه در آن ترغیب می‌کند شامل ده مورد است که به آن عنوان **Common Body of Knowledge (CBK)** یا همان اطلاعات پایه در زمینه امنیت اطلاق می‌شود که این موارد عبارتند از:

1. سامانه‌های کنترل دسترسی

2. توسعه سامانه‌ها و برنامه‌های کاربردی

3. برنامه‌ریزی برای مقابله با بلاهای طبیعی و خطرات کاری

4. رمزنگاری

5. مسائل حقوقی

6. امنیت عملیاتی

7. امنیت فیزیکی

8. مدل‌ها و معماری امنیتی

9. تمرین‌های مدیریت امنیت

10. امنیت شبکه داده‌ای و مخابراتی

زمانی که داوطلب موفق به دریافت مدرک CISSP می‌شود، باید برای حفظ این مدرک همواره خود را در وضعیت مطلوبی از لحاظ سطح دانش علمی و عملی در مقوله‌های مورد نظر نگه دارد. هر دارنده این مدرک لازم است که هر سال برای تمدید گواهینامه خود، کارهایی را برای اثبات پشتکار و علاقه خود به مقوله امنیت انجام داده و موفق به کسب سالانه ۱۲۰ امتیاز (از لحاظ ارزش کارهای انجام شده از دید انجمن) شود. به این منظور انجمن، فعالیت‌های مختلفی را برای کسب امتیازات لازم به دارندگان مدرک پیشنهاد می‌کند. به عنوان مثال کسب یک مدرک معتبر در زمینه امنیت اطلاعات، فعالیت در

زمینه‌های آموزش مفاهیم امنیتی به متخصصان دیگر، استخدام شدن در شرکت‌های معتبر، چاپ مقالات در زمینه امنیت، شرکت در سمینارهای مهم و کنفرانس‌های مربوط به حوزه امنیت، داشتن تحقیقات شخصی و امثال آن می‌تواند دارندگان مدرک را در کسب امتیازات لازم یاری دهند. کلیه فعالیت‌های مذکور به صورت مستند و مکتوب تحویل نمایندگی‌های انجمن در سراسر دنیا شده تا مورد ارزشیابی و امتیازدهی انجمن قرار گیرد. در صورتی که دارنده مدرک موفق به کسب ۱۲۰ امتیاز نشود باید جهت حفظ مدرک خود دوباره آزمون CISSP را بگذرانند. CISSP شامل ۲۵۰ سؤال چهار گزینه‌ای است که کلیه مفاهیم امنیتی را در بر می‌گیرد. CISSP یکی از محبوبترین مدارک بین‌المللی در سال ۲۰۰۳ شناخته شده به طوری که با یک افزایش ۱۳۴ درصدی در بین داوطلبان نسبت به سال پیش روبه رو بوده است. همین آمار حاکی از موفقیت ۹۸ درصدی دارندگان مدرک در حفظ مدرک خود است. به هر حال با اوضاع و احوال امروزه دنیای فناوری اطلاعات و خطرات ناشی از حملات انواع ویروس‌ها و هکرها به نظر می‌رسد هر روز نیاز به وجود متخصصان امنیتی، خصوصاً دارندگان مدارک معتبر بین‌المللی بیشتر محسوس است. هم‌اکنون دو مدرک امنیتی یعنی SECURITY+ متعلق به انجمن کامپیتر و مدرک CISSP متعلق به انجمن بین‌المللی حرفه‌ای‌های امنیت از شهرت خاصی در این زمینه برخوردارند.

وضعیت درآمد

طبق آمار مجله certification میانگین درآمد سالانه دارندگان مدرک CISSP در سال ۲۰۰۴ نزدیک به ۸۶ هزار دلار بوده است این میزان درآمد در بین درآمد مدرک‌های مختلف که طبق همین آمارگیری بدست آمده نشان می‌دهد که مدرک CISSP در جایگاه اول قرار دارد. در این مقایسه مدرک Security+ با ۶۰ هزار دلار و مدرک MCP security MCSE با ۶۷ هزار دلار در سال در رده‌های دیگر این فهرست قرار دارند که همه نشان از اهمیت و در عین حال دشوار بودن مراحل کسب و نگهداری مدرک CISSP دارد.

جستارهای وابسته

ویکی‌بوکس دارای کتابی در ارتباط با موضوع: *عوامل‌های انسانی در امنیت اطلاعات* است.

منابع

• https://web.archive.org/web/20150801025640/http://idsco.ir/information_security_assey

برگرفته از «<https://fa.wikipedia.org/w/index.php?>

«[title=امنیت_اطلاعات&oldid=33452244](https://fa.wikipedia.org/w/index.php?title=امنیت_اطلاعات&oldid=33452244)»

آخرين ويرائش ۱۰ ماه پيش توسط Hujibot انجام شده

ويکي پدیا
