## تعریف امنیت اطلاعات

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

واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاها به اشتباه به جای هم بکاربرده 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 کرده اند دارد.

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

امنیت کامپیوتر در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم کامپیوتری تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می شود.

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 می شود.اگر اطلاعات محرمانه در مورد مشتریان و یا امور مالی یا محصول جدید موسسه ای به دست رقیب بیافتد، 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 معنی داری 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 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.

این مقاله یک دید کلی از امنیت اطلاعات و مفاهیم اصلی آن فراهم میکند.

## تاریخچه

از زمانی که نوشتن و تبادل اطلاعات آغاز شد، همه انسانها مخصوصا سران حکومتها و فرماندهان نظامی در پی راهکاری برای محافظت از محرمانه بودن مکاتبات و تشخیص دستکاری آنها بودند. ژولیوس سزار ۵۰ سال قبل از میلاد یک سیستم رمزنگاری مکاتبات ابداع کرد تا از خوانده شدن پیام‌های سری خود توسط دشمن جلوگیری کند حتی اگر پیام به دست دشمن بیافتد. جنگ جهانی دوم باعث پیشرفت چشمگیری در زمینه امنیت اطلاعات گردید و این آغاز کارهای حرفه ای در حوزه امنیت اطلاعات شد. پایان قرن بیستم و سالهای اولیه قرن بیست و یکم شاهد پیشرفتهای سریع در ارتباطات راه دور، سخت افزار، نرم افزار و رمزگذاری داده‌ها بود. در دسترس بودن تجهیزات محاسباتی کوچکتر، قوی تر و ارزان تر پردازش الکترونیکی داده‌ها باعث شد که شرکت های کوچک و کاربران خانگی دسترسی بیشتری به آنها داشته باشند. این تجهیزات به سرعت از طریق شبکه‌های کامپیوتر 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 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.

**مفاهیم پایه**

همانگونه که تعریف شد، امنیت اطلاعات یعنی حفظ محرمانگی، یکپارچه بودن و قابل دسترس بودن اطلاعات از افراد غیرمجاز. در اینجا مفاهیم سه گانه "محرمانگی"، "یکپارچه بودن" و "قابل دسترس بودن" توضیح داده میشود. در بین متخصصان این رشته بحث است که 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 غیر مجاز. 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 بیافتد 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 سیستم، پشتیبان گیری، چاپ رسید، و غیره) رمز شده باقی میماند. همچنین دسترسی به اطلاعات و سیستم‌ها نیز محدود میشود. اگر فردی غیر مجاز به شماره کارت به هر نحوی دست یابد، نقض محرمانگی رخ داده است.

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

## یکپارچه بودن

یکپارچه بودن یعنی جلوگیری از تغییر داده‌ها بطور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات. یکپارچگی وقتی نقض میشود که اطلاعات در حین انتقال بصورت غیرمجاز تغییر داده میشود. سیستم‌های امنیت اطلاعات به طور معمول علاوه بر محرمانه بودن اطلاعات، یکپارچگی آنرا 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 سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سیستم‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت افزار، و ارتقاء سیستم در دسترس باقی می ماند. یک از راههای از دسترس خارج کردن اطلاعات و سیستم اطلاعاتی درخواست بیش از طریق خدمات از سیستم اطلاعاتی است که در این حالت چون سیستم توانایی و ظرفیت چنین حجم انبوده خدمات دهی را ندارد از سرویس دادن بطور کامل یا جزیی عاجز میماند.

## قابلیت حسابرسی

در بسیاری موارد، باید امکانی در سیستم اطلاعاتی تعبیه شود تا بتوان انجام دهنده عملی روی اطلاعات را حسابرسی کرد. مثلا با ثبت دسترسی افراد میتوان فرد یا افرادی که به اطلاعات دست یافته اند را حسابرسی کرد.

## قابلیت عدم انکار انجام عمل

در انتقال اطلاعات و یا انجام عملی روی اطلاعات، گیرنده یا فرستنده و یا عمل کننده روی اطلاعات نباید قادر به انکار عمل خود باشد. مثلا 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 بعضی 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 و 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 شده اند که در اینجا توضیح داده میشوند.

دسترسی به اطلاعات حفاظت شده باید محدود باشد به افراد، برنامه‌های کامپیوتری، فرآیندها و سیستم هایی که مجاز به دسترسی به اطلاعات هستند. این مستلزم وجود مکانیزم‌های برای کنترل دسترسی به اطلاعات حفاظت شده می باشد. 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 و 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. قبل 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 تایید هویت است. زمانی که "علی" به بانک میرود تا پول برداشت کند، او به کارمند بانک می گوید که او "علی" است (این ادعای هویت است). کارمند بانک کارت شناسایی عکس دار تقاضا میکند، و "علی" ممکن است گواهینامه رانندگی خود را ارئه دهد. کارمند بانک عکس روی کارت شناسایی با چهره "علی" مطابقت میدهد تا مطمئن شود که فرد ادعا کننده "علی" است. اگر عکس و نام فرد با آنچه ادعا شده مطابقت دارند تصدیق هویت انجام شده است.

از سه نوع اطلاعات می توان برای احراز و تصدیق هویت فردی استفاده کرد: چیزی که فرد می داند، چیزی که فرد دارد، و یا کسی که فرد هست. نمونه هایی از چیزی که می داند شامل مواردی از قبیل کد، رمز عبور، و یا نام فامیل قبل از ازدواج مادر فرد باشد. نمونه هایی از چیزی که دارد شامل گواهینامه رانندگی یا کارت مغناطیسی بانک است. کسی که هست اشاره به تکنیک‌های بیومتریک هستند. نمونه هایی از بیومتریک شامل اثر انگشت، اثر کف دست، صدا و اسکن شبکیه 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 می داند به علاوه آنچه دارد یعنی مثلا 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 کلمه عبور) است.

در سیستم‌های کامپیوتری امروزی، نام کاربری رایج‌ترین شکل احراز و رمز عبور رایج‌ترین شکل تصدیق هویت است. نام کاربری و کلمه عبور به اندازه کافی به امنیت اطلاعات خدمت کرده اند اما در دنیای مدرن با

سیستم‌های پیچیده تر از گذشته، دیگر کافی نمی باشند. نام کاربری و کلمه عبور بـه تـدریج بـا روش‌هـای پیچیده تری جایگزین میشوند.

پس از آنکه فرد، برنامه یا کامپیوتر 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 عمـل را صدور مجوز گویند.

صدور مجوز برای دسترسی به اطلاعات و خدمات کامپیوتری با برقراری سیاست و روش‌های مـدیریتی آغـاز می شود. سیاست دسترسی تبیین میکند که چه اطلاعات و خدمات کامپیوتری می تواند توسط چه کسی و تحت چه شرایطی دسترسی شود. مکانیسم‌های کنترل دسترسی سپس برای به اجرا درآوردن این سیاست‌ها نصب و تنظیم میشوند.

رویکردهای کنترل دسترسی مختلفی وجود دارند. سه رویکرد شـناخته شـده وجـود دارنـد کـه عبارتنـد از: رویکرد صلاحدیدی، غیرصلاحدیدی و اجباری. در رویکرد صلاحدیدی خالق یا صاحب منابع اطلاعات قابلیت دسترسی به این منابع را تعیین میکند. رویکرد غیر صلاحدیدی تمام کنترل دسترسی متمرکـز اسـت و بـه صلاحدید افراد نیست. در روش اجباری، دسترسی به اطلاعات و یـا محـروم کـردن بسـته بـه طبقـه بنـدی اطلاعات و رتبه فرد خواهان دسترسی دارد.

کنترل امنیت اطلاعات

کنترل امنیت به اقداماتی گفته میشود که منجر به حفاظـت، مقابلـه، پیشـگیری و یـا بـه حـداقل رسـاندن خطرات امنیتی است. این اقدامات را میتوان به سه دسته تقسیم کرد.

## مدیریتی

کنترل مدیریتی ( کنترل رویه ها) عبارتند از سیاست ها، رویه ها، اسـتانداردها و رهنمودهـای مکتـوب کـه توسط مراجع مسئول تایید شده است. کنترل‌های مدیریتی چارچوب روند امن کسب و کار و مدیریت افـراد را تشکیل میدهد. این کنترل‌ها به افراد نحوه امن و مطمئن انجام کسب و کار را میگویند و نیز چگونـه 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 سیاست ها، رویه ها، استانداردها و دستورالعمل‌های مختص خود دارند که باید دنبال کننـد مثـل اسـتاندارد امنیـت داده‌های صنعت کارتهای پرداخت (PCI-DSS) مورد نیاز ویزا و مستر کارت. نمونه‌هـای دیگـر از کنتـرل‌هـا مدیریتی عبارتند از سیاست امنیتی شرکت‌های بزرگ، سیاست مـدیریت رمـز عبـور، سیاسـت اسـتخدام، و سیاست‌های انضباطی. کنترل‌های مدیریتی پایه ای برای انتخاب و پیاده سازی کنترل‌های منطقی و فیزیکی است. کنترل‌های منطقی و فیزیکی پیاده سازی و ابزاری برای اعمال کنترل‌های مدیریتی هستند.

## منطقی

کنترل منطقی (کنترل فنی) استفاده از نرم افزار، سخت افزار و داده‌ها است برای نظارت و کنترل دسترسی به اطلاعات و سیستم‌های کامپیوتری. به عنوان مثال : کلمه عبور، فایروال‌ها ی شبکه و ایستگاههای کاری، سیستم‌های تشخیص نفوذ به شبکه، لیست‌های کنترل دسترسی و رمزنگاری داده‌ها نمونه هایی از کنترل منطقی می باشند.

## فیزیکی

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

امنیت شبکه و ارتباطات راه دور

امنیت اطلاعات و مدیریت ریسک

امنیت برنامه‌های کاربردی

## 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 رمز نگاری را دارد میتواند دوباره به فرم اولیه تبدیل شود(از طریق فرایند رمزگشایی). رمزنگاری برای حفاظت اطلاعات در حال انتقال (اعم از الکترونیکی و یا فیزیکی) و یا ذخیره شده است. رمزنگاری امکانات خوبی برای امنیت اطلاعات فراهم می کند از جمله روش‌های بهبود یافته تصدیق هویت، فشرده سازی پیام، امضاهای دیجیتالی، قابلیت عدم انکار و ارتباطات شبکه رمزگذاری شده.

رمزنگاری اگر درست پیاده سازی نشود می تواند مشکلات امنیتی در پی داشته باشد. راه حل‌های رمز نگاری باید با استفاده از 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 خیلی کوتاه منجر به رمزگذاری ضعیف خواهد شد. مدیریت کلید رمزنگاری موضوع مهمی است.

معماری و طراحی سیستم‌های امن

مسائل حقوقی مرتبط با امنیت اطلاعات

## حراست فیزیکی

به دنبال روشی برای مدیریت امنیت اطلاعات

به دنبال جست‌وجوی روشی به‌جز شیوه‌های سنتی امنیت شبکهٔ 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 همهٔ تلاش خود را به کار خواهد گرفت. استوارت مک‌ایروین، 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 عقیدهٔ اعضای این شورا کنترل و نظارت بر اطلاعات به این معناست که چه‌گونه یک شرکت در کنار ایجاد امکان بهره‌برداری از اطلاعات مجاز، محدودیت‌هایی را برای دست‌رسی و محافظت از بخش‌های مخفی تدارک می‌بینند. اعضای این شورا برآن‌اند تا تعریفی جدید از مدیریت کنترل اطلاعات و سیاست‌های مربوط به آن ارایه دهند. هم‌چنین پیش‌بینی شده است که این راهکارها بخش مهمی را در زیربنای سیاست‌های IT داشته باشد. مک‌آروین می‌گوید: "ایدهٔ اولیهٔ تشکیل این شورا در جلسات سه ماه یک‌بار و غیررسمی شرکت IBM با مشتریان و برخی شرکا شکل گرفت. ما با افرادی گفت‌وگو می‌کردیم که با مشکلات ناامنی اطلاعات به شکل عینی روبه‌رو بودند. برای شرکت IBM و شرکای تجاری آن مشارکت مشتریان عاملی موثر 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 آن‌را تنظیم کرده‌اند. آن‌ها داوطلب شده‌اند که برای اولین بار این روش‌ها را در مورد اطلاعات شخصی خود به کار گیرند. بدیهی است شرایط واقعی در مقایسه با وضعیت آزمایشی نتیجهٔ 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 به‌کار بگیرند او می‌گوید: "من فکر می‌کنم اکنون زمان مدیریت کنترل اطلاعات فرارسیده است." پیش از این بخش IT تمام 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 تمام مزایایی که تجارت الکترونیک بهمراه دارد، انجام تراکنش‌ها و ارتباطات آنلاین محملی بزرگتر برای سوء استفاده از 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 سیستم‌های اطلاعاتی و کامپیوتری هستند. هر ساله سازمان‌های بسیاری هدف جرائم مرتبط با امنیت اطلاعات، از حملات ویروسی گرفته تا کلاه برداری‌های تجاری از قبیل سرقت اطلاعات حساس تجاری و اطلاعات محرمانه کارت‌های اعتباری، قرار می‌گیرند. چنین حملات امنیتی موجب میلیون‌ها دلار ضرر و اخلال در فعالیت شرکت‌ها می‌شوند. بسیاری از گزارشگران و مشاوران هزینه خسارات مرتبط با نقائص امنیتی را تا میلیاردها دلار برآورد کرده اند. با اینحال آنچه مهمتر از صحت میزان این خسارات است، این واقعیت است که با افزایش کاربران سیستم‌های 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. متاسفانه، از آنجا که بسیاری از شرکت‌ها دوست ندارند نفوذ به سیستمشان را تایید 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 شده اند، را نمی‌توان بدست آورد. بی میلی به ارائه اطلاعات مربوط به نقائص امنیتی، از این ترس معمول ناشی می می‌شود که اطلاع عموم از چنین نقائصی باعث بی اعتمادی مشتریان نسبت به توانایی شرکت در حفظ داراییهای خود می‌شود و شرکت با این کار مشریان خود و در نتیجه سوددهی اش را از دست خواهد داد. از آنجایی که مصرف کنندگان امروزی نسبت به ارائه آن لاین اطلاعات مالی بی اعتماد اند، شرکت ها با تایید داوطلبانه این واقعیت که قربانی جرائم مرتبط با امنیت شده اند، 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 کاملا ضروری است. نبود اطلاعات دست اول از موارد واقعی برنامه ریزی و مقابله با تهدیدهای امنیتی را بسیار مشکلتر کرده است اما با این وجود هم فناوری‌ها و روشهای امنیت اطلاعات و فنون کلی مدیریتی در برنامه ریزی و حفاظت از منابع فناوری اطلاعات سازمان، در یک دهه گذشته پیشرفت قابل توجهی داشته اند. اکنون خبرگانی هستند که در حوزه امنیت سایبر تخصص پیدا کرده اند و راهکارهای زیادی برای حفاظت از فناوری‌های تجارت الکترونیک از مجرمین بالقوه فضای سایبر دارند. بسیاری از شرکت‌ها دریافته اند که برای موفقیت در تجارت الکترونیک، علاوه بر روشهای امنیتی که برای حفاظت از منابع فناوری اطلاعات طراحی شده اند، نیازمند سرمایه گذاری و برنامه ریزی برای ایجاد یک برنامه جامع امنیت هستند تا بدان طریق از داراییهایشان در اینترنت محافظت و از نفوذ مجرمین به سیستم هایشان 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)، افـراد، برنامه ریزی راهبردی استفاده می‌کنند و برنامه‌های مدیریتی که برای حفاظت از منـابع و عملیـات تجـارت الکترونیک شرکت طراحی و اجرا مـی‌شـوند، اسـت.چنین برنامـه‌ای بـرای بقـاء کلـی فعالیـت‌هـای تجـارت الکترونیک شرکت حیاتی است و سازمان باید آنرا به عنوان مولفه‌ای اساسـی در راهبـرد تجـارت الکترونیـک موفق به حساب آورد.موفقیت چنین برنامه‌هایی به حمایت کامل مدیران رده بـالا و مشـارکت کامـل بخـش فناوری اطلاعات و مدیریت در جهت درک تاثیر گذاری و محدودیت‌هـای برنامـه اسـت.علاوه بـر ایـن بـرای اطمینان از بروز بودن این برنامه و ابزارهای آن و هماهنگی با آخرین فناوری‌ها و فنون مـدیریت، بایـد آن را بطور مداوم مورد ارزیابی و سنجش قرار داد.

## ارزیابی عملیات تجارت الکترونیک

اولین گام برای ایجاد یک برنامه جامع امنیت تجارت الکترونیک، انجام یک ارزیابی کامل از ارزش و اهمیـت تجارت الکترونیک در موفقیت کلی اهداف و برنامه تجاری شرکت است.گام بعدی باید ارزیابی آسیب پـذیری سیستم تجارت الکترونیک شرکت از هر دو جنبهٔ تهدیات داخلی و خطرات موجود خـارجی است.شـناخت آسیب پذیریهای خارجی بسیار ساده تر از دیدن آسیب پذیری‌های خارجی است.با این وجود تمام تـلاش‌هـا باید در راستای شناخت حوزه‌هایی باشد که سیستم از داخل مـورد سوءاسـتفاده قـرار مـی‌گیـرد.این کـار را می‌توان به خوبی با صحبت با کاربران سیستم و توسعه دهندگان انجام داد.علاوه بر این بسته‌های نرم‌افـزاری بسیاری هم وجود دارند که می‌توانند توانایی نظارت بر استفاده کلی از سیستم و دسترسی داخلـی بـه آن را دارند و می‌توانند تحلیل کاملی از فعالیت‌های مشکوک احتمالی کاربران داخلی ارائه دهند.

## طرح مستمر

گام بعد ایجاد یک طرح مستمر تجارت الکترونیک است که بطور شفاف تمام نقاط ضعف احتمالی، روشـهای جلوگیری و مقابله با آنها و برنامه‌های محتمل برای ترمیم نفوذها و و تهدیـدهای امنیتـی اسـت. بسـیاری از شرکت‌ها تمایل دارند به خود بقبولانند که داشتن برنامه ضد ویروس و دیواره‌هـای آتـش، بـرای حفاظـت از سیستم هایشان کافی است. داشتن چنین نرم‌افزارهایی گام نخست خوبی است اما حتی بـا ایـن وجـود نیـز سیستم‌های تجارت الکترونیک با نقاط ضعف زیر روبرو هستند:

آتش سوزی و انفجار،

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

دزدیده شدن نرم‌افزار و سخت‌افزار،

فقدان پرسنل کلیدی امنیت تجارت الکترونیک

فقدان برنامه‌های کاربردی

فقدان فناوری

فقدان ارتباطات

فقدان فروشندگان.

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

حوزه‌های بحرانی که با مورد توجه قرار گیرند عبارتند از : حساسیت داده‌ها و اطلاعـات در دسـترس، حجـم ترافیک دسترسی و روشهای دسترسی.امنیت تجارت Socket Layer SSL (Secure) یا SET (Secure Electronic Transaction)الکترونیک مبتنی بر تکنولوژی باید با استفاده از الگوی امنیت شامل لایه‌های مختلف امنیتی باشد.هدف نهایی امنیت مبتنی بر فناوری باید فراهم کردن صحت، یکپارچگی، پنهان کـردن و غیر قابل رد بودن موثر باشد.بسیاری از شرکت‌ها ،

در طول این مرحله ایجاد برنامه جامع امنیت تجارت الکترونیک از تجربه شرکت‌های دیگـری کـه در زمینـه ارزیابی سیستم‌های امنیتی مبتنی بر فناوری تخصص دارند، استفاده می کنند.

## افراد

مهمترین مولفه هر برنامه امنیتی موثری افرادی هستند که آنرا اجرا و مدیریت می‌کنند.نقائص امنیتی بیش از آنگه ناشی از سیستم باشند، به وسیلهٔ افرادی که مدیریت سیستم را برعهده دارند و کاربران سیستم رخ می‌دهند.بیشتر مطالعات گذشته نشان داده اند تهدیدهای داخلی سیستم‌های تجارت الکترونیک اغلب بسیار مهمتر از تهدیدهای خارجی بوده اند.در بسیاری از موارد مجرمانی که در نفوذ به سیستم بوده اند یـا دانـش قبلی از سیستم داشته اند و یا شریک جرمی در داخل شرکت.مهمترین ابـزاری کـه مـدیریت بـرای کـاهش تهدید داخلی در اختیار دارد آموزش کاربران داخلی سیستم و پرسنل مدیریت آن در مورد نتیجه اخـلال در یکپارچگی و امنیت سیستم است.بسیاری از کاربران از این واقعیت که نفوذ به سیستم‌هـای اطلاعـاتی جـرم است و اخلالگران تحت پیگرد قانونی قرار مـی‌گیرنـد، اطـلاع دارند.شـرکت، بـا آگـاهی دادن بـه کـاربران و ترساندن آنها از عواقب این اعمال می‌تواند تا حد زیادی مانع آنها گردد.

## راهبرد

ایجاد یک برنامه راهبردی موثر و بی عیب اهمیت بسیاری در امنیت تجارت الکترونیک دارد.چنین راهبردی باید شامل هدف کلی برنامه جامعه امنیت تجارت الکترونیک، اهداف جزئی و محـدوده آن باشـد.این راهبـرد باید در راستای راهبرد تجاری کلی تجارت الکترونیک شرکت باشد.یکی از اهداف جزئی این راهبرد می‌توانـد

حفاظت کامل از تمامی منابع تجارت الکترونیک شرکت و فراهم کردن امکان ترمیم هر اخلال 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 تصمیم سازان

## مدیریت

موفقیت برنامه جامع امنیت تجارت الکترونیک در گروی مدیریت موثر چنین برنامه‌ای است.پشتیبانی مدیریت، از مدیران رده بالا شروع و در تمام سطوح ادامه می‌یابد.چنین برنامه‌ای در شرکت‌های بزرگ باید مستقیما بوسیله یک مدیر ارشد و در شرکت‌های متوسط و کوچکتر بوسیله 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 موثر در برنامه امنیتی سایر سازمانهاست که می‌تواند آنرا با مطالعه مقالات، کتب و مطالعات موردی منتشر شده بدست آورد.

مدرک CISSP

مدرک (Information Systems Security Professional Certified) مدرکی برای متخصصان امنیت است وکسب این مدرک مراحلی 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 سیستم‌های 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 زمینهٔ امنیت اطلاعات کنسرسیومی را تحت نام ۲(ISC) بنا نهادند که هدف ان ارایهٔ استانداردهای حفاظت از اطلاعات و آموزش همراه با ارایهٔ 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 زمینهٔ امنیت اطلاعات برای افراد علاقمند 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 پیاده سازی 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 عهدهٔ کارشناسان تازه کار 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 ارایه خط مشی ویژه و سیاست امنیت خاص کمک کننده 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 ۲(ISC) را داشته باشند . از ابتدای سال۲۰۰۳ به بعد شرط مذکور به چهار سال سابقه کاری یا سه سال سابقه کار به علاوهٔ یک مدرک دانشگاهی یا بین‌المللی در این زمینه تغیر یافت .زمینه‌های کاری امنیتی که انجمن ۲(ISC) داوطلبان را به داشتن تجربه در آن ترغیب می‌کند شامل ده مورد است کهبه آن عنوان (Common Body Of Knowlege) CBKیا همان اطلاعات پایه در زمینهٔ امنبیت اطلاق می‌شود این موارد عبارتنداز:

سیستم‌های کنترل دسترسی

توسعه سیستم‌ها وبرنامه‌های کاربردی

برنامه ریزی برای مقابله با بلاهای طبیعی وخطرات کاری

رمزنگاری

مسا ئل حقوقی

امنیت عملیاتی

امنیت فیزیکی

مدلهاومعماری امنیتی

تمرین‌های مدیریت امنیت

امنیت شبکهٔ 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 وعملی در مقوله‌های مورد نظر نگه دارد .هر دارندهی این مدرک لازم است که هرسال برای تمدید گواهینامهٔ خود، کارهایی را برای اثبات پشتکار وعلاقهٔ خود به مقولهٔ امنیت انجام داده وموفق به کسب سالانه ۱۲۰ امتیاز (از لحاظ ارزش کارهای انجام شده از دید انجمن ) شود. به این منظور انجمن، فعالیت‌های مختلفی را برای کسب امتیاز ات لازم به دارندگان مدرک پیشنهاد می‌کند. به عنوان مثال کسب یک مدرک معتبر در زمینهٔ امنیت اطلاعات، فعالیت در زمینه‌های آموزش مفاهیم امنیتی به متخصصان دیگر، استخدام شدن درشرکت‌های معتبر، چاپ مقالات در زمینهٔ امنیت، شرکت در سمینارهای مهم وکنفرانس‌های مربوط به حوزهٔ امنیت، داشتن تحقیقا ت شخصی وامثال آن می‌توانند دارندگان مدرک را در کسب امتیازات لازم یاری دهند . کلیهٔ 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 دارندهٔ مدرک موفق به کسب ۱۲۰ امتیاز نشود باید جهت حفظ مدرک خود دوباره آزمون CISSP را بگذراند. CISSP شامل ۲۵۰ سئوال چهار گزینه‌ای است که کلیهٔ 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 قبل روبه رو بوده‌است .همین آمار حاکی از موفقیت ۹۸ درصدی دارندگان مدرک در حفظ مدرک خود است . به هر حال با اوضاع و احوال امروزهٔ دنیای فناوری اطلاعات وخطرات ناشی از حملات انواع ویروس‌ها و هکرها به نظر می‌رسد هر روز نیاز به وجود متخصصان امنیتی، خصوصا دارندگان مدارک معتبر بین‌المللی بیشتر محسوس است. هم اکنون دو مدرک امنیتی یعنی SECURITY+ متعلق به انجمن کامپتیا و مدرک CISSP متعلق به انجمن بین‌المللی حرفه‌ای‌های امنیت از شهرت خاصی در این زمینه برخوردارند.

## وضعیت درآمد

طبق آمار مجلهٔ certification میانگین درآمد سالانهٔ 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 MCSE securityMCP با ۶۷ هزار دلار در سال در رده‌های دیگر این فهرست قرار دارند که همه نشان از اهمیت ودر عین حال دشوار بودن مراحل کسب و نگهداری مدرک CISSP دارد.