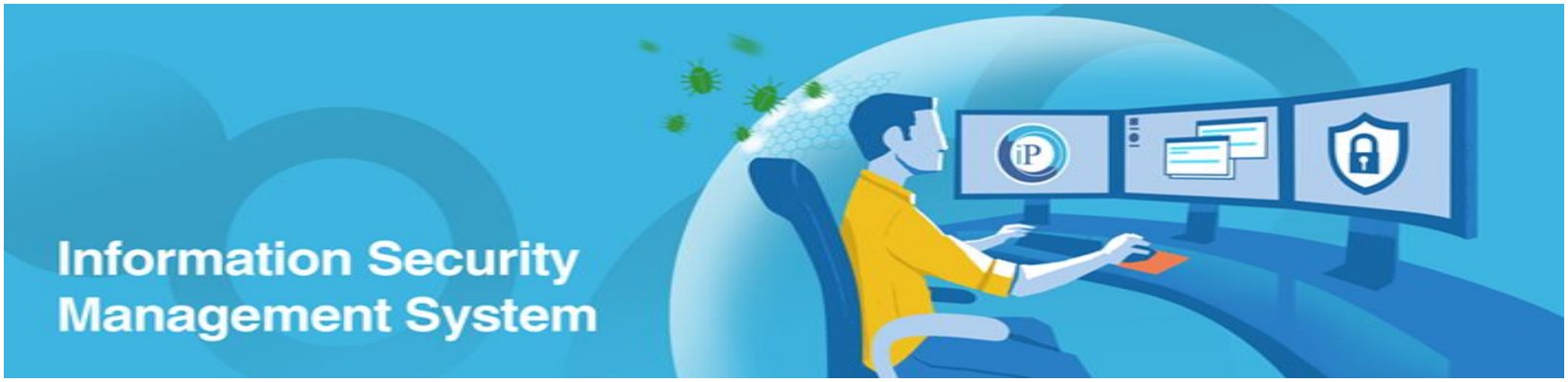
دوره آموزشی : مدیریت امنیت اطلاعات
۱۴ ساعت
موسسه تخصصی اورانوس
www.eduoranos.ir

با مجوز رسمی از سازمان مدیریت و برنامه ریزی

ISMSچیست ؟
سیستم مدیریت امنیت اطلاعات چیست ؟

موسسه تخصصی اورانوس
www.eduoranos.ir

- قبل از توضیح این موارد یک پاراگراف با شما صحبت داریم . ایـن روزهـا در ایـران در حوزه امنیت اطلاعات و ارتباطات یک بحث بسیار داغ اسـت و آن چیـزی نیسـت جـز سیستم مدیریت امنیت اطلاعات یا چیزی که ما به عنوان ISMSمی شناسیم . ایـن سیستم امروزه به شکل یک تب در بین سازمان های دولتی در آمده اسـت و بسـیاری از سازمان ها و شرکت ها بایستی به سراغ این سیستم بروند.



- این دقیقا همان مشکلی است که در خصوص سیستم مدیریت کیفیت یا ISO 9000نیز پیش آمد. از اینها که بگذریم برویم به سراغ اصل سیستم مدیریت امنیت اطلاعات و چیستی آن ، در ابتدا واژه سیستم را تعریف می کنیم و کلیات موضوع سیستم مدیریت امنیت اطلاعات و اجزاء آن را برای شما شرح خواهیم داد پس تا آخر با ما باشید.

تعریف سیستم یا Systemو استاندارد

- سیستم به معنی مجموعه ای از اجزاء است که برای رسیدن به هدف خاصی در کنار هم جمع شده اند. در واقع سیستم مدیریت امنیت اطلاعات نیز از مجموعه ای از اجزاء تشکیل شده است که برای رسیدن به هدف خاصی که در اینجا برقراری و مدیریت امنیت اطلاعات سازمان یا شرکت شما می باشد در کنار هم جمع شده اند. سیستم مدیریت امنیت یک ساختار استاندارد و تعریف شده است و این بدین معنا می باشد که ما به خودی خود نمی توانیم تعیین کنیم چگونه اطلاعات بایستی امن شوند و یک معیار و پایه و اساس برای اینکار بایستی تعریف شود.

- تعریف کردن این معیارها بر عهده یک سازمان بین المللی است که استانداردها در آن تهیه و تنظیم می شوند و این سازمان جایی نیست به غیر از سازمان ISOیا International Standardization Organization، این سازمان وظیفه تدوین استاندارد های یکپارچه در دنیا را بر عهده دارد ، تا به حال هر استانداردی که شنیده اید در این سازمان تعریف و تدوین شده است ، قطعا با ISO 9000یا استاندارد کیفیت کالا آشنایی دارید ، همین نوع استاندارد برای مدیریت سیستم امنیت اطلاعات با کد ISO 27000تعریف شده است که در ادامه با آن آشنا خواهید شد.

ساختار یک استاندارد به چه شکل است ؟

- همه استانداردها ساختاری شبیه به هم دارند اما از نظر محتوایی متفاوت هستند. در همه استانداردهای بین المللی ISOیک سری کنترل وجود دارد که بیانگر معیارهایی است که برای پیاده سازی استانداردها مورد نیاز است ، برای مثال یکی از کنترل های سیستم مدیریت امنیت اطلاعات این است که بایستی بر روی امنیت فیزیکی درب های ورود و خروج ساختمان کنترل انجام شود. بنابراین کنترل ها معیار را برای ما تشریح می کنند اما چگونگی انجام شدن آن را تعریف نمی کنند و این یک اصل است. هر استانداردی برای خود دارای یک سری کنترل است که در قالب سرفصل هایی ارائه می شوند.

- همیشه در تمامی سازمان ها لازم نیست تمامی این معیارها رعایت شود تا بتوانید سیستم مدیریتی خود را پیاده سازی کنید ، شما بر حسب سرویس و نیازی که دارید از بین این کنترل ها ، آنهایی که در محیط شما قابل استفاده هستند را انتخاب و شروع به پیاده سازی می کنید. اما بعد از اینکه شما از بین کنترل های موجود ، آنهایی که مورد نیازتان هستند را انتخاب کردید ، بایستی آنها را بصورت مدون و مرتب تشریح کنید و بر حسب نیاز خودتان آن را بهینه سازی و تدوین کنید .

- بعد از اینکه تمامی این مراحل انجام شد یک مستند متنی به وجود می آید که به آن خط مشی یا Policyگفته می شود و شما ساختار استاندارد سازمان را بر اساس آن تعریف می کنید. خط مشی امنیت اطلاعات که به بیانیه امنیت اطلاعات نیز معروف است در واقع الگوی اصلی است که شما در حوزه امنیت اطلاعات برای سازمان خود تدوین می کنید تا بر اساس آن امنیت اطلاعات خود را مدیریت کنید. توجه کنید که در این مستند چگونگی برقراری امنیت تشریح نشده است ، چگونگی انجام و پیاده سازی امنیت در مستندی جداگانه به نام دستورالعمل امنیت اطلاعات تشریح می شود.

فواید استفاده از سیستم مدیریت امنیت اطلاعات ISMSچیست ؟

- طبیعی است که شما زمانیکه به یک کشور خارجی سفر می کنید یکی از مهمترین معیارها برقرار بودن امنیت در آن کشور است ، همین موضوع باعث ترقیب شدن توریست ها برای سفر کردن و سرمایه گذاری در آن کشور می شود . در خصوص سازمان ها هم به همین شکل است ، اگر سازمانی بتواند سیستم مدیریت امنیت اطلاعات را به درستی پیاده سازی و مدیریت کند تجارتی دائمی و همراه با ریسک کمتر خواهد داشت ، تصور کنید شخصی قصد سرمایه گذاری در یک شرکت را دارد.

- اگر این شرکت که در کار تولید مواد اولیه رنگ پلاستیک است فرمول ساخت رنگ را به درستی امن نگاه ندارد و رقیبان تجاری آن فرمول را بدست بیاورند این شرکت دچار تهدید و در نهایت ممکن است بازار کار خود را از دست بدهد ، بنابراین سیستم مدیریت امنیت اطلاعات ISMS بصورت کلی باعث اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها می شود.پیاده سازی سیستم مدیریت امنیت اطلاعات علاوه بر موارد بالا می تواند باعث اطمینان از سازگاری با استانداردهای امنیت اطلاعات و محافظت از داده ها ، قابل اطمینان کردن تصمیم گیری ها و محک زدن سیستم مدیریت امنیت اطلاعات ، ایجاد اطمینان نزد مشتریان و شرکای تجاری ،امکان رقابت بهتر با سایر شرکت ها و ایجاد مدیریت فعال و پویا در پیاده سازی امنیت داده ها و اطلاعات شود.

سیستم مدیریت امنیت اطلاعات یا ISMSشامل چه مستنداتی است ؟

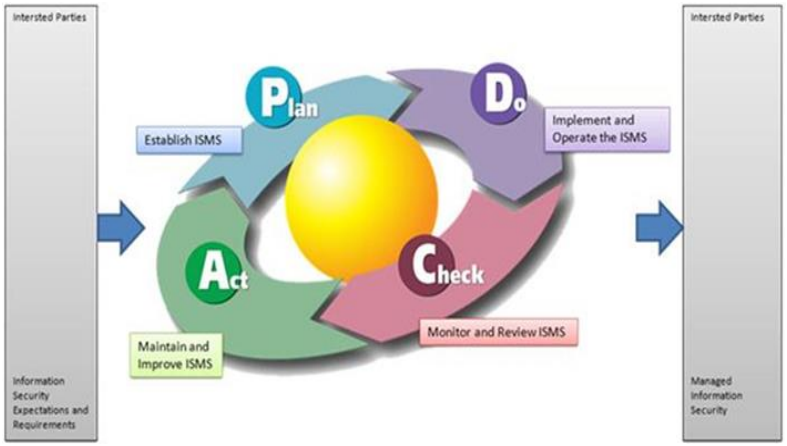
- همانطور که اشاره کردیم ، سیستم مدیریت امنیت اطلاعات به خودی خود یک مستند متنی است که بایستی بر اساس آن سازمان ها ساختار خود را پیاده سازی کنند. در ادامه گفتیم که از بین کنترل های موجود بایستی کنترل های متناسب با سازمان خود را انتخاب کنیم و مستند متنی به عنوان خط مشی امنیت تدوین کنیم. در نهایت پیاده سازی سیستم مدیریت امنیت اطلاعات منجر به تولید چندین مستند متنی می شود که به نوع می توان گفت ISMS دارای کاغذ بازی زیادی است. اما این مستندات چه هستند و چند نوع از این مستندات بایستی در یک ساختار مدیریت امنیتی درست وجود داشته باشد ؟

•مشکلات معمول در پیاده سازی سیستم مدیریت امنیت اطلاعات ISMS

- •بایستی توجه کرد که امنیت یک فرهنگ است قبل از آنکه یک فناوری باشد. براین اساس پیاده سازی مدیریت امنیت قبل ازخرید تجهیزات امنیتی توصیه می گردد. وقتی امنیت فرهنگ باشد عمری لازم است تا یک فرهنگ ایجاد شود و جا بیفتد. وقتی امنیت فرهنگ باشد نمی توان فرهنگ سازی سازمانی بومی شده در یک کشور پیشرفته اروپایی را به سادگی در یک مرحله ضربتی به یک سازمان دیگر وارد نمود. این یکی از اصلی ترین موانع در پیاده سازی استانداردهای مدیریت امنیت است

امنیت تداوم می خواهد

- حتی اگر موفق شویم در یک سازمان سیستم مدیریت امنیت را پیاده سازی نموده و گواهی استاندارد مربوطه را هم در یک مرحله اخذ نمائیم؛ عدم تداوم آن هیچ آورده ای را از نظر امنیتی برای سازمان نخواهد داشت. بنابراین همیشه در استانداردهای بین المللی از چرخه ای به نام چرخه دمینگ یا PDCA که یک چرخه مدور و دائمی است برای طراحی ، انجام ، آزمایش و اعمال مجدد طراحی استفاده می شود.



ناامنی تداوم دارد

- چون ناامنی تداوم دارد بایستی امن سازی و تفکرامنیت در همه شئون سازمان تداوم داشته باشد و اعتبار مداوم و سالیانه داشته باشد. مدیران سازمانی ما احساس نا امنی مداوم از فضای تبادل اطلاعات خود ندارند و یا مایملک اطلاعاتی ذی قیمتی را در معرض تهاجم نمی بینند. بر این اساس،حمایت جدی و همه جانبه از پیاده سازی و تداوم استانداردهای مدیریت امنیت ندارند.

امنیت نا محسوس است.

- لذا وقتی یک پروژه امنیتی (از نوع مدیریت امنیت)انجام می شود بعضاً مدیریت و کارشناسان احساس می کنند که هیچ اتفاق جدیدی نیفتادهاست و ممکن است گلایه کنند که چرا هزینه نموده اند. در پاسخ به این گلایه باید فکرکرد که اگر روی امنیت کار نمی شد چه اتفاقی ممکن بود بیفتد. پس باید در هر زمان ودر هر مکان از فضای تبادل اطلاعات سازمانی به فکر امنیت بود.

- **اثربخشی ISMS**

- فعالیت های امنیت اطلاعات، باید توسط نمایندگانی از بخش های مختلف سازمان با نقش ها و کارکردهای شغلی مرتبط، هماهنگ شوند و پیاده سازی سیستم مدیریت امنیت اطلاعات، یک پروژه ITنیست.
- آن چه مسلم است سیستم مدیریت امنیت اطلاعات فقط بحثی فنی نیست بلکه بخشی از استراتژی سازمان خواهد شد و با فرآیند های سازمانی آمیخته می گردد.این طرح نیاز به سرمایه گذاری ، حمایت مدیران ارشد سازمانی ، بلوغ IT، آموزش نیروی متخصص و آموزش کارکنان داشته و پیاده سازی این طرح به تنهایی سازمان را مقاوم نمی کند بلکه بعد از پیاده سازی نیاز به بهبود مستمر برای رسیدن به فرعنگ و بلوغ امنیت می باشد.

امنیت اطلاعات شامل سه بُعد مهم است:

- محرمانگی Confidentiality
- یکپارچگی Integrity
- دسترس پذیری Availability

- فراهم آوری صحت و تمامیت اطلاعات به گونه ای که در زمان مناسب، در دسترس افراد مجاز که نیازمند آن می باشند، عاملی است که منجر به اثربخشی کسب و کار می گردد. استاندارد ISO/IEC 27001زمینه مناسبی را برای طراحی و استقرار سیستم مدیریت امنیت اطلاعات و ارزیابی آن در سازمان ها و بهره گیری از منافع این رویکرد، فراهم آورده است.

سیستم مدیریت برحسب امنیت اطلاعات، به یک سازمان این امکان را می دهد تا موارد ذیل را ایجاد نماید:

- رضایت نیازمندی های امنیتی مشتریان و سایر ذینفعان؛
- بهبود طرح ها و فعالیت های سازمان؛
- تأمین اهداف امنیت اطلاعات سازمان؛
- تطابق با آئین نامه ها و قوانین و مقررات مربوط به کار؛
- مدیریت دارایی های اطلاعاتی در یک روش سازمان یافته که به بهبود مستمر و تعدیل با اهداف سازمانی کنونی، کمک می کند.

- استاندارد ISO27001 دارای ۱۰ گروه کنترلی می باشد که هرگروه شامل چندین کنترل زیرمجموعه است بنابراین در کل ۱۲۷ کنترل برای داشتن سیستم مدیریت امنیت اطلاعات مدنظر قراردارد . با انجام مراحل بالا شرکت یا سازمان شما پتانسیل پیاده سازی کنترل های مذکور را خواهد داشت.

این ده گروه کنترلی عبارتند از :

- سیاستهای امنیتی
- امنیت سازمان
- کنترل و طبقه بندی دارایی ها
- امنیت فردی
- امنیت فیزیکی
- مدیریت ارتباط ها
- کنترل دسترسی ها
- روشها و روالهای نگهداری و بهبود اطلاعات
- مدیریت تداوم کار سازمان
- سازگاری با موارد قانونی

رعایت نکات امنیتی شبکه و رایانه ها

- ۱- بدین وسیله اعلام می دارد هر شخصی که به شبکه دانشگاه متصل شود، بطور ضمنی مقررات و خط مشی های امنیتی را پذیرفته است.

- ۲- تمام استفاده کنندگان از سیستم‌های فناوری اطلاعات از جمله کارکنان و راهبران سیستم‌ها باید اصل خصوصی بودن اطلاعات در شبکه و حفظ حریم خصوصی را رعایت نمایند.
- ۳- با عنایت به امکان سوء استفاده و رصد اطلاعات توسط بیگانگان بر حسب ابلاغ کمیسیون عالی امنیت فضایی مجازی ،استفاده از نرم افزارهای پیام رسان خارجی در مکاتبات اداری و ارتباط کاری کارکنان دولت در هر سطح تخلف محسوب می شود.

- ۴- هر قراردادی که میان سازمان و طرف دیگری (اعم از حقیقی و حقوقی) منعقد گردد که متضمن استفاده آن طرف از امکانات فن‌آوری اطلاعات شود، باید شامل ماده‌ای باشد که در آن لزوم رعایت مقررات و خط مشی‌های امنیتی شبکه و سیستم‌های اطلاعاتی در آن تصریح گردد.

- ۵- تمامی کاربران بایستی در حفظ و استفاده بهینه از منابع اطلاعاتی شبکه و تجهیزات آن کوشا باشند.

- ۶- هیچ کاربری نبایستی با شناسه کاربر دیگری وارد شبکه شود و از منابع شبکه استفاده کند این مورد شامل :
- تلاش برای تغییر اطلاعات شخصی و یا سازمانی افراد دیگر، تلاش برای دسترسی به منابعی که خود شخص اجازه دسترسی به آنها را ندارد، تلاش برای ایجاد تغییرات در سیستم عامل ها یا منابع اطلاعاتی، تلاش برای از کار انداختن رایانه(ها) ی و یا تلاش برای از بین بردن و یا دستکاری اطلاعات موجود در شبکه سازمان ، می باشد.

- ۷- کاربران شبکه نبایستی نرم افزاری نوشته و یا نصب کنند که باعث اختلال درسایر رایانه ها و یا شبکه شود و به اطلاعات حساس و یا شخصی دیگران دسترسی پیداکنند، و یا باعث ایجاد اشکال در اجرای نرم افزاری و یا سخت افزاری شبکه شوند.

- ۸- استفاده ازهرگونه نرم افزار مخربی که باعث صدمه زدن به رایانه ها و یا دسترسی غیر مجاز به اطلاعات شبکه شود. می تواند باعث خسارت در سیستم های اطلاعاتی شود.

- ۹- کاربران شبکه سازمان نبایستی به رایانه، نرم افزار، داده و یا اطلاعات شبکه، بدون داشتن اجازه مدیر مستقیم واحد مربوطه دسترسی پیدا کنند و نبایستی درصورتی که به شبکه سازمان دسترسی دارند این دسترسی را در اختیار دیگران قرار بدهند.

- ۱۰- کاربری که به وی نام کاربری و رمز ورود اعطا شده است مسئول استفاده صحیح از این نام کاربری و رمز ورود است و استفاده غیر مجاز از آن و یا ارائه آن به دیگران تخلف می باشد. و نمی تواند ادعای مبنی بر جهل نماید و حق دارد به استناد ثبت رویداد در سیستم سرور برخورد قانونی انجام دهد.

- ۱۱- کاربران شبکه بایستی حقوق دیگر کاربران رارعایت کنند، اکثر سیستم های سازمان مکانیسم هایی برای محافظت از اطلاعات شخصی کاربران دارند، تلاش برای دور زدن این مکانیسمها برای دسترسی به اطلاعات سیستم ها و یا اطلاعات اشخاص مصداق جرم است.(استفاده از انواع فیلتر شکن و VPNو .....)

- ۱۲- کاربران نبایستی عمداً به دنبال بدست آوردن کپی یا تغییر در فایلهای اطلاعاتی، تغییر در نرم افزارها و یا تغییر در کلمات عبورسایر کاربران باشند(نفوذ در حریم خصوص موجب نقض ماده ۲ این دستور العمل می شود)

- ۱۴- الزامی است تا جایی که ممکن است در انتخاب پسوردها دقت کافی به خرج دهید. بعضی افراد شماره تلفن، شماره شناسنامه، تاریخ تولد، و ... را برای پسورد خود انتخاب می کنند همیشه در انتخاب پسورد خود از اعداد و کلیدهایی مثل Spaceو علائم مانند @,#,$ استفاده کنید. و همچنین پسورد خود را با طول زیاد انتخاب کنید. این روش امکان هک شدن کامپیوتر شما را کاهش می دهد.

- ۱۵- هنگام وارد شدن به ایمیل و یا سامانه های وب ، تیک کنار گزینه Rememberرا بردارید و حتما هنگام خارج شدن Logoutکنید تا ارتباط شما با سامانه قطع شود.

- ۱۶- مراقب سایت هایی که بازدید می کنید، باشید. چرا که بعضی سایتها آلوده به ویروس هستند و این ویروس ها بدون اطلاع فرد وارد کامپیوتر کاربر می شوند.

- ۱۷- بیشتر حملات سایبری امروزه از طریق مرورگرهای وب هستند. مرورگر خود را همیشه به روز نگه دارید.

- ۱۸- هنگامی که اطلاعات مهمی روی صفحه مانیتورتان هست، کامپیوترتان را ترک نکنید. ابتدا از تمام برنامه ها Logoutکنید و خارج شوید و سپس سیستم را ترک کنید. زیرا ممکن است شخصی در همین حین اطلاعات مهم شما را به سرقت ببرد.

- ۱۹- الزامی است کاربران مراقب آدرس های قلابی باشید مانند:
- http:// google.com.d۰۱۹i.cn//login
- شاید درابتدا فکر کنید که این آدرس متعلق به سایت گوگل است ولی اگر کمی دقت کنید می فهمید که دامنه اصلی این i ۰۱۹dاست که ربطی به گوگل ندارد و سایتی در چین می باشد که منتظر فرصت برای به سرقت بردن آدرس اطلاعات شخصی می باشد.

- ۲۰- سوء استفاده از امکانات شبکه و رایانه ای، بویژه در راستای منافع تجاری، کسب و کار شخصی، تقلب و نادیده گرفتن حقوق چاپ و تکثیر منابع و آزار و اذیت دیگران ، عملیات نفوذ و انتشار بد افزار و ویروس در هر شکلی، غیر قانونی و مشمول قوانین جرائم سایبری است.

- ۲۱- الزامی است همکاران محترم در پایان ساعت اداری به جهت جلوگیری از احتمال نفوذ و هک شدن اطلاعات از خاموش بودن سیستم تحویلی و قطع کامل برق کامپیوتر اطمینان حاصل نمایند.

موسسه تخصصی اورانوس
www.eduoranos.ir