طبقه بندی در حیطه بندی

اطّلاعات طبقه‌بندی شده اطلاعات حساسی است که، بر پایه قانون یا مقرّرات داخلی بنگاه‌های مالک آن، دسترسی به آن برای گروه خاصی منع شده است.

گاه اصطلاح «اسناد طبقه‌بندی شده» یا «اطلاعات محرمانه» نیز در این مورد بکار می‌رود.

تفریبا همه دولت‌ها ضوابطی برای طبقه‌بندی اسناد و اطلاعات دارند. بسیاری از شرکت‌های خصوصی نیز برای حفاظت از اطلاعات مالی و فنی خود نوعی نظام طبقه‌بندی دارند.

در نظام دولتی ایران معمولاً اطلاعات طبقه‌بندی شده چهار دسته است:

محرمانه

خیلی محرمانه

سری

به کلی سری

طبق ماده (۱) آئین‌نامه طرز نگاهداری اسناد سری و محرمانه دولتی شماره ۱۴–۱۷۰/م - ۲/۱۰/۱۳۵۴ وزارت دادگستری، «اسناد سری و محرمانه دولتی به اعتبار مقدار مراقبتی که باید در حفظ آن‌ها بشود به چهار طبقه تقسیم می‌شوند: طبقه اول ـ اسنادی است که افشای غیرمجاز آن‌ها به اساس حکومت و مبانی دولت ضرر جبران ناپذری برساند. طبقه دوم ـ اسنادی است که افشای غیرمجاز آن‌ها منافع عمومی و امنیت ملی را دچار مخاطره کند. طبقه سوم ـ اسنادی است که افشای غیرمجاز آن‌ها نظام امور سازمان‌ها را مختل و اجرای وظائف اساسی آن‌ها را ناممکن کند. طبقه چهارم ـ اسنادی است که افشای غیرمجاز آن‌ها موجب اختلال امور داخلی یک سازمان شود یا با مصالح اداری آن سازمان مغایر باشد.

مزایای طبقه بندی اطلاعات:

علاوه بر دلایلی که قبلا برای استفاده از طبقه بندی اطلاعات ذکر کردیم میتوانیم به مزایای دیگری از آن که برای سازمانها خوش ایند است به شرح زیر صحبت کنیم.

نشان دهنده تعهدات و حمایتهای امنیتی یک سازمان.

کمک به شناسایی اطلاعات حساس و حیاتی یک سازمان.

پشتیبانی از اصول محرمانگی, یکپارچگی و در دسترس بودن داده های مربوطه.

کمک به شناسایی داده هایی که نیازمند اعمال یک سری مسائل قانونی مرتبط با امنیت جامعه است.

مفهوم طبقه بندی اطلاعات:

در واقع اشاره به دسته بندی اطلاعات تولید وپردازش شده یک سازمان باتوجه به حساسیت, از دست رفتن و یا افشای آن داده ها دارد این رویکرد ما را قادر میسازد تا کنترل های امنیتی را به درستی اجرا و در طرح طبقه بندی خود قرار دهیم.

قوانین و مقررات طبقه بندی داده ها:

در زیر به تعریف و توصیف چند مورد از طبقه بندی داده های دولتی از پایین ترن سطح حساسیت تا بالاترین سطح را مورد بررسی قرار میدهیم.

اطلاعات طبقه بندی نشده : که عموم به راحتی به آنها دسترسی دارند و این آزادی دسترسی باعث نقض اصل محرمانگی در داده ها نمیشود.

اطلاعات حساس اما طبقه بندی نشده : (SBU) اطلاعاتی که به مانند یک راز کوچک است اما فاش شدن آنها میتواند باعث آسیب های جدی شود مانند پاسخ آزمون های یک امتهان که در این گروه قرار میگیرند.

محرمانه : گروه داده هایی که در این بخش قرار میگیرد بسیار مهم است و در صورت فاش شدن میتواند یک کشور را دچار آسیب های امنیتی کند مانند اسناد مهم دولتی که صرفا باید در دست افراد مجاز باشد.

سری : داده هایی که در این گروه قرار میگیرند در صورت افشاع باعث به خطر افتادن امنیت ملی یک کشور خواهد بود مانند تصمیمات مهم راهبردی جهت تایین نوع روابط با دیگر کشورها

فوق سری : این اطلاعات در بالاترین سطح امنیتی قرار دارند و افراد بلند پایه مثل رئیس جمهور یک کشور به آنها دسترسی خواهد داشت

همان طور که از این دسته بندی مشخص است افراد دارای دسترسی مناسب و مورد نیاز با حیطه کاری خود به داده ها دسترسی خواهند داشت و این به نظر من یکی از بزرگترن مزایای دسته بندی داده ها در سازمانها میتواند باشد که فرایند کنترل دسترسی را نیز برای مدیران آسان میکند.

دسته بندی اطلاعات به طور خاص در یک سازمان :

عمومی : همانند اطلاعات طبقه بندی نشده می ماند مانند اطلاعات معرفی شرکتها که به صورت عمومی در اختیار افراد برای برقراری روابط تجاری در اختیار دیگران قرار میگیرد .

حساس : اطلاعاتی که نیازمند سطح دسترسی بالاتری میباشند و لو رفتن آنها باعث از بین رفتن اصل محرمانگی و یکپارچگی داده ها میشود.

خصوصی : اطلاعاتی است که به عنوان ماهیت خصوصی افراد در نظر گرفته میشود هر چند که افشای آن اسیبی جدی را در سازمان ممکن است سبب نشود مانند میزان حقوق کارکنان , نوع قرارداد افراد, یا اطلاعات پزشکی شخص ولی افراد به صورت خصوصی تمایلی به افشاع آن ندارند.

محرمانه: اطلاعاتی است که در سطح بسیار حساس در نظر گرفته شده است و صرفا برای استفاده درون سازمانی در نظر گرفته شده و معاف از قانون دسترسی آزاد به اطلاعات است افشای غیر مجاز آن جدی تلقی شده وتاثیر گزار بر روابط شرکت است مانند اطلاعات مربوط به توسعه یک محصول جدید , اسرار تجاری, مذاکرات ادغام شرکتها در گروه اطلاعات محرمانه سازمان در نظر گرفته میشود.

معیار های طبقه بندی اطلاعات:

از معیار های مختلف برای تایین ارزش اطلاعاتی یک شیء استفاده میکنیم . که معیار معمول مورد استفاده برای طبقه بندی داده ها در یک سازمان در بخش خصوصی شامل داده های با ارزش یک سازمان یا مربوط به رقبای آنها میشود که نیاز به طبقه بندی دارد. دومین معیار زمان است بعضی از داده ها در اثر گذ شت زمان ماهیت امنیتی خود را از دست میدهند مانند اسنادی که پس از طی یک دهه مشخص ارزش خود را از دست خاهند داد و در طبقه بندی آنها باید تجدید نظر کرد. و بر عکس این مورد که در بعضی موارد در اثر گذشت زمان با داده هایی مواجه میشویم که هرچند در ابتدا بی اهمیت جلوه میکردند اما با تهقیقات جدید به عنوان اساس یک فورمول کاری مورد توجه قرار میگیرند و معیار سوم داده های شخصی که در ارتباط با قوانین حفظ حریم خصوصی افراد قرار میگیرند ونیاز به طبقه بندی مناسب پیدا میکنند.

روش طبقه بندی اطلاعات :

مراحل مختلفی در ایجاد یک سیستم اطلاعت طبقه بندی شده وجود دارد که متداول ترین آنها را عنوان میکنیم.

شناسایی سطح کاربری افراد مدیر/ سرایدار

تعیین معیار های طبقه بندی و برچسب های اطلاعاتی مناسب برای افراد , داده ها, اشیاع

طبقه بندی داده ها بر اساس مالکین آن که توسط یک سرپرست واجد شرایط انجام میشود.

مشخص و مستند نمودن سیاست های امنیتی برای طبقه بندی داده ها

مشخص نمودن سطح دسترسی هر یک از گروهها که باید به داده ها دسترسی داشته باشند.

تایین روش در اختیار قرار دادن اسناد محرمانه و یا انتقال اطلاعات به نهاد های دیگر

ایجاد یک برنامه مناسب جهت آگاهی و کنترل طبقه بندی داده های سازمان

توزیع اطلاعات طبقه بندی شده :

---

توزیع اطلاعات طبقه بندی شده که با اسیب هایی نیز ممکن است همراه باشد به شکل های زیر قابل ارائه است.

حکم مقامات قضایی : ممکن است برای افشاع اطلاعات مثلا حسابهای بانکی و یا داده های شخصی افراد نیاز به پیروی از حکم دادگاه باشد

قرارداد های دولتی: پیمانکاران دولتی ممکن است بر اساس پیروی از (IAW) اقدام به افشاع اطلاعات محرمانه بکنند که البته به موافقت نامه های مربوط به انجام طرح های دولتی مربوط میشود.

تایید ارشد : یکی از مدیران ارشد ممکن است اجازه انتشار اطلاعات طبقه بندی شده را به اشخاص یا سازمان های خارجی بدهد. این آزادی ممکن است با امضاء یک قرارداد محرمانه در جهت تامین منافع یک حذب انجام شده باشد.

نقش افراد در طبقه بندی اطلاعات :

نقشها و مسئولیت هایی که افراد شرکت کننده در طرح طبقه بندی اطلاعات باید برای آنها تعریف شوند و در این بازه صاحبان یا متولیان داده ها در این سیاست باید به عنوان یک نکته کلیدی مورد بررسی قرار بگیرد.بنابراین

مالک (Owner) : صاحب اطلاعات ممکن است یک مدیر اجرایی یا مدیر یک سازمان باشد این فرد در واقع مسئولی برای حفظ دارایی های اطلاعاتی سازمان است و این نکته را باید در نظر داشته باشید که صاحب متفاوت از سرپرست است و صاحبان شرکتهای بزرگ مسئولیت نهایی حفظ داده ها را برعهده خواهند داشت اما به هر هال این مفهوم ممکن است در اثر سهل انکاری صاحب در حفظ اطلاعات جزء عملکرد های یک نگهبان تلقی شود. مسئولیت مالک اطلاعات میتواند شامل این موارد باشد. تصمیم گیری اصلی در مورد اینکه چه سطحی از طبقه بندی اطلاعات نیاز اساسی کسب و کار مربوط به سازمان است. بررسی تکالیف طبقه بندی دوره ای و تغییرات مورد نیاز برای کسب و کار و محول کردن مسئولیت و وظیفه حفاظت از داده ها به نگهبان.

نگهبان (Custodian) : به عنوان نمایندگان صاحبان اطلاعات وظیفه حفظ داده ها را بر عهده دارند که پرسنل IT معمولا اجرای این نقش را به عنوان یکی از وظایف مهمشان بر عهده دارند نحوه حفاظت از داده ها توسط سرپرست it میتواند به این شکل باشد الف) پشتیبان گیری منظم از برنامه های در حال اجرا و به طور معمول تست اعتبار داده های پشتیبان گیری شده ب) انجام ترمیم داده های پشتیبان گیری شده در صورت لزوم ج) حفظ و ثبت IAW اطلاعات و ایجاد سیاست های طبقه بندی اطلاعات مورد نیاز از وظایف مسئولین it به عنوان دارنده نقش نگهبان داده ها میباشد.

کاربر (user) : در طبقه بندی نقشهای اطلاعاتی کاربر به عنوان مصرف کننده نهایی باید در نظر گرفته شود (افرادی مانند اپراتور ها و کارمندان ) که به طور معمول با استفاده از اطلاعات به عنوان بخشی از کار خود یک مصرف کننده در نظر گرفته میشود و باید در رابطه با آن سیاستهای زیر اعمال شود و درنهایت او هم ملزم به رعایت آنها باشد کاربران باید روش های عملیاتی تعریف شده در سیاست های امنیتی سازمان ها را به سورت دستورالعمل پذیرفته و بکار گیرند و ملزم به حفظ داده هایی باشند که به صورت روزانه با آنها سرو کار دارند( جهت جلوگیری از افشاء آنها) و اینکه کاربران باید منابع محاسباتی و امکانات فیزیکی شرکتها را باید در قبال اهداف سازمان مربوطه بکار گیرند و حق استفاده شخصی از داده ها و منابع را نداشته باشند ( به طور مثال اقدام به فروش اطلاعات مربوط به ساخت یک محصول تجاری سازی شده را نکنند.)

نکته اصطلاح (OPEN VIEW) اشاره به عمل خروج اسناد طبقه بندی شده دارد که یک فرد غیر مجاز میتواند آنها را به صورت عادی مشاهده کند و در نتیجه باعث نقض اصل محرمانگی داده ها را سبب شود بنابراین کاربران باید در مواقع عدم حظور در محل کار باید این داده ها را در محلهای امن و خارج از دسترس افراد قرار دهد یا در حین انتقال آنها مراقبتهای لازم را به عمل آورد.

پیاده سازی سیاستهای امنیتی :

سیاستهای امنیتی به عنوان یک رکن اساسی در برقراری امنیت داده های سازمان در قالب سیاستهایی مانند دستورالعمل ها و استادارد ها کنترلها به صورت غیر متمرکز یک کار بیهوده و بی اثر خواهد بود. در طرح ریزی این سیاستها باید به سوالاتی مانند زیر پاسخ داده شود.

سیاستها , دستورالعملها , استانداردها و روشهای اجرا چه هستند؟

چرا باید از سیاستها , دستورالعملها , استانداردها استفاده کنیم ؟

انواع سیاستهای مشترک شامل چه مواردی میشود.

سیاستها , دستورالعملها , استانداردها و روشها

سیاست : یکی از چند موردی است که میتواند در (INFOSEC) معنا پیدابکند. به عنوان مثال تعیین سیاستهای امنیتی در firewall ها که به کنترل دسترسی مراجعین ولیست مسیریابی اطلاعات (routing) , استانداردها , رویه ها, دستورالعمل ها را شامل شود در یک مفهوم گسترده تر سیاستهای امنیتی را به عنوان سیاست امنیت اطلاعات جهانی معرفی میکنند یک سیاست امنیتی خوب نوشته شده میتواند به عنوان یک عنصر اصلی و ضروری به معنای واقعی کلمه نجات بخش از یک فاجعه باشد به مانند حفظ پایه و اساس اسرار مهم تجاری شرکتها وایجاد حس مسئولیت پذیری در قبال کار انجام شده در کارمندان که این سیاستها مستلزم به وجود آمدن توابع مناسب دولتی و خصوصی و مسائل نظارتی میباشد.انواع سیاست دارای یک سلسله مراتبی از تصمیمات مدیر ارشد میباشد که عبارتند از :

الف) تصمیمات سیاستهای امنیتی مدیر ارشد

ب) سیاستهای عمومی سازمان

ج) سیاستهای کاربردی

د) استانداردهای اجباری (به عنوان خط مشی پایه واساسی)

ه) دستورالعمل های توصیه شده

و) روشهای اجرایی سیاستهای امنیتی دقیق

این سیاستهای امنیتی دارای ویژگیهای زیر باید باشند.

اذعان به اهمیت منابع محاسباتی مالی سازمان در مدل کسب و کار

رائه بیانیه ای که در بردارنده تضمین امنیت اطلاعات در سرتاسر سرمایه گزاری باشد.

تعهد به اجازه ومدیریت تعریف استانداردهای lower-level و رویه ها و دستورالعملها

(Regulatory) تنظیم مقررات: تنظیم مقررات سیاستهای امنیتی یک سازمان باید با توجه به رعایت قوانین و مقررات و یا الزامات قانونی قابل اجرا در سطح یک کشور باشد که در رابطه با موسسات مالی وشرکتهایی که خدمات عمومی ارائه میدهند باید در این ضمینه بسیار دقیق و خاص عمل کنند زیرا در جهت منافع عمومی باید عمل کنند. سیاست تنظیم مقررات معمولا دارای دو هدف اصلی است .

1- اطمینان از اینکه یک سازمان به دنبال روشهای استاندارد و یا شیوه های پایه از عملیات خاص در صنعت خود است.

2- اعتماد به نفس گرفتن یک سازمان پس از تایین سیاستهای صنعتی استاندارد قابل قبول.

نکته : اساسا هرگونه موفقیت برنامه های امنیتی مهم به مدیران ارشد وابسته است که باید درک صحیحی از فرایند سیاستهای امنیتی و مدیریتی را داشته باشند و در سطح بالایی از تعهد به امنیت اطلاعات باشند و از چکونگی کنترل های امنیتی و پیاده سازی روشهای آن درجهت حفظ و برپا نگه داشتن سازمان استفاده کنند و همواره آن را در سرتاسر سازمان حفظ کنند.

مشاوره (Advisory.) : استفاده از سیاستهای امنیتی مشورتی توسط کارمندان که به مدیران ارائه میشود میتواند شکست را به دنبال داشته باشد (مانند فسخ یک قرارداد کاری .....) به همین دلیل استفاده از سیاستهای امنیتی به وسیله شرکتها برای کارکنان و مجبور کردن آنها برای رئایت آنها و ایجاد بسیاری از این محدودیتها در ضمینه های نرم افزاری و کنترل کارمندی بیش از دیگران باتوجه به نقش و مسئولیت فرد در سازمان است مثلا برای جلوگیری از استفاده روشهای تراکنشی مورد علاقه کارمندان به جای استفاده از روش های استاندارد و اصولی که افراد سعی در اعمال نظر در اینگونه سیاستها میکنند.

اموزنده (Informative. که حاوی اطلاعاتی است): سیاستهای آموزنده سیاستهایی هستند که به راحتی به اطلاع افراد میرسند و در آن هیچ موردی به صورت ضمنی و مشخص از آن وجود ندارد و مخاطبین آن میتواند افرادی از درون سازمان یا گروههای خارجی باشد و البته این به معنی مجاز بودن این اطلاعات و سیاستها برای به کار بردن آنها نیست و استفاده از انها میتواند باعث از دست رفتن اصل محرمانگی داده ها در یک سازمان شود.

استانداردها و دستورالعمل ها و رویه ها همگی سه عنصر اصلی اجرای سیاستهای امنیتی هستند که جزئیات واقعی وچگونگی اجرا و روشهای مدیریت امنیت و سطح تعهدات مدیران ارشد را بازگو میکنند بنابراین استانداردهای مورد تقازای سازمان و نحوه اجرای آن باید با چاپ کتابچه های راهنما یا از طریق برگزاری کلاسهای اموزشی و یا با اینترنت به اطلاع افراد برسد این نکته مهم است که بدانید این سه عنصر جدا از هم هستند در هالی که به اشتباه خیلی از شرکتها آنها را بایک سند سیاستی ارائه میکنند و این به طور کلی خوب نیست دلایلی که هر عنصر باید جدا نگهداری شود میتواند به این صورت عنوان شود.

1- هر کدام از این عناصر بر تابعی با تمرکز بر افراد مختلف ارائه شده بنابر این میتوان آنها را به صورت جداگانه ودر یک قالب فیزیکی مشخص به افراد تحویل داد.

2- کنترل های امنیتی برای رئایت اصل محرمانگی برای هر نوع سیاست متفاوت است به طور مثال دسترسی به منابع برای افراد , در گروههای متفاوت ارائه میشود اما انها امکان تغییر رمز عبور را ندارند

3- به روز رسانی سیاستهای امنیتی یک پارچه و ادغام شده در هم بسیار مشکل خواهد بود.

استاندارد : با تایین مراحل عملکرد و روشهای یکسان مشخص کننده استفاده از فناوری های خاص میباشند که معمولا به صورت اجباری در سرتاسر سازمان قابل اجرا میباشند و به بهبود روشهای کنترل امنیتی ختم خواهد شد.

راهنمایی ها : که دستورالعمل های استاندارد داشته و برای رسیدن به منابع را برای افراد مشخص میکنند ودر هالی که باید اجرا شوند بهتر است بهتر است در کنار رعایت استانداردها انعطاف پذیر هم باشند.

روش (Procedures.) : مجسم گامهای دقیق است که به دنبال انجام یک وضیفه خاص پرسنل باید آن را دنبال کنند وهدف کاربران نهایی است که باید به پیاده سازی سیاستها , استانداردها , و دستورالعمل ها بپردازند.

خطوط : ذکر خطوط با اینکه مشابه استاندارد هستند اما کمی متفاوتند هنگامی که مجموعه منسجمی از خطوط ایجاد شوند ما میتوانیم معماری امنیتی یک سازمان را طراحی و استاندارد های آن را توسعه بدهیم به عنوان مثال تفاوت بین خطوط سیستم عامل های مختلف یک مجموعه برای اطمینان از اجرای یکنواخت سیاستهای امنیتی که اگر توسط سازمان به تصویب رسید اجرای خطوط اجباری میباشد. پیروز و سربلند باشید.

اسناد سری در طبقات اول و دوم و اسناد محرمانه در طبقات سوم و چهارم قرار می‌گیرند. (اسناد طبقه اول با عنوان به «کلی سری» و اسناد طبقه دوم با «عنوان سری» و اسناد طبقه سوم با عنوان «خیلی محرمانه» و اسناد طبقه چهارم با عنوان «محرمانه» مشخص می‌شود).».