معماری امنیت اطلاعات

جناب اقای مهندس شمس پور

دانشجویان امنیت اطلاعات_علمی کابردی_جهاد دانشگاهی_واحد ارومیه

۱۳۹۳_زمستان

چرا تهدیدات امنیتی ضروری هستند:

۱_ ارزش سرمایه گذاری روی تجهیزات سخت افزاری و نرم افزاری :

به دلیل هزینه بر بودن سخت افزار و نرم افزار ها، در صورت وقوع هر نوع صدمه میتواند شخص یا سازمان را دچار زیان نماید.

۲_ارزش داده های سازمانی:

این داده ها ممکن است شامل لیست مشتری ها و شماره حساب بانکی آنها باشد که درصورت دستکاری با ازبین رفتن آنها عملکرد سازمان مختل می شود

۳_ارزش داده های فردی:

ارزش داده های کاربر ممکن است چندان دارای ارزش نباشد ولی ازدست دادن آنها بسیار زیان آور بوده و ایجاد دوباره آنها زمان بسیاری زیادی را صلب میکند.

۴_تهدیدات و حملات نفوذ گران اینترنتی :

با گسترش شبکه اینترنت و استفاده عمومی از آن، افرادی که به دنبال سوء استفاده از داده های کاربران بوده روز به روز افزایش پیدا کرده و امنیت اطلاعات را مختل میکنند.

چرا در زمینه امنیت ضعف وجود دارد:

۱_ سهل انگاری:

ممکن است برنامه نویسان کامپیوتری آشنایی کافی به مسائل امنیتی نداشته باشند و برنامه نویسان برنامه هایی ناامن بنویسند .

۲_ اولویت پایین:

ممکن است مسئولان یا برنامه نویسان آگاه به مسائل امنیتی باشند ولی به دلایل هزینه بر بودن پیاده سازی آنها تمایلی به پیاده سازی سرویس های افقی نداشته باشند.

۳_ محدودیت زمان وهزینه:

بعضی مواقع ممکن است به دلیل محدود بودن زمان و هزینه فرصت پیاده سازی سرویس های افقی رانداشته باشیم

۴_ بی نظمی برنامه نویسان:

گاهی اوقات برنامه نویسان به خاطر راحتی کار بعضی از کدهای برنامه نویسی را در چنین پروژه استفاده میکنند copy paste. در این صورت اگر کد اولیه دچار خطا باشد تمامی پروژه ها دچار ضعف امنیتی خواهند بود .

۵_ خلاقیت نفوذ گران :

انسان موجود خلاقی است و افرادی با این انگیزه همیشه در پی غلبه به موانع افقی و خرابکاری هستند .

۶_ سطح پایین آگاهی کاربران:

افراد مبتدی به دلیل رعایت نکردن مسائل پیش پا افتاده امنیتی گاها امنیت خود وسازمان را مختل میکنند.

برای محافظت از داده های خود میتوانیم نسخه پشتیبان تهیه نماییم دلایلی که ممکن است داده های فردی را از بین رود:

۱_پاک شدن اتفاقی داده ها .

۲_ دزدیده شدن رایانه.

۳_ ذخیره ناخواسته یک فایل به روی فایل دیگر.

۴_ روند نادرست به اجرا درآوردن یک برنامه به گونه ای که باعث تغییر یا پاک شدن داده ها شود.

۵_وجود یک برنامه مخرب

۶_بروز مشکل در سخت افزار.

۷_ آتش سوزی در بلایای طبیعی

روش های پشتیبان گیری یا از چه چیزهایی باید پشتیبان گیری کنیم

۱_ پشتیبان گیری از فایل های شخصی

۲_ پشتیبان گیری از کل سیستم

روش پشتیبان گیری افزایشی:

چنانچه داده های شخصی زیاد شد و ممکن است ذخیره کردن تمام آنها به عنوان پشتیبان زمان و وقت زیاد و فضای زیادی را از کاربر بگیرد به این منظور در ابتدا یک نسخه کلی از فایل هایمان ، پشتیبان می گیریم و

سپسس در بازه های زمانی مشخص تنها آن فایل هایی که دچار تغییر شده اند را نسخه برداری میکنیم به این روش پشتیبان گیری افزایش گوییم طبیعی است برای باز گرداندن پشتیبان ها در این روش نیاز به پشتیبان اولیه و دوم خواهیم یافت.

امنیت در سیستم های شخصی:

برای حفظ امنیت چند بعد وجود دارد:

۱_ حفظ فیزیکی:

_ شماره سریال ها را پاک میکنیم

_ محیط را امن میکنیم

_ دوربین مدار بسته نصب میکنیم

_ محافظ برق مناسب استفاده میکنیم

_ استفاده از آنتی ویروس

_ سیستم از دسترس افراد غیر مجاز دور باشد

_ بروز کردن نرم افزار و سخت افزار های فریز

۲_ بعد منطقی و حفاظت منطقی سیستم :

_ بکاپ گیری کنید.

_استفاده از نرم افزار های سالم؛ حد اقل امکان سعی کنیم از نسخه های اصلی سیستم عامل ها استفاده کنیم و یا برای نرم افزارها از برنامه های کرک و کی جن استفاده نکنیم.

_ارتباط با فضای مجازی؛ فضای مجازی فقط ارتباط با اینترنت نمی باشد برای مثال بلوتوث موبایل نیز میتواند یک فضای مجازی نیز باشد حتی برنامه های شبکه های اجتماعی نظیر وی چت نیز میتواند امنیت شخصی را مختل نماید.

امنیت در شرکت های خصوصی کوچک

۱_ تامین امنیت فیزیکی:

در شرکت های خصوصی سیستم ها کاملا خصوصی نیستند ، علاوه بر ورود و خروج امکاناتی که باید اینگونه افراد باید از آنها استفاده کنند نیز از نظر فیزیکی ایمن شوند .

۲_کنترل ورود و خروج ساختمان برای برقراری امنیت محیط :

اولین نکته از امنیت فیزیکی ، کنترل ورود و خروج ساختمان ، استفاده از برق مناسب و ups مطمئن ، استفاده از دوربین های مداربسته ، درب ضدسرقت ، بوسیله ی این روش ها امنیت فیزیکی سیستم های موجود در شرکت را فراهم سازیم .

۳_کنترل دسترسی ها :

وقتی یک کارگاه امنیتی ایجاد گردید و ورود و خروج افراد را کنترل شده در نظر گرفتید ، سپس باید سطح دسترسی افراد را مشخص کنیم ، نکته ی دوم کنترل دسترسی سخت افزاری مانند کافی نت ها میباشند که اجازه ی دسترسی به فلش ها را نمیدهند .

۴_استفاده از فایروال های نرم افزاری و در صورت لزوم سخت افزاری :

وقتی یک شبکه را راه اندازی میکنیم برای کنترل ورود و خروج افراد بهتر است از فایروال ها استفاده کنیم که هزینه نوع نرم افزاری آن پایین تر میباشد ، در بعضی از شرکت ها بسته به اهمیت اطلاعات ، گاهی اوقات نیاز به استفاده از فایروال های سخت افزاری پیدا میکنیم ،ولی در حالت کلی برای شرکت های خصوصی به دلیل هزینه بر بودن فایروال های سخت افزاری ، این نوع از فایروال ها توصیه نمیشوند .

۵-استفاده از نرم افزارهای سالم و مجاز:

توصیه میشود در شرکت ها و سازمان های کوچک نرم افزارهایی مثل سیستمک عامل و نرم افزارهای کلیدی خود را بصورت کامل خریداری کرده واز استفاده از نسخه های کرک شده پرهیز کنند ، خطراتی که در صورت استفاده از این نسخه ها ممکن است پیش بیاید عبارت اند از :

۱. امکان اضافه شدن کد مخرب به برنامه های اصلی و انجام کارهای مخربانه
۲. عدم امکان استفاده از خدمات پشتیبانی و بروزرسانی که در بلند مدت میتواند باعث کاهش امنیت سازمان شود.

۶-استفاده از امضای دیجیتال:

امضای دیجیتال عبارت است از هر تکنیک یا مکانیزمی که باعث شود در دنیای دیجیتال هویت ما از دیگران متمایز گردد ، در ابتدا امضای دیجیتال همان نام کاربری و پسورد بود ولی با گذشت زمان و با پیدایش روش هایی مانند تشخیص چهره ، اثر انگشت ، تن صدا و ... امضای دیجیتال معنی کلی پیدا کرده و دربرگیرنده ی تمام مکانیزم های تشخیص هویت دیجیتال میباشد .

امنیت در سازمان های متوسط و بزرگ :

در بحث سازمان های بزرگ ما نمیتوانیم یک طرح امنیتی کلی برای تمام سازمان در نظر بگیریم

تفکیک سازمان ها :

برای تفکیک سازمان ها نکات زیر باید در نظر گرفته شود :

۱. **محصول یا خدمات سازمان چه هستند** ؟ برای در نظر گرفتن امنیت باید سطوح مخصوص آن سازمان در نظر گرفته شود ،مثلا در شرکت های تولیدی دستمال کاغذی نکاتی که مهم هستند مربوط به مواد اولیه و بسته بندی مطرح میباشد و امنیت در این سازمان ها بیشتر مربوط به امور مالی میشود ، ولی در مقابل آن شرکت های ارتباطی مانند همراه اول که خدمات ارتباطی ارائه میدهند و بحث حریم خصوصی در میان است ، سطح امنیت پیچیده تر و با ارزشتر میباشد .

۲. **منابع اصلی در آمد و رشد سازمان چیست** ؟ مانند شرکت همراه اول که منبع درآمد آن امکانات افراد میباشد و نکته ی امنیتی در این است که مکالمات افراد پخش نشود.

۳. **نکته مهم بعدی ساختار سازمان است :** مثلا در شرکت های مخابراتی امنیت فیزیکی مهم نیست مانند دکل های مخابراتی که در سراسر کشور وجود دارند و در مقابل بانک ها و سازمان های مالی که بحث امنیت فیزیکی در آنها بیشتر اهمیت دارد .

۴. **برای بخش های مختلف در یک سازمان چه اطلاعاتی مهم است** ؟ برای مثال در یک شرکت کوچک اطلاعات بصورت متمرکز و یکپارچه در یک سطح هستند مانند یک سرور در یک دانشگاه ولی در شرکت های بزرگ قسمت های مختلف از هم جدا هستند و فقط از اطلاعاتی که برای آن قسمت مهم هستند استفاده میکنند .

۵. **باید مشخص کنیم همکاران سازمان ، مشتریان و شرکاء چه کسانی هستند** ؟ برای مثال سازمان هایی مانند دادگستری و پزشکی قانونی که در آنها افرادی که با این سازمان ها در ارتباط هستند معمولا افرادی عصبی بوده و در این سازمان ها امنیت از اطلاعات بسیار مهم میباشد .

۶. **نکته بعدی این است که باید دشمنان و یا تهدیدات آن سازمان را بشناسیم** ، دشمن سازمان های بزرگ ۲ دسته اند :۱.خارجی ۲. داخلی ، که در سازمان های مختلف دشمنان و انگیزه های آنان متفاوت اند ، دشمنان خارجی در بستر شبکه و بستر فیزیکی ممکن است اطلاعاتی را تخریب کنند و باعث جاسوسی شوند ، دشمنان داخلی ممکن است نشآت گرفته از دشمنان بیرونی باشند که برای جاسوسی وارد سازمان شده اند و نوع دیگر دشمنان فردی اند که بخاطر خصومت شخصی با سازمان سعی در صدمه زدن به سازمان هستند .

با توجه به جمع بندی این نکات میتوانیم نسبت به سازمان اطلاعات مفیدی کسب کرده و بفهمیم که برای آن سازمان چه مسائلی از لحاظ امنیتی اهمیت دارند مانند سازمان ها و ارگان های نظامی که باید محرمانگی در سطح بالای سطوح امنیتی لحاظ شود و دسترس پذیری برای آن پایینترین سطح باشد ، برعکس بانک که دسترس پذیری اولین نکته در ایجاد سطوح امنیتی است ، بعد از این مراحل باید یک طرح جامع امنیتی را پیاده سازی کنیم که مهمترین مسئله ی آن نوشتن مستندات است که باید همیشه بروز باشند و پس از اتمام کار نیز باید مستندات را نزد خود نگاه داریم .

در طرح جامع امنیتی چه مواردی را باید لحاظ کنیم ؟

۱. **بدترین حالت های امنیتی را برای سازمان مکتوب کنیم** : منظور همان بدبینی نسبت به تمام افراد است ، ازجمله دشمنان و تهدیدات که کارشناسان IT باید تمام موارد امنیتی را برای مدیریت بازگو کنند .

۲. **برای سازمان های بزرگ پیشنهاد استخدام متخصصین امنیتی را مطرح کنیم** : (زیرا تهدیدات امنیتی مدام تغییر میکنند و روش های آن ها با دفعات قبل متفاوت میباشد) در سیستم های کوچک نیازی به این کار نیست ، زیرا حجم کار کم میباشد و قطعا نیز تجهیزات کم خواهند بود.

۳. **آموزش های مستمر** : لازم است که کارشناسان IT همیشه به کاربران عادی آموزش لازم را در زمینه ی موارد امنیتی مانند نحوه ی گذاشتن پسورد و ... را بدهند.

۴. **تدوین یک سیاست مکتوب برای سازمان :** یعنی سیاست امنیتی را باید برای سازمان مکتوب و تحویل مدیریت بدهید که مدیریت بدون داشتن تخصص امنیتی باید آن را متوجه شود و بر اساس آن تصمیمات مدیریتی را اتخاذ کند .

۵. **تعیین گزارشگران سازمان :** مانند نیروی حراست است که در سازمان های بزرگ هم متخصص امنیت و هم گزارشگر مهم است ولی در شرکت های کوچک این مسئله اهمیت چندانی ندارد و گرفتن یک مشاوره ی امنیت یکبار در طی سال کافی است ، این گزارشگر باید تجهیزات سخت افزاری افراد درون سازمان را در نظر بگیرد و در صورت لزوم نکات امنیتی را برای آنها گوشزد کند.

۶. **درک و اولویت بندی اهداف سازمان :** یعنی اهداف سازمان چه هستند و کدام یک از آنها اولویت بیشتری دارد .

این نکات ملزم یک طرح امنیتی هستند و نکات مهمتر برای آنها شامل موارد زیر میباشد :

۱. **برآورد چالش یا مخاطره امنیتی :** یعنی اینکه بدانیم از چه چیزی باید محافظت کنیم و چه زمانی را باید برای آن صرف کنیم ، در اینجا کارکرد مشاوره ای بسیار مهم است که خود شامل موارد زیر است :

الف) **تعیین اینکه سعی در حفظ چه چیزی را داریم** ، برای مثال یک سازمان نظامی در فضای امنیت فیزیکی و امنیت اطلاعات را در نظر بگیرید : در این سازمان امنیت اطلاعات بسیار حائز اهمیت میباشد ، ولی در بانک ها بیشتر امنیت فیزیکی مد نظر است.

ب) در هر سازمان مقابل چه چیزهایی نیاز به حقاظت داریم ؟ برای مثال در سازمانی که اتصال به اینترنت وجود ندارد نیازی به خریداری یک فایروال گران قیمت نداریم .

ج) برای برقراری امنیت چه مقدار باید زمان ، نیرو و پول خرج کنیم .

نکته : برآورد مخاطره ، اولین گام برای برآورد هزینه ارتقاء امنیت است .

جمع آوری اطلاعات برای ارزیابی مخاطرات باید در ۳ مرحله انجام گیرد :

۱- شناسایی دارایی های سازمان ۲- شناسایی تهدیدات ۳- مخاطره امنیتی

۱. **شناسایی دارایی های سازمان :** دارایی های سازمان ۲ دسته اند :

الف) **ملموس** : مانند تجهیزات سخت افزاری ،دستگاه های ذخیره سازی اطلاعات ، نسخه های چاپی اطلاعات ، وسایل ارتباطی ، کابل کشی های سازمان و ...

ب) **غیر ملموس** : مانند داده ها و اطلاعات موجود در سازمان ، حریم خصوصی کابران (سازمان ها تا چه میزان در حریم خصوصی کارکنان وارد میشوند یا خیر؟)، نرم افزارهای قابل استفاده در سازمان (باید نرم افزارهای مورد استفاده در سازمان را بشناسیم و نکات امنیتی نرم افزار را بدانیم) ، رمزهای عبور کارکنان (در یک سازمان ممکن است رمز عبور برای یک تیم باشد و یا اینکه هر فرد یک رمز عبور داشته باشد) ، در دسترس بودن اطلاعات جزو دارایی های غیر ملموس بحساب می آید .

راه های شناسایی دارایی های ملموس و غیرملموس :

بهترین راه این است که فرد حضورا با افراد سازمان صحبت کند که این روش ۲ مشکل دارد :

۱. ممکن است افراد سازمان به آن فرد اعتماد نداشته و اطلاعات امنیتی را بطور کامل در اختیار او نگذارند
۲. در یک سازمان بزرگ امکان صحبت کردن با تمام کارکنان ممکن است وجود نداشته باشد.

راه حل این مشکلات این است که از مدیریت سازمان بخواهیم جلسه ای برگزار نماید و در آن جلسه ، افراد کلیدی سازمان که اطلاعات امنیتی در مورد دارایی های سازمان دارند را به کارشناس امنیتی منعکس نمایند.

۲.شناسایی تهدیدات : تهدیداتی که در یک سازمان ممکن است متوجه سازمان شود ، چه است .

۳.مخاطره امنیتی : زمانی که سازمان را شناختیم باید برآورد هزینه انجام دهیم که مخاطرات همان مشکلات امنیتی سازمان میباشند و در این مرحله باید برای مقابله با آنها میزان هزینه را برآورد کنیم .

چه نکاتی باید برای شناسایی تهدیدات در نظر گرفت :

۱. بیماری افراد کلیدی را باید در نظر گرفت ، بعنوان راهکاری برای نکته میتوان اقدامات زیر را انجام داد :

الف) داشتن دو متخصص در سازمان

ب)تهیه مستندات از کارهای انجام گرفته توسط متخصص و در اختبار قرار دادن مستندات مدیر سازمان

۲. بیماری همزمان افراد سازمان را باید در نظر گرفت ، مانند بیماری های واگیردار، پس باید از سلامت کارکنان اطلاع داشته باشیم

۳. مرگ افراد کلیدی را باید در نظر گرفت .

۴. از دست دادن خدماتی مانند تلفن ، شبکه یا برق را باید در نظر گرفت که :

الف)قطع برق بصورت کوتاه مدت با UPS برطرف میشود.

ب) قطع برق بصورت بلند مدت با ژنراتور برطرف میشود.

۵. سرقت رسانه های ذخیره سازی و رایانه های کیفی و جیبی را باید در نظر گرفت ، برای مثال در سازمان هایی که اطلاعات برایشان اهمیت دارد ، اجازه ی ورود و خروج تجهیزاتی مانند گوشی همراه ، فلش مموری ، دوربین دیجیتال و ... را به داخل سازمان را نمیدهند .در این سازمان ها همچنین باید به کارکنان آموزش مراقبت از این دستگاه ها نیز داده شود ، در واقع لو رفتن فرد برابر با لو رفتن سازمان میباشد.

۶. ورشکستگی یا از هم پاشیدن شرکت های طرف قرارداد با سازمان : با از بین رفتن اطلاعات امنیتی شرکت هم از هم پاشیده شده که طرف قرارداد با سازمان ماست ، میتواند یک تهدید امنیتی برای سازمان ما باشد .

۷. خرابکاری کارمندان داخلی را باید در نظر گرفت که جزو تهدیدات قور میباشد که به هر علتی ممکن است اتفاق بیفتد.

۸. مهاجمین تفننی را باید در نظر گرفت که این افراد هدف خاصی ندارد و از سواد امنیتی کمتری نیز برخوردارند .

نکات کلیدی که در تدوین سیاست امنیتی باید لحاظ شود :

۱. **تخصیص یک مسئول :** در سازمان باید مشخص شود هر شخص چه وظیفه ای دارد، مثلا چه شخصی مسئول پسوردها است ، چه شخصی مسئول شبکه یا چه شخصی مسئول Backup گیری است.
۲. **مثبت بودن :** از عبارات و جملات مثبت استفاده کنیم و هیچ موقع با قطعیت در مورد مسائل امنیتی صحبت نکنیم .

۳. **آموزش و آگاهی :** راه کار آموزشی ارائه دهیم.
۴. **اطمینان از شناخت محیط امنیتی :** تمام نقاط تاریک و روشن امنیتی را باید بدانیم ، اینکه جایی از سازمان اطلاعات مهمتری دارد و کدام اطلاعات مهم هستند ، کدام قسمت سازمان گروه های کاری موفق تری دارد و یا در کدام قسمت از سازمان افراد مهمی قرار دارند و همچنین این نکته را باید در نظر گرفت که آیا اصلا سازمان نیاز به اینترنت دارد یا نه .
۵. **واضح نویسی :** واضح نویسی را باید در سیاستهای سازمان لحاظ کنیم ، تمامی مجلات و مقالات امنیتی باید به زبان ساده باشند تا افراد غیر متخصص بتوانند از آن استفاده نمایند .
۶. **تعیین رویکرد پایه در سازمان :** رویکرد پایه در حقیقت همان Base کاری میباشد .
۷. **دفاع در عمق :** مثل طبقه ای که رئیس کل در آن است باید از لحاظ شبکه ای ایمن باشد تا خطرات داخلی دفع شود .
۸. **اشکالات امنیتی مبتنی بر جهل مهاجم :** دردنیای شبکه هیچ امری محال نیست ، راه نفوذ برای همه موارد وجود دارد ، نباید هیچ زمانی نفوذگران را دست کم بگیریم .
۹. **افشای مسئولانه :** نقاط ضعف امنیتی از این طریق مشخص میگردد ، باید آگاهانه کاری را انجام دهیم و در اختیار عموم بگذاریم مانند اینکه اجازه ندهیم کاربران از یک حفره امنیتی استفاده کنند یا مانند اینکه به کارکنان اطلاع دهیم که ایمیل ها حاوی ویروس میباشند و نباید آنرا باز کنند .

امنیت کارکنان :

۱. **توجه به امنیت در استخدام کارکنان است :** باید پیشینه های شخصی که قرار است در سازمان استخدام شود از لحاظ امنیتی بررسی نمایید مانند محیط تحصیل ، افراد هم دانشگاهی با شخص مورد نظر و ...، همچنین باید گواهی عدم سوء پیشینه صادر شود.

۲. **بررسی سوابق اعتباری یک متخصص میباشد:** مانند استفاده از دستگاه های دروغ سنج همچنین از بدقولی های دوستانه گرفته تا مالی را شامل میشود .

۳. **ارائه ی ضمانت نامه های معتبر** مانند ضمانت کردن شخص توسط اشخاص معتبر

۴. **بررسی دوره ای افراد بسیار مهم است** ، اینکه با چه اشخاصی در ارتباط است .

۵. **آموزش های اولیه** ، افراد استخدام شده باید نسبت به سازمان آموزش ببینند و این آموزش ها نسبت به کارهایی که میخواهند انجام دهند تغییر میکند.

۶. **آموزش مدام باشد** ، مانند آموزش های ضمن خدمت که افراد باید مسائل جدید را آموزش ببینند ، مخصوصا مسائل امنیتی که بروز است و مدام در حال تغییر و تحول میباشند .

۷. **کنترل کارایی** ، بازرسی های دوره ای و واضح که این کار توسط مدیران ارشد صورت میگیرد و این کار با استفاده از نرم افزارهایی که در سازمان پیاده سازی میشوند صورت میگیرد مانند سیستم های حضور و غیاب و استفاده از دوربین های امنیتی .

۸. **باربینی دسترسی ها :** دسترسی ها باید به صورت دوره ای بررسی شوند مانند رفت و آمد به بخش های مختلف سازمان وارد شدن به سیستم های کامپیوتری, استفاده از دستگاههای ذخیره سازی و.... تمامی این موارد باید توسط مسئولین و مدیران ارشد, بازرسی و کنترل شوند.تا کارکنان به خاطر اطلاع از اینکه فعالیت های آنها در سازمان کنترل میشود از اقدامات خرابکارانه پرهیز کنند.

۹. تفکیک وظایف : در هر سازمان باید وظیفه هر شخصی کاملا مشخص باشد زیرا زمانی که وظایف مشخص باشند جوابگویی در سازمان نیز براحتی امکان پذیر خواهد بود.حدالامکان باید سعی شود به صورت کتبی وظایف هر کدام از کارکنان یادآوری شده و بصورت مستند تعهد آنها نسبت به اطلاع از وظایفشان را به صورت کتبی نگهداری کنیم.

۱۰.رعایت حداقل دسترسی ها : در هر سازمان باید برای هر یک از کارکنان حداقل دسترسی های لازم را در نظر گرفت. به عنوان مثال: لزومی ندارد در یک سازمان پسورد فایروال در اختیار تمامی کارکنان باشد.

۱۱. وابستگی , به کارمندان کلیدی را به حداقل برسانیم.باید سعی شود تمام فعالیت ها و اطلاعات کلیدی و مهم سازمان, در اختیار شخص خاصی نباشد.به دلایل مختلفی ممکن است آن شخص مورد نظر امکان کار در سازمان را برای مدتی یا همیشه نداشته باشد ,در این صورت باید سعی شود در حین دوران خدمت وی , شخص یا اشخاصی بعنوان جایگزین وی با او همکاری داشته باشند یا اینکه اطلاعات یا فعالیتهای کلیدی به صورت مستند توسط وی در اختیار سازمان قرار داده شود.

برون سپاری امنیت:

اول اینکه , سعی شود تحلیل کار و پیاده سازی و سیاست نویسی مسائل امنیتی به بیرون از سازمان سپرده شود برای این منظور باید توجه کرد که اول چه زمینه های از سازمان باید برون سپاری شوند.

دوم اینکه, آیا بخش امنیت را به عنوان بخشی از سازمان خود در نظر بگیریم یا خیر .

مراحل زیر در انجام برون سپاری باید رعایت شوند:

۱. **انتخاب فروشنده مطمئن و خوب** : مثلا در شرایط کنونی خریدار آنتی ویروسی که متعلق به کشور هایی که تحریم کننده ایران باشد, چندان مناسب نخواهد بود.در عوض میتوانیم از کشورهایی خریداری کنیم که روابطه بهتری با کشور ما داشته باشند.

۲. **انتخاب راهنما یا معرف مطمئن:** دو نکته برای انتخاب راهنما وجود دارد:

الف) خود معرف ها وسابقه کاری فرد را بررسی کنیم و همچنین خصوصیات فرد راهنما را بشناسیم.

ب)افراد در ارتباط با شخص معرف را نیز بررسی نماییم

۳.پایداری و تداوم شرکت را برسی نماییم : در این زمینه دو نکته وجود دارد

الف) قبل از تحویل کار که اولین مرحله باید مشخص شود شرکت مربوطه در گذشته چه کارهایی انجام داده و با چه مشکلاتی مواجه بوده است.

ب) قبل از تحویل کار, دادن اطمینان از اینکه در آینده تا چه حد در کنار شما خواهند بود وچه تعهداتی در قبال وظایفشان بر عهده گرفته اند .باید سعی شود به شرکتهایی با نرخ پایین, اعتماد نشود.

۴. مراقب فریبکاران باشیم : شرکتهایی که مثلا تمام کارهای مربوط به شبکه را انجام میدهند معمولا تمایل دارند مسائل امنیتی را نیز خودشان برعهده بگیرند در این صورت هنگام بروز مشکل در این سازمان , تفکیک مشکلات امنیتی در سازمان , تفکیک مشکلاته امنیتی با مشکلات شبکه بندی دشوار خواهد بود و تیم طراح شبکه میتواند سازمان را فریب دهد.

تدوین آئین نامه های دولتی وسیاست های حریم خصوصی و قانون نویسی:

در کشورهای مختلف قوانین مختلفی در رابطه با جمع آوری اطلاعات از شهروندان وجود دارد, و هر کشوری به نسبت سیاست های خود, آیین نامه های خاصی را در این زمینه اجرا میکند.

۱-آیین نامه راهکارهای اطلاعات بازار ۲-راهکارهای سازمانی همکاری و توسعه اقتصادی

۱. **آیین نامه راهکارهای اطلاعات بازار:**

منظور از بازار محل خرید و فروش و نقل و انتقال پول میباشد. بلکه محیط هایی است که اطلاعات(چه اطلاعات مالی و چه اطلاعات شخصی و سازمانی)در آن گردش دارند.

اصل اول:

این اصول بیان میکند که هیچ سیستم نگهداری سوابق داده های شخصی نباید به صورت مخفی وجود داشته باشد.

اصل دوم :

باید راهی وجود داشته باشد که هر کس بتواند از اطلاعات ذخیره شده مطلع شود.

اصل سوم :

باید راهی وجود داشته باشد که افراد بتوانند, ازهدف بکارگیری اطلاعات مطلع شده و در صورت تخلف از آن جلوگیری نمایند.

اصل چهارم :

باید راهی برای اصلاح اطلاعات توسط خود فرد وجود داشته باشد.

اصل پنجم :

هرسازمانی که داده های شخصی را جمع آوری میکند باید قابلیت اطمینان داده ها را تضمین نماید.

۲. راهکارهای سازمانی همکاری و توسعه ی اقتصادی :

اصل محدودیت جمع آوری اطلاعات :

باید تنها اطلاعاتی که مورد نیاز سازمان است, جمع آوری شود و این اطلاعات جمع آوری شده باید با رضایت خود همراه باشد.

اصل کیفیت داده ها :

داده های شخصی جمع آوری شده باید مرتبط با هدف جمع آوری شده باشد.

اصل تعریف هدف :

هدف سازمان باید برای شخصی که ازآن اطلاعات جمع آوری میشود, کاملا مشخص باشد, چرا که این اطلاعات جمع آوری میشوند اگر هدف های بعدی با هدف هایی متفاوت باشند این تغییرات باید به اطلاع شخص برساند.

اصل محدودیت استفاده :

داده های شخصی نباید افشا شوند ویا در دسترس عموم قرار گیرند و اینها اصول کلی هستند. و باید در هر کشوری بومی سازی شوند.

اصل حفاظ های امنیتی:

دادهای شخصی باید در مقابل تخریب و سرقت حفظ شوند.

اصل باز بودن :

باز بودن یا Open source بودن سیاست های امنیتی این است که اطلاعات هرشخصی برای خودش شفاف باشد.

اصل مشارکت فردی :

در این اصل گفته میشود که هر کسی باید این حق را داشته باشد که

۱. بفهمد چه اطلاعاتی از وی دردست گردآورنده آن وجود دارد.
۲. با گردآورنده اطلاعات بتواند در هر لحظه ارتباط داشته باشد.
۳. اگر یکی از خواسته های فرد, رد شود برای آن دلیلی بخواهد.

اصل پاسخگویی :

هرکسی که اطلاعاتی را جمع آوری میکند,باید درمقابل آن پاسخگو باشد.

ایجاد فرهنگ امنیت :

۱۲ لایه امنیت الکترونیکی : مدیریت مخاطرات امنیتی را می توان نوعی فرآیند دو وجهی دانست:

اولین گام آن ارزیابی مخاطره است که شامل سه قسمت می باشد :

۱. شناسایی و جمع آوری دارایی
۲. تجریه و تحلیل و تعیین ارزش هریک از دارایی ها
۳. تعیین اینکه هرکدام تز دارایی ها بترتیب اولویت چقدر حیاتی هستند

گام دوم امنیت تدوین یک شیوه برای مدیریت مخاطرات است

لایه اول

تعیین مسئول امنیت اطلاعات : ایجاد سمت مدیریت اطلاعات که از توجه به ۱۱ لایه دیگر در سیاست های سازمان کسب اطمینان کند

لایه دوم

مدیریت مخاطرات : همواره برای دارایی ها و مخاطرات مربوط به آنها از روش های تعریف شده مدیریتی استفاده کنیم

لایه سوم

کنترل دسترسی و تصدیق هویت : یعنی اینکه همیشه بررسی کنیم که هرکاری در سازمان توسط چه شخصی و با کدام کامپیوتر انجام گرفته و این موارد نیز به اطلاع تمامی کارکنان برسانیم (فرهنگ سازی کنیم)

لایه چهارم

دیوراه آتش: در سازمان از دیواره های آتش استفاده کنیم.

لایه پنجم

غربال کردن محتوا بصورت فعال : در سطح مرورگرها وب لازم است هرآنچه که مناسب محیط کارنیست و با سیاست های مصوب مغایراست تسویه شود

لایه ششم

استفاده از سیستم های مهاجم یاب: این یک سیستم مختص شناسایی نفوذها یا تلاش ها برای نفوذ می باشد ، نفوذهایی که ممکن است بصورت دستی یا به کمک سیستم های خبره نرم افزاری انجام شود

لایه هفتم

ویروس یاب ها : باید در سازمان بر روی کامپیوتر ها از نرم افزارهای ویروس یاب استفاده کنیم و همچنین آموزش استفاده از ویروس یاب ها و همچنین یک سری اصول کلی کار با کامپیوتر بصورت امن را به آنها آموزش دهیم

لایه هشتم

رمزنگاری : الگوریتم های رمز نگاری برای حفاظت از اطلاعات در حال انتقال و یا درمعرض سرقت باید به کار رفته شود

لایه نهم

آزمون آسیب پذیری : در بازه زمانی مشخص سازمان از نظر مسائل امنیتی و میزان امن بودن در برابر خطرها بررسی کنیم

لایه دهم

راهبری صحیح سیستم ها : در این موارد باید با تهیه فهرستی از خطاهای رایج که عموما در موسسات یا شرکت های مالی رخ می دهد و نیز فهرستی از الگوها سرآمدی تکمیل گردد.

لایه یازدهم

نرم افزار مدیریت سیاست : لازم است که یک برنامه نرم افزاری به کنترل اجرای صحیح سیاست ها و روال هایی که برای استفاده کارمندان از کامپیوتر ها تدوین شده اند بپردازد

لایه دوازدهم

طرح واکنش وب رخداد و تداوم کسب و کار : این سند اصلی ترین سندی است که سازمان درآن میگوید چگونه یک رخداد امنیتی را شناسایی می کنیم و چگونه به آن واکنش دهیم و آسیب های آن را ترمیم دهیم

مسئولیت های کارکنان :

به منظور ترویج فرهنگ امنیتی باید مدیران موارد زیر را در نظر بگیرند :

۱. توضیح دهند که عناصر یک برنامه امنیتی خوب چه چیزهایی هستند
۲. تاکید کنند که امنیت در تمام سطوح سازمان بسیار مهم است
۳. افراد را نسبت به پرسیدن سوال در زمینه فناروی و روال های امنیتی ترغیب نمایند
۴. ازکلیه کارکنان بخواهند در این رابطه بسیار هوشمند بوده و هرگونه فعالیت غیر معمول را گزارش دهند

فهرست کنترل بازنگری مخطرات عبارت اند از :

۱. آیا اخیرا ارزیابی مخطرات صورت گرفته است و این ارزیابی هرچند وقت یکبار صورت می گیرد
۲. آیا سیستم برحسب حساسیت مخطرات تقسیم بندی شده اند یا خیر
۳. آیا برای آزمودن نتایج ارزیابی مخطرات بازبینی های منظم انجام میگیرد یا خیر
۴. آیا تمام کارمندان براساس اهداف امنیتی مورد نظر ارزشیابی شده و منصوب شده اند یاخیر.

فهرست امنیتی شبکه داخلی عبارت اند از:

۱. آیا برای پیکربندی سیستم ها ، سیاست ها و روال های معین وجود دارد یا خیر
۲. آیا این سایت ها و روال ها شامل مجوزهای دسترسی به فایل ها ، رمز های عبور و بسته ها می شوند یا خیر
۳. آیا خدمات غیر ضروری را غیرفعال کرده ایم یا خیر
۴. آیا همه ی کاربران رمز عبور دارند یا خیر
۵. آیا حساب های پیش فرض که در سیستم موجود اند تغییر داده شده اند یا خیر
۶. آیا حساب هایی که مورد استفاده قرار نمی گیرند بصورت منظم غیر فعال می شوند یا خیر

فهرست کنترل شبکه های خارجی و دیواره های آتش :

۱. آیا فردی بصورت منظم تنظیمات دیواره آتش را بازبینی می کند و این کار را هرچند وقت یکبار میدهد
۲. آیا کسی مسئول آزمون نفوذ پذیری بر دیواره ی آتش است یا خیر
۳. آیا مشخص است که مسئولیت بروز رسانی دیواره ی آتش برعهده ی چه کسی است
۴. آیا نرم افزار مهاجم یاب روی سیستم ها و شبکه ها نصب شده اند یاخیر
۵. آیا نرم افزار ضد ویروس درتمام نقاط ورود شبکه نصب شده است یا خیر
۶. یا برای بهبود فرآیند تجربیات نفوذ به اشتراک گذاشته می شود یاخیر.

**********پایان**********

خداوندا چنان کن سرانجام کار

توخشنود

باشی و ما ...

رستگار ...