سامانه های حفاظتی :1- سخت افزار 2- نرم افزار
اهمیت :1- همیشگی و با ثبات 2- متغیر بسته به فناوریهای نوین فرق می کند .
تعریف عام حفاظت :سلسله اقداماتی است که از جانداران و اشیائ در برابر خطرات طبیعی و غیر طبیعی که به افزایش ضریب اطمینان کمک می کند .
مفهوم خاص حفاظت: به اقداماتی گفته می شود که از اهداف طبقه بندی شده سازمانها در برابر آسیبهای پذیرهای ذاخلی و تهدیدات خارجی محافظت می نماید و ضمنا تامین اعتبار و ارتقای سازمانی موجب برقراری امنیت بر جامعه می شود.
کلید واژه های تعریف : 1- طبقه بندی 2-آسیب پذیریها 3- تهدید 4- اعتبار و ارتقای سازمانی 5- تولید امنیت
اصول حفاظتی $=$ حفاظت در پدافند غیر عامل : اساس و حیات بشر اطلاعات می باشد .بدون اطلاعات بشر قادر به زندگی نیست.
1-اطلاعات :راجع به همه موضوعات مثال: شناخت آسیب پذیری ها ، تهدیدات خارجی
2- اصل تناسب : 1-اهمیت و ارزش اهداف حفاظتی 2- حساسیت ماموریت اطلاعات و ایمنی 3- ترکیب متناسب و صحیح اقدامات حفاظتی4- همسنگی اقدامات تعدیلی با جرائم حفاظتی 5- اقدامات بسته به میزان تهدید متناسب باشد 6- فرهنگ سازمانی در پذیرش حفاظت 7- توجه به شرایط زمانی و مکانی
3- زمان بندی : اقدامات حفاظتی را به موقع انجام دهیم
4- تکنیک ها و فناوریهای نوین: کمک کردن به صرفه جویی ، شناخت تهدیدات و مقابله به آن
5- اشراف حفاظتی: نقطه مقابل اشراف اطلاعاتی می باشد
6- اصل اخلاق اطلاعاتی : هر صنف و فعالیتی به یک مبانی اخلاقی اعتقاد دارند باید ها و نبایدهای که در اقدام حفاظتی باید به آنها اعتقاد باشیم و اصول اعتقادی را رعایت کنیم (زیر مجموعه ها : امانت داری ، راستگویی، خدا ترسی ، فروتنی ، حق گویی ، وفاداری و....)
7- اصل کفایت: اقدامات حفاظتی نباید در تضاد با اقدامات قبلی باشد و اختلال در اقدامات انجام ندهد (عدم غافلگیری توسط دشمن و اقدام های حفاظتی باید کافی باشد و اقدامات باید موثر واقع شود و اقدامات دشمن را خنثی نماید.)
پدافند غیر عامل : عبارتست از کلیه اقدامات احتیاطی به غیر از استفاده از جنگ افزار و تسلیحات به منظور به حداقل رساندن آسیب پذیریها و تهدیدات دشمن که شامل اعلام خبر ،اختفاء و استتار ، تفرقه و پوشش و فریب ، مقاوم سازی ، مکان یابی و....
طبقه بندی اماکن 1-مراکز ثقل : مراکز و تاسیسات پر اهمیت کشور می باشند که در صورت حمله و بمباران و انهدام آنها صدمات جدی به نظام اجتماعی و سیاسی و نظامی کشور وارد شده و آن را در یک مخاطره جدی قرار می دهد .
2-مراکز حیاتی : مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها موجب بروز بحران و صدمات قابل توجه در نظام سیاسی هدایت و کنترل فرماندهی در سراسر کشور ایجاد می شود .
3-مراکز حساس: مراکزی هستندکه در صورت انهدام آنها آسیب وصدمات محدوددر نظام سیاسی اجتماعی باسطح تاثیرگذاری منطقه در کشور میباشد.
4-مراکز مهم : مراکزی هستند با تاثیر گذاری محلی در کشور می باشد .
اصول پدافند غیر عامل : استتار ، اختفاء ، پوشش ، فریب ، تفرقه ، پراکندگی ، مقاوم سازی ، اعلام خبر
اهمیت پدافند غیر عامل :1- موجب زنده ماندن و حفظ بقای نیروی انسانی می باشد.2- صرفه جویی کلان ارزی و اقتصادی 3- جلوگیری از فلج نمودن کشور و ادامه فعالیت های حیاتی کشور 4- موجب تحلیل هزینه بر دشمن می شود 5- افزایش روحیه شهروندان 6- نسبت به دفاع عامل مخارج کمتری دارد 7- سهل الوصول بودن تجهیزات 8- پیشگیری بهتر از درمان است .
سیستم در لغت به معنای سازمان ، نظام و دستگاه است .
تعریف سیستم : یک مجموعه اجزاء و روابط میان انهاست که توسط ویژگی های معین بهم وابسته و این اجزاء با محیط آن یک کل را تشکیل می دهند.
موارد در تعریف سیستم : 1- بین انها ارتباط متقابل و منظم وجود دارد.2- برهم اثرداشته و تاثیر متقابل 3- به صورت کل عمل میکند4- هدف دار هستند
نگرش سیستمی : دیدگاهی است که به ما اجازه می دهد تا نیروها با متغیر های که در محیط داخل و خارج سازمان تاثیر اساسی دارند شناخته و به عملکرد آنها در سازمان پی ببریم .
نظریه سیستمی : فعالیت هر جزیی از سیستم به فعالیت سایر اجزا ان اثر می گذارد و موجب میشود مدیران به سازمان به صورت کل نگاه کنند.
ویزگی های سیستم : 1- حداقل از دو جزء تشکیل شده اند.2- اجزا با هم ارتباط داشته اند 3- حتما بر روی یکدیگر اثر می گذارد 4- همیشه خصوصیات سیستم متفاوت تر از اجزا می باشد.
اجزائ سیستم :1-ورودی(داده ، دورنداد):عناصری که وارد سیستم می شوند .
2-خروجی (ستاده ، برونداد): چیزهای که به محیط خود یا سیستم های مجاور صادر می کند.
3-فرایند (پردازش): پردازش و عملیاتی که روی داده انجام می دهد و انرا افزایش و یا تغییر می دهد
4- بازخورد (feedback)کسب اطلاعات لازم درباره عملکرد سیستم را گویند
5- محیط سیستم :سیستم از عوامل محیطی تاثیر می پذیرد و بر ان تاثیر می گذارد به عبارت دیگر عوامل محیطی مانند عوامل طبیعی فرهنگی ایدولوژی سیاسی و اجتماعی به هم کنش و واکنش متفاوت دار ند به این ترتیب محیط سیستم را عوامل تشکیل می دهند که اگر جزئ سیستم نیستند اما با تغییر در هر یک از انها می توانند موجب تغییراتی در سیستم شود .بنابر این محیط سیستم شامل کلیه متغیرهای است که می توانند در وضع سیستم موثر باشند و یا از سیستم تاثیر بپذیرند .
دسته بندی یا اقسام سیستم ها :
1- بر اساس ایجاد (به وجود امدن):1-طبیعی :هرموجود زنده ، طبیعت چیزی که بشر در ان نقش ندارد مثل اب و هوا
2- مصنوعی: توسط بشر ایجاد شده اند ابعاد زندگی بشر را شامل می شود مثل سامانه حفاظتی
2-بر مبنای عناصر تشکیل دهنده : 1- انسانی 2- ماشینی 3- ترکیب انسانی و ماشینی مثل خودرو ، لوازم خانگی ، دوربین اپتیک و انسان
3- از لحاظ تاثیر متقابل : 1- سامان های باز (مثل:کلیه سازمانهای پزشکی ، نظامی ، آموزشی و شهری و حمل ونقل )
2-سامانه های بسته : (مثل کاربراتور ، ترانس برق ، اسپیلیت)
4- بر حسب پایداری : 1-دائمی (کمتر به دست بشر درست شده اند )2-موقت (این سامانه ها به دست بشر ساخته شده اند)
5- بر مبنای یک نواختی:1-پایگاهی (یک طرح سامانه دفاعی که به مطالعه طولانی وهزینه زیاددارد) 2-غیر پایگاهی(مثل:ستاد انتخاباتی یاگروه تحقیقی)
6- بر اساس سلسله مراتبی : (هر سامانه درون یک سامانه بزرگتر قرار دارد )1- اصلی(مثل سیستم موتور خودرو ، بدن انسان ، جامعه ) 2- فرعی (مثل: یک انسان دورن یک کلاس درس دورن دانشگاه درون دانشگاه جامع دورن وزارت علوم و ...........................)
7-بر حسب انطباق :(سازمانهای حفاظتی در کلان دارایی انعطاف هستند شاید در جزء به صورت منعطف باشند)
1-منعطف:(بر مبنای بقا به محیط پاسخ می دهد ، متناسب با تهدید)2- غیر منعطف (مثل حسابداری اعداد رقم)
خصوصیات ویژگی های سامانه کارآمد:
1-جامعیت وجودی : همه سامانه با یکدیگر و یکجا بکار می اید و به صورت تک تک فاقد کارایی می باشد
2- سلسله مراتبی بودن : ارتباط بین جزء و کل یا خرد و کلان وجود دارد .
3- همبستگی اجزاء :در هر سازمان یک تعامل بین سامانه ها وجود دارد و با یکدیگر ارتباط و همبستگی دارند .
4- تناسب اجزاء : حداقل تناسب در بین اجزائ باشد هماهنگی وسخیت زیاد با یکدیگر داشته باشند
5- چرخه مشخص: هر سامانه باید دارایی یک چرخه مشخص باشد مثل ورودی پردازش خروجی
6- تولید مثل داشته باشد (خود احیایی): جامعه باید دارایی دگردیسی یا پیشرفت داشته باشد
7- هم پایانی : هرچند کارکرد یک سیستم ممکن است متفاوت باشد اما خروجی و هدف آن ها یکی می باشد
8-تفوق بر فنا : نباید اجازه به مردن یک سامانه دهد .بایستی از نابودی خودش جلوگیری کند
9- گرایش به تکامل داشته باشد .
سامانه حفاظتی : مجموعه از اجزای بهم وابسته که به علت وابستگی حاکم بر اجزای خود کلیت جدیدی را به منظور حفاظت و پیشگیری از آسیب ها و تهدیدات پدید می اورد .کارویژه های سامانه حفاظتی در سازمان های مختلف به وظایف و مسئولیت های قانونی آن سازمان ها بستگی دارد لیکن به طور کلی این کارویژه ها عبارتند از حراست، پیشگیری، نظارت بر محافظت یا تامین حفاظت کارکنان
ویژگی های سامانه حفاظتی : 1-رکن اصلی ساختار امنیتی است 2- مسئولیت صیانت از سرمایه های ملی را بر عهده دارد 3- از وظایف اصلی هر سازمان است 4- اختیارات فرا حیطه ای دارد و در تمام عرصه ها ورود می کند. 5- دارای حداکثری تعاملات با مجموعه سازمانی است.6- گزارش گیری از عموم و گزارش دهی بر مدیران را برعهده دارد 7- ارتباطات عمودی و افقی گسترده ای دارد
روشهای حفاظت از شخصیت ها : 1-گماردن محافظ 2- بازرسی بسته ها 3- حفاظت از مسیر حرکت 4-حفاظت در محل کار یا اقامت 5- نظارت بر مواد غذایی دارویی، آشامیدنی 6- حفاظت از وسایل نقلیه 7- اقدامات فریبنده تامینی 8- تایید صلاحیت نفرات محافظین امنیتی (احراز صلاحیت)
ابعاد تهدیدات شخصیت ها: 1- فیزیکی شخصیت مثل سلاح گرم و سرد که باعث کشته شدن می شود 2-ترورکردن مثل مواد رادیو اکتیو -پودر سرطان زا-3-از راه دور و نزدیک شیمیایی و میکروبی –انتحاری -4-تهدیدات روانی شخصیت مثل توهین-افترا جنگ رسانه ای (فتنه 88)
سامانه حفاظتی : 1- حفاظت گفتار و ارتباطات 2- حفاظت اسنادو ومدارک 3- کارکنان 4- اماکن و تاسیسات 5-وسایل و تجهیزات 6-فضای سایبر
الگوهای مقابله با تهدیدات موجود در فضای سایبر :
1- اتخاذ سیاست های حفاظتی در استفاده از فناوری :سطح بندی صحیح اطلاعات –آموزش کاربران اطلاعاتی –رمزگذاری اطلاعات و استفاده از امضای دیجیتال –تغییر مدوام در الگوریتم های استفاده شده در سیستم ها مثل صدای جنگل منحصر بفرد –استفاده از انواع امکانات امنیتی مثل آنتی ویروس و...- استفاده از آزمون نفوذپذیری –استفاده از سامانه پشتیبانی و اطلاعات –بازرسی تجهیزات سامانه های رایانه و سایبری
2- حفاظت از اسناد رایانه ای : حالت دیجیتالی و الکترونیکی نامه ها و ورقه های کاغذی می باشد – جمع آوری داده ها ،جلوگیری از انتشار غیر مجاز -
ویرایش داده ها و حذف اضافه ها و چینش صحیح – بهنگام نگه داشتن داده ها ، اطلاعات بروز باشند – تهیه نسخه های پشتیبان – برنامه بازیابی در هنگام وقوع حوادث – تعیین گزارش دوره نظارت و نوبه ای حفاظتی
3- حفاظت از بانکهای اطلاعاتی : با جهانی شدن شبکه های اطلاع رسانی و ارتباطات رایانه ها با یکدیگر از طریق شبکه های جهانی بسیاری از شرکت ها و سازمانها با مقوله ی دیگری از حفاظت اطلاعات روبرو شده اند وآن مسئله حفظ اطلاعات موجود در شبکه های محلی در قبال دسترسی غیر مجاز خارج از شبکه مورد نظر است .
انواع نظارت بر بانک اطلاعاتی : 1-نظارت تعریف داده 2- نظارت دستیابی 3- ردیابی 4- نظارت به روز بودن 5- نظارت هم زمان
امنیت فیزیکی رایانه : 1-براساس آنچه فرد می داند 2- بر اساس آنچه فرد دارد 3- براساس آنچه که فرد چه کسی است(بهترین روش ترکیبی می باشد)
حفاظت فیزیکی رایانه در برابر خطرات و مخاطرات طبیعی و انسانی : الف-سامانه اطفاء حریق ب- سامانه نظارت آب (روکشهای ضداب، کفهای زه کشی شده )ج- سامانه حرارتی ح- سامانه پشتیبانی
بانک های اطلاعاتی : مجموعه ای از داده های بهم وابسته که از افزونگی (انباشتکی)بی حاصل داده ها جلوگیری و ضمن نگهداری و اعمال قوانین حاکم برآن صحت و سلامت اطلاعات را تضمین می کند .
ویژگی یا شرایط بانک اطلاعاتی :1- امنیت بالا 2- سرعت پردازش و انتقال اطلاعات عالی 3- سهولت ترمیم و بازیابی و تصحیح داده ها در شرایط ویژه 4- با توجه به ارزشمندی دیتا سعی کنید از نرم افزار اصل استفاده شود 5- وحدت یکپارچگی ذخیره داده ها 6- امکان تهیه نسخه های جدید
رعایت نکات ایمنی در بانکهای اطلاعاتی :1-ایجاد کنترل و دسترسی کاربران در سطوح مختلف با توجه به شرح وظایف هر کارمند 2- توانایی بالا جهت کاهش خطرات احتمالی در برابر وقوع حادثه 3- اطمینان ازمحل نگهداری داده بخصوص روی سرور ها 4- تسلط و مهارت کافی مدیر سایت 5- تدوین راهکار مناسبی جهت انهدام اطلاعات موجود تحت شرایط ویژه 6- استفاده از سیستم برق اظطراری به منظور جلوگیری از صدمه خوردن به سرور ها و بانک اطلاعات 7-تهیه نسخه پشتیبان 8- تست نوبه ای و برنامه ریزی شده به منظور صحت اطلاعات
4- حفاظت شبکه های رایانه ای : تعریف: برنامه های آماده ای هستند که به منظور کنترل و به دستگیری امکانات سرور و مدیریت منابع در شبکه ها در جهت ایجاد خدمات و امکانات بیشتر و بهتر در شبکه مورد استفاده قرار می گیرد.
\*کلیه امکانات مورد نیاز مدیر شبکه را به منظور کنترل مجموعه سیستمی شبکه در اختیار وی قرار می دهد:1- کنترل کاربران بر دسترسی به اطلاعات شبکه 2- کنترل و بررسی بار سیستمی در هر لحظه 3- بررسی حجم اطلاعات قابل انتقال در خطوط شبکه
5- امنیت در اینترنت : اینترنت به طور مطلق فضای ناامنی می باشد .مثل استراق سمع-نقش بازی کردن –پست الکترونیکی-کشف رمز
6- حفاظت فیزیکی رایانه ها : 1-استفاده از رمز ورود 2- حفاظت از ساختمان و دوربین 3- جلوگیری از آسیب ناشی از حوادث و بلایای طبیعی
حفاظت از اسناد رایانه ای :1- جمع آوری داده ها و همچنین جلوگیری از ان 2- ویرایش داده ها 3- به هنگام نگه داشتن رایانه ها 4- تهیه نسخه های پشتیبان 5- برنامه بازیابی اطلاعات 6- تهیه گزارشهای دوره ای نظارت حفاظتی
\*\*\*حوادث غیر مترقبه و توجه به بلایای طبیعی در مورد رایانه ها و آسیب های وارده به رایانه ها –نظارت به دسترسی افراد به تجهیزات و اطلاعات رایانه ها استفاده از رمز ورود –حدود دسترسی کاربران تعیین شده باشد – استفاده از دوربین برای نظارت برفعالیت کارکنان

حسینی:
ضرورت توجه به امنیت فناوری اطلاعات: 1-ضعف آموزشی در شبکه های رایانه ای 2- عدم آموزش و توجیه صحیح تمامی کاربران 3- عدم وجود دستور العمل های جامع برای پیشگیری از نقایص امنیتی 4- عدم وجود سیاست های مشخص و مدون به منظور برخورد مناسب و به موقع با اشکالات امنیتی
تهدیدات: هکرها- کدهای مخرب-ویرانگران-نامه های الکترونیکی ناخواسته- نرم افزارهای جاسوسی-سیستم عامل-تهدیدات فیزیکی
نقش عوامل انسانی در تهدید شبکه های کامپیوتری: اشتباهات متداول مدیران سیستم-اشتباهات متداول مدیران سازمان-اشتباهات متداول کاربران معمولی

عباس زاده:
1- امنیت داده‌‌ها و اطلاعات : بی شک اطلاعات، یکی از ارزشمندترین دارایی های سازمان ها و کسب و کارهای امروز است و نگرش اصولی مدیران به این موضوع، دغدغه حفاظت از این دارایی ها را در ذهن آن ها ایجاد خواهد نمود نتایج تحقیقات انجام شده، بیانگر این واقعیت است که سالانه نیمی از کاربران کامپیوتر، اطلاعات خود را به اشکال مختلف از دست می دهند. بروز نقص در تجهیزات ذخیره سازی داده ها، خطاهای انسانی، سرقت کامپیوترها، حملات ویروسی و خطاهای نرم افزاری و نیز حوادثی نظیر آتش سوزی و زلزله، از شایع ترین عوامل تخریب و از دست دادن اطلاعات و داده های کامپیوتری و دیجیتال است ارتباط مستقیمی بین میزان امنیت فیزیكی و امنیت داده‌ها و اطلاعات وجود دارد.
در حقیقت، هدف بسیاری از حملات و خرابكاری‌های درسامانه‌ها، كارگزارها و شبكه‌‌ها، نفوذ ودسترسی به اطلاعات و داده‌‌های حساس سازمان‌هامیباشد.

2- كلید‌های محفظه‌‌ها/مخازن امنیتی:در این بخش منظور از كلید انواع كلید‌های مكانیكی، شماره شناسایی خصوصی، كارت‌های دسترسی و یا تركیبی از دو یا چند مورد فوق می‌باشد.
 برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:

-كلید‌های محفظه‌‌ها/ مخازن امنیتی باید با توجه به بالاترین درجه حساسیت اطلاعات و یا تجهیزاتی كه توسط آن قابل دسترسی هستند، محافظت شوند. -كلید‌های محفظه‌‌ها/ مخازن امنیتی باید زمانی كه یكی از موارد زیر محقق شد، تغییر‌كنند:

-شواهدی از حمله و یا نفوذ رؤیت شود.تهدیدات و خطرات غیرقابل قبولی مشاهده شود. -فردی كه به این مكان‌ها دسترسی داشته است، تغییر كند

-ذخیره سازی امن و پایدار داده های- حفاظت از داده های دیجیتال در برابر تخریب و دسترسی غیر مجاز

3- داده‌های در حال تبادل: شنود و یا استراق سمع الكترونیكی یكی از هوشمندانه‌ترین راه‌های سرقت داده‌های در حال تبادل محسوب می‌شود. امروزه مهاجمین با كمترین تجهیزات ممكن نیز قادر به شنود و رونوشت تمامی فعالیت‌های انجام شده روی كامپیوتر قربانی هستند؛ نظیر ثبت تمامی كلید‌هایی كه بر روی صفحه كلید فشار داده می‌شوند، تمامی اطلاعاتی كه روی یك مانیتور نمایش داده می‌شوند و تمامی فایل‌هایی كه برای چاپگر ارسال می‌شوند. انواع روش‌های شنود و محافظت در مقابل آن‌ها به شرح ذیل می‌باشد:1- شنود از طریق كابل‌ها و سیم‌ها2- شنود از طریق اینترنت 3-شنود از طریق ماهواره ها
برخی از ملاحظات پدافند غیرعامل در پشتیبانی از داده به شرح ذیل است:

پشتیبان‌‌ها در مكان‌هایی كه توسط عموم قابل دسترسی هستند، قرار داده نشوند.- پشتیبان‌ها ونسخه‌های اصلی می‌بایست در مكان‌های جداگانه نگهداری شوند.- تمامی رسانه‌‌های ذخیره‌سازی می‌بایست به صورت «غیرقابل نوشتن » ذخیره شوند.- برای حفاظت از اطلاعات نسخه‌های پشتیبان، ‌باید از قفل‌های سخت‌افزاری و نرم‌افزاری استفاده شود- قبل از دور‌انداختن رسانه‌های ذخیره‌سازی، اطمینان حاصل شود كه داده‌های موجود بر روی آن‌ها کاملاً پاك شده‌اند. یكی از مطمئن‌ترین راه‌های امحاء رسانه‌‌های ذخیره‌سازی تخریب فیزیكی می‌باشد.

امنیت فیزیكی یك شبكه در بردارنده امنیت موارد زیر است:

منابع فیزیكی موجود در شبكه- نحوه ارتباط‌دهی منابع فیزیكی (توپولوژی فیزیكی شبكه)- لینك‌های موجود بین منابع فیزیكی (كابل‌كشی)

 محیط شبكه (مرز شبكه با بیرون نظیر ارتباطات اینترنت، شبكه محلی، شبكه مجازی خصوصی ، برنامه‌های كاربردی و ...- دستگاه‌های ایمنی شبكه (مسیریاب، دیوار آتش)

برخی از خطراتی كه از جانب مهاجمین، سازمان را تهدید می‌كنند عبارتند از:

 ورود و خروج غیر‌مجاز - نظارت و كنترل از راه دور دسترسی غیر‌مجاز به كامپیوترها و سرورها و منابع اطلاعاتی حساس- سرقت داده‌ها، اطلاعات و تجهیزات- نصب سخت‌افزارها و یا نرم‌افزارهای استراق سمع- تخریب و یا دستكاری ساختارها و كابل‌های ارتباطی- سرقت كامپیوترها، سرورها و سایر عناصر شبكه- نصب برنامه‌های مخرب، ویروس‌ها و كرم‌ها

کنترل دسترسی:کنترل دسترسی یک تعامل اولیه و خاص ، بین یک فاعل و یک شئ است که در نهایت منجر به برقراری جریان اطلاعاتی از یکی از آنها به دیگری خواهد شد کنترل دسترسی روشن ترین نماد امنیت است در واقع آنرا قلب امنیت هم میدانند همچنین برای به اجرا در آمدن اهداف این دامنه یک مبنا و پیش نیاز به حساب می آید. این سامانه در اماکنی به کار می رود که نیاز به نظارت بر دسترسی افراد به بخشی های مختلف یک موسسه یا اطلاعات تحت عناوینی مانند حیطه بندی وجود داشته باشد.

اهداف عمده از به کار گرفتن کنترل دسترسی به شرح ذیل است:

جلوگیری از دسترسی کاربران غیر مجاز به امکانات تغییر اطلاعاتی- جلوگیری از دسترسی به اطلاعات بصورت غیر عمدی توسط کاربران نا آشنا و غیر مجاز- حصول اطمینان از سلامت اطلاعات و ثبات اطلاعات داخلی و خارجی

عوامل محیطی مخرب :عملكرد صحیح سامانه‌های رایانه‌ای و سخت‌افزار‌های مرتبط با آن‌ها، شرایط محیطی و فیزیكی خاصی را می‌طلبد. عواملی همچون انفجار، آتش، دود، رطوبت، ضربه، پارازیت الكتریكی، سیل و زلزله می‌تواند تأثیرات مخرب فراوانی در عملكرد و صحت تجهیزات، سامانه‌ها و اطلاعات داشته باشد.

برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:

می‌بایست پوشش‌های مستحكمی جهت استفاده از تجهیزات و سامانه‌های مهم در نواحی پر‌خطر پیش‌بینی و تهیه گردد.- لازم است در نزدیكی سامانه‌های مهم، تجهیزات اطفاء حریق نصب و به پرسنل آموزش‌های كاربری لازم ارائه شود.- علاوه بر رایانه‌ها، كابل‌كشی ساختمان نیز می‌بایست در برابر آتش‌سوزی ایمن باشد.- با توجه به مضرات دود برای سامانه‌های رایانه‌ای و این موضوع كه در برخی مواقع دود علامت خطر آتش‌سوزی می‌باشد، می‌بایست سامانه‌‌های تشخیص دود در اتاق‌های حاوی تجهیزات مهم، نصب و راه‌اندازی گردد.- هرگز نباید در اطراف مكان‌هایی كه حاوی اطلاعات وسخت‌افزار‌های حساس هستند،ازدرب‌ها و دیوار‌های شیشه‌ای استفاده شود.- رایانه‌ها نباید در مجاورت پنجره‌ها و یا در سطوح فوقانی اتاق‌ها قرارداده شوند.- لازم است از جاسازی تجهیزات سنگین در مجاورت سامانه‌های رایانه‌ای جلوگیری شود.- لازم است حسگرهای تشخیص رطوبت در كف اتاق كارگزار و سایت‌های رایانه استفاده شود.- این سنسور‌ها می‌بایست طوری تنظیم شوند كه هنگام وجود رطوبت آسیب‌زننده به صورت خودكار جریان برق را قطع نمایند

ویژگیهای مطلوب سامانه پدافند غیر عامل سایبری :

سیستم باید هر فعالیت مشکوک یا هر رویدادی که بالقوه ممکن است شروع کننده یک حمله باشد ، را شناسایی کند.- حملات قبل از آن که گسترش یابند باید در پایین ترین سطح ممکن تشخیص داده شوند.- میزبان های مختلف باید با هم ارتباط داشته و تبادل اطلاعات نمایند.- باید مکانیسم هایی برای مدیران شبکه وجود داشته باشد. - سیستم باید با تغییر روشهای حمله،قادر به وفق دادن خود با آن حملات باشدوهمچنین بتواند چندین حمله همرونده را نیز شناسایی نمایند.- سیستم باید مقیاس پذیر بوده و به سادگی قابل توسعه باشد.- باید غیر قابل انهدام باشد یعنی بتواند ازخود محافظت کرده وحملات به خودرا شناسایی نماید وهمچنین خطای سیستم کم باشد.- باید کمترین بار اضافی را بر روی سیستمی که در آن در حال اجرا می باشد تحمیل نماید. - باید پاسخی مناسبی در برا بر تغییر سطوح هشدار تولید نماید.

ملاحظات پدافند غیرعامل سایبری به شرح ذیل است: مهمترین ابزار در پدافند غیر عامل سایبری UTM (سامانه مدیریت تهدید یکپارچه و مدیریت ابزارهای امنیتی در یک بسته کامل) است . مهمترین بخش یک UTM سیستم مدیریتی آن می باشد که استفاده از همه ابزارهای امنیتی را ساده تر می کند و همچنین بازدهی را افزایش می دهد. و بهتر است قبل از خرید سامانه نسبت به نصب آزمایشی و بررسی امکانات آن اقدام گردد.

دسترسی به شبكه داخلی از نواحی پذیرش عمومی و سایر نواحی بایستی محدود شود.- جهت ورود به اتاق كارگزار و به طور كلی مكان‌های امن می‌بایست از کارت‌ شناسایی استفاده گردد.- اتاق كارگزار می‌بایست به تجهیزات نظارت ویدئویی و همچنین UPS مجهز گردد.- حدالمقدور از پنجره‌ها در مراكز داده استفاده نشود.- لازم است در اطراف سامانه‌های مهم نظیر كارگزارها، حفاظ‌های مناسب تعبیه گردد.- كابل‌ها در زیر‌زمین جاسازی شده و با پوشش‌های حفاظتی مقاوم شوند.- مانیتور‌ها و صفحه كلید‌ها در فواصل دوری از پنجره‌‌ها و درب‌ها و دریچه‌‌ها قرار داده شوند.- مدیریت پهنای باند

كابل‌‌های شبكه از سامانه‌های استراق سمع حفاظت شوند.- صفحه نمایش، میزكار و حتی تابلو‌های اتاق كنفرانس پس از اتمام كار پاك گردند.

درایو‌های فلاپی دیسك وCD-ROM از روی سامانه‌های مهم حذف گردند.- سطح امنیتی مطلوب برای Rack انتخاب گردد.- تهیه نسخه پشتیبان در اولین فرصت و به صورت مرتب- استفاده از مجوزهای امنیتیfile-level و share-level- حفاظت از فایلها و سایر مستندات با رمز عبور

تامین و تولید خدمات و محصولات امنیتی مورد نیاز بصورت بومی و قطع وابستگی از دیگر کشورها- فیلترینگ به منظور اتصالات وب

میرزایی:1-نکاتی که در پدافند سایبری باید لحاظ شود ؟کاربران و نیروی انسانی – داده ها و اطلاعات –روشها و رویه های اجرایی – نرم افزارهای رایانه ای –سخت افزار و شبکه ها
2-ویژگی های جنگهای سایبری ؟ملموس و عینی نیست – در جنگ سایبری دودی حاصل از انفجار مشاهده نمی شود – جنگی غیرکشنده است و تلفات انسانی ندارد – هزینه جنگ سایبری بسیار کمتر از نبرد فیزیکی . کلاسیک است – از راه دور صورت می گیرد – دانش بنیان و جنگ اندیشه ها –مرز مشخص جغرافیایی ندارد .

حمیدی :1- اقدامات مدیریت امنیت ؟1-تدوین سیاست های لازم 2- برآورد مخاطرات احتمالی 3- آموزش کاربران 4- تهیه نسخه پشتیبان از مستندات حیاتی 5- تعیین مشاغل کلیدی سازمانی 6- استفاده از سیاست میز پاک 7- مشارکت همه کارکنان در حفظ اطلاعات 8- اتخاذ سیاستهای حفاظتی 9- کنترل ورود و خروج به محل تجهیزات رایانه ای 10- طبقه بندی مستندات براساس اطلاعات موجود در آنها
2- تعریف کنش و واکنش و موارد هرکدام از انها : کنش :عبارتست از انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی
موارد کنش :1- رمزنگاری 2- امضا های رقومی 3- گواهی های رقومی 4- شبکه های مجازی خصوصی 5- نرم افزارهای آسیب نما 6- پویشگرهای ضد ویروس 7- پروتکل های امنیتی 8- سخت افزارهای امنیتی 9- جعبه های توسعه نرم افزار امنیتی
واکنش : عبارتست از انجام عکس العمل لازم پس از وقوع یک مشکل خاص امنیتی
موارد واکنش : 1- دیواره آتش 2- کنترل دسترسی 3- کلمات عبور 4- زیست سنج 5- نظام آشکار ساز نفوذی 6- واقعه نگاری 7- دسترسی از راه دور

فرحمند :انواع حملات سایبری : 1- حملات خاموش : بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییر نفوذ شده و منجر به سوء استفاده از منابع سیستم می گردد. 2- حملات فعال : حمله به سیستم های کامپیوتری و زیر ساختهای حیاتی ودستکاری اطلاعات حساس و بروز حوادث و مخارج ملی و جبران ناپذیر میشود .