دانشگاه پیام نور واحد شوشتر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

محافظت از شبکه های کامپیوتری

پروژه کارشناسی مهندسی فناوری اطلاعات

نجمه حسن جولایی

استاد راهنما

مهندس محمد قنبری عدیوی

تابستان ۹۵


بسم الله الرحمن الرحيم

دانشگاه پیام نورواحد شوشتر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

محافظت از شبکه های کامپیوتری

پروژه کارشناسی مهندسی فناوری اطلاعات

سپاس و ستایش مر خدای را جل و جلاله که آثار قدرت او بر چهره روز روشن، تابان است و انوار حکمت او در دل شب تار، درفشان. آفریدگاری که خویشتن را به ما شناساند و درهای علم را بر ما گشود و عمری و فرصتی عطا فرمود تا بدان، بنده ضعیف خویش را در طریق علم و معرفت بیازماید.

تقدیم به همسرم

به پاس قدر دانی از قلبی آکنده از عشق و معرفت که محیطی سرشار از سلامت و امنیت و آرامش و آسایش برای من فراهم آورده است.

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

پیشگفتار

دوران ما را بدرستی عصر اطلاعات نامیده اند. در اندیشه ما، «فناوری اطلاعات» به مفهوم گردآوری، سازماندهی و پردازش داده های خام است بگونه ای که از آن «معرفت» جدید تولید شود. ظهور شبکه های کامپیوتری در دهه هفتاد میلادی تمام اسباب و لوازم تولید معرفت و دانش را فراهم کرد و به آن شتابی انفجار گونه داد شاید به کار بردن واژه «انقلاب اطلاعاتی» برای این روند تولید دانش مناسبتر باشد.

شبکه کامپیوتری چیزی بیش از یک ابزار در خدمت تولید دانش نیست ولی همین ابزار کارهایی را که ذهن بشر به جمع آوری داده آزمایش و نتیجه گیری نیاز دارد در کوتاهترین زمان ممکن محقق می شود.دسترسی سریع و آسان به اطلاعات استفاده از قدرت پردازشی کامپیوترهای قوی و کارآمد ایجاد و بکارگیری تکنولوژی نوین ارتباطی برای تبادل اطلاعات و ایجاد نرم افزارهای هوشمند، به شکوفایی تمام شاخه های علوم مختلف انجامیده است.

در این پروژه به چگونگی محافظت از شبکه های کامپیوتری پرداخته شده است.

محافظت از شبکه‌های کامپیـــــوتری

مقدمه :

برقراری امنیت در شبکه از وظایف همه مدیران شبکه می باشد منظور از امنیت می تواند حفظ داده های محرمانه ای که روی کامپیوترهای یک شبکه ذخیره شده اند و یا محافظت از فایل ها سیستم عامل و برنامه‌های کاربردی در برابر دستکاری کاربران شبکه باشد. چون در شبکه ها شرایط مختلف نیاز به انواع روش های محافظتی وجود دارد. مکانیزم های امنیتی مختلفی وجود دارد.

حفاظت از شبکه

حفاظت از شبکه بیش از ملاحظات امنیتی را در بر می‌گیرد، اگرچه آنها نیز مهم می‌باشند.

تضمین سلامت داده ها

نادیده گرفتن مسائل مربوط به سلامت داده ها خصوصاً در این دوره مدرن از سخت افزارهای با قابلیت اطمینان بالا و سیستم های عامل شبکه پیشرفته آسان می باشد. با این حال. هنوز تعدادی از حقایق زشت ،اما مهم در مورد سرویس دهنده شبکه صادق می باشند و در صورتی که مراقب آنها نباشید در نهایت مشکلاتی را برایتان فراهم خواهند نمود.

- امکان از کار افتادن برای هر دیسک گردان وجود دارد.

دیسک گردان ها وسایل مکانیکی بسیار پیچیده می باشند که با ضرایب تحمل دقیقی ساخته شده اند. قابلیت اطمینان و طول عمر دیسک گردان ها در دهه گذشته به طور قابل ملاحظه ای افزایش یافته اند اما دیسک گردانها هنوز دچار خرابی می شوند فقط نیاز به زمان دارند. به علاوه. دیسک گردان‌ها در رابطه با عوامل محیطی بسیار حساس می باشند بسیاری از دیسک گردان های بزرگ و با سرعت بالا می توانند در مقابل کوچکترین تغییرات درجه هوا دچار خرابی شوند. اعتماد به قابلیت اطمینان دیسک مغناطیسی در مورد داده ها یک عمل جسورانه و بی احتیاطی می باشد.

- وسایل مکانیکی طول عمر محدودی دارند.

این دید توسعه ای از حقیقت اول می باشد. هر وسیله مکانیکی یا الکتریکی در هر صورت زمانی از کار خواهد افتاد که می تواند خنک کننده ها، منابع تغذیه الکتریسیته یا بوردهای اصلی باشند.

- ناپایداری الکتریسیته
- قانون

حفاظت از سیستم‌عامل

ویندوز NTمانند اکثر سیستم‌های عامل شبکه مدرن یک سیستم‌عامل با قابلیت اطمینان چشمگیر می‌باشد. عوامل بد می‌توانند و اتفاق می‌افتند و در نهایت سرویس‌دهنده شما می‌تواند از کار بیفتد و در حین این فرایند فایل‌های مهم شما را صدمه بزند و بدین ترتیب راه‌اندازی مجدد سستم غیرممکن شود. هر شخصی که چنین وضعیتی را

تجربه کرده باشد می‌تواند ترمیم یک سرویس‌دهنده ویندوز NT سِرور(یا هر سرویس‌دهنده دیگری) را به عنوان یک تجربه ناخوشایند برایتان بازگو کند، خصوصاً بسیاری از این تکنیک‌ها می‌توانند برای بسیاری غیر عاقلانه به نظر برسند.

می‌توانید آسیب پذیری را با برنامه ریزی از قبل و به کارگیری چندین مرحله ساده مشکلات مربوط به از کارافتادگی، سیستم را کاهش داده و بدین ترتیب شانس از دست دادن داده‌ها را نیز تا حد زیادی از بین ببرید.

رویه های نصب

می توانید از چندین راهبرد متفاوت در خلال عملیات نصب استفاده کنید تا به طور قابل توجهی کاهش شانس اینکه با مشکلات فراوان بخواهید سرویس دهنده را به حالت اول بازگردانید و همچنین کاهش ضریب از دست دادن داده ها پس از خرابی سیستم برایتان فراهم شود.

سیستم های فایل

سرور می توانند تعداد متفاوتی از سیستم های فایل را استفده کند اکثر کاربران برای سرویس دهنده خود فقط از NTFSاستفاده می کنند که در دید اول به نظر بهترین انتخاب به نظر می رسد. NTFS خصوصاً برای محیط سیستم عامل شبکه با عملکرد بالا که ویندوز NT در آن وجود دارد طراحی شده است در طول انجام این فرایند طراحان ویندوز NT سیستم فایل FAT را توسعه دادند و بسیاری از مشکلات آن را حذف نمودند.

NTFS از روش هوشمندتری برای انجام عملیات کلاستر استفاده می کند و بدین ترتیب به طور قابل ملاحظه ای اتلاف فضای دیسک را کاهش می‌دهد. NTFS ویژگیهایی را پشتیبانی می کند که FAT توان انجام آن را ندارد، مانند امنیت در سطح فایل و فهرست، وضعیتهای سفارشی سازی شده برای سرویس دهی به انواع سیستم فایل مختلف برای سایر سیستم را برای ویندوز فراهم می سازد. تمام این ویژگیهای عالی NTFS را یک سیستم فایل خوب برای اکثر سرویس دهنده های NT معرفی کرده است برای داده های مستقر بر روی سرویس دهنده،NTFS معمولاً بهترین و در واقع تنها انتخاب می باشد. با این حال بهتر است که نگهداری از یک بخش FAT کوچک بر روی دیسک راه انداز سرویس دهنده را در نظر گیرید.

نسخه‌های پشتیبان از فهرست داس را داشته باشید

تکنیک دیگر و مفید برای نصب سرویس دهنده ایجاد یک کپی از فهرست نصب پیش فرض سیستم‌عامل می‌باشد. انجام این کار ساده است: پس از تکمیل نصب سیستم‌عامل و عملیاتی بودن کامل سیستم فهرست را به فهرست دیگری کپی کنید(برای مثال، WINNTBKP \ ). سپس با تغییر فایل BOOT.INI/ انتخاب راه‌اندازی از فهرست دوم را برای خود فراهم سازید.

در صورت عدم راه‌اندازی سیستم،می توانید از طریق کپی پشتیبان سیستم را با تنظیم‌های سخت‌افزاری و برنامه‌های راه انداز و بانک اطلاعاتی(SAM) مشابه راه‌اندازی نمایید. امکان بازگشت به مراحل را در اختیارتان می گذارد ـ می توانید به جای ترمیم صدمه سریعاً به یک سیستم عامل عملیاتی بازگردید.

استفاده از ویژگیهای تکرارسازی قلمرو

آیا قصد استفاده از یک قلمرو ویندوز NT دارید؟ اگر چنین است، در صورت امکان، همیشه یک (BDC) را در محیط کاری داشته باشید. اگر منابع کافی ندارید، از کامپیوتر در سطح پایین تری برای BDC استفاده کنید. تنها توانایی مورد نیاز برای این کامپیوتر دریافت نسخه های به روز از بانک اطلاعاتی Domain SAM می باشد. اگر به هر دلیلی، (PDC) از کار افتاد، داشتن سرویس های ورود به سیستم و خروج از سیستم تا فعال شدن PDC عالی خواهد بود. اگر فاجعه ای رخ داد و کامپیوتر شخصی تان باید مجدداً نصب شود، هنوز یک کپی از Domain SAM خود را خواهید داشت.

اینکه به خود اطمینان دهید هرگز Domain SAM را از دست نخواهید داد بدون اعتبار می باشد، خصوصاً در مخیط های کاری بزرگ و چند قسمتی با ساختارهای پیچیده مجوزهای کاربری و روابط بر اساس Trust که می تواند همه چیز را با خرابی سیستم از کار بیندازد. در صورت وقوع چنین وضعیتی عملیات بسیار زیاد در رابطه با پیکر بندی مجدد جهت ایجاد قلمرو را خواهید داشت.

تکنیک های مراقبت از سیستم

اکنون آسیب پذیری خود را در خلال فرآیند نصب به از دست دادن داده‌ها کاهش داده اید زمان آن رسیده است که اقدامات پیشگیری در مورد سرویس دهنده جهت به حداقل رسانی زمان خرابی را مورد مطالعه قرار دهیم.

سه دیسکت راه اندازی سیستم

سه دیسکت راه اندزی اولین سه دیسکت ازسری دیسکت های نصب ویندوز NT می باشند. این سه دیسکت راه اندازی و آغاز فرآیند ترمیم یا نصب مجدد راحتی تحت کنترل کننده های NTFS را برایتان فراهم می‌سازند. این سه دیسکت را همیشه مهیا داشته باشید.

در صورتی که نمی توانید این سه دیسکت را پیدا کنید، می توانید آنها را از سی دی نصب ویندوز NT بسازید. سی دی را در درایو قرار دهید، برای سخت افزار به فهرست مناسب سؤییچ نمایید و فرمان زیر را در خط فرمان داس اجرا نمایید.به سه دیسکت فلاپی خالی نیاز خواهید داشت.

- دیسکت فلاپی راه انداز NT
- دیسکهای ترمیم اورژانس
- دیسکت Disk Administrator Configuration

حفاظت از سخت افزار

بهترین وضعیت موجود برای مراقبت از سیستم‌عامل فقط زمانی خوب خواهد بود که سخت‌افزار مربوطه نیز خوب باشد. اگر سخت‌افزار شما دائماً دارای مشکل می‌باشد ـ از طریق مسائل مربوط به قابلیت اطمینان یا مسائل خارجی ـ حتماً خرابی سیستم را تجربه خواهید کرد. خوشبختانه، چنین خرابیهای مرتبط با سخت‌افزار را می‌توان به چندین طریق کاهش داد یا جلوگیری نمود.

منابع تغذیه وقفه‌ناپذیر(UPS)

سیستم‌های کامپیوتری از الکتریسیته استفاده می‌کنند. پیچیدگی عظیم و اندازه کوچک قطعات الکترونیکی در سیستم آنها را در رابطه با مشکلات الکتریسیته بسیار حساس می‌کنند. در یک محیط ایده آل، الکتریسیته استفاده شده در سیستم همیشه با فرکانس مشابه و بدن هیچ‌گونه نوسان یا خاموشی در سرویس عمل خواهد کرد. متأسفانه، در یک محیط واقعی الکتریسیته از طریق یک شبکه بسیار بزرگ از هادی‌ها تحویل داده می‌شود که هزاران وسیله دیگر نیز آن استفاده می‌کنند. شبکه‌های الکتریسیته‌ای به کار گرفته شده امروزی هرگز برای برابری با قدرت تحمل وسایل کامپیوتری طراحی نشده بودند؛ بنابراین مشکلات مربوط به نوسانات دائم در الکتریسیته تا خرابی کامل همه از موارد ممکن می‌باشند.

همه ما در مرحله‌ای بر اثر قطعی الکتریسیته کار انجام شده بر روی کامپیوتر را از دست داده‌ایم این یک دلیل تمام عیار در رابطه با اهمیت ذخیره‌سازی کارتان می‌باشد. خوشبختانه، چنین رویدادهایی بر روی یک کامپیوتر شخصی فقط کار یک کاربر را در خطر می‌اندازد. لحظه‌ای فکر کنید، تأثیر قطع الکتریسیته بر روی یک سرویس‌دهنده شبکه که تعداد زیادی کاربر بر روی آن مشغول کار می‌باشند را در نظر گیرید. به علاوه، مشکلات مربوط به الکتریسیته می‌توانند باعث از دست دادن داده‌ها شوند؛ اگر یک سیستم در حین انجام عملیات حساس از کار بیفتد یا قطعی الکتریسیته داشته باشد، داده‌های بیهوده خواهند شد، سیستم‌عامل راه‌اندازی نخواهد شد یا سخت‌افزار حتی می‌تواند صدمه ببیند.

چهار مشکل مرتبط با الکتریسیته را باید مورد مطالعه قرار دهیم:

- قطع الکتریسیته : اولین مشکل واضع ترین می باشد. در صورت قطع الکتریسیته کامپیوترتان افلب در حین انجام عملیات حساس خاموش می شود و صدمه غیر منتظره ای را باعث می شود.

- پارازیت الکتریسیته ای : پرتوهای الکترومغناطیسی که از طریق وسایل الکترونیکی بدون حفاظ ایجاد می شوند یا پدیده های زیست محیطی. می توانند عرضه الکتریسیته را با پارازیت های الکتریسیته ای آلوده کنند و مشکلات بدی را برای وسایل الکترونیکی به وجود آورند.
- نوسانات الکتریسیته : آیا هرگز نابودی یک تلویزیون یا تلفن به وسیله رعد و برق را تجربه کرده اید؟ این مثالی کمیاب از نوسانات الکتریسیته می باشد که در آن الکتریسیته به درجه ای از قدرت می‌رسد که بسیار بیشتر از حد نیاز می باشد ، تا اندازه ای زیاد است که می تواند وسیله را نابود کند. اکثر نوسانات ناگهانی الکتریسیته بدین شدت نمی باشند اما نوسانات کوچک بسیار رایجتر بوده و حتی یک نوسان بسیار کوچک نیز می توانند بعضی از وسایل را صدمه زند.
- نیمه خاموشی ها : نیمه خاموشی ها نوسانات الکتریسیته ای منفی می باشند آنها زمانی رخ می دهند که عرضه الکتریسیته فراتر از ظرفیت موجود انجام می گیرد و بدین ترتیب الکتریسیته کمتری عرضه می شود. چراغها ناگهان کم نور می شوند و وسایل الکترونیکی به دلیل کمبود الکتریسیته خاموش و روشن یا حتی صدمه می بینند.

رایجترین وسیله از الکتریسیته استفاده شده به وسیله کاربران موج گیر می‌باشد این وسیله جهت فراهم نمودن حفاظت در مقابل نوسانات شدید در الکتریسیته طراحی شده است که جریان الکتریسیته را کاهش می دهد و بدین ترتیب جلوی الکتریسیته بیش از حد را می گیرد. بسیاری از این وسایل فیلترهایی را نیز برای مقابله با پارازیت های اضافی ارائه می دهند.

متأسفانه، تعداد زیادی از این وسایل در بازار وجود دارند که توانایی مقابله واقعی با نوسانات عظیم و حفاظت را ندارند و حفاظت آنها نیز می تواند به وسیله یک نوسان ضعیف یا حذف شود. به علاوه، آنها حفاظتی را برای مقابله با افت ولتاژ یا خاموشی کامل الکتریسیته فراهم نمی سازند.

راه حل بهتری وجود دارد، منبع تغذیه وقفه ناپذیر UPS ها فقط برای یک منظور به طوری که نامشان می رساند طراحی شده بودند. تأمین عرضه الکتریسیته مطمئن برای کامپیوترها UPS از یک باتری که هنگام موجود بودن الکتریسیته خود را شارژ می کند استفاده می نماید. در صورت قطعی الکتریسیته وسیله به باتری سوییچ می کند، زمان کافی را جهت ذخیره سازی و خاموش نمودن صحیح سیستم برای کاربران فراهم می سازد یا در UPS های بزرگتر کاربران به کار خود ادامه می دهند. تکامل UPS ها،سرویس های بیشتری به تعدادی از مدل ها اضافه شده اند. این سرویس ها شامل موج گیر، فیلترسازی الکتریسیته و توانایی های خاموش کردن از راه دور می باشند.

عوامل زیست محیطی

وسایل کامپیوتری در رابطه با محیط اطراف خود حساس می باشند حرارت و رطوبت بسیار زیاد می توانند عملیاتی بودن آنها به مقدار زیادی کاهش دهند و می توانند باعث از کار افتادن و خرابی وسیله شوند. سخت

افزارهای جدید، خوشبختانه مقاومتر و حساسیت کمتری نسبت به عوامل زیست محیطی در مقایسه با انواع قدیمی تر دارند زمانی که ساختمانها به وسیله حرارت قطعات کامپیوتر شرکتها گرمای زیادی را متحمل می شدند گذشته استو هنوز متعادل نگهداشتن حرارت و رطوبت در محدودهای قابل قبول مهم می باشد.

استفاده از یک اتاق کامپیوتر کنترل خوبی را در رابطه با چندین عامل برایتان فراهم می سازد. نخست می توانید حرارت و رطوبت اتاق را در سطح مطلوبی کنترل کنید. دوم، می توانید سخت افزارها و داده های حساس خود را در یک اتاق با محدودیتهای دسترسی لازم نگه دارید. سوم، می توانید سرویس های الکتریسیته ای مطمئن را با استفاده از فیلترسازی و باتری پشتیبان برای کل اتاق به جای وابسته بودن به UPS های مجزا فراهم سازید. چهارم،می توانید تعدادی از وظایف سازماندهی را از این مکان برای کل شرکت فراهم سازید.اتاق های کامپیوتری نیاز به سرمایه اولیه زیادی دارند برای بسیاری از شرکتها، حفاظت فراهم شده با ارزش تر از هزینه می باشد.

تکرارسازی سخت افزار

با تکامل کامپیوترها، آنها با گذشت زمان از قابلیت اطمینان بیشتری برخوردار شده اند. از کارافتادن سخت افزار دیگر مانند سابق رایج نمی باشد. هنوز می تواند رخ دهد دیسک های سخت خراب می شوند، CPU ها به دلیل حرارت زیاد خراب می شوند، خنک کننده ها عمل نمی کنند و کابل های شبکه صدمه می بینند. برای اکثر وظایف، این ریسک قابل قبول می‌باشد اگر بدترین وضعیت پیش آید و قطعه ای از سخت افزار خراب شود، این قطعه و داده های آن تعویض شده و کامپیوتر مجدداً شروع به کار می کند. تعدادی ازشرکتها دارای سیستم هایی می باشند که نمی توانند زمان مدت خرابی را تحمل کنند بدین دلیل، بسیاری از تولیدکنندگان سرویس دهنده سخت افزارهایی را توسعه داده اند که ویژگی های تکرارسازی توکار دارند.
تعدادی سیستم توانایی نصب چندین قطعه تکرارساز سخت افزار با امکانات سوییچ نمودن خودکارسازی شده را هنگام مشکل به وسیله فعال در صورت خرابی یک وسیله فراهم می سازند. چنین موارد تکرارسازی می توانند در مورد خنک کننده ها، منابع تغذیه، کارت های شبکه ها و حتی CPU ها به کار گرفته شوند. اگر چه این سیستم ها غالباً گران می باشند، بسیاری از شرکتها جهت تضمین اینکه خرابی سخت افزار که باعث زمان مدت خراب می شود را دارا نباشند حاضرند این مبلغ را پرداخت کنند.

حفاظت از داده های کاربری

نوعی خرابی حتماً اتفاق خواهد افتاد این خرابی می تواند مشکل سخت افزاری، حمل عوامل بد یا اشکالات سیستم عامل را در برداشته باشد نه تنها ممکن است بکله سیستم شما در مقطعی از زمان از کار خواهد افتاد. در این

فرایند احتمال از دست دادن داده هایی که کاربر بر روی سیستم های شما ذخیره یا با آنها کار کـرده اسـت وجـود دارد. می توانید سیستم خود راحتی در مقابل چنـین وضـعیتی بـا اسـتفاده از دو روش حفاظـت نماییـد: راهبردهـای صحیح تهیه نسخه پشتیبان و مخازن ذخیره سازی تکرارساز.

تهیه نسخه پشتیبان

ایده مرتبط به تهیه نسخه پشتیبان ساده می باشد: یک کپی پشتیبان را در صورت از کار افتادن دیسک سخت داشته باشید.
می توانید از داده های خود در انواع مختلف وسایل پشتیبان تهیه کنید:

- پشتیبان درون خطی : عبارت درون خطی در رابطه با مخازن داده ای به رسانه ذخیره سـازی ارجـاع داده می شود که دائماً و سریعاً برای سیستم موجود باشد. این مخزن استفاده شده وسـیله سیسـتم مخـزن درون خطی می باشد. تهیه پشتیبان درون خطی به اقدامات پیاده سازی آسان و ساده تهیه نسـخه پشـتیبان مـرتبط می باشد مانند تهیه یک کپی عیناً متشابه از دیسک هـای سـخت . سیسـتم پشـتیبان درون خطـی، اگرچـه سریع و ساده می باشد گران نیز است فقط در واقع نیمی از رسانه ذخیـره سـازی درون خطـی را اسـتفاده می کنید، زیرا نیمه دیگر فضای دیسک جهت نگهداری یک کپی از داده های عملیـاتی بـه کـار گرفتـه می شود.
- پشتیبان نیمه درون خطی : عبارت نیمه درون خطی یعنی رسانه ذخیره سازی که همیشه درون خطی نمـی باشد اما می توان آن را با سرعت و سادگی در دسترس قرار داد. پشتیبان نیمه درون خطی بـه طـور سـنتی بر روی رسانه قابل انتقال از دیسکت فلاپی برای فایل های کوچک تا دیسک هـای نـوری بـزرگ قابـل انتقال یا وسایل برجی بزرگ که از آرایه های دیسک های نوری یا نوارهای مغناطیسی استفاده می کننـد پیاده سازی می شود. پشتیبان نیمـه درون خطـی یـک مکـانیزم پشـتیبان قدرتمنـد مـی باشـد کـه نـه تنهـا دسترسی به پشتیبان سریع، مطمئن و آسان فراهم می کند بلکه توانایی ذخیره سازی مقدار زیـادی از داده ها که به صورت عمومی استفاده نمی شوند را در صورت نیـاز در دسـترس قـرار مـی دهـد مخـازن نیمـه درون خطی گرانقیمت بوده و معمولاً با رسانه ذخیره سازی یا با وسایل بزرگ فضای فیزیکـی زیـادی را اشغال می کنند.
- پشتیبان برون خطی : پشتیبان برون خطی نوعی می باشد که غالباً استفاده می شـود. پشـتیبان بـرون خطـی کپی نمودن داده ها بر روی رسانه های کوچک مطمئن و قابل انتقال را در بـر دارد کـه غالبـاً از تکنیـک های فشرده سازی نیز استفاده می کنند. رایجترین رسانه بـرون خطـی اسـتفاده شـده نـوار مغناطیسـی مـی باشد. ذخیره سازی برون خطی نسبتاً هزینه مناسب در بر دارد و پیاده سـازی آن آسـان مـی باشـد بـا ایـن

وجود این وسیله آهسته عمل می کند و بسیار نامطمئن می‌باشد و نیاز به اداره و استفاده با دقت زیاد دارد. اندازه کوچک و هزینه مناسب رسانه پشتیبان برون خطی این رسانه را رایجترین رسانه ها نموده است.

ذخیره سازی دیسک تکرارساز

پشتیبان داده ها چندین مشکل مربوط به سلامت داده ها را نمی تواند جواب دهد. نخست، زمان بندی تهیه پشتیبان می باشد:
هر گونه داده تغییر یافته از زمان آخرین تهیه پشتیبان در یک خرابی فاجعه‌آمیز از دست می رود. دوم، مشکل بازبودن فایل ها را داریم تهیه پشتیبان از فایل های باز غیر ممکن می باشد و بسیاری از سیستم ها تعدادی از فایل ها را به طور همیشگی برای انجام عملیات باز نگه می دارند. سوم، زمان بازیافت یک مشکل داریم: جهت بازیافت از یک نوار به چندین ساعت نیاز داریم که می تواند مشکلات زیادی را برای محیط های کاری بلادرنگ ایجاد کند.

می توان این مشکلات را با استفاده از (RAID) رفع نمود. ایده RAID ساده می باشد: از چندین دیسک جهت فراهم نمودن تکرارسازی سخت افزاری استفاده کنید و بدین ترتیب ریسک از دست دادن داده ها هنگام خرابی دیسک را کاهش دهید . ایده RAID توسعه داده شده است تا بازدهی از طریق چندین درایو برای زیر سیستم دیسک بهبود داده شود.سطوح مختلف RAID وجود دارند هر یک ویژگیهای متفاوتی را فراهم می‌سازند و دارای مزیت ها و کاستی های خاص خود می باشند.

RAID : اجرای بهتری را فراهم می سازد و داده ها را بر روی چندین دیسک درایو توزیع می کند. این سیستم بازدهی احتمالی اینکه زیر سیستم دیسک بتواند چندین بخش مختلف از یک فایل مشابه از چندین چرخش درایو در یک زمان به دست آورد را افزایش می دهد. RAID ۰ فواید بیشتر دیگری را در رابطه با تحمل خرابی فراهم نمی‌سازد در واقع، یک سیستم RAID ۰ در مقابل خرابی آسیب پذیر می باشد زیرا بیش از یک دیسک دارد که هر یک از آنها با خرابی می توانند کل حجم آن را از کار بیندازند. RAID از نظارت و یا استفاده دو طرفه از دیسک تشکیل می شود.

۱ RAID تحمل خرابی خطا و در سیستم های پیشرفته با عملکرد بالاتر را فراهم می سازد، زیرا داده های مشابه را می توان از چندین دیسک و / یا کنترل کننده ها خواند.
۲ RAID که اصلاً رایج نمی باشد داده ها را به صورت بیت به بیت بر روی دیسک ها توزیع می کند.

RAID ۳ داده ها را در سطح بابت بر روی تمام دیسک ها توزیع می کند و از یک درایو جداگانه جهت ذخیره سازی داده های checksum/parity استفاده می کند. در صورت خرابی یک درایو، داده های توازن را می توان جهت ساخت مجدد RAID بر روی یک دیسک جدید معاوضه شده بدون هیچ گونه از دست دادن داده ها استفاده نمود.

RAID ۳ اغلب به دلیل توزیع داده ها و همچنین فراهم نمودن عامل تحمل خرابی بالا به خوبی کار می کند . تهیه پشتیبان از درایو توازن می تواند تحمل خطا را به دلیل کاهش ریسک خرابی این درایو بهتر سازد.

RAID ٤ داده ها را در سطح بلوک توزیع نموده و مانند RAID۳ از درایو توازن استفاده می کند. RAID٤ می تواند به صورت بالقوه کاراتر از RAID ۳ باشد، زیرا داده ها فرایندهی خواندن و نوشتن به صورت واحد را جهت دسترسی و ذخیره سازی به کار می گیرند.

RAID ٥ داده ها را در دو سطح بلوک مانند RAID ٤ توضیح می کند، اما بر خلاف RAID ۳ و RAID ٤ داده های توازن را بر روی تمام دیسک ها توزیع می نماید. این روش مشکلات حاصله از نگهداری داده های توازن بر روی یک دیسک را حذف می کند و بدین ترتیب عملیات نوشتنی بیشتری را برای سیستم با نرخ سریعتر فراهم می سازد این روش می تواند بازسازی RAID را آهسته تر کند.

RAID را می توان در نرم افزار یا در سخت افزار با سیستم عامل خاص ، کنترل کننده های RAID ترانسپارنت - پیاده سازی نمود روشهای سخت افزاری به طور کل بسیار بهتر عمل می کنند اما غالباً هزینه زیادی را در بر دارند. روشهای سخت افزاری امکانات بیشتری مرتبط با تعویض بدون خاموش نمودن درایوها را فراهم می سازند. اگر یم دیسک در چنین وضعیتی خراب شود می توانید به سادگی درایو از کار افتاده را با نوع جدید آن عوض کنید و بدین ترتیب زمان مدت خرابی سیستم را حذف نمایید . تعدادی از سیستم های تعویض بدون خاموش کردن سیستم نصب دیسک پشتیبان را ممکن می سازند که سریعاً در صورت خرابی یک دیسک می تواند در سیستم با مابقی دیسک ها ادغام شود. سپس می توانید دیسک خراب را با یک دیسک جدید تعویض نمایید که خود به یک دیسک پشتیبان تبدیل می شود.

پیاده‌سازی برنامه سلامت داده‌ها

عوامل زیر را هنگام ارزیابی برنامه سلامت داده‌ها در نظر داشته باشید:

- اهمیت داده‌ها ـ داده‌های شما از چه درجه‌ای از اهمیت برخوردارند؟ از دست ندادن داده‌ها بسیار حساس و مهم می‌باشند یا مراقبت از سرویس‌دهنده برایتان مهم می‌باشد؟ آیا استفاده از نسخه‌های پشتیبان کافی خواهد بود یا اینکه باید از RAID نیز استفاده کنید؟ آیا می‌توانید چند ساعت خرابی سیستم را متحمل شوید، یا اینکه در هر ثانیه‌ای که سیستم کار نمی‌کند ضرر مالی برایتان خواهد داشت؟

- عملی بودن ـ آیا مدیریت این سیستم‌ها تنها وظیفه اداری شما می‌باشد یا اینکه وظایف دیگری نیز دارید که زمان مورد نیاط جهت تضمین سلامت داده‌ها را برایتان محدود می کند؟ آیا کارکنانی دارید که بتوانند این مشکلات را رفع کنند؟ آیا شرکت شما می تواند یک اتاق کامپیوتر فراهم سازد یا اینکه فقط باید از UPSاستفاده کنید و حرارت و رطوبت را خودتان کنترل کنید؟
- ریسک ـ ضریب ریسک شما چقدر است؟ آیا در یک منطقه اصلی شهری یا اینکه در منطقه دورافتاده‌ای قرار گرفته اید؟ آیا حملات امنیتی خواهید داشت؟ در رابطه با حوادث طبیعی و خدادادی تا چه حد آسیب‌پذیر می‌باشید؟

برنامه‌ریزی برای امنیت شبکه و داده‌ها

بگذارید یکی از جدی‌ترین تهدیدهایی را هر شبکه یا کاربری می‌توانند با آن مواجه شوند را مورد مطالعه قرار دهیم. اگرچه تهدید خارجی برای بسیاری مهمترین می‌باشد، مطالعات نشان داده است که تهدیدهای عمدی معمولاً در داخل شرکت شکل می گیرند. در واقع، ۸۰درصد از تخلف‌های امنیتی که عمدی می‌باشند از داخل شرکت شکل گرفته‌اند. یک لغت که بسیاری آن را با تهدید عمدی مرتبط می‌سازند لغت hackerمی‌باشد. اشخاص بد عنوان crackers شناخته می‌شوند.

Crackers ها افرادی می‌باشند که با استفاده از توانایی‌های رمزشکنی منافع شخصی خود را رفع می کنند یا مشکلات ناخوشایندی را برای دیگران به بار می‌آورند. رمزشکن‌ها باعث بهبود امنیت کامپیوترها شده و اجرای برنامه‌ها و برنامه‌های کاربردی بهتر می‌شوند.

سطوح امنیت

درجه امنیتی که یک کاربر بر روی یک سیستم دارد به وسیله امنیت واگذار شده به آن کاربر توسط گرداننده مشخص می شود. گرداننده یک سیستم خاص برای مشخص نمودن درجه امنیت برای کاربر برای منبع خاص و کاربر خاص مهم می باشد. بدین دلیل، در نظر داشتن امنیت همیشه قبل از نصب یا تنظیم عاقلانه می باشد. به علاوه، گرداننده جهت هموار نمودن اجرایی بودن امنیت با یک روش متعادل و کامل باید از یک سیاست امنیتی استفاده کند.

اولین قدم در رابطه با به اجر درآوردن هر نوع سیستم امنیتی شناسایی و اعتبارسنجی کاربر می‌باشد. اعتبار سنجی خصوصاً یک فرآیند دو مرحله‌ای می‌باشد: تصدیق و به اثبات رساندن شناسایی فرآیندی می‌باشد که در آن کاربر خود را در سیستم شناسایی می کند که خصوصاً از طریق استفاده از اسامی وارد شدن به سیستم مدیریت انجام می گیرد. جهت اعتبار سنجی کاربر، سیستم چالش جدیدی را در شکل دیگری با درخواست قسمت دوم فرآیند اعتبارسنجی تقاضا می کند: به اثبات رسانیدن.

به اثبات رسانیدن فرآیندی می باشد که سیستم جهت تأیید اطلاعات کاربر برای وارد شدن به سیستم به کار می گیرد که معمولاً در شکل عرضه یک کلمه رمز می‌باشد. فرآیندهای تأیید زیست متریکی به طور گسترده‌ای در حال به کارگیری می‌باشند ـ دستگاههای خواندن آثار انگشت، پویشگرهای قرینه چشم و امضاء که در حال معرفی در شبکه‌ها می‌باشند.

اگر کاربر بتواند شناسایی (یک نام معتبر وارد شدن به سیستم) و به اثبات رسانیدن(کلمه رمز صحیح برای نام وارد شدن به سیستم) را فراهم کند، مجوز امنیتی جهت استفاده از اشیاء خاص بر روی سیستم به کاربر داده می‌شود.

سیاستهای امنیتی

عبارت سیاست‌های امنیتی معمولاً دارای دو معنی متفاوت می‌باشد. معنی اول به استانداردی ارجاع داده می‌شود که به وسیله مدیر یا مدیران جهت به اجرا در آوردن سطحی از امنیت در کل شرکت به توافق رسیده است. معنی دوم به ابزار مدیریتی که در ویندوز NT نگارش ٤ وجود دارد ارجاع داده می‌شود. این ابزار سازماندهی Policy Editor نامیده می‌شود و جهت تنظیم و به اجرا در آوردن یک محیط خاص برای کاربران یک سیستم استفاده می‌شود.

یک سیاست امنیتی ابزار مفیدی می باشد برای تضمین اینکه تمام کاربران شرکت راهنماهای امنیتی شرکت را رعایت می کنند. یک سیاست امنیتی مؤثر دارای چندین بخش می باشد و هر یک از این بخشها از اطلاعات جمع آوری شده در خلال مراحل اولیه برقراری سیاست امنیتی تکامل می یابند: ارزیابی ریسک. ارزیابی ریسک سنجیدن شرکت و ریسک های مرتبط می‌باشد. ارزیابی ریسک کامل قابلیت های آسیب پذیری، تهدید ها و اقدامات متقابل را می سنجد.

ارزیابی قابلیت‌های آسیب‌پذیری امنیت

یک سیاست امنیتی خوب با این سؤال گرداننده شروع می‌شود، نقطه‌های آسیب‌پذیری ما کجا قرار گرفته‌اند؟ قابلیت آسیب‌پذیری در زیر لیست شده‌اند:

- سیستم تهیه پشتیبان ـ اگر اطلاعات روی یک درایو نوار مغناطیسی یا شکل دیگری از رسانه ذخیره‌سازی کپی نشود، شرکت در کل با نقطه ضعف‌هایی رو به رو است که شامل از دست‌دادن داده‌ها در صورتی که شخص یا چیزی به داده‌ها یا رسانه‌ای که داده‌ها بر روی آن قرار گرفته‌اند صدمه زنند؛ این مطلب در هر دو مورد عوامل عمدی و غیرعمدی حقیقت دارد.
- کاربران ـ کاربران می‌توانند به دو طریق آسیب‌پذیر باشند. نخست، اگر کاربری به طور صحیح در رابطه با استفاده از سیستم یا برنامه مربوطه آموزش ندیده باشد، می‌تواند اشتباهاتی را مرتکب شود که نتیجه آن از دست دادن یا صدمه زدن به اطلاعات را در بر خواهد داشت. برای مثال، کاربری که آموزش صحیح در

رابطه با استفاده، ذخیره‌سازی و ایجاد کلمه‌های رمز ندیده است می‌تواند سیستم را به طور کامل در اختیار یک متجاوز قرار دهد. همچنین، کاربر آموزش ندیده می‌تواند سعی به ذخیره‌سازی داده‌ها با استفاده از رویه غلط و رونویسی یا حذف داده‌ها به صورت تصادفی نماید. دومین روشی که یک کاربر می‌تواند یک ریسک امنیتی باشد این است که بخواهد به صورت عمد صدمه‌ای به داده‌ها وارد کند.

ارزیابی تهدیدهای امنیتی

علاوه بر سنجش قابلیت‌های آسیب‌پذیری بالقوه که یک سازمان با آنها مواجه می‌باشد. که از یک آسیب‌پذیری خاص استفاده می‌کند. مثالهای زیر را در نظر گیرید:

- رمزشکن ـ اگر یکی از آسیب‌پذیریها نوعی مشکل در سیستم باشد، مطمئن باشید که رمزشکن آن را پیدا و از آن سوء استفاده می‌کند. یک رمزشکن جهت نفوذ به سیستم روشهای مختلفی را به کار می‌گیرد و بنابراین تهدید جدی برای سیستم می‌باشد.
- ویروس‌ها ـ پویش ویروس‌ها در هر محیط کاری ضروری می‌باشد. ویروس‌ها در فایل‌ها و برنامه‌ها، پیامهای پست الکترونیکی انتقال داده شده و حتی در نرم‌افزارهای تهیه شده ظاهر می‌شوند. اگر یکی از ارزیابی‌های ریسک آسیب‌پذیری عدم پویش ویروس در سیستم می‌باشد، یک ویروس باید به عنوان تهدید به حساب آید.
- محیط‌زیست ـ هر منطقه از جهان تهدیدهای زیست‌محیطی خاص خود را دارا می‌باشد. آتش‌فشان‌ها، طوفانها، زمین‌لرزه‌ها، گردبادها، سیل‌ها و سایر حوادث بالقوه تعدادی از مشکلترین تهدیدها جهت حفاظت در مقابل آنها می‌باشند. در واقع، در بعضی مواقع تنها اقدام متقابل برای این نوع تهدید وجود یک نسخه پشتیبان و بازیافت داده‌ها در مکانی دیگر می‌باشد.

برقراری اقدامات متقابل امنیتی

پس از اینکه اعضای یک سازمان آسیب‌پذیری‌ها و تهدیدهای بالقوه را مورد مطالعه، شناسایی و ارزیابی قرار دارند. می‌توانند به مرحله بعدی ارزیابی ریسک و فرآیند سیاست امنیتی قدم بردارند: اقدام‌های متقابل، یک اقدام متقابل عاملی می‌باشد که جهت به حداقل‌رسانی ریسک ایجاد شده به وسیله یک آسیب‌پذیری یا تهدید انجام می‌گیرد. چندین مثال در زیر لیست شده‌اند:

- نسخه‌های پشتیبان ـ نگهداری یک نسخه پشتیبان از اطلاعات سیستم‌های کامپیوتری بهترین روش تضمین بازیافت داده‌ها در صورت رخ‌دادن یک فاجعه می‌باشد. این نوع اقدام متقابل در رابطه با تهدیدهایی مانند خرابی قطعات و فاجعه‌های طبیعی بسیار مفید می‌باشد.

- امنیت فیزیکی ـ به اجرا در آوردن یک سیاست امنیتی سفت و سخت فیزیکی یکی از روشهای جلوگیری از متجاوزهای خارجی می‌باشد. درهای قفل شده، کارت‌های ورود الکترونیکی و دیسک‌های سخت قابل انتقال که هر شب در اتاق قفل شده نگهداری می‌شوند چندین روش جهت جلوگیری دسترسی بدون مجوز به اطلاعات مهم می‌باشد.

امنیت کابل ـ تعدادی از سازمانها در مورد تجاوز به سیگنالهای انتقال داده شده بر روی کابل‌های شبکه نگران می‌باشند. اگر چنین می‌باشد، شاید بهتر باشد جهت انتقال تمام داده‌ها از فیبرنوری استفاده کنید، زیرا دزدیدن سیگنال از یک کابل فیبرنوری در مقایسه با کابل هم محور یا انواع سیم‌های جفت به هم تابیده مشکلتر می‌باشد.

وسایل اشتراکی با کلمه رمز

جهت تنظیم یک منبع اشتراکی در ویندوز ۹x، نخست باید قطعات صحیح Microsoft Networkingرا نصب کرده باشید که به اشتراک‌گذاری فایل و چاپگر را نیز در بر دارد. آسانترین روش به اشتراک‌گذاری یک فهرست(پوشه در زمان تخصصس ویندوز ۹x)استفاده از ویندوز اکسپلورر یا My Computerجهت مرور فهرست می‌باشد. پس از پیدا نمودن پوشه‌ای که فایل‌ها یا پوشه‌هایی را که می‌خواهید به صورت اشتراکی استفاده نمایید در بر دارد، کلید راست ماوس را کلیک کنید و منوی متنی پوشه را فعال سازید.

با انتخاب sharingکادر مکالمه share propertiesبرای این پوشه ظاهر می‌شود و سپس منبع اشتراکی را نامگذاری کنید.

چندین نکته را هنگام نامگذاری این منبع اشتراکی رعایت کنید:

- چه فردی نیاز دسترسی به وسیله اشتراکی دارد؟ اگر انتظار دارید که کاربران کامپیوترهای داس آن را پیدا کنند، بهترین کار استفاده از ۸ کاراکتر ب رعایت قوانین نامگذاری تحت داس می‌باشد تا کاربران داس دسترسی به این منبع اشتراکی برایشان ساده‌تر باشد.
- چه نامی را باید برای منبع اشتراکی به کار گیرید؟ واضح است، یک نام مانند WORDDOCSبرای یک منبع اشتراکی فایل‌های وُرد خوب خواهد بود. اما نام DOCS برای منبع اشتراکی شاید به خوبی کار کند. می‌توانید یک توضیح مفصل‌تر در کادر زیر نام منبع اشتراکی را فراهم کنید تا بدین ترتیب نامگذاری منبع اشتراکی برایتان پیچیده نشود. این مطلب را به خاطر بسپارید که هر چه نام منبع اشتراکی منطقی‌تر باشد، پیدا نمودن آن به‌وسیله کاربران ساده‌تر خواهد بود.

چه نوع مجوزی را باید به منبع اشتراکی تخصیص دهید؟ به خاطر بسپارید که انواع مجوزها را می‌توانید تخصیص دهید. کاربران می‌توانند مجوزهای ,Read full None, را داشته باشند.

با انتخاب دکمه OK زمانی که تمام فیلدها کامل شدند منبع اشتراک و تنظیم‌های مربوطه برقرار می‌شوند.

ایستگاههای کاری بدون دیسک

یک روش جلوگیری از کپی اطلاعات از سیستم‌های شبکه و قراردادن آن بر روی دیسکت‌های فلاپی یا دیسک‌های سخت محلی نداشتن یک درایو دیسک سخت یا درایو دیسک‌گردان فلاپی محلی می‌باشد. اگر سیستم کامپیوتری دیسک سخت روشی جهت راه‌اندازی از ایستگاه‌کاری نداشته‌باشد، سیستم می‌تواند یک ایستگاه‌کاری بدون ریسک برروی شبکه داشته باشد.

ایستگاههای کاری بدون دیسک خصوصاً از یک کارت رابط شبکه خاص استفاده می‌کنند که یک تراشه راه‌انداز PROM را دارا می‌باشد. تراشه PROMجهت بارگذاری نرم‌افزار شبکه به داخل حافظه کامپیوتر استفاده می‌شود و امکان متصل شدن و راه‌اندازی از فایل‌های سیستم‌عامل ذخیره شده بر روی شبکه را فراهم می‌سازد.

رمزگذاری

آخرین خط دفاع برای گردانندگان و کاربران استفده از امکانا رمزگذاری داده می‌باشد تا در صورت دسترسی شخصی به این اطلاعات قبل از استفاده از داده‌ها باید عملیات زیادی را جهت رمزگشایی به کار گیرد.داده‌های رمزگذاری شده به شکل دیگری تبدیل یا «قفل» می‌شوند که به سادگی قابل استفاده نخواهند بود و در صورت نیاز می توان آنها را به وسیله یک کلید به حالت اولیه بازگرداند. فرایند رمزگذاری در ماهیت مانند«قفل نمودن»داده‌ها می‌باشد تا بدین ترتیب شخص بدون مجوز به آنها دسترسی پیدا نکند فرآیند برداشتن قفل را رمزگشایی می‌نامیم. در ماهیت، فقط دو روش جهت رمزگذاری داده‌ها استفاده می‌شوند: جابجاسازی و جانشین سازی.

با جابجاسازی، ترتیب بیت‌های ارسالی جابجا می‌شوند. برای مثال، تصور کنید که می‌خواهید پیام "HELLO" را به کاربر دیگری ارسال کنید. شما و کاربر دیگر موافقت می‌کنید که کلید جابجاسازی انتقال حرف اول هر لغت به انتهای لغت می‌باشد، بنابراین پیام "Elloh" را ارسال خواهیم نمود. اگر از روش جانشین سازی برای رمزگذاری استفاده می‌کنید باید الگو یا ارزش دیگری را جهت جانشین نمودن پیام خود پیدا کنید. اگر کلید جانشین سازی استفاده از روشهای رقمی برای حروف الفبا می‌باشد، پیام شما به "۸۵۱۲۱۲۱۵" تبدیل می‌شود.

اگر فقط یک نوع جابجاسازی یا جانشین‌سازی را انتخاب کنید، تشخیص پیام بدون مشکل زیاد توسط فرد بدون مجوز ممکن خواهد شد. بدین دلیل، اکثر روشهای رمزگذاری معرف به کار گرفته شده امروزی از سری‌های مختلف جابه‌جاسازی و جانشین‌سازی استفاده می‌کنند. یک فرمول ریاضی جهت به دست آوردن کلید استفاده

می‌شود که جهت رمزگذاری و رمزگشایی پیام استفاده می‌شود. زمانی که هر دو طرف کلید مشابهی را جهت رمزگذاری و رمزگشایی بدانند، فن رمزگذاری با نام رمزنگاری متقارن شناخته می‌شود.

در بعضی مواقع، رمزگذاری باید بین طرفینی استفاده شود که از یک کلید مشابه استفاده نمی کنند. برای انجام این کار باید از رمزنگاری نامتقارن استفاده شود. زمزنگاری نامتقارن به یک کلید عمومی و یک کلید خصوصی برای هر دو طرف نیاز دارد.
کلیدهای عمومی و خصوصی با استفاده از توابع ریاضی به یکدیگر می‌باشند تا بدین ترتیب یک سری‌از کلیدهای استفاده شده برای رمزگذاری باشند. کلیدعمومی جهت ارسال پیام در اختیار همگان قرار می گیرد. پیام با استفاده از کلید عمومی رمزگذاری می‌شود و سپس با به کارگیری کلید خصوصی رمزگشایی می‌شود. به دلیل اینکه کاربری که پیام را ارسال می کند همیشه کلید خصوصی را در اختیار دارد، تنها شخصی خواهد بود که می‌تواند پیام ارسال شده را بخواند.

حافظه‌های ویروسی

هیچ‌گونه بحث و گفتگو درباره امنیت شبکه بدون ذکر ویروس‌ها مانند وسایل نفوذ و بمب‌های منطقی و سایر انواع حیات وحش الکترونیکی کامل نخواهد بود. یک ویروس برنامه‌ای می‌باشد که هنگام اجرای یک برنامه آلوده فعال می‌شود.
بنابراین می‌توان گفت که فقط فایل‌های اجرایی با پسوندهایی مانند SYS,COM,BAT,EXE قابلیت آلوده شدن را دارا می‌باشند. مانند یک ویروس جانوری، ویروس‌های کامپیوتری به زندگی خود با تکثیر و کپی نمودن به سایر سیستم‌ها و فایل‌ها ادامه می دهند.

تعدادی از ویروس‌ها کاری بجز تکثیر و اشغال فضا انجام نمی‌دهند، اما سایر ویروس‌ها می‌توانند صدمات عظیمی را وارد کنند و حتی با اجرا خود را نیز نابود سازند. اگر چیزی داده‌ها را صدمه زند یا دسترسی به آن راجلوگیری کند، یک تخلف امنیتی رخ داده است. ویروس‌ها حتماً نگرانی بزرگی برای تمام سیستم‌ها می‌باشند. ویروس‌ها را می‌توان از شبکه، از فایل‌های انتقال داده شده از برنامه‌های نرم‌افزاری و نرم‌افزاری رایگان و حتی از نرم افزارهای تهیه شده به سیستم وارد نمود.
جهت جلوگیری از این هیولاها برای آلوده‌سازی سیستم‌ها، باید نوعی اقدام متقابل را داشته باشید و به کار گیرید.

ویروس‌یاب‌ها و حافظ‌های ویروسی دو نوع وسیله می‌باشند که می‌توانید جهت حفاظت سیستم‌ها از آنها استفاده نمایید. هر یک نوع متفاوتی از حفاظت را فراهم می‌سازد. ویروس‌یاب‌ها در صورت تردید در مورد وجود یک ویروس می‌توانند اجرا شوند یا بر اساس یک برنامه زمان بندی به‌کار گرفته شوند. آنها کار کاملی را در مورد

بررسی هر یک از فایل‌ها انجام می‌دهند و هرگونه ویروس شناسایی شده را حذف می‌کنند. برنامه‌های ویروس‌یاب خصوصاً از یک بانک اطلاعاتی با رشته‌های کد ویروس نمونه برای هریک از فایل‌ها استفاده می‌کنند.

این فایل‌های بانک اطلاعاتی معمولاً به عنوان فایل‌های تعریف ویروس شناخته می‌شوند. اگر یک ویروس‌یاب یک رشته کد خاص را شناسایی کند، این برنامه یک ویروس پیدا کرده است. اکثر ویروس‌یاب‌ها امکانات حذف ویروس‌های امکانات حذف ویروس‌های پیدا شده را نیز دارا می‌باشند. جهت محافظت کامل سیستم در مقابل ویروس‌ها، فایل تعریف ویروس باید به طور مرتب به روز رسانیده شود.

یک حافظ ویروس نوعی برنامه می‌باشد که از زمان راه‌اندازی تا خاموش نمودن سسیستم در حافظه در تمام مدت در حال اجرا خواهد بود. حافظ ویروس به طور دائم تمام پردازش‌ها را جهت پیدانمودن ویروس تحت نظارت قرار می‌دهد. پس از شناسایی ویروس، ویروس را می‌توان قبل از وارد نمودن‌هرگونه صدمه حذف نمود و اجرای عادی برنامه می‌تواند به کار خود ادامه دهد.

محافظت با استفاده از کلمه عبور

احتمالا بدون توجه به سیستم عاملی که روی کامپیوترهای شبکه شما وجود دالرد از کلمه عبور برای کنترل دستیابی به منابع مختلف شبکه استفاده می‌کنید. برای شبکه هایی که نیاط به امنیت بسیار بالایی دارند ابزارهای حرفه ای پیچیده ای وجود دارد.
همچنین ابزارهای دیگری هم در بازار .وجود دارند که کاربران را با توجه به خصوصیات فیزیکی منحصر بفرد انها . مثل اثر انگشت و یا الگوی شبکه چشم. شناسایی می کنند. اما در اغلب شبکه ها به اینگونه روش های امنیتی پیچیده نیاز نمی باشد بلکه داشتن یک کلمه عبور برای دستیابی به درایوهای مشترک. برنامه های کاربردی روی سرور و منابع دیگر شبکه کافی می باشد.
کارا بودن یا نبودن استفاده از محافظت با کلمه عبور در حد زیادی به تدابیری بستگی دارد که مدیر شبکه از آن تدابیر برای تعیین ضوابط کلمه عبور استفاده می کند.
البته این امکان هم وجود دارد که مدیران شبکه خود به هر یک از کاربران کلمه عبوری اختصاص دهند.
در اغلب سیستم عامل ها ابزارهایی در اختیار مدیران شبکه قرار داده می شود که بتوانند با ترکیب دو روش بالا، راه حلی مناسب برای استفاده از کلمه عبور پیاده کنند.

تنظیمات مربوط به کلمه های عبور حسابهای کاربران

در ویندوز ۲۰۰۰ و یا NT زمان ایجاد یک حساب کاربری جدید، گزینه های مختلفی برای کنترل ابتدایی ترین مسائل امنیتی وجود دارد.

- User Must Change Password At Next Logon. این گزینه مدیر شبکه را قادر می سازد یک کلمه عبور یکسان به هر حساب کاربری جدیدی واگذار کند و کاربران را مجبور کند در اولین ورود به شبکه کلمه عبور را تغییر دهند.
- User Cannot Change Password . این گزینه به کاربران این امکان را نمی دهد که بتوانند کلمه عبوری را که در هنگام ایجاد حساب کاربری آنها تعیین شده است تغییر دهند. اگر مدیر شبکه ای تصمیم بگیرد که خودش برای تک تک کاربران کلمه عبور انتخاب کند با فعال کردن این گزینه در همه حسابها مطمئن خواهد بود که هیچ کاربری نمی تواند کلمه عبور خود را تغییر دهد بنابراین همه چیز تحت کنترل مدیر شبکه می ماند.
- Password Never expire . با فعال کردن این گزینه کاربران هنوز می توانند در صورت تمایل کلمه عبور خود را تغییر دهند ولی مجبور نیستند که حتماً در یک زمان خاص اینکار را انجام دهند.
- Account is disabled . این گزینه مدیر شبکه را قادر می سازد بدون اینکه نیاز به پاک کردن و ایجاد مجدد باشد، حسابی را موقتاً غیر فعال کند.

مشخص کردن طول کلمه عبور

سرویس Active Directory ویندوز ۲۰۰۰ از کلمه های عبور بطول حداکثر ۱۰٤ کاراکتر پشتیبانی می کند، گرچه در عمل هرگز استفاده از چنین کلمه عبوری امکان پذیر نمی باشد. در ویندوز NT حداکثر طول هر کلمه عبور می تواند ١٤ کاراکتر باشد. بطور کلی برای اغلب شبکه ها کلمه های عبوری بطول پنج یا شش کاراکتر مناسب است.

در جایی که امنیت بالاتری احتیاج باشد، ممکن است حداقل طول کلمه های عبور هشت کاراکتر و یا حتی بیشتر باشد.تعیین طول کلمه های عبور مانند خصوصیات دیگر توسط سیستم عامل و به روش های گوناگون انجام می شود. در ویندوز ۲۰۰۰ اینکار را می‌توانید با استفاده از ویژگی Group Policy انجام دهید.

تنظیم مدت اعتبار کلمه های عبور

فاکتور مهم دیگر در اجاد امنیت بوسیله کلمه عبور اینست که کلمه های عبور بطور مرتب تغییر داده شوند. کاربران گاهی حتی کلمه عبور خود را به کاربران دیگر می دهند و بعد معمولاً فراموش می کنند که آنرا تغییر

دهند. با مجبور کردن کاربران به تغییر کلمه های عبور خود بطور مرتب، می توانید تضمین کنید که بعد از مدتی کلمه های عبور در دست عموم قرار نخواهد گرفت.
در ویندوز ۲۰۰۰ علاوه بر این امکان شما می توانید با استفاده از گزینه Maximum Password Age کاربران را مجبور کنید هر چند یکبار کلمه عبور خود را تغییر دهند. مدت اعتبار کلمه های عبور بنابر نیازهای امنیتی شبکه معمولاً از یک هفته تا یک ماه می باشد.

الزام بر استفاده از کلمه های عبور پیچیده

معمولاً استفاده از نام همسر، بچه ها، تاریخ تولد، حروف اول اسم و فامیل و اطلاعات عمومی دیگر بعنوان کلمه عبور مناسب نیستند چون براحتی قابل حدس زدن می باشند. بعنوان انتخابی بهتر بد نیست از مثلاً نام یکی از دوستان قدیم خود استفاده کنید و بعد برای اطمینان بیشتر کاراکترهای آن اسم را بهم بریزید.

اگر در کادر Security Policy Setting گزینه password must meet complexity requirement را فعال کنید کلمه عبور منتخب کاربران باید در چهار چوب ضوابط زیر باشد:

- حداقل طول کلمه عبور باید شش کاراکتر باشد.
- کلمه عبور نمی تواند شامل هیچ بخشی از شناسه کاربری خود باشد.
- کلمه عبور باید متشکل از سه نوع کاراکتر از چهار نوع کاراکتر زیر باشد: حروف بزرگ، کوچک، اعداد،علائم.

رمزنگاری کلمه های عبور

اغلب سیستم عامل ها کلمه های عبور را بصورت رمزنگاری شده ذخیره می کنند تا کسی نتواند بوسیله نرم افزارهای مخصوص ویرایش دیسک، محتوی درایوی که کلمه های عبور روی آن ذخیره شده است را بخواند. بطور پیش فرض الگوریتمی که در ویندوز ۲۰۰۰ برای رمز نگاری بکار می رود قابل برگشت نمی باشد. اما در صورت نیاز می توانید با فعال کردن گزینه Store Password Using Reversible Encryption For All User In The Domain از روش رمزنگاری استفاده کنید که برای بازیابی کلمه های عبور فراموش شده قابل برگشت باشد.

تدابیر مربوط به بستن یک حساب

هر کسی ممکن است بتواند با حدس زدن به تعداد کافی، هر کلمه عبوری را پیدا کند این روش به brute force مشهور است. در اغلب سیستم عامل ها امکان بستن یک حساب وجود دارد تا هر کسی نتواند متناوباً سعی در حدس زدن کلمه عبور آن حساب کند.

امنیت شبکه

نرم افزار مدیریت می تواند شما را در مورد امنیت منابع شبکه نیز کمک کند. معمولاً انجام اینکار به اطلاعات مربوط به کاربران و فعالیتهای کاربران نیاز دارد.البته اکثر سیستم های عامل مدرن تهیه گزارش امنیتی از جزئیات را فراهم می سازند. اما تهیه گزارش امنیت یکی سازی شده بدین معنی است که مدیر شبکه نباید گزارشهای امنیتی هر سرور را بطور جداگانه وارسی کند. وارد شدن به سیستم توسط افراد بدون مجوزرا می توان بصورت مستقیم به کنسول مدیریت مدیر شبکه گزارش داد.

عملیات شبکه

یک مدیر شبکه باید از عملیات و اجرای شبکه گزارش تهیه کند و بسیازی از زیر بناهای مدیریتی ابزارهای ضروری را جهت اندازه گیری اجرای عملیات شبکه فراهم می سازند. مدیران شبکه میتوانند انواع گسترده ای از خصایص عملیاتی شبکه را نظارت کنند و یک baseline شبکه ایجاد کنید. بعلاوه جمع آوری اینگونه اطلاعات روند توسعه شبکه را نیز مشخص می کند و مدیر شبکه می تواند قبل از برخورد با مشکل کمی منابع اقدامات لازم را انجام دهد.

تجزیه و تحلیل هزینه شبکه

عملیات شبکه به هزینه نیاز دارد و یک شبکه فقط می تواند مقدار منابع مشخص شده ای را در اختیار یک اربر یا گروه قرار دهد. یک مدیر شبکه باید اقدامات لازم را برای روش استفاده از یک شبکه فراهم سازد. اغلب اعمال چنین وضعیتی بصورت دستی مشکل یا حتی غیر ممکن است اما زیر بناهای مدیریت ابزارهای تجزیه و تحلیل لازم را فراهم می سازند تا یک مدیر شبکه بتواند شبکه را بنحوی که مانند یک منبع مصرفی می باشد نظارت داشته باشند و بعد مالی را در مورد کاربران شبکه بکار گیرد. پس از اینکه یک مدیر شبکه کاربران و فعالیتهای مربوط را از لحاظ کمیتی مشخص نمود مرتبط نمودن هزینه با کاربران ممکن می شود در بعضی موارد ویژگیهای تجزیه و تحلیل نرم افزار مدیریت شبکه حتی می توانند امکان تغییر برای دسترسی به شبکه را فراهم سازند.

بغیراز موارد مالی، مدیریت باید کاربران و گروههایی که به منابع شبکه دسترسی دارند را شناسایی کند. با شناسایی شفاف موارد استفاده ، یک مدیر شبکه می تواند ارتقاءهای صحیح را برنامه ریزی کند یا اقدامات لازم را جهت ساده تر نمودن عملیات شبکه بکار گیرد. می توانید بر اساس بکارگیری داده ها تصمیمات مربوط به ارتقاء را اتخاذ نمایید و به این گروه سرور خاصی را تخصیص دهید. انجام اینکار سرور موجود را برای سرویس دهی به سایر کاربران آزاد می سازد.

تکنیک های مدیریت و عیب یابی

در حال حاضر انواع گوناگونی از نرم افزارهای مدیریت شبکه در بازار نرم افزار وجود دارند. همچنین شرکتهایی مانند Compaq ، HP ، Getaway و غیره نیز نرم افزارهای مدیریت عرضه کرده اند. با چنین گستردگی در انواع اینگونه نرم افزارها، انتخاب بهترین ابزار می تواند مشکل باشد.

هنگام انتخاب یک نرم افزار مدیریت شبکه عوامل زیر را در نظر داشته باشید:

- مستندات را بخوانید.
- امنیت را بخوبی درک کنید
- آسان بودن یافتن وسایل در شبکه.
- آسان بودن پیکربندی مربوط به عملیات یافتن وسایل در شبکه
- آسان بودن سفارشی سازی polling نمودن وسایل مهم
- آسان بودن پیکربندی پیامهای خطا
- آسان بودن ایجاد و سازماندهی گزارش رویداد
- آسان بودن شناسایی وسایل
- آسان بودن افزودن وسایل جدید
- آسان بودن بکارگیری اقدامات رفع عیب

دیواره های آتش

محصولی سخت افزاری و یا نرم افزاری می باشد که شبکه را از دستیابی بدون اجازه کاربران خارجی حفظ می کند. اگر شبکه شما به اینترنت متصل است حتما باید از نوعی از دیواره های آتش برای محافظت شبکه استفاده کنید چون مزاحمان خارجی می توانند براحتی شبکه را دچار اختلال کنند.

فیلتر کردن بسته ها

در این روش ، دیواره آتش بسته های دریافتی را بررسی کرده و بنابر اطلاعات موجود در هردهای پروتکلهایی که در ایجاد بسته سهیم بوده اند، تصمیم می گیرد که به آنها اجازه عبور به شبکه دیگر را بدهد یا خیر. یک دیواره آتش می تواند بسته ها را بنابر هر یک از خصوصیات زیر فیلتر کند:

- آدرس‌های سخت افزاری
- آدرس‌های IP
- شناسه پروتکل
- شماره پورت ها

NAT

یک تکنیک لایه شبکه که با مخفی کردن آدرس های IP کامپیوترهای مستقر در شبکه آنها را در مقابل مزاحمان اینترنتی محافظت می کند. اگر شبکه را بدون استفاده از یک نوع دیواره آتش به اینترنت متصل کنید، برای اینکه کامپیوترهای این شبکه بتوانند با کامپیوترهای دیگر موجود در اینترنت ارتباط برقرار کنند باید از آدرسه های IP ثبت شده استفاده کنید. از طرف دیگر بنابر تعریف، آدرس های IP ثبت شده از اینترنت قابل رؤیت هستند در نتیجه هر کسی می تواند از طریق اینترنت به کامپیوترهای شبکه شما دسترسی داشته باشد و با کمی ذکاوت به همه منابع دسترسی پیدا کند. اما استفاده از ترجمه آدرس شبکه به شما این امکان را می دهد که با واگذاری آدرس های IP ثبت نشده به کامپیوترهای خود آنها را از زاویه دید کاربران اینترنتی خارج کنید.

پروکسی سرور

محصولاتی نرم افزاری مشابه با مسیریابهای NAT ، با این تفاوت که در لایه کاربرد مدل OSI کار می کنند. یک پروکسی سرور همانند یک مسیریاب LAN بعنوان رابط بین سرویس گیرنده های موجود در یک شبکه و منابع اینترنتی مورد نیاز آنها عمل می کند. سرویس گیرنده ها در خواست های خود را به پروکسی سرور می فرستند سپس پروکسی سرور هم آن درخواست ها را به سرور اینترنتی مقصد منتقل می کند. سرور اینترنتی جواب درخواست را به پروکسی سرور می فرستد و آنهم به نوبه خود داده ها را به سرویس گیرنده منتقل می کند. به اینصورت سرویس گیرنده از طریق اینترنت قابل رویت نمی باشد.مزیت دیگر پروکسی در اینست که مدیران شبکه می توانند آنها را طوری پیکربندی کنند که بنابر نیاز ترافیک ورودی را فیلتر کنند تا جلوی کاربران را از دسترسی به یکسری از سرویس های بخصوص بگیرند.

مشکل اصلی پروکسی سرورها اینست که باید برنامه های آنها را برای اینکه بتوانند از آنها استفاده کنند پیکربندی کنید گرچه یک مسیریاب NAT کامپیوترهای شبکه شما را محافظت می کند ولی پیکربندی تعداد زیادی برنامه برای استفاده از پروکسی بسیار وقت گیر است.اما سرویس گیرنده ها و پروکسی سرورهایی با قابلیت تشخیص خودکار وجود دارند که یک برنامه را قدر به شناسایی پروکسی سرورهای موجود در شبکه و استفاده از آنها می کند.

دیوارهای آتش و سرورهای Proxy

دو ابزار مهم و محبوب استفاده شده جهت ایمن سازی شبکه ها عبارتند از دیوارهای آتش و سرورهای proxy . وظیفه اساسی یک دیوار آتش فراهم نمودن سپر حفاظ برای ترافیک شبکه است تا از دسترسی های بدون مجوز به یا از یک کامپیوتر شبکه جلوگیری شود. سرورهای proxy جهت تکمیل نمودن تقاضاهای کاربران داخلی میباشد که با منابع خارجی می خواهند ارتباط برقرار کنند. سرویسهای proxy را می توان بطور مستقیم از طریق دیوار آتش یا بر روی کی میزبان مجزا در رابطه با یک دیوار آتش فراهم نمود.

درک یک دیوار آتش

دیوارهای آتش می توانند اشکال و اندازه های متفاوت داشته باشند و در مواردی دیوار آتش در واقع مجموعه ای از چندین کامپیوتر متفاوت است.
ما در اینجا یک دیوار آتش را در نظر می گیریم که بین شبکه های داخلی و خارجی مانند اینترنت قرار می گیرند و ترافیک بین این شبکه ها را کنترل می کنند. دیوارهای آتش باید خصایص زیر را داشته باشند:

- تمامی ارتباطات باید از دیوار آتش عبور کنند.
- دیوار آتش فقط ترافیکی را اجازه می دهد که دارای مجوز است.
- دیوار آتش باید بتواند از خود نیز حفاظت کند.

اگر یک مسیر متفاوت شبکه موجود باشد، تأثیرگذاری دیوار آتش بطور قابل ملاحظه ای کاهش می یابد بعلاوه، اگر دیوار آتش نتواند تفاوت بین ترافیک با مجوز و بدون مجوز را تشخیص دهد، یا اگر بنحوی پیکربندی شده است تا ارتباطات خطرناک یا بدن نیاز را اجازه دهد، کاربرد دیوار آتش نیز از بین می رود. در نهایت دیوار آتش باید بتواند از خود حفاظت کند.
یک دیوار آتش می تواند یک مسیریاب،یک کامپیوتر شخصی، یک میزبان یا مجموعه ای از میزبانهای تنظیم شده باشد تا یک شبکه خصوصی را حفاظت کند. یک دیوار آتش معمولاً خارج از محیط شبکه و بطور مستقیم

بین شبکه و منابع خارجی قرار می گیرد. روشی که دیوار آتش عمل می کند به خود دیوار آتش و قوانین / سیاستهای پیکربندی شده برای دیوار آتش بستگی دارد چهار مقوله از تکنولوژیهای دیوار آتش موجود زیر لیست شده اند:

- Packet Filters
- Application Gateways
- Circuit – Level Getaways
- Stateful packet – inspection engineer

دیوارهای آتش و TCP/IP

TCP/IP مجموعه ای از پروتکلها و برنامه های کاربردنی است که توابع خاصی را در رابطه با لایه های خاص مدل OSI یا مدل Open System Interconnect انجام می دهد. انتقال داده ها از طریق TCP/IP بوسیله انتقال مستقل بلوکهایی از داده بر روی شبکه به شکل بسته ها صورت می گیرد. هر لایه مدل TCP/IP یک سرنام به بسته اضافی می کند. بر اساس تکنولوژی دیوار آتش مورد استفاده، دیوار آتش جهت تصمیم گیری در مورد دسترسی از اطلاعات موجود در این سرنام ها استفاده می کند.

دیوارهای آتش از نوع فیلتر سازی بسته

دیوارهای آتش فیلترسازی بسته با فیلترسازی ارتباطات شبکه بر اساس اطلاعات موجود در سرنام های TCP/IP هر بسته حفاظت سیستم را فراهم می سازد. دیوار آتش سرنام هر بسته را وارسی می کند و با استفاده از اطلاعات موجود در سرنام بسته را می یرد یا رد می کند.
فیلترهای بسته بر اساس اطلاعات زیر در سرنام تصمیم گیری می کنند:

- آدرس IP مبدأ
- آدرس IP مقصد
- پروتکل شبکه مورد استفاده
- درگاه مبدأ TCP یا UDP
- درگاه مقصد TCP یا UDP
- نوع پیام ICMP ، اگر پروتکل از نوع ICMP باشد.

مزیتها و کاستی های فیلترسازی بسته

مزیتها عبارتند از:

- سرعت – فیلترسازی را می توان مانند سرعت پردازنده های امروزی پیاده سازی کرد.
- هزینه – فیلترهای بسته تقریباً ارزان یا رایگان می باشند.
- مدیریت خوب ترافیک – فیلترهای بسته ساده را می توان جهت حذف ترافیکهای آشکار بدون مجوز استفاده نمود.
- ترانسپارانسی – رفتار عملیاتی کاربر بدلیل پیداسازی یک فیلتر بسته تغییر نمی یابد.
- کاستی ها عبارتند از:
- ارتباط مستقیم بین میزبانهای خارجی و داخلی
- فیلترهای بسته بخوبی اندازه پذیر نمی باشند.
- فیلترهای بسته در رابطه با حمله های spoofing مقاوم نمی باشند. این نوع حمله معمولاً اطلاعات قلابی در سرنام های TCP/IP در در بردارد.

دیوارهای آتش از نوع Application Gateways

Application Gateways تصمیم گیریهای دسترسی را بر اساس اطلاعات موجود در یک بسته در تمامی هفت لایه مدل OSI اتخاذ می کند. این روش درجه بالاتری از امنیت را در مقایسه با یک فیلتر بسته ارئه می دهد اما اینکار ار در رابطه با از دست دادن ترانسپارانسی سرویسها انجام می دهد. Application Gateways اغلب بعنوان واسط برای برنامه های کاربردی مانند پست الکترونیکی، FTP، Telnet ، HTTP و الی آخر عمل می کند. خصوصاًApplication Gateways به عنوان یک سرور برای سرویس گیرنده و به عنوان یک سرویس گیرنده برای سرور واقعی عمل می کند.

دیوار آتش از نوع Circuit-level gateway

این نوع دیوار آتش مانند Application Gateways می باشد، اما برنامه کاربردی مربوطه خصوصیت هوشیار بودن ندارد. یک Circuit-level gateway با ربه نمودن اتصالهای TCP از شبکه داخلی به شبکه خارجی عمل می کند. یک اتصال مستقیم بین سرویس گیرنده و سرور هرگز رخ نمی دهد. بدلیل اینکه این روش نمی تواند پروتکل برنامه کاربردی را درک کند، باید اطلاعات اتصال از طریق سرویس گیرنده هایی که پروتکل را

درک می کنند و جهت کار با این پروتکل برنامه ریزی شده اند عرضه شوند. بطور کل یک Application Gateways از روالهای تغییر یافته استفاده می کند، در حالیکه Circuit-level gateway سرویس گیرنده های تغییر یافته را بکار می گیرد.

دیوار آتش از نوع Stateful-packet-inspection-engine

بسته ها را بر اساس یک سری قاعده مشابه با قوانین packet-filtering اجازه می دهد یا رد می کند. زمانیکه یک دیوار آتش در state هوشیاری است، تصمیم گیریهای دسترسی را نه تنها بر اساس آدرسهای ip و درگاهها بلکه بر اساس Syn ، ACK اعداد سریال و سایر داده های موجود در سرنام TCP اتخاذ می کند. در حالیکه فیلترهای بسته می توانند بسته ها را بطور مجزا اجازه دهند یا رد کنند و برای ارتباطات TCP دوطرفه به قوانین مربوط به مجوز نیاز دارند، دیوارهای آتش SPI وضعیت هر جلسه را وارسی می کنند و بصورت پویا طبق نیاز جلسه های خاص درگاهها را باز می کنند و می بندند. دیوارهای آتش SPI جهت ترکیب سرعت و قابلیت انعطاف پذیری فیلترهای بسته یا امنیت Application-Level از proxy های برنامه کاربردی توسعه یافته اند.

مدل های مختلف امنیتی

یکی از مهم ترین فعالیت های مدیر شبکه، تضمین امنیت منابع شبکه است. دسترسی غیر مجاز به منابع شبکه و یا ایجاد آسیب عمدی یا غیر عمدی به اطلاعات، امنیت شبکه را مختل می کند. از طرف دیگر امنیت شبکه نباید آنچنان باشد که کارکرد عادی کاربران را مشکل سازد.

امنیت سطح – کاربر

در مدل امنیتی سطح – کاربر برای هر کابربری یک حساب کاربری مجزا ایجاد می شود. در صورتی که بخواهید به کاربران اجازه دستیابی به منابع یک کامپیوتر بخصوص را بدهید باید آنها را از لیست حسابهای کاربران انتخاب و جوازهای دلخواه را به آنها اختصاص دهید.

امنیت سطح – مشترک

در این مدل امنیتی کاربران به منابع مشترک مختلف کامپیوترهای خود یک کلمه عبور اختصاص می‌دهند. در صورتیکه کاربری بخواهد به یک منبع مشترک کامپیوتر دیگر دسترسی پیدا کند باید کلمه قبور مناسب را داشته باشد.

این کلمه های عبور مشترک روی کامپیوترهای مربوط به خود ذخیره می شوند.

پروتکل‌های امنیتی

علاوه بر امکانات امنیتی موجود در سیستم عامل های شبکه پروتکل‌های امنیتی استانداردی هم وجود دارند که برنامه های کاربردی و سیستم عامل ها از آنها برای محافظت داده های در حال عبور در شبکه استفاده می کنند. این پروتکل‌ها معمولاًروی داده ها یک رمز نگاری بخصوصی انجام می دهند و روشی که کامپیوترها باید از آن برای خواندن داده های رمزنگاری شده توسط یکدیگر استفاده کنند را تعریف می کنند.

انواع پروتکل‌های امنیتی

- **IP Sec**

IP Sec یک اصطلاح عامیانه برای توصیف استانداردهایی است که توسط IETF منتشر شده است و مربوط به ایمن سازی داده های در حال عبور روی شبکه ها با استفاده از احراز هویت و رمزنگاری می باشد. اغلب پروتکل هایی که دارای قابلیت رمزنگاری داده های در حال عبور در شبکه را دارند برای استفاده در اینترنت یا تبادل اطلاعات بین انواع بخصوصی از سرورها و سرویس گیرنده ها طراحی شده اند تا زمان IP Sec هیچ استانداردی برای محافظت از داده های در حال عبور در شبکه وجود نداشت. البته شما می توانستید دستیابی به منابع مختلف را با کلمه عبور کنترل کنید اما داده های واقعی در حال عبور در رسانه شبکه محافظت شده نبودند.

- **L۲TP**

IPsec در مد تونل هم می تواند بطور مستقل و هم با همکاری پروتکل L۲TP کار کند. این پروتکل از پروتکل CSL۲F و PPTP مشتق و در یکی از سندهای IETF تعریف شده است. L۲TP با بسته بندی فریم‌های PPP در بسته های UDP یک تونل محافظ ایجاد می کند. فریم های PPP حتی اگر حاوی داده های اتصال گرای TCP هم باشند می توانند داخل یک دیتاگرام بدون اتصال UDP حمل شوند در واقع فریم های PPP می‌توانند حتی شامل داده های IPX و یا NetBEUI هم باشند.

L۲TP بخودی خود دارای هیچگونه امکان رمزنگاری نمی‌باشد. البته امکان ایجاد یک تونل، بدون رمزنگاری داده های داخل آن وجود دارد اما به درسر آن نمی ارزد. این پروتکل برای کپسوله کردن و رمزنگاری کل دیتاگرام UDP که شامل فریم PPP هم می شود از پروتکل ESP استفاده می کند. بنابراین هر بسته آماده عبور در شبکه حاوی داده های اصلی کپسوله شده در یک فریم PPP که خود در یک فریم L۲TP ، یک دیتاگرام UDP ، یک فریم ESP ، یک دیتاگرام IP و نهایتاً یک فریم PPP دیگر کپسوله شده است می باشد.

- **SSL**

SSL یک پروتکل امنیتی تک منظوره می باشد که برای محافظت داده های در حال انتقال بین سرورهای وب و مرورگرهای سرویس گیرنده طراحی شده است. تقریباً همه سرورهای وب و مرورگرهای موجود از این پروتکل پشتیبانی می کنند.

SSL همانندIPsec دارای سرویس های احراز هویت و رمزنگاری می‌باشد. احراز هویت و توافق بر سر روش مورد استفاده برای رمز نگاری داده ها توسط پروتکل SSLHP انجام می شود. سپس پروتکل SSLRP داده ها را برای رمزنگاری بسته بندی می کند. وقتیکه یک مرورگر وب به یک سرور ایمن شده متصل می شود، سرور یک گواهی دیجیتال را که خود از یک صادر کننده گواهی بدست آورده است به سرویس گیرنده می فرستد. سرویس گیرنده با استفاده از کلید عمومی همان صادرکننده گواهی کلید عمومی سرور را از گواهی دیجیتال بیرون می کشد. وقتی مرورگر توانست کلید عمومی سرور را بدست آورد، می تواند داده هایی که توسط سرور رمزنگاری و فرستاده شده است را رمزگشایی کند.

- **Kerberos**

Kerberos یک پروتکل هویت شناس است که در سرویس های دایرکتوری از قبیل Active Directory استفاده می شود و به کاربران امکان احراز هویت و ورود به شبکه را می دهد. وقتی یک سرور در حال اجرای پروتکل Kerberos سرویس گیرنده ای را با موفقیت احراز هویت کند آن سرویس گیرنده می تواند به منابع موجود در شبکه دسترسی پیدا کند. این پروتکل در MIT طراحی و توسط IETF استاندارد شده است. ویندوز ۲۰۰۰ و سیستم عامل های دیگر برای ایمن سازی شبکه های سرویس گیرنده / دهنده خود کاملاً بر این پروتکل متکی هستند.

امنیت ارتباطات

در اینجا نگاهی به امنیت ارتباطات که در خصوص تحویل مطمئن و سری بیتها از مبداء به مقصد بدون هیچ تغییر یا دستکاری و همچنین چگونگی جلوگیری از تزریق بیتهای ناخواسته به لینک ارتباطی می اندازیم.

- **IPsec**

IP sec در مستندات REC ۲٤۰۱ ، ۲٤۰۲، ۲٤۰٦ تشریح گشت. از آنجا که تمام کاربران نمی خواهند که از رمزنگاری استفاده کنند، لذا استفاده از آن اختیاری است. البته برای آن که طرح IP sec عمومیت خود را از دست ندهد و در همان بدو کار کثرت پروتکل بوجود نیاید تصمیم بر آن شد که در تمام حالات رمزنگاری انجام

شود ولیکن در عوض، یک الگوریتم «پوچ» تعریف گردید. این الگوریتم پوچ به دلیل سادگی راحتی در پیاده سازی وسرعت بسیار بالا در RFC ۲٤۱۰ تشریح و از آن ستایش شده است!!!! شاید سریعترین الگوریتم دنیا باشد!

طراحی کامل IPsec متشکل از یک چارچوب کاری برای ارائه خدمات چندگانه، شامل تعدادی الگوریتم و مولفه است. دلیل ارائه چندین رده خدمات ان است که شاید همه نخواهند برای استفاده از تمام آنها هزینه بپردازند فلذا این خدمات به صورت انتخابی در اختیار کاربران هستند. خدمات ویژه عبارتند از «ارسال محرمانه بسته ها» ، «تضمین صحت» و حفاظت در مقابل حملاتی که بر اساس آنها یک بخش از داده ها به صورت تکراری ارسال می شوند . تمام خدمات فوق بر اساس رمزنگاری با کلید متقارن انجام می شود زیرا در سطح لایه شبکه کارایی و سرعت بسیار بالا، کاملاً حیاتی است.

دلیل استفاده از چندین الگوریتم رمزنگاری آن بوده که شاید الگوریتمی که امروزه امن به حساب می آید در آینده شکسته شود. وقتی IPsec مستقل از الگوریتم خاص طراحی شده باشد، حتی در صورت شکسته شدن یک الگوریتم در آینده، باز هم قابل استفاده خواهد بود و به حیات خود ادامه می دهد.دلیل مولفه های چندگانه ای که این پروتکل دارد انست که بتوان فقط بر روی یک اتصال TCP متمرکز شد و از داده هایی که بین دو ماشین خاص در شبکه مبادله می شود مراقبت کرد یا آنکه از بین کل مسیریابها صرفاً ترافیک بین دو مسیریاب امن، رمزنگاری شود.

یکی از جنبه های نسبتاً عجیب IPsec آن است که اگر چه این پروتکل در لایه IP قرار می گیرد ولیکن برخلاف IP ، اتصال گرا است . در واقع این مسئله چندان هم عجیب و دور از ذهن نیست زیرا برای ایجاد امنیت باید یک کلید رمز بین ماشینها توافق و ایجاد گردد که در اصل نوعی از **اتصال** محسوب می شود.
البته هزینه برقراری این چنین اتصالی بر روی حجم زیادی از بسته ها سرشکن می شود. یک «اتصال» در عرف IPsec اصطلاحاً SA نامیده می شود. یک SA ، اتصالی یکطرفه بین دو نقطه پایانی در شبکه است که به آن یک «شناسه امنیت» درون بسته هایی که در شبکه و مبتنی بر یک اتصال سیر می کنند جاسازی شده و از آن برای جستجوی کلید متناظر و همچنین بدست آوردن اطلاعات مرتبط با بسته های امن ورودی استفاده می‌شود.

- **دیوارهای آتش**

پیاده سازی مدرنی از روش قدیمی و قرون وسطایی حصارهای امنیتی است: خندقی عمیق دور تا دور قلعه خود حفر کنید این الگو همه را مجبور می کند تا برای ورود یا خروج از قلغه از یک پل متحرک و واحد بگذرند و

بتوان همه را توسط پلیس حراست بازرسی کرد. در دنیای شبکه های کامپیوتری، همین راهکار ممکن خواهد بود: یک شرکت می تواند هر تعداد شبکه محلی داشته باشد که به صورت دلخواه به هم متصل شده اند، اما تمام ترافیک ورودی یا خروجی شرکت صرفاً از طریق یک پل متحرک میسر است.

دیوار آتش با پیکربندی دو مؤلفه دارد:

- یک جفت مسیریاب که عمل غربال سازی بسته ها را انجام می دهند.
- دروازه برنامه های کاربردی. ساختار ساده تری نیز وجود دارد ولیکن حسن بزرگ این طرح آنست که هر بسته باید از دو مرحله غربال سازی و یک مرحله بازرسی محتوایی توسط دروازه، بگذرد. هیچ مسیر دیگری نیز وجود ندارد. خوانندگانی که فکر می کنند فقط یک مرحل بازرسی امنیتی کافی است، به احتمال زیاد اخیراً یک پرواز بین المللی با خطوط هوایی نداشته اند!

هر غربال کننده بسته، یک مسیریاب استاندارد با برخی از ویژگیهای بیشتر است. این قابلیت اجازه می دهد که تمام بسته های ورودی و خروج بازرسی شوند. بسته هایی که بتوانند برخی از معیارها و شرایط را احراز کنند بطور طبیعی هدایت می شوند و آنهایی که در این بازرسی مردود شوند حذف می گردند.

شبکه های خصوصی مجازی(VPN)

شبکه ای که از کامپیوترهای شرکت و خطوط اجاره ای تلفن تشکیل شده اصطلاحاً«شبکه خصوصی» نامیده می شود.
شبکه های خصوصی، بسیار خوب و مطمئن عمل می کنند. اگر خطوط در اختیار شرکت، تماماً اجاره ای باشند، هیچ ترافیکی نمی تواند به بیرون از شرکت نشت کند و اخلال گر مجبور است به صورت فیزیکی از خطوط انتقال انشعاب گرفته و بدانها متصل شود که انجام این کار نیز ساده نخواهد بود.

مشکل بزرگ شبکه های خصوصی آنست که اجاره کردن یک خط T۱ در هر ماه هزاران دلار هزینه دارد خطوط T۳ میز چندین برابر گرانتر هستند. وقتی شبکه های عمومی داده و بعد از آن اینترنت به صحنه آمد، بسیاری از شرکتها تصمیم گرفتند که انتقال داده های خود را از طریق شبکه های عمومی موجود انجام بدهند که هزینه ناچیزی دارد ولیکن در عوض امنیت یک شبکه خصوصی ندارد.
احساس این نیاز به ابداع VPN انجامید که بر روی زیر ساخت شبکه عمومی بنا شده است ولی اکثر ویژگیهای یک شبکه خصوصی را عرضه می کند. این گونه شبکه ها از آن جهت «مجازی» نامیده شده اندکه صرفاً یک توهم هستند دقیقاً مثل «مدار مجازی» که در آن هیچ مدار واقعی در کار نیست یا « حافظه مجازی» که در آن هیچ حافظه واقعی از نوع RAM وجود ندارد.

امنیت نامه های الکترونیکی

وقتی یک پیام توسط پست الکترونیکی بین دو سایت راه دور مبادله می شود بطور معمول آن نامه در طی مسیر خود از دهها ماشین میانی عبور خواهد کرد. هر یک از این ماشینها قادرند آن را بخوانند یا برای استفاده های بعدی ذخیره کنند. بر خلاف آنچه که بسیاری از مردم می اندیشند، حریم خصوصی عملاً وجود ندارد ولیکن علیرغم این بسیاری از افراد علاقمندند نامه هایی را که ارسال می کنند فقط گیرنده مورد نظر بخواند نه هیچکس دیگر نه رئیس آنها و نه حتی حکومت. این احساس نیاز بسیاری از گروهها و افراد را ترغیب کرد که اصول رمزنگاری را که تا اینجا بررسی کردیم بر روی نامه های الکترونیکی اعمال کرده و یک سیستم امن پست الکترونیکی به وجود بیاورد.

سیستم های امن پست الکترونیکی

- PGP
- PEM
- S/MIME

امنیت وب

تا اینجا دو زمینه بسیار مهم را که مقوله امنیت در آنها ضروری است مطالعه کرده ایم: امنیت در مخابره داده ها و امنیت در سیستم پست الکترونیکی. می توانید اینها را به عنوان سوپ و پیش غذا تلقی کنید. حال وقت آن رسیده تا به موضوع اصلی بپردازیم:«امنیت وب» . امروزه وب جولانگاه اخلالگران و ترودیهایی است که به کارهای کثیف خو مشغولند. در بخشهای آتی به برخی از موارد و مشکلات مربوط به امنیت وب نگاهی خواهیم انداخت.
بطور تقریبی امنیت وب را می توان در سه بخش تقسیم کرد: اول آن که چگونه اشیاء و منابع به روشی مطمئن نامگذاری شوند؟ دوم آنکه چگونه می توان ارتباطی تایید شده و مطمئن برقرار کرد؟ سوم وقتی یک وب سایت برای مشتری خود یک قطعه کد قابل اجرا می فرستد چه اتفاقی می افتد؟ پس از آنکه به تهدیدهای بالقوه در وب نگاهی انداختیم این سه مورد را در نظر داشته باشیم:

- تهدیدها
- نامگذاری مطمئن
- لایه سوکتهای امن

مبانی امنیت شبکه

دلیل اینکه از دیواره های آتش استفاده می کنیم این است که دیوارهای آتش جهت تشخیص و تصمیم گیری در رابطه با ارتباطات مجوزدار و بدون مجوز استفاده می شوند. سیستم ها و داده های شرکتی سه خصوصیت اصلی دارند که از طریق دیوار آتش محافظت می شود:

- خطر از دست دادن محرمانه بودن داده ها
- خطر از دست دادن سلامت و تمامیت داده ها
- خطر از دست دادن قابلیت دسترسی به داده ها

انواع رایج حملات

در واقع روشهای زیادی را یک فرد بدون مجوز می تواند جهت دسترسی به یک سیستم بکار گیرد. در زیر لیست خلاصه ای از حملات رایج فراهم شده است:

- مهندسی اجتماعی – یک هکر یک مدیر شبکه یا یک کاربر با مجوز را بنحوی وادار می کند تا جزئیات وارد شدن به سیستم را در اختیارش بگذارند.
- خرابیهای نرم افزاری – یک هکر یک جریان برنامه نویسی را دنبال می کند و یک برنامه کارردی را یا سرویسی را مجبور می کند تا فرامین بدون مجوز را اجرا کند.
- ویروسها یا کدهای با ویروس – یک هکر یک کاربر با مجوز را به اجرای یک برنامه خاص مجبور می کند. رایجترین روش برای چنین حمله ای استفاده از یک ویروس در یک پست الکترونیکی می باشد.
- پیکربندی ضعیف سیستم – یک هکر می تواند خطاهای پیکربندی سیستم را در سرویسها و / یا شماره های حساب موجود مورد سوء استفاده قرار دهد.

مقاوم سازی سیستم ها در برابر حملات

هنگام مقاوم سازی میزبانها،لیست زیر را در نظر داشته باشید:

۱- تمامی سرویسهای غیر ضروری را غیر فعال سازید.
۲- شماره های حساب و گروههای غیر ضروری را حذف کنید. کلمه های رمز را تغییر دهید . اشتراکهایی را که به وارد شدن به سیستم بصورت محاوره ای نیاز ندارند را غیر فعال سازید.
۳- مابقی سرویسها را برای افزایش امنیت مجدداً پیکربندی کنید.
٤- تمامی عملیات مدیریتی را ایمن سازید.
۵- از کلمه های رمز قوی استفاده کنید.

حفاظت از شبکه در برابر ویروسها

اگرچه اکثر محصولات نرم افزاری در بازار مفید، سازنده و سودمند می باشد، نرم افزارهایی وجود دارند که اهداف بدی را در بر دارند – ویروس کامپیوتری چنین نرم افزارهایی جهت وارد شدن به یک شبکه بدون دانش کاربر طراحی شده اند که غالباً در برنامه های معمولی یا حتی پیامهای پست الکترونیکی پنهان می شوند. ویروسها توابع خود را بدون دریافت مجوز از کاربر اجرا می کنند. در ماهیت یک ویروس کامپیوتری قطعه ای کد قابل اجرا استکه بطور مخفیانه اجرا می شود و می تواند خود را در سایر برنامه ها شبیه سازی کند.
شبکه ها با تمامی رفتارهای عملیاتی LAN ها باید به اینترنت نیز دسترسی داشته باشند که این خود حمله ویروسهای کامپیوتری را بسیار آسان می کند.

مفاهیم ویروس

یک ویروس در واقع فقط یکی از انواع بسیار زیاد نرم افزارهای مخرب است. انواع زیادی از نرم افزارهای مخرب شناسایی شده اند. هر یک از نرم افزارهای مخرب حالت عملیاتی متفاوت دارند.

خطاهای نرم افزاری

یک خطای نرم افزاری اساساً یک خطای کدنویسی در برنامه است که انجام عملیات غلط را در بردارد. خطاهای نرم افزاری بندرت عمدی می باشند و در اکثر سیستم های اصلی و جدی این خطاهای نرم افزاری توسط توسعه دهندگان در مراحل تست alpha و beta رفع می شوند.

اسبهای تروا

یک برنامه مخربی است که در یک برنامه مفید مانند کلمه پرداز یا برنامه گرافیکی پنهان می شود. برنامه تا فعال شدن قسمت مخرب بخوبی عمل می کند و با شدن قسمت مخرب ماهیت اصلی برنامه مشخص می شود.

بمب‌های نرم افزاری(Software Bombs)

بمب های نرم افزاری با راه اندازی برنامه آلوده اجرا می شود. بمب‌های نرم افزاری بسیار ساده می باشند. بنابراین، توسعه یک بمب نرم افزاری سریع و آسان است و جستجو برای اینگونه نر افزارها از طریق ابزارهای ویروس یاب آسانتر می باشد.

بمب‌های منطقی(Logic Bombs)

در حالیکه بمب نرم افزاری برای تخریب سریع و غیر انتخابی استفاده میشود یک بمب منطقی با برقرار شدن یک شرط خاص اجرا می شود.

بمب‌های ساعتی(Time Bombs)

بجای فعال نمودن یک بمب نرم افزاری یا از طریق شرایط وضعیت سیستم، یک بمب ساعتی از زمان یا شروط تکراری استفاده می کند.

تکرارکننده ها(Replicators)

هدف یک تکرارکننده بکارگیری منابع سیستم است. تکرارکننده اینکار را با شبیه سازی خود انجام می دهد. هر یک از کپی های شبیه سازی شده بوسیله نسل قبل خود ایجاد می شوند. تکرار کننده ها سیستم را فلج می کنند. بدلیل اینکه این نوع نرم افزار مخرب خود را شبیه سازی می کند، یافتن آن از طریق ابزار ویروس یاب آسان می باشد.

کرم ها(worms)

کرم یکی از اولین نرم افزارهای مخرب شناخته شده است که شبکه های کامپیوتر ار مورد حمل قرار داد. کرم از یک کامپوتر به کامپیوتر دیگری حرکت می کند و معمولاً صدمه جدی وارد نمی کند کرم ها جهت حرکت در شبکه خود را تکرار می کنند و هر گونه نشانی از حضور خود را حذف می کنند. بدلیل اینکه کرم ها خاص یک وضعیت طراحی می شود، یافتن آنها مشکل است مگر اینکه کرم شناخته شده باشد.

ویروسها(viruses)

ویروس رایجترین و پویا ترین نوع نرم افزار مخرب می باشد. یک ویروس جهت افزودن کد مخرب قابل اجرا سایر برنامه ها را تغییر می دهد. ویروسها تاریخ، ساعت، اندازه فایل، خصایص فایل را تغییر نمی دهند. در نتیجه شناسایی و حذف ویروسها بسیار مشکل است.

انواع ویروس‌ها

- ویروس‌های Boot-Sector
- ویروس‌های File Infection
- ویروس‌های polymorphic encryption mutating stealth
- ویروس‌های Macro
- ویروس‌های Java و ActiveX

نرم افزارهای ویروس‌یاب

نرم افزارهای ویروس‌یاب امروزی بیش از یک برنامه خدماتی ساده مبتنی بر خط فرمان می باشند. نرم افزارهای ویروس یاب مدرن در واقع ترکیبی از ابزارهای مرتبط با یکدیگر می باشند که هر ابزار هدف خاصی را بر روی سیستم سرویس‌دهی می کند.

انواع آن عبارتند از:

- Symantec System Center
- Norton Antivirus Corporate Edition
- Live Update Administratoration Utility
- Central Quarantine
- Importer Tool
- ACL Fix Tool

جستجوی ویروس(scanning)

البته بهترین نرم افزار ویروس یاب کار مفیدی انجام نخواهد داد مگر اینکه برای یافتن ویروسها و حفاظت از شبکه پیکربندی شده باشد. ابزارهای ویروس یاب مدرن امکان اجرای چندین نوع جستجو را در حالتهای معمولی و طبق نیاز فراهم می سازند.

- Virus Sweeps : این ویژگی امکان بازرسی تمامی درایوهای بر روی سرورها و سرویس گیرنده های متعلق به شیء انتخاب شده را فارهم می سازد – معمولاً یک گروه از سیستم های بر روی شبکه

که تعریف نموده اید !! این ویژگی نتایج جستجو را در رابطه با محدوه های بزرگ شبکه فراهم می سازد.

- Manual Scans : جهت بازرسی پوشه ها و درایوهای انتخاب شده بر روی کامپیوترهای انتخاب شده از این ویژگی استفاده کنید. جستجوهای بطور دستی نتایج سریع یک جستجو بر روی محدوده های بزرگ شبکه یا یک درایو دیسک سخت محلی را فراهم می سازند و خصوصاً برای تست کامپیوترهای شخصی خاص و بدون ایجاد مزاحمت برای مابقی شبکه مفید می‌باشد.
- Scheduled Scans : این ویژگی امکان بازرسی پوشه های انتخاب شده بر رنوی کامپیوترهای انتخاب شده را در زمانبندیهای ازقبل مشخص شده فراهم می کند این نوع جستجو برای محدوده های بزرگ شبکه ایده آل است زیرا می توانید جستجوها را در خلال ساعات تعطیلی یا ساعاتی که ترافیک شبکه پایین است انجام دهید.
- Real time Scans : این جستجوها فایل ها را همزمان با خواندن از یا نوشتن به یک سرور یا سرویس گیرنده بصورت بلادرنگ وارسی می کنند. نرم افزار Norton Antivirus امکان پیکربندی جستجوی محلی پست الکترونیکی برای کامپیوترهای سرویس گیرنده ۳۲ بیتی را نیز فراهم می‌سازد.
- می توانید با تنظیم جستجوهای دستی، برنامه ریزی شده و بلادرنگ برای پوشه ها و فایلها از طریق Anti-Virus Corporate Edition Client دو نوع دیگر از جستجوها را نیز انتخاب کنید.
- Custom Scans – جستجو بطور دستی را بعداً اجرا می کند.
- Startup Scans – زمانیکه کامپیوتر سرویس گیرنده شروع می شود، یک جستجو را بطور خودکار اجرا می کند.

درک جستجوهای سرور

جستجوهای معمولی سرور خصوصاًمهم می باشند زیرا آلودگی ها بطر سریع می توانند به سرویس گیرنده ها توسعه یابند و یک شبکه را فلج سازند. می توانید یک یا چند سرویس گیرنده Norton Antivirus Corporate Edition را جستجو یا پیکربندی کنید. تعداد سرورهایی را که می توانید جستجو یا پیکربندی نمایید به شیء انتخاب شده بستگی دارد:

- تمامی سرورهای شبکه
- تمامی سرورها در گروههای سرور انتخاب شده
- تمامی سرورها در یک گروه سرور
- تعدادی از سرورها در یک گروه سرور
- یک سرور واحد

درک جستجوهای سرویس گیرنده

جهت جستجو یا پیکربندی یک یا چند کامپیوترهای سرویس گیرنده Antivirus Corporate Edition از نرم افزار مدیریت و ویروس یاب استفاده کنید. درجه پیکربندی به شیء انتخاب شده بستگی دارد:

- تمامی سرویس گیرنده‌های شبکه
- تمامی سرویس گیرنده‌ها در گروههای سرور انتخاب شده
- تمامی سرویس گیرنده‌ها در یک گروه سرور
- تمامی سرویس گیرنده های متصل به یک سرور واحد
- سرویس گیرنده‌های ۳۲ بیت انتخاب شده بر روی سرور مشابه
- یک سرویس گیرنده ۳۲ بیت واحد
- سرویس گیرنده‌های ١٦ بیت

نصب ویروس یاب

نرم افزارهای ویروس یاب مانند Antivirus Internet Security باید بر روی هر یک از کامپیوترهای شخصی نصب شوند. برای کاربران شبکه، ابزارهای ویروس یاب باید بر روی سرورها و سرویس گیرنده ها نصب شوند. پس از اینکه این نرم افزار نصب شد، این نرم افزار ویروس یاب باید بصورت دوره ای بروز رسانیده شود تا ویروسهای جدید و تعاریف و جدیدترین تکنیکهای حذف ویروس را داشته باشد.

نصب بر روی:

- نصب بر روی کامپیوترهای شخصی
- نصب بر روی شبکه

حذف آلودگی

زمانیکه نرم افزار ویروس یاب را نصب می کنید، برنامه تنظیم این نرم افزار عملیات ویروس یابی را جهت تست حافظه و boot sectors دیسک سخت انجام می دهد تا بتواند با اطمینان و بدن ایجاد آلودگی فایلهای خود را بر روی کامپیوترتان کپی کند. اگر این برنامه هیچگونه آلودگی را شناسایی نکند، عملیات نصب را ادامه می دهد و پس از راه اندازی سیستم بصورت کامل سیستم را جستجو می کند.

جلوگیری از آلودگی توسط ویروس

برای محافظت شبکه در برابر ویروس ها باید تدابیری اتخاذ کنید که هم روش کار کاربران و هم پیکربندی کامپیوترها را تحت ضوابطی در بیاورند. همه کاربران باید در مقابل فلاپی دیسک ها و بخصوص فایل های ضمیمه نامه های الکترونیکی محتاطانه عمل کنند. یکی از متداولترین روش هایی که ویروس ها در حال حاضر برای انتشار خود بکار می برند اینست که باعث می شوند کامپیوتر آلوده به ویروس، یک نامه الکترونیکی که دارای ضمیمه ای آلوده می باشد را به همه کاربران موجود در دفترچه آدرس کاربر بفرستد. چون گیرنده ها،فرستنده را می شناسند و به او مطمئن هستند نامه را باز و ضمیمه آنرا اجرا می کنند و به اینصورت کامپیوتر آنها هم آلوده می شود و همین کار هم در کامپیوتر آنها دنبال می شود.

محصولات نرم افزاری ضد ویروس کامپیوترها را در برابر ویروسها و برنامه هی مخرب دیگری که از طریق فلاپی دیسک ها، فایل های دریافت شده از اینترنت و ضمیمه نامه های الکترونیک منتشر می شوند، محافظت می کنند. یک برنامه ضد ویروس نمونه مجهز به روتینی می باشد که زمان روشن شده کامپیوتر، MBR و هر فایلی که مورد دسترسی کامپیوتر قرار می گیرد را چک می کند. برنامه های ضد ویروس کامل تر ضمیمه های نامه های الکترونیکی و فایل هایی که از اینترنت گرفته می شود را بعنوان یک واسطه دریافت می کنند وبعد از بررسی به برنامه کاربردی مربوطه می فرستند.

روش کار برنامه های ضد ویروس به اینصورت است که در فایل ها بدنبال امضای بخصوصی که برای هر ویروس منحصر بفرد می باشد می گردند. این برنامه ها برای شناسایی ویروس ها در خود دارای یک پایگاه اطلاعاتی حاوی اطلاعاتی مربوط به ویروس های قابل شناسایی می باشند.

جلوگیری از ویروسهای ماکرو

ویروسهای ماکرو را می توان از طریق اکثر ابزارهای ویروس یاب موجود امروزی شناسایی نمود، اما شاید بتوانید ریسک آلودگی از طریق ویروسهای ماکرو،را با استفاده از نکات زیر کاهش دهید:

- فایل NORMAL.DOT را به یک فایل فقط خواندنی تغییر دهید. انجام اینکار فایل NORMAL.DOT را در برابر آلودگی ایمن می‌سازد.
- از work ۷.۰۹ یا جدیدتر شرکت مایکروسافت استفاده می نمایید. این ویرایشها با باز نمودن فایلهای مورد نظر که حاوی ماکروها یا اطلاعات سفارشی سازی می باشند، یک کادر Alter بنمایش می گذراند. شاید بتوانید قبل از عملیاتی شدن ماکروهای ناشناخته آنها ار غیر فعال سازید.

حذف یک ویروس ماکرو

جهت حذف ویروس ماکرو از یک فایل و بازیافت متن فایل، عملیات زیر را انجام دهید:

۱ – File Or Folders ,Find, Start را انتخاب کنید. کادر مکالمه find ظاهر می شود.
۲- NORMAL.DOT را تایپ کنید و find now را کلیک نمایید.
۳- پس از اینکه فایل پیدا شد نام فایل را با کلید راست ماوس کلیک کنید و از منـوی میـانبر، ورودی Rename را کلیک نمایید.
٤- فایل را به NORMAL.DOT تغییر نام دهید و کلید Enter را فشار دهید.
٥- کادر مکالمه Find را ببندید.
٦- word مایکروسافت را شروع کنید انجام اینکار الگوی NORMAL.DOT را مجدداً ایجاد می کند.
۷- File،open را انتخاب کنید.
۸- پوشه ای را که حاوی فایل آلوده است پیدا کنید و آنرا انتخاب نمایید.
۹- کلید SHIFT را نگهدارید و Open را کلیک کنید تا فایل آلوده در word مایکروسافت باز شود.
۱۰- Macros،Macro،Tools را انتخاب کنید.
۱۱- در کادر لیست Macros In ، ورودی All active templates and document را برگزینید.
۱۲- ماکروی آلوده را انتخاب کنید و delete را کلیک نمایید. Yes را جهت تأیید کلیک نمایید.
۱۳- مرحل قبل را برای تمامی ماکروهای آلوده تکرار نمایید.
۱٤- close را کلیک نمایید.
۱٥- Select All،Edit را برگزینید.
۱٦- جهت غیر فعال نمودن آخرین علامت پاراگراف در فایل، SHIFT – LEFT ARROWرا فشار دهید.
۱۷- copy،Edit را برگزینید.
۱۸- NEW،File را انتخاب نمایید الگوی مورد نظر را برگزینید و OK را کلیک نمایید.
۱۹- paste،Edit را انتخاب نمایید.
۲۰- جهت وارسی اینکه ماکروهای آلوده مجدداً تکرار نشده اند، مراحل ۱۰ تا ۱٤ را بازبینی کنید.
۲۱- فایل را ذخیره سازید.
۲۲- این مراحل را برای فایلهایی که احتمالاً یک ویروس ماکرو دارند تکرار نمایید.

منابع:

- شبکه‌های کامپیوتری،مؤلف آندرو اس.تنن لام،مترجمان:دکتر پدرام،مهندس علیرضا زارع‌پور،مهندس احسان ملکیان،چاپ اول پائیز۸۲،چاپ دوم زمستان۸۲، چاپ سوم پائیز ۸۳، انتشارات وزارت فرهنگ و ارشاد اسلامی

- Networking certification،مترجم :مهندس شهرام سبحانی، ناشر انتشارات گلپونه، چاپ دوم ۱۳۸٤

- مرجع کامل شبکه‌ها، مترجم مهندس محمد حسن محدوی، انتشارات نشرهزاره،چاپ اول بهار ۱۳۸۲،نشر و پخش آیلار

- راهنمای جامع پیترنورتن برای استفاده از شبکه،مترجم محمد حسن

- مهدوی، انتشارات ناقوس، چاپ اول ۱۳۷۹، چاپ دوم زمستان ۱۳۸۰

- ویلیام استالینگ، مترجم محمد مهدوی سالخورده حقیقی،انتشارات باغات،چاپ سروش، چاپ اول ۱۳۸۳