امنیت شبکه هاي کامپیوتري

شهره لیثی بهرمانی

مهمترين ركن برپائي يک شبکه پس از پيکربندي صحيح سخت افزاري مساله تضمين امنيت شبکه است. اين مساله در محورهاي زيز بررسي شده است:

- کليات امنيت شبکه کامپيوتری
- امنيت شبکه های بی سيم
- آشنايی با فايروال

کليات امنيت شبکه کامپيوتري

حفاظت، پشتيباني و نگهداري از داده‌هاي رايانه‌اي، اطلاعات مهم، برنامه‌هاي حساس، نرم‌افزارهاي مورد نياز و يا هر آنچه که در حافظه جانبي رايانه مورد توجه بوده و با اهميت مي‌باشد، امنيت رايانه‌اي ناميده مي‌شود. تفکر امنيت در شبکه برای دستيابی به سه عامل مهم است که با يک ديگر مثلث امنيتی را تشکيل می دهند. اين عوامل عبارتند از راز داری و امانت داری(Confidentiality) ، يکپارچگی (Integrity)و در نهايت در دسترس بودن هميشگی .(Availability) اين سه عامل (CIA) اصول اساسی امنيت اطلاعات - در شبکه و يا بيرون آن - را تشکيل می دهند بگونه ای که تمامی تمهيدات لازمی که برای امنيت شبکه اتخاذ ميشود و يا تجهيزاتی که ساخته می شوند، همگی ناشی از نياز به اعمال اين سه پارامتر در محيط های نگهداری و تبادل اطلاعات است.

Confidentiality

به معنای آن است که اطلاعات فقط در دسترس کسانی قرار گيرد که به آن نياز دارند و اينگونه تعريف شده است. بعنوان مثال از دست دادن اين خصيصه امنيتی معادل است با بيرون رفتن قسمتی از پرونده محرمانه يک شرکت و امکان دسترسی به آن توسط مطبوعات.

Integrity

بيشتر مفهومی است که به علوم سيستمی باز می گردد و بطور خلاصه می توان آنرا اينگونه تعريف کرد:
-تغييرات در اطلاعات فقط بايد توسط افراد يا پروسه های مشخص و مجاز انجام گيرد.
-تغييرات بدون اجازه و بدون دليل حتی توسط افراد يا پروسه های مجاز نبايد صورت بگيرد .
-يکپارچگی اطلاعات بايد در درون و بيرون سيستم حفظ شود. به اين معنی که يک داده مشخص چه در درون سيستم و چه در خارج آن بايد يکسان باشد و اگر تغيير می کند بايد همزمان درون و برون سيستم از آن آگاه شوند.

Availability

اين پارامتر ضمانت می کند که يک سيستم - مثلا اطلاعاتی - همواره بايد در دسترس باشد و بتواند کار خود را انجام دهد. بنابراين حتی اگر همه موارد ايمنی مد نظر باشد اما عواملی باعث خوابيدن سيستم شوند - مانند قطع برق - از نظر يک سيستم امنيتی اين سيستم ايمن نيست.

اما جدای از مسائل بالا مفاهيم و پارامترهای ديگری نيز هستند که با وجود آنکه از همين اصول گرفته می شوند برای خود شخصيت جداگانه ای پيدا کرده اند. در اين ميان می توان به مفاهيمی نظير

Identificationبه معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم، Authenticationبه معنی مشخص کردن هویت کاربر، Authorizationبه معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountabilityبه معنی قابلیت حسابرسی از عملکرد سیستم و ... اشاره کرد.

امنیت در يك شبكه به ۲ روش صورت مي پذيرد. ۱- برنامه هاي نرم‌افزاري ۲- قطعه‌هاي سخت‌افزاري. در بهترين حالت از برنامه هاي نرم افزاري و قطعات سخت افزاري بطور همزمان استفاده مي گردد. عموماً برنامه‌هاي نرم‌افزاري شامل برنامه‌هاي ضدمخرب (مخرب‌ها شامل ويروس، كرم‌هاي مهاجم، اسب‌هاي تراوا، مخفي‌شده‌ها و ....) و ديوار آتش مي‌باشد. قطعات سخت‌افزاري نيز عموماً شامل ديوار آتش مي‌شود. اين قطعه‌ها موجب كنترل درگاه‌هاي ورودي و خروجي به رايانه و شناخت كامل از حمله‌كننده‌ها بخصوص نشانه‌هاي خاص مهاجم را ايجاد مي نمايد.

فراموش نكنيم كه شركت مايكروسافت به عنوان عرضه‌كننده سيستم هاي عامل نسل) Windows كه در حال حاضر پرمصرف ترين گروه سيستم‌هاي عامل را تشكيل مي دهد)، به يك برنامه نرم افزاري ديوار آتش بصورت پيش فرض مجهز مي باشد، كه مي‌تواند تا امنيت را هر چند كم، براي كاربران سيستم‌هاي عامل خود فراهم نمايد اما قطعاً اين نرم افزار به تنهايي كفايت امن سازي رايانه را تأمين نمي نمايد. اما در اولين مرحله امن سازي يك شبكه ابتدا بايد سازمان را به يك برنامه ضدمخرب قوي مانندَAntivir, Symantec, Kaspersky, Nod32, BitDefender, Norton, Pandaبا قابليت بروزآوري Mac، مجهز نمود، تا بتواند در مقابل حمله برنامه هاي مخرب واكنش مناسبي ارائه نمايد. برنامه Antivir می تواند يک انتخاب مناسب در اين زمينه باشد. چرا كه اين برنامه قابليت بروزآوري را بطور مداوم دارا مي‌باشد و خود برنامه نيز هر ٦ ماه يكبار ويرايش مي‌گردد تا از موتور جستجوگر قوي تر و بهينه‌تري براي يافتن برنامه هاي مخرب بهره گيرد. خريد نسخه اصلي اين نرم‌افزار توصيه مي‌گردد، چرا كه در صورت بروز مشكل شركت اصلي نسبت به پشتيباني از رايانه‌هاي شما اقدام لازم را در اسرع وقت به انجام مي‌رساند.

در مرحله دوم امن سازي يك شبكه بايد از دستگاه تقسيم‌كننده استفاده نمود. دستگاه هاي فوق خود بر دومدل قابل تنظيم و پيكربندي و غيرقابل تنظيم و غير قابل پيكربندي تقسيم مي شوند. ممكن است در گروه اول نيز قطعاتي يافت شود كه تنظيمات جزئي پيكربندي را انجام دهند اما بطور كامل و با تمامي امكاناتي كه در گروه دوم قطعات ديده مي شوند، مجهز نمي‌باشند. عموماً اين دستگاه تقسيم كننده از مدل Core و براي ارتباط سرويس‌دهنده‌هاي مركزي به يكديگر و انجام خدمات به شبكه داخلي يا دنياي اينترنت تهيه مي‌شود و در لايه اصلي تقسيم ارتباط شبكه، از طرف سرويس‌دهنده‌هاي مركزي به سرويس گيرنده هاي داخلي و بالعكس قرار گيرد. اين قطعه مي تواند از تكثير يك برنامه ضدمخرب و همچنين ورود و خروج مهاجمان پنهان، در درون شبكه داخلي از يك رايانه به رايانه ديگر تا حد بسيار زيادي جلوگيري نمايد. اما اگر تعداد كاربران و سرويس‌گيرنده‌هاي يك سازمان بيش از تعداد درگاههاي خروجي يك تقسيم‌كننده مركزي Core Switch باشد، در اين صورت از تقسيم كننده هاي ديگري كه قابليت پيكربندي را دارا بوده و مقرون به صرفه نيز مي‌باشند، مي‌توان استفاده نمود، تا كنترل ورودي و خروجي هاي هر طبقه يا واحد را بيمه نماييم. در مورد قطعات سخت افزاري تقسيم كننده Cisco Switch گزينه مناسبی مي باشد كه برترين نام جهاني را در اين زمينه به خود اختصاص داده و با بروزآوري قطعات خود و همچنين آموزش متخصصان خود سهم بزرگي در اين بحث ايفا مي نمايد.

در مرحله سوم امن سازي، نياز به خريد برنامه نرم افزاري و يا قطعه سخت افزاري ديوار آتش احساس مي شود. بيشترين تأكيد بر روي قطعه سخت افزاري استوار است زيرا كه از ثبات، قدرت بيشتر و ايرادات كمتري نسبت به نرم افزارهاي مشابه خود برخوردار است. قطعه سخت‌افزاري دژ ايمن مي بايست در مسير ورودي اينترنت به يك سازمان قرار گيرد. دقيقاً همانجايي كه اينترنت غيرامن به يك

سازمان تزريق مي گردد. پيشنهاد ما، قطعه سخت‌افزاري Cisco ASAو يا Astaro Firewall مي باشد. فراموش نشود استفاده از دو دستگاه همزمان موازي قطعاً نياز ارجح هر سازمان مي باشد چرا كه با ايست، و توقف سرويس‌دهي يكي از قطعه‌ها، دستگاه ديگر كنترل ورودي ها و خروجي ها را بدست مي‌گيرد. اما در برنامه نرم‌افزاري نياز به نصب نرم‌افزار بر روي يك سرويس‌دهنده مركزي ديوار آتش بوده كه ورود اينترنت ناامن تنها از مسير اين سرويس‌دهنده مركزي انجام پذيرد. بايد توجه داشت در صورت تهيه قطعه‌هاي سخت‌افزاري خاصي استفاده نمود تا در قبل و بعد از قطعه مسيرياب‌ها قرار گيرد كه در اين صورت بهتر است تا از قطعه هاي Cisco ASA در ديواره داخلي و بعد از قطعه مسيرياب‌ها استفاده نمود.

در مرحله چهارم امن سازي نياز به وجود قطعه سخت‌افزاري ديگري به نام مسيرياب براي شبكه داخلي مي‌باشد كه ضمن قابليت پيكربندي، براي نشان دادن مسير ورودي ها و خروجي ها، اشتراك اينترنت، تنظيم ورودي ها و خروجي هاي ديوار آتشين، و همچنين خروج اطلاعات به شكل اينترنتي از سازمان به رايانه هاي شهري و يا بين شهري از طريق خطوط تلفن و ... استفاده نمود. پيشنهاد ما نيز محصولات شركت معتبر Cisco ميباشد.

در مرحله بعدي امن سازي يك سازمان نياز به وجود دستگاه هاي تنظيم جريان برق و دستگاه هاي پشتيبان جريان برق اضطراري براي ارائه خدمات به صورت تمام وقت، بدون قطعي و تنظيم جريان برق، تمامي قطعه‌هاي سخت افزاري راهبر يك شبكه شامل تقسيم‌كننده‌ها، مسيرياب ها ، سرويس‌دهنده‌هامي باشد. اين سيستم به دليل ايجاد خطرات احتمالي ناشي از قطع جريان برق نظير از بين رفتن اطلاعات در حال ثبت بر روي سرويس‌دهنده ها، تقسيم كننده ها، مسيرياب ها مي‌باشد.

به عنوان آخرين مرحله امن سازي، تهيه از اطلاعات و فايلهاي مورد نياز به صورت پشتيبان از برنامه‌هاي اصلي نرم‌افزاري بر روي يك سرويس‌دهنده پشتيبان ، آخرين لايه امن سازي درون سازماني را تكميل مي نمايد.

امنیت در شبکه های بی سیم

از آنجا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این بخش به «امنیت در شبکه های بی سیم» بپردازیم.

سه روش امنيتي در شبكه هاي بي سيم عبارتند از:

- WEP: Wired Equivalent Privacy

در اين روش از شنود كاربرهايي كه در شبكه مجوز ندارند جلوگيري به عمل مي آيد كه مناسب براي شبكه هاي كوچك بوده زيرا نياز به تنظيمات دستي (KEY)مربوطه در هر Client مي باشد. اساس رمز نگاري WEP بر مبناي الگوريتم RC4 بوسيله RSA مي باشد.

- SSID: Service Set Identifier

شبكه هاي WLAN داراي چندين شبكه محلي مي باشند كه هر كدام آنها داراي يك شناسه (Identifier)يكتا مي باشند اين شناسه ها در چندين Access Point قرار داده مي شوند . هر كاربر براي دسترسي به شبكه مورد نظر بايستي تنظيمات شناسه SSID مربوطه را انجام دهد.

- MAC : Media Access Control

ليستي از MAC آدرس هاي مورد استفاده در يك شبكه به (Access Point) AP مربوطه وارد شده بنابراين تنها كامپيوترهاي داراي اين MAC آدرسها اجازه دسترسي دارند به عبارتي وقتي يك كامپيوتر درخواستي را ارسال مي كند MAC آدرس آن با ليست MAC آدرس مربوطه در AP مقايسه شده و اجازه دسترسي يا عدم دسترسي آن مورد بررسي قرار مي گيرد .اين روش امنيتي مناسب براي شبكه هاي كوچك بوده زيرا در شبكه هاي بزرگ امكان ورود اين آدرسها به AP بسيار مشكل مي باشد.

ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال‌های رادیویی به‌جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای‌باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد.

در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است:

- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌یی را نیز موجب است.
- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.
- اطلاعات حیاتی‌یی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند.
- حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.
- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.
- با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.
- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به‌راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.
- یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن (که در اغلب موارد شبکه‌ی اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه‌ی بی‌سیم عملاً راهی برای دست‌یابی به منابع شبکه‌ی سیمی نیز بیابد.

- در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل‌کرد شبکه نیز وجود دارد.

راه کارهاي افزايش امنيت سيستمها

-بررسی میزان امنیت مورد نیاز کامپیوترها با توجه به اطلاعات ذخیره شده روی آنها، محیطی که در آن قرار گرفته اند، موارد و روشهای استفاده از آنها

-بررسی تنظیمات موجود روی کامپیوترها و تشخیص آسیب پذیریها و سوراخهای امنیتی با استفاده از برنامه های جدید و حرفه ای

-انجام تنظیمات و نصب برنامه های لازم جهت ارتقای امنیت منطقی کامپیوترها پیاده سازی امنیت برای فایلها

-کنترل میزان دسترسی کاربران به فایلها بر اساس موارد زیر: الف- فقط خواندن ب- خواندن و ویرایش ج- خواندن، ویرایش و حذف د- خواندن، ویرایش، حذف و کنترل دسترسی دیگران

-ثبت دسترسی کاربران مورد نظر به فایلهای تعیین شده (برای مثال جهت تشخیص کاربری که فایلهای خاصی را ویرایش می کند) - پیاده سازی رمزگذاری فایلها (Encrypting File System) جهت جلوگیری از دسترسی کاربران دیگر (حتی مدیر شبکه) به آنها

دیواره آتشFirewall

دیواره آتش برای جدا کردن شبکه ها از همدیگر به کار می رود با استفاده از یک Firewall مناسب اهداف زیر محقق می گردد.

-1می توان سیاستها و سرویسهای ارائه شده در شبکه ها را از همدیگر بصورت مجرا نگهداری ، مدیریت و کنترل نمود.

-2انتخاب سرویس های داخلی ارائه شوند به بیرون از شبکه و یا بالعکس

- 3کنترل امنیت و مدیریت دسترسی های کاربران

-4حفاظت از اطلاعات در ماقبل کسانی که قصد نفوذ به شبکه داخلی را دارند.

دیوار آتش سیستمی است که در بین کاربران یک شبکه محلی و شبکه جهانی قرار می‌گیرد و ضمن نظارت بردسترسی‌ها در تمام سطوح ورود و خروج اطلاعات راتحت نظر دارد. در این ساختار هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات را کنترل‌کند موظف است تمام ارتباطات مستقیم شبکه داخلی خود را با دنیای خارج قطع کرده و هرگونه ارتباط خارجی از طریق یک دروازه که دیوارآتش یا فیلتر نام دارد انجام‌شود. بسته‌های TCP و IPقبل از ورود به شبکه یا خروج ازآن ابتدا وارد دیواره آتش می‌شوند تا طبق معیارهای حفاظتی و امنیتی پردازش شوند.

شبکه های با قابلیت بالا جهت ارتباط با اینترنت از سخت افزاری های تخصصی استفاده می نمایند ولی نرم افزارهایی هم به همین منظور تولید شده و روی دستگاه های PC نصب می شود برای اتصال مناسب و امن به اینترنت استفاده از نرم افزار firewall ضروری می باشد. ناگفته نماند که ویندوز XP در نسخه SP2 خود این قابلیت را دارا می باشد و دارای امنیت بسیار بالائی جهت اتصال به شبکه می

باشد . علاوه بر این توصیه می شود که جهت اتصال به شبکه اینترنت علاوه بر استفاده از Firewall ، از نرم افزارهای مناسب ویروس کش و AntiSpy نیز استفاده شود.

انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم ، انجام می دهند، اما روش انجام کار توسط انواع مختلف ، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود.بر این اساس فایروالها را به ۵ گروه تقسیم می کنند.

-1فایروالهای سطح مدار :(Circuit-Level) این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از (TCP را نیز نمی دهند.

-2فایروالهای پروکسی سرور : فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

-3فیلترهای : Nosstateful packet این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد ، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IPو در بعضی موارد با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

-4فیلترهایِ : Stateful Packetاین فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند.این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند.این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای .TCP بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP

را تشخیص دهند و لذا می توانندعاعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

-5فایروالهای شخصی : فایروالهای شخصی ، فایروالهایی هستند که بر روی رایانه های شخصی نصب می شوند.آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

نصب و تنظیم فایروال

-تشخیص و تعیین کامپیوترهایی که نیاز به نصب فایروال روی آنها وجود دارد (مخصوصا سرورها(

-نصب نرم افزار فایروال مناسب روی کامپیوترها جهت جلوگیری از دسترسی های غیر مجاز

-انجام تنظیمات لازم در فایروالهای نصب شده بگونه ای که اختلالی در سرویسها و ارتباطات معمول ایجاد نگردد

-انجام آزمایشات لازم جهت کسب اطمینان از صحت و کارایی فایروال

نرم افزارSunbelt Personal Firewall

قطع ترافیک ورودی و خروجی رایانه: بسیار مناسب برای زمانی که حرکات مشکوک و نا خوشایند بر روی شبکه رخ می دهد. نگارش وقایع: با ثبت تمامی ارتباطات شبکه به شما امکان مرور و پیدا کردن مشکل احتمالی را می دهد. مرور کلی ارتباط ها و آمارگیری از وقایع: آمارگیری دقیق از ارتباطات برقرار شده و پورت های باز توسط نرم افزارهای دیگر و موقعیت بلاک شده ها و زمان های حمله و جلوگیری را نمایش می دهد. به روز رسانی: با بروز شدن نرم افزار آخرین ویرایش و قویترین آن همیشه در دسترس خواهد بود.

منابع

http://www.icrc.ac.ir/content/view/185/201
http://www.ipnetsecurity.com/archives/000019.html
http://www.ircert.com/articles/Firewall.htm
Ict.bzmed.ac.ir
www.ircert.com
Forum.persionnetworks.com