نحوه استفاده از فایروال ویندوز XP

امروزه از اینترنت در ابعاد گسترده و با اهدافی مختلف استفاده بعمل می آید . یکی از نکات قابل توجه اینترنت ، تنوع استفاده کنندگان آن در رده های سنی مختلف و مشاغل گوناگون است. در سالیان اخیر و به موازات رشد چشمگیر استفاده از اینترنت خصوصا" توسط کاربران خانگی ، مشاهده شده است به محض شیوع یک ویروس و یا کرم جدید ، اغلب قربانیان را کاربرانی تشکیل می دهند که فاقد مهارت های لازم در جهت استفاده ایمن از اینترنت بوده و دارای یک سطح حفاظتی مناسب نمی باشند . کاربران اینترنت همواره در تیررس مهاجمان بوده و همیشه امکان بروز حملات وجود خواهد داشت .

برای استفاده ایمن از اینترنت ، می بایست اقدامات متعددی را انجام داد . قطعا" استفاده از فایروال یکی از اقدامات اولیه و در عین حال بسیار مهم در این زمینه است . استفاده از اینترنت بدون بکارگیری یک فایروال ، نظیر بازنگهداشتن درب ورودی یک ساختمان است که هر لحظه ممکن است افراد غیرمجاز از فرصت ایجاد شده برای ورود به ساختمان استفاده نمایند . با نصب و استفاده از یک فایروال ، ضریب مقاومت و ایمنی کاربران در مقابل انواع حملات افزایش خواهد یافت .

شرکت مایکروسافت اخیرا Service Pack 2 "ویندوز XP را عرضه نموده است (نسخه های Professional و Home یکی از ویژگی های مهمSP2 ، نصب پیش فرض یک فایروال است) .

فایروال ویندوز XP که از آن با نام Internet Connection Firewall (ICF) نیز یاد می گردد به صورت پیش فرض ، فعال می گردد. پس از فعال شدن فایروال ، شاهد بروز تغییراتی گسترده در رابطه با عملکرد ویندوز بوده و ممکن است برخی برنامه ها ، ابزارها و یا سرویس ها در زمان اجراء با مشکلاتی مواجه گردند (بلاک شدن برخی از پورت های استفاده شده توسط برنامه ها و یا سایر ابزارهای کاربردی .

در این مطلب قصد داریم به بررسی نحوه استفاده از فایروال ویندوز XP پرداخته و به برخی از سوالات متداول در این زمینه پاسخ دهیم . احازه دهید قبل از هر چیز با فایروال ها و جایگاه آنان در استفاده ایمن از شبکه های کامپیوتری (اینترانت ، اینترنت) بیشتر آشنا شویم .

فایروال چیست ؟

فایروال یک برنامه و یا دستگاه سخت افزاری است که با تمرکز بر روی شبکه و اتصال اینترنت ، تسهیلات لازم در جهت عدم دستیابی کاربران غیرمجاز به شبکه و یا کامپیوتر شما را ارائه می نماید. فایروال ها این اطمینان را ایجاد می نمایند که صرفا" پورت های ضروری برای کاربران و یا سایر برنامه های موجود در خارج از شبکه در دسترس و قابل استفاده می باشد. به منظور افزایش ایمنی ، سایر پورت ها غیرفعال می گردد تا امکان سوء استفاده از آنان توسط مهاجمان وجود نداشته باشد . در برخی موارد و با توجه به نیاز یک برنامه می توان موقتا" تعدادی از پورت ها را فعال و پس از اتمام کار مجددا" آنان را غیرفعال نمود . بخاطر داشته باشید که به موازات افزایش تعداد پورت های فعال ، امنیت کاهش پیدا می نماید .

فایروال های نرم افزاری ، برنامه هائی هستند که پس از اجراء ، تمامی ترافیک به درون کامپیوتر را کنترل می نمایند(برخی از فایروال ها علاوه بر کنترل ترافیک ورودی ، ترافیک خروجی را نیز کنترل می نمایند) . فایروال ارائه شده به همراه ویندوز XP ، نمونه ای در این زمینه است . فایروال های نرم افزاری توسط شرکت های متعددی تاکنون طراحی و پیاده سازی شده است . تعداد زیادی از اینگونه فایروال ها، صرفا" نظاره گر ترافیک بین شبکه داخلی و اینترنت بوده و ترافیک بین کامپیوترهای موجود در یک شبکه داخلی را کنترل نمی نمایند .

ضرورت استفاده از فایروال

یک سیستم بدون وجود یک فایروال ، در مقابل مجموعه ای گسترده از برنامه های مخرب آسیب پذیر است و در برخی موارد صرفا" پس از گذشت چندین دقیقه از اتصال به اینترنت ، آلوده خواهد شد . در صورتی که تدابیر و مراقبت لازم در خصوص حفاظت از سیستم انجام نگردد ، ممکن است کامپیوتر شما توسط برنامه هائی که به صورت تصادفی آدرس های اینترنت را پویش می نمایند ، شناسائی شده و با استفاده از پورت های فعال اقدام به تخریب و یا سوء استفاده از اطلاعات گردد .

بخاطر داشته باشید با این که استفاده از فایروال ها به عنوان یک عنصر حیاتی در ایمن سازی محیط های عملیاتی مطرح می باشند ولی تمامی داستان ایمن سازی به این عنصر ختم نمی شود و می بایست از سایر امکانات و یا سیاست های امنیتی خاصی نیز تبعیت گردد . باز نکردن فایل های ضمیمه همراه یک Email قبل از حصول اطمینان از سالم بودن آنان ، پیشگیری از برنامه های جاسوسی معروف به Spyware و یا نصب برنامه های Plug-ins که با طرح یک پرسش از شما مجوز نصب را دریافت خواهند داشت ، نمونه هائی از سایر اقدامات لازم در این زمینه است .

فایروال ها قادر به غیرفعال نمودن ویروس ها و کرم های موجود بر روی سیستم نبوده و همچنین نمی توانند نامه های الکترونیکی مخرب به همراه ضمائم آلوده را شناسائی و بلاک نمایند . به منظور افزایش ضریب ایمنی و مقاومت در مقابل انواع حملات ، می بایست اقدامات متعدد دیگری صورت پذیرد :

نصب و بهنگام نگهداشتن یک برنامه آنتی ویروس

استفاده از ویندوز Upadate برطرف نمودن نقاط آسیب پذیر ویندوز و سرویس های مربوطه

استفاده از برنامه های تشخیص Spyware

نصب Plug-ins از سایت های تائید شده

نحوه فعال نمودن فایروال در ویندوز XP

در صورت نصب SP2 ویندوز XP ، فایروال به صورت پیش فرض فعال می گردد . برخی از مدیران شبکه و یا افرادی که اقدام به نصب نرم افزار می نمایند ، ممکن است آن را غیرفعال کرده باشند .

برای آگاهی از وضعیت فایروال از پنجره Security Center استفاده می شود . بدین منظور مراحل زیر را دنبال می نمائیم

Start | Control Panel | Security Center

انتخاب گزینه Recommendations در صورت غیرفعال بودن فایروال

انتخاب گزینه Enable Now به منظور فعال نمودن فایروال

در صورتی که ویندوز XP بر روی سیستم نصب شده است ولی SP2 هنوز نصب نشده باشد ، پیشنهاد می گردد که در اولین فرصت نسبت به نصب SP2 ویندوز XP ، اقدام شود (استفاده از امکانات گسترده امنیتی و فایروال ارائه شده.

نسخه های قبلی ویندوز نظیر ویندوز ۲۰۰۰ و یا ۹۸ به همراه یک فایروال از قبل تعبیه شده ارائه نشده اند . در صورت استفاده از سیستم های عامل فوق، می بایست یک فایروال نرم افزاری دیگر را انتخاب و آن را بر روی سیستم نصب نمود.

ضرورت توجه به امکانات سایر فایروال های نرم افزاری

فایروال ویندوز ، امکانات حفاظتی لازم به منظور بلاک نمودن دستیابی غیرمجاز به سیستم شما را ارائه می نماید . در این رابطه دستیابی به سیستم از طریق کاربران و یا برنامه های موجود در خارج از شبکه محلی ، کنترل خواهد شد . برخی از فایروال های نرم افزاری یک لایه حفاظتی اضافه را نیز ارائه داده و امکان ارسال اطلاعات و یا داده توسط کامپیوتر شما به سایر کامپیوترهای موجود در شبکه توسط برنامه های غیر مجاز را نیز بلاک می نمایند (سازماندهی و مدیریت یک فایروال دوطرفه) . با استفاده از این نوع فایروال ها ، برنامه ها قادر به ارسال داده از کامپیوتر شما برای سایر کامپیوترها بدون اخذ مجوز نخواهند بود . در صورت نصب یک برنامه مخرب بر روی کامپیوتر شما (سهوا" و یا تعمدا") برنامه فوق می تواند در ادامه اطلاعات شخصی شما را برای سایر کامپیوترها ارسال و یا آنان را سرقت نماید . پس از نصب فایروال های دوطرفه ، علاوه بر تمرکز بر روی پورت های ورودی (Incoming)، پورت های خروجی (Outgoing) نیز کنترل خواهند شد .

آیا می توان بیش از یک فایروال نرم افزاری را بر روی یک سیستم نصب نمود ؟

پاسخ به سوال فوق مثبت است ولی ضرورتی به انجام این کار نخواهد بود. فایروال ویندوز بگونه ای طراحی شده است که می تواند با سایر فایروال های نرم افزارهای همزیستی مسالمت آمیزی را داشته باشد ولی مزیت خاصی در خصوص اجرای چندین فایروال نرم افزاری بر روی یک کامپیوتر وجود ندارد . در صورت استفاده از یک فایروال نرم افزاری دیگر ، می توان فایروال ویندوز XP را غیر فعال نمود .

در صورتی که بر روی شبکه از یک فایروال استفاده می گردد ، آیا ضرورتی به استفاده از فایروال ویندوز وجود دارد ؟

در صورت وجود بیش از یک کامپیوتر در شبکه ، پیشنهاد می گردد که حتی در صورتی که از یک فایروال سخت افزاری استفاده می شود ، از فایروال ویندوز XP نیز استفاده بعمل آید . فایروال های سخت افزاری عموما" ترافیک بین شبکه و اینترنت را کنترل نموده و نظارت خاصی بر روی ترافیک بین کامپیوترهای موجود در شبکه را انجام نخواهند داد . در صورت وجود یک برنامه مخرب بر روی یکی از کامپیوترهای موجود در شبکه ، شرایط و یا پتانسیل لارم برای گسترش و آلودگی سایر کامپیوترها فراهم می گردد. فایروال ویندوز XP علاوه بر حفاظت کامپیوتر شما در خصوص دستیابی غیرمجاز از طریق اینترنت ، نظارت و کنترل لازم در رابطه با دستیابی غیرمجاز توسط کامپیوترهای موجود در یک شبکه داخلی را نیز انجام خواهد داد .

فایروال بر روی چه برنامه هائی تاثیر می گذارد ؟

فایروال ویندوز با هر برنامه ای که تصمیم به ارسال داده برای سایر کامپیوترهای موجود در شبکه داخلی و یا اینترنت را داشته باشد ، تعامل خواهد داشت . پس از نصب فایروال ، صرفا" پورت های مورد نیاز برنامه های متداول مبادله اطلاعات نظیر Email و استفاده از وب، فعال می گردند . در این راستا و به منظور حفاظت کاربران ، امکان استفاده از برخی برنامه ها بلاک می گردد . سرویس FTP سرویس ارسال و یا دریافت فایل) ، بازی های چند نفره ، تنظیم از راه دور Desktop و ویژگی های پیشرفته ای نظیر کنفرانس های ویدئویی و ارسال فایل از طریق برنامه های Instant Messaging (IM) ، از جمله برنامه هائی می باشند که فعالیت آنان توسط فایروال بلاک می گردد . در صورت ضرورت می توان پیکربندی فایروال را بگونه ای انجام داد که پورت های مورد نیاز یک برنامه فعال تا امکان مبادله اطلاعات برای برنامه متقاضی فراهم گردد .

چگونه می توان فایروال را برای یک برنامه خاص فعال نمود ؟

در صورتی که فایروال ویندوز فعال شده باشد ، اولین مرتبه ای که یک برنامه درخواست اطلاعات از سایر کامپیوترهای موجود در شبکه (داخلی و یا اینترنت) را می نماید ، یک جعبه محاوره ای حاوی یک پیام هشداردهنده امنیتی فعال و از شما سوال خواهد شد که آیا به برنامه متقاضی اجازه مبادله اطلاعات با سایر برنامه ها و یا کامپیوترهای موجود در شبکه داده می شود و یا دستیابی وی بلاک می گردد . در این جعبه محاوره ای پس از نمایش نام برنامه متقاضی با ارائه سه گزینه متفاوت از شما در رابطه با ادامه کار تعیین تکلیف می گردد :

Keep Blocking : با انتخاب این گزینه به برنامه متقاضی اجازه دریافت اطلاعات داده نخواهد شد .

Unblock : پس از انتخاب این گزینه پورت و یا پورت های مورد نیاز برنامه متقاضی فعال و امکان ارتباط با کامپیوتر مورد نظر فراهم می گردد . بدیهی است صدور مجوز برای باز نمودن پورت های مورد نیاز یک برنامه به شناخت مناسب نسبت به برنامه و نوع عملیات آن بستگی خواهد داشت . در صورتی که از طریق نام برنامه نمی توان با نوع فعالیت آن آشنا گردید ، می توان از مراکز جستجو برای آشنائی با عملکرد برنامه متقاضی ، استفاده نمود .

Ask Me Later : با انتخاب گزینه فوق در مقطع فعلی تصمیم به بلاک نمودن درخواست برنامه متقاضی می گردد.در صورت اجرای برنامه ، سوال فوق مجددا" مطرح خواهد شد .

در صورتی که یک برنامه بلاک شده است ولی بدلایلی تصمیم به فعال نمودن و ایجاد شرایط لازم ارتباطی برای آن را داشته باشیم ، می توان به صورت دستی آن را به لیست موسوم به Exception اضافه نمود . لیست فوق حاوی نام برنامه هائی است که به آنان مجوز لازم به منظور فعال نمودن ارتباطات شبکه ای اعطاء شده است. برای انجام این کار می توان مراحل زیر را دنبال نمود :

Start | Control Panel | Security Center

کلیک بر روی Windows Firewall از طریق Manage security settings for

انتخاب Add Program از طریق Exceptions

انتخاب برنامه مورد نظر (از طریق لیست و یا Browse نمودن

پس از انجام عملیات فوق ، می بایست نام برنامه مورد نظر در لیست Exception مشاهده گردد. در صورتی که قصد بلاک نمودن موقت فعالیت ارتباطی یک برنامه را داشته باشیم،می توان از Cehckbox موجود در مجاورت نام برنامه استفاده نمود . برای حذف دائم یک برنامه موجود در لیست Exception ، می توان از دکمه Delete استفاده نمود .

کاربرانی که دارای اطلاعات مناسب در رابطه با پورت های مورد نیاز یک برنامه می باشند ، می توانند با استفاده از Add Port ، اقدام به معرفی و فعال نمودن پورت های مورد نیاز یک برنامه نمایند . پس از فعال نمودن پورت ها ، وضعیت آنان صرفنظر از فعال بودن و یا غیرفعال بودن برنامه و یا برنامه های متقاضی ، باز باقی خواهند ماند . بنابراین در زمان استفاده از ویژگی فوق می بایست دقت لازم را انجام داد . اغلب از ویژگی فوق در مواردی که پس از اضافه نمودن یک برنامه به لیستException همچنان امکان ارتباط آن با سایر کامپیوتر و یا برنامه های موجود در شبکه وجود نداشته باشد، استفاده می گردد.

آیا فایروال با بازی های اینترنتی کار می کند ؟

پاسخ به سوال فوق مثبت است و فایروال ویندوز قادر به باز نمودن پورت های ضروری برای بازی های اینترنت و یا شبکه محلی است . در این رابطه یک حالت خاص وجود دارد که ممکن است برای کاربران ایجاد مشکل نماید. در برخی موارد ممکن است پیام هشداردهنده امنیتی که از شما به منظور ارتباط با سایر برنامه ها تعیین تکلیف می گردد ، بر روی صفحه نمایشگر نشان داده نمی شود . همانگونه که اطلاع دارید اکثر بازی های کامپیوتری به منظور نمایش تصاویر سه بعدی بر روی نمایشگر و استفاده از تمامی ظرفیت های نمایش ، از تکنولوژی DirectX استفاده می نمایند . با توجه به این موضوع که پس از اجرای یک بازی ، کنترل نمایش و خروجی بر روی نمایشگر بر عهده بازی مورد نظر قرار می گیرد ، امکان مشاهده پیام هشداردهنده امنیتی وجود نخواهد داشت . (در واقع پیام پشت صفحه بازی مخفی شده است) . بدیهی است با عدم پاسخ مناسب به پیام

هشداردهنده ، فایروال ویندوز امکان دستیابی شما به شبکه بازی را بلاک خواهد کرد . در صورت برخورد با چنین شرایطی در اکثر موارد با نگه داشتن کلید ALT و فشردن دکمه TAB می توان به Desktop ویندوز سوئیچ و پیام ارائه شده را مشاهده و پاسخ و یا واکنش مناسب را انجام داد . پس از پاسخ به سوال مربوطه می توان با فشردن کلیدهای ALT+TAB مجددا" به برنامه مورد نظر سوئیچ نمود .

تمامی بازی های کامپیوتری از کلیدهای ALT+TAB حمایت نمی نمایند . در چنین مواردی و به عنوان یک راهکار منطقی دیگر، می توان اقدام به اضافه نمودن دستی بازی مورد نظر به لیست Exception نمود (قبل از اجرای بازی) .

چرا با این که نام یک برنامه به لیست Exception اضافه شده است ولی همچنان امکان ارتباط صحیح وجود ندارد ؟ علت این امر چیست و چه اقداماتی می بایست انجام داد ؟

در صورت استفاده از یک فایروال سخت افزاری ، می بایست پورت های مورد نیاز یک برنامه بر روی آن نیز فعال گردند . فرآیند نحوه فعال نمودن پورت بر روی فایروال های سخت افزاری متفاوت بوده و به نوع آنان بستگی دارد . مثلا" در اکثر روترهائی که از آنان در شبکه های موجود در منازل استفاده می شود ، می توان با استفاده از یک صفحه وب پارامترهای مورد نظر (نظیر پورت های فعال) را تنظیم نمود . در صورتی که پس از بازنمودن پورت های مورد نیاز یک برنامه مشکل همچنان وجود داشته باشد ، می توان برای کسب آگاهی بیشتر به سایت پشتیبانی مایکروسافت مراجعه نمود .

آیا باز نمودن پورت های فایروال خطرناک است ؟

با باز نمودن هر پورت ، کامپیوتر شما در معرض تهدیدات بیشتری قرار خواهد گرفت . علیرغم باز نمودن برخی پورت ها به منظور بازی و یا اجرای یک کنفرانس ویدئویی ، فایروال ویندوز همچنان از سیستم شما در مقابل اغلب حملات محافظت می نماید. پس از معرفی یک برنامه به فایروال ویندوز ، صرفا" در زمان اجرای این برنامه پورت های مورد نیاز فعال و پس از اتمام کار ، مجددا" پورت های استفاده شده غیرفعال می گردند . در صورتی که به صورت دستی اقدام به باز نمودن پورت هائی خاص شده باشد، پورت های فوق همواره باز شده باقی خواهند ماند . به منظور حفظ بهترین شرایط حفاظتی و امنیتی ، می توان پس از استفاده از پورت و یا پورت هائی که با توجه به ضرورت های موجود فعال شده اند ، آنان را مجددا" غیرفعال نمود (استفاده از Exception checkbox موجود در مجاورت برنامه در لیست) .

چگونه می توان صفحه مربوط به نمایش پیام های هشداردهنده امنتی فایروال ویندز را غیرفعال نمود ؟

در صورتی که فایروال ویندز را اجراء نکرده باشید و مرکز امنیت ویندوز (WSC) قادر به تشخیص فایروال استفاده شده بر روی سیستم شما نباشد ، شما همواره یک پیام هشداردهنده امنیتی فایروال را مشاهده خواهید کرد . برای غیرفعال نمودن این چنین پیام هائی می توان مراحل زیر را انجام داد :

Start | Control Panel | Security Center

در بخش Windows Security Center ، بر روی دکمه Recommendation کلیک نمائید . در صورتی که دکمه فوق مشاهده نشود ، فایروال ویندوز فعال است

انتخاب گزینه I have a firewall solution that I'll monitor myself

پس از انجام عملیات فوق ، ویندوز وضعیت فایروال را اعلام نخواهد کرد . رویکرد فوق در مواردی که از یک فایروال سخت افزاری و یا نرم افزاری خاص استفاده می شود ، پیشنهاد می گردد . بدین ترتیب مرکز امنیت ویندوز ، وضعیت فایروال را مانیتور نخواهد کرد .

و اما نکته آخر و شاید هم تکراری !

برای استفاده ایمن از اینترنت ، می بایست اقدامات متعددی را انجام داد . قطعا" استفاده از فایروال یکی از اقدامات اولیه و در عین حال بسیار مهم در این زمینه است . یک سیستم بدون وجود یک فایروال ، در مقابل مجموعه ای گسترده از برنامه های مخرب آسیپ پذیر است و در برخی موارد صرفا" پس از گذشت چندین دقیقه از اتصال به اینترنت ، آلوده خواهد شد . با استفاده از یک فایروال ، ضریب مقاومت و ایمنی کاربران در مقابل انواع حملات افزایش می یابد.

شهره لیثی

دانشگاه امیر کبیر