مقدمه

شبکه های کامپیوتری زیر ساخت لازم برای عرضه اطلاعات در یک سازمان را فراهم می نمایند . بموازات رشد و گسترش تکنولوژی اطلاعات، مقوله امنیت در شبکه های کامپیوتری ، بطور چشمگیری مورد توجه قرار گرفته و همه روزه بر تعداد افرادی که علاقه مند به آشنائی با اصول سیستم های امنیتی در این زمینه می باشند ، افزوده می گردد . در این نوشته ، پیشنهاداتی در رابطه با ایجاد یک محیط ایمن در شبکه ، ارائه می گردد .

" سرویس های عرضه شده در مقابل امنیت ارائه شده ، استفاده ساده در مقابل امنیت و هزینه ایمن

ازی در مقابل ریسک از دست دادن اطلاعات "

1) چرا امنیت؟

جايگاه امنيت در شبكه‌رايانه‌اي كجاست؟ آيا واقعاً نياز به امنيت در شبكه‌هاي رايانه‌اي وجود دارد؟ شبكه رايانه‌اي بايد در مقابل چه مسائلي امن باشد؟ و يك مدير شبكه چه وقت بايد به امنيت در شبكه رايانه‌اي خود بيانديشد. در اين بخش سعي خواهد شد كه به اين سئوالات پاسخ داده شود تا بيشتر با نقش و جايگاه امنيت در شبكه آشنا شويم.

ديرزماني است كه استفاده گسترده از رايانه‌ها در ارتش و تأسيسات دفاعي، به‌كارگيري قوانين و آيين‌نامه‌هاي ويژه‌اي را براي حفظ امنيت در سيستم ضروري

ساخته است. يك اصل اساسي در زمينه امنيت سيستمهاي رايانه‌هاي، قرار دادن كل سيستم در محيطي است كه نفوذپذيري در آن تا حد قابل قبولي كاهش يافته است. افزايش استفاده از سيستمهايي كه اجزاي آنها به طور جغرافيايي گسترده هستند، مشكلات و مسايل جديدي را به ميان آورده است. اين مشكلات با توجه به سيستمهاي حفاظتي مقدماتي قابل پاسخگويي نميباشند. مشكلات امنيتي سيستمهايي كه منابعشان را در اختيار ديگران ميگذارند، به مثابه بهايي است كه افراد براي بهره‌برداري از اين سيستمها ميپردازند. با اين حال، نگاه به اين مساله از اين ديدگاه، مشكلات و بحثهاي جديدي را به ميان مي‌آورد، اول اينكه مشكل امنيت به يك نوع رايانه خاص مربوط نميشود. بلكه اين مساله، كل فن‌آوري رايانه را در بر ميگيرد. دوم اين كه سيستمهايي كه منابعشان را در اختيار ديگران قرار مي‌دهند، بايد به‌گونه‌اي طراحي شوند كه يك كاربر را از مزاحمت ديگران محافظت نمايند. به عبارت ديگر، موظفند نوعي از محافظت را براي كاربراني كه خواهان حفظ درست داده‌ها يا برنامه‌هاي خود هستند، فراهم كنند. بدين ترتيب طراحان و سازندگان چنين سيستمهايي با مشكل اساسي محافظت از اطلاعات روبرو مي‌باشند. در محافظت از اطلاعات طبقه‌بندي شده، سطوح مختلفي وجود دارد؛ اما مباحث پايه‌اي همه سطوح به طور كلي يكسان ميباشد. راه‌حلهايي كه سازندگان در نرم‌افزار و سخت‌افزار طراحي مي‌كنند، بايد بنا به درخواست ماشينهايي كه در يك محيط ايمن عمل مي‌كنند، تصحيح و تكميل شود. در نخستيم گام اين سؤال‌ها مطرح خواهد شد

كه هدف امنيت چيست؟ هدف امنيت فراهم نمودن خدمات زير براي منابع با ارزش ما مي‌باشد.

كنترل دسترسي : منظور كنترل سطوح دسترسي كاربران مي‌باشد.

تائيد هويت : به رسميت شناختن كاربران
محرمانگي : اطلاعات بايد محرمانه باقي بماند.
صحت داده‌ها : اطلاعات بايد از هر تغييري مصون بماند.
عدم انكار : فرستنده و گيرنده نتوانند ارسال و دريافت اطلاعات را انكار كنند.
اما اين سؤال باقي خواهد ماند كه منابع با ارزش چه چيزهايي هستند؟ هنگامي كه صحبت از امنيت مي‌شود، در كنار آن منابع با ارزشي وجود دارد كه هدف حفظ اين منابع مي‌باشد، اين منابع درشبكه رايانه‌اي يك مؤسسه معتبر عبارتند از:

1-1) تجهيزات رايانه‌اي

بديهي است هزينه زيادي صرف تجهيزات رايانه‌اي و شبكه شده است و چنانچه عاملي از بيرون يا داخل باعث صدمه به اين تجهيزات شود، متضمن هزينه زيادي خواهد بود. (بعنوان مثال ويروس چرنوبيل به BIOS رايانه‌ها آسيب جدي وارد مي‌كرد.)

1-2) اطلاعات رايانه‌اي

از بين رفتن و يا صدمه ديدن اطلاعات رايانه‌اي مي‌تواند به مراتب پرهزينه‌تر از تجهيزات رايانه‌اي باشد. اين اطلاعات ممكن است حاصل سالها كار و تلاش يك

مؤسسه باشد و جايگزيني آن مي‌تواند بسيار پر هزينه، وقت‌گير و يا اصلاً غيرممكن باشد.

1-3) اسرار مؤسسه

اسرار و رموز كار يك مؤسسه از گرانبهاترين منابع آن مؤسسه است. در اينجا لازم نيست اطلاعات و يا تجهيزاتي از بين برود و يا صدمه ببيند، بلكه كافي است كه اطلاعات گرانبهايي كه جزء رموز مؤسسه محسوب مي‌شود به دست افراد غير مجاز بيفتد. ضرر و زياني كه از اين طريق متوجه مؤسسه مي‌شود مي‌تواند بسيار زياد باشد. افراد غير مجاز شامل تروريستها، دشمنان برون مرزي و رقباي تجاري نوعاً به دنبال اطلاعاتي از قبيل تعداد كاركنان مؤسسه، نام مديران تصميم‌گيرنده، ميزان سرمايه در گردش، محل نگهداري و چگونگي جابجايي كالاهاي ارزشمند مؤسسه و غيره هستند. اين افراد لازم نيست مستقيماً به اطلاعات مورد نظر دست پيدا كنند، بلكه اطلاعات جانبي ظاهراً بي‌ارزش مي‌تواند به دستيابي آنها به اطلاعات دلخواهشان كمك كند.

1-4) اعتبار مؤسسه

يك مؤسسه ممكن است بدون آنكه هيچيك از تجهيزات آن آسيبي ديده باشد و هيچ يك از اسرار آن فاش شده باشد محتمل خسارات سنگيني شود. مثلاً اگر افرادي بتوانند به نوعي به صورت غير مجاز وارد سيستم رايانه‌اي مؤسسه شوند و به نوعي به همگان نشان دهند كه

موفق به چنين كاري شده اند، حتي اگر هيچ خرابكاري هم نكنند، خسارت زيادي به اعتبار مؤسسه وارد مي‌شود. در اثر آن ممكن است مثلاً برخي از مؤسسات راغب به معامله يا مذاكره با اين مؤسسه نباشند و يا در صورت اهميت مؤسسه در سطح كشور، خسارات اقتصادي و يا سياسي متوجه كل كشور گردد. يا مثلاً اگرWeb site مؤسسه مورد حمله و خرابكاري قرار گيرد و خرابكاران بر روي Home page مؤسسه شعارهاي سياسي، ضد ديني، و يا نوشته‌ها و تصاوير ضد اخلاقي را به معرض نمايش عموم بگذارند، صدمه‌اي كه به اعتبار مؤسسه وارد مي‌شود داراي عواقبي غير قابل پيش‌بيني خواهد بود و بدون ترديد موجب خسارات مادي زيادي نيز مي‌شود.

1-5) نيروي انساني

كاركنان يك مؤسسه از منابع گرانبهاي آن مؤسسه به حساب مي‌آيند. علاوه بر آن وقت اين كاركنان با توجه به حقوق دريافتي و قابليت توليد آنها ارزشمند است. چنانچه خرابي در سيستم رايانه‌اي موجب اتلاف وقت كاركنان شود، علاوه بر اينكه اين كاركنان در ازاي دريافت حقوق كار مفيدي انجام نمي‌دهند، توليد مؤسسه نيز ممكن است تحت تأثير قرار گرفته، موجب خسارات مادي زيادي شود.

1-6) مسئوليت

براي روشن شدن منظور ما از در نظر گرفتن « مسئوليت» به عنوان يك منبع با ارزش كه بايد حفظ شود به اين مثال توجه كنيد. فرض كنيد فردي به صورت غيرمجاز وارد

شبكه رايانه‌اي مؤسسه «الف» شود و از يكي از رايانه‌هاي اين مؤسسه به عنوان پايگاهي براي آسيب رساندن به رايانه‌هاي مؤسسه «ب» استفاده كند. در اين صورت مؤسسه «الف» بايد در مقابل خسارات وارد شده به مؤسسه «ب» جوابگو باشد. حتي اگر مؤسسه «الف» از نظر قانون محكوم شناخته نشود هزينه و دردسر برخورد با اين مسئله مي‌تواند قابل توجه باشد.

حال بايد ببينيم چه كساني ممكن است بخواهند به منابع خدشه وارد سازند. اهداف سياسي گروههاي تروريستي، اهداف اقتصادي شركتهاي رقيب، انگيزه‌هاي شخصي جوانان ماجراجو، مقاصد خرابكارانه كشورهاي بيگانه، انتقامجويي كارمندان اخراجي و همچنين سرقت از سوي تبهكاران را مي‌توان جزو مهمترين انگيزه‌ها براي حمله به شبكه رايانه‌اي مؤسسه دانست. آمار در مورد حملات به شبكه رايانه‌اي هشداردهنده مي‌باشند. در يك آمارگيري كه توسط پليس فدرال آمريكا در اسفند 1379 منتشر شد، نشان مي‌داد كه 85% از 528 مؤسسه مورد آمارگيري، متوجه شكستن حريم امنيتي سيستمهاي رايانه‌اي مؤسسه خود شده‌اند، تهاجماتي كه به شبكه‌هاي رايانه‌اي مي‌شود از سه نوع دستكاري اطلاعات و خرابكاري،دسترسي به اطلاعات محرمانه و ممانعت از كار عادي شبكه يا كامپيوتر مي‌باشد، خوشبختانه براي جلوگيري از اين حملات جاي اميدواري مي‌باشد، زيرا محققين دانشگاهي در آمريكا تخمين مي‌زنند كه 99% از تمامي حملات رايانه‌اي گزارش داده شده ناشي از نقاط ضعف امنيتي سيستمهاي رايانه‌اي مي‌باشد و قابل پيشگيري مي‌باشد.

با توجه به اهميت امنيت، سئوالي كه مطرح مي‌شود اين است كه يك مدير شبكه چه وقت بايد به مسئله امنيت در شبكه رايانه‌اي بيانديشد. اشتباهي كه بسياري از مديران شبكه مي‌كنند اين است كه ابتدا شبكه را راه‌اندازي مي‌كنند و سپس به فكر ايجاد امنيت در آن مي‌افتند. تجربه نشان داده است كه زمان زيادي طول نمي‌كشد تا اينكه افرادي از نقاط ضعف سيستم با اطلاع شوند و سوءاستفاده كنند. برخي از مديران شبكه گزارش داده‌اند كه تنها پس از چند روز و گاهي چند ساعت، پس از وصل‌كردن شبكه خود به اينترنت، افراد غيرمجاز موفق به نفوذ و خرابكاري در آن شده‌اند.
قبل از وصل‌كردن شبكه خود به شبكه جهاني اينترنت بايد آن را ازنظر امنيت بررسي كرد و نقاط ضعف آن را شناخت و برطرف نمود. در ضمن ايجاد امنيت در شبكه كاري نيست كه يكبار انجام شود و براي هميشه كار كند، هر روز روشهاي جديدي كشف مي‌شود كه با استفاده از آن مي‌توان به شبكه نفوذ كرد، لذا بسيار اهميت دارد كه اطلاعات مديران شبكه به روز باشد و همواره آخرين تكنيكهاي امنيتي و آخرين نرم‌افزارهاي تهيه شده در اين زمينه را برروي شبكه‌هاي رايانه‌اي خود اعمال كنند.

2- سیاست امنیتی

یک سیاست امنیتی، اعلامیه ای رسمی مشتمل بر مجموعه ای از قوانین است که می بایست توسط افرادیکه به تکنولوژی سازمان و یا سرمایه های اطلاعاتی دستیابی دارند، رعایت شود . بمنظور تحقق اهداف امنیتی ، می بایست سیاست های تدوین شده در رابطه با تمام کاربران ، مدیران شبکه و مدیران عملیاتی سازمان، اعمال گردد . اهداف مورد نظر عموما" با تاکید بر گزینه های اساسی زیر مشخص می گردند .

مهمترین هدف یک سیاست امنیتی ، دادن آگاهی لازم به کاربران، مدیران شبکه و مدیران عملیاتی یک سازمان در رابطه با امکانات و تجهیزات لازم ، بمنظور حفظ و صیانت از تکنولوژی و سرمایه های اطلاعاتی است . سیاست امنیتی ، می بایست مکانیزم و راهکارهای مربوطه را با تاکید بر امکانات موجود تبیین نماید . از دیگر اهداف یک سیاست امنیتی ، ارائه یک خط اصولی برای پیکربندی و ممیزی سیستم های کامپیوتری و شبکه ها، بمنظور تبعیت از سیاستها است . یک سیاست امنیتی مناسب و موثر، می بایست رضایت و حمایت تمام پرسنل موجود در یک سازمان را بدنبال داشته باشد .

یک سیاست امنیتی خوب دارای ویژگی های زیر است :

- امکان پیاده سازی عملی آن بکمک روش های متعددی نظیر رویه های مدیریتی، وجود داشته باشد .
- امکان تقویت آن توسط ابزارهای امنیتی ویا دستورات مدیریتی در مواردیکه پیشگیری واقعی از لحاظ فنی امکان پذیر نیست ، وجود داشته باشد .
- محدوده مسئولیت کاربران ، مدیران شبکه و مدیران عملیاتی بصورت شفاف مشخص گردد .
- پس از استقرار، قابلیت برقرای ارتباط با منابع متفاوت انسانی را دارا باشد . (یک بار گفتن و همواره در گوش داشتن)
- دارای انعطاف لازم بمنظور برخورد با تغییرات درشبکه باشد. (سیاست های تدوین شده ، نمونه ای بارز از مستندات زنده تلقی می گردند).

1-2 سیستم های عامل و برنامه های کاربردی : نسخه ها و بهنگام سازی

در صورت امکان، می بایست از آخرین نسخه سیستم های عامل و برنامه های کاربردی بر روی تمامی کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده ، سوئیچ، روتر، فایروال و سیستم های تشخیص مزاحمین) استفاده شود. سیستم های عامل و برنامه های کاربردی می بایست بهنگام بوده و همواره از آخرین امکانات موجود بهنگام سازی (hotfixes , patches,service pack) استفاده گردد در این راستا می بایست حساسیت بیشتری نسبت به برنامه های آسیب پذیرکه زمینه لازم برای متجاوزان اطلاعاتی را فراهم می نمایند ، وجود داشته باشد.

برنامه های : IIS ,OutLook , Internet Explorer , BIND و sendmail بدلیل وجود نقاط آسیب پذیر می بایست مورد توجه جدی قرار گیرند . متجاوزان اطلاعاتی ، بدفعات از نقاط آسیب پذیر برنامه های فوق برای خواسته های خود استفاده کرده اند .

2-2 شناخت شبکه موجود

بمنظور پیاده سازی و پشتیبانی سیستم امنیتی ، لازم است لیستی از تمام دستگاههای سخت افزاری و برنامه های نصب شده ، تهیه گردد . آگاهی از برنامه هائی که بصورت پیش فرض نصب شده اند، نیز دارای اهمیت خاص خود است (مثلا" برنامه IIS بصورت پیش فرض توسط SMS و یا سرویس دهنده SQL در شبکه های مبتنی بر ویندوز نصب می گردد) . فهرست برداری از سرویس هائی که بر روی شبکه در حال اجراء می باشند، زمینه را برای پیمایش و تشخیص مسائل مربوطه ، هموار خواهد کرد .

3-2 سرویس دهندگان TCP/UDP و سرویس های موجود در شبکه

تمامی سرویس دهندگان TCP/UDP در شبکه بهمراه سرویس های موجود بر روی هر کامپیوتر در شبکه، می بایست شناسائی و مستند گردند . در صورت امکان، سرویس دهندگان و سرویس های غیر ضروری، غیر فعال گردند . برای سرویس دهندگانی که وجود آنان ضروری تشخیص داده می شود، دستیابی به آنان محدود به کامپیوترهائی گردد که به خدمات آنان نیازمند می باشند . امکانات عملیاتی را که بندرت از آنان استفاده میشود و دارای آسیب پذیری بیشتری می باشند، غیر فعال تا زمینه بهره

برداری آنان توسط متجاوزان اطلاعاتی سلب گردد. توصیه می گردد ، برنامه های نمونه (Sample) تحت هیچ شرایطی بر روی سیستم های تولیدی (سیستم هائی که محیط لازم برای تولید نرم افزار بر روی آنها ایجاد و با استفاده از آنان محصولات نرم افزاری تولید می گردند) نصب نگردند .

رمزعبور

انتخاب رمزعبور ضعیف ، همواره یکی از مسائل اصلی در رابطه با هر نوع سیستم امنیتی است . کاربران، می بایست متعهد و مجبور به تغییر رمز عبورخود بصورت ادواری گردند . تنظیم مشخصه های رمزعبور در سیستم های مبتنی بر ویندوز، بکمک Account Policy صورت می پذیرد. مدیران شبکه، می بایست برنامه های مربوط به تشخیص رمز عبور را تهیه و آنها را اجراء تا آسیب پذیری سیستم در بوته نقد و آزمایش قرار گیرد .
برنامه های Ripper john the ، LOphtcrack و Crack ، نمونه هائی در این زمینه می باشند . به کاربرانی که رمز عبور آنان ضعیف تعریف شده است ، مراتب اعلام و در صورت تکرار اخطار داده شود (عملیات فوق، می بایست بصورت متناوب انجام گیرد) . با توجه به اینکه برنامه های تشخیص رمزعبور،زمان زیادی از پردازنده را بخود اختصاص خواهند داد، توصیه می گردد، رمز عبورهای کد شده (لیست SAM بانک اطلاعاتی در ویندوز) را بر روی سیستمی دیگر که در شبکه نمی باشد، منتقل کنند تا زمینه بررسی رمزهای عبور ضعیف، فراهم گردد. با انجام عملیات فوق برروی یک کامپیوتر غیر شبکه ای ، نتایج

بدست آمده برای هیچکس قابل استفاده نخواهد بود(مگراینکه افراد بصورت فیزیکی به سیستم دستیابی پیدا نمایند) .
برای تعریف رمز عبور، موارد زیر پیشنهاد می گردد :

- حداقل طول رمز عبور، دوازده و یا بیشتر باشد .
- دررمز عبور از حروف کوچک، اعداد، کاراکترهای خاص و Underline استفاده شود .
- از کلمات موجود در دیکشنری استفاده نگردد .
- رمز های عبور، در فواصل زمانی مشخصی (سی و یا نود روز) بصورت ادواری تغییر داده شوند
- کاربرانی که رمزهای عبور ساده و قابل حدسی را برای خود تعریف نموده اند، تشخیص و به آنها تذکر داده شود .(عملیات فوق بصورت متناوب و در فواصل زمانی یک ماه انجام گردد).

4-2 عدم اجرای برنامه ها ئی که منابع آنها تایید نشده است

در اغلب حالات، برنامه های کامپیوتری در یک چارچوب امنیتی خاص مربوط به کاربری که آنها را فعال می نماید، اجراء می گردند. دراین زمینه ممکن است، هیچگونه توجهی به ماهیت منبع ارائه دهنده برنامه توسط کاربران انجام نگردد. وجودیک زیرساخت PKI (Public key infrastructure) ، در این زمینه می تواند مفید باشد . در صورت عدم وجود زیرساخت امنیتی فوق، می بایست مراقبت های لازم در رابطه با طرفندهای استفاده شده توسط برخی از متجاوران اطلاعاتی را انجام داد. مثلا" ممکن است برخی آسیبها در ظاهری کاملا" موجه از طریق یک پیام الکترونیکی جلوه

نمایند . هرگز یک ضمیمه پیام الکترونیکی و یا برنامه ای را که از منبع ارسال کننده آن مطمئن نشده اید ، فعال و یا اجراء ننمائید. همواره از برنامه ای نظیر Outlook بمنظور دریافت پیام های الکترونیکی استفاده گردد . برنامه فوق در یک ناحیه محدوده شده اجراء و می بایست امکان اجرای تمام اسکریپت ها و محتویات فعال برای ناحیه فوق ، غیر فعال گردد .

5-2 ایجاد محدودیت در برخی از ضمائم پست الکترونیکی

ضرورت توزیع و عرضه تعداد زیادی از انواع فایل های ضمیمه، بصورت روزمره در یک سازمان وجود ندارد .بمنظور پیشگیری از اجرای کدهای مخرب، پیشنهاد می گردد این نوع فایل ها، غیر فعال گردند . سازمان هائی که از Outlook استفاده می نمایند، می توانند با استفاده از نسخه 2002 اقدام به بلاک نمودن آنها نمایند . (برای سایر نسخه های Outlook می توان از Patch امنیتی مربوطه استفاده کرد) .

فایل های زیر را می توان بلاک کرد :

نوع فایل هائی که می توان آنها را بلاک نمود .
.bas .hta .msp .url .bat .inf .mst .vb .chm .ins .pif .vbe .cmd .isp .pl .vbs .com .js .reg .ws .cpl .jse .scr .wsc .crt

.lnk .sct .wsf .exe .msi .shs .wsh

در صورت ضرورت می توان ، به لیست فوق برخی از فایل ها را اضافه و یا حذف کرد. مثلا" با توجه به وجود عناصر اجرائی در برنامه های آفیس ، میتوان امکان اجرای برنامه ها را در آنان بلاک نمود . مهمترین نکته در این راستا به برنامه Access بر می گردد که برخلاف سایر اعضاء خانواده آفیس ، دارای امکانات حفاظتی ذاتی در مقابل ماکروهای آسیب رسان نمی باشد .

6-2 پایبندی به مفهوم کمترین امتیاز

اختصاص حداقل امتیاز به کاربران، محور اساسی درپیاده سازی یک سیتم امنیتی است. رویکرد فوق بر این اصل مهم استوار است که کاربران می بایست صرفا" دارای حقوق و امتیازات لازم بمنظور انجام کارهای مربوطه باشند (بذل و بخشش امتیازات در این زمینه شایسته نمی باشد!) . رخنه در سیستم امنیتی از طریق کدهای مخربی که توسط کاربران اجراء می گردند، تحقق می یابد . در صورتیکه کاربر، دارای حقوق و امتیازات بیشتری باشد ، آسیب پذیری اطلاعات در اثر اجرای کدها ی مخرب ، بیشتر خواهد شد . موارد زیر برای اختصاص حقوق کاربران ، پیشنهاد می گردد :

- تعداد account مربوط به مدیران شبکه، می بایست حداقل باشد .

- مدیران شبکه، می بایست بمنظور انجام فعالیت های روزمره نظیر خواندن پیام های پست الکترونیکی ، از یک account روزمره استفاده نمایند .
- مجوزهای لازم برای منابع بدرستی تنظیم و پیکربندی گردد . در این راستا می بایست حساسیت بیشتری نسبت به برخی از برنامه ها که همواره مورد استفاده متجاوزان اطلاعاتی است ، وجود داشته باشد . این نوع برنامه ها ، شرایط مناسبی برای متجاوزان اطلاعاتی را فراهم می نمایند. جدول زیر برخی از این نوع برنامه ها را نشان می دهد .

برنامه های مورد توجه متجاوزان اطلاعاتی
explorer.exe, regedit.exe, poledit.exe, taskman.exe, at.exe, cacls.exe,cmd.exe, finger.exe, ftp.exe, nbstat.exe, net.exe, net1.exe,netsh.exe, rcp.exe, regedt32.exe, regini.exe, regsvr32.exe,rexec.exe, rsh.exe, runas.exe, runonce.exe, svrmgr.exe,sysedit.exe, telnet.exe, tftp.exe, tracert.exe, usrmgr.exe,wscript.exe,xcopy.exe

- رویکرد حداقل امتیاز ، می تواند به برنامه های سرویس دهنده نیز تعمیم یابد . در این راستا می

بایست حتی المقدور، سرویس ها و برنامه ها توسط یک account که حداقل امتیاز را دارد ،اجراء گردند .

7-2 ممیزی برنامه ها

اغلب برنامه های سرویس دهنده ، دارای قابلیت های ممیزی گسترده ای می باشند . ممیزی می تواند شامل دنبال نمودن حرکات مشکوک و یا برخورد با آسیب های واقعی باشد . با فعال نمودن ممیزی برای برنامه های سرویس دهنده و کنترل دستیابی به برنامه های کلیدی نظیر برنامه هائی که لیست آنها در جدول قبل ارائه گردید، شرایط مناسبی بمنظور حفاظت از اطلاعات فراهم می گردد .

8-2 چاپگر شبکه

امروزه اغلب چاپگرهای شبکه دارای قابلیت های از قبل ساخته شده برای سرویس های FTP,WEB و Telnet بعنوان بخشی از سیستم عامل مربوطه، می باشند . منابع فوق پس از فعال شدن، مورد استفاده قرار خواهند گرفت . امکان استفاده از چاپگرهای شبکه بصورت FTP Bound servers ، Telnet و یا سرویس های مدیریتی وب، وجود خواهد داشت . رمز عبور پیش فرض را به یک رمز عبور پیچیده تغییر و با صراحت پورت های چاپگر را در محدوده روتر / فایروال بلاک نموده و در صورت عدم نیاز به سرویس های فوق ، آنها را غیر فعال می نمایند .

9-2 پروتکل SNMP (Protocol Simple Network Management)

پروتکل SNMP ، در مقیاس گسترده ای توسط مدیران شبکه بمنظور مشاهده و مدیریت تمام کامپیوترهای موجود در شبکه (سرویس گیرنده ، سرویس دهنده، سوئیچ ، روتر، فایروال) استفاده می گردد .SNMP ، بمنظور تایید اعتبار کاربران ، از روشی غیر رمز شده استفاده می نماید . متجاوزان اطلاعاتی ، می توانند از نقطه ضعف فوق در جهت اهداف سوء خود استفاده نمایند . در چنین حالتی، آنان قادر به اخذ اطلاعات متنوعی در رابطه با عناصر موجود در شبکه بوده و حتی امکان غیر فعال نمودن یک سیستم از راه دور و یا تغییر پیکربندی سیستم ها وجود خواهد داشت . در صورتیکه یک متجاوز اطلاعاتی قادر به جمع آوری ترافیک SNMP دریک شبکه گردد، از اطلاعات مربوط به ساختار شبکه موجود بهمراه سیستم ها و دستگاههای متصل شده به آن، نیز آگاهی خواهد یافت . سرویس دهندگان SNMP موجود بر روی هر کامپیوتری را که ضرورتی به وجود آنان نمی باشد ، غیر فعال نمائید . در صورتیکه بهر دلیلی استفاده از SNMP ضروری باشد ، می بایست امکان دستیابی بصورت فقط خواندنی در نظر گرفته شود . در صورت امکان، صرفا" به تعداد اندکی از کامپیوترها امتیاز استفاده از سرویس دهنده SNMP اعطاء گردد .

10-2 تست امنیت شبکه

مدیران شبکه های کامپیوترهای می بایست، بصورت ادواری اقدام به تست امنیتی تمام کامپیوترهای موجود در شبکه (سرویس گیرندگان، سرویس دهندگان، سوئیچ ها ، روترها ، فایروال ها و سیتستم های تشخیص مزاحمین) نمایند. تست امنیت شبکه، پس از اعمال هر گونه تغییر اساسی در پیکربندی شبکه ، نیز می بایست انجام شود.

3- سیاستهای امنیتی شبکه های کامپیوتری

مقدمه

1-3 امنیت اطلاعات در شبکه های کامپیوتری

امروزه امنیت اطلاعات در سیستم های کامپیوتری بعنوان یکی از مسائل مهم مطرح است و می بایست به مقوله امنیت اطلاعات نه بعنوان یک محصول بلکه بعنوان یک فرآیند نگاه کرد.

در صورتیکه قصد ارائه و یا حتی مصرف بهینه و سریع اطلاعات را داشته باشیم، می بایست زیر ساخت مناسب را در این جهت ایجاد کنیم . شبکه های کامپیوتری ، بستری مناسب برای عرضه ، ارائه و مصرف اطلاعات می باشند(دقیقا" مشابه نقش جاده ها در یک سیستم حمل و نقل) . فراموش نکنیم که امروزه زمان کهنه شدن اطلاعات از زمان تولید اطلاعات بسیار سریعتر بوده و می بایست قبل از

اتمام تاریخ مصرف اطلاعات با استفاده از زیر ساخت مناسب (شبکه های ارتباطی) اقدام به عرضه آنان نمود. بموازات حرکت بسمت یک سازمان مدرن و مبتنی بر تکنولوژی اطلاعات، می بایست تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده گردد. مهمترین مزیت و رسالت شبکه های کامپیوتری ، اشتراک منابع سخت افزاری و نرم افزاری است. کنترل دستیابی و نحوه استفاده از منابع به اشتراک گذاشته شده ، از مهمترین اهداف یک سیستم امنیتی در شبکه است . با گسترش شبکه های کامپیوتری خصوصا" اینترنت، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده ، وارد مرحله جدیدی شده است. در این راستا، لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، پایبند به یک استراتژی خاص بوده و بر اساس آن سیستم امنیتی را اجراء و پیاده سازی نماید . عدم ایجاد سیستم مناسب امنیتی ، می تواند پیامدهای منفی و دور از انتظاری را بدنبال داشته باشد . استراتژی سازمان ما برای حفاظت و دفاع از اطلاعات چیست؟ در صورت بروز مشکل امنیتی در رابطه با اطلاعات در سازمان ، بدنبال کدامین مقصر می گردیم؟ در حالیکه یک سازمان برای خرید سخت افزار نگرانی های خاص خود را داشته و سعی در برطرف نمودن معقول آنها دارد ، آیا برای امنیت و حفاظت از اطلاعات نباید نگرانی بمراتب بیشتری در سازمان وجود داشته باشد ؟

2-3 استراتژی

دفاع در عمق، عنوان یک استراتژی عملی بمنظور نیل به تضمین و ایمن سازی اطلاعات در محیط های شبکه امروزی

است . استراتژی فوق، یکی از مناسبترین و عملی ترین گزینه های موجود است که متاثر از برنامه های هوشمند برخاسته از تکنیک ها و تکنولوژی های متفاوت تدوین می گردد . استراتژی پیشنهادی، بر سه مولفه متفاوت ظرفیت های حفاظتی ، هزینه ها و رویکردهای عملیاتی تاکید داشته و توازنی معقول بین آنان را برقرار می نماید . دراین گزارش به بررسی عناصر اصلی و نقش هر یک از آنان در استراتژی پیشنهادی، پرداخته خواهد شد.

3-3 انواع حملات اطلاعاتی

سیستم های اطلاعاتی و شبکه های کامپیوتری اهداف مناسب و جذابی برای مهاجمان اطلاعاتی می باشند . بنابراین لازم است، تدابیر لازم در خصوص حفاظت سیستم ها و شبکه ها در مقابل انواع متفاوت حملات اطلاعاتی اندیشیده گردد. بمنظور آنالیز حملات اطلاعاتی و اتخاذ راهکار مناسب بمنظور برخورد با آنان، لازم است در ابتدا با انواع حملات اطلاعاتی آشنا شده تا از این طریق امکان برخورد مناسب و سیستماتیک با هریک از آنان فراهم گردد . قطعا" وقتی ما شناخت مناسبی را نسبت به نوع و علل حمله داشته باشیم ، قادر به برخورد منطقی با آن بگونه ای خواهیم بود که پس از برخورد، زمینه تکرار موارد مشابه حذف گردد .

انواع حملات اطلاعاتی بشرح ذیل می باشند :

- غیرفعال
- فعال

- نزدیک (مجاور)
- خودی ها (محرمان)
- عرضه (توزیع)

ویژگی هر یک از انواع حملات فوق ، بشرح زیر می باشد :

- **غیر فعال (Passive)** این نوع حملات شامل: آنالیزترافیک شبکه، شنود ارتباطات حفاظت نشده، رمزگشائی ترافیک های رمز شده ضعیف و بدست آوردن اطلاعات معتبری همچون رمز عبور می باشد. ره گیری غیرفعال عملیات شبکه، می تواند به مهاجمان، هشدارها و اطلاعات لازم در خصوص عملیات قریب الوقوعی که قرار است در شبکه اتفاق افتند (قرار است از مسیر فوق در آینده محموله ای ارزشمند عبور داده شود !) را خواهد داد. پیامدهای این نوع حملات ، آشکارشدن اطلاعات و یا فایل های اطلاعاتی برای یک مهاجم، بدون رضایت و آگاهی کاربر خواهد بود .
- **فعال (Active)** این نوع حملات شامل : تلاش در جهت خنثی نمودن و یا حذف ویژگی های امنیتی ، معرفی کدهای مخرب ، سرقت و یا تغییر دادن اطلاعات می باشد . حملات فوق می تواند از طریق ستون فقرات یک شبکه، سوء استفاده موقت اطلاعاتی، نفوذ الکترونیکی در یک قلمرو بسته و حفاظت شده و یا حمله به یک کاربر تایید شده در زمان اتصال به یک ناحیه بسته و حفاظت شده، بروز نماید. پیامد حملات فوق، افشای اطلاعات، اشاعه فایل های اطلاعاتی، عدم پذیرش سرویس و یا تغییر در داده ها، خواهد بود.

- **مجاور (Close-in)** این نوع حملات توسط افرادیکه در مجاورت (نزدیکی) سیستم ها قرار دارند با استفاده از تسهیلات موجود، با یک ترفندی خاص بمنظور نیل به اهدافی نظیر : اصلاح ، جمع آوری و انکار دستیابی به اطلاعات باشد، صورت می پذیرد . حملات مبتنی بر مجاورت فیزیکی، از طریق ورود مخفیانه، دستیابی باز و یا هردو انجام می شود .
- **خودی (Insider)** حملات خودی ها ، می تواند بصورت مخرب و یا غیر مخرب جلوه نماید . حملات مخرب از این نوع شامل استراق سمع تعمدی ، سرقت و یا آسیب رسانی به اطلاعات ، استفاده از اطلاعات و یا رد دستیابی سایر کاربران تایید شده باشد. حملات غیر مخرب از این نوع ، عموما" بدلیل سهل انگاری, فقدان دانش لازم و یا سرپیچی عمدی از سیاست های امنیتی صورت پذیرد.
- **توزیع (Distribution)** . حملات از این نوع شامل کدهای مخربی است که در زمان تغییر سخت افزار و یا نرم افزار در محل مربوطه (کارخانه ، شرکت) و یا در زمان توزیع آنها (سخت افزار ، نرم افزار) جلوه می نماید . این نوع حملات می تواند، کدهای مخربی را در بطن یک محصول جاسازی نماید. نظیر یک درب از عقب که امکان دستیابی غیرمجاز به اطلاعات و یا عملیات سیستم در زمان آتی را بمنظور سوء استفاده اطلاعاتی، فراهم می نماید .

در این رابطه لازم است، به سایر موارد نظیر آتش سوزی ، سیل ، قطع برق و خطای کاربران نیز توجه خاصی صورت

پذیرد . در بخش دوم این مقاله ، به بررسی روش های ایمن سازی اطلاعات بمنظور نیل به یک استراتژی خاص امنیتی ، خواهیم پرداخت .

4-3 ایمن سازی اطلاعات

توفیق در ایمن سازی اطلاعات منوط به حفاظت از اطلاعات و سیستم های اطلاعاتی در مقابل حملات است . بدین منظور از سرویس های امنیتی متعددی استفاده می گردد. سرویس های انتخابی می بایست پتانسیل لازم در خصوص ایجاد یک سیستم حفاظتی مناسب، تشخیص بموقع حملات و واکنش سریع را داشته باشند. بنابراین می توان محور استراتژی انتخابی را بر سه مولفه حفاظت ، تشخیص و واکنش استوار نمود. حفاظت مطمئن، تشخیص بموقع و واکنش مناسب از جمله مواردی است که می بایست همواره در ایجاد یک سیستم امنیتی رعایت گردد. سازمان ها و موسسات، علاوه بر یکپارچگی بین مکانیزم های حفاظتی، می بایست همواره انتظار حملات اطلاعاتی را داشته و لازم است خود را به ابزارهای تشخیص و روتین های واکنش سریع، مجهزکنند تا زمینه برخورد مناسب با مهاجمان و بازیافت اطلاعات در زمان مناسب فراهم گردد. یکی از اصول مهم استراتژی "دفاع در عمق" ، برقراری توازن بین سه عنصر اساسی : انسان، تکنولوژی و عملیات است . حرکت بسمت تکنولوژی اطلاعات بدون افراد آموزش دیده و روتین های عملیاتی که راهنمای آنان در نحوه استفاده و ایمن سازی اطلاعات باشد ، محقق نخواهد شد .

1-4-3 انسان

موفقیت در ایمن سازی اطلاعات با پذیرش مسئولیت و حمایت مدیریت عالی یک سازمان (معمولا" در سطح مدیریت ارشد اطلاعات) و بر اساس شناخت مناسب از تهاجمات ، حاصل می گردد. نیل به موفقیت با پیگیری سیاست ها و روتین های مربوطه ، تعیین وظایف و مسئولیت ها ، آموزش منابع انسانی حساس (کاربران، مدیران سیستم) و توجیه مسئولیت های شخصی کارکنان ، حاصل می گردد.در این راستا لازم است یک سیستم امنیتی فیزیکی و شخصی بمنظور کنترل و هماهنگی در دستیابی به هر یک از عناصر حیاتی در محیط های مبتنی بر تکنولوژی اطلاعات ، نیز ایجاد گردد . ایمن سازی اطلاعات از جمله مواردی است که می بایست موفقیت خود را در عمل و نه در حرف نشان دهد . بنابراین لازم است که پس از تدوین سیاست ها و دستورالعمل های مربوطه ، پیگیری مستمر و هدفمند جهت اجرای سیاست ها و دستورالعمل ها ، دنبال گردد. بهترین استراتژی تدوین شده در صورتیکه امکان تحقق عملی آن فراهم نگردد ، (سهوا" و یا عمدا") هرگز امتیاز مثبتی را در کارنامه خود ثبت نخواهد کرد .

با توجه به جایگاه خاص منابع انسانی در ایجاد یک محیط ایمن مبتنی بر تکنولوژی اطلاعات ، لازم است به موارد زیر توجه گردد :

- تدوین سیاست ها و رویه ها
- ارائه آموزش های لازم جهت افزایش دانش
- مدیریت سیستم امنیتی
- امنیت فیزیکی

- امنیت شخصی
- تدابیر لازم در خصوص پیشگیری

2-4-3 تکنولوژی

امروزه از تکنولوژی ها ی متعددی بمنظور ارائه سرویس های لازم در رابطه با ایمن سازی اطلاعات و تشخیص مزاحمین اطلاعاتی، استفاده می گردد. سازمان ها و موسسات می بایست سیاست ها و فرآیندهای لازم بمنظور استفاده از یک تکنولوژی را مشخص تا زمینه انتخاب و بکارگیری درست تکنولوژی در سازمان مربوطه فراهم گردد. در این رابطه می بایست به مواردی همچون : سیاست امنیتی ، اصول ایمن سازی اطلاعات، استانداردها و معماری ایمن سازی اطلاعات ، استفاده از محصولات مربوط به ارائه دهندگان شناخته شده و خوش نام ، راهنمای پیکربندی ، پردازش های لازم برای ارزیابی ریسک سیستم های مجتمع و بهم مرتبط ، توجه گردد . در این رابطه موارد زیر ،پیشنهاد می گردد :

- دفاع در چندین محل . مهاجمان اطلاعاتی(داخلی و یا خارجی) ممکن است ، یک هدف را از چندین نقطه مورد تهاجم قرار دهند. در این راستا لازم است سازمان ها و موسسات از روش های حفاظتی متفاوت در چندین محل (سطح) استفاده کنند ، تا زمینه عکس العمل لازم در مقابل انواع متفاوت حملات ، فراهم گردد . در این رابطه می بایست به موارد زیر توجه گردد :
  - ◄ دفاع از شبکه ها و زیر ساخت . در این رابطه لازم است شبکه های محلی و یا سراسری حفاظت گردند .

(حفاظت در مقابل حملات اطلاعاتی از نوع عدم پذیرش خدمات)

◄ حفاظت یکپارچه و محرمانه برای ارسال اطلاعات در شبکه (استفاده از رمزنگاری و کنترل ترافیک بمنظور واکنش در مقابل مشاهده غیرفعال)

◄ دفاع در محدوده های مرزی . (بکارگیری فایروال ها و سیستم های تشخیص مزاحمین بمنظور واکنش در مقابل حملات اطلاعاتی از نوع فعال)

◄ دفاع در محیط های محاسباتی (کنترل های لازم بمنظور دستیابی به میزبان ها و سرویس دهنده بمنظور واکنش لازم در مقابل حملات از نوع خودی، توزیع و مجاور) .

- دفاع لایه ای . بهترین محصولات مربوط به ایمن سازی اطلاعات دارای نقاط ضعف ذاتی مربوط به خود می باشند. بنابراین همواره زمان لازم در اختیار مهاجمان اطلاعاتی برای نفوذ در سیستم های اطلاعاتی وجود خواهد داشت.بدین ترتیب لازم است قبل از سوءاستفاده اطلاعاتی متجاوزان، اقدامات مناسبی صورت پذیرد. یکی از روش های موثر پیشگیری در این خصوص ، استفاده از دفاع لایه ای در مکان های بین مهاجمان و اهداف مورد نظر آنان ،می باشد . هر یک از مکانیزم های انتخابی ، می بایست قادر به ایجاد موانع لازم در ارتباط با مهاجمان اطلاعاتی (حفاظت) و تشخیص بموقع حملات باشد . بدین ترتیب امکان تشخیص مهاجمان اطلاعاتی افزایش و از طرف دیگر شانس آنها بمنظور نفوذ در سیستم و کسب موفقیت،

کاهش خواهد یافت . استفاده از فایروال های تودرتو (هر فایروال در کنار خود از یک سیستم تشخیص مزاحمین ، نیز استفاده می نماید) در محدوده های داخلی و خارجی شبکه ، نمونه ای از رویکرد دفاع لایه ای است . فایروال های داخلی ممکن است امکانات بیشتری را در رابطه با فیلتر سازی داده ها و کنترل دستیابی به منابع موجود ارائه نمایند . جدول زیر رویکردهای دیگر بمنظور تحقق دفاع لایه ای را نشان می دهد .

سطح دوم	سطح اول دفاع	نوع تهاجم
برنامه های مبتنی بر امنیت	لایه ارتباطی و شبکه رمزنگاری امنیت ترافیک شبکه	غیر فعال
دفاع محیط محاسباتی	دفاع در محدوده های بسته (حفاظتی)	فعال
کنترل و بررسی دقیق	امنیت فیزیکی و شخصی	مجاور

دستیابی		
نظارت وپیشگیری فنی	امنیت فیزیکی و شخصی	خودی
کنترل های یکپارچگی زمان اجراء	نرم افزارهای مطمئن (پیاده سازی ، توزیع)	توزیع

- تعیین میزان اقتدار امنیتی هر یک از عناصر موجود در ایمن سازی اطلاعات (چه چیزی حفاظت شده و نحوه برخورد با تهاجم اطلاعاتی در محلی که از عنصر مربوطه استفاده شده ، به چه صورت است ؟) . پس از سنجش میزان اقتدار امنیتی هر یک از عناصر مربوطه ، می توان از آنان در جایگاهی که دارای حداکثر کارآئی باشند ، استفاده کرد . مثلا" می بایست از مکانیزم های امنیتی مقتدر در محدوده های مرزی شبکه استفاده گردد .
- استفاده از مدیریت کلید مقتدر و زیر ساخت کلید عمومی، که قادر به حمایت از تمام تکنولوژی های مرتبط با ایمن سازی اطلاعات بوده و دارای مقاومت مطلوب در مقابل یک تهاجم اطلاعاتی باشد.
- بکارگیری زیرساخت لازم بمنظور تشخیص مزاحمین ، آنالیز و یکپارچگی نتایج بمنظور انجام واکنش های مناسب در رابطه با نوع تهاجم . زیر ساخت مربوطه می بایست به پرسنل عملیاتی، راهنمائی لازم در

مواجه با سوالاتی نظیر : آیا من تحت تهاجم اطلاعاتی قزار گرفته ام ؟ منبع تهاجم چه کسی می باشد ؟ به چه فرد دیگری تهاجم شده است ؟ راه حل ها و راهکارهای من در این رابطه چیست ؟ ، را ارائه نماید.

3-4-3 عملیات

منظور از عملیات ، مجموعه فعالیت های لازم بمنظور نگهداری وضعیت امنیتی یک سازمان است . در این رابطه لازم است ، به موارد زیر توجه گردد :

- پشتیبانی ملموس و بهنگام سازی سیاست های امنیتی
- اعمال تغییرات لازم با توجه به روند تحولات مرتبط با تکنولوژی اطلاعات. در این رابطه می بایست داده های مورد نظر جمع آوری تا زمینه تصمیم سازی مناسب برای مدیریت فراهم گردد (تامین اطلاعات ضروری برای مدیریت ریسک) .
- مدیریت وضعیت امنیتی با توجه به تکنولوژی های استفاده شده در رابطه ایمن سازی اطلاعات (نصب Patch امنیتی، بهنگام سازی ویروس یابها ، پشتیبانی لیست های کنترل دستیابی)
- ارائه سرویس های مدیریتی اساسی و حفاظت از زیرساخت های مهم (خصوصا" زیر ساخت هائی که برای یک سازمان ختم به درآمد می گردد) .
- ارزیابی سیستم امنیتی
- هماهنگی و واکنش در مقابل حملات جاری

- تشخیص حملات و ارائه هشدار و پاسخ مناسب بمنظور ایزوله نمودن حملات و پیشگیری از موارد مشابه
- بازیافت و برگرداندن امور به حالت اولیه (بازسازی)

4 ارزیابی امنیتی سیستم عامل ویندوز

1-4 مقدمه

سیستم عامل ویندوز، یکی از ده ها سیستم عامل موجود در جهان است که مدیریت منابع سخت افزاری و نرم افزاری در یک کامپیوتر را برعهده دارد . استفاده از ویندوز بعنوان سیستم عاملی شبکه ای ، همزمان با عرضه NT ، وارد مرحله جدیدی گردید . در ادامه و بدنبال ارائه نسخه های دیگری از ویندوز ، فصل جدیدی از بکارگیری سیستم عامل فوق در شبکه های کامپیوتری گشوده گردید . استفاده از سیستم عامل ویندوز (نسخه های متفاوت) در ایران بطرز محسوسی افزایش و هم اینک، در اکثر شبکه های کامپیوتری از سیستم عامل فوق، استفاده می گردد . دامنه استفاده از ویندوز، از شبکه های کوچک سازمانی تا شبکه های بزرگ را شامل و حتی اکثر مراکز ASP ، برای میزبانی وب سایت ها از گزینه فوق ، بهمراه مجموعه نرم افزارهای مربوطه استفاده می نمایند . با توجه به جایگاه سیستم عامل در کامپیوتر و نقش آنان در برپاسازی یک شبکه مقتدر و ایمن ، لازم است با نگاهی دقیق به ارزیابی امکانات امنیتی آنان پرداخته و پس از شناسائی نقاط آسیب پذیر، در اسرع وقت نسبت به برطرف نمودن حفره های امنیتی اقدام لازم صورت گیرد . ما عادت کرده ایم اکثر نرم افزارها را با تنظیمات پیش فرض نصب و در این راستا از دکمه طلائی Next ، بدفعات استفاده نمائیم! بدیهی نصب و پیکربندی مناسب

یک سیستم عامل شبکه ای با رویکرد فوق، می تواند اثرات مخربی را در رابطه با حفاظت از اطلاعات در یک سازمان بدنبال داشته باشد . طراحی و پیاده سازی یک سیستم ایمنی مناسب در شبکه های کامپیوتری ، یکی از مهمترین چالش های موجود در دنیای گسترده تکنولوژی اطلاعات است . در این راستا لازم است، سازمان ها و موسسات در این رابطه با یک هدفمندی خاص بسمت برپاسازی یک محیط ایمن در شبکه های کامپیوتری حرکت نموده و قبل از وقوع هرگونه پیشامد ناگوار اطلاعاتی، پیشگیری های لازم صورت پذیرد . با توجه به استفاده گسترده از سیستم عامل ویندوز در ایران ، لازم است به بررسی و ارزیابی امنیتی سیستم عامل فوق پرداخت . شرکت ماکروسافت خود در این زمینه تلاش های گسترده ای را آغاز و اخیرا" توجه خاصی را به این مقوله اختصاص و پروژه های بزرگی را بمنظور نیل به یک سیستم عامل شبکه ای ایمن با توجه واقعیت های موجود تعریف و دنبال می نماید .

شرکت ماکروسافت پس از عرضه نسخه های خاصی از ویندوز و با مشاهده اشکالات و نواقص خصوصا" نواقص امنیتی اقدام به ارائه نرم افزارهای تکمیلی بمنظور بهنگام ساری ویندوز می نماید . Hotfix,Patch و Service pack نمونه های متفاوتی در این زمینه می باشند . با توجه به نقش نرم افزارهای فوق در صحت عملکرد امنیتی ویندوز ، لازم است در ابتدا به نرم افزارهای فوق اشاره گردد .

2-4 Service Pack و HotFix

Service Pack ، یک بهنگام سازی ادواری در رابطه با سیستم عامل بمنظور رفع اشکالات و نواقص موجود است .

ماکروسافت برای ویندوز NT 4.0 (نسخه قبل از ویندوز 2000 با نگرش امکانات شبکه ای) شش و برای ویندوز 2000 تاکنون ، سه Service Pack متفاوت را ارائه کرده است .
بمنظور برطرف نمودن مشکلات احتمالی در فاصله زمانی بین دو service pack ، اقدا م به عرضه Hotfix می گردد.
هر service Pack ، شامل تمام hotfix های قبلی نسبت به نسخه service pack قبلی است .
علاوه بر نصب آخرین نسخه های service Pack ، می بایست اقدام به نصب نسخه های hotfix نیز گردد . معمولا" hotfix ، با توجه به شیوع و گسترش یک مسئله خاص (مثلا" یک حمله اینترنتی) در شبکه، از طرف شرکت مایکروسافت، ارائه می گردد . با اینکه شرکت ماکروسافت توصیه کرده است در صورت بروز مشکل، اقدام به نصب نسخه های Hotfix گردد، ولی پیشنهاد می گردد که بلافاصله پس از نصب آخرین نسخه Service Pack ، اقدام به نصب تمام نسخه های امنیتی Hotfix مربوطه نیز گردد .
یکی از مهمترین چالش های مدیران شبکه ، بهنگام سازی سیستم و نصب آخرین نسخه های Patch است . ماکروسافت در این راستا ، یک برنامه خاص را بمنظور بررسی وضعیت امنیتی Hotfix ها ، ارائه کرده که مدیران شبکه را قادر به پیمایش سرویس دهنده های موجود در شبکه می نماید (برنامه Hfnetchk.exe) . برنامه فوق قادر به تشخیص صحت نصب تمام نسخه های Patch در رابطه با ویندوز 2000 و سایر نرم افزارهای سرویس دهنده نظیر IIS ، IE و SQL است (وضعیت موجود را تشخیص و کمبودها را اعلام می نماید) . برنامه HFNetChk یک ابزار خط دستوری بوده که

مدیران شبکه را قادر به بررسی آخرین وضعیت Patch ها در رابطه با تمام کامپیوترهای موجود در شبکه از یک محل مرکزی می نماید .(مشاهده جزئیات برنامه HFNetChk) . شرکت ماکروسافت در این زمینه ، برنامه جامعی را بمنظور بررسی وضعیت سیستم امنیتی ارائه نموده که برنامه Hfnetchk.exe نیز بخشی از آن است .

پس از معرفی امکانات موجود برای بهنگام سازی ویندوز و برطرف نمودن مشکلات و مسائل موجود در هر یک از نسخه های ویند وز، در ادامه به بررسی و ارزیابی سیستم امنیتی ویندوز پرداخته و در این راستا پیشنهاداتی مطرح می گردد.

3-4 سنجش امنیت در ویندوز 2000

تاکنون بیش از 400 نقطه آسیب پذیر در نسخه های ویندوز 2000، NT و برنامه های مرتبط با آنان شناخته شده و نحوه برطرف نمودن آنان مستند شده است. در این بخش به بررسی برخی از نقاط آسیب پذیر اشاره و نحوه برخورد با آنان بیان می گردد. لازم است به این نکته مهم دقت شود که کاهش برخی از نقاط آسیب پذیر در یک شبکه به معنی عرضه یک شبکه ایمن نمی باشد (تلاشی است در جهت ایمن شدن) .

- از سیستم فایل NTFS در مقابل FAT استفاده شود. سیستم فایل فوق، امکان کنترل دستیابی به فایل ها را برخلاف FAT فراهم می نماید .

- اطلاعات و میدان عمل اتصالات بی هویت (Anonymous users) ، می بایست به حداقل مقدار خود برسد . یک اتصال بی هویت (کاربران ناشناس و گمنام) عضوی از گروه Everyone (گروه از قبل ایجاد شده) خواهد بود . بدین ترتیب آنان قادر به دستیابی تمام منابعی خواهند بود که برای گروه Everyone مجاز شناخته شده است . ویندوز NT پس از نصب آخرین نسخه(6a) Service Pack اکثر عملیاتی را که یک کاربر گمنام قادر به انجام آنها می باشد, محدود می نماید . بمنظورر پیشگیری از شمارش اسامی account ها ، توسط کاربران گمنام ، از کلید ریجستری زیر بهمراه تنظیمات مربوطه استفاده می شود .

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Lsa
Name: RestrictAnonymous
Type: REG_DWORD
Value: 1

- امتیاز Access this computer from the network را در رابطه با کاربران عضو گروه Everyone حذف و آن را با گروه معتبر Users ، جایگزین نمائید . در ویندوز NT 4.0 ، برای انجام عملیات فوق از مسیر زیر و در ویندوز 2000 از Policy Group و یا Security Configuration Toolset استفاده می شود.

User Manager -> Policies -> User Rights

- امکان دستیابی از راه دور به ریجستری را سلب نمائید . کلیدهای ریجستری متعددی وجود دارد، که این امکان را به گروه Everyone و بالطبع کاربران ناشناس خواهد داد که از راه دور قادر به ویرایش ریجستری باشند(خواندن و تنظیم مقادیر مربوط به مجوزها). در صورتیکه کاربر تایید نشده ای ، قادر به ویرایش مقادیر موجود در ریجستری گردد، امکان تغییر مقادیر موجود و بدست آوردن امتیازات با درجه بالا نیز در اختیار وی قرار خواهد گرفت. توصیه می گردد که صرفا" مدیران شبکه و سیستم ، دارای امکان دستیابی از راه دور به ریجستری باشند . بمنظور اعمال محدودیت در رابطه با دستیابی از راه دور به ریجستری ، از کلید زیر برای تنظیم مجوزهای امنیتی استفاده می شود .

HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

- Account مربوط به Guest غیر فعال گردد. در این راستا پیشنهاد می گردد، که تمام Account ها (سرویس ها و کاربران) دارای رمز عبورگردند. (صرفنظر از اینکه account فعال و یا غیر فعال باشد) .
- تایید اعتبار LanMan را غیر فعال نمائید . رمز عبورهای LanMan بمنظور سازگاری با نسخه های قبلی ویندوز (X9) مطرح و عملا" رمزهای عبوری مشابه ویندوز 2000 بوده که تماما" به حروف بزرگ تبدیل

و با استفاده از یک روش خاص رمز شده اند .رمزهای عبور LanMan ، نسبت به سایر رمزهای عبور بمراتب ساده تر کشف و مورد استفاده متجاوزان اطلاعاتی قرار می گیرند . پیشنهاد می گردد، رمزهای عبور LanMan غیر فعال گردند . بمنظور غیر فعال نمودن رمزهای عبور فوق ، کلید ریجستری مربوطه ، می بایست مطابق زیر تغییر تنظیم گردد .

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Lsa
Name: LMCompatibilityLevel
Type: REG_DWORD
Value: 5

- پورت های 135,137,138 و 139 در محدوده روتر و یا فایروال را غیر فعال نمائید (Colse) . برای شبکه های مبتنی بر ویندوز 2000 ، می بایست پورت 445 نیز بلاک گردد . پورت های فوق، برای شبکه های داخلی لازم بوده ولی برای شبکه های خارجی مورد نیاز نخواهند بود . با بلاک نمودن پورت های فوق ، از تعداد حملات متجاوزان اطلاعاتی در شبکه های مبتنی بر ویندوز NT 4.0 و 2000 بنحو چشمگیری کاسته خواهد شد . در این راستا لازم است ، پروتکل های غیر ضروری (نظیر NetBeui و IPX) نیز غیر فعال گردند .
- بر روی فولدرها و فایل های سیستمی ویندوز نیز می بایست لایه های امنیتی مناسبی ایجاد گردد. در این راستا لازم است بر روی فولدرهای حیاتی سیستم نظیر

WINNT و System32 و کلیدهای ریجستری HKLM\Software\Microsoft\Windows\Run و HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AEDebug امکان استفاده از گروه Everyone سلب وبه گروه معتبر Users (شامل لیست کاربران مجاز) اختصاص یابد .

- در رابطه با منابع اشتراکی در شبکه، می بایست محدودیت های لازم اعمال گردد. زمانیکه منبعی در شبکه به اشتراک گذاشته می شود، کنترل دستیابی بصورت پیش فرض گروه Everyone با امتیازFull control خواهد بود . در این راستا پیشنهاد می گردد ، امکان استفاده از منابع اشتراکی ، صرفا" در اختیار کاربرانی قرار گیرد که نیازمند دستیابی به منابع فوق، می باشند .
- تمام سرویس های غیر ضروری نظیر Telnet,FTP,WEB را غیر فعال نمائید. از صحت محل استقرار سرویس ها بر روی شبکه اطمینان حاصل نمائید . مثلا" سرویس دهنده RAS و WEB نباید بر روی یک کنترل کننده Domain ، نصب گردند .
- امکان ممیزی (auditing) در شبکه را فعال نمائید . در ساده ترین حالت ممیزی مربوط به ورود و خروج از شبکه ، دستیابی به امتیازات کاربران و رویدادهای سیستمی نظیر غیر فعال نمودن سیستم (Shutdown) است .

- اعتماد (Trust) موجود بین حوزه ها (Domian) را بررسی و در صورت امکان، موارد غیر ضروری را حذف نمائید .

1-3-4 برنامه های ماکروسافت

وجود نقاط آسیب پذیر در برنامه هائی نظیر outlook,Microsoft Exchange,SQL Server و IIS ، بستر مناسب برای متجاوران اطلاعاتی بمنظور نفوذ در شبکه را ایجاد می نماید . بنابراین لازم است که از آخرین Service Pack و Patch مربوط به هر یک از برنامه ها استفاده گردد .
شرکت مایکروسافت، بمنظور بهبود امنیت برنامه ها ، ابزارهای متعددی را ارائه نموده است . لیست برخی از این برنامه ها در جدول زیر نشان داده شده است .

برنامه	توضیحات
URL Scan Security Tool	به مدیران سرویس دهنده وب امکان اعمال محدودیت در رابطه با پاسخ به درخواست های معتبر را خواهد داد
IIS Lockdown Tool	ابزاری برای ایمن سازی سرویس دهنده وب IIS ، نسخه های چهار و پنج .
Improved Outlook E-mail Security Update	یک نسخه جدید از برنامه بهنگام سازی Outlook بمنظور حفاظت در مقابل انواع حملات اینترنتی مبتنی بر نامه های

الکترونیکی .	
ابزاری بمنظور بررسی آخرین نسخه های Patch نصب شده در رابطه با سیستم عامل و برخی از برنامه ها نظیر IIS, IE و SQL .	HFNetChk Security Tool
ابزاری بمنظور بررسی صحت عملکرد امنیتی سرویس گیرندگان .	Microsoft Personal Security Advisor
برنامه ای جامع برای بررسی وضعیت امنیتی یک کامپیوتر .	Microsoft Baseline Security Analyzer

2-3-4 سومین نقطه آسیب پذیر : Authentication Windows

استفاده از رمزعبور، روش های تائید کاربر و کدهای امنیتی در هر گونه تعامل ارتباطی بین کاربران وسیستم های اطلاعاتی ، امری متداول و رایج است . اکثر روش ها ی تائید کاربران ، نظیر حفاظت فایل و داده ، مستقیما" به رمزهای عبور ارائه شده توسط کاربران، بستگی خواهد داشت . پس از تائید کاربران، امکان دستیابی آنان به منابع مشخص شده فراهم و هر یک از آنان با توجه به امتیازات و مجوزهای نسبت داده شده ، قادر به استفاده از منابع موجودخواهند بود. در اغلب موارد ، فعالیت کاربرانی که مجاز بودن آنان برای دستیابی به منابع ، تائید شده است ، لاگ نشده و یا در

صورتیکه فعالیت آنان ثبت گردد ، کمتر سوء ظنی به آنان می تواند وجود داشته باشد . (آنان پس از تائید وارد میدانی شده اند که بدون هیچگونه ردیابی ، قادر به انجام فعالیت های گسترده ای خواهند بود) . بنابراین ، رمز عبور دارای نقشی حیاتی و اساسی در ایجاد اولین سطح دفاع در یک سیستم اطلاعاتی بوده و از دست رفتن رمز عبور و یا ضعف آن می تواند سیستم را در معرض تهدیدات جدی قرار دهد . مهاجمان پس از دستیابی به رمز عبور کاربران تائید شده (استفاده از مکانیزم های متفاوت) قادر به دستیابی منابع سیستم و حتی تغییر در تنظیمات سایر account های تعریف شده و موجود بر روی سیستم خواهند بود،عملیاتی که می تواند پیامدهای بسیار منفی را بدنبال داشته باشد . پس می بایست بپذیریم که وجود یک account ضعیف و یا فاقد رمز عبور می تواند تهدیدی جدی در یک سازمان باشد . در این راستا علاوه بر اینکه می بایست از پتانسیل های ارائه شده توسط سیستم عامل با دقت استفاده نمود ، ضروری است ، تابع یک سیاست امنیتی تدوین شده در رابطه با رمز عبور در سازمان متبوع خود باشیم . تعریف و نگهداری یک account بهمراه رمز عبور مربوطه در سازمان ما تابع چه سیاست امنیتی است ؟ مهمترین و متداولترین نقاط آسیب پذیر در ارتباط با رمز عبور شامل موارد زیر است :

- Account تعریف شده دارای رمز عبور ضعیف و یا فاقد رمز عبور است .
- عدم حفاظت مناسب کاربران از رمزهای عبور ،صرفنظر از استحکام رمزهای عبور تعریف شده .

- سیستم عامل و یا سایر نرم افزارهای موجود، امکان ایجاد account مدیریتی ضعیف و فاقد رمز عبور را فراهم می نمایند .
- الگوریتم های Hashing رمز عبور(رمزنگاری مبتنی بر کلید عمومی بر پایه یک مقدار hash ، استوار بوده و بر اساس یک مقدار ورودی که دراختیار الگوریتم hashing گذاشته می شود ، ایجاد می گردد. در حقیقت مقدار hash ، فرم خلاصه شده و رمز شده ای از مقدار اولیه خود است) ، شناخته شده بوده و در اغلب موارد مقدار Hashe بدست آمده، بگونه ای ذخیره می گردد که امکان مشاهده آن توسط سایرین وجود خواهد داشت. مناسبترین نوع حفاظت در این راستا ، تبعیت از یک سیاست رمز عبور قدرتمند بوده که در آن دستورالعمل ها ی لازم برای تعریف یک رمز عبورمناسب مشخص و در ادامه با استفاده از ابزارهای موجود، بررسی لازم در خصوص استحکام و بی نقص بودن رمز عبور صورت گیرد.

ویندوز، رمزهای عبور را بصورت متن شفاف ذخیره و یا ارسال نمی نماید و در این راستا از یک مقدار Hash متناظر با رمزعبور ، بمنظور تائید کاربران ، استفاده می نماید . یک مقدار Hash دارای طولی ثابت است که توسط بکارگیری یک تابع ریاضی (الگوریتم hashing) بر روی حجم دلخواهی از داده (message digest نامیده می شود) ایجاد می شود.در ویندوز سه نوع الگوریتم تائید وجود دارد :

- LM (ایمنی کمتر و سازگاری بیشتر)
- NTLM
- NTLMv2 (ایمنی بیشتر و سازگاری کمتر)

با اینکه اکثر محیط های فعلی ویندوز ، ضرورتی به حمایت از (Lan Manager (LM را ندارند، ولی ویندوز بصورت محلی رمز های عبور Hash شده مربوط به LM را (LANMAN Hashes نیز نامیده می شود) بصورت پیش فرض در ویندوز NT ، 2000 و XP (در ویندوز 2003 وضعیت بدین شکل نیست) ذخیره می نماید. با توجه به اینکهLM از یک مدل رمزنگاری بمراتب ضعیف تر نسبت به رویکردهای فعلی مایکروسافت (NTLM,NTLMv2) ، استفاده می نماید، رمزهای عبور LM می توانند در مدت زمانی کوتاه شکسته گردند. حتی رمزهای عبوری که دارای قدرت و استحکام مناسبی می باشند ، در کمتر از یک هفته با استفاده از روش هائی خاص و با اتکاء به قدرت سخت افزارهای موجود ، شکسته خواهند شد .
http://www.msdn.miscrosoft.com/library/default.asp?url=/library/en-us/security/Security/h_gly.asp

ضعف LM hashes بدلایل زیر است :

- رمزهای عبور محدود به چهارده کاراکتر می باشند .
- رمزهای عبور با استفاده از فضای خالی ، به چهارده کاراکتر تبدیل می شوند .
- رمزهای عبور تماما" به حروف بزرگ تبدیل می گردند .

- رمزهای عبور به دو بخش هفت کاراکتری مجزا تقسیم می گردند .

با توجه به ماهیت فرآیند hashing ،یک مهاجم صرفا" می بایست عملیات تشخیص رمز عبور(cracking) را محدود به دو مجموعه نماید که هر یک دارای هفت کاراکتر بوده که به حروف بزرگ تبدیل شده اند . با تکمیل عملیات فوق و اخذ نتایج مثبت ، یک مهاجم قادر به تشخیص رمز عبور یک کاربر تائید شده می گردد وبدین ترتیب ، امکان دستیابی وی به منابع سیستم فراهم خواهد شد. پیچیدگی عملیات تشخیص Hashe ، متنا سب با طول Hash افزایش می یابد ، بنابراین رشته هائی که صرفا" شامل هفت کاراکتر می باشند ، بمراتب راحت تر نسبت به رشته هائی که دارای چهارده کاراکتر می باشند ، تشخیص داده و اصطلاحا" شکسته می گردند. با توجه به این موضوع که تمامی رشته ها شامل هفت کاراکتر بوده و تمامی آنان به حروف بزرگ نیز تبدیل می گردند ، یک تهاجم به "سبک - دیکشنری" (dictionary-style) نیز بسادگی محقق و موفقیت آن تضمین شده خواهد بود. بنابراین، روش hashing LM ، آسیبی جدی را متوجه سیاست های امنیتی رمز عبور نموده و سیستم را در معرض تهدید قرار خواهد داد .

علاوه بر تهدید و خطر ذخیره سازی LM hashes در SAM ، فرآیند تائید Lan Manager ، اغلب و بصورت پیش فرض بر روی سرویس گیرندگان فعال و توسط سرویس دهنده پذیرفته می گردد . لازم است به این نکته اشاره گردد که ، ماشین هائی که بر روی آنان ویندوز نصب شده است ، قادر به

استفاده از الگوریتم های hash بمراتب قویتر در مقابل روش ضعیف hashes LM بمنظور ارسال داده های حساس نظیر رمز عبور می باشند .حداقل پیامد منفی استفاده از روش LM hashes ، آسیب پذیری سیستم تائید کاربران در ویندوز بوده و قطعا" در چنین مواردی نمی توان به فرآیند تائید کاربران ، اعتماد نمود چراکه در این وضعیت عملا" امکان استراق سمع (شنود اطلاعاتی) فراهم و یک مهاجم قادر به تشخیص و بدست آوردن رمزهای عبور خواهد بود.

- **سیستم های عامل در معرض تهدید :**

  تمامی نسخه های ویندوز در معرض این تهدید قرار دارند .

- **نحوه تشخیص آسیب پذیری سیستم**

با اینکه دلایل و علل متفاوتی می تواند در رابطه با ضعف رمز عبور مورد توجه قرار گیرد ، مثلا" وجود Account های فعال برای کاربرانی که سازمان خود را ترک نموده ویا سرویس هائی که اجراء نشده اند، ولی یکی از مناسبترین روش ها بمنظور آگاهی از استحکام یک رمز عبور، بررسی و تست تمامی آنان در مقابل نرم افزارهای cracking رمزهای عبور استفاده شده توسط مهاجمان است . لازم است به این نکته مهم اشاره گردد که از برنامه های تشخیص دهنده رمز عبور بر روی سیستم هائی که حتی مجوز دستیابی به آنان را دارید ، بدون اخذ مجوزهای لازم از مدیران ارشد سیستم ، نمی بایست استفاده نمود. برای دریافت نمونه برنامه هائی در این زمینه می توان

از l0phtcrack version (LC4 4) و John the Ripper استفاده کرد . صرفنظر از رویکرد ذخیره سازی محلی hash LAN Manager ، موارد زیر می بایست موردتوجه قرار گیرد :

- در صورتیکه ویندوز NT ، 2000 و یا XP بصورت پیش فرض نصب شده اند،سیستم در معرض آسیب خواهد بود. در چنین مواردی Lan Manager hashes بصورت پیش فرض و محلی ذخیره می گردد.
- در صورتیکه ، بدلایلی نیازمند تائید مبتنی بر LM در یک سازمان بمنظور ارتباط با سرویس دهنده وجود داشته باشد ، سیستم مجددا" در معرض آسیب قرار خواهد گرفت .چراکه این نوع از ماشین ها اقدام به ارسال LM hashes نموده و پتانسیل شنود اطلاعاتی در شبکه را ایجاد خواهند کرد.

❖ نحوه حفاظت در مقابل نقطه آسیب پذیر :

بهترین و مناسبترین دفاع در مقابل رمزهای عبور ضعیف ، استفاده از یک سیاست مستحکم مشتمل بر دستورالعملهای لازم بمنظور ایجاد رمز عبور قدرتمند و بررسی مستمر آنان بمنظور اطمینان از استحکام و صحت عملکرد می باشد . در این رابطه موارد زیر پیشنهاد می گردد :

- **اطمینان ازاستحکام و انسجام رمز های عبور** . با استفاده از سخت افزار مناسب و اختصاص زمان کافی ، می توان هر رمز عبوری را crack نمود. در این راستا می توان با استفاده ازروش های ساده و در عین حال موفقیت آمیز، عملیات تشخیص رمز عبور را

انجام داد . اغلب برنامه های تشخیص دهنده رمزعبوراز روشی موسوم به "حملات مبتنی بر سبک دیکشنری " ، استفاده می نمایند. با توجه به اینکه روش های رمز نگاری تا حدود زیادی شناخته شده می باشند ، برنامه های فوق ، قادر به مقایسه شکل رمز شده یک رمز عبور در مقابل شکل های رمز شده کلمات دیکشنری می باشند(در زبان های متعدد و استفاده از اسامی مناسب بهمراه جایگشت های مختلف آنان) . بنابراین ، رمز عبوری که ریشه آن در نهایت یک کلمه شناخته شده باشد ، دارای استعداد ذاتی در رابطه با این نوع از حملات خواهد بود .
تعداد زیادی از سازمان ها ، آموزش های لازم در خصوص نحوه تعریف رمزهای عبور را به کارکنان خود داده و به آنان گفته شده است که رمزهای عبور مشتمل بر ترکیبی از حروف الفبائی و کاراکترهای ویژه را برای خود تعریف نمایند.متاسفانه اکثر کاربران این موضوع را رعایت ننموده و بمنظور تعریف یک رمز عبور با نام "password" ، صرفا" اقدام به تبدیل حروف به اعداد و یا حروف ویژه می نمایند (pa$$w0rd) . چنین جایگشت هائی نیز قادر به مقاومت در مقابل یک تهاجم مبتنی بر دیکشنری نبوده و "pa$$w0rd" به روش مشابهی "password" تشخیص داده شده ، crack خواهد شد .
یک رمز عبور خوب ، نمی بایست از ریشه یک کلمه و یا نام شناخته شده ای اقتباس شده باشد .در این راستا لازم است به کاربران آموزش لازم در خصوص انتخاب و ایجاد رمزهای عبور از موارد تصادفی

نظیر یک عبارت ، عنوان یک کتاب ،نام یک آواز و یا نام یک فیلم داده شود. با انتخاب یک رشته طولانی که بر اساس رویکردهای خاصی می تواند انتخاب گردد (گرفتن اولین حرف هر کلمه ، جایگزینی یک کاراکتر خاص برای یک کلمه ، حذف تمامی حروف صدادارو سایر موارد) ، کاربران قادر به ایجاد رمزهای عبور مشتمل بر ترکیبی از حروف الفبائی و حروف ویژه بوده که در صورت مواجه شدن با حملات مبتنی بر دیکشنری ، تشخیص آنان بسختی انجام می شود. لازم است به این نکته نیز اشاره گردد که رمزعبور می بایست براحتی بخاطر سپرده شده و بازیابی (یادآوری) آن مشکل نباشد (هدف از ذخیره سازی ، بازیابی است اگر چیزی را ذخیره نمائیم ولی در زمان مورد نظر قادر به بازیابی آن نباشیم ، سیستم ذخیره و بازیابی ما با اشکال مواجه شده است !). پس از تدوین دستورالعمل لازم بمنظور تولید رمزهای عبور مناسب و آموزش کاربران بمنظور پایبندی به اصول امنیتی تعریف شده ، می بایست از روتین ها ی جانبی متعددی بمنظور اطمینان از پیروی کاربران از دستورالعمل های اعلام شده ، استفاده گردد. بهترین گزینه در این راستا ، بررسی صحت رمزهای عبور پس از اعمال تغییرات توسط کاربران است .

ویندوز 2000 ، XP و 2003 دارای ابزارهای قدرتمندی بمنظورافزایش توان سیاست های امنیتی می باشند . در اکثر نسخه های ویندوز بمنظور مشاهده سیاست تعریف شده در رابطه با رمز می توان از مسیر زیر

استفاده و برنامه Local Security Policy را فعال نمود:

Local Security Policy Program
Start| Programs|Administrative Tools
|Local Security Policy
Select : Account Policies , Then Password Policy

- برنامه Local Security Policy دارای تنظیمات زیر است : Password must meet complexity requirements ، با فعال نمودن سیاست فوق ، رمزهای عبور ملزم به رعایت استانداردهای موجود بمنظور استحکام و پیچیدگی بیشتر در زمان ایجاد و یا تغییر می باشند. در چنین حالتی ، رمزهای عبور تعریف شده می بایست با لحاظ نمودن موارد زیر ایجاد گردند:

◄ رمز عبور، نمی بایست شامل تمام و یا بخشی از نام account کاربر باشد .

◄ رمز عبور می بایست دارای حداقل شش کاراکتر باشد .

◄ رمز عبور می بایست شامل کاراکترهائی از سه گروه از چهار مجموعه زیر باشد :

- حروف بزرگ الفبای انگلیسی (A تا Z)
- حروف کوچک الفبای انگلیسی (a تا z)
- ارقام پایه دهدهی (رقم های 0 تا 9)
- کاراکترهای غیر الفبائی (مثلا" ! ، $ ، #

(% ،

(Enforce password history (range: 0-24 . اغلب کاربران تمایل دارند که پس از انقضاء تاریخ استفاده از رمز عبور خود ، مجددا" همان رمز عبور قبلی را تعریف و از آن استفاده نمایند . با استفاده از سیاست فوق ، می توان مشخص نمود که در چه زمانی و پس از چندین رمز عبور تعریف شده جدید ، کاربران مجاز به استفاده از رمزهای عبور قبلی خود برای وضعیت جدید می باشند .بدین ترتیب ،مدیران شبکه اطمینان لازم در خصوص عدم استفاده مستمر و دائمی یک رمز عبور توسط کاربران را بدست آورده و این موضوع می تواند از زوایای مختلفی بهبود وضعیت امنیتی شبکه را بدنبال داشته باشد . بمنظور نگهداری موثر تاریخچه رمز عبور، نمی بایست امکان تغییر رمزهای عبور بلافاصله پس از پیکربندی سیاست minimum password age ، وجود داشته باشد .

(Maximum password age (range: 0-999 days . سیاست فوق ، حداکثر عمر(اعتبار) یک رمز عبور را بر حسب روز ، مشخص می نماید.(قبل از اینکه سیستم کاربر را ملزم به تغییر رمز عبور نماید) . با در نظر گرفتن مقدار صفر ، رمز عبور دارای عمری جاودانه خواهد شد !

(days Minimum password age (range: 0-999 . سیاست فوق ، حداقل عمر(اعتبار) یک رمز عبور را بر حسب روز

، مشخص می نماید (قبل از اینکه کاربر قادر به تغییر رمزعبور گردد) . با در نظر گرفتن مقدار صفر ، به کاربران اجازه داده خواهد شد که بلافاصله رمز عبور خود را تغییر دهند. minimum password age می بایست کمتر از maximum password age باشد .

پیکربندی minimum password age می بایست بگونه ای انجام شود که دارای مقداری بیش از صفر باشد تا سیاست password history نیز لحاظ شده باشد. بدون وجود یک minimum password age ، کاربران قادر به تغییر ادواری و زمانبندی نشده رمزهای عبور شده و امکان استفاده مجدد از رمزهای عبور قدیمی در یک محدوده زمانی کمتر برای آنان فراهم می گردد.مقادیر پیش فرض تامین کننده اهداف و خواست های امنیتی در یک سازمان نبوده و لازم است مدیران سیستم در ابتدا یک رمز عبور مناسب را برای کاربر تعریف و پس از سپری شدن مدت زمان مشخصی (مدت زمان فوق را minimum password age مشخص می نماید) کاربر را ملزم به تعریف (تغییر) رمز عبور تعریف شده توسط مدیریت شبکه نمایند. زمانیکه کاربران ،عملیاتLog on را انجام و در صورتیکه password history مقدار صفر را دارا باشد ، الزامی در رابطه با انتخاب یک رمز عبور جدید برای کاربران وجود نخواهد داشت . بدین دلیل password history دارای مقدار پیش فرض یک است .

Minimum password length (range: 0-14) characters ، سیاست

فوق ، حداقل تعداد کاراکتر لازم برای تعریف یک رمز عبور را مشخص می نماید (حداقل طول یک رمز عبور) می توان در این رابطه حداقل طول یک رمز عبور را بین یک تا چهارده کاراکتر در نظر گرفت . با اختصاص مقدار صفر ، ضرورت وجود رمز عبور حذف می گردد. حداقل طول رمز عبور، می بایست متناسب و سازگار با سیاست های امنیتی سازمان باشد. در صورتیکه در این رابطه سیاست مشخص و شفافی وجود ندارد می توان مقدار هشت را در نظر گرفت .برخی از سازمان های امنیت اطلاعات شبکه ، مقدار دوازده را در این رابطه پیشنهاد داده اند .

in the Store password using reversible encryption for all users domain . سیاست فوق ، مشخص می نماید که می بایست رمزعبور با استفاده از رمزنگاری وارونه ، ذخیره گردد . در این رابطه ، امکانات حمایتی لازم درخصوص برنامه هائی که از پروتکل هائی بمنظور آگاهی از رمز عبور کاربر بمنظور انجام فرآیند تائید کاربران استفاده می نمایند، نیز ارائه شده است . ذخیره سازی رمزهای عبوری که از رمزنگاری وارونه استفاده می نمایند ، مشابه رمزهای عبورمعمولی است (رمز عبور بصورت متن ذخیره می گردد). بنابراین فعال شدن سیاست فوق می بایست با لحاظ نمودن پارامترهای متعددی نظیر الزام یک برنامه بمنظور استفاده از یک رمز عبور حفاظت شده ، صورت پذیرد . یکی از روش هائی که می توان از آن بمنظور ایجاد اتوماتیک و نسبت دهی رمزهای عبور پیچیده به هر

یک از account های کاربران استفاده نمود ، اجرای دستورالمل زیر از طریق خط دستور است :

From Command Line Prompt :

Net User Username / random

- با اجرای دستورالعمل فوق ، رمزهای عبور تصادفی و پیچیده (همواره هشت کاراکتر طول) به یک account نسبت داده شده و در ادامه رمزعبور مورد نظر بر روی صفحه نمایش داده می شود. روش فوق ، امکانی مناسب بمنظور نسبت دهی رمزهای عبوردر ارتباط با Service accounts بوده و کمتر در ارتباط با کاربران واقعی استفاده می گردد.

بهترین روش برای ممیزی کیفیت رمزهای عبور ، اجرای برنامه های cracking رمز عبور در وضعیتStand-alone است (بخشی از فرآیند بررسی رمزهای عبور) . می بایست عملیات فوق را بر روی یک ماشین حفاظت شده انجام داد.کاربرانی که رمزهای عبور آنان crack می گردد، می بایست موضوع بصورت محرمانه به اطلاع آنان رسیده و دستورالعمل های لازم در خصوص نحوه انتخاب یک رمز عبور مناسب ، در اختیار آنان قرار داده شود.اخیرا" و در پاسخ به رمزهای عبور ضعیف ، استفاده از روش هائی دیگر بمنظور تائید کاربران، نظیر بیومتریک (زیست سنجی) ، نیز مورد توجه واقع شده است .

- **کنترل مستمر account ها** . مدیران سیستم و شبکه می بایست حضوری موثر و مستمر در ارتباط با

مدیریت account های موجود داشته باشند .

- هر گونه account مبتنی بر سرویسی خاص و یا مدیریتی که از آن استفاده نمی گردد، می بایست حذف گردد .

- ممیزی account ها بر روی سیستم را انجام داده و لازم است در این رابطه یک لیست اصلی ایجاد گردد .در این رابطه می بایست رمزهای عبور در ارتباط با سیستم هائی نظیر روترها ، چاپگرهای دیجیتالی متصل شده به اینترنت و سایر موارد دیگر نیز مورد بررسی قرار گیرد.

- روتین هائی خاص بمنظور افزودن account های تائید شده به لیست و یا حذف account هائی که ضرورتی به استفاده از آنان نمی باشد، پیاده سازی و همواره خود را پایبند به آن بدانیم .

- اعتبار لیست را در فواصل زمانی خاصی بررسی تا از بهنگام بودن آن اطمینان حاصل گردد.

- از روتین های خاصی بمنظورحذف account متعلق به کارکنان و یا پیمانکارانی که سازمان را ترک نموده اند ، استفاده گردد .

- **نگهداری و پشتیبانی از سیاست رمزعبور .** بمنظور پشتیبانی و نگهداری مناسب رمز عبور، می توان علاوه بر استفاده از امکانات کنترلی ارائه شده توسط سیستم عامل و یا سرویس های شبکه ، از ابزارهای گسترده ای که در این رابطه ارائه شده است ،نیز استفاده گردد . بدین ترتیب، نگهداری سیاست رمز عبور ، مبتنی بر آخرین تکنولوژی های موجود خواهد

بـود .

- **غیر فعال نمودن تائید LM در شبکه** . بهترین گزینه بمنظور جایگزینی با Lan Manager ، استفاده از روش NTLMv2 NT LAN Manager (version 2) است . متدهای چالش / پاسخ NTLMv2 ، با استفاده از رمزنگاری مستحکم تر و بهبود مکانیزم های تائید ، اکثر صعف های LM را برطرف نموده است جدول زیر ، کلید ریجستری موردنظری را که قابلیت فوق را در ویندوز NT و 2000 کنترل می نماید، نشان می دهد:

Rgistry key
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\LSA
Value: LMCompatibilityLevel
Value Type: REG_DWORD - Number
Valid Range: 0-5
Default: 0

- پارامتر فوق ، نوع و روش تائید را مشخص و می تواند مقداری بین صفر تا پنج را دارا باشد :

0 - ارسال پاسخ بر اساس روش LM و NTLM ، هرگز از امکانات امنیتی NTLMv2 استفاده نمی شود .

1 - استفاده از امکانات امنیتی NTLMv2

2 - ارسال بر اساس روش تائید NTLM

3 - ارسال بر اساس روش تائید NTLMv2

4 - DC باعث رد تائید LM می گردد.
5 - DC باعث رد تائید LM و NTLM شده و صرفا" تائید NTLMv2 پذیرفته می گردد .

- در ویندوز 2000 ، 2003 و XP نیز امکاناتی ارائه شده است که می توان با استفاده از آنان اقدام به پیکربندی تنظیمات مورد نظر در ارتباط با سطح تائید Lan Manager نمود . در این رابطه لازم است برنامه Policy Local Security فعال و در ادامه گزینه های Local Policies و Security Options بترتیب انتخاب گردند . در ویندوز 2000 سیاست LAN Manager authentication level ، و در ویندوز XP و 2003 سیاست security: LAN Manager authentication level Network ، بمنظور پیکربندی ومقداردهی مناسب انتخاب گردند .
در صورتیکه بر روی تمامی سیستم ها ، ویندوز NT SP4 و یا بعد از آن نصب شده باشد ، می توان مقدارپارامتر فوق را بر روی تمامی سرویس گیرندگان سه و بر روی Domain Controllers مقدار پنج درنظر گرفت (پیشگیری از ارسال LM hashes بر روی شبکه) .
سیستم هائی نظیر ویندوز 95 و 98 از NTLMv2 بصورت پیش فرض بهمراه Microsoft Network Client استفاده نمی نمایند ، بنابراین لازم است بمنظور استفاده از قابلیت های NTLMv2 ، برنامه Directory Services Client بر روی آنان نصب گردد. پس از نصب سرویس فوق ، مقدار ریجستری با نام LMCompatibility می تواند مقدار صفر و یا سه را دارا باشد .در صورتیکه نمی توان سرویس گیرندگان قدیمی (ویندوز 95 و یا

ویندوز 98) را ملزم به استفاده از NTLMv2 نمود ، می توان تغییر مورد نظر را در رابطه با LM hashing نسبت به استفاده از NTLM (NT Lan Manager, version) در Domain Controller اعمال نمود.در این رابطه می توان مقدار LMCompatibilityLevel را چهار در نظر گرفت . درصورت استفاده از ابزاری نظیر Local Security Policy،می بایست مقدار LAN Manager authentication level را Send NTLMv2 Response only\Refuse LM درنظر گرفت . لازم است به این نکته اشاره گردد که ایمن ترین گزینه در این رابطه، اعمال محدودیت برروی سرویس گیرندگان است .

- **ممانعت از ذخیره سازی LM hash** . یکی از مسائل اصلی در ارتباط با حذف LM hashes در شبکه ، ذخیره سازی آنان در SAM و یا اکتیو دایرکتوری است .مایکروسافت دارای مکانیزمی بمنظور غیرفعال نمودن ایجاد LM hashes بوده ولی امکان استفاده از آن صرفا" در سیستم های ویندوز 2000 (SP2 و یا بعد بر روی آنان نصب شده است) ، 2003 و XP بوجود دارد. کلید ریجستری زیر، کنترل عملیات فوق راانجام می دهد. در صورتیکه بر روی Windows 2000 Domain Controller کلید فوق ایجاد شده باشد ، LanMan hashes ، در ادامه ایجاد نخواهد شد و در اکتیو دایرکتوری نیز ذخیره نمی گردد. در ویندوز 2003 و XP ، می توان با فعال نمودن گزینه :Network security LAN Manager hash value on next password change Do not store

به اهداف موردنظر در رابطه با ذخیره سازی LM hash دست یافت . در این رابطه لازم است برنامه Local Policy Security فعال و در ادامه گزینه های Local Policies و Security Options بترتیب انتخاب گردند . پس از اعمال تغییرات فوق ، می بایست سیستم راه اندازی شده تا تغییرات ایجاد شده ، موثر واقع شوند . لازم است به این نکته مهم اشاره گردد که روش های ارائه شده ، صرفا" پیشگیری لازم در خصوص ایجاد LM hashes جدید راانجام داده و LM hashes موجود بصورت انفرادی و در زمانیکه کاربر رمز عبور خود را تغییر دهد ، حذف خواهند شد .

Rgistry key
Hive: HKEY_LOCAL_MACHINE Key: System\CurrentControlSet\Control\LSA\NoLMHash

- **ممانعت و پیشگیری از تکثیر Hash و بانک های اطلاعاتی SAM**

ابزارهای cracking رمزعبور، بمنظور بدست آوردن رمزهای عبور hashes از روش های زیر استفاده می نمایند :

- *کشف رمزهای عبور از شبکه* . بدین منظور موارد زیر پیشنهاد می گردد :

- استفاده از شبکه های سوئیچ شده .

- تشخیص و حذف کارت های شبکه بی هدف موجود در شبکه (در این رابطه می توان از ابزارهای امنیتی

خاصی نظیر *ethereal* استفاده کرد) .

- *تکثیر فایل SAM* . فایل فوق در ویندوز NT4 و 2000 در فولدر %SystemRoot%\System32\Config (عموما" در مسیر C:\Winnt\System32\Config) و در ویندوز XP و یا 2003 در فولدر C:\Windows\System32\Config مستقرمی باشد.، فایل فوق ، توسط سیستم عامل ویندوز Lock و صرفا" زمانی امکان تکثیرآن وجود خواهد داشت که ماشین با یک سیستم عامل دیگر راه اندازی شده باشد. فایل SAM را می توان با استفاده از فایل Backup مربوطه نیز بدست آورد.

بمنظور پیشگیری از تکثیر فایل SAM و افزایش سطح امنیتی سیستم لازم است دستیابی فیزیکی به سیستم های موجود خصوصا"Domain Controllers محدود و همواره از اطلاعات Backup گرفته شده و دیسک Repair نیز بمنظور برخورد با مشکلات آتی ایجاد گردد .

برای اخذ اطلاعات تکمیلی می توان از مقالات زیر استفاده نمود:

- How to Disable LM Authentication on Windows NT
- How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT
- New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager

7-4 ششمین نقطه آسیب پذیر : (Microsoft Data Access Components (MDAC

MDAC ، شامل مجموعه ای از تکنولوژی های مرتبط با بانک اطلاعاتی است که در تعدادی از نسخه های اخیر ویندوز، بکارگرفته شده است . مهاجمان با استفاده از نقاط آسیب پذیر MDAC ، تاکنون حملات متعددی را در این رابطه سازماندهی و توانسته اند از سیستم های آسیب پذیر در جهت اهداف خود (اجراء کد و دستورات مخرب) استفاده نمایند . حملات فوق ، می تواند دلایل متعددی داشته باشد ولی می توان به دو عامل اصلی در این زمینه اشاره نمود : استفاده از رویکردهای قدیمی (نظیر RDS) و وجود مسائل جدید در محصولات ارائه شده که یک مهاجم را قادر می سازد با ایجاد یک buffer overflow ، تمامی سیستم را به مخاطره اندازد .

RDS که از کلمات Remote Data Services اقتباس شده است ، نسخه قدیمی MDAC بوده و دارای یک ضعف امنیتی است که کاربران از راه دور را قادر می سازد ، دستوراتی را بصورت محلی بهمراه مجوزها و امتیازات مدیریتی، اجراء نمایند. ترکیب ضعف فوق بهمراه ضعف امنیتی موجود در Microsoft Jet Database Engine 3.5 (بخشی از MS Access) ، آسیب پذیری سیستم افزایش و زمینه تهدیدات متعددی فراهم می گردد (دستیابی به بانک های اطلاعاتی) .ضعف ها و مشکلات فوق ، بطور کامل شناخته شده و بیش از سه سال است که مستندات لازم بمنظور مقابله با آنان تهیه و ارائه شده است . وجود سیستم های قدیمی که هنوز خود را با آخرین وضعیت موجود بهنگام نکرده و یا عدم پیکربندی مناسب سیستم ها ، از دلایل اصلی آسیب پذیری سیستم ها ی موجود می باشد .

مهاجمان تاکنون با استفاده از ضعف فوق ،حملات متنوعی

را سازماندهی و به سرانجام رسانده اند . یکی ازحملات اخیر در این رابطه ، بدلیل Buffer Overflow در MDAC بوده که در بولتن (خبرنامه) امنیتی شماره MS03-033 مایکروسافت به آن اشاره شده است . نسخه MDAC در ویندوز 2003 ، دارای این نقطه آسیب پذیر نمی باشد .

4-7-1 سیستم های عامل در معرض تهدید

اکثر سیستم های ویندوزNT 4 که بر روی آنان نسخه های سه و یا چهار برنامه IIS ، ویژوال استودیو شش و یا RDS 1.5 ، نصب شده باشد ، دارای ضعف امنیتی فوق می باشند. ویندوز 2000 و XP همانند سیستم هائی که بر روی آنان آفیس 2000 (بهمراه SP1) ، نسخه SQL Server 7 (که بر روی آنان SP2 و به بعد نصب شده است) ، Server SQL 2000 از MDAC استفاده می نمایند . همانگونه که مشاهده می شود، اکثر نسخه های ویندوز دارای نقطه آسیب پذیر فوق می باشند .

4-7-2 نحوه تشخیص آسیب پذیر ی سیستم

درصورتیکه بر روی کامپیوتری ویندوز NT 4.0 بهمراه IIS نسخه سه ویا چهار نصب شده باشد ، می بایست بررسی لازم در خصوص وجود فایل "msadcs.dll" انجام شود (فایل فوق، عموما" در آدرس C:\Program Files\Common Files\System\Msadc\msadcs.dll ، قرار دارد، آدرس فوق ممکن است با توجه به پیکربندی سیستم متفاوت باشد). در صورتیکه سیستم مورد نظر شامل فایل فوق باشد ، بهنگام سازی و یا Patching سیستم ، منطقی ترین کاری است که می توان انجام داد.در صورت وجود نرم افزارهای قدیمی و

سیستم های عامل اشاره شده، سیستم در معرض تهدید و آسیب قرار خواهد داشت. بمنظور آگاهی از جزیئات لازم در خصوص نقاط آسیب پذیر اخیر MDAC می توان از بولتن امنیتی شماره MS03-033مایکروسافت استفاده نمود . در این رابطه می توان از Windows Update نیز بمنظور تشخیص آسیب پذیری سیستم ، استفاده نمود. امکان فوق ، بررسی لازم در خصوص نرم افزارهای نصب شده بر روی ماشین را انجام و متناسب با شرایط موجود اقدام به بهنگام سازی نرم افزارها خواهد نمود.

3-7-4 نحوه حفاظت در مقابل نقطه آسیب پذیر

در رابطه با ضعف های RDS ، Jet و نحوه تصحیح و مقابله با آنان می توان از آدرس http://www.wiretrip.net/rfp/txt/rfp9907.txt استفاده نمود.
مایکروسافت نیز در این رابطه چندین بولتن (خبرنامه) امنیتی را منتشر که در آنان نحوه برخورد وحفاظت در مقابل این نقطه آسیب پذیر نشریح شده است .

http://support.microsoft.com/support/kb/articles/q184/3/75.asp
http://www.microsoft.com/technet/security/bulletin/ms98-004.asp
http://www.microsoft.com/technet/security/bulletin/ms99-025.asp
http://www.microsoft.com/security/security_bulletins/ms03-033.asp
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-033.asp
http://support.microsoft.com/default.aspx?scid=kb;en-us;823718

بمنظور برخورد با ضعف امنیتی فوق ، می توان MDAC موجود را به نسخه MDAC ver 2.8 ، ارتقاء داد . آخرین

نسخه MDAC و سایر عناصر مرتبط با بانک های اطلاعاتی را می‌توان از طریق آدرس http://msdn.microsoft.com/library/default.asp?url=/downloads/list/dataaccess.asp مشاهده و دریافت نمود. در این رابطه می توان از Windows Update نیز استفاده نمود.

8-4 هفتمین نقطه آسیب پذیر : Windows Scripting Host (WSH)

WSH، تکنولوژی ارائه شده توسط مایکروسافت بمنظور افزایش عملکرد وتوانائی های ویندوز می باشد .تکنولوژی فوق ، از جاوا اسکریپت و VBScript حمایت و اولین مرتبه بهمراه IEنسخه پنج ارائه و در ادامه بعنوان یک استاندارد بهمراه سایر نسخه های سیستم عامل ویندوز ارائه گردید (آغاز آن با ویندوز 98 همراه بوده است). تکنولوژی WSH ، امکان دستیابی به پوسته ویندوز ، سیستم فایل ، ریجستری و سایر موارد دیگر را با استفاده از کدهای ساده اسکریپت فراهم می نماید(پتانسیل های فوق در جهت اتوماسیون عملیات ویندوز ارائه شده است). اسکریپت ها می توانند مستقیما" از طریق Desktop و با کلیک نمودن بر روی یک فایل اسکریپت و یا از طریق یک برنامه اجراء گردند(نظیر یک برنامه سرویس گیرنده پست الکترونیکی) .

ویژگی اجراء اتوماتیکWSH ، عامل اصلی عرضه و انتشار کرم ILOVEYOU (کد نوشته شده توسط VBScript) در سالیان گذشته بوده که باعث میلیونها دلار خسارت گردید.کرم فوق و سایر کرم هائی که پس از آن مطرح گردیدند ، بمنظور نیل به اهداف مخرب خود از مزایای

WSH استفاده نموده اند . بدین ترتیب، امکان اجرای هر نوع فایل متنی با انشعاب vbs,.vbe, .js, .jse . وwsf . ،بعنوان یک اسکریپت ویژوال بیسیک و یا Jscript با مجوزهای سطح سیستم و یا برنامه ، فراهم می گردد .

1-8-4 سیستم های عامل در معرض تهدید

WSH ، می تواند بصورت دستی و یا از طریق IE (نسخه پنج به بعد) ، بر روی ویندوز NT و 95 نصب گردد .درویندوز ME , 98 , 98SE , 2000 , XP و 2003 ، WSH بصورت پیش فرض نصب می گردد . برای دریافت آخرین نسخه Windows Scrpt می توان از آدرس Windows Script Download استفاده نمود .

2-8-4 نحوه تشخیص آسیب پذیر ی سیستم

- سیستم هائی که بر روی آنان ویندوز 95 و یا NT بهمراه نسخه IE 5.5 نصب شده است .
- سیستم هائی که بر روی آنان ویندوز 98، ME ، 2000, XP و یا 2003 نصب شده است.

در صورتیکه WSH بر روی سیستم نصب و رفتار آن کنترل شده نباشد ، سیستم در معرض آسیب قرار خواهد داشت . در این رابطه لازم است که بررسی لازم در خصوص سیستم هائی که WSH بر روی آنان نصب شده است را انجام و در ادامه با استفاده از روش هائی که دربخش بعد به آنان اشاره خواهد شد ، از یک راهکار منطقی بمنظور حفاظت در مقابل آن استفاده گردد..

3-8-4 نحوه حفاظت در مقابل نقطه آسیب پذیر

در ابتدا لازم است به این نکته مهم اشاره گردد که برخی برنامه ها وعملیات مدیریتی، نیازمند استفاده از WSH بوده و در صورت غیر فعال نمودن و یا حذف پتانسیل فوق ، برنامه های فوق با اشکال مواجه خواهند شد .

غیرفعال نمودن WSH

تکنولوژی WSH ، بخشی اختیاری از سیستم عامل ویندوز بوده و می توان با اطمینان و بدون نگرانی خاصی آن را در موارد متعددی از روی کامپیوترها ، حذف و یا غیر فعال نمود.پیشنهاد می گردد ، بمنظور حفاظت در مقابل حملات و مسائل امنیتی مرتبط با WSH ، پتانسیل فوق غیر فعال گردد (در مواردیکه به عملکرد آن بر روی سیستم نیاز نمی باشد)

.

برنامه Noscript.exe ، ارائه شده توسط Symantec ، سرویس WSH را با تغییر نام فایل کلاس های مربوط به هر کلاسی که دارای Wscript.exe و یا Cscript.exe در کلید های ریجستری Shell\Open2\Command و یا Shell\Open\Command است ، غیر فعال می نماید.بدین ترتیب ، پیشگیری لازم در خصوص اجرای تمامی اسکریپت ها صرفنظر از اهداف مثبت و یا منفی آنان ، انجام خواهد شد . بمنظور نصب برنامه Noscript.exe مراحل زیر را دنبال می نمائیم :

- دریافت برنامه Noscript.exe از سایت Symantec

- پس از اجراء برنامه Noscript (برنامه Norton Script Disabler/Enabler ، نمایش داده می شود) با توجه به آخرین وضعیت WSH (فعال و یا غیر فعال) ، امکان فعال و یا غیر فعال نمودن آن فراهم می گردد.

تغییر در رفتار پیش فرض WSH

بمنظور حفاظت و پیشگیری لازم در خصوص عملکرد WSH در جهت انجام پردازش های اتوماتیک Desktop و مدیریتی با لحاظ نمودن تهدیدات و مسائل ایمنی ، می توان رفتار پیش فرض ویندوز را در ارتباط با فایل های اسکریپت (فایل هائی با انشعاب vbs, .vbe, .js, jse, .wsf .) ، تغییر داد. . نحوه برخورد پیش فرض ویندوز با فایل ها ی اسکریپت ، مشابه فایل های استاندارد اجرائی ویندوز بوده (فایل های با انشعاب EXE. و یا COM.) و بلافاصله آنان اجراء خواهند شد . با تغییر تنظیمات و پیکربندی انجام شده می توان امکان اجرای اتوماتیک اسکریپت های WSH را حذف تا اطمینان لازم در خصوص عدم فعال شدن اسکریپت های غیر مجاز ، فراهم نمود .در چنین مواردی پس از فعال شدن فایل حاوی اسکریپت ، فایل مورد نظر در مقابل اجرای اتوماتیک در یک ادیتور متنی نمایش داده خواهد شد . بدین ترتیب ، کاربران می توانند پس از اطمینان از صحت اسکریپت های نوشته شده ، تصمیم لازم در خصوص اجرای آنان را اتخاذ نمایند . بنابراین ، عرصه برای اسکریپت هائی که سعی در تهدید و آسیب سیستم را دارند ، محدود و در عین حال کنترل شده می گردد.

اسکریپت های مجاز WSH ، همچنان امکان اجراء را خواهند داشت . بدین منظور می توان نام فایل حاوی

اسکریپت را بعنوان آرگومان برنامه های cscript.exe و یا wscript.exe تعریف و مشخص نمود .

cscript.exe myscript.vbs

wscript.exe myscript.vbs

بمنظور کسب اطلاعات بیشتر در رابطه با نحوه حذف و یا غیر فعال نمودنWSH می توان از آدرس http://www.symantec.com/avcenter/venc/data/win.script.hosting.html استفاده نمود .

آنتی ویروس ها

پیشنهادمی گردد که برنامه آنتی ویروس بهنگام شده ای در gatways ، سرویس دهندگان و میزبانان ، نصب گردد.(علاوه بر غیر فعال نمودنWSH) . بدین ترتیب، می توان با استفاده از پتانسیل های ارائه شده توسط نرم افزارهای فوق ، برخورد لازم در ارتباط با نامه های الکترونیکی که دارای ضمائم حاوی اسکریپت های مخرب بمنظور انتشار ویروس ها و کرم ها می باشند را انجام داد(نظیر فایل های .vbs, .vbe, .js, .jse, .wsf, .bat, .exe , pif and .scr.). مثلا" برنامه Norton AntiVirus 2001 به بعد، امکان Script Blocking را ارائه که می تواند میزبانان را در مقابل ویروسهای مبتنی بر WSHحفاظت نماید .

بهنگام سازی موتور (هسته) اسکریپت

WSH طی سالیان اخیر ، بدفعات ارتقاء یافته است .آخرین نسخه آن را می توان از آدرس Windows Download Script دریافت نمود .

مجوزهای NTFS

از مجوزهای دستیابی NTFS می توان بمنظور تعریف سطح دستیابی قابل دسترس برای wscript.exe و jscript.exe در ارتباط با کاربران و یا گروه هائی ازکاربران بهمراه account های معتبر ویندوز،استفاده نمود . زمانیکه یک دایرکتوری و یا فایل به اشتراک گذاشته می شود ، تنظیمات پیش فرض دستیابی برای دایرکتوری ها و فایل های NTFS ، بصورت Full Control و برای گروه Everyone که شامل تمامی کاربران می باشد ، در نظر گرفته می شود. بدین ترتیب ، تمامی کاربران دارای مجوز لازم در خصوص اصلاح ، انتقال وحذف فایل ها و یا دایرکتوری ها ، می باشند.تنظیمات پیش فرض فوق برای wscript.exe و cscript.exe مناسب نمی باشند . ایمن سازی فایل ها و فولدرها شامل حذف کاربران و گروه هائی است که ضرورتی در رابطه با دستیابی به منابع را ندارند . بمنظور تغییر مجوزهای NTFS در ارتباط با یک دایرکتوری و یا فایل مراحل زیر را دنبال می نمائیم :

- فعال نمودن My Computer ، انتخاب درایو ، دایرکتوری و یا فایلی که قصد ایمن سازی آن وجود داشته باشد.
- فعال نمودن صفحه Property مربوط به شی انتخاب شده (درایو ، دایرکتوری ، فایل)
- در بخش Security صفحه خصایص ، Account مورد نظری که قصد تغییر مجوزهای مرتبط با آن وجود دارد را انتخاب می نمائیم .

- در بخش Permission ، نوع دستیابی را برای کاربر و یا گروه مربوطه مشخص می نمائیم .گزینه Allow امکان دستیابی و Deny عدم دستیابی در ارتباط با یک مجوز (خواندن ، نوشتن و ...) را مشخص می نماید .

در صورتیکه در صفحه Property مربوط به فایل ، درایو و یا دایرکتوری ، Security tab مشاهده نمی گردد ، سیستم فایل کامپیوتر میزبان بصورت NTFS پیکربندی نشده است . بمنظور تبدیل سیستم فایل به NTFS ، می توان از دستور Convert استفاده نمود (convert drive_letter: /fs:ntfs) . بمنظور کسب اطلاعات بیشتر در خصوص نحوه تنظیم مجوزهای NTFS ، برای یک دایرکتوری و یا فایل می توان از آدرس http://www.microsoft.com/windows2000/en/server/iis/htm/core/iidfpsc.htm استفاده نمود .

هشتمین نقطه آسیب پذیر : Outlook , Outlook Microsoft Express

برنامه Outlook (بخشی از مجموعه نرم افزارهای آفیس) ، یک مدیر اطلاعات شخصی و سرویس گیرنده پست الکترونیکی ارائه شده توسط مایکروسافت است . برنامه فوق ، علاوه بر ارائه خدمات اولیه مرتبط با یک برنامه پست الکترونیکی ، امکان مدیریت تماس ها ، فعالیت ها و زمان را نیز فراهم می نماید .در صورت ارتباط Outlook با برنامه Server Exchange (سرویس دهنده پست الکترونیکی ارائه شده توسط مایکروسافت) ، توانائی و پتانسیل های آن مضاعف می گردد. حمایت از چندین کاربر

، ارائه تسهیلات لازم در خصوص تنظیم قرار ملاقات ، زمان ، اشتراک تقویم و صندوق پستی ، نمونه هائی از پتانسیل های موجود در این زمینه می باشند .

OE (Express Outlook) ، نخسه ای رایگان و با قابلیت های کمتر نسبت به Outlook بوده که همزمان با ارائه IE نسخه یک ، بهمراه آن بر روی سیستم نصب می گردد (از زمان معرفی ویندوز 95 ، همواره بعنوان یک بخش لاینفک مطرح بوده است) . با تلفیق محصولاتی نظیر IE و OE در سایر نرم افزارهای تولیدی مایکروسافت نظیر Backoffice ، آفیس و سایر نسخه های سیستم عامل ویندوز ، امکان استفاده از تکنولوژی های متداول و کد مربوطه بین پلات فرم، فراهم می گردد . بعنوان نمونه ، برنامه OutLook 98 مشابه Outlook Express از پارسینگ HTML مربوط به IE و موتور rendering استفاده می نماید . بنابراین در صورت نصب Outlook 98 (بدون نسخه چهار و یا بالاتر) ،امکان نصب برنامه IE نیز فراهم خواهد شد . استفاده از رویکرد فوق ، دستاوردهای مثبتی همچون :استفاده موثرتر از کد را بدنبال خواهد داشت ولی با توجه به استفاده مشترک از عناصر موجود ، در صورت بروز اشکال در یک نقطه ، دامنه آن گریبانگیر محصولات متعددی خواهد شد. مثلا" در صورت وجود یک ضعف امنیتی در یک عنصر خاص ، ضعف موجود بسرعت گسترش و زمینه سوء استفاده از آن در یک محدوده وسیعتر در اختیار مهاجمان قرار خواهد گرفت .قطعا" در چنین شرایطی نگهداری یک محیط عملیاتی ایمن و مطمئن ، چالش های خاص خود را بدنبال خواهد داشت .

یکی از اهداف مایکروسافت ، پیاده سازی یک راه حل

مناسب بمنظور مدیریت اطلاعات و نامه های الکترونیکی با قابلیت استفاده مجدد بوده است. ویژگی های اتوماتیک ارائه شده با کنترل های امنیتی ایجاد شده در تعارض بوده و این موضوع می تواند زمینه بروز تهدیدات و خطراتی را از ناحیه ویروس های مبتنی بر نامه های الکترونیکی ، کرم ها و کدهای مخرب بدنبال داشته باشد .

سیستم های عامل در معرض تهدید

OE ، سرویس گیرنده نامه های الکترونیکی رایگان ارائه شده بهمراه تمامی نسخه های IE و ویندوز است . بمنظور آگاهی از نسخه نرم افزار OE ، پس از اجرای برنامه IE ، با فعال نمودن گزینه About از طریق منوی Help ، می توان از شماره نسخه نرم افزار فوق بر روی سیستم آگاهی یافت . نسخه های پایئن تر از پنج می بایست بلافاصله به نسخه جدید ارتقاء داده شوند.

OutLook ، یک مدیر اطلاعاتی با قابلیت های فراوان است که هم بعنوان یک برنامه جداگانه و هم بعنوان عضوی از خانواده آفیس ارائه می گردد . برنامه فوق بصورت اتوماتیک بر روی یک سیستم نصب نخواهد شد و می بایست در خصوص نصب آن ، تصمیم گیری گردد.(نصب پیش فرض جایگاهی ندارد) .

برنامه Outlook دارای نسخه های متعددی است :

- 5Outlook 9
- Outlook 97
- Outlook 2000 (به آن Outlook 9 نیز گفته می شود)

- Outlook XP (که به آن Outlook 10 و یا Outlook 2002 نیز گفته می شود)

با فعال نمودن گزینه About از طریق منوی Help ، (پس از اجرای برنامه IE) می توان از شماره نسخه برنامه OE نصب شده بر روی سیستم ، آگاهی یافت . نسخه های پائین تر از 2000 می بایست بسرعت patch و بهنگام گردند . در این رابطه می توان از منابع اطلاعاتی زیر استفاده نمود :

- http://www.microsoft.com/windows/oe/
- http://www.microsoft.com/office/outlook/

نحوه تشخیص آسیب پذیر ی سیستم

تمامی کامپیوترهائی که بر روی آنان سیستم های عامل ویندوز نصب و یا دارای یک نسخه از IE می باشند که بهمراه آن برنامه Outlook Express نیز نصب شده است ، در معرض آسیب قرار خواهند داشت . با استفاده از برنامه نصب مجموعه برنامه های آفیس ، می توان اقدام به نصب برنامه Outlook نمود . نسخه های ارائه شده OE و Outlook برای مکینتاش نیز دارای مسائل امنیتی خاص خود می باشند. در صورت عدم بهنگام سازی نسخه نصب شده و یا عدم رعایت تنظیمات امنیتی مربوطه ، سیستم در معرض تهدید قرار خواهد داشت .

نحوه حفاظت در مقابل نقطه آسیب پذیر

بمنظور حفاظت در مقابل نقطه آسیب پذیر فوق و کاهش تهدیدات موجود در این زمینه می باسیت عملیات مختلفی

را انجام داد:

ایمن سازی Outlook و Outlook Express

نصب و تنظیمات پیش فرض برنامه های Outlook و Outlook Express دارای ضعف امنیتی است . در این رابطه می بایست بررسی لازم در خصوص تنظیمات امنیتی انجام و از بهنگام بودن نسخه نصب شده مطمئن گردید. در اینخصوص موارد زیر پیشنهاد می گردد :

- استفاده مستمر از سایت http://windowsupdate.microsoft.com و نصب تمامی Patch های ارائه شده خصوصا" Critical (بحرانی)
- غیر فعال نمودن پانل نمایش اولیه (Preview) . با انتخاب گزینه Layout از طریق منوی View زمینه غیر فعال نمودن گزینه Show preview pane فراهم می گردد.
- مستحکمتر نمودن تنظیمات ناحیه امنیتی (Security zone) مرتبط با نامه های الکترونیکی . در این رابطه از طریق منوی Tools گزینه Options انتخاب و پس از کلیک نمودن بر روی Security Tab ، گزینه (sites zone(More secure Restricted انتخاب و مقدار موردنظر High در نظر گرفته شود.

آموزش کاربر ان

با توجه به نقش بسیار مهم عوامل انسانی در ارتباط با فرآیند ایمن سازی اطلاعات ، می بایست کاربران در رابطه با استفاده از نامه های الکترونیکی بدرستی آموزش و

توصیه های امنیتی لازم به آنان ارائه گردد. ذکر موارد زیر به کاربران ضروری می باشد :

- در زمان دریافت یک فایل ضمیمه ، حتی اگر منبع ارسال کننده آن مطمئن باشد ، می بایست در ابتدا و قبل از فعال نمودن آن ، بررسی لازم در خصوص ویروس های کامپیوتری انجام شود .
- در زمان دریافت یک فایل ضمیمه ، لازم است در ابتدا آن را در یک فولدر (غیر از My Documents) ذخیره نمود . (آدرس فوق ، توسط تعداد زیادی از ویروس ها بعنوان نقطه شروع یک تهاجم انتخاب می گردد) .در این راستا می توان فولدر دیگری و یا حتی ماشینی دیگر را انتخاب نمود (تفکیک مناسب فیل های ضمیمه دریافتی از سایر فایل های موجود بر روی کامپیوتر) .
- از فعال نمودن فایل های ضمیمه همراه یک نامه الکترونیکی خودداری شود. لازم است به این نکته مهم اشاره گردد که حتی فایل های DOC و یا XSL می توانند شامل کدهای مخربی باشند که سیستم را در معرض تهدید و آسیب قرار دهد.
- درصورتیکه لازم است فایل دریافتی با استفاده از سایر محصولات مایکروسافت فعال گردد (نظیر Word) ، می بایست مقدار High برای گزینه macro Disable درنظر گرفته شود.

آنتی ویروس

نرم افزارهای آنتی ویروس ، امکانات مناسبی را در خصوص حفاظت کامپیوترها در مقابل اکثر کرم ها ، ویروس ها و

سایر کدهای مخرب ، ارائه می نمایند . بانک های اطلاعاتی آنتی ویروس ها حداقل بصورت هفتگی بهنگام می گردند. بمنظور اطمینان از حفاظت در مقابل جدیدترین تهدیدات، اکثر برنامه های پیشرفته آنتی ویروس ، عملیات بهنگام سازی را بصورت اتوماتیک انجام می دهند. برنامه های جدید و پیشرفته آنتی ویروس دارای قابلیت بررسی و پویش تمامی نامه های وارده وصادره بمنظور اطمینان از بلاک نمودن فایل های شامل کد مخرب و یا اسکریپت ، قبل از تهدید سیستم ها توسط آنان می باشند. پیشنهاد می گردد ،ابزارهای حفاظتی آنتی ویروس قبل از استفاده از نامه های الکترونیکی و یا اینترنت ، بهنگام گردند. تعداد زیادی از ویروس ها وکرم ها از طریق سرویس گیرندگان نامه های الکترونیکی بصورت فایل های ضمیمه و یا کد اسکریپت مخرب، در زمان مشاهده Preview ،گسترش می یابند .بمنظور دستیابی به مرجع برنامه های آنتی ویروس در سایت مایکروسافت ، می توان از آدرس http://www.microsoft.com/security/protect/antivirus.asp استفاده نمود.

بهنگام سازی Outlook و Outlook Express .

برنامه Outlook Express طی سالیان اخیر بدفعات ارتقاء یافته است (با هدف افزایش قابلیت ها و ایمنی بالاتر) . بمنظور دریافت آخرین نسخه برنامه فوق، می توان از آدرس http://www.microsoft.com/windows/oe ، استفاده نمود. بمنظور اطمینان ازبهنگام بودن Outlook و سایر برنامه های آفیس می توان از آدرس Office Product Updates page استفاده نمود . سایت فوق بصورت اتوماتیک موارد بحرانی

را تشخیص و بهنگام سازی لازم وضروری را پیشنهاد می نماید . بمنظور آگاهی از جزئیات مربوط به سایر موارد ایمنی و تنظیمات مرتبط به نسخه آفیس XP ، می توان از آدرس XP Security white paper Office استفاده نمود . لازم است به این نکته مهم اشاره گردد که در صورتیکه سیستم شما بخشی از یک شبکه می باشد ، می بایست قبل از اعمال هر گونه تغییرات بر روی سیستم ، موضوع به اطلاع مدیریت سیستم رسانده شود. مدیران سیستم می توانند بمنظور آشنائی با جزئیات مربوط به بهنگام سازی امنیتی نامه های الکترونیکی در Outlook ، از Resource Kit Office استفاده نمایند .

Uninstall نمودن Outlook و Outlook Express

در صورتیکه از یک برنامه خاص دیگر بمنظور نامه های الکترونیکی و یا سرویس گیرنده مدیریت اطلاعات استفاده می گردد ، می توان اقدام به Uninstall نمودن برنامه های Outlook و Outlook Express از روی سیستم نمود:

- در صورت نصب Outlook بر روی تمامی نسخه های ویندوز می توان با استفاده از گزینه Add/Remove Program اقدام به Uninstall نمودن برنامه نمود.
- در صورت نصب Outlook Express بر روی ویندوز 98 و یا ME ، می توان با انتخاب آیکون Add/Remove Program و گزینه Windows Setup و انتخاب Outlook Express امکان حذف آن رافراهم نمود .
- در صورت نصب Outlook Express بر روی ویندوز 2000 و یا XP ، می توان با توجه به پیچیدگی عملیات

مربوطه از آدرس های زیر استفاده نمود :

- کاربران ویندوز 2000 که از نسخه Outlook Express Version 5.x/6.0 استفاده می نمایند ، می توانند از آدرس http://support.microsoft.com/default.aspx?scid=kb;EN-US;q263837 استفاده نمایند .
- کاربران ویندوز 98 و یا ME که از نسخه Outlook Expree Version 5.x/6.0 استفاده می نمایند ، می توانند از آدرس http://support.microsoft.com/default.aspx?scid=kb;EN-US;q256219 استفاده نمایند .

نهمین نقطه آسیب پذیر : (Windows Peer to Peer File Sharing (P2P

نقطه آسیب پذیر فوق ، با سایر موارد اشاره شده متفاوت بوده و این امکان را فراهم می نماید که برنامه های نظیر به نظیر ، بمنزله برنامه های User mode در نظر گرفته شوند . این نوع از برنامه ها در سالیان اخیر بسرعت رشد و مورد استفاده قرار می گیرند. از برنامه های فوق ، بمنظور Download و توزیع انواع متفاوتی از داده (موزیک ، ویدئو ، گرافیک ، متن ، code Source برنامه) استفاده می گردد . داده های مبادله شده از طریق برنامه های فوق اغلب مشکوک و دراکثر موارد قوانین کپی رایت بین المللی را نقض می نمایند. بر اساس گزارشات ارائه شده توسط Napster ، برنامه های فوق اغلب بصورت یک برنامه سرویس گیرنده توزیع و زمینه اشتراک فایل ها ، دایرکتوری ها و حتی تمامی فضای ذخیره سازی هارد دیسک را فراهم می نماید . کاربران با استفاده از برنامه های سرویس گیرنده ، پارامتر مورد

نظر خود برای جستجو را مشخص و در ادامه یک و یا چندین کانال ارتباطی بین شرکت کنندگان بعنوان نرم افزار سرویس گیرنده و ارتباط با سایر شرکت کنندگان در شبکه های دیگر بمنظور مکان یابی فایل های مورد نظر ایجاد می گردد. سرویس گیرندگان قادر به دریافت فایل از سایر کاربران بوده و می توانند داده های موجود بر روی سیستم خود را برای استفاده دیگران به اشتراک گذارند. فرآیند ارتباطات نظیر به نظیر شامل دریافت درخواست ها ، پاسخ به آنان و ارسال فایل ها می باشد . یک سرویس گیرنده (شرکت کننده) می تواند بطور همزمان چندین download را انجام و در همان زمان اقدام به انجام چندین upload نماید . جستجو برای یافتن محتوی می تواند شامل هر نوع رشته حرفی مورد نظر کاربر باشد . اکثر برنامه های فوق در حال حاضر از پورت های پیش فرض استفاده می نمایند ولی می توان بصورت اتوماتیک و یا دستی آن را بمنظور استفاده از پورت دیگر تنظیم نمود . سمت و سوی این تکنولوژی بسمت استفاده از http wrappers بوده که با ارائه تسهیلات لازم محدودیت های اعمال شده در سطح یک سازمان بمنظور استفاده از اینترنت را نادیده خواهد گرفت . با توجه به ماهیت multithread برنامه های فوق در ارتباط با جستجو و انتقال فایل ها ، ترافیک شبکه های LAN افزایش و حتی در موارد خاص امکان اشباع کامل لینک های WAN نیز وجود خواهد داشت . در زمان استفاده از برنامه های P2P ، سیتستم ها در معرض آسیب و تهدید جدی قرار خواهند گرفت . تهدیدات فوق ، می تواند باعث حملاتی از

نوع DoS ، دستیابی غیر مجاز به تمامی شبکه (بدلیل ضعف در پیکربندی سرویس گیرنده P2P) و بمخاطره انداختن اطلاعات محرمانه (هیچگونه محدودیتی دررابطه با نوع فایلی که به اشتراک گذاشته می شود ، وجود ندارد) گردد .در این رابطه مسائل قانونی (کپی رایت) مربوطه نیز وجود داشته که بطور جدی توسط شرکت های ارائه دهنده محصولات (صوتی ، تصویری ، نرم افزارهای کاربردی و ...) دنبال می گردد .محتوی ارائه شده از طریق برنامه های P2P شامل قانونی کپی رایت بوده (موزیک ، فیلم و برنامه) و استفاده کنندگان از این نوع برنامه ها می بایست به این موضوع مهم نیز توجه نمایند !

سیستم های عامل در معرض تهدید

از برنامه های P2P ، می توان در ارتباط با تمامی نسخه های موجود سیستم عامل ویندوز استفاده نمود(نسخه های متعددی بمنظور نصب بر روی ویندوز نوشته شده است) . البته در این رابطه نسخه های مربوط به سیستم های عامل یونیکس و لینوکس نیز وجود داشته و آنان نیز در معرض این تهدید می باشند .

نحوه تشخیص آسیب پذیر ی سیستم

تشخیص استفاده از برنامه های P2P بر روی شبکه ، چالش های خاص خود را بدنبال خواهد داشت .دراین رابطه موارد زیر پیشنهاد می گردد :

- مانیتورینگ ترافیک شبکه بر روی پورت های متداول استفاده شده توسط این نوع از برنامه ها

- جستجو ترافیک شبکه برای application layer strings که عموما" توسط برنامه های P2P استفاده می گردد.
- بررسی مکان های ذخیره سازی شبکه بمنظور کنترل محتوی download شده توسط کاربر (فایل های mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif, *.zip و *.exe *)
- مانیتورینگ فضاء ذخیره سازی شبکه برای کاهش ناگهانی ظرفیت آزاد دیسک

نحوه حفاظت در مقابل نقطه آسیب پذیر

بمنظور حفاظت در مقابل نقطه آسیب پذیر فوق ، می بایست عملیات متفاوتی را انجام داد :

سیاست شرکت / سازمان

- استفاده از یک سیاست معقول در ارتباط با downloading و قانون کپی رایت در هر سازمان
- استفاده از یک سیاست معقول در ارتباط با نحوه استفاده از اینترنت در هر سازمان
- بررسی مستمر فضای ذخیره سازی شبکه و ایستگاههای شبکه برای محتوی غیر مجاز

محدودیت شبکه

- کاربران معمولی نمی بایست قادر به نصب نرم افزار خصوصا" نرم افزارهای P2P باشند .
- استفاده از یک سرویس دهنده پروکسی بمنظور کنترل دستیابی به اینترنت

- فیلتریتگ (خروجی / ورودی) پورت ها ی استفاده شده توسط برنامه های P2P
- مانیتورینگ شبکه خصوصا" در ارتباط با ترافیک P2P
- استفاده روزانه از نرم افزارهای آنتی ویروس بهنگام شده

پورت های متدوال استفاده شده توسط برنامه های P2P :

- برنامه Napsster (پورت های TCP شماره : 8888 ، 8875 ، 6699)
- برنامه eDonkey (پورت های TCP شماره 4661 ، 4662 ، 4665)
- برنامه Gnutella (پورت های TCP/UDP شماره 6345 ، 6346 ، 6347)
- برنامه Kazza (پورت TCP شماره هشتاد برای www ، و پورت TCP/UDP شماره 1214)

دهمین نقطه آسیب پذیر : (Simple Network Management Protocol) SNMP)

از پروتکل SNMP بمنظور کنترل ، مانیتورینگ از راه دور و پیکربندی تمامی دستگاه های پیشرفته مبتنی بر TCP/IP استفاده می شود.با اینکه استفاده از SNMP در بین پلات فرم های متفاوت شبکه استفاده می گردد، ولی در اغلب موارد از آن بمنظور پیکربندی و مدیریت دستگاههائی نظیر چاپگر ، روترها ، سوئیچ ها ، Access point ها و دریافت داده های مورد نیاز دستگاههای

مانیتورینگ شبکه ، استفاده می شود .
SNMP ، از روش های متفاوتی بمنظور مبادله پیام بین ایستگاههای مدیریت SNMP و دستگاههای شبکه ای استفاده می نماید . روش های استفاده شده بمنظور برخورد با پیام های مبادله شده و مکانیزم تائید و معتبر سازی پیا م ها، از جمله عوامل اصلی در رابطه با نقاط آسیب پذیر SNMP می باشند .
نقاط آسیب پذیر مرتبط با روش های استفاده شده در SNMP (نسخه یک) بهمراه جزئیات مربوطه را می توان در آدرس CERT – 2002 – 03 ، مشاهده نمود . نقاط آسیب پذیر متعددی در SNMP متاثر از روش برخورد با پیام ها توسط ایستگاه های مدیریتی است . نقاط آسیب پذیر فوق، به نسخه ای خاص از SNMP محدود نبوده و محصولات متعدد ارائه شده توسط تولید کنندگان را نیز شامل می گردد .
مهاجمان با استفاده از نقاط آسیب پذیر فوق ، قادر به انجام حملات متفاوت از نوع DoS (از کار افتادن یک سرویس) تا پیکربندی و مدیریت ناخواسته ماشین آلات و تجهیزات مبتنی بر SNMP ، می باشند .
برخی از نقاط آسیب پذیر در ارتباط با SNMP متاثر از روش های استفاده شده بمنظور تائید و معتبر سازی پیام ها در نسخه های قدیمی SNMP است (توارث مشکلات) .
نسخه های یک و دو SNMP ، از یک " رشته مشترک " غیررمز شده بعنوان تنها گزینه موجود برای تائید پیام ها استفاده می نمایند . عدم استفاده از روش های مناسب رمزنگاری ، می تواند عاملی مهم در پیدایش نقاط آسیب پذیر باشد. نگرش پیش فرض نسبت به " رشته

مشترک " که توسط تعداد زیادی از دستگاههای SNMP استفاده می گردد ، از ذیگر عوامل مهم در ارتباط با عرضه نقاط آسیب پذیر است(برخی از تولید کنندگان بمنظور افزایش سطح ایمنی مربوط به داده های حساس ، رشته را بصورت "اختصاصی " تغییر و استفاده می نمایند) . شنود اطلاعاتی و ترافیک SNMP ، می تواند افشاء اطلاعات و ساختار شبکه (سیستم ها و دستگاههای متصل شده به آن) را بدنبال داشته باشد . مهاجمین با استفاده از اطلاعات فوق ، قادر به انتخاب مناسب و دقیق هدف خود بمنظور برنامه ریزی حملات خود می باشند .
اکثر تولید کنندگان بصورت پیش فرض نسخه یک SNMP را فعال و تعدادی دیگر، محصولاتی را ارائه می نمایند که قادر به استفاده ازمدل های امنیتی نسخه شماره سه SNMP نمی باشند. (با استفاده از مدل های امنیی ارائه شده در نسخه شماره سه SNMP ، می توان پیکربندی لازم در خصوص روش های تائید را بهبود بخشید) .

SNMP ، بصورت پیش فرض در ویندوز فعال نمی گردد .و اغلب بعنوان یک سرویس تکمیلی توسط مدیر یت سیستم و یا شبکه ، نصب می گردد . سایر محصولات مدیریت شبکه ممکن است مستلزم Windows Service و یا نصب مربوط به خود باشند . SNMP یک روش ارتباطی استفاده شده بمنظور مدیریت چاپگرها ، سیستم های UPS ، دستگاه های point access و Bridges است . از SNMP اغلب در نسخه های متفاوت یونیکس و لینوکس نسخه های متفاوت سیستم عامل نت ور ، تجهیزات شبکه ای و دستگاههای embedded استفاده می شود. با توجه به نتایج حاصل از آنالیز حملات مبتنی

بر SNMP ، مشخص شده است که اکثر حملات در این رابطه بدلیل ضعف در پیکربندی SNMP در سیستم های یونیکس است .

سیستم های عامل در معرض تهدید

تقریبا" تمامی نسخه های سیستم عامل ویندوز بهمراه یک گزینه نصب انتخابی در اینخصوص ارائه شده اند . سرویس فوق بصورت پیش فرض نصب و فعال نمی باشد. اکثر دستگاه ها و سیستم های عامل شبکه ای مبتنی بر SNMP دارای نقطه آسیب پذیر فوق بوده و در معرض تهدید قرار خواهند داشت .

نحوه تشخیص آسیب پذیری سیستم

بمنظور بررسی نصب SNMP بر روی دستگاههای موجود و متصل شده در شبکه ، می توان از یک برنامه کمکی و یا روش دستی استفاده نمود. برنامه پویشگر SNScan ، نمونه ای در این زمینه بوده که می توان آن را از طریق آدرس http://www.foundstone.com/knowledge/free_tools.html دریافت نمود.
در مواردیکه امکان استفاده از ابزارهای پویشگر وجود ندارد ، می توان بررسی لازم در خصوص نصب و اجراء SNMP را بصورت دستی انجام داد. در این راستا می توان به مستندات سیستم عامل مربوطه مراجعه تا پس از آگاهی از نحوه پیاده سازی SNMP ، عملیات لازم بمنظور تشخیص فعال بودن SNMP را انجام داد
در این رابطه می توان با بررسی اجراء سرویس در Services applet ، در لیست پردازه ها نسبت به این موضوع آگاه و یا با دستور " net stat " در خط دستور و یا با مشاهده و

جستجوی سرویس های اجرائی بر روی پورت های 161 و 162 با استفاده از دستور "netstat -an" این عملیات را انجام داد . در صورت تحقق یکی از شرایط زیر و نصب SNMP ، سیستم در معرض آسیب و تهدید قرار خواهد داشت :

- وجود اسامی SNMP Community پیش فرض و یا خالی (اسامی استفاده شده بعنوان رمزهای عبور)
- وجود اسامی SNMP Community قابل حدس
- وجود رشته های مخفی SNMP Community

نحوه حفاظت در مقابل نقطه آسیب پذیر

بمنظور حفاظت در مقابل نقطه آسیب پذیر فوق ،در دو زمینه می توان اقدامات حفاظتی را سازماندهی نمود .

حفاظت در مقابل درخواست های آسیب رسان و تهدید کننده :

- غیر فعال نمودن SNMP در صورت عدم ضرورت استفاده از آن
- استفاده از یک مدل امنیتی مبتنی بر کاربر SNMPv3 ، بمنظور تائید پیام ها و رمزنگاری داده ها (در صورت امکان)
- در صورت استفاده از SNMP نسخه یک و یا دو ، می بایست آخرین نسخه Patch ارائه شده توسط تولید کننده ، نصب گردد برای آگاهی از مشخصات تولیدکنندگان، می توان به بخش ضمیمه CERT Advisory CA-2002-03 ، مراجعه نمود .

- SNMP را در گلوگاه های ورودی شبکه فیلتر نمائید (پورت 161 مربوط به TCP/UDP و پورت 162 مربوطه به TCP/UDP) . عملیات فوق را در مواردیکه ضرورتی به مدیریت دستگاهها بصورت خارجی وجود ندارد ، می بایست انجام داد .
- از کنترل دستیابی مبتنی بر میزبان بر روی سیستم های SNMP agent استفاده گردد . ویژگی فوق ممکن است توسط SNMP agent سیستم های عامل دارای محدودیت هائی باشد ، ولی می توان کنترل لازم در خصوص پذیرش درخواست ها توسط agent مربوطه را انجام داد. در اکثر نسخه های ویندوز 2000 و به بعد از آن ، می توان عملیات فوق را توسط یک فیلتر IPSEC انجام داد . استفاده از یک فایروال فیلترینگ بسته های اطلاعاتی مبتنی بر agent بر روی یک میزبان نیز می تواند در بلاک نمودن درخواست های ناخواسته SNMP موثر واقع شود .

حفاظت در مقابل رشته های قابل حدس

- غیر فعال نمودن SNMP در صورت عدم ضرورت استفاده از آن
- استفاده از یک مدل امنیتی مبتنی بر کاربر SNMPv3 ، بمنظور تائید پیام ها و رمزنگاری داده ها (در صورت امکان)
- در صورت استفاده از SNMP نسخه یک و یا دو ، می بایست از یک سیاست خاص بمنظور اسامی community (استفاده شده بعنوان رمزهای عبور) استفاده گردد.

در این راستا لازم است اسامی بگونه ای انتخاب گردند که غیر قابل حدس بوده و بصورت ادواری و در محدوده های خاص زمانی نیز تغییر داده شوند .

- با استفاده از امکانات موجود می بایست بررسی لازم در خصوص استحکام اسامی در نظر گرفته شده برای رمزهای عبور راانجام داد.در این رابطه می توان از خودآموز و ابزار ارائه شده در آدرس http://www.sans.org/resources/idfaq/snmp.php ، استفاده کرد.
- SNMP را در گلوگاه های ورودی شبکه فیلتر نمائید (پورت 161 مربوط به TCP/UDP و پورت 162 مربوطه به TCP/UDP) . عملیات فوق را در مواردیکه ضرورتی به مدیریت دستگاهها بصورت خارجی وجود ندارد ، می بایست انجام داد . پیکربندی فیلترینگ را صرفا" بمنظور ترافیک مجاز SNMP بین subnet های ممیزی شده ، انجام دهید.

دفاع در مقابل کرم ها و ویروس ها

5 مهر 82 – srco - کرم ها و ويروس ها نوع خاصي از برنامه هاي كامپيوتري موسوم به " كد مخرب " مي باشند. علت ظهور كرم ها و ويروس ها ، وجود ضعف در برنامه ها ي كامپيوتري است . آنان نسخه هائي از خود را تكرار و يا به ساير برنامه ها متصل، بسرعت گسترش و بسادگي از سيستمي به سيستم ديگر توزيع مي شوند.درابتدا لازم است كه تعريف مناسبي براي هر يک از آنان ارائه گردد .

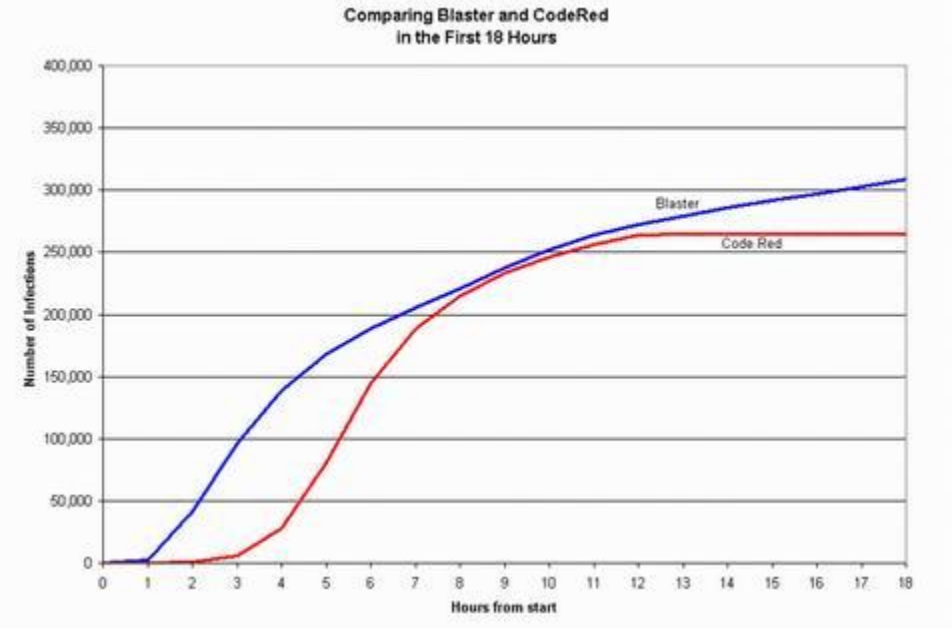
كرم ها ، نوع خاصي ازبرنامه هاي كامپيوتري مي باشند كه پس از آغاز فعاليت خود ، بدون مداخله انساني منتشر و توزيع خواهند شد. ويروس ها ، نوع ديگري از برنامه هاي كامپيوتري مي باشند كه بمنظور انتشار و توزيع خود نيازمند انجام عمليات خاصي توسط كاربر نظير فعال شدن فايل همراه يک نامه الكترونيكي مي باشند.كاربران در اغلب موارد و در مشاهده با فايل هاي ضميمه همراه نامه هاي الكترونيكي ، اغوا و بدون لحاظ نمودن مسائل امنيتي آنان را باز و به عاملي براي گسترش يک ويروس تبديل مي شوند. كاربران بدليل كنجكاوي مربوط به موضوع يک نامه و يا ظاهر شدن نامه بگونه اي كه براي مخاطب خود آشنا است ، اقدام به باز نمودن ضمائم يک نامه الكترونيكي مي نمايند. كرم ها و ويروس مي توانند اقدامات پيشگيرانه امنيتي نظير فايروال ها و سيستم هاي حفاظتي را ناديده و اهداف خود را دنبال نمايند.

كرم ها و ويروس ها در مقايسه با گذشته با سرعت بمراتب بيشتري اقدام به خرابي سيستم هاي آسيب پذير نموده و در اين راستا نسخه هائي از خود را براي اكثر سيستم هاي فوق ، توزيع و منتشر مي نمايند. كامپيوترهاي موجود در منازل ، نمونه مناسبي از سيستم هاي آسيب پذير بوده كه شرايط و استعداد مناسبي را در اين رابطه دارند.

كرم Code Red در سال 2001 بسرعت در سطح جهان منتشر گرديد . سرعت انتشار كرم فوق، بمراتب بيشتر از كرم Morris در سال 1988 و ويروس مليزا در سال 1999 بود. بديهي است، افزايش سرعت انتشار اين نوع از كدهاي مخرب ، سرعت در بروز خرابي و آسيب را بدنبال خواهد داشت . مثلا" فاصله زماني بين شناسائي اولين نسخه كرم Code Red و خرابي گسترده آن ، صرفا" چندين روز بيشتر نبوده است و دراين فاصله زماني محدود، Code Red بسرعت اشاعه و گسترش پيدا كرده بود. پس از گذشت يک ماه از ظهور كرم Red Code ، كرم ديگري با نام "نيمدا" توانست در اولين ساعت فعاليت خود ، خرابي بسيار گسترده اي را ايجاد نمايد . در ژانويه همان سال ، " اسلامر" توانست صرفا" در مدت چندين دقيقه خرابي گسترده اي را بوجود آورد .

شكل زير،سرعت انتشار و ميزان آسيب رساني " اسلامر" ، بلستر و Code red در اولين روز فعال شدن را نشان مي دهد . همانگونه كه مشاهده مي شود ، اسلامر توانسته است با سرعت بيشتري در اولين ساعات فعال شدن خود ، تعداد زيادي از سيستم ها را آلوده نمايد. سرعت انتشار بلستر از اسلامر كندتر ولي از Code Red سريعتر بوده است . پس از گذشت بيست و چهار ساعت، بلستر به 336،000 ، . Code Red به 265،000 و اسلامر به 55،000 دستگاه كامپيوتر آسيب رسانده بودند. دقت داشته باشيد كه بلستر در هيجده ساعت اوليه فعاليت خود تواسنه است بيش از 336،000 كامپيوتر را آلوده نمايد. بلستر نسبت به اسلامر توانسته است عليرغم كند بودن انتشار در ساعات اوليه ، تعداد بمراتب بيشتري از سيستم ها را آلوده نمايد . بنابراين ، ما از يكطرف سرعت در انتشار و از طرف ديگر افزايش بالاي تعداد سيستم هاي آسيب پذير را مي توانيم مشاهده نمائيم .

شكل زير، عملكرد كرم بلستر و Code Red در هيجده ساعت اوليه فعاليت آنان را نشان مي دهد. در هر دو حالت در ساعات بين سه تا پنج اوليه فعاليت ، نزديک به 100،000 كامپيوتر آلوده شده بود. سرعت انتشار و آسيب به اندازه اي سريع بوده است كه اغلب مديران سيستم و كاربران زمان لازم بمنظور ايمن سازي سيستم ها پس از اعلام ضعف امنيتي را نداشته اند .



عملكرد كرم ها و ويروس ها

در بهترين حالت ، كرم ها و ويروس ها بمنزله مزاحميني مي باشند كه بمنظور برخورد با آنان مي بايست هزينه هاي زيادي صرف گردد . در بدترين حالت ، آنان بمنزله دشمنان خانمان سوزي بوده كه قادرند سرمايه هاي اطلاعاتي را نابود و ويران نمايند. بر اساس گزارشات منتشر شده ، صرفا" در دوازده ماه گذشته ، حملات كرم ها و ويروس ها ميليون ها دلار خسارت را متوجه سازمان ها و موسسات نموده است .
براساس نظر سنجي انجام شده توسط CSI/FBI در سال 2003 ، بيش از هشتاد و دو درصد از پاسخ دهندگان با نوع خاصي از حملات توسط ويروس ها و كرم ها برخورد داشته كه هزينه اي معادل 27،382،340 دلار صرف برطرف نمودن مشكلات مربوطه شده است . كمترين هزينه گزارش شده 40،000

دلار و بيشترين هزينه گزارش شده بالغ بر 6،000،000 دلار بوده است . در يک نظر سنجي ديگر و در استراليا نيز نتايجي مشابه بدست آمده است . در اين نظر سنجي بيش از هشتاد درصد از پاسخ دهندگان با نوع خاصي از حملات توسط کرم ها و يا ويروس ها مواجه بوده اند . در بررسي انجام شده توسط موسسه تحقيقاتي استراليا ، 33 % درصد از پاسخ دهندگان اعلام نموده اند که مشکل آنان در کمتراز يک روز ، 30 % اعلام نموده اند که مشکل آنان بين يک تا هفت روز و 37 % ديگر اعلام نموده اند که بيش از يک هفته صرف برطرف نمودن مشکل آنان شده است . (برخي از سازمان ها و موسسات نيز اعلام نموده اند که مشکل آنان هرگز برطرف نشده است) .
ميزان صدمات وخرابي گزارش شده در ارتباط با کرم بلستر، بالغ بر 525 ميليون دلار و در ارتباط با سوبيگ (نوع F) ، بين 500 ميليون تا يک ميليارد دلار برآورد شده است.هزينه فوق ، شامل ازدست دادن بهره وري ، ساعات تلف شده ، عدم فروش کالا و يا خدمات و هزينه هاي اضافي مربوط به پهناي باند است . بر اساس اظهارات ارائه شده در نشريه اکونوميست 23 اگوست 2003 ، سوبيگ (نوع F)، مسئول يکي از شانزده نامه الکترونيکي ارسال شده بر روي اينترنت بوده است . برخي سازمان هاي بزرگ ، صرفا" طي يک روز بيش از 10،000 نامه الکترونيکي آلوده را دريافت نموده اند (در هر 6. 8 ثانيه ، يک پيام) . سوبيگ ، قادر به ارسال چندين نامه الکترونيکي در يک زمان بود و بدين ترتيب ضريب نفوذ و اشاعه آن بشدت بالا بود . (هزاران پيام در يک دقيقه) . با توجه به اينکه، سوبيگ چندين مرتبه تغيير و نسخه هاي جديدتري از آن ارائه مي شد، برخورد و غير فعال نمودن آن با مشکل مواجه مي گرديد . (حرف F نشاندهنده نسخه شماره شش سوبيگ است) .

وضعيت آينده

نتايج و تجارب کسب شده ، صرفا" محدود به عملکرد خاص برخي از کرم ها و ويروس ها نظير بلستر و سوبيگ بوده و ما مي بايست به اين واقعيت مهم توجه نمائيم که کرم ها و ويروس ها يک تهديد جدي در رابطه با امنيت اينترنت بوده و مي توانند مسائل متعدد و غيرقابل پيش بيني را در آينده براي هر يک از شهروندان حقوقي و يا حقيقي اينترنت بدنبال داشته باشند .بنابراين مي توان اين ادعا را داشت که اينترنت نه تنها در حال حاضر در مقابل اينگونه حملات آسيب پذير است بلکه آسيب پذيري آن در آينده نيز قابل پيش بيني و واقعيتي غيرقابل کتمان است. کامپيوترهاي موجود در سازمان ها ، موسسات دولتي و خصوصي ، مراکز تحقيقاتي ، مدارس ، دانشگاه ها در حال حاضر نسبت به ضعف هاي امنيتي کشف شده آسيب پذير بوده و قطعا" نسبت به ضعف هائي که در آينده مشخص مي گردند، نيز آسيب پذيري خود را خواهند داشت . بنابراين ، سيستم هاي کامپيوتري هم در مقابل حملات در حال حاضر و هم براي حملات در آينده ، داراي استعداد لازم بمنظور پذيرش آسيب خواهند بود. بديهي است ، همزمان با افزايش وابستگي سازمان ها و موسسات دولتي و خصوصي به اينترنت ، انجام فعاليت هاي تجاري، تهديدات و خطرات خاص خود را بدنبال خواهد داشت .

محدوديت راه حل هاي واکنشي

پس از گذشت قريب به پانزده سال از عموميت يافتن اينترنت و مطالعات گسترده انجام شده بمنظور کاهش خطرات ، خرابي و سرعت در تشخيص و غلبه بر حملات ، مي توان اين ادعا را نمود که راه حل هاي واکنشي به تنهائي کافي نخواهند بود. ادعاي فوق ، ماحصل توجه به عوامل زير است :

• اينترنت در حال حاضر بيش از 171،000،000 کامپيوتر را بيديگر متصل و رشد آن همچنان ادامه دارد . در حال حاضر ، ميليون ها کامپيوتر آسيب پذير در اينترنت وجود دارد که مستعد يک نوع خاص از حملات توسط مهاجمين مي باشند.

• تکنولوژي حملات بسيار پيشرفته شده و مهاجمان مي توانند با اتکاء بر آخرين فنآوري ها ي موجود ، بسادگي از نقاط ضعف موجود در سيستم هاي آسيب پذير استفاده و به آنان آسيب مورد نظر خود را برسانند(حملات مبتني بر آخرين تکنولوژي موجود).

• تعداد زيادي از حملات در حال حاضر بصورت کاملا" اتوماتيک عمل نموده و با سرعت بسيار بالائي در اينترنت و صرفنظر از منطقه جغرافيائي ويا محدوديت هاي ملي ، توزيع و گسترش مي يابند.

• تکنولوژي بکارگرفته شده در حملات بسيار پيچيده و در برخي موارد تعمد پنهاني در آنان دنبال مي گردد . بنابراين ، کشف و آناليز مکانيزمهاي استفاده شده بمنظور توليد پادزهر و برطرف نمودن مشکل ، مستلزم صرف زمان زيادي خواهد بود .

• کاربران اينترنت وابستگي زيادي به اينترنت پيدا کرده و از آن بمنظور انجام کارهاي حياتي خود نظير: فعاليت هاي تجاري Online استفاده مي نمايند. کوچکترين وقفه در ارائه خدمات مي تواند ازدست دادن منابع اقتصادي و بمخاطره افتادن سرويس هاي حياتي را بدنبال داشته باشد .

توجه به هر يک از موارد اشاره شده ، شاهدي است بر اين ادعا که ما همچنان در معرض طيف گسترده اي از حملات قرار گرفته ايم . حملاتي که از دست دادن منابع اقتصادي و عدم امکان عرضه سرويس ها را

بدنبال خواهد داشت .در اين راستا مي بايست از تمامي امكانات و پتانسيل هاي موجود بمنظور سرعت در پاسخ و برخورد با حملات استفاده نمود. بازنگري در راه حل ها ي موجود و استفاده از رويكردهاي علمي و جامع مي تواند عاملي موثر در جهت برخورد مناسب با حملات باشد.

وظايف مديران سيستم

شناسائي تهديدات كرم ها و ويروس ها عمليات ساده و ايستائي نبوده و در اين رابطه مي بايست از رويكردهاي كاملا" پويا و مبتني بر آخرين دستاوردهاي تكنولوژي استفاده گردد. با كشف بيش از چهار هزار نوع نقطه آسيب پذير در طي هر سال ، مديران سيستم و شبكه در وضعيت دشواري قرار دارند . آنان با چالش هاي جدي در ارتباط با تمامي سيستم ها ي موجود و Patch هاي مورد نظر كه براي برطرف نمودن نقايص امنيتي ارائه مي گردد ، مواجه مي باشند .

استفاده و بكارگيري Patch ها ي ارائه شده در عين مفيد بودن بمنظور مقابله با مشكل امنيتي ايجاد شده ، مي تواند زمينه بروز مسائل و اثرات جانبي غيرقابل پيش بيني را فراهم نمايد . در اين رابطه لازم است به اين نكته مهم نيز اشاره گردد كه پس از ارائه يک Patch امنيتي ، مدت زمان زيادي طول خواهد كشيد كه مديران سيستم و يا شبكه مشكل تمامي سيستم هاي آسيب پذير خود را برطرف نمايند. مدت زمان برطرف سازي مشكلات و اشكالات بوجود آمده در برخي موارد مي تواند ماه ها ويا حتي سالها پس از ارائه patch پياده سازي شده ،بطول مي انجامد . مثلا" هنوز گزاشاتي در رابطه با ويروس مليزا كه چهار سال از فعال شدن آن گذشته است ، توسط برخي سازمان ها و موسسات در سطح جهان ارائه مي گردد. ريشه كن نمودن يک كرم و يا ويروس شايع ، با توجه به گستردگي اينترنت ، عملياتي نيست كه در يک بازه زماني محدود، بتوان موفق به انجام آن گرديد ومي بايست براي نيل به موفقيت فوق ، زمان زيادي صرف گردد . شايد اين سوال مطرح گردد كه دلايل اينهمه تاخير در ريشه كن نمودن يک ويروس و يا كرم چيست ؟ در پاسخ مي توان به موارد متعددي نظير صرف زمان زياد ، پيچيدگي گسترده آنان و عدم اختصاص اولويت مناسب براي مقابله با آنان در يک سازمان و يا موسسه ، اشاره نمود.متاسفانه ، بسياري از مديران شناخت كامل و جامعي نسبت به تهديدات نداشته و هرگز به مقوله امنيت با يک اولويت سطح بالا نگاه نكرد و حتي منابع لازم را به اين مقوله اختصاص نمي دهند. علاوه بر اين ، سياست هاي تجاري در برخي موارد سازمان ها را بسمت انتخاب يكي از دو گزينه : اهداف تجاري و نيازهاي امنيتي هدايت كه در اكثر موارد رسيدن به اهداف تجاري داراي اولويت و جايگاه بالاتري براي آنان مي باشند. علاوه بر تمامي مسائل فوق، مي بايست به اين نكته مهم نيز اشاره گردد كه تقاضا براي مديران سيستم ورزيده و كارشناس بيش ازميزان موجود بوده و همين امر همواره استفاده از متخصصين و كارشناسان امنيتي را با مشكل جدي مواجه مي سازد(عدم توازن بين عرضه و تقاضا) .

بمنظور برخورد مناسب با وضعيت فوق ، مديران سيستم در يک سازمان مي توانند با دنبال نمودن مراحل زير عمليات لازم در جهت تسهيل در امر حفاظت سيستم هاي سازمان را انجام دهند:

• اتخاذ روش هاي امنيتي .انتخاب سيستم هاي ارزيابي امنيت اطلاعات ، مديريت سياست ها و تبعيت از روش هاي امنيتي براي تمامي سازمان ها (بزرگ و كوچک) امري حياتي است . سازمان ها و موسسات مي توانند بر اساس وضعيت موجود خود ، يكي از روش هاي مناسب امنيتي را انتخاب نمايند. در اين راستا مي توان از پتانسيل ها و تجارب بخش دولتي و يا خصوصي استفاده گردد. در اين رابطه مي توان از منابع متعدد اطلاع رساني موجود بمنظور اتخاذ سياست هاي كلي امنيتي استفاده و پس از بررسي آنان نسبت به تدوين و پياده سازي سياست امنيتي در سازمان مربوطه ، اقدام نمود.

• بهنگام نمودن دانش و اطلاعات . مديران سيستم مي بايست بمنظور ارتقاء سطح دانش و معلومات خود ، دوره هاي آموزشي خاصي را بگذرانند . شركت در دوره هاي آموزشي مستمر و اختصاص وقت لازم براي استفاده مفيد از دوره هاي آموزشي مي بايست در دستور كار مديران سيستم در سازمان ها و موسسات قرار گيرد . مديران سيستم لازم است ضمن آشنائي با آخرين تهديدات و حملات با ابزارهاي لازم در جهت افزايش حفاظت سيستم ها نيز شناخت مناسبي را پيدا نمايند .لازم است به اين نكته مهم اشاره گردد كه امنيت ، داراي ماهيتي كاملا" پويا بوده كه همزمان با بروز حملات جديد و شناسائي نقاط آسيب پذير جديد بصورت روزانه تغيير و ارتقاء مي يابد. با دانش استاتيک و محدود نمي توان با مقوله هاي پويا و گسترده برخوردي مناسب و علمي داشت .

• آموزش كاربراني كه از سيستم ها استفاده مي نمايند . مديران سيستم مي بايست برنامه هاي آموزشي خاصي را در رابطه با امنيت ، بمنظور ارتقاء دانش كاربران نسبت به مسائل امنيتي ، ارائه نمايند. دوره ها و برنامه هاي آموزشي مي بايست كاملا" هدفمند بوده و كاربران پس از شركت وگذراندن دوره هاي فوق ، به سطح مطلوبي از توانائي بمنظور تشخيص يک مسئله ، انجام عمليات لازم بمنظور افزايش حفاظت سيستم، برخورد مناسب در صورت مواجه با يک مشكل امنيتي دست پيدا كرده باشند . بمنظور پياده سازي سياست امنيتي در يک سازمان ،وجود كاربران آگاه با مسائل ايمني اطلاعات و حفاظت از

اطلاعات حساس ، امري ضروري و لازم است .

• وظايف ارائه دهندگان تكنولوژي

مديران سيستم با دنبال نمودن پيشنهادات ارائه شده، صرفا" قادر به حل بخش هائي از مسئله امنيت اطلاعات مي باشند. با توجه به جايگاه شركت هاي ارائه دهنده تكنولوژي، حركات و تدابير مثبت آنان مي تواند تاثير زيادي در جهت ممانعت و گسترش كرم ها و ويروس ها را بدنبال داشته باشد . با اينكه برخي شركت ها بسمت ارتقاء و بهبود امنيت در محصولات خود حركت نموده اند ، ولي هنوز راهي طولاني در پيش است . متاسفانه ، پياده كنندگان نرم افزار از تجارب گذشته در رابطه با نقايص امنيتي در ارائه نسخه ها ي جديد نرم افزار خود استفاده نمي نمايند. بر اساس مطالعات انجام شده ، مشاهده شده است كه برخي از نقاط آسيب پذير جديد در نسخه هاي جديد برخي محصولات در نسخه هاي قبلي هم وجود داشته و تلاش مناسبي در جهت بهسازي وضعيت امنيتي نسخه جديد صورت نگرفته است .

وجود برخي از نقاط آسيب پذير بدليل عدم پيكربندي ايمن سيستم هاي عامل و برنامه هاي كاربردي است . محصولات فوق ، بسيار پيچيده بوده و اغلب با غير فعال نمودن برخي از ويژگي ها ي امنيتي به مشتريان عرضه مي شوند .شركت هاي ارائه دهنده بر اين اعتقاد مي باشند كه همزمان با استفاده از محصول ارائه شده ، كاربران مي توانند ويژگي هاي امنيتي غير فعال شده را در زمان لازم و بدلخواه خود فعال نمايند. بدين ترتيب تعداد زيادي از سيستم هاي متصل شده به اينترنت داراي پيكربندي مناسب در رابطه با امنيت اطلاعات نبوده و شرايط مناسبي را براي نفوذ كرم ها و ويروس ها فراهم مي نمايند.

ارائه محصولاتي كه در مقابل كرم ها و ويروس ها نفوذناپذير باشند ، براي هر شركت ارائه كننده محصولات ،امري ضروري و حياتي است . اعتقاد به اين رويكرد امنيتي كه " كاربر مي بايست مواظب باشد " ، در عصر حاضر پذيرفتني نيست ، چراكه سيستم ها بسيار پيچيده بوده و سرعت حملات نيز باورنكردني است و در برخي موارد فرصت مناسب براي برخورد با نقص امنيتي از كاربر سلب مي گردد . توليد كنندگان محصولات مي توانند با اتكاء و استفاده از روش هاي مهندسي نرم افزار تلاش خود را در جهت توليد محصولات مقاوم در برابر حملات ، مضاعف نمايند . در اين راستا موارد زير پيشنهاد مي گردد :

• نرم افزار ضد ويروس / مقاوم در مقابل ويروس . كامپيوترها و نرم افزارها داراي امكانات ذاتي بمنظور ايمن شدن در مقابل تهديدات و حملات كرم ها و ويروس ها نمي باشند. طراحي كامپيوترها و يا نرم افزارهاي كامپيوتري بگونه اي است كه امكان توزيع و انتشار ويروس ها و آلودگي سيستم ها را فراهم مي نمايد. در برخي موارد طراحي انجام شده بگونه اي است كه شرايط لازم براي حملات و نفوذ كرم ها و ويروس ها را فراهم و استعداد فوق در بطن محصول ارائه شده وجود خواهد داشت . اجراء يک كد نامشخص و وارده از يک منبع ناشناس و گمنام نمونه اي از استعداد اشاره شده در بطن محصولات بوده كه امكان فعال شدن يک كد اجرائي بدون محدوديت و نظارت خاصي بر روي يک ماشين ، فراهم مي گردد.بدين ترتيب سيستم در مقابل حملات ويروس ها آسيب پذير و لازم است توليد كنندگان، سيستم ها و نرم افزارهاي خود را بگونه اي ارائه نمايند كه باعث محدوديت در اجراي كدهاي وارده ، خصوصا" كدهائي كه از منابع تائيد نشده و ناشناخته سرچشمه مي گيرند، گردند. در اين رابطه مي توان از روش هاي شناخته شده و مبتني بر مهندسي نرم افزار متعددي استفاده نمود.

• كاهش خطاء پياده سازي . اكثر نقاط آسيب پذير موجود در محصولات از خطاهاي موجود در مرحله پياده سازي نرم افزار، ريشه مي گيرد. اين نوع خطاها در محصولات باقي مانده و شايد منتظرند كه در زمان بكارگيري نرم افزار شناسائي گردند ! تشخيص و برطرف نمودن اين نوع خطاها ، صرفا" زماني ميسر مي گردد كه محصول در حال استفاده و كاربري است . در موارد زيادي ، نقايص امنيتي مشابه بصورت پيوسته در نسخه هاي جديد محصولات، مجددا" مشاهده و كشف مي گردد.مهمترين علت بروز اينگونه نقاط آسيب پذير، طراحي سطح پائين و يا عدم برخورد مناسب با خطاها در زمان پياده سازي است . توليدكنندگان و ارائه دهندگان محصولات نرم افزاري لازم است با مطالعه و بررسي اشتباهات گذشته و بكارگيري روش هاي موثر موجود در مهندسي نرم افزار سعي در كاهش حفره ها و نقايص امنيـي در محصولات خود نمايند .

• پيكربندي پيش فرض با امنيت بالا . امروزه با توجه به پيچيدگي محصولات نرم افزاري ، پيكربندي مناسب سيستم ها و شبكه ها بمنظور استفاده از تدابير امنيتي پيش بيني شده ، امري دشوار بنظر مي رسد . حتي در برخي موارد افراديكه داراي مهارت هاي فني قابل قبولي بوده و آموزش هاي لازم را نيز فراگرفته اند ، بمنظور استفاده و بكارگيري امكانات امنيتي در يک محصول نرم افزاري، داراي مشكلات خاص خود مي باشند.اشتباهات كوچک مي تواند سيستم ها را در معرض تهديد و كاربران را با حملات غير قابل پيش بيني مواجه نمايد. توليد كنندگان و ارائه دهندگان تكنولوژي مي توانند محصولات خود را با پيكربندي پيش فرض ايمن،ارائه نمايند . در چنين مواردي اكثر گزينه ها و امكانات امنيتي موجود ، بصورت پيش فرض و در زمان نصب فعال خواهند بود. بدين ترتيب كاربران در آغاز استفاده از يک محصول نيازمند تغييرات خاصي در رابطه با

پيكربندي محصول نداشته و در ادامه و در صورت ضرورت ،مي توانند پيكربندي هاي پيش فرض را متناسب با خواسته خود تغيير نمايند . بنابراين ، كاربران با يک سطح امنيتي قابل قبول استفاده از محصول را آغاز مي نمايند.

وظايف تصميم گيرندگان

تصميم گيرندگان در يک سازمان ، موسسه و ساير بخش ها ي كلان يک كشور، مي توانند بمنظور افزايش امنيت از رويكردهاي متفاوتي استفاده نمايند . در اين راستا موارد زير پيشنهاد مي گردد :

• تقويت انگيزه هاي لازم براي ارائه محصولات با ايمني بيشتر و كيفيت بالا . بمنظور ترغيب ارائه دهندگان بمنظور توليد محصولات باكيفيت و ايمني مناسب ، پيشنهاد مي گردد كه تصميم گيرندگان از قدرت خريد خود بمنظور تقاضاي نرم افزار با كيفيت بالا استفاده نمايند . در هنگام تهيه نرم افزار و عقد قرارداد مربوطه مي بايست عبارت " كد بي نقص " با صراحت در متن قرارداد آورده شود. بدين ترتيب توليد كنندگان و ارائه دهندگان محصولات در مواردي كه نقايص خاصي نظير نقايص امنيتي در محصول مربوطه تشخيص و كشف مي گردد ، ملزم به رفع عيب و اشكال موجود خواهند بود. پايبندي به رويكرد فوق ، انگيزه هاي مناسبي را براي توليدكنندگان ايجاد و هر توليد كننده كه محصول بي نقصي را توليد و ارائه نمائيد ، شانس موفقيت بيشتري را خواهد داشت .

دراين رابطه لازم است ، تصميم گيرندگان با مسائل متعددي همچون فرآيندهاي تهيه يک محصول آشنا و بصورت مستمر اطلاعات خود را نيز ارتقاء تا بتوانند در زمان لازم تصميمات منطقي و مبتني بر دانش را براي تهيه يک محصول اتخاذ نمايند.بمنظور حمايت از چنين فرآيندهائي، تهيه كنندگان مي بايست آموزش هاي لازم در خصوص نظارت ، سياست هاي امنيتي ، اصول و مفاهيم امنيتي و معماري مربوطه را فرا بگيرند .بهرحال هدف ، تهيه و بكارگيري سيستمهائي است كه با روح يک سازمان مطابقت و افزايش كارآئي و بهره وري را بدنبال داشته باشند .

• تحقيق در رابطه با تضمين ايمن سازي اطلاعات . تصميم گيرندگان ، مي بايست همواره بدنبال راه حل هاي تكنيكي بمنظور افزايش ضريب امنيت اطلاعات بوده و در اين راستا لازم است تحقيقات گسترده و سازمان يافته اي را بمنظور آگاهي از روش هاي كنشگرايانه وپيشگيرانه در دستور كار خود قرار دهند (استفاده از روش هاي واكنشي و انفعالي به تنهائي كفايت نخواهد كرد) . بنابراين ، تصميم گيرندگان مي بايست از يک برنامه منسجم تحقيقاتي حمايت تا بكمک آن بتوان با رويكردهاي جديد در ارتباط با امنيت اطلاعات و سيستم آشنا گرديد.رويكردهاي فوق ، شامل طراحي و پياده سازي استراتژي ها ، روش هاي بازسازي اطلاعات ، استراتژي هاي مربوط به مقاومت در مقابل تهاجمات ، آناليزهاي مستمر و پياده سازي معماري هاي امنيتي باشد . از جمله فعاليت هائي كه مي بايست در اين خصوص مورد توجه و براي آنان راهكارهاي مناسب ايجاد گردد، عبارتند از :

- ايجاد يک چارچوب يكپارچه و يكنواخت براي آناليز و طراحي تضمين اطلاعات
- ايجاد روش هاي مستحكم و مطمئن بمنظور دستيابي و مديريت خطرات برخا سته از تهديد سرمايه هاي اطلاعاتي
- ايجاد روش هاي ارزيابي بمنظور مشخص كردن و بدست آوردن نسبت هزينه / مزيت ، استراتژي هاي ريسک
- ايجاد و استفاده از تكنولوژي هاي جديد بمنظور مقاومت در برابر حملات ، تشخيص حملات و بازيابي خرابي ها
- ايجاد روش هاي سيستماتيک و ابزارهاي شبيه سازي براي آناليز حملات ، تصادمات و خرابي بين سيستم هاي وابسته

• استفاده از متخصصين فني بيشتر . تصميم گيرندگان ، مي بايست از مراكز امنيتي بمنظور ارتقاء سطح دانش عمومي امنيت حمايت نموده تا از اين طريق بتوان كارآموزان و دانشجويان را جذب و با تدوين يک برنامه آموزشي هدفمند نسبت به تربيت كارشناسان ماهر امنيتي اقدام نمود .بديهي است استفاده از كارشناسان فوق ، بمنظور ايمن سازي سيستم ها و شبكه امري ضروري و اجتناب ناپذير است . برنامه هاي آموزشي تدوين شده در فواصل زماني خاصي مي بايست بازنگري تا بتوان افرادي را تربيت كه همواره پاسخگوي نيازهاي امنيتي در سطح سازمان ها و موسسات بوده و با دانش روز نيز كاملا" آگاه باشند.

• ارائه آموزش و آگاهي لازم به كاربران اينترنت : دستيابي آسان و وجود اينترفيس هاي مناسب ، باعث شده است كه كاربران با هر نوع شرايط سني از اينترنت در تمامي سطوح زندگي استفاده نمايند.تعداد زيادي از كاربران اينترنت داراي شناخت اندكي نسبت به تكنولوژي اينترنت و يا روش هاي امنيتي لازم براي استفاده ، مي باشند . تصميم گيرندگان ، مي توانند با دنبال نمودن پيشنهادات زير ، سطح دانش كاربران اينترنت را افزايش دهند :

- طراحي و پياده سازي برنامه ها و مواد آموزشي لازم در خصوص ارتقاء سطح دانش عمومي تمامي كاربران اينترنت .آموزش و افزايش آگاهي كابران در خصوص : خصايص امنيتي ، تهديدات ، فرصت ها و رفتار مناسب در اينترنت به امري ضروري و حياتي تبديل شده است . در اين رابطه لازم است به اين نكته مهم اشاره گردد كه بقاء سيستم وابسته به امنيت سيستم ها در سمت ديگر بوده و حل مشكل سيستم خود به تنهائي كافي نخواهد بود و در اين رابطه لازم است به تمامي كاربران در خصوص نحوه استفاده از كامپيوترهاي خود با لحاظ نمودن پارامترهاي ايمني و امنيتي ، آموزش هاي لازم و مستمر ارائه گردد .علاوه بر موارد فوق ، لازم است به مصرف كنندگان محصولات نرم افزاري آموزش هاي خاصي در رابطه با نحوه تهيه و نصب نرم افزارهاي ايمن ارائه گردد . بدين ترتيب توليدكنندگان محصولات نرم افزاري ترغيب به ارائه محصولات خود با نقاط آسيب پذيري كمتر خواهند شد .

- طراحي و پياده سازي برنامه هاي آموزشي خاص در زمينه استفاده مناسب و اوليه از كامپيوتر . آموزش هاي فوق ، مي بايست بهمراه آموزش هاي عمومي ارائه و نحوه استفاده از كامپيوتر بدرستي تبين گردد . اين نوع از آموزش ها را مي توان از سطوح پائين آموزشي ، آغاز نمود. كاربران نوجوان و جوان اينترنت مي بايست نسبت به رفتارهاي درست و ناشايست در زمان استفاده از كامپيوتر خصوصا" در زمان استفاده از اينترنت بدرستي توجيه و آموزش هاي لازم به آنان ارائه گردد .(مشابه آموزش هاي ارائه شده به كودكان در زمان استفاده از كتابخانه ها ، چه نوع رفتاري قابل قبول است و چه نوع رفتاري پذيرفتني نيست) معلمان مدارس و والدين نيز مي بايست در اين رابطه آموزش هاي لازم را فراگرفته تا از يكطرف قادر به رفتاري قابل قبول در زمان استفاده از كامپيوتر وشبكه هاي كامپيوتري خصوصا" اينترنت بوده و از طرف ديگر و در جايگاه خود بتوانند نظارت لازم را انجام دهند .

خلاصه

وابستگي ما به سيستم هاي كامپيوتري بهم مرتبط خصوصا" اينترنت ، بسرعت در حال افزايش بوده و حتي بروز اختلال اندک توسط ويروس ها و كرم ها مي تواند پيامدهاي ناگواري را بدنبال داشته باشد . راه حل هاي واكنشي استفاده شده براي مقابله با كرم ها و ويروس ها به تنهائي كفايت نخواهد كرد. افزايش قدرت و سرعت حملات باعث شده است كه زيرساخت هاي اطلاعاتي در معرض تهديد و خطر قرار داشته باشند. با دنبال نمودن راه حل هاي موجود مي توان سطح مناسبي از حفاظت در مقابل تهديدات را ايجاد نمود. بمنظور ارتقاء و بهبود وضعيت موجود ، مديران سيستم ، ارائه دهندگان تكنولوژي و تصميم گيرندگان مي توانند با رعايت و پيگيري برخي اصول اوليه ، زمينه برخورد با كرم ها و يا ويروس ها را از ابعاد متفاوت فراهم نمايند.

تغيير در طراحي نرم افزارها ، روش هاي پياده سازي ، افزايش تعداد مديران سيستم آموزش ديده ، بهبود سطح آگاهي كاربران ، افزايش تحقيقات در رابطه با سيستم هاي ايمن و پايدار، طراحي و پياده سازي دوره هاي آموزشي خاص دررابطه با كامپيوتر و امنيت شبكه ، نمونه هائي در اين زمينه بوده كه مي تواند دستاوردهاي مثبتي را در ارتباط با امنيت اطلاعات براي تمامي شهروندان اينترنت بدنبال داشته باشد.حركات مثبت هر يک از شهروندان اينترنت (حقوقي و يا حقيقي) در خصوص پايبندي به اصول امنيتي ، تاثيري مثبت در ايمن سازي سرمايه هاي اطلاعاتي را بدنبال خواهد داشت .

با توجه به اينكه بسياري از اشكالاتي كه در امنيت و دسترسي به شبكه و سرويسهاي آن ايجاد مي‌شود ناشي از پيكربندي غير امن و نادرست تجهيزات مي‌باشد، رعايت نكات ضروري در پيكربندي تجهيزات شبكه بسيار حياتي است

با در دست داشتن يک محصول، مهمترين کاري که در جهت ايجاد امنيت در آن مي‌توان انجام داد، پيکربندي امن آن مي‌باشد. بسياري از اشکالات امنيتي در نتيجة پيکربندي نا امن تجهيزات مي‌باشد. در پيکربندي امن تجهيزات استفاده از ويژگيهايي که مي‌توانند امنيت خود وسيله و وظايفي که بايد انجام دهد را بهبود دهند، مد نظر مي‌باشد. البته راه‌حل ديگري که براي افزايش امنيت يک محصول مشخص مي‌توان داشت، استفاده از نرم‌افزار (و يا بعضاً سخت‌افزار)هاي جديدي است که در آنها اشکالات امنيتي قبلي برطرف شده است. بنابراين همواره بايد نسبت به آخرين آسيب‌پذيريها و روش برطرف کردن آنها مطلع بود و راه‌حل مناسب را بکار گرفت. در تجهيزات خاص‌منظوره نظير روترها معمولاً شرکت سازنده براي برطرف کردن اشکالات امنيتي نسخة جديدي از سيستم‌عامل را ارائه مي‌کند ، اما در تجهيزات عام‌منظوره نظير

رایانه‌ها علاوه بر نسخه‌های جدید سیستم‌عامل معمولاً نرم‌افزارهای خاصی نیز برای افزایش امنیت ارائه می‌شود

) پیکربندی امنیت در روترها :

carrier-classوظیفة اصلی شبکة ملی دیتا بعنوان یک شبکة برقراری اتصال ما بین شبکه‌های داخلی و شبکة جهانی اینترنت می‌باشد که این وظیفه در سطح لایة 3 بر عهدة روترها و سوئیچ‌روترها می‌باشد. بنابراین امنیت روترها و دردسترس بودن آنها در چنین شبکه‌ای بسیار حیاتی و در بالاترین سطح اهمیت می‌باشد. در این بخش نحوة پیکربندی امنیت در روترهای شبکة ملی دیتا بمنظور ایجاد امنیت دسترسی مدیریتی، امنیت ارتباطات مابین روترها (پروتکلهای مسیریابی) و امنیت دربرابر حملات از کار)، رویدادنگاری مناسب و محافظت DOSانداختن سرویس(مابقی شبکه با ذکر دستورات لازم در هر مورد ارائه شده است. همچنین موارد مهمی در انتخاب و تغییر سیستم‌عامل و محافظت فیزیکی نیز در این بخش ذکر شده است.

2-1) امنیت دسترسی مدیریتی

امکان دسترس از راه دور به روترها در عین اینکه امکان مدیریت ساده‌تر و متمرکز روترها را فراهم می‌آورد، خطر دسترسی غیرمجاز به روتر را نیز افزایش می‌دهد. بمنظور مدیریت روتر از راه‌دور باید حتی‌الامکان از امن‌ترین مکانیسمها استفاده شود. در حال حاضراستفاده از تونل بعنوان امن‌ترین روش برای مدیریت مطرح می‌باشد. لازمIPSec به ذکر است که بهرحال برای مدیریت تجهیزات نیاز به ، HTTP، SNMP، Telnetاستفاده از یک پروتکل مدیریتی نظیر می‌باشد که این پروتکلها می‌توانند توسط تونلهای SSHیا به امنیت لازم برسند. در این قسمت نحوة پیکربندی IPSEC و امنیت پروتکلهای مدیریتی ذکر شده در IPSECتونلهای بالا ارائه می‌شود.

پیکر بندی تونلهای IPSEC

لازم است که روترها از این پروتکل پشتیبانی کنند. روترهایCisco با نرم‌افزار IOS 11.3 و بالاتر IPSec را پشتیبانی می‌کنند و می‌توانند بعنوان یکی از نقاط انتهایی تونلهای IPSec پیکربندی شوند. با توجه به اینکه

IPSec از پروتكلهاي 50 و 51 IP و پورت 500 UDP در ارتباطاتش استفاده مي‌كند در ليستهاي دسترسي بايد اين پروتكلها و پورت براي آدرسهايي كه مجاز به استفاده از IPSec براي مديريت روترها هستند باز باشد. در اين قسمت نحوة پيكربندي يک تونل مابين دو روتر كه يكي مي‌تواند روتر سايت مديريتي (يا فايروال سايت مديريتي) و ديگري يک روتر تحت مديريت آن سايت باشد، توضيح داده شده است .
بمنظور ايجاد يک تونل IPSec بين دو روتر Cisco سه مرحلة زير بايد انجام شود :

مقدمه (دهستانی)

امروزه اهمیت شبکه های دیتا در جهان حس گردیده و این امر به گسترش چنین شبکه هایي انجامیده است . کارایي , سادگی وقدرت شبکه های دیتا باعث گشته تا اطلاعات مهمی نیز روی شبکه های دیتا تردد کند. اطلاعات مدیریتی برای کنترل و پیکر بندی منابع شبکه , اطلاعات خصوصی , محرمانه و سری شرکتها و مؤسسات , اطلاعات مالی و جابجایي های مالی مربوط به مشترکین و بانکها از جمله دیتایي هستند که بخشی مهم از ترافیک شبکه های دیتا را تشکیل می دهند. در همین راستا افراد سودجو و هکرها به فکر نفوذ به شبکه ها افتاده و در طول زمان تا کنون ضربات و خسارات سنگینی را برای مشترکین برحق شبکه و دولت وارد آورده اند. برای پیشگیری , تشخیص و رفع این خسارات وضربات وارده به شبکه ها و شناسایي

هکرها , مبحث ایجاد شبکه های امن مطرح گردیده که در طول زمان علوم هکرها و علوم امنیت شبکه یکدیگر را توانمندتر کرده اند.

نیازهای امنیتی و طرح امنیتی شبکه ملی دیتا در جهت برآورد سه اصل مهم در ایجاد یک شبکه فنی کامل گام برداشته است این سه اصل عبارتند از قابلیت دسترسی , تمامیت داده ها و محرمانگی .
قابلیت دسترسی(availability) وقتی حاصل شده است که یک کاربر بر حق یک شبکه که از طرف مدیر شبکه اجازه دسترسی به منبعی را دارد , دقیقاً مطابق تعریف محدوده دسترسی اش در زمان دلخواه متصل شده و تا زمان دلخواهش اتصالش را ادامه دهد.
تمامیت داده ها(integrity) وقتی حاصل می گردد که یک کاربر شبکه منطبق با تعریف محدوده اش دیتايي کامل و بي نقص را از شبکه دریافت و یا به شبکه ارسال کند. بدین معنی که ترافیک دیتا بطور غیر عادی در بین راه تغییر نکند.
محرمانگی(confidentiality) اطلاعات که بمنظور جلوگیری از مشاهده اطلاعات مدیریتی یا هرگونه اطلاعات حساس درون شبکه , توسط یک موجودیت غیر مجاز ایجاد شده است , تأمین می شود.
همانطور که در فاز تعیین نیازهای امنیتی مشخص گردید هدف نیازهای امنیتی شبکه ملی دیتا محافظت از تجهیزات (شامل مسیریابها , سوئیچها ,لینکهای ارتباطی و سرویس دهنده ها),اطلاعات (شامل اطلاعات مدیریتی و اطلاعات سرویسهای لایه کاربرد) و سرویسهای شبکه ملی دیتا (شامل سرویسهای لایه شبکه از قبیل VoIP , MPLS/IPsec) در مقابل حملات و دسترسی غیر مجازمی باشد .
در این نسخه از طرح امنیتی شبکه ملی دیتا و در راستای اهداف بنیادین فوق و نیازهای امنیتی شبکه ملی دیتا طراحی سیستم امنیتی شبکه ملی انجام شده و با هدف تعیین مکانیزم ها و تجهیزات امنیتی مورد نیاز شبکه

ملی دیتا به تکمیل طرح قبل و تغییرات مورد نیاز پرداخته شده است.
این طرح با تقسیم بندی ماجولار بصورت فیزیکی و منطقی شبکه مذکور ایجاد شده است . ماجولهای مشترکین , سایتهای مدیریتی امن شاملNMCها و INMC , سرویسهای لایه کاربرد امن (ALS) و ماجول گیت وی امن که همراه با بخشی از لایه توزیع به سمت لایه دسترسی در ماجول امنیت پیرامونی قرار گرفته است, تمهیدات لازم جهت ایمن سازی این ماجولها و در نهایت ایمن سازی شبکه IP پیش بینی شده از ماجولهای بکاررفته در طرح امنیتی شبکه ملی دیتا هستند. ماجول توزیع و هسته امن ,از دیگر قسمتهای این طرح میباشدکه سرویسهای شبکه ملی دیتا (سرویسهای عمومی, VoIP,MPLS/IPSec) روی این بخشها پیاده سازی میگردند.بطور کلی طرح بترتیب شامل 4 بخش, طرح تجهیزاتی , مکانیزمهای امنیتی , تشکیلات و روال اجرایي امنیت شبکه وهمپوشانی سیاست امنیتی و طرح امنیتی می باشد.
در طرح تجهیزاتی به محافظت از مراکز مدیریت شبکه , محافظت ازتجهیزات و سرویسهای شبکه Backbone , محافظت پیرامونی و محافظت ازسایت سرویسهای لا یه کاربرد پرداخته شده است .