موضوع:

امنیت در شبکه های کامپیوتری

SECURITY IN NETWORK COMPUTER

گرد آورنده :

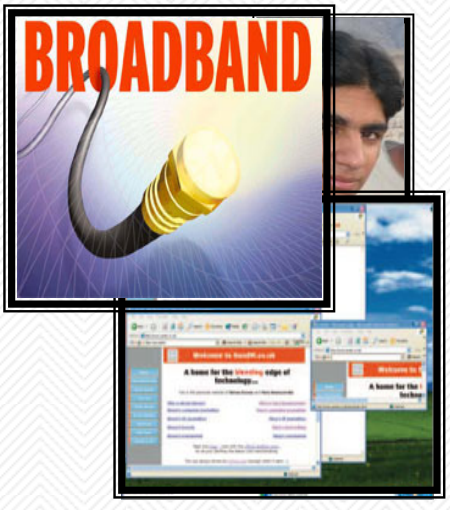
داوود خرسند

D_KHORSAND

Email:

DKHX2000yahoo.com

DKHX2000@Gmail.com



AUTUMN 2005 پائیز۸۴

امنيت برنامه هاي وب (بخش اول)

هر برنامه كامپيوتري كه براي اجراء در محيط شبكه، طراحي و پياده سازي مي گردد ، مي بايست توجه خاصي به مقوله امنيت داشته باشد .برنامه هاي وب از زيرساخت شبكه (اينترانت ، اينترانت) براي ارائه خدمات خود به كاربران استفاده نموده و لازم است نحوه دستيابي كاربران به اين نوع از برنامه ها ، كنترل و با توجه به سياست هاي موجود ، امكان دستيابي فراهم گردد .در ابتدا مي بايست كاربران شناسائي و پس از تائيد هويت آنان ، امكان دستيابي به برنامه با توجه به مجوزهاي تعريف شده ، فراهم گردد. ASP.NET (پلات فرم مايكروسافت براي طراحي و پياده سازي برنامه هاي وب) ، از سه روش عمده به منظور شناسائي كاربران و اعطاي مجوزهاي لازم در جهت دستيابي و استفاده از يک برنامه وب ، استفاده مي نمايد :

Windows Authentication

Forms Authentication

Authentication Passport

در مجموعه مقالاتي كه ارائه خواهد شد به بررسي هر يک از روش هاي فوق در جهت پياده سازي امنيت در برنامه هاي وب خواهيم پرداخت . در بخش اول اين مقاله ، به بررسي نحوه برخورد ASP.NET با كاربران ناشناس (Anonymous) ، روش هاي متفاوت شناسائي كاربران و پارامترهاي لازم در خصوص انتخاب يک استراتژي به منظور شناسائي كاربران با توجه به نوع برنامه ها ، خواهيم پرداخت .

شناسائي و تائيد كاربران

Authentication ، فرآيندي است كه بر اساس آن كاربران شناسائي مي گردند . Authorization ، فرآيند اعطاي دستيابي به كاربران با توجه به هويت آنان مي باشد . با تلفيق Authentication و Authorization، امكان ايمن سازي برنامه هاي وب در مقابل افراد مزاحم و غير مجاز ، فراهم مي گردد .

دستيابي از طريق كاربران ناشناس (Anonymous)

اغلب سايت هاي وب از روش دستيابي "Anonymous" ، استفاده مي نمايند . در چنين مواردي ، اطلاعات موجود بر روي سايت جنبه عمومي داشته و امكان دستيابي تمامي كاربران به اطلاعات وجود خواهد داشت . اين نوع سايت ها ، ضرورتي به بررسي مجاز بودن كاربران براي استفاده از منابع موجود ، نخواهند داشت . برنامه هاي وب ASP.NET ، امكان دستيابي Anonymous را به منابع موجود بر روي سرويس دهنده توسط Impersonation ارائه مي نمايند . Impersonation ، فرآيند نسبت دهي يک Account به يک كاربر ناشناس است . Account دستيابي Anonymous بصورت پيش فرض ، IUSER_computername ، مي باشد. با استفاده از Account فوق ، امكان كنترل كاربران ناشناس كه به منابع موجود بر سرويس دهنده دستيابي دارند ، وجود خواهد داشت . به منظور مشاهده و تغيير مجوزهاي دستيابي در نظر گرفته شده براي Account فوق از برنامه Computer Management استفاده مي گردد :

ورود به شبكه (Logon) به عنوان مديريت شبكه

اجراي Computer Management (از طريق : Administrator | Programs | Tools Start)

انتخاب فولدر Users به منظور نمايش ليست كاربران

مشاهده گروههائي كه Account فوق به عنوان عضوي از آنان مي باشد(كليک بر روي Member of) . كاربران Anonymous ، بصورت پيش فرض ، عضوي از گروه Guests بوده كه داراي مجوزهاي اندكي مي باشد. ASP.NET از ASP.NET Account (با توجه به تنظيمات پيش فرض) ، به منظور اجراي برنامه وب استفاده مي نمايد . بدين ترتيب ، در صورتيكه برنامه اي سعي در انجام عملياتي نمايد كه در ليست مجوزهاي ASP.NET Account وجود نداشته باشد ، يک مورد خاص امنيتي بوجود آمده و امكان دستيابي آن تائيد نخواهد شد.

به منظور اعمال محدوديت در دستيابي كاربران ناشناس مي توان از تنظيمات مربوط به مجوزهاي فايل ويندوز استفاده نمود . براي ايمن سازي ، سرويس دهنده مي بايست داراي سيستم فايل NTFS باشد . سيستم هاي فايل FAT و يا FAT32 ، ايمن سازي در سطح فايل را ارائه نمي نمايند .

دستيابي از طريق كاربران تائيد شده

دستيابي Anonymous ، گزينه اي مناسب براي دستيابي به اطلاعات عمومي و عام است . در صورتيكه برنامه هاي وب شامل اطلاعاتي خاص و خصوصي باشند ، مي بايست در ابتدا كاربران شناسائي و در ادامه با توجه به مجوزهاي تعريف شده ، امكان دستيابي فراهم گردد. در برنامه هاي وب ASP.NET از سه روش عمده به منظور Authentication و Authorization كاربران استفاده مي گردد :

Windows integrated authentication : در روش فوق ، شناسائي و تائيد كاربران بر اساس ليست كاربران تعريف شده بر روي سرويس دهنده انجام خواهد شد. در ادامه با توجه به مجوزها و امتيازات نسبت داده شده به هر Account ، امكان دستيابي و يا عدم دستيابي به منابع موجود بر روي سرويس دهنده ، فراهم مي گردد.

authentication Forms : در روش فوق ، كاربران به يک فرم وب Logon ، هدايت مي گردند . در ادامه ، اطلاعات مربوط به نام و رمز عبور آنان اخذ و فرآيند شناسائي و تائيد بر اساس يک ليسيت كاربران و يا از طريق يک بانک اطلاعاتي كه برنامه حمايت مي نمايد ، انجام خواهد شد.

Passport authentication : در روش فوق ، كاربران جديد به يک سايت كه توسط مايكروسافت ميزبان شده است ، هدايت مي گردند .پس از ريجستر شدن كاربران ، امكان دستيابي آنان به چندين سايت ، فراهم خواهد شد(تمركز در شناسائي كاربران و استفاده از سايت هاي متعدد با توجه به تائيد بعمل آمده) .

هر يک از رويكردهاي فوق ، به همراه روش دستيابي Anonymous ، داراي مزاياي مختص به خود بوده و براي نوع خاصي از برنامه هاي وب ، مناسب مي باشند :

نوع برنامه : برنامه وب عمومي اينترنت

روش تائيد كاربران : Anonymous

توضيحات : روش عمومي دستيابي براي اغلب سايت هاي وب ، مي باشد. در اين روش ، ضرورتي به Logon وجود نداشته و با استفاده از مجوزهاي سيستم فايل NTFS ، مي توان ايمن سازي منابعي را كه قصد اعمال محدوديت در رابطه با دستيابي به آنان وجود دارد را انجام داد .

نوع برنامه : برنامه وب اينترانت

روش تائيد كاربران : integrated Windows

توضيحات : در روش فوق ، سيستم معتبر سازي ويندوز ، كاربران شبكه را از طريق كنترل كننده Domain ، تائيد مي نمايد. امكان دستيابي به منابع برنامه هاي وب بر اساس مجوزهاي تعريف شده بر روي سرويس دهنده ، براي هر يک از كاربران فراهم مي گردد .

نوع برنامه : برنامه هاي وب تجاري

روش تائيد كاربران : Forms

توضيحات : برنامه هائي كه نيازمند دريافت اطلاعات مالي مي باشند ، مي بايست از روش فوق به منظور اخذ و ذخيره سازي اطلاعات ، استفاده نمايند .

نوع برنامه : برنامه هاي متعدد تجاري

روش تائيد كاربران : Passport

توضيحات : در روش فوق ، كاربران يک مرتبه Sign in نموده (از طريق يک مركز تائيد كاربران) و امكان دستيابي و استفاده آنان از تمامي برنامه هائي كه از Passport SDK استفاده مي نمايند ، وجود خواهد داشت . اطلاعات كاربران در يک Passport profile نگهداري خواهدشد (در مقابل استفاده از يک بانک اطلاعاتي محلي) .

استفاده از Authentication در فايل هاي HTM و يا HTML

سه روش تائيد كاربران كه توسط ASP.NET ارائه شده است ، صرفا" در رابطه با فايل هائي كه به عنوان بخشي از برنامه وب مي باشند ، بكار گرفته مي شود .فرم هاي وب (فايل هائي با انشعاب aspx .) ، ماژول ها (فايل هائي با انشعاب asax .) ، نمونه هائي در اين زمينه مي باشند. فرآيند فوق ، صفحات HTML (فايل هائي با انشعاب HTM و يا HTML) را شامل نمي گردد و مسئوليت آن بصورت پيش فرض به IIS (در مقابل ASP.NET) واگذار شده است. در

صورتيكه فصد تائيد كاربراني (استفاده از يكي از روش هاي Windows,Forms و Passport) را داشته باشيم كه به صفحات HTML از طريق برنامه وب دستيابي دارند ، مي بايست اين نوع فايل ها به executable ASP.NET ، مپ گردند .به منظور مپ نمودن فايل هاي html به ASP.NET executable ، پس از اجراي IIS مراحل زير را دنبال مي نمائيم :

انتخاب فولدر شامل برنامه وب و Properties از طريق Action Menu . در ادامه برنامه IIS ، جعبه محاوره اي Properties را نمايش خواهد داد .

بر روي Directory Tab كليک نموده و در ادامه گزينه Configuration را انتخاب مي نمائيم . IIS در ادامه جعبه محاوره اي Application Configuration را نمايش خواهد داد

بر روي دكمه Add كليک نموده و در ادامه IIS جعبه محاوره اي Add/Edit Application Extension Mapping را نمايش خواهد داد .

بر دكمه Browse كليک نموده و فايل aspnet_isapi.dll را انتخاب مي نمائيم .فايل فوق در دايركتوري Windows Microsoft .Net Framework قرار داشته و مسير آن مشابه زير است :

aspnet_isapi.dll Path for

C:\windows\Microsoft.NET\Framework\versionnumber\aspnet_isapi.dll

htm. را در فيلد File Extension تايپ مي نمائيم .

مراحل فوق ، براي فايل هاي با انشعاب html ، تكرار مي گردد.

امنيت برنامه هاي وب (بخش دوم)

در اين مقاله به بررسي Windows Authentication خواهيم پرداخت .
همانگونه كه در بخش اول اين مقاله اشاره گرديد ، برنامه هاي وب ASP.NET از سه روش عمده به منظور تائيد كاربران استفاده مي نمايند :
Authentication Windows
Forms Authentication
Passport Authentication
در Windows Authentication ، برنامه هاي وب مسئوليتي را در ارتباط با تائيد كاربران برعهده نگرفته و اين وظيفه تماما" به سيستم عامل ويندوز ، واگذار مي گردد. فرآيند تائيد كاربران در روش فوق، بصورت زير است :
كاربر درخواستي مبني بر دريافت يک صفحه وب ايمن را از برنامه وب ، مي نمايد .
پس از دريافت درخواست توسط سرويس دهنده وب ، IIS عمليات بررسي صلاحيت كاربر را انجام خواهد داد . در اين راستا ، اطلاعات ارائه شده توسط كاربر در زمان logon (نام و رمز عبور) ، با اطلاعات موجود بر روي سرويس دهنده وب و يا Domain ، مقايسه مي گردد .
در صورتيكه پس از بررسي مدارک ارائه شده توسط كاربر (نام و رمز عبور) ، وي به عنوان كاربر غير مجاز تشخيص داده شود ، درخواست وي ناديده گرفته خواهد شد .
كامپيوتر سرويس گيرنده ، يک جعبه محاوره اي Logon را توليد و از كاربر درخواست درج اطلاعات مورد نياز (نام و رمز عبور) ، مي گردد . پس از درج اطلاعات درخواستي توسط كاربر و ارسال آنان براي سرويس دهنده ، مجددا" IIS بررسي لازم در خصوص صحت آنان را انجام خواهد داد . در صورتيكه صحت اطلاعات ارسالي كاربر (نام و رمز عبور) تائيد گردد ، IIS درخواست اوليه كاربر را به سمت برنامه وب هدايت مي نمايد .
در آخرين مرحله و پس از بررسي و تائيد صلاحيت كاربر ، صفحه وب درخواستي براي كاربر ارسال مي گردد .
مهمترين مزيت روش Authentication Windows ، استفاده مشترک از يک مدل امنيتي به منظور دستيابي به منابع موجود در شبكه و برنامه هاي وب است . پس از تعريف و اعطاي مجوزهاي لازم به كاربر ، امكان دستيابي وي به منابع موجود در شبكه و برنامه هاي وب بر اساس يک سيستم امنيتي مشابه و يكسان ، فراهم مي گردد .
در زمان ايجاد يک پروژه جديد برنامه وب توسط ويژوال استوديو دات نت ، از روش Windows Authentication بصورت پيش فرض به منظور تائيد كاربران استفاده مي گردد .پس از ايجاد يک پروژه جديد برنامه وب در ويژوال استوديو دات نت ، فايل Web.Config بصورت اتوماتيک ايجاد مي گردد . (يک فايل XML كه اطلاعات متفاوتي را در ارتباط با پيكربندي رنامه وب در خود ذخيره مي نمايد) . محتوي پيش فرض اين فايل بصورت زير است (صرفا" بخشي كه با موضوع اين مقاله ارتباط دارد ، منعكس مي گردد) :
.

```
Web.Config default setting
<authentication mode="Windows" />
<authorization>
<allow users="*" /> <!-- تمامي كاربران -->
</authorization>
```

در بخش مربوط به عنصر authentication ، سياست تائيد كاربران برنامه هاي وب مخشص مي گردد . براي مشخص نمودن سياست فوق از خصلت mode مربوط به عنصر authentication ، استفاده شده كه مي تواند يكي از مقادير : Windows , Forms ,Passport و يا None را دارا باشد . در بخش authorization ، سياست هاي مربوط به كاربران مجاز

برنامه وب مشخص مي گردد . در اين رابطه مي توان ، امكان دستيابي و يا عدم دستيابي به برنامه هاي وب را با مشخص نمودن كاربران و يا با توجه به وظايف آنان ، فراهم نمود. (استفاده از كاراكتر " * " ، به معني همه كاربران بوده و كاراكتر "؟" به منزله كاربران ناشناس و غيرمجاز است) . براي آشنائي با عملكرد روش Windows Authentication ، مراحل زير را دنبال مي نمائيم :
بخش authorization در فايل Web.Config را بصورت زير تغيير مي نمائيم :

```
Authorization element
<authorization>
<deny users="?" />
</authorization>
```

تگ هاي زير را كه يک جدول HTML را تعريف مي نمايند ، در فرم وب شروع برنامه وب ، قرار مي دهيم :

```
HTML Table in Startup web form
<TABLE id="tblUser">
<tr>
<TD><STRONG>است ؟ آيا كاربر تائيد شده</STRONG></TD>
<TD><Span runat="server" id="spnAuthenticated"></Span></TD>
</tr>
<tr>
<TD><STRONG>كاربر نام </STRONG></TD>
<TD><Span runat="server" id="spnUserName"></Span></TD>
</tr>
<tr>
<TD><STRONG>تائيد كاربر نوع</STRONG></TD>
<TD><Span runat="server" id="spnAuthenticationtype"></Span></TD>
</tr>
</TABLE>
```

به حالت Design view سوئيچ نموده و كد زير را در فايل Code Behind فرم وب شروع برنامه ، قرار مي دهيم :

```
Web form's code-behind file
Private Sub Page_Load( ByVal sender As System.Object,ByVal e As System.EventArgs ) Handles
Mybase.Load
spnAuthenticated.InnerText = User.Identity.IsAuthenticated
spnUserName .InnerText = User.Identity.Name
spnAuthenticationType.InnerText = User.Identity.AuthenticationType
End Sub
```

پس از اجراي پروژه بصورت محلي ، ASP.NET تائيد كاربر را بر اساس نام و رمز عبوري كه براي ورود به ويندوز استفاده شده است ، انجام خواهد د اد .

پس از اجراي پروژه از راه دور (مثلا" دستيابي از طريق اينترنت) ، ASP.NET يک جعبه محاوره اي رادر مرورگر نمايش داده تا از طريق آن نام و رمز عبور کاربر دريافت گردد .

در صورتيکه نام و رمز عبور درج شده توسط کاربر با تعاريف انجام شده در Domain شبکه ، مطابقت نمايد ، ASP.NET کاربر را تائيد و مجوز لازم به منظور استفاده از برنامه وب صادر خواهد شد . در اين رابطه ASP.NET ، يک authorization certificate را به شکل يک کوکي صادر که در حين Session کاربر ، نگهداري و از آن استفاده مي گردد. Session کاربر، پس از اتمام زمان Time out و يا بستن مرورگر ، خاتمه مي يابد . برنامه وب اجراي خود را متناسب با مجوزهاي تعريف شده در ارتباط با Account آغاز مي نمايد .
روش integrated authentication Windows در يک شبکه مبتني بر Domain بهتر کار خواهد کرد . شبکه هائي که از Workgroup استفاده مي نمايند (در مقابل استفاده از Domain) داراي محدوديت هاي خاص خود به منظور استفاده از ويژگي هاي امنيتي ، مي باشند. شبکه هاي مبتني بر Domain ، از يک کنترل کننده Domain به منظور تائيد و معتبرسازي کاربران شبکه ، استفاده مي نمايد .
با استفاده از امکانات ارائه شده در فايل Web.Config مي توان يک لايه امنيتي مضاعف را ايجاد نمود . دراين راستا ، مي توان تنظيمات لازم به منظور دستيابي و يا عدم دستيابي کاربران و يا گروه هاي خاصي از کاربران را نيز انجام داد .
اعمال محدوديت براي کاربران خاص (دستيابي و يا عدم دستيابي)
در مواردیکه از روش Windows integrated authentication استفاده مي گردد ، ASP.NET ، ليست تائيد موجود در فايل Web.Config را به منظور آگاهي از صلاحيت کاربران شبکه براي استفاده ازبرنامه وب ، بررسي مي نمايد. کاراکترهاي "*" و "؟" داراي معاني خاصي در ليست تائيد مي باشند : کاراکتر "* " ، نشاندهنده تمامي کاربران و کاراکتر "؟"، نشاندهنده کاربران غير مجاز(ناشناس) مي باشد . مثلا" ليست تائيد زير در Web.Config ، امکان دستيابي تمامي کاربران ناشناس به برنامه وب را حذف و مي بايست تمامي کاربران به منظور استفاده از برنامه وب ،تائيد گردند .

Authorization element
<authorization>
<deny users="?" />
</authorization>

به منظور اعمال محدوديت در دستيابي کاربراني خاص ،مي توان از عنصر <allow> استفاده و اسامي تمامي کاربران مجاز را با صراحت مشخص نمود (اسامي توسط ويرگول از يکديگر تفکيک مي گردند) . پس از معرفي کاربران مجاز با استفاده از عنصر <allow> ، مي بايست با بکارگيري عنصر <deny> ، امکان دستيابي به برنامه توسط کاربران غير مجاز، سلب مي گردد .

Authorization element
<authorization>
<allow users="Ali Reaz , Reza Ali " />
<deny users="*" />
</authorization>

ليست مجاز فوق ، امکان دستيابي دو کاربر که اسامي آنان با صراحت مشخص شده است را به برنامه وب خواهد داد. ساير کاربران ، امکان دستيابي به برنامه وب را دارا نخواهند بود (نقش عنصر deny در مثال فوق) علاوه بر ليست مجاز فوق که اسامي دو کاربر را مشخص و آنان را براي استفاده از برنامه وب مجاز مي نمايد ، دو کاربر فوق ، مي بايست داراي Account لازم در Domain شبکه نيز باشند .

تائيد كاربران بر اساس نوع وظيفه

براي تائيد كاربران به منظور استفاده از يک برنامه مي توان ، مجوزهاي لازم را بر اساس وظيفه آنان در سازمان ، صادر و امكان دستيابي و يا عدم دستيابي را براي آنان فراهم نمود. در ويندوز NT و XP ، وظايف به اسامي مپ شده تا از اين طريق امكان شناسائي گروه هاي كاربران ، فراهم گردد. ويندوز، چندين گروه را بصورت اتوماتيک از قبل ايجاد مي نمايد : Users, Administrators و Guests . در اين رابطه مي توان از عنصر <roles> در ليست استفاده كنندگان مجاز برنامه وب در فايل Web.Config استفاده و امكان دستيابي به يک برنامه را با توجه به وظايف كاربر ، فراهم نمود. مثلا" ليست زير، امكان دستيابي به برنامه وب را صرفا" براي كاربراني كه به عنوان Administrator به شبكه وارد مي شوند ، فراهم مي نمايد.

```
Authorization element
<authorization>
<allow roles ="Administrators" />
<deny users="*" />
</authorization>
```

پس از تائيد كاربر و صدور مجوز لازم به منظور استفاده از برنامه وب ، مي توان با استفاده از خصلت Identity مربوط به شي User ، هويت كاربر (نام و نوع وظيفه) را از طريق برنامه شناسائي نمود.خصلت فوق، يک شي را كه شامل اطلاعات مربوط به نام و وظيفه كاربراست را برمي گرداند .

```
Web form's code-behind file
Private Sub Page_Load( ByVal sender As System.Object,ByVal e As System.EventArgs ) Handles
Mybase.Load
spnAuthenticated.InnerText = User.Identity.IsAuthenticated
spnUserName .InnerText = User.Identity.Name
spnAuthenticationType.InnerText = User.Identity.AuthenticationType
End Sub
```

به منظور آگاهي و انجام عمليات لازم با توجه به نوع وظيفه كاربر كه از برنامه وب استفاده مي نمايد ، مي توان از متد IsInRole شي User ، استفاده نمود .

```
IsInRole method
If User.IsInRole("Administrators") Then
'انجام عمليات دلخواه
End If
```

استفاده از تنظيمات IIS به همراه Authentication Windows

تنظيمات Authorization در فايل Web.Config با تنظيمات انجام شده در IIS با يكديگر Overlap مي شوند . در صورتيكه Authorization هم در فايل Web.Config و هم توسط IIS تنظيم شده باشد ، در ابتدا تنظيمات IIS بررسي و در ادامه تنظيمات موجود در فايل Web.Config ، مورد توجه قرار خواهند گرفت. به منظور مشاهده تنظيمات authorization در IIS مراحل زير را دنبال مي نمائيم :

در IIS بر روي فولدر برنامه وب كليک سمت راست نموده و در ادامه گزينه Properties را انتخاب مي نمائيم . برنامه IIS در ادامه جعبه محاوره اي Properties مربوط به فولدر را نمايش خواهد داد .

بر روي Directory Security Tab كليک و در ادامه دكمه Edit را در گروه Anonymous Access And Authentication Control كليک مي نمائيم . IIS ، جعبه محاوره اي Authentication Methods را نمايش خواهد داد .
اولين گروه از تنظيمات در جعبه محاوره اي ، كنترل دستيابي Anonymous را انجام مي دهد (همه كاربران). غير فعال نمودن گزينه فوق ، معادل <deny User = "?"> در فايل Web.config است.
Check Box هاي موجود در قسمت دوم جعبه محاوره اي ، مجاز بودن برنامه به منظور استفاده از Basic و يا Digest Authentication را علاوه بر Windows Authentication ، مشخص مي نمايد. روش هاي فوق ، ايمني بمراتب كمتري را نسبت به Windows Integrated ارائه مي نمايند .مي توان چندين روش authentication را در IIS فعال نمود . در صورتيكه چندين روش فعال شده باشد ، مي توان با استفاده از متد AuthenticationType مربوط به شي Identity ، از روش استفاده شده به منظور تائيد كاربر ، آگاهي يافت .

AuthenticationType method

```
Response.Write(User.Identity.AuthenticationType)
```

امنیت برنامه های وب (بخش سوم)

در اين مقاله به بررسي Authentication Forms خواهيم پرداخت .

همانگونه كه در بخش اول اين مقاله اشاره گرديد ، برنامه هاي وب ASP.NET از سه روش عمده به منظور تائيد كاربران استفاده مي نمايند :

Windows Authentication

Forms Authentication

Authentication Passport

در Forms Authentication ، برنامه IIS مسئوليتي را در ارتباط با تائيد كاربران برعهده نگرفته و تنظيمات امنيتي IIS در رابطه با برنامه وب ، دستيابي Anonymous مي باشد . فرآيند تائيد كاربران در روش فوق، بصورت زير است :

زمانيكه سرويس گيرنده درخواست يک صفحه ايمن را مي نمايد ، IIS كاربر را به عنوان Anonymous، تائيد و در ادامه درخواست وي را براي ASP.NET ارسال مي نمايد .

ASP.NET ، بررسي لازم در خصوص وجود يک كوكي خاص بر روي كامپيوتر سرويس گيرنده را انجام خواهد داد .

در صورتيكه كوكي ، موجود نبوده و يا غيرمعتبر باشد ، ASP.NET درخواست كاربر را نادیده گرفته و براي وي يک صفحه Logon را ارسال مي نمايد (مثلا" Login.aspx).

كاربر اطلاعات لازم (نام و رمز عبور) را در صفحه Logon.aspx (به عنوان نمونه) درج و در ادامه دكمه Submit موجود بر روي فرم را به منظور ارسال اطلاعات براي سرويس دهنده ، فعال مي نمايد.

IIS ، مجددا" كاربر را به عنوان Anonymous، تائيد و درخواست وي را براي ASP.NET ارسال مي نمايد .

ASP.NET ، تائيد كاربر را بر اساس اطلاعات ارسالي (نام و رمز عبور) انجام و يک كوكي را ايجاد مي نمايد .

در نهايت ، صفحه وب ايمن درخواست شده به همراه كوكي جديد براي سرويس گيرنده ارسال مي گردد. مادامیكه كوكي معتبر باشد ، كاربر قادر به درخواست و مشاهده ساير صفحات وب مي باشد.

فرآيند فوق را مي توان به دو حالت متفاوت تعميم و مورد توجه قرار داد :

حالت اول : درخواست يک صفحه ايمن از سرويس دهنده ، توسط يک كاربر غيرمجاز و تائيد نشده

مرحله اول : پس از درخواست يک سرويس گيرنده براي دستيابي به يک صفحه ايمن ، درخواست ارسالي وي در ابتدا توسط IIS بررسي و با توجه به اينكه تنظيمات IIS بصورت Anonymous پيكربندي شده تا امكان استفاده از Forms Authentication فراهم گردد ، درخواست كاربر ، مستقيما" براي ماژول ASP.NET Forms Authentication ارسال مي گردد .

مرحله دوم : ASP.NET ، بررسي لازم در خصوص وجود (داشتن) يک كوكي Authentication را انجام خواهد داد . با توجه به اينكه كاربر اولين مرتبه است كه درخواست اطلاعاتي را نموده و داراي يک كوكي نمي باشد ، سرويس گيرنده به صفحه Logon ، هدايت مي گردد .

مرحله سوم : كاربراطلاعات ضروري (نام و رمز عبور) خود را در صفحه Logon درج و پس ازارسال آنان ،فرآيند بررسي اطلاعات ارسالي آغاز مي گردد. در يک برنامه بزرگ ، بررسي اطلاعات كاربر از طريق يک بانک اطلاعاتي شامل

مشخصات کاربران انجام مي شود .
مرحله چهارم : در صورتيکه اطلاعات ارسالي کاربر (نام و رمز عبور) ، پس از بررسي توسط برنامه وب ، معتبر شناخته نگردند ، مجوز دستيابي براي کاربر صادر نشده و امکان دستيابي وي سلب مي گردد .
مرحله پنجم : در صورتيکه پس از بررسي اطلاعات ارسالي، اعتبار وصحت آنان تائيد گردد ، يک کوکي تائيد ايجاد و در ادامه به کاربر مجوز لازم به منظور دستيابي به صفحه ، اعطاء مي گردد .(هدايت کاربر به صفحه درخواست اوليه) .
حالت دوم : درخواست يک صفحه ايمن از سرويس دهنده ، توسط يک کاربر مجاز و تائيد شده
مرحله اول : پس از درخواست يک صفحه ايمن توسط سرويس گيرنده ، کوکي Authentication بهمراه درخواست وي براي سرويس دهنده ، ارسال مي گردد.
مرحله دوم :درخواست ارسالي توسط سرويس گيرنده در ابتدا توسط IIS دريافت و با توجه به تنظيمات انجام شده (دسيتابي Anonymous) ، درخواست وي مستقيما" براي ASP.NET Forms Authentication ارسال مي گردد .
مرحله سوم : ماژول ASP.NET Forms Authentication ، بررسي لازم در خصوص کوکي را انجام و در صورتيکه کوکي معتبر باشد ، سرويس گيرنده تائيد و امکان دستيابي و مشاهده صفحه وب درخواستي براي وي ، فراهم مي گردد .
در روش Forms Authentication ، بصورت اتوماتيک يک فرم وب طراحي شده به منظور اخذ اطلاعات مربوط به نام و رمز عبور کاربران ، نمايش داده مي شود . کد مرتبط با فرم وب ، عمليات تائيد و معتبرسازي کاربر را بر اساس ليست ذخيره شده در فايل Web.Config برنامه و يا از طريق يک بانک اطلاعاتي جداگانه ، انجام مي دهد. مزيت مهم Forms Authentication ، عدم ضرورت عضويت کاربران در Domain شبکه به منظور دستيابي به برنامه وب ، مي باشد .
فعال نمودن Forms Authentication
به منظور استفاده از روش فوق ، مي بايست مراحل زير را دنبال نمود :
مقداردهي Authentication mode در فايل Web.config به Forms
ايجاد يک فرم وب به منظور اخذ اطلاعات کاربران (Logon Page)
ايجاد يک فايل و يا بانک اطلاعاتي به منظور ذخيره نام و رمز عبور کاربران
نوشتن کد لازم به منظور افزودن کاربر جديد به فايل و يا بانک اطلاعاتي کاربران
نوشتن کد لازم به منظور تائيد کاربران با استناد به فايل و يا بانک اطلاعاتي کاربران
Forms Authentication ، از کلاس هاي موجود در namespace با نام System.Web.Security استفاده مي نمايد . به منظور استفاده از کلاس هاي فوق، مي بايست در ويژوال بيسک دات نت از عبارت Imports و در ويژوال سي شارپ از Using استفاده گردد (در ابتداي هر ماژول که عمليات تائيد را انجام خواهد داد : System.Web.Security Imports) .
مقداردهي Authentication mode
نوع تائيد کاربران در يک برنامه وب ، مي بايست با استفاده از عنصر <authentication> در فايل Web.config مشخص گردد. به منظور تنظيم برنامه مورد نظر خود براي استفاده از Forms Authentication ، تغييرات زير را در فايل Web.Config ، اعمال مي نمائيم :

```
Web.Config setting for Forms Authentication
<authentication mode="Forms">
<forms loginUrl = Login.aspx" >
<credentials passwordFormat = "Clear" >
<user name = "Ali" Password ="110" />
<user name = "Kaveh" Password ="111" />
</credentials>
</forms>
</authentication>
```

كد فوق، يک نوع ساده از تائيد کاربران به روش Forms را نشان مي دهد . در اين رابطه ، اغلب از تعاريف و تنظيمات پيش فرض و يک ليست کاربران مجاز، استفاده شده است. از عناصر متفاوتي در ارتباط با Forms Authentication در فايل Web.Config استفاده مي گردد.هر يک از عناصر داراي خصلت هاي خاص خود مي باشند :

عنصر <authentication>

خصلت Mode ، با استفاده از خصلت فوق ، روش تائيد و شناسائي کاربران مشخص مي گردد. با مقدار دهي خصلت فوق به Forms ، روش Authentication Forms انتخاب خواهد شد.

عنصر <forms>

خصلت name . از خصلت فوق به منظور مشخص نمودن نام کوکي که اطلاعات مربوط به نام و رمز عبور را ذخيره مي نمايد ، استفاده مي شود . مقدار پيش فرض ، authaspx . مي باشد . در صورتيکه بيش از يک برنامه بر روي سرويس دهنده از روش Forms Authentication استفاده مي نمايند ، مي بايست براي هر يک از آنان نام منحصربفردي در نظر گرفته شود .

خصلت loginUrl .از خصلت فوق به منظور مشخص نمودن نام فرم وب Login براي کاربران تائيد نشده ، استفاده مي گردد . مقدار پيش فرض خصلت فوق، Default.aspx است .

خصلت protection . با استفاده از خصلت فوق روش حفاظت کوکي Authentication که بر روي کامپيوتر سرويس گيرنده ذخيره مي گردد ، مشخص خواهد شد. مقدار پيش فرض خصلت فوق ، All بوده که عمليات رمزنگاري و بررسي اعتبار و صحت داده در رابطه با آن اعمال مي گردد. ساير گزينه هاي موجود در اين راستا ، Encryption,Validation و None مي باشد .

خصلت timeout . با استفاده از خصلت فوق ، مدت زمان نگهداري کوکي Authentication بر روي ماشين کاربر مشخص مي گردد . مقدار پيش فرض ۳۰ دقيقه است . ASP.NET ، پس از دريافت يک درخواست جديد توسط کاربر و مشروط به گذشت بيش از نصف زمان تعريف شده ، کوکي را تجديد (Renew) خواهد کرد .

خصلت path . با استفاده از خصلت فوق ، مسير مورد نظر به منظور ذخيره سازي کوکي بر روي ماشين کاربر مشخص مي گردد . مقدار پيش فرض ، "\" است .

عنصر <credentials>

خصلت passwordFormat ، با استفاده از خصلت فوق ، الگوريتم لازم به منظور رمزنگاري رمز عبور کاربر ، مشخص مي گردد . مقدار پيش فرض ، SHA1 مي باشد . ساير گزينه هاي موجود در اين رابطه ، MD5 و Clear (بدون رمزنگاري) مي باشد .

عنصر <users>

خصلت name ، با استفاده از خصلت فوق ، نام کاربر مشخص مي گردد.

خصلت password ، با استفاده از خصلت فوق ، رمز عبور کاربر مشخص مي گردد.

عنصر <credentilas> ، امکان ذخيره سازي ليست کاربران را در Web.Config فراهم مي نمايد . رويکرد فوق ، روشي ساده به منظور تعريف کاربران مجاز يک برنامه وب مي باشد . در چنين مواردي ، مديريت سيستم مي تواند بسادگي و در صورت لزوم نام و رمز عبور کاربران ديگري را به ليست مجاز کاربران ، اضافه نمايد . مکانيزم فوق ، در مواردي که قصد داشته باشيم ، امکان تعريف نام و رمز عبور را در اختيار کاربران قرار دهيم ، گزينه مناسبي نبوده و مي بايست از يک فايل و يا بانک اطلاعاتي به منظور ذخيره سازي اطلاعات کاربران ، استفاده گردد.

استراتژي حفاظت از اطلاعات در شبكه هاي كامپيوتري (بخش اول)

مقدمه

اطلاعات در سازمان ها و موسسات مدرن، بمنزله شاهرگ حياتي محسوب مي گردد . دستيابي به اطلاعات و عرضه مناسب و سريع آن، همواره مورد توجه سازمان هائي است كه اطلاعات در آنها داراي نقشي محوري و سرنوشت ساز است . سازمان ها و موسسات مي بايست يک زير ساخت مناسب اطلاعاتي را براي خود ايجاد و در جهت انظباط اطلاعاتي در سازمان خود حركت نمايند . اگر مي خواهيم ارائه دهنده اطلاعات در عصر اطلاعات بوده و صرفا" مصرف كننده اطلاعات نباشيم ، در مرحله نخست مي بايست فرآيندهاي توليد ،عرضه و استفاده از اطلاعات را در سازمان خود قانونمند نموده و در مراحل بعد ، امكان استفاده از اطلاعات ذيربط را براي متقاضيان (محلي،جهاني) در سريعترين زمان ممكن فراهم نمائيم . سرعت در توليد و عرضه اطلاعات ارزشمند ، يكي از رموز موفقيت سازمان ها و موسسات در عصر اطلاعات است . پس از ايجاد انظباط اطلاعاتي، مي بايست با بهره گيري از شبكه هاي كامپيوتري زمينه استفاده قانومند و هدفمند از اطلاعات را براي سايرين فراهم كرد . اطلاعات ارائه شده مي تواند بصورت محلي (اينترانت) و يا جهاني (اينترنت) مورد استفاده قرار گيرد . فراموش نكنيم در اين هنگامه اطلاعاتي، مصرف كنندگان اطلاعات داراي حق مسلم انتخاب مي باشند و در صورتيكه سازمان و يا موسسه اي در ارائه اطلاعات سهوا" و يا تعمدا" دچار اختلال و يا مشكل گردد ، دليلي بر توقف عملكرد مصرف كنندگان اطلاعات تا بر طرف نمودن مشكل ما ، وجود نخواهد داشت . سازمان ها و موسسات مي بايست خود را براي نبردي سخت در عرضه و ارائه اطلاعات آماده نمايند و در اين راستا علاوه بر پتانسيل هاي سخت افزاري و نرم افزاري استفاده شده ، از تدبير و دوراندیشي فاصله نگيرند . در ميدان عرضه و ارائه اطلاعات ، كسب موفقيت نه بدليل ضعف ديگران بلكه بر توانمندي ما استوار خواهد بود. مصرف كنندگان اطلاعات، قطعا" ارائه دهندگان اطلاعاتي را برمي گزينند كه نسبت به توان و پتانسيل آنان اطمينان حاصل كرده باشند . آيا سازمان ما در عصر اطلاعات به پتانسيل هاي لازم در اين خصوص دست پيدا كرده است ؟ آيا در سازمان ما بستر و ساختار مناسب اطلاعاتي ايجاد شده است ؟ آيا گردش امور در سازمان ما مبتني بر يک سيستم اطلاعاتي مدرن است ؟ آيا سازمان ما قادر به تعامل اطلاعاتي با ساير سازمان ها است ؟ آيا در سازمان ما نقاط تماس اطلاعاتي با دنياي خارج از سازمان تدوين شده است ؟ آيا فاصله توليد و استفاده از اطلاعات در سازمان ما به حداقل مقدار خود رسيده است ؟ آيا اطلاعات قابل عرضه سازمان ما ، در سريعترين زمان و با كيفيتي مناسب در اختيار مصرف كنندگان متقاضي قرار مي گيرد ؟ حضور يک سازمان در عرصه جهاني ، صرفا" داشتن يک وب سايت با اطلاعات ايستا نخواهد بود . امروزه ميليون ها وب سايت بر روي اينترنت وجود داشته كه هر روز نيز به تعداد آنان افزوده مي گردد . كاربران اينترنت براي پذيرش سايت سازمان ما ، دلايل موجه اي را دنبال خواهند كرد . در اين هنگامه سايت داشتن و راه اندازي سايت ، اصل موضوع كه همانا ايجاد يک سازمان مدرن اطلاعاتي است ، فراموش نگردد. سازمان ما در اين راستا چگونه حركت كرده و مختصات آن در نقشه اطلاعاتي يک سازمان مدرن چيست ؟

بديهي است ارائه دهندگان اطلاعات خود در سطوحي ديگر به مصرف كنندگان اطلاعات تبديل و مصرف كنندگان اطلاعات ، در حالات ديگر، خود مي تواند بعنوان ارائه دهنده اطلاعات مطرح گردند. مصرف بهينه و هدفمند اطلاعات در صورتيكه به افزايش آگاهي ، توليد و ارائه اطلاعات ختم شود، امري بسيار پسنديده خواهد بود . در غير اينصورت، مصرف مطلق و همیشگي اطلاعات بدون جهت گيري خاص ، بدترين نوع استفاده از اطلاعات بوده كه قطعا" به سرانجام مطلوبي ختم نخواهد شد .

شبكه هاي كامپيوتري

در صورتيكه قصد ارائه و يا حتي مصرف بهينه و سريع اطلاعات را داشته باشيم، مي بايست زير ساخت مناسب را در اين جهت ايجاد كنيم . شبكه هاي كامپيوتري ، بستري مناسب براي عرضه ، ارائه و مصرف اطلاعات مي باشند(دقيقا" مشابه نقش جاده ها در يک سيستم حمل و نقل) . عرضه ، ارائه و مصرف يک كالا نيازمند وجود يک سيستم حمل و نقل مطلوب خواهد بود. در صورتيكه سازمان و يا موسسه اي محصولي را توليد ولي قادر به عرضه آن در زمان مناسب (قبل از اتمام تاريخ مصرف) براي متقاضيان نباشد، قطعا" از سازمان ها ئي كه توليدات خود را با بهره گيري از يک زير

ساخت مناسب ، بسرعت در اختيار متقاضيان قرار مي دهند ، عقب خواهند افتاد . شايد بهمين دليل باشد كه وجود جاده ها و زير ساخت هاي مناسب ارتباطي، بعنوان يكي از دلايل موفقيت برخي از كشورها در عصر انقلاب صنعتي ، ذكر مي گردد. فراموش نكنيم كه امروزه زمان كهنه شدن اطلاعات از زمان توليد اطلاعات بسيار سريعتر بوده و مي بايست قبل از اتمام تاريخ مصرف اطلاعات با استفاده از زير ساخت مناسب (شبكه هاي ارتباطي) اقدام به عرضه آنان نمود. براي عرضه اطلاعات مي توان از امكاناتي ديگر نيز استفاده كرد ولي قطعا" شبكه هاي كامپيوتري بدليل سرعت ارتباطي بسيار بالا داراي نقشي كليدي و منحصر بفرد مي باشند . مثلا" مي توان مشخصات كالا و يا محصول توليد شده در يک سازمان را از طريق يک نامه به متقاضيان اعلام نمود ولي در صورتيكه سازماني در اين راستا از گزينه پست الكترونيكي استفاده نمايد ، قطعا" متقاضيان مربوطه در زماني بسيار سريعتر نسبت به مشخصات كالاي توليده شده ، آگاهي پيدا خواهند كرد .

امنيت اطلاعات در شبكه هاي كامپيوتري

بموازات حركت بسمت يک سازمان مدرن و مبتني بر تكنولوژي اطلاعات، مي بايست تدابير لازم در رابطه با حفاظت از اطلاعات نيز انديشيده گردد. مهمترين مزيت و رسالت شبكه هاي كامپيوتري ، اشتراک منابع سخت افزاري و نرم افزاري است . كنترل دستيابي و نحوه استفاده از منابع به اشتراک گذاشته شده ، از مهمترين اهداف يک سيستم امنيتي در شبكه است . با گسترش شبكه هاي كامپيوتري خصوصا" اينترنت ، نگرش نسبت به امنيت اطلاعات و ساير منابع به اشتراک گذاشته شده ، وارد مرحله جديدي شده است . در اين راستا ، لازم است كه هر سازمان براي حفاظت از اطلاعات ارزشمند ، پايبند به يک استراتژي خاص بوده و بر اساس آن سيستم امنيتي را اجراء و پياده سازي نمايد . عدم ايجاد سيستم مناسب امنيتي ، مي تواند پيامدهاي منفي و دور از انتظاري را بدنبال داشته باشد . استراتژي سازمان ما براي حفاظت و دفاع از اطلاعات چيست؟ در صورت بروز مشكل امنيتي در رابطه با اطلاعات در سازمان ، بدنبال كدامين مقصر مي گرديم ؟ شايد اگر در چنين مواردي ، همه مسائل امنيتي و مشكلات بوجود آمده را به خود كامپيوتر نسبت دهيم ، بهترين امكان برون رفت از مشكل بوجود آمده است ، چراكه كامپيوتر توان دفاع كردن از خود را ندارد . آيا واقعا" روش و نحوه برخورد با مشكل بوجود آمده چنين است ؟ در حاليكه يک سازمان براي خريد سخت افزار نگراني هاي خاص خود را داشته و سعي در برطرف نمودن معقول آنها دارد ، آيا براي امنيت و حفاظت از اطلاعات نبايد نگراني بمراتب بيشتري در سازمان وجود داشته باشد ؟

استراتژي

دفاع در عمق ، عنوان يک استراتژي عملي بمنظور نيل به تضمين و ايمن سازي اطلاعات در محيط هاي شبكه امروزي است . استراتژي فوق، يكي از مناسبترين و عملي ترين گزينه هاي موجود است كه متاثر از برنامه هاي هوشمند برخاسته از تكنيک ها و تكنولوژي هاي متفاوت تدوين مي گردد . استراتژي پيشنهادي ، بر سه مولفه متفاوت ظرفيت هاي حفاظتي ، هزينه ها و رويكردهاي عملياتي تاكيد داشته و توازني معقول بين آنان را برقرار مي نمايد . دراين مقاله به بررسي عناصر اصلي و نقش هر يک از آنان در استراتژي پيشنهادي، پرداخته خواهد شد.

دشمنان، انگيزه ها ، انواع حملات اطلاعاتي

بمنظور دفاع موثر و مطلوب در مقابل حملات به اطلاعات و سيستم هاي اطلاعاتي ، يک سازمان مي بايست دشمنان، پتانسيل و انگيزه هاي آنان و انواع حملات را بدرستي براي خود آناليز تا از اين طريق ديدگاهي منطقي نسبت به موارد فوق ايجاد و در ادامه امكان برخورد مناسب با آنان فراهم گردد .اگر قصد تجويز دارو براي بيماري وجود داشته باشد ، قطعا" قبل از معاينه و آناليز وضعيت بيمار، اقدام به تجويز دارو براي وي نخواهد شد. در چنين مواري نمي توان براي برخورد با مسائل پويا از راه حل هاي مشابه و ايستا استفاده كرد .بمنظور ارائه راهكارهاي پويا و متناسب با مسائل متغير، لازم است در ابتدا نسبت به كالبد شكافي دشمنان ، انگيزه ها و انواع حملات ، شناخت مناسبي ايجاد گردد.
دشمنان ، شامل سارقين اطلاعاتي ، مجرمان ،دزدان كامپيوتري ، شركت هاي رقيب و ... مي باشد.
انگيزه ها ي موجود شامل : جمع آوري هوشمندانه، دستبرد فكري (عقلاني) ،عدم پذيرش سرويس ها ، كنف كردن ،احساس غرور و مورد توجه واقع شدن ، با شد .
انواع حملات شامل : مشاهده غيرفعال ارتباطات ، حملات به شبكه هاي فعال، حملات از نزديک(مجاورت سيستم ها)

، سوء استفاده و بهره برداري خوديان (محرمان) و حملات مربوط به ارائه دهندگان صنعتي يکي از منابع تکنولوژي اطلاعات ، است .
سيستم هاي اطلاعاتي و شبکه هاي کامپيوتري اهداف مناسب و جذابي براي مهاجمان اطلاعاتي مي باشند .
بنابراين لازم است، تدابير لازم در خصوص حفاظت سيستم ها و شبکه ها در مقابل انواع متفاوت حملاتي اطلاعاتي انديشيده گردد. بمنظور آناليز حملات اطلاعاتي و اتخاذ راهکار مناسب بمنظور برخورد با آنان، لازم است در ابتدا با انواع حملات اطلاعات آشنا شده تا از اين طريق امکان برخورد مناسب و سيستماتيک با هريک از آنان فراهم گردد . قطعا" وقتي ما شناخت مناسبي را نسبت به نوع و علل حمله داشته باشيم ، قادر به برخورد منطقي با آن بگونه اي خواهيم بود که پس از برخورد، زمينه تکرار موارد مشابه حذف گردد .
انواع حملات اطلاعاتي بشرح ذيل مي باشند :
غيرفعال
فعال
نزديک (مجاور)
خودي ها (محرمان)
عرضه (توزيع)
ويژگي هر يک از انواع حملات فوق ، بشرح زير مي باشد :
غير فعال (Passive) . اين نوع حملات شامل: آناليزترافيک شبکه ،شنود ارتباطات حفاظت نشده، رمزگشائي ترافيک هاي رمز شده ضعيف و بدست آوردن اطلاعات معتبري همچون رمز عبور مي باشد . ره گيري غيرفعال عمليات شبکه ، مي تواند به مهاجمان، هشدارها و اطلاعات لازم را در خصوص عمليات قريب الوقوعي که قرار است در شبکه اتفاق افتند بدهد(قرار است از مسير فوق در آينده محموله اي ارزشمند عبور داده شود !) ، را خواهد داد .پيامدهاي اين نوع حملات ، آشکارشدن اطلاعات و يا فايل هاي اطلاعاتي براي يک مهاجم ، بدون رضايت و آگاهي کاربر خواهد بود .
فعال (Active) .اين نوع حملات شامل : تلاش در جهت خنثي نمودن و يا حذف ويژگي هاي امنيتي ، معرفي کدهاي مخرب ، سرقت و يا تغيير دادن اطلاعات مي باشد . حملات فوق ، مي تواند از طريق ستون فقرات يک شبکه ، سوء استفاده موقت اطلاعاتي ، نفوذ الکترونيکي در يک قلمرو بسته و حفاظت شده و يا حمله به يک کاربر تاييد شده در زمان اتصال به يک ناحيه بسته و حفاظت شده ، بروز نمايد . پيامد حملات فوق ، افشاي اطلاعات ، اشاعه فايل هاي اطلاعاتي ، عدم پذيرش سرويس و يا تغيير در داده ها ، خواهد بود.
مجاور (Close-in) .اين نوع حملات توسط افرادیکه در مجاورت (نزديکي) سيستم ها قرار دارند با استفاده از تسهيلات موجود ، با يک ترفندي خاص بمنظور نيل به اهدافي نظير : اصلاح ، جمع آوري و انکار دستيابي به اطلاعات باشد، صورت مي پذيرد . حملات مبتني بر مجاورت فيزيکي ، از طريق ورود مخفيانه ، دستيابي باز و يا هردو انجام مي شود .
خودي (Insider) . حملات خودي ها ، مي تواند بصورت مخرب و يا غير مخرب جلوه نمايد . حملات مخرب از اين نوع شامل استراق سمع تعمدي ، سرقت و يا آسيب رساني به اطلاعات ، استفاده از اطلاعات بطرزي کاملا" شيادانه و فريب آميز و يا رد دستيابي ساير کاربران تاييد شده باشد . حملات غير مخرب از اين نوع ، عموما" بدليل سهل انگاري (حواس پرتي) ، فقدان دانش لازم و يا سرپيچي عمدي از سياست هاي امنيتي صورت پذيرد.
توزيع (Distribution) . حملات از اين نوع شامل کدهاي مخربي است که در زمان تغيير سخت افزار و يا نرم افزار در محل مربوطه (کارخانه ، شرکت) و يا در زمان توزيع آنها (سخت افزار ، نرم افزار) جلوه مي نمايد . اين نوع حملات مي تواند، کدهاي مخربي را در بطن يک محصول جاسازي نمايد . نظير يک درب از عقب که امکان دستيابي غيرمجاز به اطلاعات و يا عمليات سيستم در زمان آتي را بمنظور سوء استفاده اطلاعاتي ، فراهم مي نمايد .
در اين رابطه لازم است ، به ساير موارد نظير آتش سوزي ، سيل ، قطع برق و خطاي کاربران نيز توجه خاصي صورت پذيرد . در بخش دوم اين مقاله ، به بررسي روش هاي ايمن سازي اطلاعات بمنظور نيل به يک استراتژي خاص امنيتي ، خواهيم پرداخت .

استراتژي حفاظت از اطلاعات در شبكه هاي كامپيوتري (بخش دوم)

در بخش اول اين مقاله به چالش هاي سازمانها و موسسات براي حركت بسمت يک سازمان مدرن اطلاعاتي اشاره و پس از بررسي اهميت ايمن سازي اطلاعات بر لزوم تدوين يک استراتژي امنيتي تاكيد گرديد . در اين زمينه به انواع حملات اطلاعاتي نيز اشاره و مشخصات هر يک از آنان توضيح داده شد . در اين بخش ، به بررسي عناصر اساسي در استراتژي پيشنهادي يعني انسان ، تكنولوژي و عمليات خواهيم پرداخت .

ايمن سازي اطلاعات

توفيق در ايمن سازي اطلاعات منوط به حفاظت از اطلاعات و سيستم هاي اطلاعاتي در مقابل حملات است . بدين منظور از سرويس هاي امنيتي متعددي استفاده مي گردد. سرويس هاي انتخابي ، مي بايست پتانسيل لازم در خصوص ايجاد يک سيستم حفاظتي مناسب ، تشخيص بموقع حملات و واكنش سريع را داشته باشند. بنابراين مي توان محور استراتژي انتخابي را بر سه مولفه حفاظت ، تشخيص و واكنش استوار نمود . حفاظت مطمئن ، تشخيص بموقع و واكنش مناسب از جمله مواردي است كه مي بايست همواره در ايجاد يک سيستم امنيتي رعايت گردد. سازمان ها و موسسات، علاوه بر يكپارچگي بين مكانيزم هاي حفاظتي ، مي بايست همواره انتظار حملات اطلاعاتي را داشته و لازم است خود را به ابزارهاي تشخيص و روتين هاي واكنش سريع ، مجهز تا زمينه برخورد مناسب با مهاجمان و بازيافت اطلاعات در زمان مناسب فراهم گردد . يكي از اصول مهم استراتژي "دفاع در عمق" ، برقراري توازن بين سه عنصر اساسي : انسان، تكنولوژي و عمليات ، است . حركت بسمت تكنولوژي اطلاعات بدون افراد آموزش ديده و روتين هاي عملياتي كه راهنماي آنان در نحوه استفاده و ايمن سازي اطلاعات باشد ، محقق نخواهد شد .

انسان

موفقيت در ايمن سازي اطلاعات با پذيرش مسئوليت و حمايت مديريت عالي يک سازمان (معمولا" در سطح مديريت ارشد اطلاعات) و بر اساس شناخت مناسب از تهاجمات ، حاصل مي گردد. نيل به موفقيت با پيگيري سياست ها و روتين هاي مربوطه ، تعيين وظايف و مسئوليت ها ، آموزش منابع انساني حساس (كاربران، مديران سيستم) و توجيه مسئوليت هاي شخصي كاركنان ، حاصل مي گردد.در اين راستا لازم است يک سيستم امنيتي فيزيكي و شخصي بمنظور كنترل و هماهنگي در دستيابي به هر يک از عناصر حياتي در محيط هاي مبتني بر تكنولوژي اطلاعات ، نيز ايجاد گردد . ايمن سازي اطلاعات از جمله مواردي است كه مي بايست موفقيت خود را در عمل و نه در حرف نشان دهد . بنابراين لازم است كه پس از تدوين سياست ها و دستورالعمل هاي مربوطه ، پيگيري مستمر و هدفمند جهت اجراي سياست ها و دستورالعمل ها ، دنبال گردد. بهترين استراتژي تدوين شده در صورتيكه امكان تحقق عملي آن فراهم نگردد ، (سهوا" و يا عمدا") ، هرگز امتياز مثبتي را در كارنامه خود ثبت نخواهد كرد .

با توجه به جايگاه خاص منابع انساني در ايجاد يک محيط ايمن مبتني بر تكنولوژي اطلاعات ، لازم است به موارد زير توجه گردد :

تدوين سياست ها و رويه ها

ارائه آموزش هاي لازم جهت افزايش دانش

مديريت سيستم امنيتي

امنيت فيزيكي

امنيت شخصي

تدابير لازم در خصوص پيشگيري

تكنولوژي

امروزه از تكنولوژي ها ي متعددي بمنظور ارائه سرويس هاي لازم در رابطه با ايمن سازي اطلاعات و تشخيص مزاحمين اطلاعاتي، استفاده مي گردد. سازمان ها و موسسات مي بايست سياست ها و فرآيندهاي لازم بمنظور استفاده از يک تكنولوژي را مشخص تا زمينه انتخاب و بكارگيري درست تكنولوژي در سازمان مربوطه فراهم گردد. در اين رابطه مي

بايست به مواردي همچون : سياست امنيتي ، اصول ايمن سازي اطلاعات، استانداردها و معماري ايمن سازي اطلاعات ، استفاده از محصولات مربوط به ارائه دهندگان شناخته شده و خوش نام ، راهنماي پيكربندي ، پردازش هاي لازم براي ارزيابي ريسک سيستم هاي مجتمع و بهم مرتبط ، توجه گردد . در اين رابطه موارد زير ،پيشنهاد مي گردد : دفاع در چندين محل . مهاجمان اطلاعاتي(داخلي و يا خارجي) ممكن است ، يک هدف را از چندين نقطه مورد تهاجم قرار دهند. در اين راستا لازم است سازمان ها و موسسات از روش هاي حفاظتي متفاوت در چندين محل (سطح) استفاده ، تا زمينه عكس العمل لازم در مقابل انواع متفاوت حملات ، فراهم گردد . در اين رابطه مي بايست به موارد زير توجه گردد :

? دفاع از شبكه ها و زير ساخت . در اين رابطه لازم است شبكه هاي محلي و يا سراسري حفاظت گردند . (حفاظت در مقابل حملات اطلاعاتي از نوع عدم پذيرش خدمات)

? حفاظت يكپارچه و محرمانه براي ارسال اطلاعات در شبكه (استفاده از رمزنگاري و كنترل ترافيک بمنظور واكنش در مقابل مشاهده غيرفعال)

? دفاع در محدوده هاي مرزي . (بكارگيري فايروال ها و سيستم هاي تشخيص مزاحمين بمنظور واكنش در مقابل حملات اطلاعاتي از نوع فعال)

? دفاع در محيط هاي محاسباتي (كنترل هاي لازم بمنظور دستيابي به ميزبان ها و سرويس دهنده بمنظور واكنش لازم در مقابل حملات از نوع خودي، توزيع و مجاور) .

دفاع لايه اي . بهترين محصولات مربوط به ايمن سازي اطلاعات داراي نقاط ضعف ذاتي ، مربوط به خود مي باشند. بنابراين همواره زمان لازم در اختيار مهاجمان اطلاعاتي براي نفوذ در سيستم هاي اطلاعاتي وجود خواهد داشت.بدين ترتيب لازم است قبل از سوءاستفاده اطلاعاتي متجاوزان، اقدامات مناسبي صورت پذيرد. يكي از روش هاي موثر پيشگيري در اين خصوص ، استفاده از دفاع لايه اي در مكان هاي بين مهاجمان و اهداف مورد نظر آنان ،مي باشد . هر يک از مكانيزم هاي انتخابي ، مي بايست قادر به ايجاد موانع لازم در ارتباط با مهاجمان اطلاعاتي (حفاظت) و تشخيص بموقع حملات باشد . بدين ترتيب امكان تشخيص مهاجمان اطلاعاتي افزايش و از طرف ديگر شانس آنها بمنظور نفوذ در سيستم و كسب موفقيت، كاهش خواهد يافت . استفاده از فايروال هاي تودرتو (هر فايروال در كنار خود از يک سيستم تشخيص مزاحمين ، نيز استفاده مي نمايد) در محدوده هاي داخلي و خارجي شبكه ، نمونه اي از رويكرد دفاع لايه اي است . فايروال هاي داخلي ممكن است امكانات بيشتري را در رابطه با فيلتر سازي داده ها و كنترل دستيابي به منابع موجود ارائه نمايند

تعيين ميزان اقتدار امنيتي هر يک از عناصر موجود در ايمن سازي اطلاعات (چه چيزي حفاظت شده و نحوه برخورد با تهاجم اطلاعاتي در محلي كه از عنصر مربوطه استفاده شده ، به چه صورت است ؟) . پس از سنجش ميزان اقتدار امنيتي هر يک از عناصر مربوطه ، مي توان از آنان در جايگاهي كه داراي حداكثر كارآئي باشند ، استفاده كرد . مثلا" مي بايست از مكانيزم هاي امنيتي مقتدر در محدوده هاي مرزي شبكه استفاده گردد .

استفاده از مديريت كليد مقتدر و زير ساخت كليد عمومي، كه قادر به حمايت از تمام تكنولوژي هاي مرتبط با ايمن سازي اطلاعات بوده و داراي مقاومت مطلوب در مقابل يک تهاجم اطلاعاتي باشد.

بكارگيري زيرساخت لازم بمنظور تشخيص مزاحمين ، آناليز و يكپارچگي نتايج بمنظور انجام واكنش هاي مناسب در رابطه با نوع تهاجم . زير ساخت مربوطه مي بايست به پرسنل عملياتي، راهنمائي لازم در مواجه با سوالاتي نظير : آيا من تحت تهاجم اطلاعاتي قزار گرفته ام ؟ منبع تهاجم چه كسي مي باشد ؟ به چه فرد ديگري تهاجم شده است ؟ راه حل ها و راهكارهاي من در اين رابطه چيست ؟ ، را ارائه نمايد.

عمليات

منظور از عمليات ، مجموعه فعاليت هاي لازم بمنظور نگهداري وضعيت امنيتي يک سازمان است . در اين رابطه لازم است ، به موارد زير توجه گردد :

پشتيباني ملموس و بهنگام سازي سياست هاي امنيتي

اعمال تغييرات لازم با توجه به روند تحولات مرتبط با تكنولوژي اطلاعات. در اين رابطه مي بايست داده هاي مورد نظر

جمع آوري تا زمينه تصميم سازي مناسب براي مديريت فراهم گردد (تامين اطلاعات ضروري براي مديريت ريسک) .
مديريت وضعيت امنيتي با توجه به تكنولوژي هاي استفاده شده در رابطه ايمن سازي اطلاعات (نصب Patch امنيتي، بهنگام سازي ويروس ها ، پشتيباني ليست هاي كنترل دستيابي)
ارائه سرويس هاي مديريتي اساسي و حفاظت از زيرساخت هاي مهم (خصوصا" زير ساخت هائي كه براي يک سازمان ختم به درآمد مي گردد) .

ارزيابي سيستم امنيتي

هماهنگي و واكنش در مقابل حملات جاري
تشخيص حملات و ارائه هشدار و پاسخ مناسب بمنظور ايزوله نمودن حملات و پيشگيري از موارد مشابه
بازيافت و برگرداندن امور به حالت اوليه (بازسازي)

مدرسه هكرها !

اشاره

در حال حاضر سياست كشورهاي جهان بر اين است كه نفوذ و نفوذگري را ممنوع كنند و هر آن چه را كه بوي هك از آن به مشام مي‌رسد محكوم نمايند. اما ميوه ممنوعه وسوسه‌كننده است و اقداماتي كه در جهت بستن دست هكرها صورت مي‌گيرد، غالباً براي خود هكرها مثل مبارزه‌جويي و حريف‌طلبي است. اما در بارسلونِ اسپانيا با پديده هك نوع ديگري برخورد مي‌شود. در اين شهر براي مبارزه با نفوذگري پروژه جديدي طرح شده است.

• مدرسه هكرها

همان دپارتماني در دانشگاه <لاساله> كه برخي از بهترين طراحان بارسلون را فارغ‌التحصيل مي‌كند، متولي تشكيل <دبيرستان هك> نيز شده است. هدف از اين طرح، برخلاف آن چه كه در ابتداي امر به ذهن مي‌رسد، راه‌اندازي يك <كارگاه شيطاني> نبوده، بلكه هدف آگاه‌سازي و آشنا كردن جوانان با يك تابو مدرن امروزي، يعني پديده هك است. به گفته پت هرتزوگ، مدير اجرايي دبيرستان: <هك چيزي است كه در دنياي واقعي وجود دارد و نمي‌توان آن را كتمان كرد. اما هيچ كس نيامده بگويد اين هك واقعاً چگونه است. همه مي‌گويند صندوق‌پستي شما ممكن است با كرم آلوده شود، يك نفر ممكن است تروجاني را به كامپيوتر شما وارد كند يا مي‌آيند و اطلاعات شما را مي‌دزدند. ولي هيچ كس تا به حال ياد نداده كه اين كارها را چگونه انجام مي‌دهند. همه صرفاً مي‌گويند اين كار غيرقانوني است و هر كس از اين كارها بكند آدم بدي است>.

اين برنامه از طرف ISECOM، مؤسسه امنيت و متدولوژي‌هاي باز (نشاني www.isecom.org) تنظيم شده است، يك مؤسسه غيرانتفاعي كه سعي دارد جوانان را با ناهنجارهاي اينترنتي و بدآموزي‌هايي كه از طرف نااهلان ترويج مي‌شود آشنا كند. دانش‌آموزان به نوعي يك دوره دفاع شخصي ديجيتالي مي‌بينند و ياد مي‌گيرند با كلاهبرداري‌هاي اينترنتي چگونه برخورد كنند، دزدان را چگونه تشخيص دهند و در مقابل حملاتي كه به سيستم‌شان مي‌شود چگونه به دفاع بپردازند. پت هرتزوگ ادامه مي‌دهد: <ما به بچه‌ها نشان مي‌دهيم كه اين كارهاي غيرقانوني چگونه انجام مي‌شود و چه اتفاقي در سيستم مي‌افتد. با اين كار، آن‌ها يك درك فني از موضوع به دست مي‌آورند و مي‌فهمند كه چگونه با حملات مقابله كنند>.
يكي از معلمين اين مدرسه مي‌گويد: <دانش‌آموز بايد ياد بگيرد كه وقتي نامه‌اي دريافت مي‌كند چگونه تشخيص بدهد كه اين نامه واقعاً از طرف چه كسي فرستاده شده، آيا محتواي آن راست است يا دروغ. آن‌ها بايد به همه چيز شك داشته باشند و هر چه مي‌بينند زود باور نكنند>.
بديهي است كه براي ياد دادن اين مسائل، به سيستم‌هاي واقعي نفوذ نمي‌كنند، بلكه مسؤولين ISECOM براي آموزش و آزمايش دانش‌آموزان، چهار سرور آزمايشي تهيه كرده‌اند كه دانش‌آموزان كارهاي خود را روي آن‌ها انجام دهند:

<اگر بچه‌ها دوست داشته باشند هك كردن را تجربه كنند، ما محيط كنترل‌شده‌اي را در اختيارشان قرار مي‌دهيم تا هر كار دلشان مي‌خواهد انجام دهند. منتها از آن‌ها مي‌خواهيم كه به معلمشان بگويند چه كرده‌اند و از چه راهي وارد شده‌اند. ما مي‌خواهيم نفوذگري سالم را به آن‌ها ياد بدهيم و از آن‌ها هكرهاي بااخلاقي بسازيم كه توانايي‌هاي خود را مي‌دانند و حدود خود را هم مي‌دانند>.
مسؤولين مدرسه معتقدند كه براي اين هكرهاي با اخلاق شغل در بازار بيرون فراوان پيدا مي‌شود، چرا كه يكي از پررونق‌ترين مشاغل در صنعت كامپيوتر همين مشاغل حوزه امنيت است.

• متجاوزين فضاي سايبر

در علم حقوق معروف است كه مي‌گويند: اگر ۹۰ درصد چيزي را تصاحب كني، قانوناً مالك آن هستي. اما به نظر مي‌رسد در فضاي سايبر از اين حرف‌ها خبري نيست. وقتي بنيامين كوهن دامنه itunes.co.uk را خريد، فكر مي‌كرد تا هر وقت بخواهد مي‌تواند صاحبش باشد. اما بعدها اپل آمد و سايتي را براي دانلود موسيقي راه انداخت به نام iTunes.com. و از اينجا بود كه موضوع جالب شد.
نام، يكي از ارزشمندترين دارايي‌هاي هر شركت يا شخص است، و از زماني كه سرمايه‌گذاران براي نشاني سايت‌هاي اينترنتي خود شروع به خريد اسامي مشهور كردند، شكايت‌هاي بسياري از سوي اشخاص حقيقي و حقوقي مطرح شد. بسياري از اشخاص يا سازمان‌ها قانوناً موفق شدند كنترل سايت‌هاي همنام خودشان را به دست بگيرند، و <متجاوزين فضاي سايبر> را عقب بنشانند. اما اگر كسي اسمي را بخرد كه بعدها مشهور مي‌شود، چه؟ بنيامين كوهن يك جوان ۲۲ ساله است كه در ساختماني در شرق لندن زندگي مي‌كند. اين جوان در اينترنت ناشناس نيست، چرا كه در سن ۱۷ سالگي با راه‌اندازي چندين وب‌سايت مشهور از همين اتاق كوچك خودش، به يك ميليونر <دات‌كام> تبديل شد. و انتظار داشت از iTunes.co.uk هم سود كلاني ببرد.

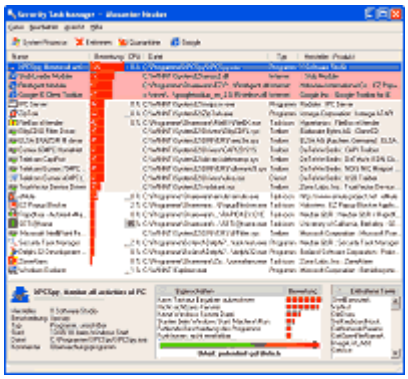
<شركت من در دوره‌اي كه به غرش دات‌كام معروف شد نزديك به ۲۰۰ نام دامنه را ثبت كرد، و ما يك سرويس دانلود موسيقي راه انداختيم كه موتور جستجو هم داشت. Itunes.co.uk داشت به عضو مهمي در مجموعه وب‌سايت‌هاي دانلود موسيقي تبديل مي‌شد. آن زمان اصلاً ITunes اپل وجود نداشت>. اين اظهارات بن كوهن بود.
يك سال بعد، شركت بزرگ كامپيوتري اپل iPod، را خلق كرد، و دو سال بعد از آن، در سال ۲۰۰۳، يك وب‌سايت براي دانلود موسيقي به نام iTunes را افتتاح كرد. اپل خيلي زود توانست از طريق اين سايت هزاران آهنگ را در هر روز به فروش برساند. اپل تصميم گرفت با كوهن تماس بگيرد و پيشنهاد خوبي به او بدهد. خود بنيامين مي‌گويد: <آن‌ها گفتند حاضرند پنج‌هزار دلار بابت اين نام به من بدهند، اما من قبول نكردم. گفتند خودت چقدر در نظر داري؟ من گفتم حداقل پنجاه‌هزار تا، چون به نظر ما اين اسم بيشتر از اين‌ها مي‌ارزد>.
اپل عقب ننشست و شكايتي را تنظيم كرد. در حال حاضر، چهار ميليون نام دامنه با پسوند UK وجود دارد، كه تمام آن‌ها از طريق يك شركت خصوصي به نام Nominet ثبت مي‌شوند. همه مي‌توانند با پرداخت ۵ دلار از اين دامنه‌ها براي خود ثبت كنند و هر كس زودتر بيايد، دامنه به اسم او ثبت مي‌شود. اين شركت يك نقش مهم ديگر هم دارد و آن اين است كه اگر اختلافي بر سر نام دامنه‌ها در بگيرد، شركت به حل و فصل آن مي‌پردازد. خيلي از اين اختلافات با ميانجيگري Nominet و به طور رايگان رفع مي‌شوند، اما بعضي از آن‌ها كه جدي‌تر هستند (مثل همين مورد اپل) به يك كارشناس مستقل امور حقوقي سپرده مي‌شود تا مورد رسيدگي دقيق‌تر قرار بگيرد. اميلي تايلور، مدير بخش حقوقي اين شركت مي‌گويد: <اكثر اختلافات خيلي زود با پادرمياني ما حل مي‌شوند و به ندرت كار به شكايت حقوقي مي‌كشد>.
اپل حتي به دنبال اين نبوده كه از طريق آدرس انگليسي iTunes به فروش بيشتري برسد، چرا كه كوهن پس از مدت كوتاهي، سرويس دانلود موسيقي را از سايت خود حذف كرده بوده است. اين سايت سال‌ها كار نمي‌كرد، يا گاهي هم كه كار مي‌كرد، بازديدكننده را به سايت ديگري مي‌برد كه كوهن براي فروش يك سري خرت و پرت برپا كرده بود. اما اپل

زماني واقعاً نگران شد كه كوهن بازديدكنندگان سايت خود را به Napster هدايت كرد، يعني رقيب اپل. اما وقتي اپل از كوهن خواست كه لينك سايتش را از Napster قطع كند، كوهن پذيرفت و اين كار را كرد.
بعد كوهن به سراغ Napster رفت و پيشنهاد فروش سايتش را به آن‌ها داد: <ما به اين علت اين پيشنهاد را به Napster داديم كه فكر مي‌كرديم يك شركت فعال در زمينه موسيقي به موتور جستجوي سايت ما علاقه‌مند باشد. درست است كه ما از فروش اين سايت به رقيب اپل سود مي‌بريم, ولي اين كار كه غيرقانوني نيست>.
اما Nominet نظر ديگري دارد: <نام دامنه كه مثل ملك و اتومبيل نيست كه از يك دست بخري و از دست ديگر بفروشي. دامنه را مي‌گيري تا از آن استفاده كني. ثبت هر دامنه‌اي يك سري الزامات را به دنبال دارد كه بايد رعايت شوند>.
ماه گذشته، كارشناس مستقل حقوقي Nominet تشخيص داد كه iTunes.co.uk بايد به اپل سپرده شود. اما بن كوهن، اولين نوجوان ميليونر دات‌كام، نه تنها قصد دارد شكايتي را از اپل به دادگاه عالي ببرد، بلكه مي‌خواهد از Nominet سؤال كند كه به چه حقي چنين كاري كرده است. Nominet معتقد است كه تصميمش قانوني و منصفانه است و هفته گذشته كنترل اين نام را به اپل داد. در حال حاضر، اپل از اين آدرس براي عرضه و نمايش iPod و iTunes بهره مي‌گيرد

معرفي نرم‌افزار: Security Task Manager

اشاره :

آيا تا به حال براي شما پيش‌آمده است كه به برخي از برنامه‌هاي مقيم در حافظه كامپيوترتان مشكوک شويد و بخواهيد بدانيد آيا اين برنامه‌ها كار غير مجازي انجام ميدهند يا نه؟



اگر كاربر سيستم‌عامل ويندوز باشيد و هشدارهايي پي در پي كه اين روزها نسبت به اهميت ايمن كردن كامپيوترها منتشر مي شود را جدي گرفته باشيد، احتمالا براي شما پيش آمده مواقعي كه نسبت به هويت يک برنامه بارگذاري شده در حافظه سيستم مشكوک مي‌شويد.

احتمالا پنجره Task Manager ويندوز را باز كرده‌ايد و در آنجا اسامي چند فايل DLL و EXE را ديده‌ايد كه معلوم نيست برخي از آنها واقعا متعلق به كدام برنامه‌اند و چه مي‌كنند.
در اين مواقع خيلي مايليد بدانيد كدام يک از اين برنامه‌ها مشكوک هستند و دست‌كم مي‌خواهيد محل فيزيكي آنها روي هارد ديسک را بدانيد تا شايد با مراجعه به پوشه‌اي كه دربرگيرنده آن فايل است، بتوانيد هويت برنامه را معلوم كنيد.

نرم‌افزار Security Task Manager برنامه ساده و مفيدي براي پاسخ دادن به همين سوالات است. پس از نصب و اجراي اين نرم‌افزار مي‌توانيد فهرستي از برنامه‌هاي مقيم در حافظه، يعني همانهايي كه در پنجره Task Manager ويندوز ديده مي‌شوند را مشاهده كنيد. اين فهرست به ترتيب ميزان مشكوک بودن اين برنامه ها از ديدگاه Security Task Manager (STM) مرتب شده است و با كليک روي نام هر برنامه مي‌توانيد تمام اطلاعاتي كه STM درباره آن فايل جمع آوري كرده است را ببينيد. اگر STM نتواند اطلاعات چنداني درباره آن برنامه بدست آورد، با اختصاص يک نوار قرمز رنگ كه طول آن بيانگر درصد مشكوک بودن STM به آن فايل است، نظر خود را دراين باره نشان مي‌دهد.

خوشبختانه بسياري از فايلهايي كه در رديف فايلهاي مشكوک قرار مي‌گيرند، توسط اطلاعاتي كه خود برنامه جمع اوري كرده است قابل تشخيص هستند. مثلا اگر يک برنامه متعلق به شركت سيمانتک بود، مي‌توانيد نتيجه بگيريد كه خطري از ناحيه آن متوجه كامپيوتر شما نيست زيرا احتمالا بخشي از برنامه امنيتي نورتون است. ولي برخي از فايلها هستند كه در صدر ليست برنامه‌هاي مظنون قرارگرفته‌اند و هويت درست و حسابي هم ندارد. در اين صورت براي مشخصي كردن هويت آنها مي‌توانيد با رايت كليک روي نام آن برنامه، گزينه Google It را از منويي كه باز مي‌شود انتخاب كنيد و ببينيد آيا مي‌توانيد اطلاعاتي درباره آن فايل در اينترنت بيابيد يا نه. در اينصورت ابتدا برنامه مي‌كوشد صفحه‌اي هم نام فايل مذكور در بانک اطلاعاتي مربوط به سايت شركت سازنده STM بيابد، در غير اينصورت مي توانيد به كمک موتور جستجوي گوگل تحقيق كنيد و مطمئن باشيد كه اگر آن فايل مثلا يک اسب تروا يا نرم‌افزار غير مجاز شناخته شده در اينترنت باشد، حتما اطلاعات سودمندي درباره آن پيدا خواهيد كرد كه شما را براي تصميم‌گيري نسبت به حذف آن فايل يا باقي نگهداشتن آن ياري خواهد كرد.

اگر گزينه Remove را از منوي مذكور انتخاب كنيد، مي‌توانيد موقتا يک برنامه مشكوک را از حافظه خارج كنيد و يا آنرا براي هميشه در قرنطينه (پوشه مخصوصي كه يک نسخه پشتيباني از اين فايل در آنجا ذخيره مي‌شود) نگه داريد و آن را پوشه فعلي دربرگيرنده آن حذف كنيد.

سازندگان اين برنامه ادعا مي‌كنند كه شركت مايكروسافت از آن براي آزمايش امن بودن ويندوز لانگ هورن (ويستا) استفاده كرده است و شركت هاي سازنده آنتي ويروس آن را براي يافتن انواع جديد اسب تروا به‌كار مي‌گيرند. اگر مبناي اين ادعا را اطلاعات اندک اما مفيدي قرار دهيم كه اين برنامه درباره هر فايل مقيم در حافظه مي دهد، ممكن است آن را باور كنيم.

شما هم مي‌تواينند STM را امتحان كنيد. نسخه Shareware اين نرم‌افزار سودمند از اين نشاني قابل دريافت است.

نفوذ در يك چشم برهم زدن

سارقان اطلاعات چگونه ممكن است بتوانند از ديواره آتش شما عبور كرده و صدها مگابايت اطلاعات را به سرقت ببرند بدون اين كه هيچ ردپايي از خود به جاي بگذارند؟ يك راهِ ممكن، از طريق همين درايوهاي كوچك USB است كه امروزه من و شما در جيب خود مي‌گذاريم و به هر جايي مي‌بريم. همان طور كه مي‌دانيد، به اين درايوها Flash Disk و Flash Drive هم مي‌گويند، اما اسمشان هرچه كه باشد، بسياري از شركت‌ها و سازمان‌ها هيچ سياست مشخصي براي شناسايي اين درايوها و قاعده‌مند كردن موارد استفاده آنها وضع نكرده‌اند. به همين جهت يك مشتري كه به ملاقات شما آمده، كارشناسي كه سيستمتان را چك مي‌كند، همكاري كه هر روز به شما سر مي‌زند، يا هر فرد باهوش ديگري، به آساني مي‌تواند فلش ديسك خود را در اولين فرصت به پورت USB كامپيوتر شما وصل كرده و صدها فايل اطلاعاتي مهم را با سرعت بالاي USB 2.0 براي خود كپي كند. ظرفيت فلش ديسك‌هاي امروزي از مرز دو گيگابايت گذشته است و همچنان رو به بالا در حركت است و با ابعاد كوچكي كه دارند، خيلي راحت مي‌توان آنها را پنهان كرد. پس چاره چيست؟

سرقت اطلاعات تنها تهديد از جانب اين وسيله كوچك نيست. از آنجا كه كاربران فلش ديسك عمدتاً به خاطر قابل حمل بودن آن، به استفاده از اين وسيله روي

آورده‌اند، بنابراين در حال سفر يا مأموريت نيز از آن استفاده مي‌كنند و زماني كه به اداره برمي‌گردند، بدون توجه به احتمال ويروسي بودن فايل‌ها، فلش ديسك را به كامپيوتر خود وصل و سيستم را آلوده مي‌كنند. نفوذگران مي‌توانند انواع ابزارهاي تخصصي خود را به اين وسيله منتقل كنند، از جمله جاسوس‌افزارها، رمزشكن‌ها، كليدنگارها، و پورت‌خوان‌ها، كه براي شروع نفوذ به يك سيستم اساسي‌ترين ابزار نفوذگر محسوب مي‌شوند. بعد از اين كار، نفوذگر به شيوه‌هاي گوناگون مهندسي اجتماعي، سعي مي‌كند به اتاق‌تان راه يافته يا به كامپيوترتان دست پيدا كند، تا از طريق درايو USB به اعمال شيطاني خود بپردازد. گذشته از اينها، در صورت مفقود شدن فلش ديسك، تمام فايل‌هاي موجود در آن به دست كسي مي‌افتد كه آن را پيدا كرده و اين مي‌تواند براي كل سازمان خطرناك باشد.
چگونه مي‌توان از شبكه سازمان در مقابل اين تهديد محافظت كرد؟ اولين قدم، آموزش دادن به پرسنل است. ابتدا در مجموعه سياست‌هاي امنيتي سازمان، استفاده صحيح و ناصحيح از درايوهاي USB را تشريح كرده و لزوم داشتن مجوز براي استفاده از فلش ديسك را توضيح دهيد. سپس اين موارد را به پرسنل خود آموزش داده و دلايل وجودي هر كدام را برايشان بازگو كنيد.

قدم بعدي اين است كه كامپيوترها را طوري تنظيم كنيد كه در صورت بي‌كار ماندن، بعد از ۳ تا ۵ دقيقه (يا هر مدتي كه خودتان صلاح مي‌دانيد) به طور خودكار قفل شوند. در ويندوز اكس‌پي آسان‌ترين راه براي اين كار، استفاده از screen saver است. نرم‌افزارهاي جانبي زيادي نيز وجود دارند كه از جمله مي‌توان به Desktop Lock محصول شركت نرم‌افزاي TopLang Software، PC Lockup محصول Ixis،SpyLock محصول Spytech Software و StayOut محصول Tomorroware اشاره كرد.
قدم ديگر اين است كه براي پرسنل مورد نظر خود، USB درايوهاي مطئمني را تهيه كنيد. به عنوان مثال، Lexar Media JumpDrive Secure يك فلش‌درايو USB است كه به صورت توكار با رمزعبور محافظت مي‌شود. شركت SanDisk نرم‌افزاري به نام CruzerLock را همراه با فلش‌درايوهاي خود عرضه مي‌كند كه امكان گذاشتن كلمه عبور و رمز كردن فايل‌ها را به شما مي‌دهد. حتي بعضي شركت‌ها محصولاتي دارند كه فقط با اثر انگشت صاحب اصلي كار مي‌كنند.
نكته ديگر اين است كه نرم‌افزار ويروس‌ياب خود را طوري تنظيم كنيد كه تمام درايوها و ابزارهاي جابه‌جا شدني را در هنگام اسكن در نظر بگيرد. به كاربران ياد بدهيد كه قبل از كپي كردن چيزي به كامپيوتر خود، ابتدا مطمئن شوند اسكن حتماً انجام گرفته يا خودشان به طور دستي به اسكن فلش ديسك بپردازند.
حتي براي تضمين امنيت بيشتر، مي‌توانيد پورت‌هاي USB را غيرفعال كنيد. اين يكي شايد زيادي امنيتي باشد، ولي اگر لازم است مي‌توانيد حتي از طريق رمزعبور BIOS كامپيوترها را قفل كنيد. اما اگر به دنبال يك شيوه حفاظتي حرفه‌اي هستيد، راه‌حلSecureNT محصول SecureWave را پيش بگيريد، كه اجازه مي‌دهد دسترسي كاربران نهايي به بعضي قطعات ورودي-خروجي (از جمله پورت‌هاي USB) را تحت كنترل خود درآوريد. با استفاده از اين نرم‌افرار حتي مي‌توانيد فهرستي از قطعات مورد تأييد را ايجاد كنيد تا دسترسي به هر وسيله‌اي خارج از اين فهرست ممنوع شود. همچنين مي‌توانيد بر موارد استفاده تمام اين وسايل نظارت داشته باشيد.

نكته آخر اين كه، به تمام كاربران بگوييد يك فايل متني حاوي اسم و نشاني خود روي فلش ديسك درست كنند تا در صورت مفقود شدن آن، يابنده بتواند آنها را پيدا كند. منتها دقت كنيد كه خود اين فايل نبايد رمز شده باشد.

يكي از استدلال‌هايي كه طرفداران جنبش اپن‌سورس در حمايت از اين حركت مطرح مي‌كنند (اگر بخواهيم خيلي كلي و خودماني بگوييم) اين است كه مي‌گويند شركت‌هايclosedsource ، كه معروف‌ترين‌شان مايكروسافت است، در اشتباهند كه فكر مي‌كنند در دسترس نبودن سورس كد برنامه‌هاي آنها امنيت محصولات‌شان را بالاتر مي‌برد.

مدافعان اپن‌سورس با تحقير چنين طرز فكري آن را تأمين> امنيت از طريق ابهام security through obscurity <مي‌نامند و تأكيد دارند كه اشكالات و حفره‌هاي موجود در محصولات، خواهي‌نخواهي برملا مي‌شوند و در مقابل اين استدلال كاملاً متضاد را مي‌آورند كه محصولات اپن‌سورس اتفاقاً امنيت بيشتري خواهند داشت، چرا كه هر كس مي‌تواند به معاينه آن‌ها پرداخته و اشكالات آن را برطرف كند.

چنين نظريه‌اي تا چه اندازه مي‌تواند صحيح باشد؟ به زودي خواهيم فهميد، چرا كه قسمت‌هايي از سورس ويندوز NT4 و 2000 به اينترنت نشت كرده است.

پيش‌بيني شده است كه انتشار اين كد موجب افزايش حملات به ويندوز خواهد شد. اگر اين پيش‌بيني درست از آب در بيايد، پس بايد قبول كنيم كه امنيت با ابهام تأمين مي‌شود. اگر با پنهان كردن چيزي امنيت آن بيشتر نمي‌شود، پس با آشكار كردن آن نبايد امنيتش كمتر شود .

توجه داشته باشيد كه بحث ما بر سر كد دو محصولي است كه سال‌ها از عمرشان مي‌گذرد. سورس NT4 مربوط به سرويس پك ۳ انتي است، كه IIS نداشت و IE آن هم ۴ بود. كد ويندوز ۲۰۰۰ هم زيرمجموعه بسيار كوچكي از سرويس پك ۱ ويندوز ۲۰۰۰ است كه شامل IE5 ، SNMP، PKIو يك سري كد SDK مي‌شود. بعيد است كه افشا شدن اين كدها خطر جديد آنچنان مهمي براي ويندوزهاي جديد باشد. با آن همه شلوغ‌كاري‌هايي كه براي نوشتن يك برنامه در آن زمان‌ها مجبور بوديم انجام دهيم، بعيد است كسي حاضر شود كه ميان ۵۵ هزار فايل به جستجو بپردازد تا حفره يا راه نفوذي پيدا كند.

اولاً كسي كه سيستمي با اين نسخه‌هاي ويندوز داشته باشد، خود به خود در معرض خطر حمله به نقطه‌ضعف‌هاي شناخته شده‌اي قرار داد كه قبل از افشا اين سورس‌ها كشف شده بودند. پس غيرمنطقي نيست كه فرض كنيم كسي از اين سورس‌ها سوءاستفاده نخواهد كرد. ثانياً مگر چه مقدار از كد ويندوز امروز با كد ويندوزهاي نامبرده مشترك است؟ به عبارت ديگر، چه ميزان از حملات امروز مي‌تواند بر اساس سورس‌هاي ۳ يا ۴ سال گذشته پايه‌ريزي شده باشد؟ اگر اين ميزان زياد باشد، پس باز هم بايد قبول كنيم در ابهام است كه امنيت بهتر حفظ مي‌شود. نفوذگران كلاه سياه و كلاه سفيد سال‌ها توان خود را براي شكستن اين كدها صرف كردند و حالا اگر حمله قابل ملاحظه‌اي با افشاي اين كدها صورت بگيرد، پس بايد بپذيريم كه سورس‌ها مهم بوده‌اند.

اگر به فهرست مؤسساتي كه مجوز سورس كد ويندوز را دارند نگاه كنيد) در اين نشاني (تعجب مي‌كنيد كه پس چرا درز كردن سورس‌هاي ويندوز اين همه طول كشيده است. ولي با توجه به توافق‌نامه‌هايي كه مايكروسافت امضاء آن‌ها را هنگام ارائه مجوز از خريداران مي‌گيرد و يك سري الزامات قانوني ديگر، معلوم است كه چرا چنين اتفاقاتي زود به زود رخ نمي‌دهند.

تحليلگر ديگري در اين رابطه معتقد است كه اين حادثه همان قدر بي‌اهميت است كه مثلاً يك ژنرال روسي جنگ جهاني دوم را امروز دستگير كنيم .البته اين حرف شايد خيلي اغراق‌آميز باشد، ولي به هر ترتيب نشان‌دهنده اين واقعيت است كه كد افشا شده تا حدود زيادي منسوخ شده است.

در مجموع، تمام حرف و حديث‌هايي كه بعد از افشا شدن اين كدها درباره افزايش احتمالي حملات به ويندوز در گوشه و كنار نقل مي‌شوند (صرف‌نظر از صحت و سقم آن‌ها) نشان مي‌دهند كه مردود دانستن استدلال امنيت از طريق ابهام زياد هم آسان نيست. به هر ترتيب، در اين رابطه حد مياني وجود ندارد: بسته بودن كد يا موجب امنيت بيشتر مي‌شود يا نمي‌شود. بايد صبر كنيم ببينيم در آينده چه اتفاقي مي‌افتد.

شبکه اترنت

دستیابی به اطلاعات با روش های مطمئن و با سرعت بالا یکی از رموز موفقیت هر سازمان و موسسه است . طی سالیان اخیر هزاران پرونده و کاغذ که حاوی اطلاعات با ارزش برای یک سازمان بوده ، در کامپیوتر ذخیره شده اند. با تغذیه دریائی از اطلاعات به کامپیوتر ، امکان مدیریت الکترونیکی اطلاعات فراهم شده است . کاربران متفاوت در اقصی نقاط جهان قادر به اشتراک اطلاعات بوده و تصویری زیبا از همیاری و همکاری اطلاعاتی را به نمایش می گذارند.

شبکه های کامپیوتری در این راستا و جهت نیل به اهداف فوق نقش بسیار مهمی را ایفاء می نمایند.اینترنت که عالی ترین تبلور یک شبکه کامپیوتری در سطح جهان است، امروزه در مقیاس بسیار گسترده ای استفاده شده و ارائه دهندگان اطلاعات ، اطلاعات و یا فرآورده های اطلاعاتی خود را در قالب محصولات تولیدی و یا خدمات در اختیار استفاده کنندگان قرار می دهند. وب که عالی ترین سرویس خدماتی اینترنت می باشد کاربران را قادر می سازد که در اقصی نقاط دنیا اقدام به خرید، آموزش ، مطالعه و ... نمایند.

با استفاده از شبکه، یک کامپیوتر قادر به ارسال و دریافت اطلاعات از کامپیوتر دیگر است . اینترنت نمونه ای عینی از یک شبکه کامپیوتری است . در این شبکه میلیون ها کامپیوتر در اقصی نقاط جهان به یکدیگر متصل شده اند.اینترنت شبکه ای است مشتمل بر زنجیره ای از شبکه های کوچکتراست . نقش شبکه های کوچک برای ایجاد تصویری با نام اینترنت بسیار حائز اهمیت است . تصویری که هر کاربر با نگاه کردن به آن گمشده خود را در آن پیدا خواهد کرد. در این بخش به بررسی شبکه های کامپیوتری و جایگاه مهم آنان در زمینه تکنولوژی اطلاعات و مدیریت الکترونیکی اطلاعات خواهیم داشت .

شبکه های محلی و شبکه های گسترده

تاکنون شبکه های کامپیوتری بر اساس مولفه های متفاوتی تقسیم بندی شده اند. یکی از این مولفه ها " حوزه جغرافیائی " یک شبکه است . بر همین اساس شبکه ها به دو گروه عمده Local area network LAN)) و Wide(WAN network area) تقسیم می گردند. در شبکه های LAN مجموعه ای از دستگاه های موجود در یک حوزه جغرافیائی محدود، نظیر یک ساختمان به یکدیگر متصل می گردند . در شبکه های WAN تعدادی دستگاه که از یکدیگر کیلومترها فاصله دارند به یکدیگر متصل خواهند شد. مثلا" اگر دو کتابخانه که هر یک در یک ناحیه از شهر بزرگی مستقر می باشند، قصد اشتراک اطلاعات را داشته باشند، می بایست شبکه ای WAN ایجاد و کتابخانه ها را به یکدیگر متصل نمود. برای اتصال دو کتابخانه فوق می توان از امکانات مخابراتی متفاوتی نظیر خطوط اختصاصی (Leased) استفاده نمود. شبکه های LAN نسبت به شبکه های WAN دارای سرعت بیشتری می باشند. با رشد و توسعه دستگاههای متفاوت مخابراتی میزان سرعت شبکه های WAN ، تغییر و بهبود پیدا کرده است . امروزه با بکارگیری و استفاده از فیبر نوری در شبکه های LAN امکان ارتباط دستگاههای متعدد که در مسافت های طولانی نسبت بیکدیگر قرار دارند، فراهم شده است .

تقسیم بندی شبکه ها

.شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد .

- تقسیم بندی بر اساس نوع وظایف . کامپیوترهای موجود در شبکه را با توجه به نوع وظایف مربوطه به دو گروه عمده : سرویس دهندگان (Servers) و یا سرویس گیرندگان (Clients) تقسیم می نمایند. کامپیوترهائی در شبکه که

برای سایر کامپیوترها سرویس ها و خدماتی را ارائه می نمایند ، سرویس دهنده نامیده می گردند. کامپیوترهائی که از خدمات و سرویس های ارائه شده توسط سرویس دهندگان استفاده می کنند ، سرویس گیرنده نامیده می شوند .

در شبکه های Client-Server ، یک کامپیوتر در شبکه نمی تواند هم بعنوان سرویس دهنده و هم بعنوان سرویس گیرنده ، ایفای وظیفه نماید.

در شبکه های Peer-To-Peer ، یک کامپیوتر می تواند هم بصورت سرویس دهنده و هم بصورت سرویس گیرنده ایفای وظیفه نماید.

یک شبکه LAN در ساده ترین حالت از اجزای زیر تشکیل شده است :

- دو کامپیوتر شخصی . یک شبکه می تواند شامل چند صد کامپیوتر باشد. حداقل یکی از کامپیوترها می بایست بعنوان سرویس دهنده مشخص گردد. (در صورتیکه شبکه از نوع Client-Server باشد). سرویس دهنده، کامپیوتری است که هسته اساسی سیستم عامل بر روی آن نصب خواهد شد.

- یک عدد کارت شبکه (NIC) برای هر دستگاه. کارت شبکه نظیر کارت هائی است که برای مودم و صدا در کامپیوتر استفاده می گردد. کارت شبکه مسئول دریافت ، انتقال ، سازماندهی و ذخیره سازی موقت اطلاعات در طول شبکه است . بمنظور انجام وظایف فوق کارت های شبکه دارای پردازنده ، حافظه و گذرگاه اختصاصی خود هستند.

• تقسیم بندی بر اساس توپولوژی . الگوی هندسی استفاده شده جهت اتصال کامپیوترها ، توپولوژی نامیده می شود. توپولوژی انتخاب شده برای پیاده سازی شبکه ها، عاملی مهم در جهت کشف و برطرف نمودن خطاء در شبکه خواهد بود. انتخاب یک توپولوژی خاص نمی تواند بدون ارتباط با محیط انتقال و روش های استفاده از خط مطرح گردد. نوع توپولوژی انتخابی جهت اتصال کامپیوترها به یکدیگر ، مستقیما" بر نوع محیط انتقال و روش های استفاده از خط تاثیر می گذارد. با توجه به تاثیر مستقیم توپولوژی انتخابی در نوع کابل کشی و هزینه های مربوط به آن ، می بایست با دقت و تامل به انتخاب توپولوژی یک شبکه همت گماشت . عوامل مختلفی جهت انتخاب یک توپولوژی بهینه مطرح می شود. مهمترین این عوامل بشرح ذیل است :

- هزینه . هر نوع محیط انتقال که برای شبکه LAN انتخاب گردد، در نهایت می بایست عملیات نصب شبکه در یک ساختمان پیاده سازی گردد. عملیات فوق فرآیندی طولانی جهت نصب کانال های مربوطه به کابل ها و محل عبور کابل ها در ساختمان است . در حالت ایده آل کابل کشی و ایجاد کانال های مربوطه می بایست قبل از تصرف و بکارگیری ساختمان انجام گرفته باشد. بهرحال می بایست هزینه نصب شبکه بهینه گردد.

- انعطاف پذیری . یکی از مزایای شبکه های LAN ، توانائی پردازش داده ها و گستردگی و توزیع گره ها در یک محیط است . بدین ترتیب توان محاسباتی سیستم و منابع موجود در اختیار تمام استفاده کنندگان قرار خواهد گرفت . در ادارات همه چیز تغییر خواهد کرد.(لوازم اداری، اتاقها و ...) . توپولوژی انتخابی می بایست بسادگی امکان تغییر پیکربندی در شبکه را فراهم نماید. مثلا" ایستگاهی را از نقطه ای به نقطه دیگر انتقال و یا قادر به ایجاد یک ایستگاه جدید در شبکه باشیم .

سه نوع توپولوژی رایج در شبکه های LAN استفاده می گردد :

§ BUS § STAR § RING

توپولوژی . BUS یکی از رایجترین توپولوژی ها برای پیاده سازی شبکه های LAN است . در مدل فوق از یک کابل بعنوان ستون فقرات اصلی در شبکه استفاده شده و تمام کامپیوترهای موجود در شبکه) سرویس دهنده ، سرویس گیرنده) به آن متصل می گردند .

مزایای توپولوژی BUS

- کم بودن طول کابل . بدلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها ، در توپولوژی فوق از کابل کمی استفاده می شود.موضوع فوق باعث پایین آمدن هزینه نصب و ایجاد تسهیلات لازم در جهت پشتیبانی شبکه خواهد بود.

- ساختار ساده . توپولوژی BUS دارای یک ساختار ساده است . در مدل فوق صرفا" از یک کابل برای انتقال اطلاعات استفاده می شود.

- توسعه آسان . یک کامپیوتر جدید را می توان براحتی در نقطه ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاههای بیشتر در یک سگمنت ، می توان از تقویت کننده هائی به نام Repeater استفاده کرد.

معایب توپولوژی BUS

- مشکل بودن عیب یابی . با اینکه سادگی موجود در تویولوژی BUS امکان بروز اشتباه را کاهش می دهند، ولی در صورت بروز خطاء کشف آن ساده نخواهد بود. در شبکه هائی که از توپولوژی فوق استفاده می نمایند ، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطاء می بایست نقاط زیادی بمنظور تشخیص خطاء بازدید و بررسی گردند.

- ایزوله کردن خطاء مشکل است . در صورتیکه یک کامپیوتر در توپولوژی فوق دچار مشکل گردد ، می بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می توان یک گره را از شبکه جدا کرد. در حالتیکه اشکال در محیط انتقال باشد ، تمام یک سگمنت می بایست از شبکه خارج گردد.

- ماهیت تکرارکننده ها . در مواردیکه برای توسعه شبکه از تکرارکننده ها استفاده می گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود. موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است .

توپولوژی . STAR در این نوع توپولوژی همانگونه که از نام آن مشخص است ، از مدلی شبیه "ستاره" استفاده می گردد. در این مدل تمام کامپیوترهای موجود در شبکه معمولا" به یک دستگاه خاص با نام " هاب " متصل خواهند شد .

مزایای توپولوژی STAR

- سادگی سرویس شبکه . توپولوژی STAR شامل تعدادی از نقاط اتصالی در یک نقطه مرکزی است . ویژگی فوق تغییر در ساختار و سرویس شبکه را آسان می نماید.

- در هر اتصال یکدستگاه . نقاط اتصالی در شبکه ذاتا" مستعد اشکال هستند. در توپولوژی STAR اشکال در یک اتصال ، باعث خروج آن خط از شبکه و سرویس و اشکال زدائی خط مزبور است . عملیات فوق تاثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت .

- کنترل مرکزی و عیب یابی . با توجه به این مسئله که نقطه مرکزی مستقیما" به هر ایستگاه موجود در شبکه متصل است ، اشکالات و ایرادات در شبکه بسادگی تشخیص و مهار خواهند گردید.

- روش های ساده دستیابی . هر اتصال در شبکه شامل یک نقطه مرکزی و یک گره جانبی است . در چنین حالتی دستیابی به محیط انتقال جهت ارسال و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

معایب توپولوژی STAR

- زیاد بودن طول کابل . بدلیل اتصال مستقیم هر گره به نقطه مرکزی ، مقدار زیادی کابل مصرف می شود. با توجه به اینکه هزینه کابل نسبت به تمام شبکه ، کم است ، تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبنی آنها بطور قابل توجهی هزینه ها را افزایش خواهد داد.

- مشکل بودن توسعه . اضافه نمودن یک گره جدید به شبکه مستلزم یک اتصال از نقطه مرکزی به گره جدید است . با اینکه در زمان کابل کشی پیش بینی های لازم جهت توسعه در نظر گرفته می شود ، ولی در برخی حالات نظیر زمانیکه طول زیادی از کابل مورد نیاز بوده و یا اتصال مجموعه ای از گره های غیر قابل پیش بینی اولیه ، توسعه شبکه را با مشکل مواجه خواهد کرد.

- وابستگی به نقطه مرکزی . در صورتیکه نقطه مرکزی (هاب) در شبکه با مشکل مواجه شود ، تمام شبکه غیرقابل استفاده خواهد بود.

کامپیوترها بصورت یک حلقه به یکدیگر مرتبط می گردند. تمام کامپیوترهای در این نوع توپولوژی تمام . RING توپولوژی می گردند. شبکه (سرویس دهنده ، سرویس گیرنده) به یک کابل که بصورت یک دایره بسته است ، متصل موجود در از گره مجاور دریافت و به گره بعدی در مدل فوق هر گره به دو و فقط دو همسایه مجاور خود متصل است . اطلاعات .حرکت کرده و از ایستگاهی به ایستگاه دیگر انتقال پیدا می کنند ارسال می شوند. بنابراین داده ها فقط در یک جهت

مزایای توپولوژی RING

- کم بودن طول کابل . طول کابلی که در این مدل بکار گرفته می شود ، قابل مقایسه به توپولوژی BUS نبوده و طول کمی را در بردارد. ویژگی فوق باعث کاهش تعداد اتصالات (کانکتور) در شبکه شده و ضریب اعتماد به شبکه را افزایش خواهد داد.

- نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود.بدلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش ، اختصاص محل هائی خاص بمنظور کابل کشی ضرورتی نخواهد داشت .

- مناسب جهت فیبر نوری . استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده ها در یک جهت است ، می توان از فیبر نوری بمنظور محیط انتقال استفاده کرد.در صورت تمایل می توان در هر بخش ازشبکه از یک نوع کابل بعنوان محیط انتقال استفاده کرد . مثلا" در محیط های ادرای از مدل های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

معایب توپولوژی RING

- اشکال در یک گره باعث اشکال در تمام شبکه می گردد. در صورت بروز اشکال در یک گره ، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانیکه گره معیوب از شبکه خارج نگردد ، هیچگونه ترافیک اطلاعاتی را روی شبکه نمی توان داشت .

- اشکال زدائی مشکل است . بروز اشکال در یک گره می تواند روی تمام گرههای دیگر تاثیر گذار باشد. بمنظور عیب یابی می بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.

- تغییر در ساختار شبکه مشکل است . در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه ، بدلیل ماهیت حلقوی شبکه مسائلی بوجود خواهد آمد .

- توپولوژی بر روی نوع دستیابی تاثیر می گذارد. هر گره در شبکه دارای مسئولیت عبور دادن داده ای است که از گره مجاور دریافت داشته است . قبل از اینکه یک گره بتواند داده خود را ارسال نماید ، می بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است .

- تقسیم بندی بر اساس حوزه جغرافی تحت پوشش . شبکه های کامپیوتری با توجه به حوزه جغرافیائی تحت پوشش به سه گروه تقسیم می گردند :

  - شبکه های محلی (کوچک) LAN
  - شبکه های متوسط MAN
  - شبکه های گسترده WAN

شبکه های LAN . حوزه جغرافیائی که توسط این نوع از شبکه ها پوشش داده می شود ، یک محیط کوچک نظیر یک ساختمان اداری است . این نوع از شبکه ها دارای ویژگی های زیر می باشند :

  - توانائی ارسال اطلاعات با سرعت بالا
  - محدودیت فاصله
  - قابلیت استفاده از محیط مخابراتی ارزان نظیر خطوط تلفن بمنظور ارسال اطلاعات
  - نرخ پایین خطاء در ارسال اطلاعات با توجه به محدود بودن فاصله

شبکه های MAN . حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه یک شهر و یا شهرستان است . ویژگی های این نوع از شبکه ها بشرح زیر است :

  - پیچیدگی بیشتر نسبت به شبکه های محلی
  - قابلیت ارسال تصاویر و صدا
  - قابلیت ایجاد ارتباط بین چندین شبکه

شبکه های WAN . حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه کشور و قاره است . ویژگی این نوع شبکه ها بشرح زیر است :

- § قابلیت ارسال اطلاعات بین کشورها و قاره ها
- § قابلیت ایجاد ارتباط بین شبکه های LAN
- § سرعت پایین ارسال اطلاعات نسبت به شبکه های LAN
- § نرخ خطای بالا با توجه به گستردگی محدوده تحت پوشش

راه هايي آسانتر براي عيب يابي شبكه ها

راهنماي عيب يابي اولين چيزي كه باعث مي شود تكنسين شبكه بتواند ايراد احتمالي را تشخيص دهد ، بررسي اين موضوع است كه پيش از اين شبكه در چه شرايطي به طور صحيح كار مي كرده است . شناخت آن شرايط باعث تشخيص آسانتر عامل پديد آورنده خطا مي گردد . اما متاسفانه بعضي از تجهيزات شبكه فاقد داده هاي فني لازم براي رفع عيب يا مستنداتي براي آگاهي يافتن از شرايط كاركرد صحيح آن ها هستند و متخصصان هنگامي در كار با آن هاموفق هستند كه نمونه هاي مختلفي از آن ها را ديده ، نصب كرده و با شرايط كاركرد آن ها آشنا باشند . اما همان متخصصان هم ممكن است فراموش كنند كه كدام يك از دستگاه ها ، در كدام شرايط بهترعمل مي كردند يا كدام پيكر بندي براي كدام محيط مناسب تر بوده است . براي آنكه فاصله بين تكنسين هاي مختلف با يكديگر كمتر شود و راه يافتن خطا ها كوتاه تر گردد ، رعايت نج نكته ضروري است . اين موارد را مي توان پنج گام براي كسب موفقيت در كشف خطا نام گذاشت .

گام اول : مستند سازي شبكه

در دست داشتن آخرين نقشه هاي فيزيكي و منطقي شبكه ، كمك شاياني به شناخت وضعيت فعلي شبكه مي نمايد . با اين نقشه ها مي توان ادوات مختلف ، پيكر بندي ها ، و آدرس ها راتحت نظارت داشت . ضمن آنكه از اين طريق كار عيب يابي آسانتر مي گردد.

گام دوم : جمع آوري كليه اطلاعات و تحليل خطاي پيش آمده

فرض كنيد كه اشكال كار مي دانيد ، آيا مي توانيد آن را مستند كنيد ؟ آيا قبل ازبروز خطا ، هشداري از ايستگاه هاي كاري صادر نشده است ؟ براي اين كه اين مرحله را ساده تر كنيئ . مي توانيد از دستگاه LinkRunner، محصول شركت Fluke Networks استفاده كنيد . اين ابزار كه به سادگي قابل حمل است مي تواند اشكالات اوليه درلايه فيزيكي را نشان دهد . اين ابزار مي تواند در خدمت تكنسين ها باشد تا در صورتي كه اشكال شبكه ، فراتر از اشكالات معمولي بود ، از متخصصان مجرب تري استفاده گردد. پس در گام دوم ، با استفاده از ابزارهاي كمكي به جمع آوري كليه اطلاعات موجود مي پردازيم و اشكالات لايه فيزيكي رابررسي مي نماييم .

گام سوم : دامنه مشكل ايجاد شده را محدود كنيد

قدم بعدي محدود كردن دامنه مشكل ايجاد شده است . بايد بررسي كنيم كه مشكل مربوط به بخشي از شبكه است يا فقط به يك كانيت محدود است ؟ مثلا اگر مشكل مربوط ب هكلانيت است پس به كابل فيزيكي يا ايستگاه كاري محدود مي گردد. يعني پس از جمع آوري اطلاعات،بايد آن را به مشكل پيش آمده محدود نماييم .

گام چهارم : مشكل را رفع كنيد

پس از محدود كردن دامنه مشكل ، رفع آن آسان خواهد شد . در مورد ادوات سخت افزاري ، معمولا بايد آن را تعويض نمود . مثلا تعويض Patch Cable يا تغيير پورت سوئيچ يا تعويض كارت شبكه كلانيت . اين گام وقتي تكميل مي شود كه پس از رفع عيب ، شبكه مجددا تست شودتا ازرفع كامل اشكال اطمينان حاصل گردد.

گام پنجم : كارهاي انجام نشده را مستند كنيد

حالا بايد مجددا گام اول را تكرار كنيد . يعني مشكل پيش آمده و نحوه رفع آن را مستند سازي كنيد . اين كاربر براي مراجعات بعدي بسيار مفيد خواهد بود .

اما آيا انجام اين دادن همه اين مراحل لازم است ؟

گاهي پيش مي آيد كه مشكلات شبكه ، ناشي از اشكلات سيستم عامل است . غلب تكنسين هايي كه در واحدهاي فني مستقر هستند ، هنگام انجام راهنمايي تلفني ، به كاربران مي گويند كه «يك بار كامپيوترتان را بوت كنيد .» اين راه حل ، در بعضي موارد مشكل را مرتفع مي كند و ديگر نياز به طي كردن گام هاي پنج گانه نيست .

حسن اين كاردر اين است كه تكنسين بدون اين كه محل كارش را ترك كند ، مشكل را برطرف نموده است .

اما بعضي مشكلات با بوت كردن ساده از بين نمي روند . در اين موقع ، در صورتي كه كاربر كامپيو تر بتواند از خط فرمان (Command Prompt) سيستم عامل استفاده نمايد ، راهنمايي تلفني را همچنان مي توان ادامه داد . يعني فرمان IPCONFIG مي تواند وجود اتصال فيزيكي را بررسي نمايد .

مثلا وقتي PC براي پروتكل DHCPپيكر بندي شده اما آدرس پيش فرض ويندوز (X.X.۱۶۹,۲۵۴) را بر مي گرداند ، مشخص مي شود كه كلانيت نمي تواند با سرورDHCP ارتباط برقرار كند .

يا وقتي يك كامپيوتر پر تابل را به شبكه متصل مي كنيم ، بايستي آدرس همان شبكه راداشته باشد . اما آگاهي اوقات DHCP ارتباط برقرار كند .

يا وقتي يك كامپيوتر پرتابل را به شبكه متصل مي كنيم ، بايستي آدرس همان شبكه را داشته باشد . اما گاهي گاهي اوقات DHCP، آدرس subnet ديگري را به آن اختصاص مي دهد . اكنون كاربر مي تواند دودستور ipconfig/release<\:C و ipconfig/renew<\:C را وارد مي نمايد. يعني مي خواهد كه آدرس IP جديدي داشته باشد . اگر سيستم پاسخ دهد كه انجام عمل DHCP ميسر نيست . آن گاه اين احتمال وجو دارد كه كاربر از پيكر بندي IP االستاتيك استفاده كرده باشد . در اين حالت جهت بررسي صحت گزارش ، بايد به مستندات شبكه مراجعه نمود .

در حالتي ديگر ، اگركاربر يك آدرس IP را اعلام كند ، بايد از طريق ping كردن ، آن بررسي نمود . اگر PC كاربر ، پاسخ مناسب مي دهد ، يعني آ ن كه انجام فعاليت هاي متداول نظير باز كردن صفحه وب انجام پذير است . در غيراين صورت بايستي كامپيوتر را از نزديك مورد بررسي قرارداد.

بررسي مشكل به صورت حضوري

پس از حضور در محل كاربر ، كار جمع آوري اطلاعات شروع مي شود . سؤال اول اين است كه انجام كدام عمل باعث بروز مشكل شد ه است . گاهي اوقات پاسخ اين سؤال، چندان روشنگرنيست . زيرا كاربرمي گويد كه وي كارخاصي انجام نداده است و همه كارها صورت گرفته در حد كارهاي معمولي روزانه بوده است يا آن كه دقيقا مي داند چه اتفاقي افتاده ولي ترجيح مي دهد درباره آن توضيحي ندهد ، يا مسئوولیت انجام آن را بر عهده نگيرد .

در اين مواقع بايد كاربر را مطمئن سازيد كه توضيح درباره نحوه بروز مشكل به رفع سريع آن كمك خواهد كرد . به غير از اين ها از انجام تغييرات محلي نيز سؤال كنيد . مثلا اين كه به تازگي دكوراسيون اتاق محل كار تغيير كرده است ي يك برنامه محافظ نمايش جديد نصب شده است يا مواردي از اين دست .

بعد از آن كه تا حد ممكن دانسته هايتان را افزايش داديد ، موارد ي كه تلفني به كاربر گفتيد را مجددا خودتان آزمايش كنيد . اگر عمل ping به سرور شبكه به درستي انجام مي شود يا ادوات شبكه به درستي پاسخ مي دهند ، نشان دهنده آن است كه ايستگاه كاري در لايه ۳، به درستي به شبكه متصل است و در نتيجه به انجام تست در لايه هاي پايين تر نيازي نيست . پس بايد توجه را به لايه هاي بالايي شبكه معطوف نمود . اگر اين قسمت درست جواب ندهد يعني اين كه بايد به سراغ لايه هاي پايين تر رفت . حالا بايد از يك لايه شروع كنيد . اگراتصال شبكه قطع باشد ، دستورping اين موضوع را به خوبي نشان مي دهد . براي ديدن زمان پاسخ (response Time) ، دستور زيزر استفاده مي شود : C:\ping-t x x x x

نتيجه حاصله را مي توان با استفاده ازTERACERT و PATHPING براي بررسي مسير ها به سمت device مورد نظر تحليل نموده است .

route Trace نمودن به شما مي گويد كه چگونه در طول مسير شبكه ، پكت ممكن است از بين برود . يعني رفع عيب

لايه يك شبكه را مي توان از همين راه آغاز كرد . دستور tracert x.x.x.x<\:C يا patping<\:C اين كار را انجام مي دهند.

آيا به سطح پيشرفته تري از اشكال يابي احتياج است ؟

اگر هنوز ايراد مشخص نشده است يا براي تعيين آن به اطلاعات يا به جزييات بيشتري نياز است ،بايد چند آزمايش ديگر را نيز انجام داد .

پس از اطمينان از اين كه ، وارد نشدن كاربربه شبكه دراثرجابه جايي كابل يت جدا شدن كابل و اتصالات آن نمي باشد ، به اين نتيجه مي رسيد كه مشكل پيش آمده ، پيچيده تر از اشكلات معمولي شبكه هااست.

در اين جا داشتن ابزاري مانند LinkRunner مي تواند به سرعت به كشف اشكالات كمك كند .

آزمون هاي مستقيم

۱. تست لينك

۲. بررسي فعاليت Segmentها

۳. استفاده از DHCP به عنوان ابزار تشخيص

۴. انجام ping به صورت محلي و راه دور

تست لينك

بعضي از تكنسين هاي شبكه معتقد ند كه روشن بودن چراغ (LED) روي كارت شبكه نشان دهنده برقرار بودن لينك است . اما اين مساله در مورد تجهيزات مختلف ، معاني متفاوتي دارد . در بعضي تجهيزات ، چراغ هاي لينك (Link LED) توسط نرم افزارهاي مستقر در سيستم ميزبان كنترل مي شوند و وقتي روشن مي شوند كه لايه هاي بالايي شبكه مشغول فعاليت باشند . بعضي كارت هاي شبكه چراغ لينك را وقتي روشن مي كنند كه ترافيكي روي شبكه در جريان باشد . در نتيجه روشن بودن LED ، دليل محكمي بر سالم بودن يا سالم نبودن لينك ارتباطي نيست . حتي بعضي از تجهيزات از LEDها براي نشان دادن يك طرفه يا دو طرفه بودن ارتباط (haft or full Dplex) يا نشان دادن سرعت ارتباط (۱۰/۰۰) استفاده مي كنند .

برقراري لينك از طريق انجام روندي به نام Negotiation-Auto انجام مي شود كه در طي آن ، طرف لينك اطلاعاتي را با يكديگر تبادل مي كنند . اين اطلاعات شامل سرعت ارتباط يا يك طرفه / دو طرفه بودن آن مي شود . در حين اين تبادل ، دو طرف ارتباط قابليت هاي يكديگر را مقايسه مي كنند و سعي مي كنند ارتباط رابابالاترين سرعت ممكن برقرار نمايند . اگر يكي از طرفين ارتباط نتوانند به درستي خود را پيكر بندي كنند يا درايو هاي مورد نياز نداشته باشند . اينارتباط نمي تواند ادامه پيدا كند . آن گاه يا روند فوق مجددا تكرار مي گردد و يا ارتباط به كلي قطع مي گردد.

وقتي ارتباط در يك شبكه قطع شده است . Link Runner سعي مي كند ابتدا ارتباط خودش را با هر يك از طرفين لينك برقرار سازد . مثلا خودش را به كارت شبكه يا سوئيچ (دو طرف يك ارتباط) متصل مي كند . سپس روند Auto_Negotiation را بااستفاده از استاندارد IEEE 802.3 آغاز مي كند . اين ارتباط در سطح سخت افزار خواهد بود و توسط نرم افزار كنترل نخواهد شد . پس از انجام اين كار ، چراغ سبز رنگ LinkRunner روشن مي شود و سرعت و نوع ارتباط (يك طرفه / دو طرفه) روي صفحه نمايش دستگاه نشان داده مي شود.

آموزش راه‌اندازي شبكه خصوصي مجازي (VPN)

شبكه خصوصي مجازي يا VPN (Virtual Private Network) در اذهان تصور يك مطلب پيچيده براي استفاده و پياده كنندگان آن به وجود آورده است . اما اين پيچيدگي ، در مطالب بنيادين و مفهومي آن است نه در پياده‌سازي .

اين نكته را بايد بدانيد كه پياده‌سازي VPN داراي روش خاصي نبوده و هر سخت‌افزار و نرم‌افزاري روش پياده‌سازي خود را داراست و نمي‌توان روش استانداردي را براي كليه موارد بيان نمود . اما اصول كار همگي به يك روش است .

مختصري درباره تئوري VPN

مفهوم اصلي VPN چيزي جز برقراري يك كانال ارتباطي خصوصي براي دسترسي كاربران راه دور به منابع شبكه

نيست . در اين كانال كه بين دو نقطه برقرار مي‌شود ، ممكن است كه مسيرهاي مختلفي عبور كند اما كسي قادر به وارد شدن به اين شبكه خصوصي شما نخواهد بود . گرچه مي‌توان از VPN در هر جايي استفاده نمود اما استفاده آن در خطوط Dialup و Leased كار غير ضروري است (در ادامه به‌دليل آن پي خواهيد برد).

در يك ارتباط VPN شبكه يا شبكه‌ها مي‌توانند به هم متصل شوند و از اين طريق كاربران از راه دور به شبكه به راحتي دسترسي پيدا مي‌كنند. اگر اين روش از ارائه دسترسي كاربران از راه دور را با روش خطوط اختصاصي فيزيكي (Leased) مقايسه كنيم ، مي‌بينيد كه ارائه يك ارتباط خصوصي از روي اينترنت به مراتب از هر روش ديگري ارزان‌تر تمام مي‌شود .

از اصول ديگري كه در يك شبكه VPN در نظر گرفته شده بحث امنيت انتقال اطلاعات در اين كانال مجازي مي‌باشد . يك ارتباط VPN مي‌تواند بين يك ايستگاه كاري و يك شبكه محلي و يا بين دو شبكه محلي صورت گيرد. در بين هر دو نقطه يك تونل ارتباطي برقرار مي‌گردد و اطلاعات انتقال يافته در اين كانال به صورت كد شده حركت مي‌كنند ، بنابراين حتي در صورت دسترسي مزاحمان و هكرها به اين شبكه خصوصي نمي‌توانند به اطلاعات رد و بدل شده در آن دسترسي پيدا كنند.

جهت برقراري يك ارتباط VPN ، مي‌توان به كمك نرم‌افزار يا سخت‌افزار و يا تركيب هر دو ، آن را پياده‌سازي نمود . به طور مثال اكثر ديواره‌هاي آتش تجاري و روترها از VPN پشتيباني مي‌كنند . در زمينه نرم‌افزاري نيز از زمان ارائه ويندوز NT ويرايش ۴ به بعد كليه سيستم عامل‌ها داراي چنين قابليتي هستند .

در اين مقاله پياده‌سازي VPN بر مبناي ويندوز ۲۰۰۰ گفته خواهد شد .

پياده‌سازي VPN

براي پياده‌سازي VPN بر روي ويندوز ۲۰۰۰ كافيست كه از منوي Program/AdministrativeTools/ ، گزينه Routing and Remote Access را انتخاب كنيد . از اين پنجره گزينه VPN را انتخاب كنيد . پس از زدن دكمه Next وارد پنجره ديگري مي‌شويد كه در آن كارت‌هاي شبكه موجود بر روي سيستم ليست مي‌شوند .

براي راه‌اندازي يك سرور VPN مي‌بايست دو كارت شبكه نصب شده بر روي سيستم داشته باشيد .

از يك كارت شبكه براي ارتباط با اينترنت و از كارت ديگر جهت برقراري ارتباط با شبكه محلي استفاده مي‌شود. در اين‌جا بر روي هر كارت به‌طور ثابت IP قرار داده شده اما مي‌توان اين IPها را به صورت پويا بر روي كارت‌هاي شبكه قرار داد .

در پنجره بعد نحوه آدرس‌دهي به سيستم راه دوري كه قصد اتصال به سرور ما را دارد پرسيده مي‌شود . هر ايستگاه كاري مي تواند يك آدرس IP براي كار در شبكه محلي و يك IP براي اتصال VPN داشته باشد . در منوي بعد نحوه بازرسي كاربران پرسيده مي‌شود كه اين بازرسي مي تواند از روي كاربران تعريف شده در روي خود ويندوز باشد و يا آنكه از طريق يك سرويس دهنده RADIUS صورت گيرد در صورت داشتن چندين سرور VPN استفاده از RADIUS را به شما پيشنهاد مي‌كنيم . با اين روش كاربران ، بين تمام سرورهاي VPN به اشتراك گذاشته شده و نيازي به تعريف كاربران در تمامي سرورها نمي‌باشد.

پروتكل‌هاي استفاده شونده

عملياتي كه در بالا انجام گرفت تنها پيكربندي‌هاي لازم جهت راه‌اندازي يك سرور VPN مي‌باشد .

اما RRAS Remote Routing (Access Service) داراي دو پروتكل جهت برقراري تونل ارتباطي VPN مي‌باشد. ساده‌ترين پروتكل آن PPTP (Point to Point Tunneling Protocol) است ، اين پروتكل برگرفته از PPP است كه در سرويس‌هاي Dialup مورد استفاده واقع مي‌شود ، در واقع PPTP همانند PPP عمل مي‌كند .

پروتكل PPTP در بسياري از موارد كافي و مناسب است ، به كمك اين پروتكل كاربران مي‌توانند به روش‌هاي PAP (Password Authentication Protocol) و Chap (Challenge Handshake Authentication Protocol) بازرسي شوند.

جهت كد كردن اطلاعات مي‌توان از روش كد سازي RSA استفاده نمود.

PPTP براي كاربردهاي خانگي و دفاتر و افرادي كه در امر شبكه حرفه‌اي نيستند مناسب است اما در جايگاه امنيتي داراي پايداري زيادي نيست . پروتكل ديگري به نام L2TP (Layer2 Forwarding) به وسيله شركت CISCO ارائه شده كه به لحاظ امنيتي بسيار قدرتمندتر است.

اين پروتكل با استفاده از پروتكل انتقال اطلاعات UDP (User Datagram Protocol) به‌جاي استفاده از TCP به مزاياي زيادي دست يافته است . اين روش باعث بهينه و ملموس‌تر شدن براي ديواره‌هاي آتش شده است ، اما باز هم اين پروتكل در واقع چيزي جز يك كانال ارتباطي نيست . جهت حل اين مشكل و هر چه بالاتر رفتن ضريب امنيتي در VPN شركت مايكروسافت پروتكل ديگري را به نام IPSec (IP Security) مطرح نموده كه پيكربندي VPN با آن كمي دچار پيچيدگي مي‌گردد.

اما در صورتي كه پروتكل PPTP را انتخاب كرده‌ايد و با اين پروتكل راحت‌تر هستيد تنها كاري كه بايد در روي سرور انجام دهيد فعال كردن قابليت دسترسي Dial in مي‌باشد. اين كار را مي‌توانيد با كليك بر روي Remote Access Polices در RRAS انجام دهيد و با تغيير سياست كاري آن ، آن را راه‌اندازي كنيد (به طور كلي پيش‌فرض سياست كاري ، رد كليه درخواست‌ها مي‌باشد).

دسترسي ايستگاه كاري از طريق VPN

حالا كه سرور VPN آماده سرويس‌دهي شده ، براي استفاده از آن بايد بر روي ايستگاه كاري نيز پيكربنديهايي را انجام دهيم . سيستم عاملي كه ما در اين‌جا استفاده مي‌كنيم ويندوز XP مي‌باشد و روش پياده‌سازي VPN را بر روي آن خواهيم گفت اما انجام اين كار بر روي ويندوز ۲۰۰۰ نيز به همين شكل صورت مي‌گيرد . بر روي ويندوزهاي ۹۸ نيز مي‌توان ارتباط VPN را برقرار نمود ، اما روش كار كمي متفاوت است و براي انجام آن بهتر است به آدرس زير مراجعه كنيد :

www.support.microsot.com

بر روي ويندوزهاي XP ، يك نرم‌افزار جهت اتصال به VPN براي هر دو پروتكل PPTP و L2TP وجود دارد. در صورت انتخاب هر كدام ، نحوه پيكربندي با پروتكل ديگر تفاوتي ندارد . راه‌اندازي VPN كار بسيار ساده‌اي است ، كافيست كه بر روي Network Connection كليك نموده و از آن اتصال به شبكه خصوصي از طريق اينترنت (Private Network Through Internet) را انتخاب كنيد .

در انجام مرحله بالا از شما يك اسم پرسيده مي‌شود . در همين مرحله خواسته مي‌شود كه براي اتصال به اينترنت يك ارتباط تلفني (Dialup) تعريف نماييد ، پس از انجام اين مرحله نام و يا آدرس سرور VPN پرسيده مي‌شود .

مراحل بالا تنها مراحلي است كه نياز براي پيكربندي يك ارتباط VPN بر روي ايستگاه‌هاي كاري مي‌باشد . كليه عمليات لازمه براي VPN به صورت خودكار انجام مي‌گيرد و نيازي به انجام هيچ عملي نيست . براي برقراري ارتباط كافيست كه بر روي آيكوني كه بر روي ميز كاري ايجاد شده دو بار كليك كنيد پس از وارد كردن كد كاربري و كلمه عبور چندين پيام را مشاهده خواهيد كرد كه نشان‌دهنده روند انجام برقراري ارتباط VPN است .

اگر همه چيز به خوبي پيش رفته باشد مي‌توانيد به منابع موجود بر روي سرور VPN دسترسي پيدا كنيد اين دسترسي مانند آن است كه بر روي خود سرور قرار گرفته باشيد .

ارتباط سايت به سايت (Site-to-Site VPN)

در صورتي كه بخواهيد دو شبكه را از طريق يك سرور VPN دومي به يكديگر وصل كنيد علاوه بر مراحل بالا بايد چند كار اضافه‌تر ديگري را نيز انجام دهيد .

جزئيات كار به پروتكلي كه مورد استفاده قرار مي‌گيرد . جهت اين كار بايد سرور را در پنجره RRAS انتخاب كرده و منوي خاص (Properties) آن را بياوريد .

در قسمت General مطمئن شويد كه گزينه‌هاي LAN و Demand Dial انتخاب شده باشند (به طور پيش گزيده انتخاب شده هستند). همچنين اطمينان حاصل كنيد كه پروتكل را كه قصد روت (Route) كردن آن را داريد فعال است .

پس از مراحل بالا نياز به ايجاد يك Dial Demand داريد ، اين كار را مي‌توانيد با يك كليك راست بر روي واسط روت (Interface Routing) انجام دهيد .

در پنجره بعدي كه ظاهر مي‌شود بايد براي اين ارتباط VPN خود يك نام تعيين كنيد اين نام بايد همان اسمي باشد كه در طرف ديگر كاربران با آن به اينترنت متصل مي‌شوند در صورتي كه اين مطلب را رعايت نكنيد ارتباط VPN شما برقرار نخواهد شد .

پس از اين مرحله بايد آدرس IP و يا نام دامنه آن را مشخص كنيد و پس از آن نوع پروتكل ارتباطي را تعيين نمود .
اما مرحله نهايي تعريف يك مسير (Route) بر روي سرور ديگر مي‌باشد بدين منظور بر روي آن سرور در قسمت RRAS ، Demand Dial را انتخاب كنيد و آدرس IP و ساب‌نت را در آن وارد كنيد و مطمئن شويد كه قسمت
Use This to Initate Demand
انتخاب شده باشد . پس از انجام مرحله بالا كار راه‌اندازي اين نوع VPN به پايان مي‌رسد .

پايان

همان‌طور كه ديديد راه‌اندازي يك سرور VPN بر روي ويندوز ۲۰۰۰ تحت پروتكل PPTP كار ساده‌اي بود اما اگر بخواهيد از پروتكل L2TP/IPSec استفاده كنيد كمي كار پيچيده خواهد شد . به خاطر بسپاريد كه راه‌اندازي VPN بار زيادي را بر روي پردازنده سرور مي‌گذارد و هرچه تعداد ارتباطات VPNبيشتر باشد بار زيادتري بر روي سرور است كه مي‌توانيد از يك وسيله سخت‌افزاري مانند روتر جهت پياده‌سازي VPN كمك بگيرد .

آشنايي با هاب و نحوه عملكرد آن

هاب از جمله تجهیزات سخت افزاری است که از آن به منظور برپاسازی شبکه های کامپیوتری استفاده می شود . گرچه در اکثر شبکه هائی که امروزه ایجاد می گردد از سوئیچ در مقابل هاب استفاده می گردد، ولی ما همچنان شاهد استفاده از این نوع تجهیزات سخت افزاری در شبکه های متعددی می باشیم . در این مطلب قصد داریم به بررسی هاب و نحوه عملکرد آن اشاره نمائیم . قبل از پرداختن به اصل موضوع لازم است در ابتدا با برخی تعاریف مهم که در ادامه بدفعات به آنان مراجعه خواهیم کرد ، بیشتر آشنا شویم .

Domain : تمامی کامپیوترهای عضوء یک domain هر اتفاق و یا رویدادی را که در domain اتفاق می افتد ، مشاهده و یا خواهند شنید .

Collision Domain : در صورت بروز یک تصادم (Collision) بین دو کامپیوتر، سایر کامپیوترهای موجود در domain آن را شنیده و آگاهی لازم در خصوص آن چیزی که اتفاق افتاده است را پیدا خواهند کرد . کامپیوترهای فوق عضوء یک Collision Domain یکسان می باشند. تمامی کامپیوترهائی که با استفاده از هاب به یکدیگر متصل می شوند ، عضوء یک Domain Collision یکسان خواهند بود (بر خلاف سوئیچ) .

Broadcast Domain : در این نوع domain ، یک پیام broadcast (یک فریم و یا داده که برای تمامی کامپیوترها ارسال می گردد) برای هر یک از کامپیوترهای موجود در doamin ارسال می گردد . هاب و سوئیچ با موضوع broadcast domain برخورد مناسبی نداشته (ایجاد حوزه های مجزاء) و در این رابطه به یک روتر نیاز خواهد بود .

به منظور برخورد مناسب (ایجاد حوزه های مجزاء) با collision domain، broadcast domain و افزایش سرعت و کارائی یک شبکه از تجهیزات سخت افزاری متعددی استفاده می شود . سوئیچ ها collision domain مجزائی را ایجاد می نمایند ولی در خصوص broadcast doamin بدین شکل رفتار نمی نمایند . روترها ، broadcast domain و collision domain مجزائی را ایجاد نموده و در مقابل هاب ، قادر به ایجاد broadcast doamin و Collision domain جداگانه نمی باشد . شکل زیر یک نمونه هاب هشت پورت را نشان می دهد (D-Link DE-808TP 10Mbps Ethernet Port Mini--۸ Hub) .

آشنائی با نحوه عملکرد هاب

هاب ، یکی از تجهیزات متداول در شبکه های کامپیوتری و ارزانترین روش اتصال دو و یا چندین کامپیوتر به یکدیگر است . هاب در اولین لایه مدل مرجع OSI فعالیت می نماید . آنان فریم های داده را نمی خوانند (کاری که سوئیچ و یا روتر انجام می دهند) و صرفا" این اطمینان را ایجاد می نمایند که فریم های داده بر روی هر یک از پورت ها ، تکرار خواهد شد.

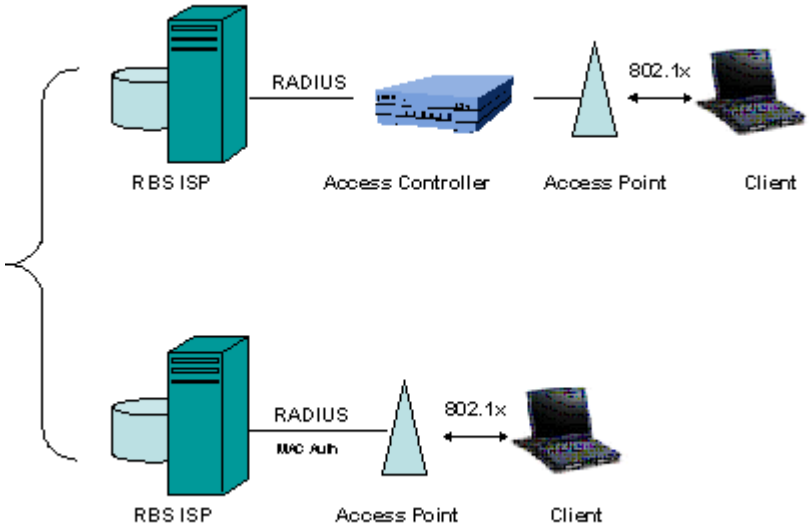
گره هائی که یک اترنت و یا Fast Ethernet را با استفاده از قوانین CSMA/CD به اشتراک می گذارند ، عضوء یک

Collision Domain مشابه می باشند . این بدان معنی است که تمامی گره های متصل شده به هاب بخشی از Collision domain مشابه بوده و زمانی که یک collision اتفاق می افتد ، سایر گره های موجود در domain نیز آن را شنیده و از آن متاثر خواهند شد .
کامپیوترها و یا گره های متصل شده به هاب از کابل های (UTP (Unshielded Twisted Pair ، استفاده می نمایند. صرفا" یک گره می تواند به هر پورت هاب متصل گردد. مثلا" با استفاده از یک هاب هشت پورت ، امکان اتصال هشت کامپیوتر وجود خواهد داشت .زمانی که هاب ها به متداولی امروز نبودند و قیمت آنان نیز گران بود ، در اکثر شبکه های نصب شده در ادارات و یا منازل از کابل های کواکسیال، استفاده می گردید.
نحوه کار هاب بسیار ساده است . زمانی که یکی از کامپیوترهای متصل شده به هاب اقدام به ارسال داده ئی می نماید ، سایر پورت های هاب نیز آن را دریافت خواهند کرد (داده ارسالی تکرار و برای سایر پورت های هاب نیز فرستاده می شود) .
همانگونه که در شکل فوق مشاهده می نمائید ، گره یک داده ئی را برای گره شش ارسال می نماید ولی تمامی گره های دیگر نیز داده را دریافت خواهند کرد . در ادامه ، بررسی لازم در خصوص داده ارسالی توسط هر یک از گره ها انجام و در صورتی که تشخیص داده شود که داده ارسالی متعلق به آنان نیست ، آن را نادیده خواهند گرفت . عملیات فوق از طریق کارت شبکه موجود بر روی کامپیوتر که آدرس MAC مقصد فریم ارسالی را بررسی می نماید ، انجام می شود .کارت شبکه بررسی لازم را انجام و در صورت عدم مطابقت آدرس MAC موجود در فریم ، با آدرس MAC کارت شبکه ، فریم ارسالی دور انداخته می گردد .
اکثر هاب ها دارای یک پورت خاص می باشند که می تواند به صورت یک پورت معمولی و یا یک پورت uplink رفتار نماید . با استفاده از یک پورت uplink می توان یک هاب دیگر را به هاب موجود، متصل نمود. بدین ترتیب تعداد پورت ها افزایش یافته و امکان اتصال تعداد بیشتری کامپیوتر به شبکه فراهم می گردد .روش فوق گزینه ای ارزان قیمت به منظور افزایش تعداد گره ها در یک شبکه است ولی با انجام این کار شبکه شلوغ تر شده و همواره بر روی آن حجم بالائی داده غیر ضروری در حال جابجائی است. تمامی گره ها ، عضوء یک Broadcast domain و collision domain یکسانی می باشند ، بنابراین تمامی آنان هر نوع collision و یا Broadcast را که اتفاق خواهد افتاد ، می شنوند .
در اکثر هاب ها از یک LED به منظور نشان دادن فعال بودن ارتباط برقرار شده بین هاب و گره و از LED دیگر به منظور نشان دادن بروز یک collision ، استفاده می گردد . (دو LED مجزاء) . در برخی از هاب ها دو LED مربوط به فعال بودن لینک ارتباطی بین هاب و گره و فعالیت پورت با یکدیگر ترکیب و زمانی که پورت در حال فعالیت است ، LED مربوطه چشمک زن شده و زمانی که فعالیتی انجام نمی شود، LED فوق به صورت پیوسته روشن خواهد بود .
LED مربوط به Collision موجود بر روی هاب ها زمانی روشن می گردد که یک collision بوجود آید . Collision زمانی بوجود می آید که دو کامپیوتر و یا گره سعی نمایند در یک لحظه بر روی شبکه صحبت نمایند . پس از بروز یک Collision ، فریم های مربوط به هر یک از گره ها با یکدیگر برخورد نموده و خراب می گردند . هاب به منظور تشخیص این نوع تصادم ها به اندازه کافی هوشمند بوده و برای مدت زمان کوتاهی چراغ مربوط به collision روشن می گردد . (یک دهم ثانیه به ازای هر تصادم) .
تعداد اندکی از هاب ها دارای یک اتصال خاص از نوع BNC بوده که می توان از آن به منظور اتصال یک کابل کواکسیال ، استفاده نمود . پس از اتصال فوق ، LED مربوط به اتصال BNC روی هاب روشن می گردد.

هفت مشکل امنیتی مهم شبکه های بی سیم 802.11 :بخش اول

موفقیت حیرت انگیز 802.11 به علت توسعه «اترنت بی سیم» است. همچنانکه 802.11 به ترقی خود ادامه می دهد، تفاوت هایش با اترنت بیشتر مشخص می شود. بیشتر این تفاوت ها به دلیل نا آشنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مدیران شبکه باید درک پایه ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آنها به خدمت گرفته می شوند. آنالایزرهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده اند که به آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می دهد.

در این سلسله مقاله هفت مشکل از مهم ترین آسیب پذیری های امنیتی موجود در LANهای بی سیم، راه حل آنها و در نهایت چگونگی ساخت یک شبکه بی سیم امن مورد بحث قرار می گیرد. بسیاری از پرسش ها در این زمینه در مورد ابزارهایی است که مدیران شبکه می توانند استفاده کنند. یک آنالایزر از اولین خریدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزرها علاوه بر عملکردهای سنتی تحلیل پروتکل و ابزار تشخیص عیب، می توانند برای تشخیص بسیاری از نگرانی های امنیتی که استفاده از شبکه بی سیم را کند می کنند، استفاده شوند. این سلسله مقاله هریک از این «هفت مسأله امنیتی» را بررسی می کند و توضیح می دهد که چگونه و چرا آنالایزر بی سیم، یک ابزار حیاتی برای تضمین امنیت شبکه های بی سیم است.



مسأله شماره ۱: دسترسی آسان

LANهای بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنها، شبکه ها باید فریم های Beacon با پارامتر های شبکه را ارسال کنند. البته، اطلاعات مورد نیاز برای پیوستن به یک شبکه، اطلاعاتی است که برای اقدام به یک حمله روی شبکه نیاز است. فریم های Beacon توسط هیچ فانکشن اختصاصی پردازش نمی شوند و این به این معنی است که شبکه 802.11 شما و پارامترهایش برای هر شخصی با یک کارت 802.11 قابل استفاده است. نفوذگران با آنتن های قوی می توانند شبکه ها را در مسیرها یا ساختمان های نزدیک بیابند و ممکن است اقدام به انجام حملاتی کنند حتی بدون اینکه به امکانات شما دسترسی فیزیکی داشته باشند.

راه حل شماره ۱: تقویت کنترل دسترسی قوی

دسترسی آسان الزاماً با آسیب پذیری مترادف نیست. شبکه های بی سیم برای ایجاد امکان اتصال مناسب طراحی

شده اند، اما می توانند با اتخاذ سیاستهای امنیتی مناسب تا حد زیادی مقاوم شوند. یک شبکه بی سیم می تواند تا حد زیادی در این اتاق محافظت شده از نظر الکترومغناطیس محدود شود که اجازه نشت سطوح بالایی از فرکانس رادیویی را نمی دهد. به هرحال، برای بیشتر موسسات چنین برد هایی لازم نیستند. تضمین اینکه شبکه های بی سیم تحت تأثیر کنترل دسترسی قوی هستند، می تواند از خطر سوءاستفاده از شبکه بی سیم بکاهد.

تضمین امنیت روی یک شبکه بی سیم تا حدی به عنوان بخشی از طراحی مطرح است. شبکه ها باید نقاط دسترسی را در بیرون ابزار پیرامونی امنیت مانند فایروال ها قرار دهند و مدیران شبکه باید به استفاده از VPNها برای میسر کردن دسترسی به شبکه توجه کنند. یک سیستم قوی تأیید هویت کاربر باید به کار گرفته شود و ترجیحاً با استفاده از محصولات جدید که برپایه استاندارد IEEE 802.1x هستند. 802.1x انواع فریم های جدید برای تأیید هویت کاربر را تعریف می کند و از دیتابیس های کاربری جامعی مانند RADIUS بهره می گیرد. آنالایزرهای باسیم سنتی می توانند با نگاه کردن به تقاضاهای RADIUS و پاسخ ها، امکان درک پروسه تأیید هویت را فراهم کنند. یک سیستم آنالیز خبره برای تأیید هویت 802.11 شامل یک روتین عیب یابی مشخص برای LANهاست که ترافیک تأیید هویت را نظاره می کند و امکان تشخیص عیب را برای مدیران شبکه فراهم می کند که به آنالیز بسیار دقیق و کدگشایی فریم احتیاج ندارد. سیستم های آنالیز خبره که پیام های تأیید هویت 802.1x را دنبال می کنند، ثابت کرده اند که برای استفاده در LANهای استفاده کننده از 802.1x فوق العاده باارزش هستند.

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چینش فعلی را با اهداف امنیتی طراحی تضمین کند. بعضی موتورهای آنالیز تحلیل عمیقی روی فریم ها انجام می دهند و می توانند چندین مسأله معمول امنیت 802.1x را تشخیص دهند. تعدادی از حملات روی شبکه های باسیم در سال های گذشته شناخته شده اند و لذا وصله های فعلی به خوبی تمام ضعف های شناخته شده را در این گونه شبکه ها نشان می دهند. آنالایزرهای خبره پیاده سازی های ضعیف را برای مدیران شبکه مشخص می کنند و به این ترتیب مدیران شبکه می توانند با به کارگیری سخت افزار و نرم افزار ارتقاء یافته، امنیت شبکه را حفظ کنند.

پیکربندی های نامناسب ممکن است منبع عمده آسیب پذیری امنیتی باشد، مخصوصاً اگر LANهای بی سیم بدون نظارت مهندسان امنیتی به کارگرفته شده باشند. موتورهای آنالیز خبره می توانند زمانی را که پیکربندی های پیش فرض کارخانه مورد استفاده قرار می گیرند، شناسایی کنند و به این ترتیب می توانند به ناظران کمک کنند که نقاطی از دسترسی را که بمنظور استفاده از ویژگی های امنیتی پیکربندی نشده اند، تعیین موقعیت کنند. این آنالایزرها همچنین می توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPNها یا 802.1x استفاده نمی کنند، علائم هشدار دهنده را ثبت کنند.

رویکردی عملی به امنیت شبکه لایه بندی شده (۱)

مقدمه

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است. {گروه امداد امنیت کامپیوتری ایران}

در این سلسله مقالات رویکردی لایه بندی شده برای امن سازی شبکه به شما معرفی می گردد. این رویکرد هم یک استراتژی تکنیکی است که ابزار و امکان مناسبی را در سطوح مختلف در زیرساختار شبکه شما قرار می دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیأت مدیره تا قسمت فروش را می طلبد.

رویکرد امنیتی لایه بندی شده روی نگهداری ابزارها و سیستمهای امنیتی و روال ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می گردد.

۱- پیرامون

۲- شبکه

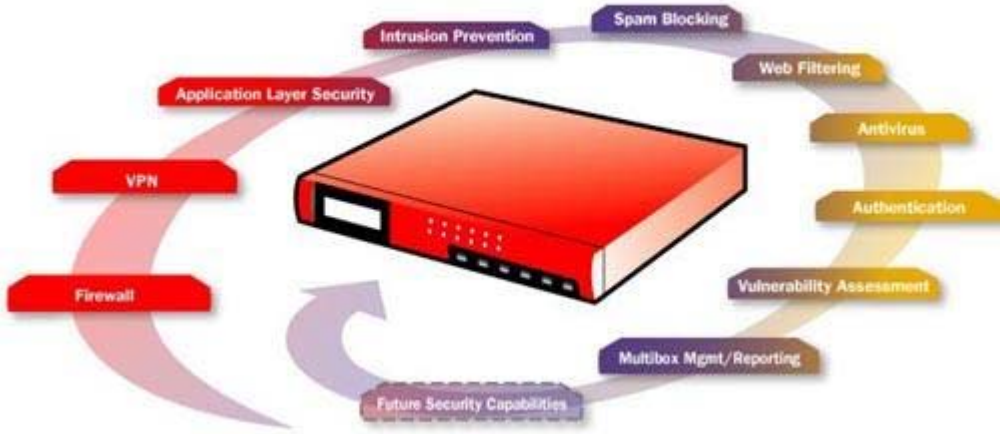
۳- میزبان

۴- برنامه کاربردی

۵- دیتا

در این سلسله مقالات هریک از این سطوح تعریف می شوند و یک دید کلی از ابزارها و سیستمهای امنیتی گوناگون که روی هریک عمل می کنند، ارائه می شود. هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک رویکرد عملی مناسب برای محافظت از دارایی های دیجیتال است. مخاطبان این سلسله مقالات متخصصان فناوری اطلاعات، مدیران تجاری و تصمیم گیران سطح بالا هستند.

محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسأله، خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد. بعلاوه، با رویکرد عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلال گران امنیتی ایجاد کنید.



افزودن به ضریب عملکرد هکرها

متخصصان امنیت شبکه از اصطلاحی با عنوان ضریب عملکرد (work factor) استفاده می کنند که مفهومی مهم در پیاده سازی امنیت لایه بندی است. ضریب عملکرد بعنوان میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تأثیر قراردادن یک یا بیشتر از سیستمها و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود. یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرار می گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود. اگر هکرها تشخیص دهند که شبکه شما ضریب عملکرد بالایی دارد، که فایده رویکرد لایه بندی شده نیز هست، احتمالاً شبکه شما را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزیست که شما می خواهید.

تکنولوژی های بحث شده در این سری مقالات مجموعاً رویکرد عملی خوبی برای امن سازی دارایی های دیجیتالی شما را به نمایش می گذارند. در یک دنیای ایده آل، شما بودجه و منابع را برای پیاده سازی تمام ابزار و سیستم هایی

که بحث می کنیم خواهید داشت. اما متأسفانه در چنین دنیایی زندگی نمی کنیم. بدین ترتیب، باید شبکه تان را ارزیابی کنید – چگونگی استفاده از آن، طبیعت داده های ذخیره شده، کسانی که نیاز به دسترسی دارند، نرخ رشد آن و غیره – و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می کنند، با توجه به منابع در دسترس پیاده سازی کنید.

مدل امنیت لایه بندی شده

در این جدول مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند. این تکنولوژی ها با جزئیات بیشتر در بخش های بعدی مورد بحث قرار خواهند گرفت.

ردیف	سطح امنیتی	ابزار و سیستم های امنیتی قابل استفاده
۱	پیرامون	فایروال آنتی ویروس در سطح شبکه رمزنگاری شبکه خصوصی مجازی
۲	شبکه	سیستم تشخیص/جلوگیری از نفوذ (IDS/IPS) سیستم مدیریت آسیب پذیری تبعیت امنیتی کاربر انتهایی کنترل دسترسی/ تایید هویت کاربر
۳	میزبان	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان تبعیت امنیتی کاربر انتهایی آنتی ویروس کنترل دسترسی/ تایید هویت کاربر
۴	برنامه کاربردی	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان کنترل دسترسی/ تایید هویت کاربر تعیین صحت ورودی
۵	داده	رمزنگاری کنترل دسترسی/ تایید هویت کاربر

رویکردی عملی به امنیت شبکه لایه بندی شده (۲)

در شماره قبل به لایه های این نوع رویکرد به اختصار اشاره شد. طی این شماره و شماره های بعد به هریک از این لایه ها می پردازیم.

سطح ۱: امنیت پیرامون

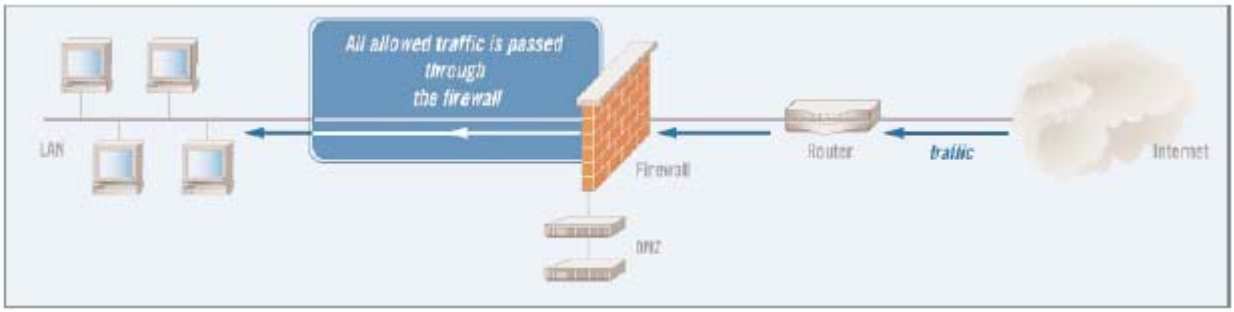
منظور از پیرامون، اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیرقابل اعتماد است. «پیرامون» اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است. این ناحیه ای است که شبکه به پایان می رسد و

اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند که بعنوان DMZ (zone demilitarized) شناخته می شود. DMZ معمولاً وب سرورها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای DNS را دربرمی گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سفت و سختی در مورد اینکه چه چیزی می تواند وارد شبکه شود و چگونه سرورها در DMZ می توانند با اینترنت و شبکه داخلی تعامل داشته باشند، دارد.

پیرامون شبکه، به اختصار، دروازه شما به دنیای بیرون و برعکس، مدخل دنیای بیرون به شبکه شماست.

تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند:

- **فایروال ـ** معمولاً یک فایروال روی سروری نصب می گردد که به بیرون و درون پیرامون شبکه متصل است. فایروال سه عمل اصلی انجام می دهد ۱- کنترل ترافیک ۲- تبدیل آدرس و ۳- نقطه پایانی VPN. فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک واردشونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال ها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کنند. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می کند. یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN (که بعداً بیشتر توضیح داده خواهد شد) عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند.
- **آنتی ویروس شبکه ـ** این نرم افزار در DMZ نصب می شود و محتوای ایمیل های واردشونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود.
- **VPN ـ** یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند. VPN اساساً یک تونل رمزشده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیریاب برپایه VPN، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمام بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود.



مزایا

تکنولوژی های ایجاد شده سطح پیرامون سال هاست که در دسترس هستند، و بیشتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه اقتصادی هستند. بعضیاز فروشندگان راه حل های سفت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند.

معایب

از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدت هاست که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمزشده قرار نداشته باشد. اگرچه VPN رمزنگاری مؤثری ارائه می کند، اما کار اجرایی بیشتری را برروی کارمندان IT تحمیل می کنند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند.

ملاحظات

پیچیدگی معماری شبکه شما می تواند تأثیر قابل ملاحظه ای روی میزان اثر این تکنولوژی ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هرکدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند.

انواع ابزاری که در DMZ شما قرار دارد نیز یک فاکتور مهم است. این ابزارها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

رویکردی عملی به امنیت شبکه لایه بندی شده (۳)

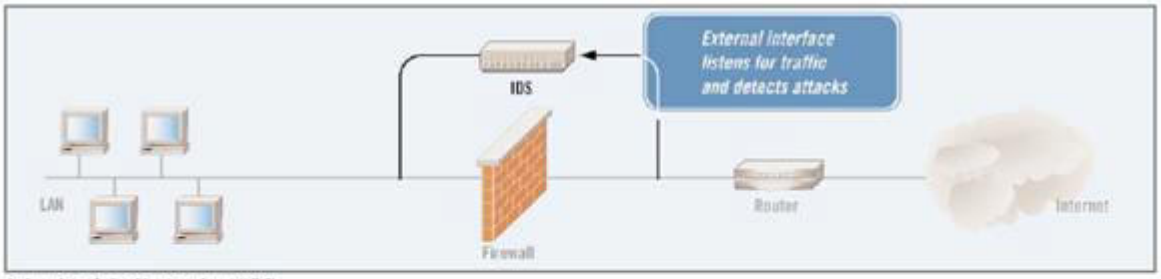
در مطلب قبلی به اولین لایه که لایه پیرامون است، اشاره شد، در این شماره به لایه امنیت شبکه می پردازیم.

سطح ۲- امنیت شبکه

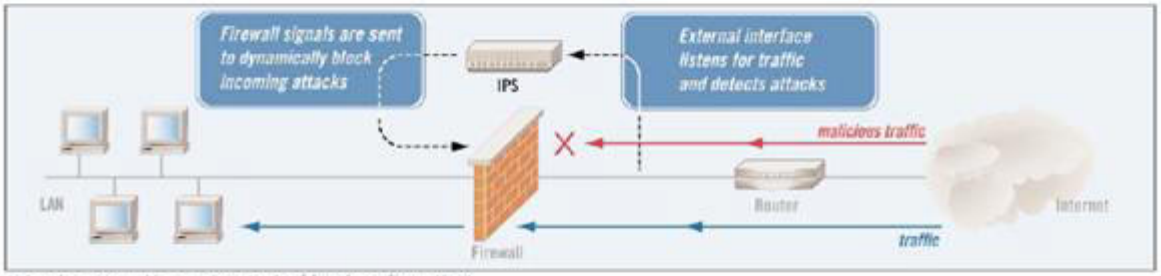
سطح شبکه در مدل امنیت لایه بندی شده به WAN و LAN داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی

در میان شبکه حرکت کنید. این قضیه بخصوص برای سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل می شوند. تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند:

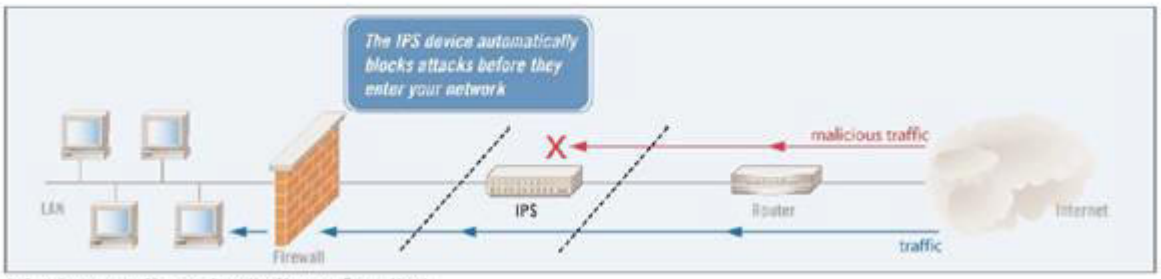
- **IDSها (سیستم های تشخیص نفوذ) و IPSها (سیستم های جلوگیری از نفوذ)** ـ تکنولوژیهای IDS و IPS ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند. ابزارهای IDS مسؤولین IT را از وقوع یک حمله مطلع می سازند؛ ابزارهای IPS یک گام جلوتر می روند و بصورت خودکار ترافیک آسیب رسان را مسدود می کنند. IDSها و IPSها مشخصات مشترک زیادی دارند. در حقیقت، بیشتر IPSها در هسته خود یک IDS دارند. تفاوت کلیدی بین این تکنولوژی ها از نام آنها استنباط می شود. محصولات IDS تنها ترافیک آسیب رسان را تشخیص می دهند، در حالیکه محصولات IPS از ورود چنین ترافیکی به شبکه شما جلوگیری می کنند. پیکربندی های IDS و IPS استاندارد در شکل نشان داده شده اند:



Intrusion detection system (IDS)



Intrusion prevention system (out-of-band configuration)



Intrusion prevention system (in-line configuration)

بری – سیستم های مدیریت آسیب پذیری دو عملکرد مرتبط را انجام می دهند: (۱) شبکه را برای آسیب پذیری ها پیمایش می کنند و (۲)روند مرمت آسیب پذیری یافته شده را مدیریت می کنند. در گذشته، این تکنولوژی VA (تخمین آسیب پذیری) نامیده می شد. اما این تکنولوژی اصلاح شده است، تا جاییکه بیشتر سیستم های موجود، عملی بیش از تخمین آسیب پذیری ابزار شبکه را انجام می دهند.

سیستم های مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه ها و آسیب پذیری هایی که می توانند توسط هکرها و ترافیک آسیب رسان مورد بهره برداری قرار گیرند، پیمایش می کنند. آنها معمولاً پایگاه

داده ای از قوانینی را نگهداری می کنند که آسیب پذیری های شناخته شده برای گستره ای از ابزارها و برنامه های شبکه را مشخص می کنند. در طول یک پیمایش، سیستم هر ابزار یا برنامه ای را با بکارگیری قوانین مناسب می آزماید.
همچنانکه از نامش برمی آید، سیستم مدیریت آسیب پذیری شامل ویژگیهایی است که روند بازسازی را مدیریت می کند. لازم به ذکر است که میزان و توانایی این ویژگی ها در میان محصولات مختلف، فرق می کند.

- **تابعیت امنیتی کاربر انتهایی** – روش های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می کنند که تضمین می کنند کاربران انتهایی استانداردهای امنیتی تعریف شده را قبل از اینکه اجازه دسترسی به شبکه داشته باشند، رعایت کرده اند. این عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستم های ناامن کارمندان و ابزارهای VPN و RAS می گیرد.
روش های امنیت نقاط انتهایی براساس آزمایش هایی که روی سیستم هایی که قصد اتصال دارند، انجام می دهند، اجازه دسترسی می دهند. هدف آنها از این تست ها معمولاً برای بررسی (۱) نرم افزار مورد نیاز، مانند سرویس پک ها، آنتی ویروس های به روز شده و غیره و (۲) کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی است.

- **کنترل دسترسی\تأیید هویت** – کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما دسترسی دارند. هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند.

نکته: در این سلسله مباحث، به کنترل دسترسی و تأییدهویت در سطوح شبکه، میزبان، نرم افزار و دیتا در چارچوب امنیتی لایه بندی شده می پردازیم. میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در مقابل دید کاربر اتفاق می افتد. اما به خاطر داشته باشید که کنترل دسترسی و تأیید هویت مراحل پیچیده ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به دقت مدیریت شوند.

مزایا

تکنولوژی های IDS، IPS و مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدیدها و آسیب پذیری های شبکه انجام می دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می دهد، ابزار IPS و IDS تجزیه و تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آنها خاتمه داده خواهند شد.

سیستم های مدیریت آسیب پذیری روند بررسی آسیب پذیری های شبکه شما را بصورت خودکار استخراج می کنند. انجام چنین بررسی هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدود زیادی غیرعملی خواهد بود. بعلاوه، شبکه ساختار پویایی دارد. ابزار جدید، ارتقاءدادن نرم افزارها و وصله ها، و افزودن و کاستن از کاربران، همگی می توانند آسیب پذیری های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیری های جدید پیمایش کنید.

روش های تابعیت امنیتی کاربر انتهایی به سازمان ها سطح بالایی از کنترل بر روی ابزاری را می دهد که به صورت سنتی کنترل کمی بر روی آنها وجود داشته است. هکرها بصورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، همچانکه پدیده های اخیر چون Mydoom، Sobig، و Sasser گواهی بر این مدعا هستند. برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند.

معایب

IDSها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند، که به عنوان false positives نیز شناخته می شوند. در حالیکه IDS ممکن است که یک حمله را کشف و به اطلاع شما برساند، این اطلاعات می تواند زیر انبوهی از هشدارهای غلط یا دیتای کم ارزش مدفون شود. مدیران IDS ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیرگذاری بالا، یک IDS باید بصورت پیوسته بررسی شود و برای الگوهای مورد استفاده و آسیب پذیری های کشف شده در محیط شما تنظیم گردد. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می کند.

سطح خودکار بودن در IPSها می تواند به میزان زیادی در میان محصولات، متفاوت باشد. بسیاری از آنها باید با دقت پیکربندی و مدیریت شوند تا مشخصات الگوهای ترافیک شبکه ای را که در آن نصب شده اند منعکس کنند. تأثیرات جانبی احتمالی در سیستمهایی که بهینه نشده اند، مسدود کردن تقاضای کاربران قانونی و قفل کردن منابع شبکه معتبر را شامل می شود.

بسیاری، اما نه همه روش های امنیتی کاربران انتهایی، نیاز به نصب یک عامل در هر نقطه انتهایی دارد. این عمل می تواند مقدار قابل توجهی بار کاری اجرایی به نصب و نگهداری اضافه کند.

تکنولوژی های کنترل دسترسی ممکن است محدودیت های فنی داشته باشند. برای مثال، بعضی ممکن است با تمام ابزار موجود در شبکه شما کار نکنند، بنابراین ممکن است به چند سیستم برای ایجاد پوشش نیاز داشته باشید. همچنین، چندین فروشنده سیستم های کنترل دسترسی را به بازار عرضه می کنند، و عملکرد می تواند بین محصولات مختلف متفاوت باشد. پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد. چنین عمل وصله-پینه ای یعنی رویکرد چند محصولی ممکن است در واقع آسیب پذیری های بیشتری را در شبکه شما به وجود آورد.

ملاحظات

موفقیت ابزارهای امنیت سطح شبکه به نحوی به سرعت اتصالات داخلی شبکه شما وابسته است. زیرا ابزارهای IDS/IPS ، مدیریت آسیب پذیری و امنیت کاربر انتهایی ممکن است منابعی از شبکه ای را که از آن محافظت می کنند، مصرف کنند. سرعت های اتصالی بالاتر تأثیری را که این ابزارها بر کارایی شبکه دارند به حداقل خواهد رساند. در پیاده سازی این تکنولوژی ها شما باید به مصالحه بین امنیت بهبودیافته و سهولت استفاده توجه کنید، زیرا بسیاری از این محصولات برای کارکرد مؤثر باید به طور پیوسته مدیریت شوند و این ممکن است استفاده از آن محصولات را در کل شبکه با زحمت مواجه سازد.

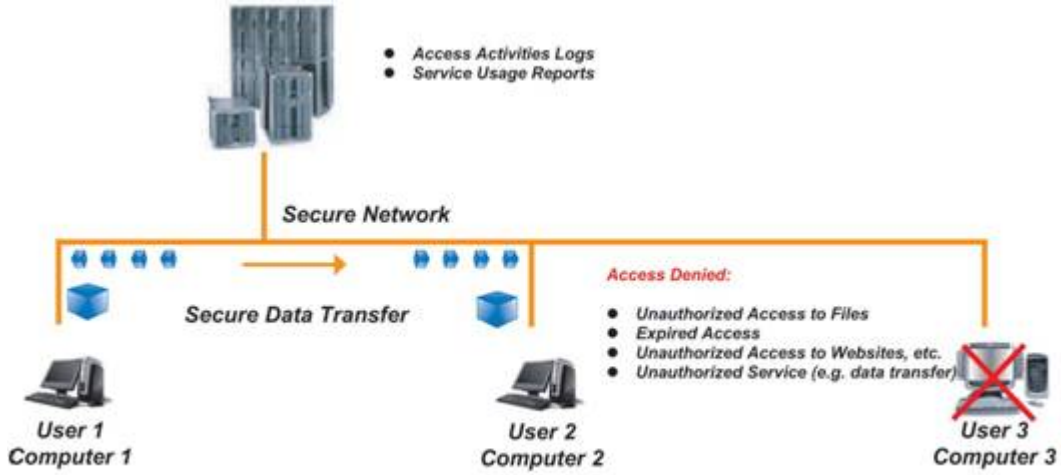
وقتی که این تکنولوژی ها را در اختیار دارید، بهبود پیوسته شبکه را در خاطر داشته باشید. در شبکه هایی با پویایی و سرعت گسترش بالا، تطبیق با شرایط و ابزار جدید ممکن است مسأله ساز گردد.

رویکردی عملی به امنیت شبکه لایه بندی شده (۴)

در شماره قبل به دومین لایه که لایه شبکه است، اشاره شد، در این شماره به لایه میزبان به عنوان سومین لایه می پردازیم.

سطح ۳- امنیت میزبان

سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، سوئیچ ها، روترها و غیره در شبکه است. هر ابزار تعدادی پارامتر قابل تنظیم دارد و هنگامی که به نادرستی تنظیم شوند، می توانند سوراخ های امنیتی نفوذپذیری ایجاد کنند. این پارامترها شامل تنظیمات رجیستری، سرویس ها، توابع عملیاتی روی خود ابزار یا وصله های سیستم های عامل یا نرم افزارهای مهم می شود.

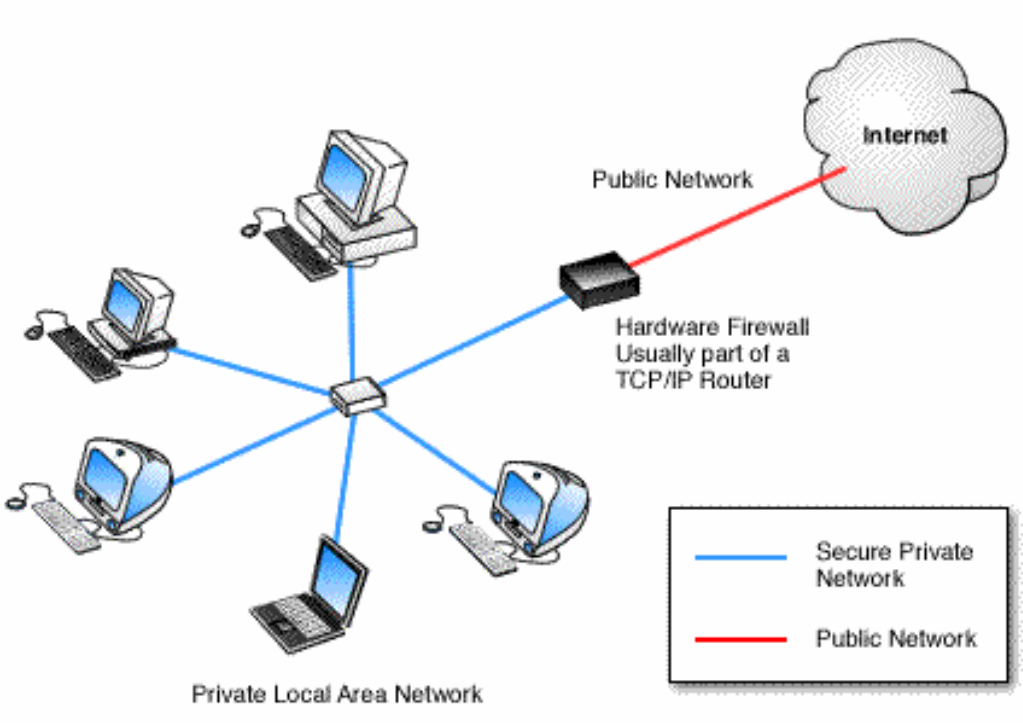


تکنولوژی های زیر امنیت را در سطح میزبان فراهم می کنند:

- **IDS در سطح میزبان** ـ IDSهای سطح میزبان عملیاتی مشابه IDSهای شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDSهای سطح میزبان برای مشخصات عملیاتی بخصوصی از ابزار میزبان تنظیم می گردند و بنابراین اگر به درستی مدیریت شوند، درجه بالایی از مراقبت را فراهم می کنند.
- **VA (تخمین آسیب پذیری) سطح میزبان** - ابزارهای VA سطح میزبان یک ابزار شبکه مجزا را برای آسیب پذیری های امنیتی پویش می کنند. دقت آنها نسبتا بالاست و کمترین نیاز را به منابع میزبان دارند. از آنجایی که VA ها بطور مشخص برای ابزار میزبان پیکربندی می شوند، درصورت مدیریت مناسب، سطح بسیار بالایی از پوشش را فراهم می کنند.
- **تابعیت امنیتی کاربر انتهایی** – روش های تابعیت امنیتی کاربر انتهایی وظیفه دوچندانی ایفا می کنند و هم شبکه (همانگونه در بخش قبلی مطرح شد) و هم میزبان های جداگانه را محافظت می کنند. این روش ها بطور پیوسته میزبان را برای عملیات زیان رسان و آلودگی ها بررسی می کنند و همچنین به نصب و به روز بودن فایروال ها و آنتی ویروس ها رسیدگی می کنند.
- **آنتی ویروس** - هنگامی که آنتی ویروس های مشخص شده برای ابزار در کنار آنتی ویروس های شبکه استفاده می شوند ، لایه اضافه ای برای محافظت فراهم می کنند.
- **کنترل دسترسی\تصدیق هویت**- ابزار کنترل دسترسی در سطح ابزار یک روش مناسب است که تضمین می کند دسترسی به ابزار تنها توسط کاربران مجاز صورت پذیرد. در اینجا نیز، احتمال سطح بالایی از تراکنش بین ابزار کنترل دسترسی شبکه و کنترل دسترسی میزبان وجود دارد.

مزایا

این تکنولوژی های در سطح میزبان حفاظت بالایی ایجاد می کنند زیرا برای برآورده کردن مشخصات عملیاتی مخصوص یک ابزار پیکربندی می گردند. دقت و پاسخ دهی آنها به محیط میزبان به مدیران اجازه می دهد که به سرعت مشخص کنند کدام تنظمیات ابزار نیاز به به روز رسانی برای تضمین عملیات امن دارند.



معایب

بکارگیری و مدیریت سیستم های سطح میزبان می تواند بسیار زمان بر باشند. از آنجایی که این سیستم ها نیاز به نمایش و به روز رسانی مداوم دارند، اغلب ساعات زیادی برای مدیریت مناسب می طلبند. اغلب نصبشان مشکل است و تلاش قابل ملاحظه ای برای تنظیم آنها مورد نیاز است. همچنین، هرچه سیستم عامل بیشتری در شبکه داشته باشید، یک رویکرد برپایه میزبان، گران تر خواهد بود و مدیریت این ابزار مشکل تر خواهد شد. همچنین، با تعداد زیادی ابزار امنیتی سطح میزبان در یک شبکه، تعداد هشدارها و علائم اشتباه می تواند بسیار زیاد باشد.

ملاحظات

بدلیل هزینه ها و باراضافی مدیریت، ابزار در سطح میزبان باید بدقت بکار گرفته شوند. بعنوان یک اصل راهنما، بیشتر سازمان ها این ابزار را فقط روی سیستم های بسیار حساس شبکه نصب می کنند. استثناء این اصل یک راه حل تابعیت امنیتی کاربر انتهایی است، که اغلب برای پوشش دادن به هر ایستگاه کاری که تلاش می کند به شبکه دسترسی پیدا کند، بکار گرفته می شود.

رویکردی عملی به امنیت شبکه لایه بندی شده ۵

در شماره قبل به سومین لایه که لایه میزبان است، اشاره شد. در این شماره به لایه برنامه کاربردی بعنوان چهارمین لایه و لایه دیتا بعنوان پنجمین لایه می پردازیم.

سطح ۴- امنیت برنامه کاربردی

در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خود کرده است. برنامه هایی که به میزان کافی محافظت نشده اند، می توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند. حقیقت تلخ این است که بیشتر برنامه نویسان هنگام تولید کد به امنیت توجه ندارند. این یک مشکل تاریخی در بسیاری از برنامه های با تولید انبوه است. ممکن است شما از کمبود امنیت در نرم افزارها آگاه شوید، اما قدرت تصحیح آنها را نداشته باشید.

برنامه ها برای دسترسی مشتریان، شرکا و حتی کارمندان حاضر در محل های دیگر، روی وب قرار داده می شوند. این برنامه ها، همچون بخش فروش، مدیریت ارتباط با مشتری، یا سیستم های مالی، می توانند هدف خوبی برای افرادی که نیات بد دارند، باشند. بنابراین بسیار مهم است که یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

تکنولوژی های زیر امنیت را در سطح برنامه فراهم می کنند:

- **پوشش محافظ برنامه** – از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای کاربر شفاف است و با درجه بالایی با سیستم یکپارچه می شود.

  یک پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد. برای مثال، یک پوشش روی سرور ایمیل به این منظور پیکربندی می شود تا جلوی اجرای خودکار برنامه ها توسط ایمیل های وارد شونده را بگیرد، زیرا این کار برای ایمیل معمول یا لازم نیست.
- **کنترل دسترسی/تصدیق هویت**- مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می توانند به برنامه دسترسی داشته باشند.
- **تعیین صحت ورودی** - ابزارهای تعیین صحت ورودی بررسی می کنند که ورودی گذرنده از شبکه برای پردازش امن باشد. اگر ابزارهای امنیتی مناسب در جای خود مورد استفاده قرار نگیرند، هر تراکنش بین افراد و واسط کاربر می تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود مگر اینکه خلافش ثابت شود!

به عنوان مثال، یک فرم وبی با یک بخش zip code را در نظر بگیرید. تنها ورودی قابل پذیرش در این قسمت فقط پنج کاراکتر عددی است. تمام ورودی های دیگر باید مردود شوند و یک پیام خطا تولید شود. تعیین صحت ورودی باید در چندین سطح صورت گیرد. در این مثال، یک اسکریپت جاوا می تواند تعیین صحت را در سطح مرورگر در سیستم سرویس گیرنده انجام دهد، در حالیکه کنترل های بیشتر می تواند در سرور وب قرار گیرد. اصول بیشتر شامل موارد زیر می شوند:

- کلید واژه ها را فیلتر کنید. بیشتر عبارات مربوط به فرمانها مانند «insert»، باید بررسی و در صورت نیاز مسدود شوند.
- فقط دیتایی را بپذیرید که برای فلید معین انتظار می رود. برای مثال، یک اسم کوچک ۷۵ حرفی یک ورودی استاندارد نیست.

مزایا

ابزارهای امنیت سطح برنامه موقعیت امنیتی کلی را تقویت می کنند و به شما اجازه کنترل بهتری روی برنامه هایتان را می دهند. همچنین سطح بالاتری از جوابگویی را فراهم می کنند چرا که بسیاری از فعالیت های نمایش داده شده توسط این ابزارها، ثبت شده و قابل ردیابی هستند.

معایب

پیاده سازی جامع امنیت سطح برنامه می تواند هزینه بر باشد، چرا که هر برنامه و میزبان آن باید بصورت مجزا ارزیابی، پیکربندی و مدیریت شود. بعلاوه، بالابردن امنیت یک شبکه با امنیت سطح برنامه می تواند عملی ترسناک! و غیرعملی باشد. هرچه زودتر بتوانید سیاست هایی برای استفاده از این ابزارها پیاده کنید، روند مذکور موثرتر و ارزان تر خواهد بود.

ملاحظات

ملاحظات کلیدی برنامه ها و طرح های شما را برای بلندمدت اولویت بندی می کنند. امنیت را روی برنامه ها کاربردی خود در جایی پیاده کنید که بیشترین منفعت مالی را برای شما دارد. طرح ریزی بلندمدت به شما اجازه می دهد که ابزارهای امنیتی را با روشی تحت کنترل در طی رشد شبکه تان پیاده سازی کنید و از هزینه های اضافی جلوگیری می کند.

سطح ۵ - امنیت دیتا

امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را دربرمی گیرد. رمزنگاری دیتا، هنگامی که ذخیره می شود و یا در شبکه شما حرکت می کند، به عنوان روشی بسیار مناسب توصیه می گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می کند. امنیت دیتا تا حد زیادی به سیاست های سازمانی شما وابسته است. سیاست سازمانی می گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می دهد که سیاست های دسترسی و ابزار امنیتی مناسبی را که باید بکار گرفته شوند، مشخص کنید.

تکنولوژی های زیر امنیت در سطح دیتا را فراهم می کنند:

- **رمزنگاری** – طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می شوند. تقریباً تمام طرح ها شامل کلیدهای رمزنگاری/رمزگشایی هستند که تمام افرادی که به دیتا دسترسی دارند، باید داشته باشند. استراتژی های رمزنگاری معمول شامل PKI، PGP و RSA هستند.
- **کنترل دسترسی / تصدیق هویت** – مانند تصدیق هویت سطوح شبکه، میزبان و برنامه، تنها کاربران مجاز دسترسی به دیتا خواهند داشت.

مزایا

رمزنگاری روش اثبات شده ای برای محافظت از دیتای شما فراهم می کند. چنانچه نفوذگران تمام ابزارهای امنیتی دیگر در شبکه شما را خنثی کنند، رمزنگاری یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال شما فراهم می کند.

معایب

بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می تواند تبدیل به یک بار اجرایی در سازمان های بزرگ یا در حال رشد گردد.

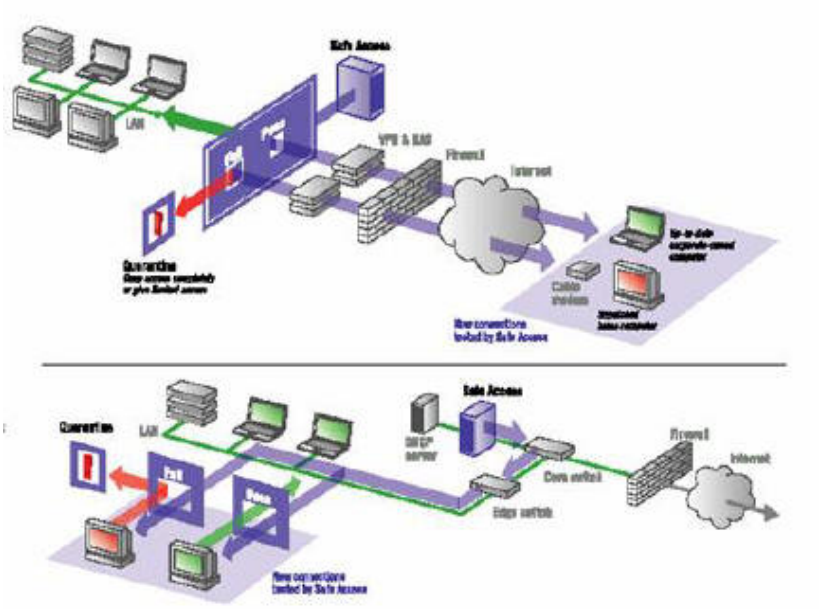
ملاحظات

رمزنگاری تا عمق مشخص باید به دقت مدیریت شود. کلیدهای رمزنگاری باید برای تمام ابزارها و برنامه های تحت تأثیر تنظیم و هماهنگ شوند. به همین دلیل، یک بار مدیریتی برای یک برنامه رمزنگاری موثر مورد نیاز است.

رویکردی عملی به امنیت شبکه لایه بندی شده (٦) : جمع بندی

در شماره های قبل به لایه های مختلف در امنیت شبکه لایه بندی شده پرداختیم. در این شماره به اختصار به جمع بندی مباحث فوق می پردازیم.

دفاع در مقابل تهدیدها و حملات معمول



مقالات گذشته نشان می دهد که چگونه رویکرد امنیت لایه بندی شده در مقابل تهدیدها و حملات معمول از شبکه شما محافظت می کند و نشان می دهد که چگونه هر سطح با داشتن نقشی کلیدی در برقراری امنیت شبکه جامع و مؤثر، شرکت می کند. بعضی حملات معمول شامل موارد زیر می شود:

- **حملات به وب سرور** ـ حملات به وب سرور دامنه زیادی از مشکلاتی را که تقریباً برای هر وب سرور ایجاد می شود، در برمی گیرد. از دستکاری های ساده در صفحات گرفته تا در اختیار گرفتن سیستم از راه دور و تا حملات DOS. امروزه حملات به وب سرور یکی از معمول ترین حملات هستند. Code Red و Nimda به عنوان حمله کنندگان به وب سرورها از شهرت زیادی! برخوردارند.
- **بازپخش ایمیل ها بصورت نامجاز** ـ سرورهای ایمیلی که بصورت مناسب پیکربندی نشده اند یک دلیل عمده برای ارسال هرزنامه ها بشمار می روند. بسیاری از شرکت های هرزنامه ساز در پیدا کردن این سرورها و ارسال صدها و هزاران پیام هرزنامه به این سرورها، متخصص هستند.
- **دستکاری میزبان دور در سطح سیستم** ـ تعدادی از آسیب پذیری ها، یک سیستم را از راه دور در اختیار حمله کننده قرار می دهند. بیشتر این نوع کنترل ها در سطح سیستم است و به حمله کننده اختیاراتی برابر با مدیر محلی سیستم می دهد.
- **فراهم بودن سرویس های اینترنتی غیرمجاز** ـ توانایی آسان بکارگیری یک وب سرور یا سرویس اینترنتی دیگر روی یک کامپیوتر ریسک افشای سهوی اطلاعات را بالا می برد. اغلب چنین سرویس هایی کشف نمی شوند، در حالی که در شعاع رادار دیگران قرار می گیرند!
- **تشخیص فعالیت ویروسی** ـ در حالی که برنامه ضدویروس در تشخیص ویروس ها مهارت دارد، این نرم افزار برای تشخیص فعالیت ویروسی طراحی نشده است. در این شرایط بکارگیری یک برنامه تشخیص نفوذ یا IDS شبکه برای تشخیص این نوع فعالیت بسیار مناسب است.

نتیجه گیری

هکرها و تروریست های فضای سایبر به طور فزاینده ای اقدام به حمله به شبکه ها می کنند. رویکرد سنتی به امنیت ـ یعنی یک فایروال در ترکیب با یک آنتی ویروس ـ در محافظت از شما در برابر تهدیدهای پیشرفته امروزی ناتوان است.

اما شما می توانید با برقراری امنیت شبکه با استفاده از رویکرد لایه بندی شده دفاع مستحکمی ایجاد کنید. با نصب گزینشی ابزارهای امنیتی در پنج سطح موجود در شبکه تان (پیرامون، شبکه، میزبان، برنامه و دیتا) می توانید از دارایی های دیجیتالی خود محافظت کنید و از افشای اطلاعات خود در اثر ایجاد رخنه های مصیبت بار تا حد زیادی بکاهید.

کلیدها در رمزنگاری

با روشن شدن اهمیت وجود کلیدها در امنیت داده‌ها، اکنون باید به انواع کلیدهای موجود و مکان مناسب برای استفاده هر نوع کلید توجه کنیم.

۱- کلیدهای محرمانه (Secret keys)

الگوریتمهای متقارن مانند DES از کلیدهای محرمانه استفاده می‌کنند؛ کلید باید توسط دو طرف تراکنش منتقل و ذخیره شود. چون فرض بر این است که الگوریتم شناخته شده و معلوم است، این قضیه اهمیت امن بودن انتقال و ذخیره کلید را مشخص می‌سازد. کارتهای هوشمند معمولا برای ذخیره کلیدهای محرمانه استفاده می‌شوند. در این حالت تضمین اینکه قلمرو کلید محدود است، مهم است: باید همیشه فرض کنیم که یک کارت ممکن است با موفقیت توسط افراد غیرمجاز تحلیل گردد، و به این ترتیب کل سیستم نباید در مخاطره قرار گیرد.

۲- کلیدهای عمومی و اختصاصی (Public and private keys)

امتیاز اصلی و مهم سیستمهای کلید نامتقارن این است که آنها اجازه می‌دهند که یک کلید (کلید اختصاصی) با امنیت بسیار بالا توسط تولید کننده آن نگهداری شود در حالیکه کلید دیگر (کلید عمومی)می‌تواند منتشر شود. کلیدهای عمومی می‌توانند همراه پیامها فرستاده شوند یا در فهرستها لیست شوند (شروط و قوانینی برای کلیدهای عمومی در طرح فهرست پیامرسانی الکترونیکی ITU X.500 وجود دارد)، و از یک شخص به شخص بعدی داده شوند. مکانیسم توزیع کلیدهای عمومی می‌تواند رسمی (یک مرکز توزیع کلید) یا غیررسمی باشد.

محرمانگی کلید اختصاصی در چنین سیستمی مهمترین مساله است؛ باید توسط ابزار منطقی و فیزیکی در کامپیوتری که ذخیره شده، محافظت گردد. کلیدهای اختصاصی نباید هرگز بصورت رمزنشده در یک سیستم کامپیوتر معمولی یا بشکلی که توسط انسان قابل خواندن باشد، ذخیره شوند. در اینجا نیز کارت هوشمند برای ذخیره کلیدهای اختصاصی یک فرد قابل استفاده است، اما کلیدهای اختصاصی سازمانهای بزرگ معمولا نباید در یک کارت ذخیره شود.

۳- کلیدهای اصلی و کلیدهای مشتق‌شده (keys Master keys and derived)

یک روش کاستن از تعداد کلیدهایی که باید منتقل و ذخیره شوند، مشتق گرفتن از آنهاست هر زمانی که استفاده می‌شوند. در یک برنامه اشتقاق کلید، یک کلید اصلی همراه با چند پارامتر مجزا برای محاسبه کلید مشتق‌شده استفاده می‌شود که بعدا برای رمزنگاری استفاده می‌گردد. برای مثال، اگر یک صادرکننده با تعداد زیادی کارت سروکار دارد، می‌تواند برای هر کارت، با استفاده از کلید اصلی، شماره کارت را رمز کند و به این ترتیب کلید مشتق‌شده حاصل می‌شود و به آن کارت اختصاص داده می‌شود.

شکل دیگری از کلیدهای مشتق‌شده با استفاده از tokenها که محاسبه‌گرهای الکترونیکی با عملکردهای بخصوص هستند، محاسبه می‌شوند. آنها ممکن است بعنوان ورودی از یک مقدار گرفته شده از سیستم مرکزی، یک PIN وارد شده توسط کاربر و تاریخ و زمان استفاده کنند. خود token شامل الگوریتم و یک کلید اصلی است. چنینی tokenهایی اغلب برای دسترسی به سیستمهای کامپیوتری امن استفاده می‌شوند.

۴- کلیدهای رمزکننده‌کلید (keys Key-encrypting)

از آنجا که ارسال کلید یک نقطه ضعف از نظر امنیتی در یک سیستم بشمار می‌رود، رمزکردن کلیدها هنگام ارسال و ذخیره آنها بشکل رمزشده منطقی بنظر می‌رسد. کلیدهای رمزکننده کلید هرگز به خارج از یک سیستم کامپیوتری (یا کارت هوشمند) ارسال نمی‌شوند و بنابراین می‌توانند آسانتر محافظت شوند تا آنهایی که ارسال می‌شوند. اغلب الگوریتم متفاوتی برای تبادل کلیدها از آنچه که برای رمزکردن پیامها استفاده می‌شود، مورد استفاده قرار می‌گیرد.

از مفهوم دامنه کلید (domain key) برای محدود کردن میدان کلیدها و محافظت کردن کلیدها در دامنه‌شان استفاده می‌کنیم. معمولا یک دامنه، یک سیستم کامپیوتری خواهد بود که می‌تواند بصورت فیزیکی و منطقی محافظت گردد. کلیدهای استفاده شده در یک دامنه توسط یک کلید رمزکننده‌کلید محلی ذخیره می‌شوند.هنگامی که کلیدها می‌خواهند به یک سیستم کامپیوتری دیگر فرستاده شوند، رمزگشایی و تحت یک کلید جدید رمز می‌شوند که اغلب

بعنوان کلید کنترل ناحیه (key zone control) شناخته می‌شوند. با دریافت این کلیدها در طرف دیگر، تحت کلید محلی سیستم جدید رمز می‌شوند. بنابراین کلیدهایی که در دامنه‌های یک ناحیه قرار دارند از دامنه‌ای به دامنه دیگر بصورتی که بیان گردید منتقل می‌شوند.

۵- کلیدهای نشست (keys Session)

برای محدودکردن مدت زمانی که کلیدها معتبر هستند، اغلب یک کلید جدید برای هر نشست یا هر تراکنش تولید می‌شود. این کلید ممکن است یک عدد تصادفی تولید شده توسط ترمینالی باشد که در مرحله تصدیق کارت قرار دارد باشد. اگر کارت قادر به رمزگشایی روش کلید عمومی باشد، یعنی کلید نشست می‌تواند با استفاده از کلید عمومی کارت رمز شود.

بخشی از تراکنش که در آن کلید منتقل می‌شود اغلب در مقایسه با بقیه تراکنش کوتاهتر است؛ بنابراین بار اضافی این بخش نسبت به کل تراکنش قابل صرفنظر است. چنانچه بقیه تراکنش بسبب استفاده از کلید متقارن با بالاسری کمتری رمز شود، زمان پردازش برای فاز تایید هویت و انتقال کلید قابل پذیرش است. (توضیح اینکه روشهای رمز متقارن از نامتقارن بمراتب سریعتر هستند بنابراین می‌توان ابتدا یک کلید متقارن را با استفاده از روش نامتقارن انتقال داد و سپس از آن کلید متقارن برای انجام بقیه تراکنش استفاده کرد.)

شکل خاصی از کلید نشست، سیستم انتقال کلید است که در برخی سیستمهای پرداخت الکترونیک و مبادله دیتای الکترونیک استفاده می‌شود. بدین صورت که در پایان هر تراکنش، یک کلید جدید منتقل می‌شود و این کلید برای تراکنش بعدی مورد استفاده قرار می‌گیرد.

موفق و پیروز باشید