

■ موضوع:



امنیت در شبکه های کامپیوتری

SECURITY IN NETWORK COMPUTER



گرد آورنده :

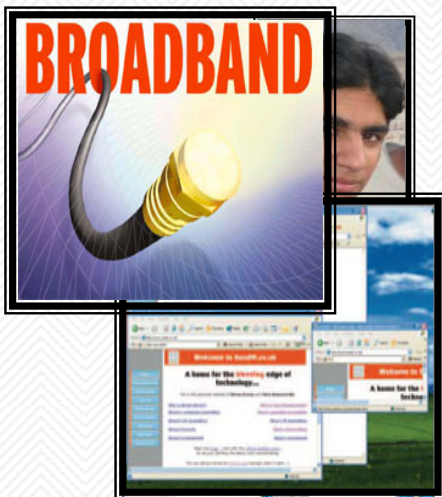
داوود خرسند

D_KHORSAND

Email:

DKHX2000yahoo.com

DKHX2000@Gmail.com



AUTUMN 2005

پائیز ۱۴۰۵

امنیت برنامه های وب (بخش اول)

هر برنامه کامپیوتری که برای اجراء در محیط شبکه، طراحی و پیاده سازی می گردد، می بایست توجه خاصی به مقوله امنیت داشته باشد. برنامه های وب از زیرساخت شبکه (اینترنت، اینترانت) برای ارائه خدمات خود به کاربران استفاده نموده و لازم است نحوه دستیابی کاربران به این نوع از برنامه ها، کنترل و با توجه به سیاست های موجود، امکان دستیابی فراهم گردد. در ابتدا می بایست کاربران شناسائی و پس از تأیید هویت آنان، امکان دستیابی به برنامه با توجه به مجوزهای تعریف شده، فراهم گردد. ASP.NET (پلات فرم مایکروسافت برای طراحی و پیاده سازی برنامه های وب)، از سه روش عمده به منظور شناسائی کاربران و اعطای مجوزهای لازم در جهت دستیابی و استفاده از یک برنامه وب، استفاده می نماید:

Windows Authentication

Forms Authentication

Authentication Passport

در مجموعه مقالاتی که ارائه خواهد شد به بررسی هر یک از روش های فوق در جهت پیاده سازی امنیت در برنامه های وب خواهیم پرداخت. در بخش اول این مقاله، به بررسی نحوه برخورد ASP.NET با کاربران ناشناس (Anonymous)، روش های متفاوت شناسائی کاربران و پارامترهای لازم در خصوص انتخاب یک استراتژی به منظور شناسائی کاربران با توجه به نوع برنامه ها، خواهیم پرداخت.

شناسائی و تأیید کاربران

Authentication، فرآیندی است که بر اساس آن کاربران شناسائی می گردند. Authorization، فرآیند اعطای دستیابی به کاربران با توجه به هویت آنان می باشد. با تلفیق Authentication و Authorization، امکان ایمن سازی برنامه های وب در مقابل افراد مزاحم و غیر مجاز، فراهم می گردد.

دستیابی از طریق کاربران ناشناس (Anonymous)

اغلب سایت های وب از روش دستیابی "Anonymous"، استفاده می نمایند. در چنین مواردی، اطلاعات موجود بر روی سایت جنبه عمومی داشته و امکان دستیابی تمامی کاربران به اطلاعات وجود خواهد داشت. این نوع سایت ها، ضرورتی به بررسی مجاز بودن کاربران برای استفاده از منابع موجود، نخواهند داشت. برنامه های وب ASP.NET، امکان دستیابی Anonymous را به منابع موجود بر روی سرور دهنده توسط Impersonation ارائه می نمایند. Impersonation، فرآیند نسبت دهی یک Account به یک کاربر ناشناس است. Account دستیابی Anonymous بصورت پیش فرض، IUSER_computername، می باشد. با استفاده از Account فوق، امکان کنترل کاربران ناشناس که به منابع موجود بر سرور دهنده دستیابی دارند، وجود خواهد داشت. به منظور مشاهده و تغییر مجوزهای دستیابی در نظر گرفته شده برای Account فوق از برنامه Computer Management استفاده می گردد:

ورود به شبکه (Logon) به عنوان مدیریت شبکه

اجرای Computer Management (از طریق : Administrator | Programs | Tools Start)

انتخاب فولدر Users به منظور نمایش لیست کاربران

مشاهده گروههایی که Account فوق به عنوان عضوی از آنان می باشد (کلیک بر روی Member of). کاربران Anonymous، بصورت پیش فرض، عضوی از گروه Guests بوده که دارای مجوزهای اندکی می باشد. ASP.NET از ASP.NET Account (با توجه به تنظیمات پیش فرض)، به منظور اجرای برنامه وب استفاده می نماید. بدین ترتیب، در صورتیکه برنامه ای سعی در انجام عملیاتی نماید که در لیست مجوزهای ASP.NET Account وجود نداشته باشد، یک مورد خاص امنیتی بوجود آمده و امکان دستیابی آن تأیید نخواهد شد.

به منظور اعمال محدودیت در دستیابی کاربران ناشناس می توان از تنظیمات مربوط به مجوزهای فایل ویندوز استفاده نمود. برای ایمن سازی، سرور دهنده می بایست دارای سیستم فایل NTFS باشد. سیستم های فایل FAT و یا FAT32، ایمن سازی در سطح فایل را ارائه نمی نمایند.

دستیابی از طریق کاربران تأیید شده

دستیابی Anonymous ، گزینه ای مناسب برای دستیابی به اطلاعات عمومی و عام است . در صورتیکه برنامه های وب شامل اطلاعاتی خاص و خصوصی باشند ، می بایست در ابتدا کاربران شناسائی و در ادامه با توجه به مجوزهای تعریف شده ، امکان دستیابی فراهم گردد. در برنامه های وب ASP.NET از سه روش عمده به منظور Authentication و Authorization کاربران استفاده می گردد :

Windows integrated authentication : در روش فوق ، شناسائی و تأیید کاربران بر اساس لیست کاربران تعریف شده بر روی سرورس دهنده انجام خواهد شد. در ادامه با توجه به مجوزها و امتیازات نسبت داده شده به هر Account ، امکان دستیابی و یا عدم دستیابی به منابع موجود بر روی سرورس دهنده ، فراهم می گردد.

authentication Forms : در روش فوق ، کاربران به یک فرم وب Logon ، هدایت می گردند . در ادامه ، اطلاعات مربوط به نام و رمز عبور آنان اخذ و فرآیند شناسائی و تأیید بر اساس یک لسیت کاربران و یا از طریق یک بانک اطلاعاتی که برنامه حمایت می نماید ، انجام خواهد شد.

Passport authentication : در روش فوق ، کاربران جدید به یک سایت که توسط مایکروسافت میزبان شده است ، هدایت می گردند . پس از رجیستر شدن کاربران ، امکان دستیابی آنان به چندین سایت ، فراهم خواهد شد (تمرکز در شناسائی کاربران و استفاده از سایت های متعدد با توجه به تأیید بعمل آمده) .

هر یک از رویکردهای فوق ، به همراه روش دستیابی Anonymous ، دارای مزایای مختص به خود بوده و برای نوع خاصی از برنامه های وب ، مناسب می باشند :

نوع برنامه : برنامه وب عمومی اینترنت

روش تأیید کاربران : Anonymous

توضیحات : روش عمومی دستیابی برای اغلب سایت های وب ، می باشد. در این روش ، ضرورتی به Logon وجود نداشته و با استفاده از مجوزهای سیستم فایل NTFS ، می توان ایمن سازی منابعی را که قصد اعمال محدودیت در رابطه با دستیابی به آنان وجود دارد را انجام داد .

نوع برنامه : برنامه وب اینترنت

روش تأیید کاربران : integrated Windows

توضیحات : در روش فوق ، سیستم معتبر سازی ویندوز ، کاربران شبکه را از طریق کنترل کننده Domain ، تأیید می نماید. امکان دستیابی به منابع برنامه های وب بر اساس مجوزهای تعریف شده بر روی سرورس دهنده ، برای هر یک از کاربران فراهم می گردد .

نوع برنامه : برنامه های وب تجاری

روش تأیید کاربران : Forms

توضیحات : برنامه هایی که نیازمند دریافت اطلاعات مالی می باشند ، می بایست از روش فوق به منظور اخذ و ذخیره سازی اطلاعات ، استفاده نمایند .

نوع برنامه : برنامه های متعدد تجاری

روش تأیید کاربران : Passport

توضیحات : در روش فوق ، کاربران یک مرتبه Sign in نموده (از طریق یک مرکز تأیید کاربران) و امکان دستیابی و استفاده آنان از تمامی برنامه هایی که از Passport SDK استفاده می نمایند ، وجود خواهد داشت . اطلاعات کاربران در یک Passport profile نگهداری خواهد شد (در مقابل استفاده از یک بانک اطلاعاتی محلی) .

استفاده از Authentication در فایل های HTML و یا HTML

سه روش تأیید کاربران که توسط ASP.NET ارائه شده است ، صرفاً در رابطه با فایل هایی که به عنوان بخشی از برنامه وب می باشند ، بکار گرفته می شود . فرم های وب (فایل هایی با انشعاب aspx .) ، ماژول ها (فایل هایی با انشعاب asax .) ، نمونه هایی در این زمینه می باشند. فرآیند فوق ، صفحات HTML (فایل هایی با انشعاب HTML و یا HTML) را شامل نمی گردد و مسئولیت آن بصورت پیش فرض به IIS (در مقابل ASP.NET) واگذار شده است. در

صورتیکه قصد تأیید کاربرانی (استفاده از یکی از روش های Windows,Forms و Passport) را داشته باشیم که به صفحات HTML از طریق برنامه وب دستیابی دارند ، می بایست این نوع فایل ها به executable ASP.NET ، مپ گردند . به منظور مپ نمودن فایل های html به ASP.NET executable ، پس از اجرای IIS مراحل زیر را دنبال می نمائیم :

انتخاب فولدر شامل برنامه وب و Properties از طریق Action Menu . در ادامه برنامه IIS ، جعبه محاوره ای Properties را نمایش خواهد داد .

بر روی Directory Tab کلیک نموده و در ادامه گزینه Configuration را انتخاب می نمائیم . IIS در ادامه جعبه محاوره ای Application Configuration را نمایش خواهد داد

بر روی دکمه Add کلیک نموده و در ادامه IIS جعبه محاوره ای Add/Edit Application Extension Mapping را نمایش خواهد داد .

بر دکمه Browse کلیک نموده و فایل aspnet_isapi.dll را انتخاب می نمائیم . فایل فوق در دایرکتوری Windows Microsoft .Net Framework قرار داشته و مسیر آن مشابه زیر است :

aspnet_isapi.dll Path for

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

.htm را در فیلد File Extension تایپ می نمائیم .

مراحل فوق ، برای فایل های با انشعاب html ، تکرار می گردد.

امنیت برنامه های وب (بخش دوم)

در این مقاله به بررسی Windows Authentication خواهیم پرداخت .

همانگونه که در بخش اول این مقاله اشاره گردید ، برنامه های وب ASP.NET از سه روش عمده به منظور تأیید کاربران استفاده می نمایند :

Authentication Windows

Forms Authentication

Passport Authentication

در Windows Authentication ، برنامه های وب مسئولیتی را در ارتباط با تأیید کاربران برعهده نگرفته و این وظیفه تماماً به سیستم عامل ویندوز ، واگذار می گردد. فرآیند تأیید کاربران در روش فوق ، بصورت زیر است :

کاربر درخواستی مبنی بر دریافت یک صفحه وب ایمن را از برنامه وب ، می نماید .

پس از دریافت درخواست توسط سرویس دهنده وب ، IIS عملیات بررسی صلاحیت کاربر را انجام خواهد داد . در این راستا ، اطلاعات ارائه شده توسط کاربر در زمان logon (نام و رمز عبور) ، با اطلاعات موجود بر روی سرویس دهنده وب و یا Domain ، مقایسه می گردد .

در صورتیکه پس از بررسی مدارک ارائه شده توسط کاربر (نام و رمز عبور) ، وی به عنوان کاربر غیر مجاز تشخیص داده شود ، درخواست وی نادیده گرفته خواهد شد .

کامپیوتر سرویس گیرنده ، یک جعبه محاوره ای Logon را تولید و از کاربر درخواست درج اطلاعات مورد نیاز (نام و رمز عبور) ، می گردد . پس از درج اطلاعات درخواستی توسط کاربر و ارسال آنان برای سرویس دهنده ، مجدداً IIS بررسی لازم در خصوص صحت آنان را انجام خواهد داد . در صورتیکه صحت اطلاعات ارسالی کاربر (نام و رمز عبور) تأیید گردد ، IIS درخواست اولیه کاربر را به سمت برنامه وب هدایت می نماید .

در آخرین مرحله و پس از بررسی و تأیید صلاحیت کاربر ، صفحه وب درخواستی برای کاربر ارسال می گردد .

مهمترین مزیت روش Authentication Windows ، استفاده مشترک از یک مدل امنیتی به منظور دستیابی به منابع موجود در شبکه و برنامه های وب است . پس از تعریف و اعطای مجوزهای لازم به کاربر ، امکان دستیابی وی به منابع موجود در شبکه و برنامه های وب بر اساس یک سیستم امنیتی مشابه و یکسان ، فراهم می گردد .

در زمان ایجاد یک پروژه جدید برنامه وب توسط ویژوال استودیو دات نت ، از روش Authentication Windows بصورت پیش فرض به منظور تأیید کاربران استفاده می گردد . پس از ایجاد یک پروژه جدید برنامه وب در ویژوال استودیو دات نت ، فایل Web.Config بصورت اتوماتیک ایجاد می گردد . (یک فایل XML که اطلاعات متفاوتی را در ارتباط با پیکربندی برنامه وب در خود ذخیره می نماید) . محتوی پیش فرض این فایل بصورت زیر است (صرفاً بخشی که با موضوع این مقاله ارتباط دارد ، منعکس می گردد) :

Web.Config default setting

```
<authentication mode="Windows" />
```

```
<authorization>
```

```
<allow users="*" /> <!-- تمامی کاربران -->
```

```
</authorization>
```

در بخش مربوط به عنصر authentication ، سیاست تأیید کاربران برنامه های وب مشخص می گردد . برای مشخص

نمودن سیاست فوق از خصلت mode مربوط به عنصر authentication ، استفاده شده که می تواند یکی از مقادیر :

Windows , Forms ,Passport و یا None را دارا باشد . در بخش authorization ، سیاست های مربوط به کاربران مجاز

برنامه وب مشخص می گردد . در این رابطه می توان ، امکان دستیابی و یا عدم دستیابی به برنامه های وب را با مشخص نمودن کاربران و یا با توجه به وظایف آنان ، فراهم نمود. (استفاده از کاراکتر " * " ، به معنی همه کاربران بوده و کاراکتر "?" به منزله کاربران ناشناس و غیرمجاز است) . برای آشنایی با عملکرد روش Windows Authentication ، مراحل زیر را دنبال می نمائیم :

بخش authorization در فایل Web.Config را بصورت زیر تغییر می نمائیم :

Authorization element

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

تگ های زیر را که یک جدول HTML را تعریف می نمایند ، در فرم وب شروع برنامه وب ، قرار می دهیم :

HTML Table in Startup web form

```
<TABLE id="tblUser">
<tr>
<TD><STRONG>آیا کاربر تأیید شده</STRONG></TD>
<TD><Span runat="server" id="spnAuthenticated"></Span></TD>
</tr>
<tr>
<TD><STRONG>نام کاربر</STRONG></TD>
<TD><Span runat="server" id="spnUserName"></Span></TD>
</tr>
<tr>
<TD><STRONG>نوع کاربر</STRONG></TD>
<TD><Span runat="server" id="spnAuthenticationtype"></Span></TD>
</tr>
</TABLE>
```

به حالت Design view سوئیچ نموده و کد زیر را در فایل Code Behind فرم وب شروع برنامه ، قرار می دهیم :

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 اجرای پروژه بصورت محلی ، ASP.NET تأیید کاربر را بر اساس نام و رمز عبوری که برای ورود به ویندوز استفاده شده است ، انجام خواهد داد .

پس از اجرای پروژه از راه دور (مثلاً " دستیابی از طریق اینترنت) ، ASP.NET یک جعبه محاوره ای رادر مرورگر نمایش داده تا از طریق آن نام و رمز عبور کاربر دریافت گردد .

در صورتیکه نام و رمز عبور درج شده توسط کاربر با تعاریف انجام شده در Domain شبکه ، مطابقت نماید ، ASP.NET کاربر را تأیید و مجوز لازم به منظور استفاده از برنامه وب صادر خواهد شد . در این رابطه ASP.NET ، یک authorization certificate را به شکل یک کوکی صادر که در حین Session کاربر ، نگهداری و از آن استفاده می گردد. Session کاربر، پس از اتمام زمان Time out و یا بستن مرورگر ، خاتمه می یابد . برنامه وب اجرای خود را متناسب با مجوزهای تعریف شده در ارتباط با Account آغاز می نماید .

روش integrated authentication Windows در یک شبکه مبتنی بر Domain بهتر کار خواهد کرد . شبکه هائی که از Workgroup استفاده می نمایند (در مقابل استفاده از Domain) دارای محدودیت های خاص خود به منظور استفاده از ویژگی های امنیتی ، می باشند. شبکه های مبتنی بر Domain ، از یک کنترل کننده Domain به منظور تأیید و معتبرسازی کاربران شبکه ، استفاده می نماید .

با استفاده از امکانات ارائه شده در فایل Web.Config می توان یک لایه امنیتی مضاعف را ایجاد نمود . دراین راستا ، می توان تنظیمات لازم به منظور دستیابی و یا عدم دستیابی کاربران و یا گروه های خاصی از کاربران را نیز انجام داد . اعمال محدودیت برای کاربران خاص (دستیابی و یا عدم دستیابی)

در مواردیکه از روش Windows integrated authentication استفاده می گردد ، ASP.NET ، لیست تأیید موجود در فایل Web.Config را به منظور آگاهی از صلاحیت کاربران شبکه برای استفاده از برنامه وب ، بررسی می نماید. کاراکترهای "*" و "?" دارای معانی خاصی در لیست تأیید می باشند : کاراکتر "*" ، نشاندهنده تمامی کاربران و کاراکتر "?" ، نشاندهنده کاربران غیر مجاز(ناشناس) می باشد . مثلاً " لیست تأیید زیر در Web.Config ، امکان دستیابی تمامی کاربران ناشناس به برنامه وب را حذف و می بایست تمامی کاربران به منظور استفاده از برنامه وب ، تأیید گردند .

Authorization element

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

به منظور اعمال محدودیت در دستیابی کاربرانی خاص ، می توان از عنصر <allow> استفاده و اسامی تمامی کاربران مجاز را با صراحت مشخص نمود (اسامی توسط ویرگول از یکدیگر تفکیک می گردند) . پس از معرفی کاربران مجاز با استفاده از عنصر <allow> ، می بایست با بکارگیری عنصر <deny> ، امکان دستیابی به برنامه توسط کاربران غیر مجاز، سلب می گردد .

Authorization element

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

لیست مجاز فوق ، امکان دستیابی دو کاربر که اسامی آنان با صراحت مشخص شده است را به برنامه وب خواهد داد. سایر کاربران ، امکان دستیابی به برنامه وب را دارا نخواهند بود (نقش عنصر deny در مثال فوق) علاوه بر لیست مجاز فوق که اسامی دو کاربر را مشخص و آنان را برای استفاده از برنامه وب مجاز می نماید ، دو کاربر فوق ، می بایست دارای Account لازم در Domain شبکه نیز باشند .

تأیید کاربران بر اساس نوع وظیفه

برای تأیید کاربران به منظور استفاده از یک برنامه می توان ، مجوزهای لازم را بر اساس وظیفه آنان در سازمان ، صادر و امکان دستیابی و یا عدم دستیابی را برای آنان فراهم نمود. در ویندوز NT و XP ، وظایف به اسامی مپ شده تا از این طریق امکان شناسایی گروه های کاربران ، فراهم گردد. ویندوز، چندین گروه را بصورت اتوماتیک از قبل ایجاد می نماید :

Users, Administrators و Guests . در این رابطه می توان از عنصر <roles> در لیست استفاده کنندگان مجاز برنامه وب در فایل Web.Config استفاده و امکان دستیابی به یک برنامه را با توجه به وظایف کاربر ، فراهم نمود. مثلاً "لیست زیر، امکان دستیابی به برنامه وب را صرفاً" برای کاربرانی که به عنوان Administrator به شبکه وارد می شوند ، فراهم می نماید.

Authorization element

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

پس از تأیید کاربر و صدور مجوز لازم به منظور استفاده از برنامه وب ، می توان با استفاده از خصلت Identity مربوط به شی User ، هویت کاربر (نام و نوع وظیفه) را از طریق برنامه شناسایی نمود. خصلت فوق، یک شی را که شامل اطلاعات مربوط به نام و وظیفه کاربر است را برمی 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 آگاهی و انجام عملیات لازم با توجه به نوع وظیفه کاربر که از برنامه وب استفاده می نماید ، می توان از متد IsInRole شی User ، استفاده نمود .

IsInRole method

```
If User.IsInRole("Administrators") Then  
انجام عملیات دلخواه  
End If
```

استفاده از تنظیمات IIS به همراه Authentication Windows

تنظیمات Authorization در فایل Web.Config با تنظیمات انجام شده در IIS با یکدیگر Overlap می شوند . در صورتیکه Authorization هم در فایل Web.Config و هم توسط IIS تنظیم شده باشد ، در ابتدا تنظیمات IIS بررسی و در ادامه تنظیمات موجود در فایل Web.Config ، مورد توجه قرار خواهند گرفت. به منظور مشاهده تنظیمات authorization در IIS مراحل زیر را دنبال می نمایم :

در IIS بر روی فولدر برنامه وب کلیک سمت راست نموده و در ادامه گزینه Properties را انتخاب می نمایم . برنامه IIS در ادامه جعبه محاوره ای Properties مربوط به فولدر را نمایش خواهد داد .

بر روی Directory Security Tab کلیک و در ادامه دکمه Edit را در گروه Anonymous Access And Authentication Control کلیک می‌نمایم . IIS ، جعبه محاوره ای Authentication Methods را نمایش خواهد داد . اولین گروه از تنظیمات در جعبه محاوره ای ، کنترل دستیابی Anonymous را انجام می‌دهد (همه کاربران). غیر فعال نمودن گزینه فوق ، معادل < deny User = "?" > در فایل Web.config است.

Check Box های موجود در قسمت دوم جعبه محاوره ای ، مجاز بودن برنامه به منظور استفاده از Basic و یا Digest Authentication را علاوه بر Windows Authentication ، مشخص می‌نماید. روش های فوق ، ایمنی بمراتب کمتری را نسبت به Windows Integrated ارائه می‌نمایند .می‌توان چندین روش authentication را در IIS فعال نمود . در صورتیکه چندین روش فعال شده باشد ، می‌توان با استفاده از متد AuthenticationType مربوط به شی Identity ، از روش استفاده شده به منظور تأیید کاربر ، آگاهی یافت .

AuthenticationType method

Response.Write(User.Identity.AuthenticationType)

امنیت برنامه های وب (بخش سوم)

در این مقاله به بررسی Authentication Forms خواهیم پرداخت .

همانگونه که در بخش اول این مقاله اشاره گردید ، برنامه های وب ASP.NET از سه روش عمده به منظور تأیید کاربران استفاده می نمایند :

Windows Authentication

Forms Authentication

Authentication Passport

در Forms Authentication ، برنامه IIS مسئولیتی را در ارتباط با تأیید کاربران برعهده نگرفته و تنظیمات امنیتی IIS در رابطه با برنامه وب ، دستیابی Anonymous می باشد . فرآیند تأیید کاربران در روش فوق ، بصورت زیر است :

زمانیکه سرویس گیرنده درخواست یک صفحه ایمن را می نماید ، IIS کاربر را به عنوان Anonymous ، تأیید و در ادامه درخواست وی را برای ASP.NET ارسال می نماید .

ASP.NET ، بررسی لازم در خصوص وجود یک کوکی خاص بر روی کامپیوتر سرویس گیرنده را انجام خواهد داد . در صورتیکه کوکی ، موجود نبوده و یا غیرمعتبر باشد ، ASP.NET درخواست کاربر را نادیده گرفته و برای وی یک صفحه Logon را ارسال می نماید (مثلاً "Login.aspx").

کاربر اطلاعات لازم (نام و رمز عبور) را در صفحه Logon.aspx (به عنوان نمونه) درج و در ادامه دکمه Submit موجود بر روی فرم را به منظور ارسال اطلاعات برای سرویس دهنده ، فعال می نماید.

IIS ، مجدداً کاربر را به عنوان Anonymous ، تأیید و درخواست وی را برای ASP.NET ارسال می نماید .

ASP.NET ، تأیید کاربر را بر اساس اطلاعات ارسالی (نام و رمز عبور) انجام و یک کوکی را ایجاد می نماید .

در نهایت ، صفحه وب ایمن درخواست شده به همراه کوکی جدید برای سرویس گیرنده ارسال می گردد. مادامیکه کوکی معتبر باشد ، کاربر قادر به درخواست و مشاهده سایر صفحات وب می باشد.



فرآیند فوق را می توان به دو حالت متفاوت تعمیم و مورد توجه قرار داد :

حالت اول : درخواست یک صفحه ایمن از سرویس دهنده ، توسط یک کاربر غیرمجاز و تأیید نشده

مرحله اول : پس از درخواست یک سرویس گیرنده برای دستیابی به یک صفحه ایمن ، درخواست ارسالی وی در ابتدا توسط IIS بررسی و با توجه به اینکه تنظیمات IIS بصورت Anonymous پیکربندی شده تا امکان استفاده از Forms Authentication فراهم گردد ، درخواست کاربر ، مستقیماً برای مازول ASP.NET Forms Authentication ارسال می گردد .

مرحله دوم : ASP.NET ، بررسی لازم در خصوص وجود (داشتن) یک کوکی Authentication را انجام خواهد داد . با توجه به اینکه کاربر اولین مرتبه است که درخواست اطلاعاتی را نموده و دارای یک کوکی نمی باشد ، سرویس گیرنده به صفحه Logon ، هدایت می گردد .

مرحله سوم : کاربر اطلاعات ضروری (نام و رمز عبور) خود را در صفحه Logon درج و پس از ارسال آنان ، فرآیند بررسی اطلاعات ارسالی آغاز می گردد. در یک برنامه بزرگ ، بررسی اطلاعات کاربر از طریق یک بانک اطلاعاتی شامل

مشخصات کاربران انجام می شود .

مرحله چهارم : در صورتیکه اطلاعات ارسالی کاربر (نام و رمز عبور) ، پس از بررسی توسط برنامه وب ، معتبر شناخته نگردند ، مجوز دستیابی برای کاربر صادر نشده و امکان دستیابی وی سلب می گردد .

مرحله پنجم : در صورتیکه پس از بررسی اطلاعات ارسالی، اعتبار وصحت آنان تأیید گردد ، یک کوکی تأیید ایجاد و در ادامه به کاربر مجوز لازم به منظور دستیابی به صفحه ، اعطاء می گردد .(هدایت کاربر به صفحه درخواست اولیه) .

حالت دوم : درخواست یک صفحه ایمن از سرویس دهنده ، توسط یک کاربر مجاز و تأیید شده

مرحله اول : پس از درخواست یک صفحه ایمن توسط سرویس گیرنده ، کوکی Authentication به همراه درخواست وی برای سرویس دهنده ، ارسال می گردد.

مرحله دوم :درخواست ارسالی توسط سرویس گیرنده در ابتدا توسط IIS دریافت و با توجه به تنظیمات انجام شده (دستیابی Anonymous) ، درخواست وی مستقیماً" برای ASP.NET Forms Authentication ارسال می گردد .

مرحله سوم : مازول ASP.NET Forms Authentication ، بررسی لازم در خصوص کوکی را انجام و در صورتیکه کوکی معتبر باشد ، سرویس گیرنده تأیید و امکان دستیابی و مشاهده صفحه وب درخواستی برای وی ، فراهم می گردد .

در روش Forms Authentication ، بصورت اتوماتیک یک فرم وب طراحی شده به منظور اخذ اطلاعات مربوط به نام و رمز عبور کاربران ، نمایش داده می شود . کد مرتبط با فرم وب ، عملیات تأیید و معتبرسازی کاربر را بر اساس لیست ذخیره

شده در فایل Web.Config برنامه و یا از طریق یک بانک اطلاعاتی جداگانه ، انجام می دهد. مزیت مهم Forms

Authentication ، عدم ضرورت عضویت کاربران در Domain شبکه به منظور دستیابی به برنامه وب ، می باشد .

فعال نمودن Forms Authentication

به منظور استفاده از روش فوق ، می بایست مراحل زیر را دنبال نمود :

مقداردهی Authentication mode در فایل Web.config به Forms

ایجاد یک فرم وب به منظور اخذ اطلاعات کاربران (Logon Page)

ایجاد یک فایل و یا بانک اطلاعاتی به منظور ذخیره نام و رمز عبور کاربران

نوشتن کد لازم به منظور افزودن کاربر جدید به فایل و یا بانک اطلاعاتی کاربران

نوشتن کد لازم به منظور تأیید کاربران با استناد به فایل و یا بانک اطلاعاتی کاربران

Forms Authentication ، از کلاس های موجود در namespace با نام System.Web.Security استفاده می نماید . به

منظور استفاده از کلاس های فوق، می بایست در ویژوال بیسک دات نت از عبارت Imports و در ویژوال سی شارپ از

Using استفاده گردد (در ابتدای هر مازول که عملیات تأیید را انجام خواهد داد : System.Web.Security Imports) .

مقداردهی Authentication mode

نوع تأیید کاربران در یک برنامه وب ، می بایست با استفاده از عنصر <authentication> در فایل Web.config مشخص

گردد. به منظور تنظیم برنامه مورد نظر خود برای استفاده از Forms Authentication ، تغییرات زیر را در فایل

Web.Config ، اعمال می نمائیم :

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>
```

کد فوق، یک نوع ساده از تائید کاربران به روش Forms را نشان می دهد . در این رابطه ، اغلب از تعاریف و تنظیمات پیش فرض و یک لیست کاربران مجاز، استفاده شده است. از عناصر متفاوتی در ارتباط با Forms Authentication در فایل Web.Config استفاده می گردد. هر یک از عناصر دارای خصلت های خاص خود می باشند :

عنصر <authentication>

خصلت Mode ، با استفاده از خصلت فوق ، روش تائید و شناسایی کاربران مشخص می گردد. با مقدار دهی خصلت فوق به Forms ، روش Authentication Forms انتخاب خواهد شد.

عنصر <forms>

خصلت name . از خصلت فوق به منظور مشخص نمودن نام کوکی که اطلاعات مربوط به نام و رمز عبور را ذخیره می نماید ، استفاده می شود . مقدار پیش فرض ، auth.aspx . می باشد . در صورتیکه بیش از یک برنامه بر روی سرور دهنده از روش Forms Authentication استفاده می نمایند ، می بایست برای هر یک از آنان نام منحصریفردي در نظر گرفته شود .

خصلت loginUrl . از خصلت فوق به منظور مشخص نمودن نام فرم وب Login برای کاربران تائید نشده ، استفاده می گردد . مقدار پیش فرض خصلت فوق ، Default.aspx است .

خصلت protection . با استفاده از خصلت فوق روش حفاظت کوکی Authentication که بر روی کامپیوتر سرور گیرنده ذخیره می گردد ، مشخص خواهد شد. مقدار پیش فرض خصلت فوق ، All بوده که عملیات رمزنگاری و بررسی اعتبار و صحت داده در رابطه با آن اعمال می گردد. سایر گزینه های موجود در این راستا ، Encryption, Validation و None می باشد .

خصلت timeout . با استفاده از خصلت فوق ، مدت زمان نگهداری کوکی Authentication بر روی ماشین کاربر مشخص می گردد . مقدار پیش فرض ۳۰ دقیقه است . ASP.NET ، پس از دریافت یک درخواست جدید توسط کاربر و مشروط به گذشت بیش از نصف زمان تعریف شده ، کوکی را تجدید (Renew) خواهد کرد .

خصلت path . با استفاده از خصلت فوق ، مسیر مورد نظر به منظور ذخیره سازی کوکی بر روی ماشین کاربر مشخص می گردد . مقدار پیش فرض ، "\" است .

عنصر <credentials>

خصلت passwordFormat ، با استفاده از خصلت فوق ، الگوریتم لازم به منظور رمزنگاری رمز عبور کاربر ، مشخص می گردد . مقدار پیش فرض ، SHA1 می باشد . سایر گزینه های موجود در این رابطه ، MD5 و Clear (بدون رمزنگاری) می باشد .

عنصر <users>

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

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

عنصر <credentialas> ، امکان ذخیره سازی لیست کاربران را در Web.Config فراهم می نماید . رویکرد فوق ، روشی ساده به منظور تعریف کاربران مجاز یک برنامه وب می باشد . در چنین مواردی ، مدیریت سیستم می تواند بسادگی و در صورت لزوم نام و رمز عبور کاربران دیگری را به لیست مجاز کاربران ، اضافه نماید . مکانیزم فوق ، در مواردی که قصد داشته باشیم ، امکان تعریف نام و رمز عبور را در اختیار کاربران قرار دهیم ، گزینه مناسبی نبوده و می بایست از یک فایل و یا بانک اطلاعاتی به منظور ذخیره سازی اطلاعات کاربران ، استفاده گردد.

استراتژی حفاظت از اطلاعات در شبکه های کامپیوتری (بخش اول)

مقدمه

اطلاعات در سازمان ها و موسسات مدرن، بمنزله شاهرگ حیاتی محسوب می گردد . دستیابی به اطلاعات و عرضه مناسب و سریع آن، همواره مورد توجه سازمان هائی است که اطلاعات در آنها دارای نقشی محوری و سرنوشت ساز است . سازمان ها و موسسات می بایست یک زیر ساخت مناسب اطلاعاتی را برای خود ایجاد و در جهت انطباق اطلاعاتی در سازمان خود حرکت نمایند . اگر می خواهیم ارائه دهنده اطلاعات در عصر اطلاعات بوده و صرفاً مصرف کننده اطلاعات نباشیم ، در مرحله نخست می بایست فرآیندهای تولید ، عرضه و استفاده از اطلاعات را در سازمان خود قانونمند نموده و در مراحل بعد ، امکان استفاده از اطلاعات ذیربط را برای متقاضیان (محلی، جهانی) در سریعترین زمان ممکن فراهم نمائیم . سرعت در تولید و عرضه اطلاعات ارزشمند ، یکی از رموز موفقیت سازمان ها و موسسات در عصر اطلاعات است . پس از ایجاد انطباق اطلاعاتی، می بایست با بهره گیری از شبکه های کامپیوتری زمینه استفاده قانونمند و هدفمند از اطلاعات را برای سایرین فراهم کرد . اطلاعات ارائه شده می تواند بصورت محلی (اینترنت) و یا جهانی (اینترنت) مورد استفاده قرار گیرد . فراموش نکنیم در این هنگامه اطلاعاتی، مصرف کنندگان اطلاعات دارای حق مسلم انتخاب می باشند و در صورتیکه سازمان و یا موسسه ای در ارائه اطلاعات سهواً و یا تعمداً دچار اختلال و یا مشکل گردد ، دلیلی بر توقف عملکرد مصرف کنندگان اطلاعات تا بر طرف نمودن مشکل ما ، وجود نخواهد داشت . سازمان ها و موسسات می بایست خود را برای نبردی سخت در عرضه و ارائه اطلاعات آماده نمایند و در این راستا علاوه بر پتانسیل های سخت افزاری و نرم افزاری استفاده شده ، از تدبیر و دوراندیشی فاصله نگیرند . در میدان عرضه و ارائه اطلاعات ، کسب موفقیت نه بدلیل ضعف دیگران بلکه بر توانمندی ما استوار خواهد بود. مصرف کنندگان اطلاعات، قطعاً ارائه دهندگان اطلاعاتی را برمی گیرند که نسبت به توان و پتانسیل آنان اطمینان حاصل کرده باشند . آیا سازمان ما در عصر اطلاعات به پتانسیل های لازم در این خصوص دست پیدا کرده است ؟ آیا در سازمان ما بستر و ساختار مناسب اطلاعاتی ایجاد شده است ؟ آیا گردش امور در سازمان ما مبتنی بر یک سیستم اطلاعاتی مدرن است ؟ آیا سازمان ما قادر به تعامل اطلاعاتی با سایر سازمان ها است ؟ آیا در سازمان ما نقاط تماس اطلاعاتی با دنیای خارج از سازمان تدوین شده است ؟ آیا فاصله تولید و استفاده از اطلاعات در سازمان ما به حداقل مقدار خود رسیده است ؟ آیا اطلاعات قابل عرضه سازمان ما ، در سریعترین زمان و با کیفیتی مناسب در اختیار مصرف کنندگان متقاضی قرار می گیرد ؟ حضور یک سازمان در عرصه جهانی ، صرفاً داشتن یک وب سایت با اطلاعات ایستا نخواهد بود . امروزه میلیون ها وب سایت بر روی اینترنت وجود داشته که هر روز نیز به تعداد آنان افزوده می گردد . کاربران اینترنت برای پذیرش سایت سازمان ما ، دلایل موجه ای را دنبال خواهند کرد . در این هنگامه سایت داشتن و راه اندازی سایت ، اصل موضوع که همانا ایجاد یک سازمان مدرن اطلاعاتی است ، فراموش نگردد. سازمان ما در این راستا چگونه حرکت کرده و مختصات آن در نقشه اطلاعاتی یک سازمان مدرن چیست ؟

بدیهی است ارائه دهندگان اطلاعات خود در سطوحی دیگر به مصرف کنندگان اطلاعات تبدیل و مصرف کنندگان اطلاعات ، در حالات دیگر، خود می تواند بعنوان ارائه دهنده اطلاعات مطرح گردند. مصرف بهینه و هدفمند اطلاعات در صورتیکه به افزایش آگاهی ، تولید و ارائه اطلاعات ختم شود، امری بسیار پسندیده خواهد بود . در غیر اینصورت، مصرف مطلق و همیشگی اطلاعات بدون جهت گیری خاص ، بدترین نوع استفاده از اطلاعات بوده که قطعاً به سرانجام مطلوبی ختم نخواهد شد .

شبکه های کامپیوتری

در صورتیکه قصد ارائه و یا حتی مصرف بهینه و سریع اطلاعات را داشته باشیم، می بایست زیر ساخت مناسب را در این جهت ایجاد کنیم . شبکه های کامپیوتری ، بستری مناسب برای عرضه ، ارائه و مصرف اطلاعات می باشند(دقیقاً مشابه نقش جاده ها در یک سیستم حمل و نقل) . عرضه ، ارائه و مصرف یک کالا نیازمند وجود یک سیستم حمل و نقل مطلوب خواهد بود. در صورتیکه سازمان و یا موسسه ای محصولی را تولید ولی قادر به عرضه آن در زمان مناسب (قبل از اتمام تاریخ مصرف) برای متقاضیان نباشد، قطعاً از سازمان ها ئی که تولیدات خود را با بهره گیری از یک زیر

ساخت مناسب ، سرعت در اختیار متقاضیان قرار می دهند ، عقب خواهند افتاد . شاید بهمین دلیل باشد که وجود جاده ها و زیر ساخت های مناسب ارتباطی، بعنوان یکی از دلایل موفقیت برخی از کشورها در عصر انقلاب صنعتی ، ذکر می گردد. فراموش نکنیم که امروزه زمان کهنه شدن اطلاعات از زمان تولید اطلاعات بسیار سریعتر بوده و می بایست قبل از اتمام تاریخ مصرف اطلاعات با استفاده از زیر ساخت مناسب (شبکه های ارتباطی) اقدام به عرضه آنان نمود. برای عرضه اطلاعات می توان از امکاناتی دیگر نیز استفاده کرد ولی قطعاً شبکه های کامپیوتری دلیل سرعت ارتباطی بسیار بالا دارای نقشی کلیدی و منحصر بفرد می باشند . مثلاً می توان مشخصات کالا و یا محصول تولید شده در یک سازمان را از طریق یک نامه به متقاضیان اعلام نمود ولی در صورتیکه سازمانی در این راستا از گزینه پست الکترونیکی استفاده نماید ، قطعاً متقاضیان مربوطه در زمانی بسیار سریعتر نسبت به مشخصات کالای تولید شده ، آگاهی پیدا خواهند کرد .

امنیت اطلاعات در شبکه های کامپیوتری

بموازات حرکت بسمت یک سازمان مدرن و مبتنی بر تکنولوژی اطلاعات، می بایست تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده گردد. مهمترین مزیت و رسالت شبکه های کامپیوتری ، اشتراک منابع سخت افزاری و نرم افزاری است . کنترل دستیابی و نحوه استفاده از منابع به اشتراک گذاشته شده ، از مهمترین اهداف یک سیستم امنیتی در شبکه است . با گسترش شبکه های کامپیوتری خصوصاً اینترنت ، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده ، وارد مرحله جدیدی شده است . در این راستا ، لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند ، پایبند به یک استراتژی خاص بوده و بر اساس آن سیستم امنیتی را اجراء و پیاده سازی نماید . عدم ایجاد سیستم مناسب امنیتی ، می تواند پیامدهای منفی و دور از انتظاری را بدنبال داشته باشد . استراتژی سازمان ما برای حفاظت و دفاع از اطلاعات چیست؟ در صورت بروز مشکل امنیتی در رابطه با اطلاعات در سازمان ، بدنبال کدامین مقصر می گردیم ؟ شاید اگر در چنین مواردی ، همه مسائل امنیتی و مشکلات بوجود آمده را به خود کامپیوتر نسبت دهیم ، بهترین امکان برون رفت از مشکل بوجود آمده است ، چراکه کامپیوتر توان دفاع کردن از خود را ندارد . آیا واقعاً" روش و نحوه برخورد با مشکل بوجود آمده چنین است ؟ در حالیکه یک سازمان برای خرید سخت افزار نگرانی های خاص خود را داشته و سعی در برطرف نمودن معقول آنها دارد ، آیا برای امنیت و حفاظت از اطلاعات نباید نگرانی بمراتب بیشتری در سازمان وجود داشته باشد ؟

استراتژی

دفاع در عمق ، عنوان یک استراتژی عملی بمنظور نیل به تضمین و ایمن سازی اطلاعات در محیط های شبکه امروزی است . استراتژی فوق ، یکی از مناسبترین و عملی ترین گزینه های موجود است که متاثر از برنامه های هوشمند برخاسته از تکنیک ها و تکنولوژی های متفاوت تدوین می گردد . استراتژی پیشنهادی ، بر سه مولفه متفاوت ظرفیت های حفاظتی ، هزینه ها و رویکردهای عملیاتی تاکید داشته و توازن معقول بین آنان را برقرار می نماید . دراین مقاله به بررسی عناصر اصلی و نقش هر یک از آنان در استراتژی پیشنهادی، پرداخته خواهد شد.

دشمنان، انگیزه ها ، انواع حملات اطلاعاتی

بمنظور دفاع موثر و مطلوب در مقابل حملات به اطلاعات و سیستم های اطلاعاتی ، یک سازمان می بایست دشمنان، پتانسیل و انگیزه های آنان و انواع حملات را بدرستی برای خود آنالیز تا از این طریق دیدگاهی منطقی نسبت به موارد فوق ایجاد و در ادامه امکان برخورد مناسب با آنان فراهم گردد . اگر قصد تجویز دارو برای بیماری وجود داشته باشد ، قطعاً" قبل از معاینه و آنالیز وضعیت بیمار، اقدام به تجویز دارو برای وی نخواهد شد. در چنین مواردی نمی توان برای برخورد با مسائل پویا از راه حل های مشابه و ایستا استفاده کرد . بمنظور ارائه راهکارهای پویا و متناسب با مسائل متغیر، لازم است در ابتدا نسبت به کالبد شکافی دشمنان ، انگیزه ها و انواع حملات ، شناخت مناسبی ایجاد گردد. دشمنان ، شامل سارقین اطلاعاتی ، مجرمان ، دزدان کامپیوتری ، شرکت های رقیب و ... می باشد. انگیزه ها ی موجود شامل : جمع آوری هوشمندانه، دستبرد فکری (عقلانی) ، عدم پذیرش سرویس ها ، کشف کردن ، احساس غرور و مورد توجه واقع شدن ، با شد .

انواع حملات شامل : مشاهده غیرفعال ارتباطات ، حملات به شبکه های فعال، حملات از نزدیک (مجاورت سیستم ها)

، سوء استفاده و بهره برداری خودیان (محرمان) و حملات مربوط به ارائه دهندگان صنعتی یکی از منابع تکنولوژی اطلاعات، است.

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

انواع حملات اطلاعاتی بشرح ذیل می باشند:

غیرفعال

فعال

نزدیک (مجاور)

خودی ها (محرمان)

عرضه (توزیع)

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

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

مجاور (Close-in). این نوع حملات توسط افرادی که در مجاورت (نزدیکی) سیستم ها قرار دارند با استفاده از تسهیلات موجود، با یک ترفندی خاص بمنظور نیل به اهدافی نظیر: اصلاح، جمع آوری و انکار دستیابی به اطلاعات باشد، صورت می پذیرد. حملات مبتنی بر مجاورت فیزیکی، از طریق ورود مخفیانه، دستیابی باز و یا هردو انجام می شود. خودی (Insider). حملات خودی ها، می تواند بصورت مخرب و یا غیر مخرب جلوه نماید. حملات مخرب از این نوع شامل استراق سمع عمدی، سرقت و یا آسیب رسانی به اطلاعات، استفاده از اطلاعات بطرز کاملاً شایدانه و قریب آمیز و یا رد دستیابی سایر کاربران تایید شده باشد. حملات غیر مخرب از این نوع، عموماً "بدلیل سهل انگاری (حواس پرتی)، فقدان دانش لازم و یا سرپیچی عمدی از سیاست های امنیتی صورت پذیرد.

توزیع (Distribution). حملات از این نوع شامل کدهای مخربی است که در زمان تغییر سخت افزار و یا نرم افزار در محل مربوطه (کارخانه، شرکت) و یا در زمان توزیع آنها (سخت افزار، نرم افزار) جلوه می نماید. این نوع حملات می تواند، کدهای مخربی را در بطن یک محصول جاسازی نماید. نظیر یک درب از عقب که امکان دستیابی غیرمجاز به اطلاعات و یا عملیات سیستم در زمان آتی را بمنظور سوء استفاده اطلاعاتی، فراهم می نماید.

در این رابطه لازم است، به سایر موارد نظیر آتس سوزی، سیل، قطع برق و خطای کاربران نیز توجه خاصی صورت پذیرد. در بخش دوم این مقاله، به بررسی روش های ایمن سازی اطلاعات بمنظور نیل به یک استراتژی خاص امنیتی، خواهیم پرداخت.

استراتژی حفاظت از اطلاعات در شبکه های کامپیوتری (بخش دوم)

در بخش اول این مقاله به چالش های سازمانها و موسسات برای حرکت بسمت یک سازمان مدرن اطلاعاتی اشاره و پس از بررسی اهمیت ایمن سازی اطلاعات بر لزوم تدوین یک استراتژی امنیتی تاکید گردید . در این زمینه به انواع حملات اطلاعاتی نیز اشاره و مشخصات هر یک از آنان توضیح داده شد . در این بخش ، به بررسی عناصر اساسی در استراتژی پیشنهادی یعنی انسان ، تکنولوژی و عملیات خواهیم پرداخت .

ایمن سازی اطلاعات

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

انسان

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

تدوین سیاست ها و رویه ها

ارائه آموزش های لازم جهت افزایش دانش

مدیریت سیستم امنیتی

امنیت فیزیکی

امنیت شخصی

تدابیر لازم در خصوص پیشگیری

تکنولوژی

امروزه از تکنولوژی های متعددی بمنظور ارائه سرویس های لازم در رابطه با ایمن سازی اطلاعات و تشخیص مزاحمین اطلاعاتی، استفاده می گردد. سازمان ها و موسسات می بایست سیاست ها و فرآیندهای لازم بمنظور استفاده از یک تکنولوژی را مشخص تا زمینه انتخاب و بکارگیری درست تکنولوژی در سازمان مربوطه فراهم گردد. در این رابطه می

بایست به مواردی همچون: سیاست امنیتی، اصول ایمن سازی اطلاعات، استانداردها و معماری ایمن سازی اطلاعات، استفاده از محصولات مربوط به ارائه دهندگان شناخته شده و خوش نام، راهنمای پیکربندی، پردازش های لازم برای ارزیابی ریسک سیستم های مجتمع و بهم مرتبط، توجه گردد. در این رابطه موارد زیر، پیشنهاد می گردد: دفاع در چندین محل. مهاجمان اطلاعاتی (داخلی و یا خارجی) ممکن است، یک هدف را از چندین نقطه مورد تهاجم قرار دهند. در این راستا لازم است سازمان ها و موسسات از روش های حفاظتی متفاوت در چندین محل (سطح) استفاده، تا زمینه عکس العمل لازم در مقابل انواع متفاوت حملات، فراهم گردد. در این رابطه می بایست به موارد زیر توجه گردد:

? دفاع از شبکه ها و زیر ساخت. در این رابطه لازم است شبکه های محلی و یا سراسری حفاظت گردند. (حفاظت در مقابل حملات اطلاعاتی از نوع عدم پذیرش خدمات)

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

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

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

دفاع لایه ای. بهترین محصولات مربوط به ایمن سازی اطلاعات دارای نقاط ضعف ذاتی، مربوط به خود می باشند. بنابراین همواره زمان لازم در اختیار مهاجمان اطلاعاتی برای نفوذ در سیستم های اطلاعاتی وجود خواهد داشت. بدین ترتیب لازم است قبل از سوءاستفاده اطلاعاتی متجاوزان، اقدامات مناسبی صورت پذیرد. یکی از روش های موثر پیشگیری در این خصوص، استفاده از دفاع لایه ای در مکان های بین مهاجمان و اهداف مورد نظر آنان، می باشد. هر یک از مکانیزم های انتخابی، می بایست قادر به ایجاد موانع لازم در ارتباط با مهاجمان اطلاعاتی (حفاظت) و تشخیص بموقع حملات باشد. بدین ترتیب امکان تشخیص مهاجمان اطلاعاتی افزایش و از طرف دیگر شانس آنها بمنظور نفوذ در سیستم و کسب موفقیت، کاهش خواهد یافت. استفاده از فایروال های تودرتو (هر فایروال در کنار خود از یک سیستم تشخیص مزاحمین، نیز استفاده می نماید) در محدوده های داخلی و خارجی شبکه، نمونه ای از رویکرد دفاع لایه ای است. فایروال های داخلی ممکن است امکانات بیشتری را در رابطه با فیلتر سازی داده ها و کنترل دستیابی به منابع موجود ارائه نمایند.

تعیین میزان اقتدار امنیتی هر یک از عناصر موجود در ایمن سازی اطلاعات (چه چیزی حفاظت شده و نحوه برخورد با تهاجم اطلاعاتی در محلی که از عنصر مربوطه استفاده شده، به چه صورت است؟). پس از سنجش میزان اقتدار امنیتی هر یک از عناصر مربوطه، می توان از آنان در جایگاهی که دارای حداکثر کارایی باشند، استفاده کرد. مثلاً می بایست از مکانیزم های امنیتی مقتدر در محدوده های مرزی شبکه استفاده گردد.

استفاده از مدیریت کلید مقتدر و زیر ساخت کلید عمومی، که قادر به حمایت از تمام تکنولوژی های مرتبط با ایمن سازی اطلاعات بوده و دارای مقاومت مطلوب در مقابل یک تهاجم اطلاعاتی باشد.

بکارگیری زیرساخت لازم بمنظور تشخیص مزاحمین، آنالیز و یکپارچگی نتایج بمنظور انجام واکنش های مناسب در رابطه با نوع تهاجم. زیر ساخت مربوطه می بایست به پرسنل عملیاتی، راهنمایی لازم در مواجهه با سوالاتی نظیر: آیا من تحت تهاجم اطلاعاتی قرار گرفته ام؟ منبع تهاجم چه کسی می باشد؟ به چه فرد دیگری تهاجم شده است؟ راه حل ها و راهکارهای من در این رابطه چیست؟، را ارائه نماید.

عملیات

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

پشتیبانی ملموس و بهنگام سازی سیاست های امنیتی

اعمال تغییرات لازم با توجه به روند تحولات مرتبط با تکنولوژی اطلاعات. در این رابطه می بایست داده های مورد نظر



جمع آوري تا زمينه تصميم سازي مناسب براي مديريت فراهم گردد (تامين اطلاعات ضروري براي مديريت ريسك) .

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 (خصوصاً زير ساخت هائي كه براي يك 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 مي رسد محكوم نمايند. اما ميوه ممنوعه وسوسه كننده است و اقداماتي كه در جهت بستن دست هكرها صورت مي گيرد، غالباً براي خود هكرها مثل مبارزه جويي و حريفطلبي است. اما در بارسلون اسپانيا با پديده هك نوع ديگري برخورد مي شود. 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 فارغ التحصيل مي كند، متولي تشكيل <دبيرستان هك> نيز شده است. هدف از اين طرح، برخلاف آن چه كه در ابتدای امر به ذهن مي رسد، راه اندازي يك <كارگاه شيطاني> نبوده، بلكه هدف آگاه سازي و آشنا كردن جوانان با يك تابو مدرن امروزي، يعني پديده هك است. به گفته پت هرتزوك، مدير اجرايي دبيرستان: <هك چيزي است كه در دنياي واقعي وجود دارد و نمي توان آن را كتمان كرد. اما هيچ كس نيامده بگويد اين هك واقعاً چگونه است. همه مي گويند صندوق پستي شما ممكن است با كرم آلوده شود، يك نفر ممكن است تروجاني را به كامپيوتر شما وارد كند يا مي آيند و اطلاعات شما را مي دزدند. ولي هيچ كس تا به حال ياد نداده كه اين كارها را چگونه انجام مي دهند. همه صرفاً مي گويند اين كار غيرقانوني است و هر كس از اين كارها بكنند آدم بد است.>

اين برنامه از طرف ISECOM، مؤسسه امنيت و متدولوژي هاي باز (نشاني www.isecom.org) تنظيم شده است، يك مؤسسه غيرانتفاعي كه سعي دارد جوانان را با ناهنجارهاي اينترنتي و بدآموزي هايي كه از طرف نااهلان ترويج مي شود آشنا كند. دانش آموزان به نوعي يك دوره دفاع شخصي ديجيتالي مي بينند و ياد مي گيرند با كلاهبرداري هاي اينترنتي چگونه برخورد كنند، دزدان را چگونه تشخيص دهند و در مقابل حملاتي كه به سيستمشان مي شود چگونه به دفاع بپردازند. پت هرتزوك ادامه مي دهد: <ما به بچه ها نشان مي دهيم كه اين كارهاي غيرقانوني چگونه انجام مي شود و چه اتفاقي در سيستم مي افتد. با اين كار، آنها يك درك فني از موضوع به دست مي آورند و مي فهمند كه چگونه با حملات مقابل كنند.>

يكي از معلمين اين مدرسه مي گويد: <دانش آموز بايد ياد بگيرد كه وقتي نامه اي دريافت مي كند 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 مي بينند زود باور نكنند.>

بديهي است كه براي ياد دادن اين مسائل، به سيستم هاي واقعي نفوذ نمي كنند، بلكه مسئولين ISECOM براي آموزش و آزايش دانش آموزان، چهار سرور آزمايشي تهيه كرده اند كه دانش آموزان 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 هك‌رهي با اخلاقي بسازيم كه توانايي‌هاي خود را مي‌دانند و حدود خود را هم مي‌دانند.

مسئولين مدرسه معتقدند كه براي اين هك‌رهي با اخلاق شغل در بازار بيرون فراوان پيدا مي‌شود، چرا كه يكي از پرونق‌ترين مشاغل در صنعت كامپيوتر همين مشاغل حوزه امنيت است.

• متجاوزين فضاى ساير

در علم حقوق معروف است كه مي‌گويند: اگر ۹۰ درصد چيزي را تصاحب كني، قانوناً مالك آن هستي. اما به نظر مي‌رسد در فضاى ساير 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 ايل 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 فضاى ساير> 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 ميليون <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 ايل وجود نداشت. اين اظهارات بن كوهن بود. يك سال بعد، شركت بزرگ كامپيوتر ايل iPod، را خلق كرد، و دو سال بعد از آن، در سال ۲۰۰۳، يك وب‌سايت براي دانلود موسيقي به نام iTunes را افتتاح كرد. ايل خيلي زود توانست از طريق اين سايت هزاران آهنگ را در هر روز به فروش برساند. ايل 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>.

ايل عقب نشست و شكايتهاي 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 ميانجيجري Nominet و به طور رايگان رفع مي‌شوند، اما بعضي از آنها كه جدي‌تر هستند (مثل همين مورد ايل) 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 شكايتهاي حقوقي مي‌كشد>.

ايل حتي به دنبال اين نبوده كه از طريق آدرس انگليسي iTunes به فروش بيشتري برسد، چرا كه كوهن پس از مدت کوتاهی، 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 ايل

زمانی واقعاً نگران شد که کوهن بازديدکنندگان سایت خود را به Napster هدایت کرد، یعنی رقیب اپل. اما وقتی اپل از کوهن خواست که لینک سایتش را از Napster قطع کند، کوهن پذیرفت و این کار را کرد. بعد کوهن به سراغ Napster رفت و پیشنهاد فروش سایتش را به آن‌ها داد: <ما به این علت این پیشنهاد را به Napster دادیم که فکر می‌کردیم یک شرکت فعال در زمینه موسیقی به موتور جستجوی سایت ما علاقه‌مند باشد. درست است که ما از فروش این سایت به رقیب اپل سود می‌بردیم، ولی این کار که غیرقانونی نیست>.

اما Nominet نظر دیگری دارد: <نام دامنه که مثل ملک و اتومبیل نیست که از یک دست بخری و از دست دیگر بفروشی. دامنه را می‌گیری تا از آن استفاده کنی. ثبت هر دامنه‌ای یک سری الزامات را به دنبال دارد که باید رعایت شوند>.

ماه گذشته، کارشناس مستقل حقوقی Nominet تشخیص داد که iTunes.co.uk باید به اپل سپرده شود. اما بن کوهن، اولین نوجوان میلیونر دات‌کام، نه تنها قصد دارد شکایتی را از اپل به دادگاه عالی ببرد، بلکه می‌خواهد از Nominet سؤال کند که به چه حقی چنین کاری کرده است. Nominet معتقد است که تصمیمش قانونی و منصفانه است و هفته گذشته کنترل این نام را به اپل داد. در حال حاضر، اپل از این آدرس برای عرضه و نمایش iPod و iTunes بهره می‌گیرد.

معرفی نرم‌افزار: Security Task Manager

اشاره :

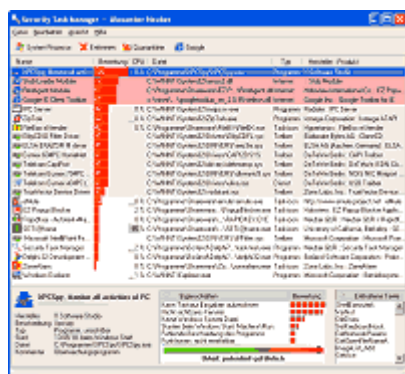
آیا تا به حال برای شما پیش آمده است که به برخی از برنامه‌های مقیم در حافظه کامپیوترتان مشکوک شوید و بخواهید بدانید آیا این برنامه‌ها کار غیر مجازی انجام می‌دهند یا نه؟

اگر کاربر سیستم‌عامل ویندوز باشید و هشدارهایی پی در پی که این روزها نسبت به اهمیت ایمن کردن کامپیوترها منتشر می‌شود را جدی گرفته باشید، احتمالاً برای شما پیش آمده مواقعی که نسبت به هویت یک برنامه بارگذاری شده در حافظه سیستم مشکوک می‌شوید.

احتمالاً پنجره Task Manager ویندوز را باز کرده‌اید و در آنجا اسامی چند فایل DLL و EXE را دیده‌اید که معلوم نیست برخی از آنها واقعاً متعلق به کدام برنامه‌اند و چه می‌کنند.

در این مواقع خیلی مایلید بدانید کدام یک از این برنامه‌ها مشکوک هستند و دست‌کم می‌خواهید محل فیزیکی آنها روی هارد دیسک را بدانید تا شاید با مراجعه به پوشه‌ای که دربرگیرنده آن فایل است، بتوانید هویت برنامه را معلوم کنید.

نرم‌افزار Security Task Manager برنامه ساده و مفیدی برای پاسخ دادن به همین سوالات است. پس از نصب و اجرای این نرم‌افزار می‌توانید فهرستی از برنامه‌های مقیم در حافظه، یعنی همانهایی که در پنجره Task Manager ویندوز دیده می‌شوند را مشاهده کنید. این فهرست به ترتیب میزان مشکوک بودن این برنامه‌ها از دیدگاه Security Task Manager (STM) مرتب شده است و با کلیک روی نام هر برنامه می‌توانید تمام اطلاعاتی که STM درباره آن فایل جمع آوری کرده است را ببینید. اگر STM نتواند اطلاعات چندانی درباره آن برنامه بدست آورد، با اختصاص یک نوار قرمز رنگ که طول آن بیانگر درصد مشکوک بودن STM به آن فایل است، نظر خود را در این باره نشان می‌دهد.



خوشبختانه بسیاری از فایل‌هایی که در ردیف فایل‌های مشکوک قرار می‌گیرند، توسط اطلاعاتی که خود برنامه جمع‌آوری کرده است قابل تشخیص هستند. مثلاً اگر یک برنامه متعلق به شرکت سیمانتک بود، می‌توانید نتیجه بگیرید که خطری از ناحیه آن متوجه کامپیوتر شما نیست زیرا احتمالاً بخشی از برنامه امنیتی نورتون است. ولی برخی از فایل‌ها هستند که در صدر لیست برنامه‌های مظنون قرار گرفته‌اند و هویت درست و حسابی هم ندارند. در این صورت برای مشخصی کردن هویت آنها می‌توانید با رایت کلیک روی نام آن برنامه، گزینه Google It را از منویی که باز می‌شود انتخاب کنید و ببینید آیا می‌توانید اطلاعاتی درباره آن فایل در اینترنت بیابید یا نه. در اینصورت ابتدا برنامه می‌کوشد صفحه‌ای هم نام فایل مذکور در بانک اطلاعاتی مربوط به سایت شرکت سازنده STM بیابد، در غیر اینصورت می‌توانید به کمک موتور جستجوی گوگل تحقیق کنید و مطمئن باشید که اگر آن فایل مثلاً یک اسب تروا یا نرم‌افزار غیر مجاز شناخته شده در اینترنت باشد، حتماً اطلاعات سودمندی درباره آن پیدا خواهید کرد که شما را برای تصمیم‌گیری نسبت به حذف آن فایل یا باقی نگه‌داشتن آن یاری خواهد کرد.

اگر گزینه Remove را از منوی مذکور انتخاب کنید، می‌توانید موقتاً یک برنامه مشکوک را از حافظه خارج کنید و یا آنرا برای همیشه در قرنطینه (پوشه مخصوصی که یک نسخه پشتیبانی از این فایل در آنجا ذخیره می‌شود) نگه دارید و آن را پوشه فعلی دربرگیرنده آن حذف کنید.

سازندگان این برنامه ادعا می‌کنند که شرکت مایکروسافت از آن برای آزمایش امن بودن ویندوز لانگ هورن (ویستا) استفاده کرده است و شرکت‌های سازنده آنتی ویروس آن را برای یافتن انواع جدید اسب تروا به کار می‌گیرند. اگر مبنای این ادعا را اطلاعات اندک اما مفیدی قرار دهیم که این برنامه درباره هر فایل مقیم در حافظه می‌دهد، ممکن است آن را باور کنیم.

شما هم می‌توانید STM را امتحان کنید. نسخه Shareware این نرم‌افزار سودمند از این [نشانی](#) قابل دریافت است.



نفوذ در يك چشم برهم زدن

سارقان اطلاعات چگونه ممکن است بتوانند از دیواره آتش شما عبور کرده و صدها مگابایت اطلاعات را به سرقت ببرند بدون این که هیچ ردیایی از خود به جای بگذارند؟ يك راه ممکن، از طریق همین درایوهای کوچک USB است که امروزه من و شما در جیب خود می‌گذاریم و به هر جایی می‌بریم. همان طور که می‌دانید، به این درایوها Flash Disk و Flash Drive هم می‌گویند، اما اسمشان هرچه که باشد، بسیاری از شرکت‌ها و سازمان‌ها هیچ سیاست مشخصی برای شناسایی این درایوها و قاعده‌مند کردن موارد استفاده آنها وضع نکرده‌اند. به همین جهت يك مشتري که به ملاقات شما آمده، کارشناسی که سیستم‌تان را چک می‌کند، همکاری که هر روز به شما سر می‌زند، یا هر فرد باهوش دیگری، به آسانی می‌تواند فلش دیسک خود را در اولین فرصت به پورت USB کامپیوتر شما وصل کرده و صدها فایل اطلاعاتی مهم را با سرعت بالای USB 2.0 برای خود کپی کند. ظرفیت فلش دیسک‌های امروزی از مرز دو گیگابایت گذشته است و همچنان رو به بالا در حرکت است و با ابعاد کوچکی که دارند، خیلی راحت می‌توان آنها را پنهان کرد. پس چاره چیست؟



سرقت اطلاعات تنها تهدید از جانب این وسیله کوچک نیست. از آنجا که کاربران فلش دیسک عمده‌تاً به خاطر قابل حمل بودن آن، به استفاده از این وسیله روی

آورده‌اند، بنابراین در حال سفر یا مأموریت نیز از آن استفاده می‌کنند و زمانی که به اداره برمی‌گردند، بدون توجه به احتمال ویروسی بودن فایل‌ها، فلش دیسک را به کامپیوتر خود وصل و سیستم را آلوده می‌کنند. نفوذگران می‌توانند انواع ابزارهای تخصصی خود را به این وسیله منتقل کنند، از جمله جاسوس‌افزارها، رمزشکن‌ها، کلیدنگارها، و پورت‌خوان‌ها، که برای شروع نفوذ به یک سیستم اساسی‌ترین ابزار نفوذگر محسوب می‌شوند. بعد از این کار، نفوذگر به شیوه‌های گوناگون مهندسی اجتماعی، سعی می‌کند به اتاق‌تان راه یافته یا به کامپیوترتان دست پیدا کند، تا از طریق درایو USB به اعمال شیطانی خود بپردازد. گذشته از اینها، در صورت مفقود شدن فلش دیسک، تمام فایل‌های موجود در آن به دست کسی می‌افتد که آن را پیدا کرده و این می‌تواند برای کل سازمان خطرناک باشد. چگونه می‌توان از شبکه سازمان در مقابل این تهدید محافظت کرد؟ اولین قدم، آموزش دادن به پرسنل است. ابتدا در مجموعه سیاست‌های امنیتی سازمان، استفاده صحیح و ناصحیح از درایوهای USB را تشریح کرده و لزوم داشتن مجوز برای استفاده از فلش دیسک را توضیح دهید. سپس این موارد را به پرسنل خود آموزش داده و دلایل وجودی هر کدام را برایشان بازگو کنید.

قدم بعدی این است که کامپیوترها را طوری تنظیم کنید که در صورت بی‌کار ماندن، بعد از ۳ تا ۵ دقیقه (یا هر مدتی که خودتان صلاح می‌دانید) به طور خودکار قفل شوند. در ویندوز اکس‌پی آسان‌ترین راه برای این کار، استفاده از screen saver است. نرم‌افزارهای جانبی زیادی نیز وجود دارند که از جمله می‌توان به Desktop Lock محصول شرکت نرم‌افزاری PC Lockup، TopLang Software، SpyLock، Ixis محصول Spytech Software و StayOut محصول Tomorrowware اشاره کرد.

قدم دیگر این است که برای پرسنل مورد نظر خود، USB درایوهای مطمئنی را تهیه کنید. به عنوان مثال، Lexar Media JumpDrive Secure یک فلش‌درایو USB است که به صورت توکار با رمزعبور محافظت می‌شود. شرکت SanDisk نرم‌افزاری به نام CruzerLock را همراه با فلش‌درایوهای خود عرضه می‌کند که امکان گذاشتن کلمه عبور و رمز کردن فایل‌ها را به شما می‌دهد. حتی بعضی شرکت‌ها محصولات می‌دارند که فقط با اثر انگشت صاحب اصلی کار می‌کنند.

نکته دیگر این است که نرم‌افزار ویروس‌یاب خود را طوری تنظیم کنید که تمام درایوها و ابزارهای جابه‌جا شدنی را در هنگام اسکن در نظر بگیرد. به کاربران یاد بدهید که قبل از کپی کردن چیزی به کامپیوتر خود، ابتدا مطمئن شوند اسکن حتماً انجام گرفته یا خودشان به طور دستی به اسکن فلش دیسک بپردازند.

حتی برای تضمین امنیت بیشتر، می‌توانید پورت‌های USB را غیرفعال کنید. این یکی شاید زیادی امنیتی باشد، ولی اگر لازم است می‌توانید حتی از طریق رمزعبور BIOS کامپیوترها را قفل کنید. اما اگر به دنبال یک شیوه حفاظتی حرفه‌ای هستید، راه‌حل SecureNT محصول SecureWave را پیش بگیرید، که اجازه می‌دهد دسترسی کاربران نهایی به بعضی قطعات ورودی-خروجی (از جمله پورت‌های USB) را تحت کنترل خود درآورید. با استفاده از این نرم‌افزار حتی می‌توانید فهرستی از قطعات مورد تأیید را ایجاد کنید تا دسترسی به هر وسیله‌ای خارج از این فهرست ممنوع شود. همچنین می‌توانید بر موارد استفاده تمام این وسایل نظارت داشته باشید.

👉 نکته آخر این که، به تمام کاربران بگویید یک فایل متنی حاوی اسم و نشانی خود روی فلش دیسک درست کنند تا در صورت مفقود شدن آن، یابنده بتواند آنها را پیدا کند. منتها دقت کنید که خود این فایل نباید رمز شده باشد.

یکی از استدلال‌هایی که طرفداران جنبش این‌سورس در حمایت از این حرکت مطرح می‌کنند (اگر بخواهیم خیلی کلی و خودمانی بگوییم) این است که می‌گویند شرکت‌های closedsource، که معروف‌ترین‌شان مایکروسافت است، در اشتباهند که فکر می‌کنند در دسترس نبودن سورس کد برنامه‌های آنها امنیت محصولات‌شان را بالاتر می‌برد.



مدافعان این سورس با تحقیر چنین طرز فکری آن را تأمین < امنیت از طریق ابهام security through obscurity > می نامند و تأکید دارند که اشکالات و حفره های موجود در محصولات، خواهی نخواهی بر ملا می شوند و در مقابل این استدلال کاملاً متضاد را می آورند که محصولات این سورس اتفاقاً امنیت بیشتری خواهند داشت، چرا که هر کس می تواند به معاینه آن ها پرداخته و اشکالات آن را برطرف کند.

چنین نظریه ای تا چه اندازه می تواند صحیح باشد؟ به زودی خواهیم فهمید، چرا که قسمت هایی از سورس ویندوز NT4 و 2000 به اینترنت نشت کرده است.

پیش بینی شده است که انتشار این کد موجب افزایش حملات به ویندوز خواهد شد. اگر این پیش بینی درست از آب در بیاید، پس باید قبول کنیم که امنیت با ابهام تأمین می شود. اگر با پنهان کردن چیزی امنیت آن بیشتر نمی شود، پس با آشکار کردن آن نباید امنیتش کمتر شود.

توجه داشته باشید که بحث ما بر سر کد دو محصولی است که سال ها از عمرشان می گذرد. سورس NT4 مربوط به سرویس پک ۳ ان تی است، که IIS نداشت و IE آن هم ۴ بود. کد ویندوز ۲۰۰۰ هم زیرمجموعه بسیار کوچکی از سرویس پک ۱ ویندوز ۲۰۰۰ است که شامل IE5، SNMP، PKI و یک سری کد SDK می شود. بعید است که افشا شدن این کدها خطر جدید آنچنان مهمی برای ویندوزهای جدید باشد. با آن همه شلوغ کاری هایی که برای نوشتن یک برنامه در آن زمان ها مجبور بودیم انجام دهیم، بعید است کسی حاضر شود که میان ۵۵ هزار فایل به جستجو بپردازد تا حفره یا راه نفوذی پیدا کند.

اولاً کسی که سیستمی با این نسخه های ویندوز داشته باشد، خود به خود در معرض خطر حمله به نقطه ضعف های شناخته شده ای قرار داد که قبل از افشا این سورس ها کشف شده بودند. پس غیرمنطقی نیست که فرض کنیم کسی از این سورس ها سوءاستفاده نخواهد کرد. ثانیاً مگر چه مقدار از کد ویندوز امروز با کد ویندوزهای نامبرده مشترک است؟ به عبارت دیگر، چه میزان از حملات امروز می تواند بر اساس سورس های ۳ یا ۴ سال گذشته پایه ریزی شده باشد؟ اگر این میزان زیاد باشد، پس باز هم باید قبول کنیم در ابهام است که امنیت بهتر حفظ می شود. نفوذگران کلاه سیاه و کلاه سفید سال ها توان خود را برای شکستن این کدها صرف کردند و حالا اگر حمله قابل ملاحظه ای با افشای این کدها صورت بگیرد، پس باید بپذیریم که سورس ها مهم بوده اند.

اگر به فهرست مؤسساتی که مجوز سورس کد ویندوز را دارند نگاه کنید) در این نشانی (تعجب می کنید که پس چرا درز کردن سورس های ویندوز این همه طول کشیده است. ولی با توجه به توافق نامه هایی که مایکروسافت امضاء آن ها را هنگام ارائه مجوز از خریداران می گیرد و یک سری الزامات قانونی دیگر، معلوم است که چرا چنین اتفاقاتی زود به زود رخ نمی دهند.

تحلیلگر دیگری در این رابطه معتقد است که این حادثه همان قدر بی اهمیت است که مثلاً یک ژنرال روسی جنگ جهانی دوم را امروز دستگیر کنیم. البته این حرف شاید خیلی اغراق آمیز باشد، ولی به هر ترتیب نشان دهنده این واقعیت است که کد افشا شده تا حدود زیادی منسوخ شده است.

در مجموع، تمام حرف و حدیث هایی که بعد از افشا شدن این کدها درباره افزایش احتمالی حملات به ویندوز در گوشه و کنار نقل می شوند (صرف نظر از صحت و سقم آن ها) نشان می دهند که مردود دانستن استدلال امنیت از طریق ابهام زیاد هم آسان نیست. به هر ترتیب، در این رابطه حد میانی وجود ندارد؛ بسته بودن کد یا موجب امنیت بیشتر می شود یا نمی شود. باید صبر کنیم ببینیم در آینده چه اتفاقی می افتد.

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 کوچکتر است . 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. مثلاً 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 به یکدیگر 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. کامپیوترهایی در شبکه که

برای سایر کامپیوترها سرویس ها و خدماتی را ارائه می نمایند ، سرویس دهنده نامیده می گردند. کامپیوترهایی 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 ، مستقیماً 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. مثلاً "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 :

RING §

STAR §

BUS §

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 صرفاً از یک کابل برای انتقال اطلاعات استفاده می شود.

- توسعه آسان . یک کامپیوتر جدید را می توان راحتی 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 توپولوژی 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 معمولاً 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 ذاتاً 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 تأثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت .

- کنترل مرکزی و عیب یابی . با توجه به این مسئله که نقطه مرکزی مستقیماً 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 پشتیبانی 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 زمانی که 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 از شبکه از یک نوع کابل بعنوان محیط انتقال استفاده کرد . مثلاً در محیط های اداری از مدل های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

- 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 خطا 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 هایی آسانتر برای عیب یابی شبکه ها

راهنمای عیب یابی اولین چیزی که باعث می شود تکنسین شبکه بتواند ایراد احتمالی را تشخیص دهد ، بررسی این موضوع است که پیش از این شبکه در چه شرایطی به طور صحیح کار می کرده است . شناخت آن شرایط باعث تشخیص آسانتر عامل پدید آورنده خطا می گردد . اما متأسفانه بعضی از تجهیزات شبکه فاقد داده های فنی لازم برای رفع عیب یا مستنداتی برای آگاهی یافتن از شرایط کارکرد صحیح آن ها هستند و متخصصان هنگامی در کار با آن ها موفق هستند که نمونه های مختلفی از آن ها را دیده ، نصب کرده و با شرایط کارکرد آن ها آشنا باشند . اما همان متخصصان هم ممکن است فراموش کنند که کدام یک از دستگاه ها ، در کدام شرایط بهتر عمل می کردند یا کدام پیکر بندی برای کدام محیط مناسب تر بوده است . برای آنکه فاصله بین تکنسین های مختلف با یکدیگر کمتر شود و راه یافتن خطا ها کوتاه تر گردد ، رعایت نچ نکته ضروری است . این موارد را می توان پنج گام برای کسب موفقیت در کشف خطا نام گذاشت .

گام اول : مستند سازی شبکه

در دست داشتن آخرین نقشه های فیزیکی و منطقی شبکه ، کمک شایانی به شناخت وضعیت فعلی شبکه می نماید . با این نقشه ها می توان ادوات مختلف ، پیکر بندی ها ، و آدرس ها را تحت نظارت داشت . ضمن آنکه از این طریق کار عیب یابی آسانتر می گردد.

گام دوم : جمع آوری کلیه اطلاعات و تحلیل خطای پیش آمده

فرض کنید که اشکال کار می دانید ، آیا می توانید آن را مستند کنید ؟ آیا قبل از بروز خطا ، هشداري از ایستگاه های کاری صادر نشده است ؟ برای این که این مرحله را ساده تر کنی . می توانید از دستگاه LinkRunner، محصول شرکت Fluke Networks استفاده کنید . این ابزار که به سادگی قابل حمل است می تواند اشکالات اولیه در لایه فیزیکی را نشان دهد . این ابزار می تواند در خدمت تکنسین ها باشد تا در صورتی که اشکال شبکه ، فراتر از اشکالات معمولی بود ، از متخصصان مجرب تری استفاده گردد. پس در گام دوم ، با استفاده از ابزارهای کمکی به جمع آوری کلیه اطلاعات موجود می پردازیم و اشکالات لایه فیزیکی را بررسی می نماییم .

گام سوم : دامنه مشکل ایجاد شده را محدود کنید

قدم بعدی محدود کردن دامنه مشکل ایجاد شده است . باید بررسی کنیم که مشکل مربوط به بخشی از شبکه است یا فقط به یک کانیت محدود است ؟ مثلاً اگر مشکل مربوط به کلانیت است پس به کابل فیزیکی یا ایستگاه کاری محدود می گردد. یعنی پس از جمع آوری اطلاعات، باید آن را به مشکل پیش آمده محدود نماییم .

گام چهارم : مشکل را رفع کنید

پس از محدود کردن دامنه مشکل ، رفع آن آسان خواهد شد . در مورد ادوات سخت افزاری ، معمولاً باید آن را تعویض نمود . مثلاً تعویض Patch Cable یا تغییر پورت سوئیچ یا تعویض کارت شبکه کلانیت . این گام وقتی تکمیل می شود که پس از رفع عیب ، شبکه مجدداً تست شود تا ازرفع کامل اشکال اطمینان حاصل گردد.

گام پنجم : کارهای انجام نشده را مستند کنید

حالا باید مجدداً گام اول را تکرار کنید . یعنی مشکل پیش آمده و نحوه رفع آن را مستند سازی کنید . این کاربر برای مراجعات بعدی بسیار مفید خواهد بود .

اما آیا انجام این دادن همه این مراحل لازم است ؟

گاهی پیش می آید که مشکلات شبکه ، ناشی از اشکالات سیستم عامل است . غلب تکنسین هایی که در واحدهای فنی مستقر هستند ، هنگام انجام راهنمایی تلفنی ، به کاربران می گویند که «یک بار کامپیوترتان را بوت کنید .» این راه حل ، در بعضی موارد مشکل را مرتفع می کند و دیگر نیاز به طی کردن گام های پنج گانه نیست . حسن این کاردر این است که تکنسین بدون این که محل کارش را ترک کند ، مشکل را برطرف نموده است . اما بعضی مشکلات با بوت کردن ساده از بین نمی روند . در این موقع ، در صورتی که کاربر کامپیوتر بتواند از خط فرمان (Command Prompt) سیستم عامل استفاده نماید ، راهنمایی تلفنی را همچنان می توان ادامه داد . یعنی فرمان IPCONFIG می تواند وجود اتصال فیزیکی را بررسی نماید .

مثلاً وقتی PC برای پروتکل DHCP پیکر بندی شده اما آدرس پیش فرض ویندوز (X.X.۱۶۹,۲۵۴) را بر می گرداند ، مشخص می شود که کلانیت نمی تواند با سرور DHCP ارتباط برقرار کند .

یا وقتی یک کامپیوتر پرتابل را به شبکه متصل می کنیم ، بایستی آدرس همان شبکه را داشته باشد . اما آگاهی اوقات DHCP ارتباط برقرار کند .

یا وقتی یک کامپیوتر پرتابل را به شبکه متصل می کنیم ، بایستی آدرس همان شبکه را داشته باشد . اما گاهی گاهی اوقات DHCP ، آدرس subnet دیگری را به آن اختصاص می دهد . اکنون کاربر می تواند دستور C:\ipconfig/release و C:\ipconfig/renew را وارد می نماید. یعنی می خواهد که آدرس IP جدیدی داشته باشد . اگر سیستم پاسخ دهد که انجام عمل DHCP میسر نیست . آن گاه این احتمال وجود دارد که کاربر از پیکر بندی IP استاتیک استفاده کرده باشد . در این حالت جهت بررسی صحت گزارش ، باید به مستندات شبکه مراجعه نمود .

در حالتی دیگر ، اگر کاربر یک آدرس IP را اعلام کند ، باید از طریق ping کردن ، آن بررسی نمود . اگر PC کاربر ، پاسخ مناسب می دهد ، یعنی آن که انجام فعالیت های متداول نظیر باز کردن صفحه وب انجام پذیر است . در غیراین صورت بایستی کامپیوتر را از نزدیک مورد بررسی قرارداد.

بررسی مشکل به صورت حضوری

پس از حضور در محل کاربر ، کار جمع آوری اطلاعات شروع می شود . سؤال اول این است که انجام کدام عمل باعث بروز مشکل شده است . گاهی اوقات پاسخ این سؤال ، چندان روشنگر نیست . زیرا کاربر می گوید که وی کار خاصی انجام نداده است و همه کارها صورت گرفته در حد کارهای معمولی روزانه بوده است یا آن که دقیقاً می داند چه اتفاقی افتاده ولی ترجیح می دهد درباره آن توضیحی ندهد ، یا مسئولیت انجام آن را بر عهده نگیرد . در این مواقع باید کاربر را مطمئن سازید که توضیح درباره بروز مشکل به رفع سریع آن کمک خواهد کرد . به غیر از این ها از انجام تغییرات محلی نیز سؤال کنید . مثلاً این که به تازگی دکوراسیون اتاق محل کار تغییر کرده است یا یک برنامه محافظ نمایش جدید نصب شده است یا مواردی از این دست .

بعد از آن که تا حد ممکن دانسته هایتان را افزایش دادید ، مواردی که تلفنی به کاربر گفتید را مجدداً خودتان آزمایش کنید . اگر عمل ping به سرور شبکه به درستی انجام می شود یا ادوات شبکه به درستی پاسخ می دهند ، نشان دهنده آن است که ایستگاه کاری در لایه ۳ ، به درستی به شبکه متصل است و در نتیجه به انجام تست در لایه های پایین تر نیازی نیست . پس باید توجه را به لایه های بالایی شبکه معطوف نمود . اگر این قسمت درست جواب ندهد یعنی این که باید به سراغ لایه های پایین تر رفت . حالا باید از یک لایه شروع کنید . اگر اتصال شبکه قطع باشد ، دستور ping این موضوع را به خوبی نشان می دهد . برای دیدن زمان پاسخ (response Time) ، دستور زیر استفاده می شود : C:\ping-t x x x x

نتیجه حاصله را می توان با استفاده از TERACERT و PATHPING برای بررسی مسیر ها به سمت device مورد نظر تحلیل نموده است .

route Trace نمودن به شما می گوید که چگونه در طول مسیر شبکه ، پکت ممکن است از بین برود . یعنی رفع عیب

لايه يك شبکه 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 آزمون ديگر را نيز انجام داد .

پس از اطمینان از این که ، وارد نشدن کاربر به شبکه در اثر جابه جایی کابل یا جدا شدن کابل و اتصالات آن نمی باشد ، به این نتیجه می رسید که مشکل پیش آمده ، پیچیده تر از اشکالات معمولی شبکه ها است . در این جا داشتن ابزاری مانند LinkRunner می تواند به سرعت به کشف اشکالات کمک کند .

آزمون های مستقیم

۱. تست لینک

۲. بررسی فعالیت Segmentها

۳. استفاده از DHCP به عنوان ابزار تشخیص

۴. انجام ping به صورت محلی و راه دور

تست لینک

بعضی از تکنسین های شبکه معتقد ند که روشن بودن چراغ (LED) روی کارت شبکه نشان دهنده برقرار بودن لینک است . اما این مساله در مورد تجهیزات مختلف ، معانی متفاوتی دارد . در بعضی تجهیزات ، چراغ های لینک (Link LED) توسط نرم افزارهای مستقر در سیستم میزبان کنترل می شوند و وقتی روشن می شوند که لایه های بالایی شبکه مشغول فعالیت باشند . بعضی کارت های شبکه چراغ لینک را وقتی روشن می کنند که ترافیک روی شبکه جریان باشد . در نتیجه روشن بودن LED ، دلیل محکمی بر سالم بودن یا سالم نبودن لینک ارتباطی نیست . حتی بعضی از تجهیزات از LEDها برای نشان دادن یک طرفه یا دو طرفه بودن ارتباط (half or full Dplx) یا نشان دادن سرعت ارتباط (۱۰/۰۰) استفاده می کنند .

برقراری لینک از طریق انجام روندی به نام Negotiation-Auto انجام می شود که در طی آن ، طرف لینک اطلاعاتی را با یکدیگر تبادل می کنند . این اطلاعات شامل سرعت ارتباط یا یک طرفه / دو طرفه بودن آن می شود . در حین این تبادل ، دو طرف ارتباط قابلیت های یکدیگر را مقایسه می کنند و سعی می کنند ارتباط را بالاترین سرعت ممکن برقرار نمایند . اگر یکی از طرفین ارتباط نتواند به درستی خود را پیکر بندی کند یا درایو های مورد نیاز نداشته باشند . این ارتباط نمی تواند ادامه پیدا کند . آن گاه یا روند فوق مجدداً تکرار می گردد و یا ارتباط به کلی قطع می گردد.

وقتی ارتباط در یک شبکه قطع شده است . Link Runner سعی می کند ابتدا ارتباط خودش را با هر یک از طرفین لینک برقرار سازد . مثلاً خودش را به کارت شبکه یا سوئیچ (دو طرف یک ارتباط) متصل می کند . سپس روند Auto.Negotiation را با استفاده از استاندارد IEEE 802.3 آغاز می کند . این ارتباط در سطح سخت افزار خواهد بود و توسط نرم افزار کنترل نخواهد شد . پس از انجام این کار ، چراغ سبز رنگ LinkRunner روشن می شود و سرعت و نوع ارتباط (یک طرفه / دو طرفه) روی صفحه نمایش دستگاه نشان داده می شود.

آموزش راه اندازی شبکه خصوصی مجازی (VPN)

شبکه خصوصی مجازی یا (Virtual Private Network) VPN در اذهان تصور یک مطلب پیچیده برای استفاده و پیاده کنندگان آن به وجود آورده است . اما این پیچیدگی ، در مطالب بنیادین و مفهومی آن است نه در پیاده سازی . این نکته را باید بدانید که پیاده سازی VPN دارای روش خاصی نبوده و هر سخت افزار و نرم افزاری روش پیاده سازی خود را داراست و نمی توان روش استاندارد را برای کلیه موارد بیان نمود . اما اصول کار همگی به یک روش است .

مختصری درباره تئوری VPN

مفهوم اصلی VPN چیزی جز برقراری یک کانال ارتباطی خصوصی برای دسترسی کاربران راه دور به منابع شبکه

نیست . در این کانال که بین دو نقطه برقرار می‌شود ، ممکن است که مسیرهای مختلفی عبور کند اما کسی قادر به وارد شدن به این شبکه خصوصی شما نخواهد بود . گرچه می‌توان از VPN در هر جایی استفاده نمود اما استفاده آن در خطوط Dialup و Leased کار غیر ضروری است (در ادامه به دلیل آن پی خواهید برد). در یک ارتباط VPN شبکه یا شبکه‌ها می‌توانند به هم متصل شوند و از این طریق کاربران از راه دور به شبکه به راحتی دسترسی پیدا می‌کنند. اگر این روش از ارائه دسترسی کاربران از راه دور را با روش خطوط اختصاصی فیزیکی (Leased) مقایسه کنیم ، می‌بینید که ارائه یک ارتباط خصوصی از روی اینترنت به مراتب از هر روش دیگری ارزان‌تر تمام می‌شود .

از اصول دیگری که در یک شبکه VPN در نظر گرفته شده بحث امنیت انتقال اطلاعات در این کانال مجازی می‌باشد . یک ارتباط VPN می‌تواند بین یک ایستگاه کاری و یک شبکه محلی و یا بین دو شبکه محلی صورت گیرد. در بین هر دو نقطه یک تونل ارتباطی برقرار می‌گردد و اطلاعات انتقال یافته در این کانال به صورت کد شده حرکت می‌کنند ، بنابراین حتی در صورت دسترسی مزاحمان و هکرها به این شبکه خصوصی نمی‌توانند به اطلاعات رد و بدل شده در آن دسترسی پیدا کنند.

جهت برقراری یک ارتباط VPN ، می‌توان به کمک نرم‌افزار یا سخت‌افزار و یا ترکیب هر دو ، آن را پیاده‌سازی نمود . به طور مثال اکثر دیوارهای آتش تجاری و روترها از VPN پشتیبانی می‌کنند . در زمینه نرم‌افزاری نیز از زمان ارائه ویندوز NT ویرایش ۴ به بعد کلیه سیستم‌عامل‌ها دارای چنین قابلیت‌هایی هستند . در این مقاله پیاده‌سازی VPN بر مبنای ویندوز ۲۰۰۰ گفته خواهد شد .

پیاده‌سازی VPN

برای پیاده‌سازی VPN بر روی ویندوز ۲۰۰۰ کافیست که از منوی Program/AdministrativeTools / ، گزینه Routing and Remote Access را انتخاب کنید . از این پنجره گزینه VPN را انتخاب کنید . پس از زدن دکمه Next وارد پنجره دیگری می‌شوید که در آن کارت‌های شبکه موجود بر روی سیستم لیست می‌شوند . برای راه‌اندازی یک سرور VPN می‌بایست دو کارت شبکه نصب شده بر روی سیستم داشته باشید . از یک کارت شبکه برای ارتباط با اینترنت و از کارت دیگر جهت برقراری ارتباط با شبکه محلی استفاده می‌شود. در اینجا بر روی هر کارت به‌طور ثابت IP قرار داده شده اما می‌توان این IPها را به صورت پویا بر روی کارت‌های شبکه قرار داد . در پنجره بعد نحوه آدرس‌دهی به سیستم راه دوری که قصد اتصال به سرور ما را دارد پرسیده می‌شود . هر ایستگاه کاری می‌تواند یک آدرس IP برای کار در شبکه محلی و یک IP برای اتصال VPN داشته باشد . در منوی بعد نحوه بازرسی کاربران پرسیده می‌شود که این بازرسی می‌تواند از روی کاربران تعریف شده در روی خود ویندوز باشد و یا آنکه از طریق یک سرویس دهنده RADIUS صورت گیرد در صورت داشتن چندین سرور VPN استفاده از RADIUS را به شما پیشنهاد می‌کنیم . با این روش کاربران ، بین تمام سرورهای VPN به اشتراک گذاشته شده و نیازی به تعریف کاربران در تمامی سرورها نمی‌باشد.

پروتکل‌های استفاده شونده

عملیاتی که در بالا انجام گرفت تنها پیکربندی‌های لازم جهت راه‌اندازی یک سرور VPN می‌باشد . اما (RRAS Remote Routing) (Access Service) دارای دو پروتکل جهت برقراری تونل ارتباطی VPN می‌باشد. ساده‌ترین پروتکل آن PPTP (Point to Point Tunneling Protocol) است ، این پروتکل برگرفته از PPP است که در سرویس‌های Dialup مورد استفاده واقع می‌شود ، در واقع PPTP همانند PPP عمل می‌کند . پروتکل PPTP در بسیاری از موارد کافی و مناسب است ، به کمک این پروتکل کاربران می‌توانند به روش‌های PAP (Protocol (Password Authentication و CHAP (Challenge Handshake Authentication Protocol) بازرسی شوند. جهت کد کردن اطلاعات می‌توان از روش کد سازی RSA استفاده نمود. PPTP برای کاربردهای خانگی و دفاتر و افرادی که در امر شبکه حرفه‌ای نیستند مناسب است اما در جایگاه امنیتی دارای پایداری زیادی نیست . پروتکل دیگری به نام L2TP (Layer2 Forwarding) به وسیله شرکت CISCO ارائه شده که به لحاظ امنیتی بسیار قدرتمندتر است.

این پروتکل با استفاده از پروتکل انتقال اطلاعات (UDP (User Datagram Protocol به جای استفاده از TCP به مزایای زیادی دست یافته است. این روش باعث بهینه و ملموس تر شدن برای دیوارهای آتش شده است، اما باز هم این پروتکل در واقع چیزی جز یک کانال ارتباطی نیست. جهت حل این مشکل و هر چه بالاتر رفتن ضریب امنیتی در VPN شرکت مایکروسافت پروتکل دیگری را به نام IPSec (IP Security) مطرح نموده که پیکربندی VPN با آن کمی دچار پیچیدگی می گردد.

اما در صورتی که پروتکل PPTP را انتخاب کرده اید و با این پروتکل راحت تر هستید تنها کاری که باید در روی سرور انجام دهید فعال کردن قابلیت دسترسی Dial in می باشد. این کار را می توانید با کلیک بر روی Remote Access Policies در RRAS انجام دهید و با تغییر سیاست کاری آن، آن را راه اندازی کنید (به طور کلی پیش فرض سیاست کاری، رد کلیه درخواست ها می باشد).

دسترسی ایستگاه کاری از طریق VPN

حالا که سرور VPN آماده سرویس دهی شده، برای استفاده از آن باید بر روی ایستگاه کاری نیز پیکربندی های را انجام دهیم. سیستم عاملی که ما در اینجا استفاده می کنیم ویندوز XP می باشد و روش پیاده سازی VPN را بر روی آن خواهیم گفت اما انجام این کار بر روی ویندوز ۲۰۰۰ نیز به همین شکل صورت می گیرد. بر روی ویندوزهای ۹۸ نیز می توان ارتباط VPN را برقرار نمود، اما روش کار کمی متفاوت است و برای انجام آن بهتر است به آدرس زیر مراجعه کنید:

www.support.micosot.com

بر روی ویندوزهای XP، یک نرم افزار جهت اتصال به VPN برای هر دو پروتکل PPTP و L2TP وجود دارد. در صورت انتخاب هر کدام، نحوه پیکربندی با پروتکل دیگر تفاوتی ندارد. راه اندازی VPN کار بسیار ساده ای است، کافیه که بر روی Network Connection کلیک نموده و از آن اتصال به شبکه خصوصی از طریق اینترنت (Private Network Through Internet) را انتخاب کنید.

در انجام مرحله بالا از شما یک اسم پرسیده می شود. در همین مرحله خواسته می شود که برای اتصال به اینترنت یک ارتباط تلفنی (Dialup) تعریف نمایید، پس از انجام این مرحله نام و یا آدرس سرور VPN پرسیده می شود. مراحل بالا تنها مراحل اولیه است که نیاز برای پیکربندی یک ارتباط VPN بر روی ایستگاه های کاری می باشد. کلیه عملیات لازمه برای VPN به صورت خودکار انجام می گیرد و نیازی به انجام هیچ عملی نیست. برای برقراری ارتباط کافیه که بر روی آیکنی که بر روی میز کاری ایجاد شده دو بار کلیک کنید پس از وارد کردن کد کاربری و کلمه عبور چندین پیام را مشاهده خواهید کرد که نشان دهنده روند انجام برقراری ارتباط VPN است. اگر همه چیز به خوبی پیش رفته باشد می توانید به منابع موجود بر روی سرور VPN دسترسی پیدا کنید این دسترسی مانند آن است که بر روی خود سرور قرار گرفته باشید.

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

در صورتی که بخواهید دو شبکه را از طریق یک سرور VPN دومی به یکدیگر وصل کنید علاوه بر مراحل بالا باید چند کار اضافه تر دیگری را نیز انجام دهید.

جزئیات کار به پروتکلی که مورد استفاده قرار می گیرد. جهت این کار باید سرور را در پنجره RRAS انتخاب کرده و منوی خاص (Properties) آن را بیاورید.

در قسمت General مطمئن شوید که گزینه های LAN و Demand Dial انتخاب شده باشند (به طور پیش گزیده انتخاب شده هستند). همچنین اطمینان حاصل کنید که پروتکل را که قصد روت (Route) کردن آن را دارید فعال است. پس از مراحل بالا نیاز به ایجاد یک Dial Demand دارید، این کار را می توانید با یک کلیک راست بر روی واسط روت (Interface Routing) انجام دهید.

در پنجره بعدی که ظاهر می شود باید برای این ارتباط VPN خود یک نام تعیین کنید این نام باید همان اسمی باشد که در طرف دیگر کاربران با آن به اینترنت متصل می شوند در صورتی که این مطلب را رعایت نکنید ارتباط VPN شما برقرار نخواهد شد.

پس از این مرحله باید آدرس IP و یا نام دامنه آن را مشخص کنید و پس از آن نوع پروتکل ارتباطی را تعیین نمود . اما مرحله نهایی تعریف یک مسیر (Route) بر روی سرور دیگر می باشد بدین منظور بر روی آن سرور در قسمت RRAS ، Demand Dial را انتخاب کنید و آدرس IP و سابنت را در آن وارد کنید و مطمئن شوید که قسمت Use This to Initiate Demand

انتخاب شده باشد . پس از انجام مرحله بالا کار راه اندازی این نوع VPN به پایان می رسد .

پایان

همانطور که دیدید راه اندازی یک سرور VPN بر روی ویندوز ۲۰۰۰ تحت پروتکل PPTP کار ساده ای بود اما اگر بخواهید از پروتکل L2TP/IPSec استفاده کنید کمی کار پیچیده خواهد شد . به خاطر بسپارید که راه اندازی VPN بار زیادی را بر روی پردازنده سرور می گذارد و هرچه تعداد ارتباطات VPN بیشتر باشد بار زیادی بر روی سرور است که می توانید از یک وسیله سخت افزاری مانند روتر جهت پیاده سازی VPN کمک بگیرید .

آشنایی با هاب و نحوه عملکرد آن

هاب از جمله تجهیزات سخت افزاری است که از آن به منظور برپاسازی شبکه های کامپیوتری استفاده می شود . گرچه در اکثر شبکه هایی 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 عضو 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 عضو یک Collision Domain یکسان می باشند. تمامی کامپیوترهایی که با استفاده از هاب به یکدیگر متصل می شوند ، عضو یک Domain Collision 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 domain ارسال می گردد . هاب و سوئیچ با موضوع broadcast domain برخورد مناسبی نداشته (ایجاد حوزه های مجزا) و در این رابطه به یک روتر نیاز خواهد بود . به منظور برخورد مناسب (ایجاد حوزه های مجزا) با collision domain ، broadcast domain و افزایش سرعت و کارایی یک شبکه از تجهیزات سخت افزاری متعددی استفاده می شود . سوئیچ ها collision domain مجزائی را ایجاد می نمایند ولی در خصوص broadcast domain بدین شکل رفتار نمی نمایند . روترها ، broadcast domain و collision domain مجزائی را ایجاد نموده و در مقابل هاب ، قادر به ایجاد broadcast domain 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--Hub) .

آشنایی 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 صرفاً این اطمینان را ایجاد می نمایند که فریم های داده بر روی هر یک از پورت ها ، تکرار خواهد شد.

گره هایی که یک اترنت و یا Fast Ethernet را با استفاده از قوانین CSMA/CD به اشتراک می گذارند ، عضو 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 متأثر خواهند شد .

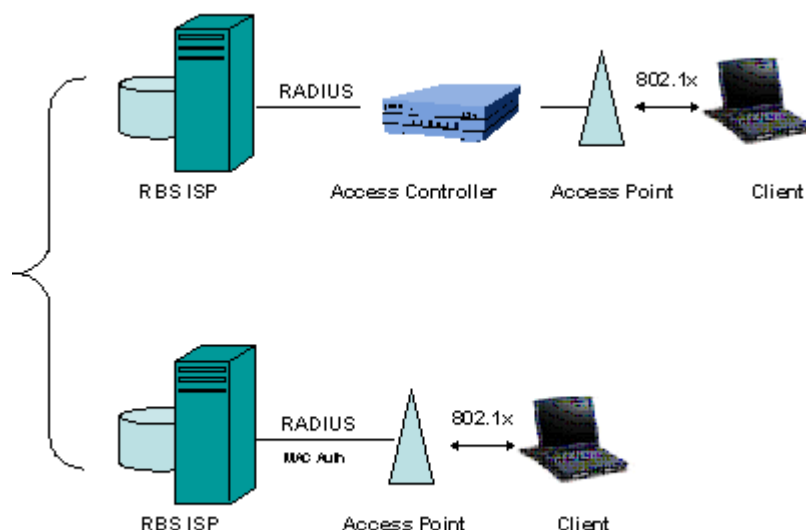
کامپیوترها و یا گره های متصل شده به هاب از کابل های (Unshielded Twisted Pair) UTP ، استفاده می نمایند . صرفاً یک گره می تواند به هر پورت هاب متصل گردد . مثلاً با استفاده از یک هاب هشت پورت ، امکان اتصال هشت کامپیوتر وجود خواهد داشت . زمانی که هاب ها به متداولی امروز نبودند و قیمت آنان نیز گران بود ، 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 ، عضو یک Broadcast domain و collision domain یکسانی می باشند ، بنابراین تمامی آنان هر نوع collision و 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 .

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. آنالایزهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزها 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. آنالایزها 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 پارامترهای 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 هر حال، 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 VPN ها 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. آنالیزهای 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 LAN ها است 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 LAN های استفاده کننده از 802.1x فوق العاده باارزش هستند.

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چالش 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. آنالیزهای 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 LAN های بی سیم بدون نظارت مهندسان امنیتی به کار گرفته 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 آنالیزها همچنین می توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPN ها یا 802.1x استفاده نمی کنند، علائم هشدار دهنده را ثبت کنند.

رویکردی عملی به امنیت شبکه لایه بندی شده (۱)

مقدمه

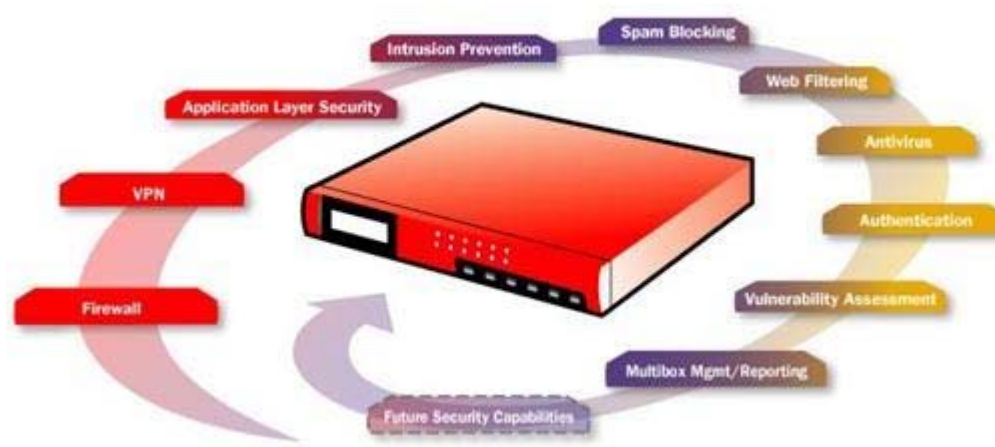
امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است. {گروه امداد امنیت کامپیوتری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

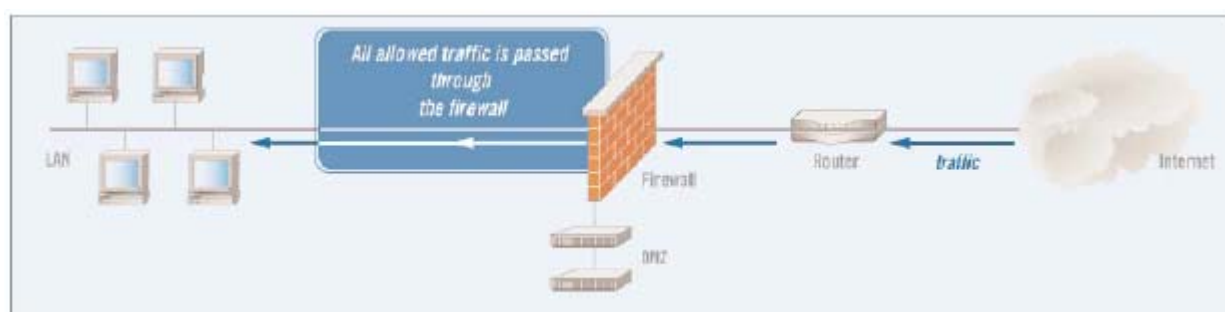
اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند که بعنوان DMZ (zone demilitarized) شناخته می شود. DMZ معمولاً وب سرورها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای DNS را دربرمی گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سخت 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** - 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 مبدأ 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** - 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** - 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 رمز شده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیر یاب 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 سخت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند.

معایب

از آنجا که بیشتر این سیستم‌ها تقریباً پایه‌ای هستند و مدت‌هاست که در دسترس بوده‌اند، بیشتر هک‌های پیشرفته روش‌هایی برای دور زدن آنها نشان داده‌اند. برای مثال، یک ابزار آنتی‌ویروس نمی‌تواند 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 می‌کند، اما کار اجرایی بیشتری را بر روی کارمندان IT تحمیل می‌کند، چرا که کلیدهای رمزنگاری و گروه‌های کاربری باید بصورت مداوم مدیریت شوند.

ملاحظات

پیچیدگی معماری شبکه شما می‌تواند تأثیر قابل ملاحظه‌ای روی میزان اثر این تکنولوژی‌ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی‌ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هرکدام از تکنولوژی‌های مذکور اجازه می‌دهد 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 سیاست‌های امنیتی سفت و سخت‌تری 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 می‌پردازیم.

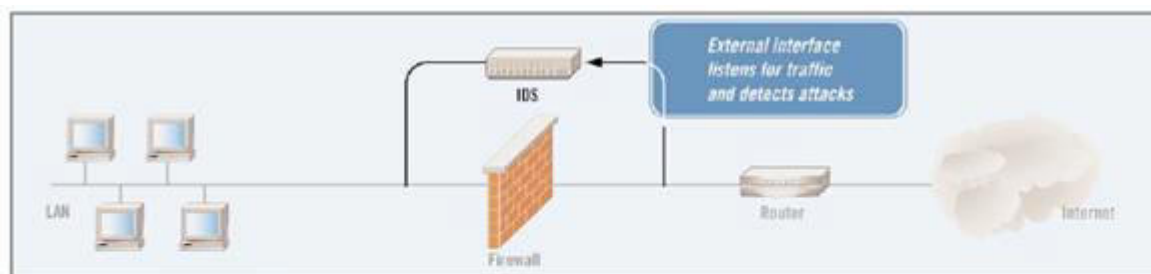
سطح ۲- امنیت شبکه

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

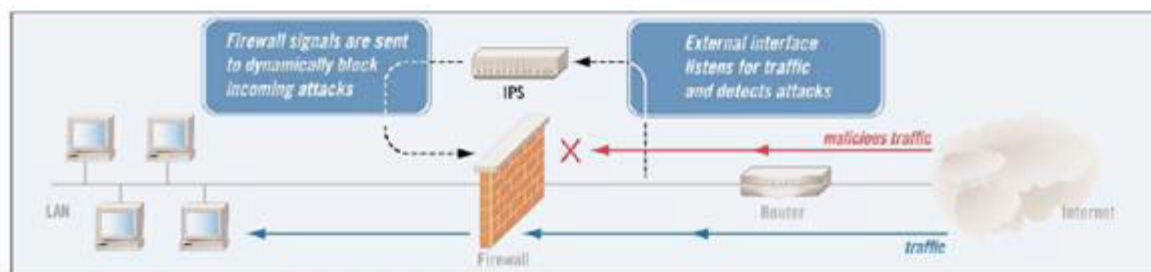
در میان شبکه حرکت کنید. این قضیه بخصوص برای سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل می شوند. تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند:

IDS ها (سیستم های تشخیص نفوذ) و IPS ها (سیستم های جلوگیری از نفوذ) - تکنولوژیهای IDS

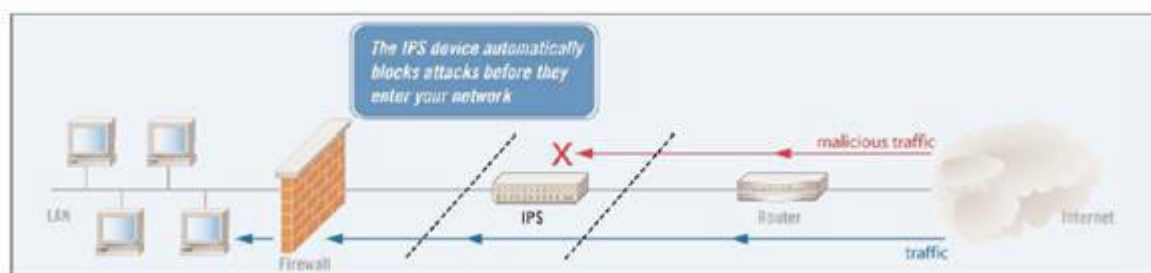
IPS و ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند. ابزارهای IDS مسئولین 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. IDS ها و IPS ها مشخصات مشترک زیادی دارند. در حقیقت، بیشتر IPS ها 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)

پری - 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 آزمایش.

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 تأیید هویت 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، ارتقاء دادن 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. هرکرا بصورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، همچنانکه 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،

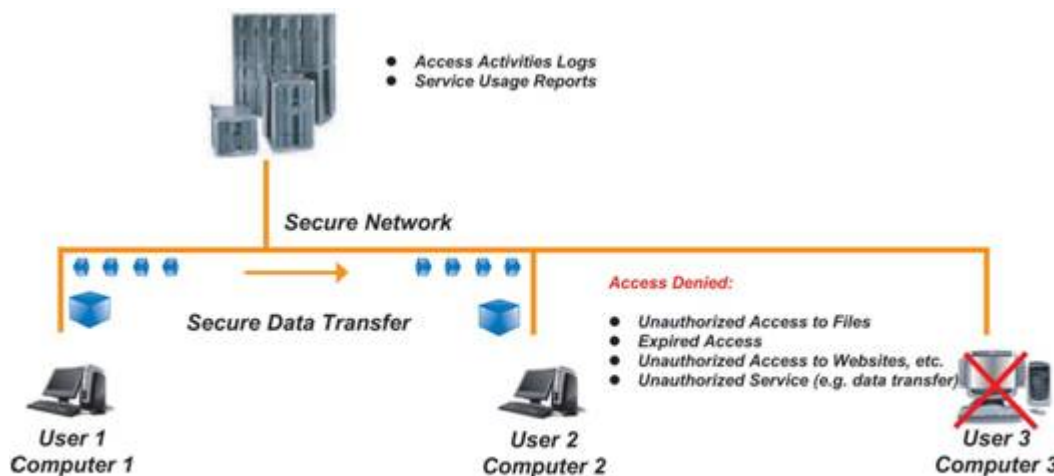
توابع عملیاتی

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** - IDS های سطح میزبان عملیاتی مشابه IDS های شبکه انجام می دهند؛ تفاوت

اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDS های سطح میزبان برای مشخصات عملیاتی خصوصی 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 پوشش می کنند. دقت آنها نسبتاً بالاست و کمترین نیاز را به منابع میزبان دارند. از آنجایی که VA ها بطور مشخص برای ابزار میزبان پیکربندی می شوند، در صورت مدیریت مناسب، سطح بسیار بالایی از پوشش را فراهم می کنند.

• **تابعیت امنیتی کاربر انتهایی** - روش های تابعیت امنیتی کاربر انتهایی وظیفه دوجندانی 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 زبان 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.

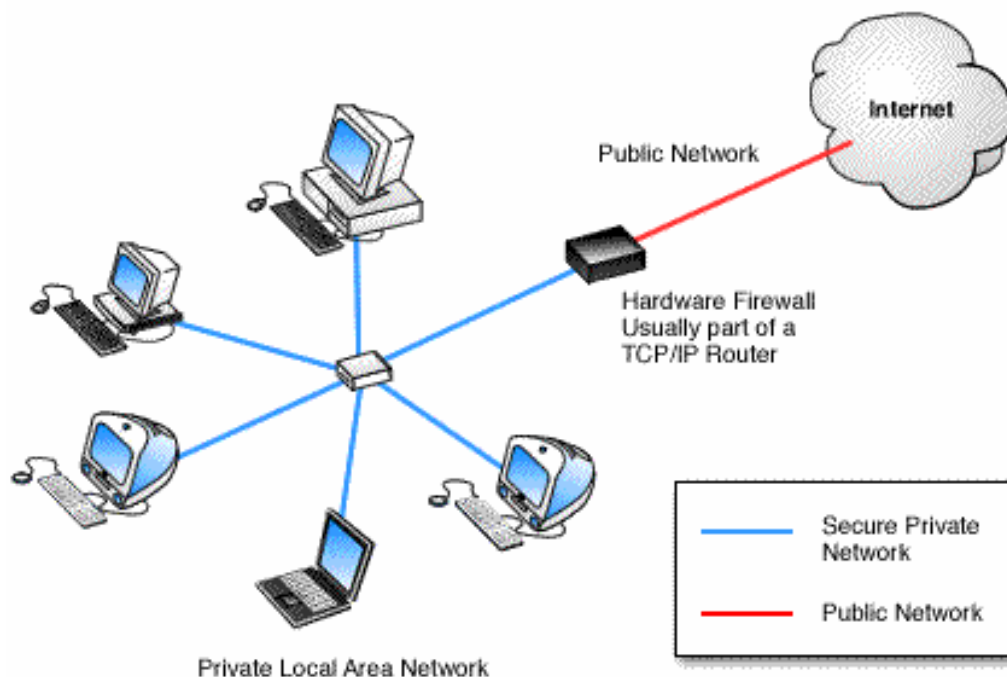
مزایا

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

تنظیمات 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 نیت 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 مسئول 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 PGP، RSA و PKI 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 (6) : جمع بندی

در شماره های قبل به لایه های مختلف در امنیت شبکه لایه بندی شده پرداختیم. در این شماره 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** - 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.

• **بازیش ایمیل ها بصورت نامجاز** - 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** - 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.

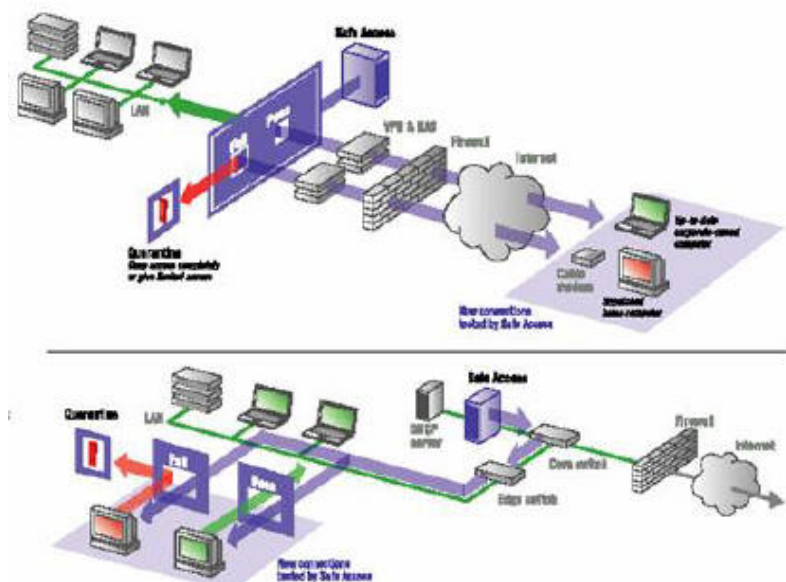
• **فراهم بودن سرویس های اینترنتی غیرمجاز** - توانایی آسان بکارگیری یک وب سرور یا سرویس اینترنتی دیگر روی یک کامپیوتر ریسک افشای سبوی اطلاعات را بالا می برد. اغلب چنین سرویس هایی کشف نمی شوند، در حالی که در شعاع رادار دیگران قرار می گیرند!

• **تشخیص فعالیت ویروسی** - 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 - یعنی یک فایروال در ترکیب با یک آنتی ویروس - 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 معمولاً 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 رمز نشده 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 معمولاً نباید در یک کارت ذخیره شود.

۳- کلیدهای اصلی و کلیدهای مشتق شده (Master keys and derived keys)

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 مشتق شده استفاده می‌شود که بعداً 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 مشتق شده حاصل می‌شود و به آن کارت اختصاص داده می‌شود.

شکل دیگری از کلیدهای مشتق شده 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 رمزکننده کلید (Key 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 رمز شده 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. معمولاً یک دامنه، یک سیستم کامپیوتری خواهد بود که می‌تواند بصورت فیزیکی و منطقی محافظت گردد. کلیدهای استفاده شده در یک دامنه توسط یک کلید رمزکننده کلید 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