۷ نکته در مورد امنیت شبکه‌های بی سیم

بسیاری از کسانی که اینترنت را به صورت وایرلس در خانه های خود به اشتراک می گذارند، این کار را آن قدر از سر اشتیاق سریع انجام می‌دهند که فراموش می کنند برخی نکات امنیتی را رعایت کنند. این موضوع کاملا قابل درک است اما ریسک بالای امنیتی ایجاد می کند. شبکه های وای فای امروزی قابلیت های زیادی دارند که با کمک آن ها می توانید شبکه وایرلس خود را تا حد امکان امن کنید.

۱. کلمه عبور پیش‌فرض مدیر سیستم(administrator) را روی نقاط دسترسی و مسیریاب‌های بی‌سیم تغییر دهید

اغلب نقاط دسترسی (Access Point)و مسیریاب‌های بی‌سیم امکان مدیریت شبکه WiFi را از طریق یک حساب کاربری مدیریتی فراهم می‌کنند. این حساب کاربری امکان دسترسی ابزار و پیکربندی آن را با نام کاربری و کلمه عبور فراهم می‌کند. اغلب تولیدکنندگان نام کاربری و کلمه عبور را در کارخانه تنظیم می‌کنند. نام کاربری معمول admin یا administrator و کلمه عبور یا خالی است یا کلماتی مثل admin ،password ،public و.... می‌باشد.

اولین گام برای افزایش امنیت شبکه بی‌سیم تغییر کلمه عبور پیش‌فرض نقاط دسترسی و مسیریاب‌های بی‌سیم بلافاصله پس از نصب است. اغلب ابزارها اجازه تغییر نام کاربری را نمی‌دهند اما اگر ابزارهای شما این امکان را می‌دهند، اکیدا توصیه می‌شود که نام کاربری را هم تغییر دهید.

برای امن نگه‌داشتن شبکه در آینده، می‌بایست به‌طور منظم این کلمه عبور را تغییر دهید. اغلب کارشناسان توصیه می‌کنند کلمه عبور را بعد از ۳۰ تا ۹۰ روز تغییر دهید.

۲. فعال‌سازی قابلیت WPA/WEP

WPA (WiFi Protected Access) یک استاندارد امنیتی برای شبکه‌های بی‌سیم است (با Windows XP Product Activation اشتباه نشود). برای استفاده از WPA با Windows XP باید Clientهای دارای Windows XP را به صورت دستی patch کنید و هم‌چنین مطمئن شوید کارت شبکه‌ها و نقاط دسترسی به درستی پیکربندی شده‌اند.

برای پیکربندی WPA در شبکه با clientهای دارای ویندوز XP مراحل زیر را انجام دهید:

۱. نوشتار Overview of the WPA wireless security update in Windows XP را مطالعه کنید.

۲. بررسی کنید که تمام Client ها حداقل Service Pack۱ داشته باشند.

۳. روی هر Client بررسی کنید که کارت شبکه با سرویس WZC(Windows Zero Configuration) سازگار باشد.

۴. برای هر client وصله Windows XP Support Patch for Wi-Fi Protected Access را بارگزاری و نصب کنید.

۵. تغییرات لازم برای نقاط دسترسی بی‌سیم از گام ۱ را اعمال کنید.

۶. تغییرات لازم برای کارت شبکه‌های بی‌سیم از گام ۱ را اعمال کنید.

۳. تغییر SSID پیش فرض

نقاط دسترسی و مسیریاب‌های بی‌سیم دارای یک نام شبکه SSID(Service Set Identifier) هستند که توسط تولیدکنندگان به‌طور پیش‌فرض انتخاب می‌شود. SSID از ابزارهای پیکربندی بر مبنای وب یا ویندوز این سازندگان قابل دسترسی است. اغلب SSID های پیش فرض کلمات ساده‌ای مثل linksys، netgear، wireless default و... هستند. هرچند نفوذگر صرفا با دانستن SSID قادر به نفوذ به شبکه شما نیست ولی این مساله به عنوان یک نقطه شروع خوب برای نفوذگر به حساب می آید. زمانی که کسی شبکه ای با SSID پیش فرض بیابد، با دانستن این نکته که به احتمال فراوان این شبکه به درستی پیکربندی نشده است، ترغیب به نفوذ به شبکه می‌شود.

SSID می تواند هر زمانی تغییر کند به شرطی که این تغییر در تمام clientها نیز اعمال شود. برای افزایش امنیت شبکه های بی سیم، نام پیش فرض SSID را تغییر دهید. در انتخاب SSID توصیه های زیر را در نظر داشته باشید:

ـ از نام، آدرس، تاریخ تولد، شماره تلفن یا دیگر اطلاعات شخصی تان به عنوان بخشی از SSID استفاده نکنید.

-از کلمات عبور نام کاربری ویندوزتان یا emailتان یا... استفاد نکنید.

- با استفاده از عباراتی مثل «FUNNY_»، «TOP_SECRET BOX» و... نفوذگران را وسوسه نکنید.!!!

- از ترکیب حروف و اعداد استفاده کنید.

- عباراتی با طول حداکثر یا نزدیک به حداکثر انتخاب کنید.

- هرچند ماه یک بار SSIDتان را تغییر دهید.

۴. قابلیت پالایش آدرس MAC را روی نقاط دسترسی و مسیریاب‌های بی‌سیم فعال کنید

اغلب نقاط دسترسی و مسیریاب های بی سیم دارای قابلیتی به نام پالایش آدرس MAC (MAC Address Filtering) هستند. این مشخصه اغلب به‌طور پیش فرض فعال نیست. برای افزایش امنیت شبکه بی سیم تان این قابلیت را فعال کنید. در صورتی که این قابلیت فعال نباشد، هر clientای با دانستن SSID شبکه شما (در نظر داشته باشید که فهمیدن SSID کار بسیار ساده ای است) شاید چند پارامتر امنیتی دیگر مثل کلید رمزگذاری (در صورتی که قابلیت WEP فعال باشد) می تواند به شبکه شما وصل شود.

برای تنظیم قابلیت پالایش آدرس MAC شما به عنوان مدیر شبکه بی سیم باید لیست clientهایی که مجازند به شبکه وصل شوند را پیکربندی کنید. ابتدا آدرس MAC هر client را از طریق سیستم عامل یا ابزارهای پیکربندی به دست آورید و سپس آن ها را در صفحه پیکربندی نقاط دسترسی و مسیریاب های بی سیم وارد کنید و نهایتا قابلیت پالایش را فعال کنید. از این پس هر درخواست اتصال به شبکه

بی سیم که برسد آدرس MAC آن با لیست تنظیم شده بررسی شده و در صورتی که در لیست نباشد اجازه اتصال به شبکه را نمی یابد. البته باید نوجه داشت که نفوذگران با جعل آدرس MAC (MAC Spoofing) قادرند به شبکه بی سیم شما وصل شوند ولی این مساله نباید باعث شود که شما از خیر این قابلیت بگذرید.

۵. قابلیت همه‌پخشی SSID را روی نقاط دسترسی و مسیریاب‌های بی‌سیم غیرفعال کنید

اغلب نقاط دسترسی و مسیریاب های بی سیم به‌طور خودکار SSID خوشان را در فواصل زمانی مشخص پخش می کنند. این مشخصه برای این است که clientها بتوانند به‌طور پویا شبکه های بی سیم را تشخیص دهند و بین آن ها جابه‌جا شوند (از شبکه ای به شبکه دیگر نقل مکان کنند). لازم به ذکر است که این مشخصه برای hotspotهای تجاری و سیار طراحی شده است که clientهای زیادی می آیند و می روند ولی برای شبکه های خانگی لازم نیست. از آن جایی که SSID به صورت واضح پخش می شود و هیچ رمزگذاری روی آن صورت نمی‌گیرد، به دست آوردن آن توسط نفوذگران کار راحتی است. همان‌طور که در گام ۳ اشاره شد نفوذگر با دانستن SSID یک مرحله به هدف نزدیک تر می شود.

در یک شبکه بی سیم بحث roaming (جابه‌جایی بین دو شبکه بی سیم) مطرح نیست و پخش کردن SSID هیچ ضرورتی ندارد. برای افزایش امنیت شبکه بی سیم باید این قابلیت را غیرفعال کنید. یک بار که client شما با SSID درست پیکربندی شد دیگر نیازی به پیغام های همه‌پخشی نیست.

دقت داشته باشید که غیرفعال کردن قابلیت همه‌پخشی SSID فقط یکی از تکنیک‌های محکم‌سازی و افزایش امنیت شبکه‌های بی سیم است. این روش ۱۰۰ درصد موثر نیست و نفوذگرها هنوز می توانند با sniff کردن پیغام های مختلف پخش شده در پروتکل WiFi، SSID را تشخیص دهند. در واقع تکنیک هایی مثل غیرفعال کردن همه‌پخشی SSID باعث می شئد که شبکه بی سیم شما هدف راحتی برای نفوذگران نباشد.

۶. به شبکه های WiFi باز وصل نشوید

مطمئن شوید که تنظیمات سیستم به گونه‌ای است که مانع اتصال خودکار به نقاط دسترسی ناامن شود.

اتصال به یک شبکه WiFi باز مثل یک hotspot یا مسیریاب بی‌سیم آزاد، کامپیوتر شما را در معرض خطرات فراوانی قرار می دهد. هرچند به طور معمول این امکان فعال نیست ولی اغلب کامپیوترها دارای تنظیماتی هستند که امکان اتصال خودکار بدون اطلاع کاربر را فراهم می‌کنند. این تنظیمات به‌جز در موارد ضروری و به‌طور موقت نباید فعال باشد.

برای بررسی این‌که آیا اتصال خودکار به شبکه‌های WiFi باز، مجاز است یا نه، تنظیمات بی‌سیم کامپیوتر را بررسی کنید. برای مثال در کامپیوترهایی که دارای Windows XP هستند، تنظیمات بی‌سیم Automatically connect to non-preferred networks نامیده می‌شود. برای بررسی مراحل زیر را انجام دهید:

- از منوی start به گزینه Windows Control Panel بروید.
- به گزینه Network Connections بروید
- بر روی Wireless Network Connection کلیک راست کنید و گزینه Properties را انتخاب کنید.
- روی گزینه Wireless Networks کلیک کنید.
- بر روی دکمه Advanced کلیک کنید.
- گزینه Automatically connect to non-preferred networks را پیدا کنید، اگر انتخاب شده بود این تنظیمات فعال است در غیر این صورت غیرفعال است.

اگرچه در Windows XP به‌طور پیش فرض Automatically connect to non-preferred networks فعال نیست، برخی کاربران برای سهولت اتصال به شبکه خودشان آن را فعال می‌کنند. کاربران باید شبکه خودشان را به عنوان Windows XP Preferred networks تنظیم کنند که اجازه اتصال خودکار را می‌دهد و اتصال خودکار به بقیه شبکه‌ها را غیرفعال کنند.

۷. به تجهیزات آدرس (IP) ایستا اختصاص دهید

اختصاص آدرس ایستا جایگزینی برای پروتکل DHCP است. اختصاص آدرس پویا با استفاده از DHCP راحت تر است و هم چنین به کامپیوترهای سیار اجازه می دهد که بین شبکه های مختلف جابه جا شوند.

آدرس دهی ایستا نیز مزایایی دارد، از جمله:

- آدرس ثابت ترجمه آدرس را بهتر پشتیبانی می کند، بنابراین یک کامپیوتر روی شبکه با نام دامنه اش به طور مطمئن قابل دستیابی است. مخصوصا سرورهایی مثل سرور وب و سرور FTP بهتر است آدرس ایستا داشته باشند.
- استفاده از آدرس دهی ایستا در مقابل DHCP محافظت بیشتری در برابر حملات امنیتی فراهم می کند.
- برخی تجهیزات شبکه پروتکل DHCP را پشتیبانی نمی کنند.
- استفاده از آدرس دهی ایستا برای تمام اجزای شبکه تضمین می کند که ناسازگاری آدرس ها رخ نمی دهد.

آدرس های ایستا باید از محدوده آدرس های خصوصی استاندارد انتخاب شود

این محدوده ها تعداد زیادی آدرس را پشتیبانی می کنند. برخلاف تصور اکثر افراد، تمام آدرس های این محدوده ها نمی توانند انتخاب شوند. برای انتخاب آدرس درست نکات زیر را مدنظر داشته باشد:

۱. آدرس هایی که با «۰» یا «۲۵۵» تمام می شوند را انتخاب نکنید. این آدرس ها برا ی استفاده پروتکل های شبکه رزرو شده اند.

۲. آدرس های ابتدای یک محدود آدرس خصوصی را انتخاب نکنید. آدرس هایی مثل «۱۰،۰،۰،۱۰» یا «۱۹۲،۱۶۸،۰،۱» معمولا به مسیریاب ها ی شبکه اختصاص می یابند. این آدرس ها اولین آدرس هایی هستند که معمولا یک نفوذگر تلاش می کند به آن ها نفوذ کند، بنابراین بهتر است از آن ها استفاده نکنید.

۳. از آدرس هایی که خارج از محدوده mask شبکه شما می باشد استفاده نکنید. برای مثال، برای پشتیبانی تمام آدرس های محدوده «x.x.x.۱۰، mask» شبکه برای تمام سیستم ها باید به «۲۵۵،۰،۰،۰» تنظیم شود، در غیراین صورت برخی آدرس های ایستای این محدوده کار نمی کنند.