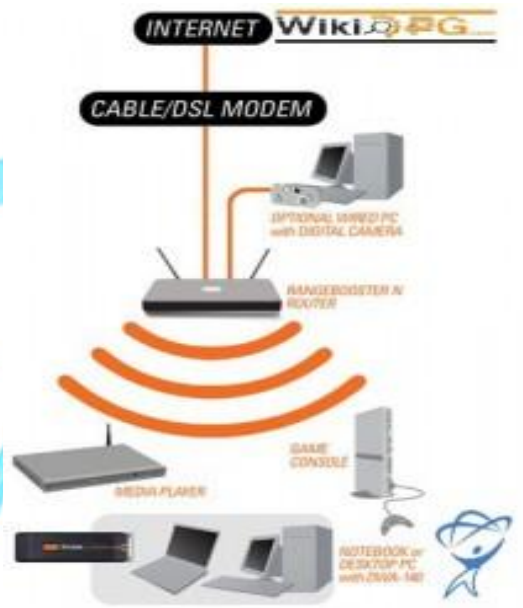
آموزش جلوگیری از نفوذ دیگران به اینترنت بی سیم

برخی از استفاده کنندگان اینترنت بی سیم، اعلام می کنند که میزان مصرف واقعی آنها از اینترنت، کمتر از چیزی است که گزارشات مصرف نشان می دهد. یعنی شخص دیگری از اینترنت آنها استفاده می کند و خودشان خبر ندارند!

اینترنت بی سیم شما چه از طریق شبکه های بزرگ وایرلس تامین شود، و چه از طریق WiFi ، احتمال نفوذ و استفاده از آن توسط دیگران وجود دارد. البته شرکت های ارائه دهنده خدمات اینترنت بی سیم ، از طرف خودشان امنیت را تامین می کنند. اما شما نیز به عنوان کاربر نهایی، باید مراقبت های لازم را انجام دهید تا کسی نتواند از اینترنت شما به صورت غیر مجاز و مخفیانه استفاده کند.

شما هم اگر احساس می کنید که حجمی از اینترنت شما توسط شخصی غیر از خودتان استفاده می شود، باید یک بار دیگر مراقبت های امنیتی را کنترل کنید. شاید شخصی اکانت شما را هک کرده باشد و از اینترنت شما به صورت مخفیانه استفاده کند. اگر از دسته افرادی هستید که یک شبکه بی‌سیم ناامن دارید، باید بدانید همه انسان‌ها به اندازه شما پایبند به اصول اخلاقی نیستند و ممکن است علاوه بر استفاده از پهنای باند و دانلودهای مکرر بتوانند به اطلاعات شخصی شما هم دسترسی پیدا کنند. بنابراین با توجه به اصل «پیش‌گیری به از درمان» بهتر است زودتر به فکر بیفتید و امنیت شبکه بی‌سیم خود را با خواندن این مطلب فراهم کنید.

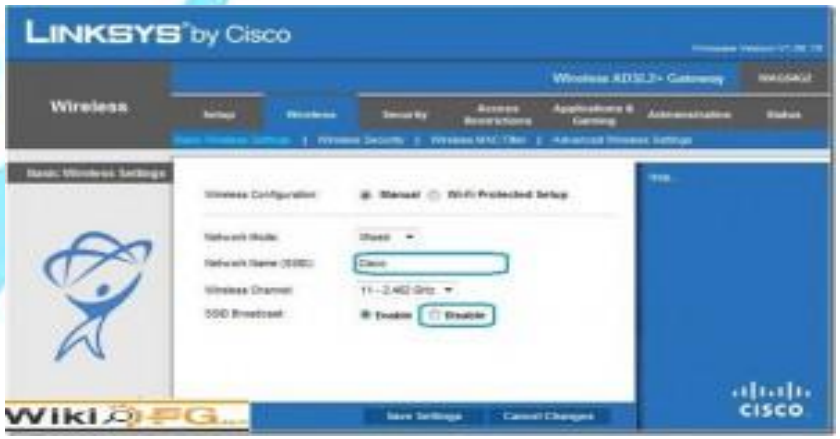


نام روتر خود را از دید دیگران مخفی کنید

SSIDدر واقع مخفف عبارت Service Set Identifier و نام مشخص‌کننده یک شبکه مبتنی بر استاندارد ۸۰۲,۱۱ است. اکثر روترهای وای‌فای امروزی در حالت پیش‌فرض، SSIDیا نام خود را به کلیه سیستم‌های اطراف ارسال می‌کنند. بنابراین اگر شبکه شما در وضعیت «ارسال به همه» یا «Broadcast» باشد هر فرد نزدیک شما با یک تبلت، تلفن هوشمند یا رایانه‌ای با کارت شبکه بی‌سیم می‌تواند نام شبکه‌تان را بداند که این موضوع چندان خوبی نیست. اولین کار امنیتی که باید برای یک شبکه بی‌سیم انجام داد انتخاب یک نام منحصربه‌فرد برای روتر است که تا حد امکان بهتر است از واژه‌هایی که مربوط به برندهای مختلف این دستگاه می‌شود خودداری کرد. تعداد کاراکترهای مورد استفاده برای SSID می‌تواند حداکثر ۳۲ کاراکتر باشد. پس از آنکه نام روتر خود را تغییر دادید باید آن را از وضعیت Broadcastدرآورید تا SSID برای همه افرادی که در محدوده شبکه شما هستند، ارسال نشود. در این حالت کاربری که می‌خواهد به شبکه بی‌سیم متصل شود باید SSID را به صورت دستی وارد کند. جهت مخفی کردن نام روتر مراحل زیر را طی کنید:

۱ -در مرورگر خود ip مربوط به روتر (معمولا ۱۹۲،۱۶۸،۱،۱) را وارد کنید و با نام کاربری و کلمه عبور (معمولا هر دو به طور پیش‌فرض admin هستند) وارد بخش تنظیمات روتر شوید.

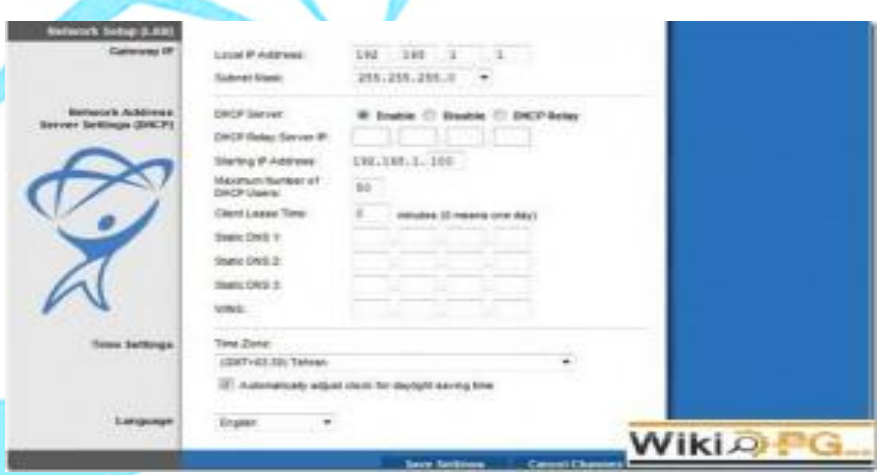
۲ -به دنبال گزینه‌ای با عنوان Wireless بگردید. در روترهای TP-LINK این گزینه در بخش Interface Setup قرار دارد .SSIDپیش‌فرض را به نام دلخواهی که قابل حدس زدن نباشد تغییر داده و آن را از وضعیت Broadcast درآورید؛ یعنی در بخش Broadcast SSID گزینه NO را انتخاب کنید.



آدرس های آی پی را محدود کنید

هر سیستم یا دستگاه موجود در شبکه باید به طور منحصربه‌فرد یک آدرس آی‌پی داشته باشد. دستگاه‌های مختلف در شبکه از این آدرس استفاده کرده و با یکدیگر ارتباط برقرار می‌کنند. در بخش تنظیمات روترها بخشی با عنوان DHCP وجود دارد که توسط پروتکل مربوط به صورت خودکار به دستگاه‌های شبکه آدرس آی‌پی اختصاص می‌دهد .DHCP در سازمان‌های بزرگ با تعداد سیستم‌های زیاد می‌تواند

مفید واقع شود و از اتلاف وقت جلوگیری کند اما در صورتی که دستگاه‌های زیادی به شبکه بی‌سیم شما متصل نیست بهتر است آدرس‌های آی‌پی را به صورت دستی وارد کنید و به لپ‌تاپ، تلفن همراه، کنسول بازی و... آدرس‌های منحصربه‌فرد بدهید. در غیر این صورت به بخش تنظیمات DHCP بروید و اگر به عنوان مثال شش دستگاه متصل به شبکه دارید تعداد آی‌پی‌هایی را که DHCP باید به آنها بدهد به عدد شش محدود کنید.

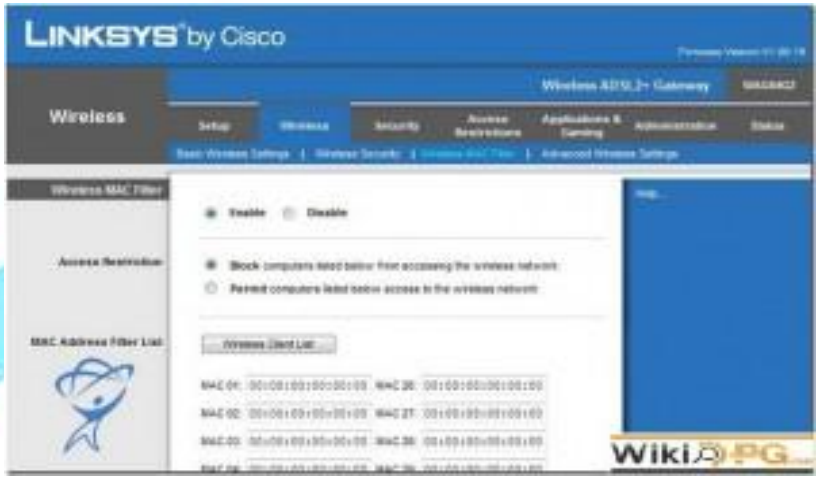


آدرسهای سخت افزاری (MAC)را فیلتر کنید

MACمخفف Media Access Control است. هر کارت شبکه دارای یک آدرس MACبوده و بسته‌های شبکه نیز برای یافتن راه خود از این آدرس استفاده می‌کنند. سومین کاری که باید برای تنظیمات روترخود انجام دهید آن است که دسترسی به شبکه را محدود به کارت شبکه‌های مورد نظرتان کنید تا هر فرد از خارج نتواند به راحتی وارد شبکه بی‌سیم شما شود. برای انجام این کار ابتدا باید لیستی از آدرس‌های MAC مربوط به سیستم‌هایی که می‌خواهید به آنها اجازه استفاده از شبکه را بدهید تهیه کرده و سپس مراحل زیر را طی کنید:

۱ -در مرورگر خود ip مربوط به AP را وارد و Login کنید تا تنظیمات AP نشان داده شود.

۲ -مجددا به بخش تنظیمات Wireless بروید و Filter By MAC را با انتخاب Activate فعال کنید و در نهایت در لیست موجود آدرس‌های MAC مورد نظرتان را وارد کنید:



برای شبکه خود کلمه عبور انتخاب کنید

بهتر است برای کدگذاری شبکه بی‌سیم به جای استفاده از مکانیسم WEP از WPA و یا LEAP استفاده کنید تا نفوذ بیگانگان به شبکه را به حداقل برسانید. زمانی که از یک روتر یا اکسس پوینت در شبکه بی‌سیم خود استفاده می‌کنید، همان طور که شما قادر به انتقال داده بین سیستم‌های شبکه محلی خود هستید ممکن است فردی از خارج محدوده شبکه‌تان هم بتواند این داده‌ها را دریافت کند. در اینجا کدگذاری داده‌ها با روش‌های مختلف به کمک شبکه بی‌سیم می‌آید. اما تفاوت بین دو نوع کدگذاری WEP و WPA در چیست؟ چرا روش WPA نسبت به WEP ترجیح داده می شود؟

WEPمخفف عبارت Wired Equivalent Privacy یا Wireless Encryption Protocol است. در واقع WEP جزئی از استانداردهای IEEE به شمار می‌رود که در ابتدا برای شبکه‌های مبتنی بر سیم (Wired) طراحی شد و امروزه برای شبکه‌های بی‌سیم نیز مورد استفاده قرار می‌گیرد. به دلیل آنکه داده‌ها در شبکه‌های بی‌سیم توسط امواج رادیویی منتشر می‌شوند WEP مکانیسمی برای کدگذاری این امواج رادیویی در خود دارد. سیستم کدگذاری WEP برای نسل اول شبکه‌های بی‌سیم مورد استفاده قرار می‌گرفت. امروزه به این نتیجه رسیده‌اند که این نوع کدگذاری آنقدرها هم که پیش‌بینی شده بود امن نیست. کدگذاری WEP در دو لایه زیرین مدل OSI یعنی لایه داده و لایه فیزیکی کار می‌کند و در واقع امنیت نهایی را برقرار نمی‌سازد.

بزرگـترین مشکل سیستم کدگذاری WEP آن است که از روش کلیدهای استاتیک برای انجام این کار استفاده می‌کند. زمانی که در روتر شبکه خود از روش WEP استفاده می‌کنید، این روش یک کلید مخصوص تولید می‌کند که روتر و بقیه سیستم‌های شبکه برای انتقال هر جزء کوچک داده از آن کلید استفاده می‌کنند. به این دلیل که پیدا کردن این کلید خاص امروزه کار شاقی نیست، روش کدگذاری WEP را مناسب نمی‌دانند. امروزه پیدا کردن یک کلید WEP به کمتر از یک دقیقه زمان نیاز دارد. در واقع با انتقال تنها ۱۰۰هزار بسته در شبکه می‌توان آن را پیدا کرد.

زمان زیادی نیست که روش WPA به داد شبکه‌های بی‌سیم می‌رسد .مخفف عبارت Wi-Fi Protected Access است . هیچ تضمینی بر هک نشدن کدگذاری به روش WPAوجود ندارد، با این وجود بسیار بهتر از WEP عمل می‌کند. برتری‌های این روش عبارتند از:

۱ -با استفاده از پروتکل TKIP کلیدهایی که تولید می‌شوند حالت موقتی دارند. علاوه بر آن توسط یک تابع یا الگوریتم که Hash نام دارد این کدگذاری‌ها صورت می‌گیرد. تابع Hashای که در روش WPA به کار می‌رود بسیار بهینه‌تر از WEP عمل می‌کند.

۲ -شناسایی کاربر در این روش به صورت بهینه‌تری انجام می‌گیرد. با استفاده از پروتکل EAP که مخفف Extensible Authentication Protocol است، به بررسی کلیدی با عنوان Public می‌پردازد و به افراد خارج از شبکه موجود اجازه وارد شدن به شبکه را نمی‌دهد.

زمانی که می‌خواهید یک مودم ADSL بی‌سیم تهیه کنید و در عین حال نمی‌خواهید به دیگران اجازه استفاده از کاربری اینترنت خود را بدهید، بهتر است به فردی که در حال نصب مودم است بگویید کدگذاری را به روش WPA انجام دهد. البته خودتان می‌توانید به روش زیر نحوه کدگذاری را تغییر دهید، هرچند بسته به نوع مودم ممکن است مراحل متفاوت باشد:

۱ -مرورگر اینترنتی خود را باز کرده و آی‌پی مودم بی‌سیم خود را ۱۹۲,۱۶۸,۱,۱ وارد کنید. نام کاربری و کلمه عبور مدیریت امکانات مودم را وارد کنید تا صفحه‌ای شبیه صفحه زیر برایتان باز شود:

۲ -گزینه Interface Setup و سپس Wireless را انتخاب کنید. در بخش Authentication Type و از منوی کشویی آن به جای WEP گزینه WPAرا انتخاب و کلمه عبور مورد نظرتان برای اتصال به مودم را تایپ کنید.در نهایت تغییرات را ذخیره و مودم را ری‌استارت کنید.

اقدامات امنیتی به هنگام اتصال به شبکه های Wireless

شبکه های Wireless یا بی‌سیم مدت زمانی است که در کشور ما روند رو به رشدی داشته است. در حال حاضر در دانشگاه ها، فرودگاه ها، مراکز تجاری و اماکنی نظیر آنها دسترسی به اینترنت از طریق شبکه Wireless امکان پذیر است. اما نکته ای که وجود داردابن است که اگر ایجاد به یک شبکه بی‌سیم برای همه امکان پذیر است بنابراین استفاده از آن برای مجرمان و خلافکاران نیز مجاز می‌باشد! پس شما به عنوان یک کاربر در این زمان نبایستی ایمنی سیستم خود را فراموش کنید. یکی از ترفندهای هکرها این است که یک سرور دروغین ایجاد کرده و باعث میشوند شما به جای اتصال به سرور اصلی شبکه

ناآگاهانه به کامپیوتر هکر که نقش سرور را ایفا میکند متصل شوید! به همین سادگی خودتان باعث شده اید هکر بتواند به سادگی به کامپیوتر یا لپتاپ شما نفوذ کرده و سوءاستفاده نماید. برای جلوگیری از این مشکلات چه باید کرد؟ در این ترفند به معرفی اقدامات احتیاطی به هنگام اتصال به شبکه Wireless می پردازیم.

هیچگاه ناآگاهانه آن‌لاین نشوید

اگر نیازی به اینترنت ندارید، اتصال Wi-fi دستگاه خودرا قطع نمایید و علاوه بر آن همواره قابلیت اتصال اتوماتیک به شبکه ها در سیستم خودغیر فعال کنید. این کار عمر باتری را نیز بیشتر می‌کند.

از شبکه مناسب ودرست استفاده کنید

وقتی به شبکه بی‌سیم وصل می‌شوید، ویندوزSSID های (Service set Identifiers) تمام شبکه‌های این مجموعه و محدوده را به شما نشان می‌دهد.

همچنین اطمینان حاصل کنید که به شبکه درست وصل شده‌اید، برای این کار کافی است از متصدی مربوطه در محل نام صحیح کانکشن اصلی شبکه را پرس و جو نمایید. در صورت مشاهده کانکشن های مشکوک حتماً مراتب را به مسئولان گزارش دهید.

به اشتراک گذاری پرینتر و فایل خود را قطع نمایید.

این کار را حتماً صورت دهید؛

درویندوزXP ، از منوی Start وارد My Network Places شوید. در پنجره Network Connections بر روی شبکه راست کلیک کرده و Properties را انتخاب نمایید. در پنجره محاوره پایانی در قسمتGeneral ، گزینه Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks را از حالت انتخاب درآورید و سپس بر روی OK کلیک کنید.

در ویندوز ویستا قابلیت جالبی نهفته است که خود ویندوز در صورت تشخیص نا امنی شبکه، به طور خودکار حالت به اشتراک‌گذاری را لغو و این ویژگی راخاموش و غیرفعال می‌سازد. جهت کنترل و تغییر این حالت از این روش پیروی نمایید:

ابتدا از منوی Start وارد Network شوید، سپس بر روی عبارت Network and Sharing Center را کلیک کنید، اگر کنار نام شبکه عبارت Public network به معنای شبکه عمومی ظاهر شد و شما به شبکه عمومی وصل شدید، فقط باید این پنجره را ببندید چون در معرض دید قرار گرفته‌اید. در غیر این صورت روی کلید Customize را از روی نام شبکه کلیک کنید Public .را انتخاب کرده و روی کلمه Next و سپس روی Close کلیک کنید.

کاری که انجام میدهید ۱ –**نام کاربری و رمز عبور (Admin)خود را تغییر دهید**

هسته مرکزی بیشتر شبکه های خانگی بی سیم, به مسیر یاب ها دسترسی دارند. برای تنظیم این قسمت، شرکت سازنده در داخل دستگاه, صفحه تنظیم اطلاعات را قرار داده است که به کاربر اجازه ورود و تغییر داده ها را می دهد. این ابزار توسط صفحه ورودی حمایت می شود و فقط به کاربر اصلی اجازه ورود می دهد. به هر حال هکرهای اینترنتی به راحتی می توانند به این امکانات دسترسی پیدا کنند. پس فورا این تنظیمات را تغییر دهید.

۲ –**قابلیت پنهان سازی WPA / WEPرا فعال کنید**

تکنولوژی بی سیم تلاش می کند پیغام را به گونه ای ارسال کند که به وسیله سایر دستگاه ها قابل خواندن نباشد. امروزه چنین تکنولوژی برای کپسوله سازی وجود دارد. طبیعتا شما خواستار انتخاب بهترین شکل از کپسوله سازی هستید که بتواند با ساده ترین تنظیمات کار کند. پس برای این کار همه ی ابزار های (wireless) شبکه باید از تنظیمات کپسوله سازی شناخته شده ای استفاده کنند. محبوب ترین آن ها WEP WPA /می باشد که استفاده از آن ها را به شما توصیه می کنیم.

۳ **SSID –پیش فرض را تغییر دهید**

همه نقاط دستیابی/مسیر یاب ها از نام شبکه ای استفاده می کنند که SSID نام دارد و کارخانه ها معمولا محصولاتشان را با SSID یکسان وارد بازار می کنند. برای مثال SSID همه دستگاه های شرکت LINKSYS, به طور عادی <Linksys>قرار داده شده اند. دانستن SSID به تنهایی موجب ورود دیگران به شبکه شما نمی شود ولی برای شروع نقطه ی خوبی است. مهم تر این است که هکر با دیدن SSIDپیش فرض, برای ورود مشتاق تر می شود, چون می داند که شبکه به درستی تنظیم نشده است. پس SSID پیش فرض را تغییر دهید.

۴ –**پخش عمومی SSIDرا خاموش کنید**

در شبکه های بی سیم, نقطه دستیابی یا مسیریاب به طور معمول نام شبکه (SSID) را تا فاصله ای مشخص پخش می کند. این خاصیت برای مشترکانی که در حال حرکت بین خارج و داخل این محدوده هستند, طراحی شده است. در منزل به این ویژگی نیازی نیست و این ویژگی, تعداد افرادی که دوست دارند به شبکه شما وارد شوند را افزایش می دهد. خوشبختانه بسیاری از wireless ها اجازه غیرفعال کردن ویژگی پخش عمومی SSID را به مدیر شبکه می دهد.

۵ -از فیلتر Mac Addressاستفاده کنید

هر قطعه از اجزای ,wireless دارای یک شناسه منحصر به فرد است که آدرس فیزیکی یا Mac Address نام دارد. نقاط دستیابی و مسیریابی Mac Address ,تمام دستگاه هایی که به آن وصل هستند را در خود دارد. توسط این ویژگی می توان MAC Address دستگاه هایی که می خواهیم به شبکه وصل شوند را وارد مودم کنیم و از پس فقط و فقط این دستگاه ها توانایی برقراری ارتباط را دارند. فقط توجه داشته باشید این ویژگی آنقدر که به نظر می رسد قدرتمند نیست و هکر ها به راحتی می توانند Mac Address ها را جعل کنند.

۶ –اتصال خودکار شبکه های Wi-Fiرا باز نکنید

اتصال به شبکه بی سیم باز, مانند شبکه بی سیم رایگان یا مسیریاب همسایه شما، کامپیوترتان را در معرض خطر امنیتی قرار می دهد. هر چند به طور معمول فعال نیست ولی بسیاری از کامپیوتر ها تنظیماتی در دسترس دارند که اجازه می دهد این اتصال بدون اطلاع کاربر اتفاق بیافتد.

۷ -به ابزار ها Static IPاختصاص دهید

بیشتر شبکه های خانگی تمایل به داشتن IP Address های پویا دارند. تکنولوژی DHCP براستی، برای تنظیم کردن راحت است اما متاسفانه این مزیت, ابزاری برای دزدان شبکه می باشد. کسانی که می توانند به راحتی IP Address مجاز را از لیست DHCP شبکه شما بدست آورند. برای حفظ امنیت بیشتر از IP های ثابت استفاده کنید.

۸ –از Firewallاستفاده کنید

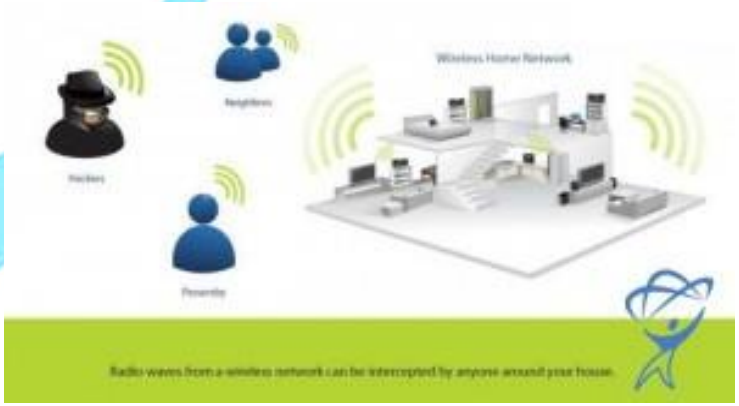
مسیریاب های مدرن دارای Firewall های داخلی هستند اما گزینه هایی برای غیر فعال کردن آنها نیز موجود است. مطمئن شوید که Firewall مسیریاب شما روشن است. دیوار آتش از ورود غیر مجاز جلوگیری می کند و در صورت صحیح بودن کلیه تنظیمات, می تواند بسیاری از درخواست های آلوده را شناسایی کند.

۹ –مسیریاب یا نقطه دستیابی را در مکانی امن قرار دهید

سیگنال های Wireless معمولا به خارج از خانه می رسند. نشت میزان کمی از سیگنال ها به بیرون مشکلی ندارد اما دسترسی بیشتر به این سیگنال ها کار را برای ردیابی و بهره برداری دیگران آسان می کند. موقعیت مسیریاب/نقطه دسترسی تعیین کننده ی این دسترسی می باشد. در ساده ترین حالت, دستگاه مرکز یک دایره می باشد و داده ها را توسط امواج به صورت دایره ای شکل ارسال می کند. پس بهتر است مودم در قسمت های مرکزی خانه قرار دهیم.

۱۰ –شبکه را در دوره ی طولانی بی استفاده, خاموش کنید

اقدام نهایی برای امنیت wireless ها, خاموش کردن دستگاه در مدت زمانی (طولانی) است که از آن استفاده نمی کنید. برای مثال اگر قصد سفر دارید, بهتر است دستگاه را خاموش کنید تا از نفوذ هکرها جلوگیری نمایید.



پنج اشتباه متداول درباره امنیت شبکه های بیسیم

ظهور شاخه های جدید فناوری بیسیم، تعداد شرکتهایی که با استفاده از روشهای نامناسب تأمین امنیت، سیستمهای خود را در معرض خطر قرار میدهند، باورکردنی نیست. به نظر میرسد، اغلب شرکتهای دارای LANبیسیم، به واسطه شناسایی نقاط دسترسی غیرمعتبر که ابزارها را به طور رایگان مورداستفاده قرار میدهند، به دنبال احراز شرایط استاندارد PCI هستند. با هدف آگاهی کاربران از آخرین ضعف های

امنیتی (و البته بعضی از شکافهای امنیتی قدیمی) تصمیم گرفتیم، فهرستی از پنج اشتباه متداول را در تأمین امنیت شبکه های بیسیم در این مقاله ارائه کنیم. شناسایی این اشتباهها حاصل تجربه های شخصی در جریان آزمون و ایمن سازی شبکه های مشتریان است.

.۱دیواره آتش= تأمین امنیت کامل در برابر ورود غیرمجاز به شبکه

اغلب سازمانها، شبکه های بیسیم را به عنوان بخش مکملی برای شبکه سیمی خود راه اندازی میکنند. اتصال بیسیم، یك رسانه فیزیکی است و برای تأمین امنیت آن نمی توان تنها به وجود یك دیوار آتش تکیه کرد. کاملاً واضح است که نقاط دسترسی غیرمجاز، به واسطه ایجاد راه های ورود مخفی به شبکه و مشکل بودن تعیین موقعیت فیزیکی آنها، نوعی تهدید علیه شبکه به شمار میروند. علاوه براین نقاط دسترسی، باید نگران لپتاپهای بیسیم متصل به شبکه سیمی خود نیز باشید. یافتن لپتاپهای متصل به شبکه سیمی که یك کارت شبکه بیسیم فعال دارند، اقدامی متداول برای ورود به شبکه محسوب میشود. در اغلب موارد این لپتاپها توسط SSID شبکه هایی را که قبلاً مورد دسترسی قرار دادهاند، جست وجو میکنند و در صورت یافتن آنها صرفنظر از این که اتصال به شبکه قانونی یا مضر باشد یا شبکه بیسیم در همسایگی شبکه فعلی قرار داشته باشد، به طور خودکار به آن وصل میشوند. به محض اینکه لپتاپ به یك شبکه مضر متصل شود، مهاجمان آن را مورد حمله قرار داده و پس از اسکن و یافتن نقاط ضعف ممکن است کنترل آن را به دست گرفته و به عنوان میزبانی برای اجرای حمله ها به کار گیرند. در این شرایط علاوه بر افشای اطلاعات مهم لپتاپ، مهاجم میتواند از آن به عنوان نقطه شروعی برای حمله به شبکه سیمی استفاده کند. مهاجم درصورت انجام چنین اقداماتی، به طور کامل از دیواره آتش شبکه عبور میکند.

ما امنیت شبکه های معتبر و غیرمعتبر را ارزیابی کرده ایم و به این نتیجه رسیدیم که اغلب سازمانها دیواره آتش شبکه را به گونهای تنظیم میکنند که از آنها در برابر حمله های مبتنی بر اینترنت محافظت میکند، اما امنیت شبکه در مقابل خروج از شبکه (Extrusion) و خروج غیرمجاز اطلاعات (leakage) تأمین نمیشود. اصولاً زمانی که درباره خروج غیرمجاز اطلاعات صحبت میکنیم، منظورمان خروج اطلاعات از شبکه است.

بسیاری از سازمانها تنظیمات دیواره آتش را برای کنترل ترافیك اطلاعات خروجی به درستی انجام نمیدهند. در نتیجه این سهل انگاری معمولاً اطلاعات محرمانه سازمان به خارج منتقل میشود. به عنوان مثال، یکی از متداولترین مواردی که هنگام انجام آزمونهای امنیتی با آن مواجه شدیم، خروج اطلاعات شبکه سیمی از طریق نقاط دسترسی بیسیم بود. در این آزمونها با استفاده از یك نرم افزار ردیاب (Sniffer) بیسیم توانستیم حجم زیادی از ترافیك اطلاعات خروجی ناخواسته را شناسایی کنیم. این اطلاعات شامل دادههای مربوط به STP سرنام IGRP ، Speaning TreeProtocol)سایر سرویس های شبکه و حتی در مواردی اطلاعات مربوط به NetBIOS بودند.

چنین نقطه ضعفی شبکه را به یك اسباب سرگرمی برای مهاجم تبدیل میکند. در حقیقت، نفوذ به چنین شبکهای حتی نیازمند یك اسکن فعال یا حمله واقعی نیست. بهواسطه ردیابی جریان اطلاعاتی یك شبکه بیسیم علاوه بر شناسایی توپولوژی بخش سیمی آن میتوان اطلاعات مربوط به تجهیزات حیاتی شبکه و حتی گاهی اطلاعات مربوط به حسابهای کاربری را بهدست آورد.

۲. دیواره آتش= تأمین امنیت کامل در برابر ورود غیرمجاز به شبکه

این تصور اشتباه، بسیار گیج کننده است. چگونه میتوان بدون اسکن شبکه از نبود تجهیزات بیسیم در آن مطمئن شد؟! در محلهایی که شبکه های LAN بیسیم راه اندازی نشده اند، علاوه بر نقاط دسترسی غیرمجاز، میتوان از شبکه هایAd-Hoc ، دسترسی تصادفی لپتاپها و ایجاد پلهای ارتباطی با شبکه، به عنوان تهدیدات بالقوه برای امنیت شبکه نام برد. دسترسی تصادفی لپتاپهای بیسیم یك خطر امنیتی برای صاحبان این لپتاپها محسوب میشود. اگر شرکت مجاور شما از یك نقطه دسترسی بیسیم یا یك شبکه Ad-Hoc استفاده میکند، احتمال اتصال تصادفی لپتاپهای بیسیم عضو شبکه شما به این شبکه های بیسیم زیاد است. این اتصال نوعی خروج از شبکه است. مهاجمان نحوه بهره برداری از این شرایط را به خوبی میدانند و در نتیجه میتوانند از یك نقطه دسترسی نرم افزاری یا) Soft AP نرم افزاری که از روی یك لپتاپ اجرا میشود) برای ارسال شناسه های SSID موجود روی لپتاپ به یك کامپیوتر خارج از شبکه و حتی ارسال آدرس IP لپتاپ برای کامپیوتر خارجی استفاده کنند. چنان که گفته شد، این نقطه ضعف امکان کنترل لپتاپ و حمله به شبکه سیمی را برای مهاجمان فراهم میکند. به علاوه، مهاجمان میتوانند از طریق لپتاپ، حمله های) MITM سرنام (Man In The Middle یا سرقت هویت را به اجرا درآورند.

۳. اسکن دستی= شناسایی تمام نقاط دسترسی غیرمجاز

در این مورد، تلاش مدیران شبکه برای اتخاذ یك رویکرد پیشگیرانه به منظور شناسایی نقاط دسترسی غیرمجاز در شبکه قابل تقدیر است. اما متأسفانه ابزارهایی که در اختیار این افراد قرار دارد، کارایی لازم را برای شناسایی نقاط دسترسی غیرمجاز ندارد. به عنوان مثال، بسیاری از مدیران شبکه از ابزارهای مدیریتی اسکن نقاط ضعف شبکه های سیمی به منظور شناسایی نقاط دسترسی غیرمجاز متصل به شبکه استفاده میکنند. تجربهکاری نگارنده با ابزارهای اسکن نقاط ضعف از هر دو نوع اپن سورس و تجاری، بیانگر این است که اغلب مدیران شبکه با تعداد انگشت شماری نقطه دسترسی مواجه میشوند که توسط سیستم عامل شناسایی شده است و هنگامی که شبکه را اسکن میکنند، این تجهیزات در قالب یك سیستم مبتنی بر لینوکس همراه یك وب سرور شناسایی میشوند. هنگام اسکن شبکه های Class C و بزرگتر، دستگاههای غیرمجاز بین سایر تجهیزات شبکه پنهان شده و نتایج حاصل از اسکن شبکه برای شناسایی نقاط دسترسی غیرمجاز حقیقی نیست.

کارکرد ابزارهای اسکن بیسیم مانند NetStumbler و Kismet بسیار خوب است، اما زمانی که نوبت به شناسایی نقاط دسترسی غیرمجاز میرسد، این ابزارها از کارایی لازم برخوردار نیستند. به عنوان نمونه این ابزارها نمیتوانند مشخص کنند که نقاط دسترسی شناسایی شده واقعاً به شبکه شما متصل هستند یا خیر. علاوه براین، در تعیین موقعیت تقریبی دستگاه بیسیم مشکوك نیز دچار مشکل میشوند. اگر شرکت شما در یك ساختمان چندطبقه یا یك برج قراردارد، باید امواج دریافتی آنتن های بزرگ و دستگاههای منتشرکننده سیگنال را نیز به این مشکلات بیافزایید. در چنین شرایطی یك مدیر شبکه با مهارت متوسط در ردگیری و شناسایی تجهیزات بیسیم شبکه با مشکلات بزرگی روبه رو خواهد شد.

٤. به روزرسانی تمام نقاط دسترسی به منظور حذف پروتکل WEP= تأمین امنیت کامل شبکه

پروتکل WEP سالیان دراز مورد حمله مهاجمان قرار گرفته است. علاوه براین، براساس اعلان PCI پروتکل WEP باید تا ماه ژوئن سال ۲۰۱۰ به طور کامل کنار گذاشته شود. بعضی از شرکتها نیز به سراغ روشهای توانمندتر کدگذاری و اعتبارسنجی رفته اند.

برای جایگزینی این پروتکل، چندگزینه مختلف وجود دارد. متأسفانه بعضی از این گزینه ها نیز دارای نقاط ضعف هستند. بعنوان مثال، نسخه PSK (Pre-Shared Key سرنام) از پروتکل WPA به دلیل نیاز به انتشار اطلاعات موردنیاز برای ساخت و تأیید کلید رمزگشایی اطلاعات، در مقابل نوعی حمله Offline که روی واژه نامه آن انجام میشود، آسیب پذیر است. برای اجرای این حمله ها چندین ابزار مختلف شامل coWPAtty و aircrack-ng وجود دارد. اغلب حمله ها شامل گردآوری تعداد زیادی از بسته های اطلاعاتی و استفاده از ابزار درمقابل سیستم دریافت بسته های اطلاعاتی است. بسته نرم افزاری Backtrack ۳تمام ابزارهای لازم را برای اجرای این نوع حمله ها فراهم میکند. در نوامبر سال ۲۰۰۸ به منظور اثبات این ضعف، پروتکل TKIP هک شد.

در این حمله صرفنظر از به کارگیری سیستم اعتبار سنجی PSK یا ۸۰۲,۱ xمهاجمان توانستند به تمام نسخه های پروتکل TKIP شامل WPA و WPA۲ نفوذ کنند. با وجود این،کلیدهای TKIP شناسایی نشدند و در نتیجه محتوای تمام قابهای کدشده افشا نشد. یك حمله میتواند در هر دقیقه یك بایت از داده های یك بسته اطلاعاتی رمزنگاری شده را افشا کرده و به ازای هر بسته کدگشایی شده تا پانزده قاب رمزنگاری شده را به سیستم تحمیل میکند. چنین سیستمی، یك گزینه مناسب برای آلودگی ARP محسوب میشود. درك این نکته ضروری است که آن دسته از شبکه های WPA و WPA۲ که الگوریتمهای کدگذاری AES-CCMP پیچیده تر را مورد استفاده قرار میدهند، در برابر حمله ها مقاومتر هستند و استفاده از چنین الگوریتمهایی به عنوان بهترین رویکرد تدافعی پیشنهاد میشود.

اگر هیچ گزینه دیگری به غیر از راه اندازی یك سیستم WPA-PSK پیش رو ندارید، از یك کلمه عبور بسیار مطمئن که حداقل هشت کاراکتر دارد، استفاده کنید. کلمه عبور پیچیده‌ای که از شش کاراکتر تشکیل شده باشد، به طور متوسط ظرف سیزده روز کشف میشود.

۵.استفاده از نرم افزار کلاینت VPN = محافظت از کارمندان سیار

با وجود این که استفاده از برنامه کلاینت VPN همراه یك دیواره آتش نخستین گام برای حفاظت از کارمندان سیار به شمار می رود، تعداد بسیاری از نقاط ضعف چنین ارتباطی بدون محافظت باقی می ماند. کاربرانی که در حال مسافرت هستند، به ناچار در هتل ها، کافی شاپ ها و فرودگاه ها از شبکه های وای فای استفاده می کنند.

ابزارهایی مانند Hotspotter که در بسته نرم افزاری BackTrack در اختیار همگان قرار می گیرند، برای مهاجم امکان ایجاد یك ناحیه خطرناك را فراهم می کنند که اغلب توسط شبکه به عنوان یك ناحیه خطرناك مجاز شناخته می شود. این فرآیند شامل ایجاد یك نقطه دسترسی جعلی با استفاده از یك شناسه SSID متداول و همچنین صفحات وب شبیه به یك ناحیه خطرناك واقعی است. سپس مهاجم منتظر اتصال کاربران بی اطلاع، به نقطه دسترسی جعلی شده و با استفاده از پروتکل DHCP برای آن ها یك آدرس IP و یك صفحه وب ایجاد می کند. به این ترتیب، کاربر فریب خورده و به منظور ورود به ناحیه خطرناك

اعتبارنامه خود را در اختیار مهاجم قرار می دهد. در بعضی موارد مهاجم حتی دسترسی کاربران به اینترنت را امکان پذیر کرده و به این ترتیب برای اجرای حمله های MITM و سرقت سایر اطلاعات مهم کاربران مانند شناسه و کلمه عبور و شماره حساب بانکی آن ها اقدام می کند.

حفاظت از کارمندان سیار به ویژه در برابر این نوع حمله ها، اقدامی چالش برانگیز بوده و علاوه بر استفاده از نرم افزار کلاینت VPN و دیواره آتش نیازمند تمهیدات امنیتی دیگری است. البته، هیچ یك از این اقدامات به طور کامل از کاربر محافظت نمی کند، اما خطرات امنیتی را کاهش می دهند. مدیران شبکه های مبتنی بر ویندوز با استفاده از گزینه Access point (infrastructure) networks only می توانند از اتصال کاربران به شبکه های Ad-Hoc جلوگیری می کنند.

بسیاری از ابزارهای مهاجمان که برای شبیه سازی عملکرد نقاط دسترسی به کارگرفته می شوند، در حقیقت، شبکه های Ad-Hock را شبیه سازی می کنند. غیرفعال کردن گزینه مذکور در سیستم عامل ویندوز می تواند از کاربران در برابر چنین حمله هایی محافظت کند. به علاوه، غیرفعال کردن گزینه Any Available Network (Access Point Preferred) نیز از بروز چنین حملاتی جلوگیری می کند. سرانجام، با غیرفعال کردن گزینه AutomaticallyConnect to Non-Preferred networks نیز می توان از اتصال تصادفی کاربران به شبکه های Ad-Hock جلوگیری کرد.