داده پردازی فن آوا

بسمه تعالی

سیستم مدیریت کیفیت

راهنمای تشریح راهکارهای بهبود امنیت شبکه خانگی

سطح محرمانگی: عمومی ■ داخلی □ محرمانه □

تهیه کننده:	تایید کننده:
واحد تضمین کیفیت	مدیر امور مشترکین
کدسند: SD-GL-06	تاریخ تهیه اولیه: ۱۳۹۵/۰۹/۰۶

جدول شرح تغییرات راهنما

ردیف	شماره اصلاحیه / شماره ویرایش فعلی	تاریخ ویرایش	شرح تغییر	منشاء ویرایش

استفاده از رمزنگاری(Encryption)

امنیت وایرلس مودم خود را فعال کنید (wireless security) رمزنگاری WEP (Wired Equivalent Privacy) قدیمی ترین و ضعیف ترین مدل رمزنگاری است. به جای آن از WPA (Wi-Fi Protected Access) و WPA-2 که از بهترین مدل های رمزنگاری هستند، استفاده کنید.

Firmware مودم را به روز کنید.

همه مودم ها تراشه فقط خواندنی دارند (read-only chip) که توسط شرکت سازنده آن قابل به روز شدن است. شرکت سازنده مودم ها معمولا firmware محصول خود را به روز می کنند تا کارایی آن را افزایش داده و باگ ها و ایرادات امنیتی را رفع کنند. بنابراین بهتر است firmwareمودم خود را به روز نگه دارید .برای دریافت بسته به روزرسانی firmware به وب سایت شرکت سازنده آن محصول بروید.

رمز عبور ادمین را عوض کنید.

هر مودمی یک رمز عبور پیش فرض دارد که برای دسترسی به تنظیمات آن مورد استفاده قرار می گیرد. بیشتر ویزاردهای نصب و راه اندازی مودم شما را مجبور به عوض کردن آن می کنند اما نه همه آنها. در هر صورت رمز عبور را عوض کنید تا مانع از هک شدن سریع و آسان مودم خود شوید.

به تنظیمات پیش فرض برگردید.

اگر رمز عبور مودم خود را فراموش کردید می توانید برای رهایی از این مشکل مودم خود را به حالت پیش فرض برگردانید. این کار با نگه داشتن دکمه Reset Factory به مدت ۳۰ ثانیه قابل انجام است ضمن اینکه بعد از ریست کردن به حالت پیش فرض و به منظور دسترسی به تنظیمات مودم نیاز به نام کاربری و رمز عبور پیش فرض مودم دارید که هر دو آن را می توانید دردفترچه راهنمای مودم بدست بیاورید.

SSID Broadcast را غیر فعال کنید.

وقتی SSID Broadcast فعال است مودم اسم وایرلس - اسم شبکه - را پخش می کند. (SSID) که به همسایگان اجازه می دهد تا شبکه شما را ببینند و شاید هم اقدام به دسترسی به آن نمایند. برای جلوگیری از این موضوع broadcasting را غیر فعال کنید تا باعث شود SSID شما مخفی بماند. در این صورت برای دسترسی به وایرلس خود به قسمت unnamed network رفته و SSID شبکه خود را وارد کنید.

SSID پیش فرض مودم را عوض کنید.

SSID پیش فرض مودم برای مثال (Linksys) راعوض کنید . وقتی آن را به حال خود رها می کنید به مردم دنیا اعلام می کنید که مودم خود را از نظر امنیتی پیکر بندی نکرده اید و هکر ها را طلب می کنید.

با MAC address فیلتر کنید.

هر یک از تجهیزات شبکه دارای اثر انگشتی به نام MAC است. می توانید مودم خود را با استفاده از MAC طوری فیلتر کنید که فقط کامپیوترهای شما بتوانند به شبکه وصل شوند. اکثر مودم ها، کامپیوتر ها و اسمارت فون هایی را که به شبکه شما وصل هستند را نشان می دهند. با اضافه کردن MAC آن ها دسترسی غیرمجاز دیگر سیستم ها را به مودم قطع می کنید.

تعداد کلاینت های DHCP را کم کنید.

اکثر کاربران از مودم خود به عنوان سرور DHCP استفاده می کنند وقتی کاربران وصل می شوند مودم به صورت خودکار یک آدرس IP به هر یک از آنها اختصاص می دهد. با کم کردن تعداد IP های موجود (به تعداد کلاینت های موجود در خانه) باعث می شوید نفر دیگری نتواند خود را به شبکه تحمیل کند.

استفاده از فایروال مودم

دو امکانی که باعث می شود فایروال های سخت افزای از نوع نرم افزاری قدرتمند باشند SPI وNATSPI محتوای بسته ها را مورد آزمایش قرار داده و بعد از آن دسترسی لازم را می دهد و NAT نیز کامپیوترهای وصل شده به مودم را از دسترسی از خارج شبکه مصون نگه می دارد.

مراقب WPS باشید.

WPS امکانی است که به کاربران اجازه می‌دهد برای اتصال به شبکه بی‌سیم از تولید یک کد ساده اما موقت استفاده کنند یا اینکه با فشردن یک دکمه روی مسیریاب، با لپ‌تاپ، تبلت یا موبایل به شبکه متصل شوند. بدین ترتیب اگر کسی به صورت فیزیکی به مودم دسترسی داشته باشد، به صورت بالقوه امکان متصل‌شدن به شبکه را دارد؛ اگر دستگاه کد موقت ساده تولید کند هم، با توجه به ساده بودن کد، امکان شکستن آن با شیوه‌های ساده هک وجود دارد.