ترفند ویندوز

اندازه گیری مصرف اینترنت در ویندوز

یکی از مواردی که کاربران اینترنت همیشه مدنظر دارند، میزان ترافیک مصرفی آن‌ها در طول دوره است. این مسأله به کاربران کمک می‌کند که مدیریت بهتری بر ترافیک مصرفی و هزینه‌های خود داشته باشند. این کار نیز معمولاً به کمک نرم‌افزارهای متفاوتی که در دسترس هستند انجام می‌شود. اما ویندوز در این مورد حرف‌هایی برای گفتن دارد و شما در این سیستم‌عامل می‌توانید یک کانکشن وای‌فای را به عنوان محاسبه‌گر میزان ترافیک معرفی کنید. یکی از امکانات جدید ویندوز ، اتصال بی‌سیم با قابلیت محاسبه ترافیک است. در گذشته، شما قادر بودید با اجرای نرم‌افزارهای ویندوزی، میزان ترافیک مصرفی خود را مانیتور کنید. اما این نرم‌افزارها کار مؤثری برای کاهش ترافیک مصرفی انجام نمی‌دادند. با گسترش هات‌اسپات‌های همراه، اینترنت‌های بی‌سیم رو به افزایش بوده و دوره ترافیک‌های نامحدود رو به انقراض است. برای همین هر کیلوبایتی که صرفه‌جویی شود در حقیقت به جیب شما کمک کرده است برای فعال‌سازی سنجش‌گر، به لیست شبکه‌های وای‌فای بروید و بر روی کانکشن مورد نظر خود راست‌کلیک کنید. در تبلت به جای راست‌کلیک، باید انگشت خود را مدتی بر روی کانکشن نگه دارید. بعد از نمایش منو، گزینه Set as metered connection را انتخاب کنید.

غیرفعال‌سازی مصرف ترافیک در اتصال سنجش‌گر

دو تنظیم متفاوت برای کاهش ترافیک مصرفی در قابلیت تنظیم ترافیک مصرفی وجود دارد. تنظیم اول مربوط به دانلود نرم‌افزارهای دستگاه است.

برای ورود به این بخش از Settings به Change PC Settings رفته و Devices را انتخاب کرده و در این قسمت، وضعیت ویژگی Download over metered connection را در حالت Off قرار دهید.

دومین تنظیم به همگام‌سازی برمی‌گردد.

برای این تنظیم از Settings به Change PC settings و سپس به Sync your settings بروید و مطمئن شوید هر دو ویژگی Sync setting over metered connection و Sync settings over metered connection even i'm roaming در حالت Off هستند.

بررسی دیتای مصرفی

برای مشاهده میزان ترافیک مصرفی، به لیست شبکه‌های دستگاه بازگردید و بر روی اتصال مورد نظرتان کلیک کنید. متأسفانه امکانی برای ریست خودکار شمارنده حجم ترافیک مصرفی وجود ندارد اما شما می‌توانید به صورت دستی و در ابتدای دوره و با کلیک روی کلید Reset، شمارنده را صفر کنید.

با گسترش شبکه‌های ارتباطی و دستگاه‌های متصل به این شبکه و شکل گیری آنچه به آن اینترنت اشیاء(Internet of Things) گفته می‌شود، نیاز به رویکردی کاملا بدیع برای امنیت(Security) شبکه‌ها و محافظت(Protect) از خدمات اصلی این شبکه‌ها نسبت به حملات سایبری(Cyberattack) بیش از پیش احساس می‌شود. در واقع با اتصال یک قطعه/دستگاه به یک شبکه، حمله کنندگان سایبری مسیری برای حمله می‌یابند. اگر امنیت در طراحی این دستگاه‌های تعبیه شده یا دستگاه‌های نهفته (embedded de-vices)- دستگاه‌هایی هستند که خود سیستمی دارند که برای هدفی خاص و با قابلیت پردازش محدود طراحی شده است که به آنها در مواردی سامانه‌های نهفته(embedded systems) نیز می‌گویند- تامین نشود، زیرساخت‌های(Infrastructure) حیاتی این شبکه در خطر هستند. به بیان دیگر زیرساخت‌های حیاتی هر شبکه‌ای همان نظارت لحظه‌ای(Real-time) که دستگاه‌های فیزیکی دارند را نیز نیاز دارند. برای مثال یک سد را در نظر بگیرید، رایانه‌هایی وجود دارند که مستمرا دستگاه‌ها و قطعات فیزیکی این سیستم را نظارت می‌کنند اما هیچ سیستم نظارتی برای نظارت لحظه‌ای بر این شبکه نظارت وجود ندارد. با شکل گیری مفهوم اینترنت اشیا، شبکه‌ها در همه جا گسترده شده‌اند؛ از دستگاه‌های تعبیه شده، ریزرایانه‌ها، دستگاه‌های خودپرداز و چراغ‌های راهنمایی گرفته تا زنگ در و سیستم روشنایی خانه‌ها. پیش از این دستگاه‌های(تعبیه شده) هوش و قابلیت اتصال به شبکه(اینترنت) را نداشتند، اما امروزه همه چیز تغییر کرده است، در حال حاضر آنها به عنوان حسگرهای بی سیم و عناصر شبکه‌ای هستند برای امنیت فیزیکی برای مثال حسگرهایی که به متصدیان یک ساختمان در خصوص حرکت‌های صورت گرفته در آنجا هشدار می‌دهند. طبق تحقیقات موسسه گارتنر تا سال ۲۰۲۰ میلادی بیش از ۲۰۸ میلیون دستگاه متصل به شبکه وجود خواهند داشت. همچنین این موسسه تحقیقاتی مدعی است که تا این سال بیش از نیمی از کسب و کارها به نوعی از فناوری اینترنت اشیا بهره می‌گیرند که محافظت از این دستگاه‌های متصل به شبکه اینترنت اشیا تا ۲۰٪ از بودجه سالانه امنیتی آنها را شکل می‌دهد. از آنجایی که این دستگاه‌های تعبیه شده بسیار تخصصی هستند و غالبا نیازمند مهارت‌های برنامه نویسی و سخت افزاری خاصی هستند، محافظت از این دستگاه‌ها خود یک چالش است. اگر از این سیستم متشکل از چند قطعه و دستگاه به خوبی محافظت نشود، هر کدام از اجزای آن می‌توانند مسیری برای حمله باشند. نمونه‌ای از این حملات را ما در سال ۲۰۰۹ میلادی در حمله به تاسیسات اتمی ایران با ویروس استاکس نت دیدیم. در حالیکه رایانه‌ها و شبکه‌های قدیمی دامنه گسترده‌ای از راهکارهای امنیتی را در اختیار داشتند که می‌توان یکی از آنها را انتخاب کرد، در فضای اینترنت اشیا چنین گزینه‌ای وجود ندارد. در اینجا استفاده از برنامه‌های ویروس کش(Antivirus) سنتی روی این دستگاه‌ها با قدرت کم به تنهایی به کار نمی‌آید یا ممکن است صورت دستگاه را کم کرده و عملکرد مطلوب آن را نداشته باشد. در واقع بسیاری از این دستگاه‌ها با هدف کاهش چرخه پردازش و مصرف حافظه تعبیه شده‌اند که استفاده ویروس کش‌ها خود به این کار لطمه می زند. در حال حاضر چالشی که متخصصان امنیت دارند این است که با زیاد بودن بورد شبکه وای فای، ترافیک زیاد شبکه، این شبکه و اجزای آن برق زیادی مصرف می‌کنند که حاصل آن کوتاه آمدن در زمینه امنیت می‌شود، زیراکه استفاده از ابزارهای امنیتی در مصرف انرژی توسط شبکه و اجزای آن که بیشتر شبکه موبایل یا بی سیم هستند، تاثیر می‌گذارد. به بیان ساده‌تر چالش فعالان حوزه اینترنت اشیا و امنیت آن این است که دستگاه‌های به کار برده شده در این فضا را با قیمتی معقول و در مدت زمانی مناسب با امنیت معقول و مناسب به بازار ارائه دهند. تلاش برای عبور از چالش امنیت کار ساده‌ای برای توسعه دهندگان فعال در فضای اینترنت اشیا نیست. اخیرا تلاش‌های زیادی به منظور ایجاد استانداردهای امنیتی برای اینترنت اشیا توسط متخصصان بزرگ امنیت مانند شرکت سیمانتک(Symantec) و AMR انجام شده است. اما حقیقت این است که با توجه به وجود تعداد زیادی دستگاه متصل به شبکه‌ها در حال حاضر، این فعالیت‌ها را می‌توان کم و دیر قلمداد کرد. رویکردهای گسترده امنیتی به منظور حفاظت از شبکه بطور کلی وجود دارند، اگر اجزای این شبکه مانند دستگاه‌های تعبیه شده نتوانند از خود محافظت کنند. روش‌های داده محور(data-centric) مانند یادگیری ماشینی (Machine Learning) می‌توانند پلی بین راهکارهای سنتی امنیتی، اینترنت اشیا، رایانش ابری و فناوری‌های شبکه باشند. مسئله امنیت دستگاه‌های تعبیه شده هیچگاه به آسانی تامین نمی‌شود. اما با افزایش اهمیت امنیت در مراحل توسعه‌ای و استفاده از تحلیل داده‌ها(analytics) به منظور نظارت بر دستگاه‌ها و حفاظت از شبکه‌ای که دستگاه‌ها در آن قرار گرفته‌اند برای جلوگیری از نفوذ حمله کنندگان به دستگاه‌های کم توان ضروری است تا به اهداف حیاتی‌تر و مهمتر برسند. باید توجه داشت که رویکرد استاندارد و ثابتی برای محافظت از دستگاه‌های تعبیه شده وجود ندارند. عناصر زیادی برای ایجاد محیط قابل اتکای اینترنت اشیاء باید با هم کار کنند.