اتخاذ رویکردی منطقی به منظور مقابله با هکرها

5 باور اشتباه پیرامون بهبود امنیت وای‌فای

فناوری وای‌فای در سال‌های اخیر پیشرفت‌های فراوانی داشته و به‌موازات این پیشرفت‌ها راهکارهای ایمن‌سازی شبکه‌های وای‌فای نیز پیشرفت کرده‌اند. درحالی‌که رویکردهای ایمن‌سازی متنوعی برای دفاع از شبکه‌های وای‌فای در برابر هکرها وجود دارد، اما واقعیت این است که برخی از راهکارهایی که ممکن است از طریق یک جست‌وجوی ساده اینترنتی آن‌ها را پیدا کنید نه تنها سود چندانی ندارند، بلکه ممکن است در برخی موارد دردسرهای مضاعفی برای شما به همراه آورند. با توجه به این‌که امروزه بیشتر کاربران از وای‌فای برای دسترسی به اینترنت و فضای مجازی استفاده می‌کنند در این نوشتار تصمیم گرفتیم، به بررسی پنج باور یا به عبارت دقیق‌تر افسانه‌ای بپردازیم که پیرامون ایمن‌سازی شبکه‌های وای‌فای وجود دارند اما در عمل از وای‌فای شما در برابر نفوذ هکری محافظت نمی‌کنند.

امروزه، بیشتر سازمان‌ها و کسب‌وکارها برای انجام فعالیت‌های تجاری‌شان، شبکه بی‌سیم خاص خود را پیاده‌سازی می‌کنند. کمتر هتل یا کافی‌شاپی را پیدا می‌کنید که فاقد یک شبکه وای‌فای باشد. اگر در نظر دارید، از شبکه وای‌فای برای انجام کارهای تجاری در شرایطی استفاده کنید که شرکت شما دپارتمانی موسوم به فناوری اطلاعات را ندارد، کار چندان پیچیده‌ای پیش رو ندارید. اما اگر در نظر دارید در محل کار خود یک اکسس پوینت ایجاد کنید تا کارمندان به آن متصل شوند و سعی کنید از پارامترهای پیش‌فرض برای این منظور استفاده کنید، آنگاه کسب‌وکار شما در معرض چالش جدی قرار می‌گیرد. پژوهشی که از سوی سایت nakedsecurity انجام‌شده و شهرهای مختلف جهان مانند لندن، نیویورک، واشنگتن و سان‌فرانسیسکو را مورد بررسی قرار داده نشان می‌دهد، بیشتر کسب‌وکارهای واقع در این شهرها از وای‌فای غیر ایمن استفاده می‌کنند. در واقع بیشتر کسب‌وکارها از رویکردهای امنیتی تاریخ‌مصرف گذشته و البته نادرستی استفاده می‌کنند که هیچ‌گونه امنیتی را برای آن‌ها به ارمغان نمی‌آورد. در این پژوهش آمده، در شهر لندن تنها 17 درصد هات‌اسپات‌های وای‌فای از پیکربندی WPA2 برای رمزنگاری ترافیک شبکه بی‌سیم خود استفاده کرده‌اند و نزدیک به یک‌چهارم هات‌اسپات‌ها در اصل شبکه‌های وای‌فای باز هستند که بدون هیچ‌گونه الگوریتم رمزنگاری مورداستفاده قرار می‌گیرند. همچنین اغلب این شبکه‌های وای‌فای از نام شبکه (SSID) پیش‌فرض در تعامل با نام کاربری و گذرواژه پیش‌فرض استفاده کرده‌اند. اما برای آن‌که بتوانید یک شبکه وای‌فای ایمن را پیاده‌سازی کنید، ابتدا باید با یکسری باورهای اشتباه در زمینه **امنیت شبکه** آشنا شوید. باورهایی که تنها باعث گمراهی‌تان می‌شوند.

باور اشتباه یک؛

پنهان‌سازی نام شبکه SSID

هر روتر یا اکسس پوینت بی‌سیمی یک نام شبکه دارد. نامی که از سوی کاربر تعیین‌شده است. به این نام شبکه

SSID گفته می‌شود. در حالت پیش‌فرض روترها SSID خاص خود را برای همه دستگاه‌ها و کاربرانی که در محدوده تحت پوشش قرار دارند، ارسال می‌کنند تا دستگاه‌ها بتوانند به روترها متصل شوند. بسیاری بر این باورند که اگر SSID مربوط به روتری را از دید دستگاه‌ها و کاربران پنهان ساخت به این شکل می‌توان از شبکه در برابر

ها محافظت کرد. در ظاهر به نظر می‌رسد، این ایده خوب کار می‌کند. اما واقعیت این است که دستگاه‌های مجهز به سیستم‌عامل‌های مدرن همچون ویندوز 10 به‌خوبی می‌توانند همه شبکه‌های موجود را کشف کنند، حتی اگر این توانایی را نداشته باشند تا نام هر شبکه را به شکل متمایز از دیگری نشان دهند. همچنین پیداکردن یک SSID پنهان‌شده کار پیچیده‌ای نیست و به‌سادگی انجام می‌شود. در حقیقت، اگر سعی کنید SSID شبکه خود را پنهان سازید، شک و تردید هکرها را بیشتر کرده‌اید و آن‌ها احساس می‌کنند که شبکه وای‌فای شما اطلاعات حساسی دارد که پنهان‌شده است. شاید بتوانید مانع از آن شوید تا روترتان SSID را ارسال کند، اما این توانایی را ندارید تا از ارسال اطلاعات یادشده در قالب بسته‌های داده‌ای، درخواست‌های ارتباط یا برقراری ارتباط مجدد و.... ممانعت به عمل آورید. یک ابزار تحلیلگر شبکه‌های بی‌سیم شبیه Kismet یا CommView for Wifi به‌راحتی قادر است SSID مربوط به شبکه‌های پنهان را به‌سرعت شناسایی کند. در بهترین حالت پنهان‌سازی ارسال نام شبکه از شما در برابر کاربران معمولی محافظت می‌کند، اما در مقابل نفوذگران حرفه‌ای هیچ کمکی به شما نمی‌کند.

مطلب پیشنهادی

نظارت بر شبکه وای‌فای
چگونه می‌توانیم دستگاه‌های متصل به شبکه وای‌فای را پیدا کنیم؟

باور اشتباه دو؛

فعال کردن فیلتر مربوط به مک آدرس

همه دستگاه‌های موجود در شبکه یک آدرس مک منحصربه‌فردی دارند که برای شناسایی دستگاه‌ها استفاده می‌شود. یک آدرس مک، مشتمل بر حروف و اعدادی است که از طریق کاراکتر : از یکدیگر تفکیک‌شده است.
D1:1A:2D:12:00:02 نمونه‌ای از یک آدرس مک است. دستگاه‌هایی که درون یک شبکه قرار دارند برای ارسال یا دریافت داده‌ها در یک شبکه و شناسایی یکدیگر از مک آدرس استفاده می‌کنند. اشتباه بزرگی که بسیاری از کاربران انجام می‌دهند این است که تصور می‌کنند اگر روتر خود را به‌گونه‌ای پیکربندی کنند که تنها به دستگاه‌هایی با آدرس مک خاص اجازه دسترسی به روتر و اتصال به شبکه را بدهند، به این شکل می‌توانند از شبکه خود محافظت کرده و از اتصال دستگاه‌های غیرمجاز ممانعت به عمل آورند. پیاده‌سازی چنین تنظیماتی کاری ساده اما در مقابل زمان‌بر است. به‌واسطه آن‌که شما در ابتدا باید مک آدرس همه دستگاه‌هایی را که در نظر دارید به شبکه متصل شوند، شناسایی کرده، در ادامه جدولی که در ارتباط با روتر قرار دارد را به‌درستی پر کنید. در این حالت هیچ دستگاهی که آدرس مک آن درون جدول قرار نداشته باشد، این شانس را نخواهد داشت که به شبکه متصل شود، حتی اگر گذرواژه شبکه بی‌سیم شما را در اختیار داشته باشد. اما باید بدانید که چنین موضوعی صحت ندارد. یک **هکر** از طریق به‌کارگیری ابزارهای تحلیل‌گر شبکه‌های بی‌سیم به‌راحتی می‌تواند آدرس مک همه دستگاه‌هایی را که اجازه اتصال به شبکه دارند، به دست آورده و در ادامه آدرس مک دستگاه خود را به یکی از آدرس‌های مکی که شما تعریف کرده‌اید، تغییر دهد. در نتیجه همان‌گونه که مشاهده می‌کنید شما کاری جز از دست دادن زمان انجام نداده‌اید. فعال‌سازی فیلتر آدرس‌های مک ممکن است از شما در برابر اتصال کاربران عادی به شبکه محافظت کند، اما در مقابل یک **هکر** این‌گونه عمل نخواهد کرد. همچنین فراموش نکنید اگر این کار را انجام دادید و در ادامه مجبور شدید دسترسی یک کامپیوتر به شبکه را به شکل موقت غیرفعال کنید، کار سختی پیش‌رو خواهید داشت.

باور اشتباه سه؛

محدودسازی آدرس‌های آی‌پی روتر

هر دستگاه متصل به شبکه از طریق آدرس آی‌پی منحصربه‌فردی که در اختیار دارد، شناسایی می‌شود. یک آدرس آی‌پی از سوی روتر به یک دستگاه تخصیص داده می‌شود که رشته‌ای مشتمل بر اعداد همچون 192.168.1.10 است. اما برخلاف آدرس مک که از سوی دستگاه به روتر اعلام می‌شود، روتر از طریق به‌کارگیری پروتکل پویای کنترل میزبان (DHCP) یک آدرس آی‌پی خاص را برای هر دستگاهی که به شبکه متصل شده است، تخصیص می‌دهد.
فرضیه‌ای اشتباه در دنیای ایمن‌سازی شبکه‌ها شکل‌گرفته که اعلام می‌دارد شما با محدود کردن تعداد آی‌پی‌هایی که روتر شما به دستگاه‌ها تخصیص می‌دهد قادر هستید از خود در برابر هکرها محافظت کنید. به‌عنوان مثال، اگر یک محدوده آدرس آی‌پی همچون 192.168.1.1 تا 192.168.1.10 را مشخص کنید، تنها دستگاه‌هایی که در این بازه آدرس آی‌پی قرار دارند اجازه خواهند داشت تا به شبکه متصل شوند و به این شکل شبکه در برابر هکرها ایمن می‌شود. اما این فرضیه اشتباه بوده و ما در باور بعدی نشان می‌دهیم چرا این فرضیه اشتباه است.

باور اشتباه چهار؛

غیرفعال کردن سرور DHCP در روتر از ما محافظت می‌کند

عده‌ای از کاربران و حتی کارشناسان شبکه بر این باورند با غیرفعال کردن سرور DHCP و تخصیص آی‌پی به هر دستگاه آن هم به شکل دستی، **امنیت شبکه** به‌شدت افزایش پیدا می‌کند. در این راهکار فرض بر این است، دستگاه‌هایی که فرایند تخصیص آدرس آی‌پی در خصوص آن‌ها اعمال نشده این شانس را ندارند تا به شبکه متصل شوند. در این تکنیک نیز مشابه فیلتر کردن آدرس‌های مک، کاربر جدولی از آدرس‌های آی‌پی را که متناظر به هر دستگاه است، ایجاد می‌کند. در این حالت کاربر باید آدرس آی‌پی را برای هر دستگاه به شکل دستی تنظیم و وارد کند. اما این تکنیک یک ایراد بزرگ دارد. اگر هکری موفق شده باشد به شبکه شما نفوذ کند، آنگاه از طریق یک اسکن ساده شبکه به‌راحتی می‌تواند آدرس‌های آی‌پی را که در شبکه به کار گرفته شده‌اند، مشاهده کند.
در ادامه هکر یکی از آدرس‌های معتبر آی‌پی را که درون شبکه قرار دارد و به دستگاهی تخصیص داده‌شده برای دستگاه خود مشخص کرده و در ادامه بدون مشکل خاصی به شبکه شما متصل می‌شود. درست شبیه به فیلتر کردن آدرس‌های مک پیاده‌سازی این تکنیک چیزی جزء کار مضاعف برای شما به همراه نخواهد داشت. به‌ویژه زمانی که در نظر دارید دستگاه‌های جدیدی را به شبکه خود
اضافه کنید.

باور اشتباه پنج؛

هکرها به‌سختی می‌توانند به شبکه‌های کوچک نفوذ کنند

یک باور اشتباه کاربران شبکه‌های بی‌سیم این است که هرچه قدرت ارسال سیگنال روتر کم شود، به همان نسبت شانس افرادی که در خارج از محل قرار دارند در اتصال به شبکه کم می‌شود. به‌واسطه آن‌که افراد به‌راحتی نمی‌توانند شبکه را شناسایی کنند. اما باید بدانید اگر هکری مصمم باشد به شبکه شما نفوذ کند از آنتن‌های بزرگی استفاده می‌کند که قادر هستند سیگنال‌های روتر شما را به‌خوبی دریافت کنند. باید بدانید زمانی‌که قدرت سیگنال‌های مسیریاب ضعیف می‌شوند تنها برد مؤثر و امکان اتصال برای افرادی که جزء کاربران معتبر هستند، کم می‌شود.

مطلب پیشنهادی

اضافه کردن یک لایه امنیتی مضاعف
چگونه می‌توانیم یک دیوارآتش به گوشی اندرویدی خود اضافه کنیم؟

چگونه می‌توانیم از شبکه وای‌فای خود محافظت کنیم؟

بهترین راهکاری که در این زمینه پیش روی شما قرار دارد به‌کارگیری یک الگوی رمزنگاری ایمن است. در دنیای سامانه‌های کامپیوتری رمزنگاری به‌خوبی می‌تواند از فایل‌ها و پوشه‌های شما محافظت به عمل آورد. در دنیای شبکه‌های وای‌فای نیز رمزنگاری می‌توانند داده‌هایی را که در یک شبکه انتقال پیدا می‌کنند، کدگذاری کرده و به این

شکل مانع از آن شود تا افراد غیرمجاز به داده‌های شما دسترسی پیدا کنند. در این حالت هکرها موفق خواهند شد داده‌هایی را که شما در حال ارسال آن‌ها هستید، ردیابی کرده و ضبط کنند، اما مادامی‌که کلید رمزنگاری را در اختیار نداشته باشند، موفق نخواهند شد به اطلاعات و گذرواژه‌ها دسترسی پیدا کرده و به این شکل به حساب‌های کاربری و بانکی شما نفوذ کنند. در سال‌های گذشته الگوریتم‌های رمزنگاری متعددی برای این منظور ارائه شده‌اند که WEP یکی از بهترین الگوریتم‌هایی بود که در ابتدا قادر بود از شبکه‌های وای‌فای محافظت کند. اما امروزه، با پیشرفت‌های صورت گرفته این الگوریتم تنها طی چند دقیقه شکسته می‌شود. اگر روتر شما تنها از این الگوریتم پشتیبانی می‌کند یا دستگاه‌های متصل به شبکه قادر نیستند از الگوریتم‌های جدیدتر پشتیبانی کنند، بهتر است به فکر یک جایگزین مناسب برای آن‌ها باشید. پس از آن‌که مشکلات WEP خود را نشان دادند در ادامه الگوریتم WPA عرضه شد که به‌واسطه مشکلات متعدد 10 سال بعد با WPA2 جایگزین شد. لازم به توضیح است که از اواخر سال جاری میلادی WPA3 جایگزین WPA2 خواهد شد.

هر دو الگوریتم رمزنگاری WPA و WPA2 دارای دو وضعیت مختلف شخصی (Personal) هستند که با PSK3 تشخیص داده می‌شود و سازمانی (Enterprise) که با RAIDIUS5 تشخیص داده می‌شود، در اختیار کاربران قرار دارد. حالت شخصی برای کاربران خانگی طراحی‌شده و پیاده‌سازی آن ساده است. شما گذرواژه‌ای را برای روتر خود مشخص کرده و در ادامه هر دستگاهی که قرار است به شبکه بی‌سیم شما متصل شود باید از این گذرواژه استفاده کند. اگر گذرواژه‌ای که برای این منظور استفاده می‌کنید ترکیبی از حروف بزرگ و کوچک و همچنین اعداد بوده و طولی بیشتر از 13 کاراکتر داشته باشد، در این حالت شبکه شما در وضعیت ایمن قرار دارد. اما اگر از واژگانی استفاده کنید که در دیکشنری نرم‌افزارهای نفوذ قرار دارد، همچون نام اشخاص یا مکان‌ها **امنیت شبکه** شما کاهش پیدا می‌کند. یک گذرواژه قدرتمند می‌تواند چیزی شبیه h&5U2v$(q7F4* باشد. امروزه، بیشتر روترها به دکمه‌ای به نام WPS تجهیز شده‌اند. ویژگی WPS به شما اجازه می‌دهد دو دستگاه را که از الگوریتم رمزنگاری WPA2 پشتیبانی می‌کنند، تنها با فشار یک دکمه در روتر و دکمه‌ای که در دستگاه قرار دارد، به شبکه متصل کنید. رویکردی که امروزه به شکل نرم‌افزار نیز انجام می‌شود. اما ویژگی فوق یک ایراد بزرگ هم دارد. این ویژگی به‌شدت در برابر حملات جست‌وجوی فراگیر آسیب‌پذیر است.

در نتیجه، اگر مقوله امنیت برای شما حائز اهمیت است بهتر است ویژگی WPS روتر خود را غیرفعال کنید. اما حالت دوم به‌کارگیری الگوی WPA2 در ارتباط با سازمان‌ها است. سازمان‌ها برای بهره‌مندی از این ویژگی به سرور RADIUS یا یک سرویس RADIUS میزبانی‌شده نیاز دارند. نکته دیگری که لازم است به آن توجه داشته باشید این است که از پروتکل WPA2 در تعامل با EAP-TLS استفاده کنید.

در حال حاضر، مهم‌ترین تهدید پیش روی شبکه‌های وای‌فای از جانب حمله مرد میانی است. حمله‌ای که کاربران یک شبکه را به سمت یک سایت مخرب هدایت کرده و در ادامه اطلاعات مهمی همچون گذرواژه‌ها و نام‌های کاربری را به سرقت می‌برند. اگر سایتی از پروتکل انتقال ابرمتن ایمن استفاده کند، محتوای مبادله شده میان کاربر و سایت به‌صورت رمزنگاری‌شده درمی‌آیند، با وجود این، هکرها بازهم قادر هستند سایت‌هایی را که کاربران به آن‌ها مراجعه کرده‌اند، مشاهده کنند. اما اگر از پروتکل WPA2 در تعامل با پروتکل احراز هویت EAP-TLS استفاده کنید، آنگاه می‌توانید اطمینان حاصل کنید که تنها کاربران مجاز اجازه خواهند داشت به شبکه دسترسی پیدا کنند. زمانی‌که از پروتکل احراز هویت EAP-TLS استفاده کنید، آنگاه کاربران ضمن آن‌که باید گذرواژه موردنظر را وارد کنند باید گواهی مربوط را نیز به کار ببرند.

دیوار آتش در تعامل با رمزنگاری توان دفاعی شما را دوچندان می‌کند

زمانی‌که هکری موفق شود به شبکه وای‌فای شما نفوذ کند، در حقیقت به‌کل شبکه شما واردشده و این حرف به معنای آن است که این هکر به همه سرورها و داده‌های محرمانه شما دسترسی خواهد داشت. حتی اگر از قدرتمندترین الگوهای رمزنگاری استفاده کنید بازهم باید از طریق دیوارهای آتش، شبکه وای‌فای را از سرورها و بقیه شبکه جدا کنید. در سازمان‌های بزرگ، شبکه‌ها ضمن آن‌که باید به کاربران اجازه دسترسی به سایر بخش‌ها را بدهند باید از مشتریان نیز پشتیبانی به عمل آورند.

در نتیجه باید سطوح مختلفی از دسترسی به شبکه مشخص شود. و ضمن آن‌که یک شبکه اصلی دارید، شبکه دومی نیز داشته باشید که به شکل متمایز و جداشده از شبکه اصلی کار کند.

مطلب پیشنهادی

رمزگذاری به‌دنبال محدودسازی دسترسی‌های غیرمجاز
فناوری رمزگذاری چگونه از اطلاعات ما محافظت می‌کند و آیا نفوذپذیر است؟

بهتر است قدرت سیگنال وای‌فای را تنظیم کنید

تاکنون چند مرتبه از بابت ضعیف بودن قدرت سیگنال وای‌فای گلایه کرده‌اید و حتی بخش‌هایی از محیط کاری یا خانه خود را پیدا کرده‌اید که به لحاظ سیگنال‌دهی جزو مناطق مرده (Dead zones) به شمار می‌روند؟ اما ضعیف بودن سیگنال‌ها همواره دلیل بر عملکرد ضعیف روتر یا وجود موانع نیست. باید بدانید که سیگنال‌های روتر به‌راحتی از پنجره‌ها عبور کرده و همان‌گونه که در پنج باور اشتباه به آن اشاره کردیم، شخصی از طریق یک آنتن قدرتمند می‌تواند سیگنال‌های روتر شما را دریافت کرده و از طریق آن به شبکه شما متصل شود. گزارشی که به‌تازگی منتشرشده اعلام می‌دارد، هکرها حتی از فاصله یک مایلی نیز می‌توانند سیگنال‌های وای‌فای دیگران را دریافت کرده و مورد بهره‌برداری قرار دهند. برای حل این مشکل بهتر است قدرت اکسس پوینت خود را تنها در محدوده‌ای که در نظر دارید تحت پوشش قرار دهد، تنظیم کنید

منبع:

datanumen
nakedsecurity.sophos
cio

تاریخ انتشار:
17 آبان 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/14090/5-%D8%A8%D8%A7%D9%88%D8%B1-%D8%A7%D8%B4%D8%AA%D8%A8%D8%A7%D9%87-%D9%BE%DB%8C%D8%B1%D8%A7%D9%85%D9%88%D9%86-%D8%A8%D9%87%D8%A8%D9%88%D8%AF-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D9%88%D8%A7%DB%8C%E2%80%8C%D9%81%D8%A7%DB%8C