Siguen Siendo Vulnerables Las Redes Wi-Fi Con Cifrado WPA2

Por ahora, la mayoría de la gente sabe que una red Wi-Fi abierta permite a las personas a ***espiar todo el tráfico***. El cifrado estándar WPA2-PSK se supone que evita que esto suceda, pero no es tan infalible como se podría pensar. Esto no es algo nuevo sobre un **recién fallo de seguridad**. Más bien, esta es la forma en que WPA2-PSK siempre se ha implementado. Pero es algo que la mayoría de la gente no sabe.

Redes Wi-Fi Sin Seguridad vs. Redes Wi-Fi Cifradas

Sin duda no es seguro usar una red Wi-Fi abierta en casa, pero puede que te encuentres utilizando una en público, por ejemplo, en una cafetería, al pasar por un aeropuerto o en un hotel. Las **redes Wi-Fi abiertas no tienen cifrado**, lo que significa, que todo lo que se envía, es rastreable. Así es, tu usuario y contraseña pueden ser obtenidas con facilidad en una red inalámbrica sin protección.

El cifrado WPA2-PSK, es un poco mas seguro en cuanto al rastreo de datos. Pero claro, puede que alguien tenga acceso en la red, y desde allí poder sniffear todo el trafico que circule entre los dispositivos y el router o modem. Aunque este cifrado brinde una mejora en la seguridad, aun existe una debilidad.

WPA2-PSK Usa Una Clave Compartida

El problema con WPA2-PSK es que utiliza un «Pre-Shared Key«. Esta clave es la contraseña o frase de paso, tiene que introduces para conectarse a la red Wi-Fi. Todo el mundo que se conecta utiliza la misma contraseña.

Es bastante fácil para alguien ***rastrear el tráfico cifrado***. Todo lo que necesitan es:

- **La frase de contraseña**: Todas las personas con permiso para conectarse a la red Wi-Fi tendrán esto.
- **El tráfico asociado de un cliente**: Si alguien está capturando los paquetes enviados entre el router y un dispositivo cuando se conecta, tienen todo lo que necesitan para descifrar el tráfico (suponiendo que también tienen la frase de paso, por supuesto). También es trivial conseguir este tráfico a través de ataques «deauth», el cual fuerza a desconectar un dispositivo de una red WI-FI y le obligan a volver a conectar, haciendo que el proceso de asociación vuelva a suceder.

¿Qué significa en realidad?

En realidad, el cifrado WPA2-PSK no es mucho más seguro contra los sniffeos, si no confías en todo el mundo en la red, este cifrado no te podrá salvar. En la red del hogar, debes estar seguro porque su frase de contraseña Wi-Fi es un secreto.

Sin embargo, si vas a una tienda de café, y esta usa WPA2-PSK

en lugar de una red Wi-Fi abierta, usted puedes sentir más seguridad en tu privacidad. Pero no cuidado! Cualquier persona con conexión a la red de la cafetería podría rastrear su tráfico de navegación.

¿Por Qué El Cifrado WPA2-PSK No Puede Detener Esto?

El cifrado WPA2-PSK en realidad no tratar de detener esto a través del uso de una «clave de parejas transitoria» (PTK). Cada cliente inalámbrico tiene un PTK único. Sin embargo, esto no ayuda mucho porque la clave única por cliente siempre se deriva de la clave pre-compartida (la frase de acceso Wi-Fi.) Es por eso que es trivial capturar la clave única de un cliente, siempre y cuando tengas la frase de acceso al Wi Fi y puede capturar el tráfico enviado a través del proceso de asociación.

WPA2-Enterprise resuelve esto… Para las grandes redes

Para las grandes organizaciones que demandan redes Wi-Fi seguras, esta debilidad en la seguridad se puede evitar mediante el uso de la ***autenticación EAP*** con un servidor RADIUS, a veces llamado WPA2-Enterprise. Con este sistema, cada cliente Wi-Fi recibe una clave única. Ningún cliente Wi-

Fi tiene información suficiente para comenzar simplemente espiar a otro cliente, por lo que este ofrece mucha más seguridad. Las grandes oficinas corporativas o agencias gubernamentales deberían estar utilizando WPA2-Enteprise por esta razón.

Pero esto es demasiado complicado y complejo para la gran mayoría de la gente, o incluso la mayoría de los frikis para usar en casa. En lugar de una contraseña de Wi-FI tiene que introducir en los dispositivos que desee conectar, usted tendría que **administrar un servidor RADIUS** que se encarga de la autenticación y gestión de claves. Esto es mucho más complicado de configurar para los usuarios domésticos.

Finalmente

Ten esto en cuenta: Cuando esté conectado a una red WPA2-PSK, otras personas con acceso a dicha red podrían **espiar fácilmente tu tráfico**. A pesar de lo que mucha gente puede creer, que el cifrado no proporciona protección contra otras personas con acceso a la red.

Si tienes acceso a sitios sensibles en una red Wi-Fi pública, en particular los sitios web que no utilizan el cifrado HTTPS, la posibilidad de hacerlo a través de una VPN o incluso un túnel SSH. El cifrado WPA2-PSK en las redes públicas no es lo suficientemente bueno.