

Recomendaciones básicas de seguridad para redes inalámbricas

Extracto

Este artículo aborda el tema de la protección de las redes inalámbricas. Presenta algunas aclaraciones y recomendaciones prácticas para configurar y mantener segura una red de este tipo.

Prólogo

Las redes inalámbricas son cada vez más comunes, y la mayoría de los ordenadores portátiles que se venden actualmente poseen los dispositivos físicos necesarios para conectarse a ellas.

Estar conectado, y a la vez poder moverse, es una enorme ventaja en el uso de Internet, ya sea en el trabajo o con fines personales. Para estar en línea, ya no es necesario permanecer en un sitio fijo, limitado por los cables.

Las áreas de actividad inalámbrica en aeropuertos y hoteles son la norma hoy en día, y muchos dispositivos de mano están equipados con módulos WiFi (*Wireless Fidelity*, un conjunto de estándares para redes inalámbricas) que posibilitan el acceso permanente a Internet.

Las señales inalámbricas viajan a través de las paredes, pisos y otros obstáculos físicos, de modo que se puede disfrutar de la abundante información de Internet y de la vida al aire libre al mismo tiempo, mientras un encaminador (*router*) inalámbrico proporciona la señal de la Red a cada ordenador en el hogar.

Pero, obviamente, toda esta libertad trae aparejada una advertencia: una mayor necesidad de estar alertas acerca de los riesgos de seguridad en Internet, y tomar medidas adicionales para proteger la conexión inalámbrica adecuadamente.

Seguridad y acceso inalámbrico público

Partamos del supuesto que las redes inalámbricas son más susceptibles a intrusiones y a ser espiadas que las redes físicas, basadas en cables. Esto se debe a la debilidad inherente a las transmisiones de radio.

Un intruso tiene que estar conectado físicamente a la red cableada objetivo, para poder capturar o monitorizar los datos en tránsito, mientras que para penetrar en una red inalámbrica solo necesita permanecer dentro del radio de la señal.

Las áreas de actividad inalámbrica públicas representan un gran riesgo, porque los datos podrían viajar a través de ellas bajo una forma no cifrada, haciéndose visibles para los piratas informáticos.

Con las herramientas apropiadas, estos delincuentes pueden rastrear paquetes de datos fácilmente, reensamblarlos, y extraer información sensible como contraseñas de cuentas de correo electrónico, conversaciones privadas a través de mensajería instantánea y otros datos no cifrados que inevitablemente salen de su ordenador, al conectarse a diferentes servidores de autorización en Internet.

Una técnica denominada tecnología de túneles VPN (*Virtual Private Network*, Red privada virtual) puede ayudar a mitigar los riesgos de seguridad de las conexiones no cifradas, pero ese tema está fuera del alcance de este artículo.

Entonces, ¿qué puede hacer una persona con un ordenador portátil conectado a una red inalámbrica, para asegurar su privacidad al acceder a la red en espacios públicos?

- En primer lugar, es importante acordarse de mantener actualizadas todas las aplicaciones del ordenador: instalar los últimos parches de seguridad del sistema operativo y los programas, y verificar el sitio del fabricante de su adaptador inalámbrico en busca de los últimos controladores y actualizaciones para las instrucciones guardadas en la memoria ROM (*Read Only Memory*, Memoria de solo lectura).
- A continuación, hay que desactivar la opción **Compartir archivos e impresoras** para cualquier red pública con la cual se intenta establecer conexión. Esto restringe el acceso a los recursos compartidos del ordenador a través de la red local inalámbrica no confiable, sin impedir la conectividad a Internet.
- Por supuesto, también hay que tener instalado un cortafuegos como Outpost Firewall Pro para proteger las conexiones contra ataques del tipo "hombre en el medio", donde los perpetradores intentan configurar un punto de acceso falso y forzar la conexión hacia este, o interceptar paquetes de datos en tránsito utilizando las técnicas de rastreo mencionadas anteriormente.

- A continuación, se debe configurar el programa del adaptador inalámbrico, o el asistente para la configuración de redes inalámbricas de Windows para que **no** se conecte automáticamente a cualquier red inalámbrica recientemente detectada.
Si hay más de una red de este tipo en la zona desde donde estamos intentando conectarnos, hay que construir un conjunto de reglas de prioridades, de acuerdo al nivel de confianza. También hay que asegurarse de desactivar el interruptor del adaptador inalámbrico en el ordenador portátil cuando no se está usando Internet.
- En caso de viajar, se recomienda adoptar como rutina averiguar las redes inalámbricas disponibles en el área: cuál está operativa y qué entidad la controla. Cuando sea posible, es preferible conectarse a la red recomendada por el lugar donde nos encontramos (por ejemplo: hotel, cabina de información del aeropuerto, café).
- Un elemento clave para recordar es que nunca hay que realizar ninguna tarea en la que sea necesario enviar contraseñas u otros datos confidenciales a través de una red inalámbrica que no ha sido protegida con cifrado WPA2 (*WiFi Protected Access 2, Acceso inalámbrico protegido 2*).
Esto incluye el envío y la recepción de correo electrónico, registrarse en páginas no protegidas por el protocolo https, o la realización de transacciones financieras.
Navegar la Red y consultar el pronóstico del tiempo, los resultados de los eventos deportivos, o leer las noticias gratuitas probablemente no represente un gran riesgo de seguridad. Pero, una actividad que implique la identificación personal no debería realizarse durante el transcurso de una sesión de navegación no cifrada.

Un comentario final: dos dispositivos inalámbricos pueden conectarse entre sí directamente a través de las ondas aéreas para establecer una red. En varios adaptadores inalámbricos, algunas configuraciones pasadas por alto permiten montar una red de este tipo, sin solicitar el consentimiento de los usuarios. Es necesario asegurarse de que el sistema no esté configurado de esa manera.

Cómo configurar una red inalámbrica personal, y conectarse a ella de forma segura

En las redes inalámbricas, el cifrado es la clave para la seguridad de los datos. Para implementar una red inalámbrica personal segura, es necesario tener un encaminador o punto de acceso que permita el cifrado WPA2. E, incluso entonces, se debe escoger una frase secreta poderosa, que resista los ataques de descifrado de contraseñas por fuerza bruta.

Existen muchos generadores de claves seguras, como el que se puede encontrar en <http://www.goodpassword.com/index.htm>. Los algoritmos de cifrado más débiles, tales como WPA (*WiFi Protected Access, Acceso inalámbrico protegido*) con una frase secreta corta, o WEP (*Wired Equivalency Privacy, Privacidad equivalente a la del cableado*), pueden ser vulnerados en cuestión de minutos. Por ello se recomienda enfáticamente el uso del cifrado WPA2. Algunos encaminadores proporcionan una actualización a WPA2 desde algoritmos anteriores, a través de una modificación en las instrucciones grabadas en la memoria ROM.

Otra forma para mejorar la seguridad básica en una red inalámbrica, es cambiar el nombre de acceso predeterminado para entrar a la página de configuración del punto de acceso.

Si este dispositivo viene con la combinación de nombre de usuario y contraseña estándar, "Admin"/"Admin", asignados en la fábrica, hay que cambiarlos tan pronto como sea posible, y elegir palabras más crípticas y específicas. Esto servirá para evitar que intrusos potenciales alteren la configuración de seguridad del encaminador, con el fin de otorgarse acceso a la red personal del usuario desprevenido, usando sus propias credenciales.

Otras precauciones recomendadas incluyen:

- Asignar un SSID (*Service Set Identifier, Identificador del conjunto de servicios*) único a la red: este es el nombre que será visible a quienes buscan una red inalámbrica disponible.
Hay que comunicar la frase secreta de WPA2, de un modo seguro a las personas autorizadas que se conectarán a esta red (clientes), o configurar manualmente los parámetros de acceso de dichos clientes, y especificarles que se conecten únicamente con el nombre especificado.
- Monitorizar la aparición de nuevos puntos de acceso en las proximidades, y recordar a los clientes móviles los peligros de conectarse a un punto de acceso equivocado o malicioso. Estos, podrían incluir piratas informáticos leyendo el tráfico desde y hacia los clientes, e incluso tomando el control de una red cableada si el cliente está conectado simultáneamente a una red local Ethernet.
- Habilitar el filtrado de IP y MAC en la configuración del encaminador.
El filtrado MAC permite incluir manualmente los adaptadores de red con sus números de identificación específicos en una lista de dispositivos autorizados. De este modo, cualquier identificador que no se encuentre en la lista, tendrá prohibido el acceso a la red. El filtrado IP utiliza el mismo principio: solo se les permitirá la conexión a los clientes con los números de IP autorizados, pero para esto es necesario desactivar el servidor DHCP (*Dynamic Host Configuration Protocol, Protocolo de configuración dinámica de servidores*) en el encaminador, y asignar manualmente los números IP permitidos.

Además, podría ser útil definir el número de clientes que se pueden conectar al encaminador, limitando los números de subred al mínimo necesario, y especificar intervalos de tiempo durante los cuales el dispositivo de conexión permitirá que el cliente acceda a la red. Esta última opción podría no estar disponible en algunos los encaminadores.

- Limitar el rango de la distribución de señal del punto de acceso, de modo que los clientes puedan conectarse solo hasta cierta distancia: pasado el límite establecido no habrá señal disponible. Esta funcionalidad está disponible únicamente en algunos dispositivos.
- Considerar la ocultación de SSID, opción presente en la página de configuración del encaminador, de modo que la red no aparezca en la lista de redes disponibles cuando los clientes realizan una nueva búsqueda. Así, se aplicarán todos los parámetros configurados previamente en el cliente, y los ordenadores que ya han sido asociados con el SSID, tendrán la capacidad de continuar detectando esta estación.

Conclusiones

Las redes inalámbricas extienden la movilidad y el acceso a Internet, cualidad sumamente útil en muchas situaciones. Desafortunadamente, la mayoría de ellas no están convenientemente protegidas por la configuración predeterminada, y el usuario debe hacer un esfuerzo adicional para asegurarlas.

Al seguir los consejos descritos en este artículo, habremos tomado el camino correcto para asegurar que nuestras comunicaciones inalámbricas están libres de riesgos.