8 CONSEJOS PARA REFORZAR LA SEGURIDAD DE TU RED WIFI

Por Fabrizio Ferri-Benedetti

27 julio, 2012

¿Sabías que 6 de cada 10 hogares españoles tiene WiFi en casa? Es una cifra enorme comparada con la de hace unos años, que plantea retos sobre todo relacionados con la seguridad. Y es que el 12% de los españoles se conecta a la red del vecino.

Las redes abiertas ascienden a un 6,2%, y un 20% de los routers usan el débil cifrado WEP, según un estudio de Inteco. Para colmo de males, casi un tercio de los encuestados desconocen el tipo de protección en uso en su red. Un panorama del que es fácil aprovecharse.

Te damos 8 consejos para maximizar la protección de tu red WiFi. Seguir algunos de ellos contribuirá a reforzar la seguridad de tu conexión y evitar desagradables sorpresas.

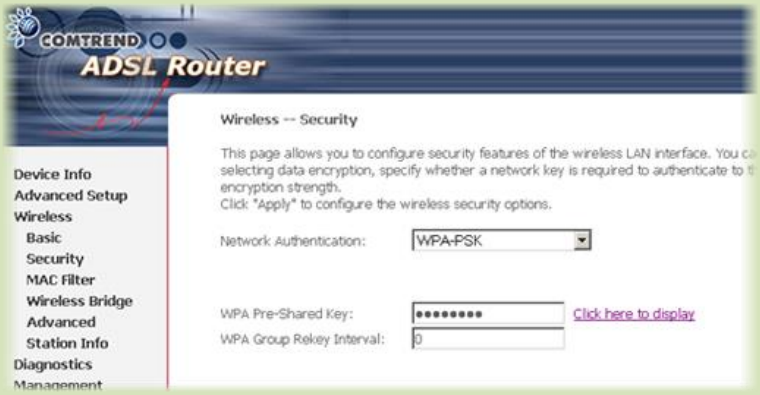
1- Conoce tu router y los principales conceptos WiFi

El router, esa cajita tan linda, no funciona como por arte de magia: en su interior hay un sistema operativo que tu proveedor de Internet ha preparado lo mejor que podía. Pero rara vez una configuración incluida de fábrica se adapta a las necesidades de los usuarios: contraseñas débiles, puertos sin abrir, velocidad baja...

Es por eso que conviene que te armes de paciencia y aprendas más sobre tu router: cómo acceder a su configuración interna, qué hace cada opción y cómo actualizar su firmware. Al mismo tiempo, viene bien que te informes sobre cada tipo de cifrado WiFi y sobre el funcionamiento básico de la tecnología WiFi.

2- Cambia la configuración por defecto del router

Una vez que has aprendido más sobre tu router, debes cambiar su configuración para que se adapte a tus necesidades. Un router que mantiene las opciones de fábrica es un router que está gritando "¡hackeame!" a los cuatro vientos. Es una presa fácil para cualquiera que sepa usar herramientas de auditoría.



El panel de configuración de un router Comtrend, marca elegida por Movistar

Entre los pasos recomendados por los expertos están el cambiar el nombre de la red (SSID), usar un cifrado de tipo WPA2-AES con una contraseña segura y limitar el número de direcciones IP asignables.

Ningún cifrado está a prueba de ataques criptográficos, pero si eliges las tecnologías más robustas, la probabilidad de que tu red sea invadida por extraños se reduce bastante.

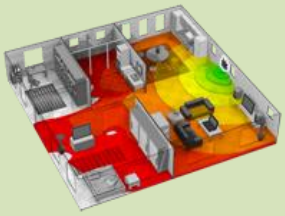
3- Aprende a usar herramientas de auditoría de seguridad

En su "El Arte de la Guerra", el sabio Sun Tzu decía que para vencer hay que conocer al enemigo y conocerse a uno mismo. Es un principio que también se aplica al arte de la seguridad informática: para impedir que alguien supere las defensas de tu red hay que saber qué herramientas se usan para hackear redes WiFi...

pulWiFi es una potente herramienta de auditoría para Android

En nuestra monografía sobre cómo obtener claves WiFi hicimos un repaso rápido a las herramientas más importantes. Son utilidades en general muy fáciles de usar y su propósito es, al menos sobre el papel, estrictamente educacional. La única manera de saber si tu configuración de seguridad es sólida es usarlas contra tu red WiFi y ver si consigues entrar.

4- Controla la cobertura de tu red WiFi



La señal de una red inalámbrica se propaga hacia todas las direcciones desde el router. Si tu punto de acceso se encuentra al lado del apartamento del vecino, este disfrutará de casi la mitad de tu señal. Es una invitación a disfrutar de tu red WiFi. Para evitar que la señal se extienda a lugares desde los que no conectarás, debes pensar en dónde situar el punto de acceso.

Los escapes de señal son inevitables cuando se vive en lugares pequeños, pero es posible minimizarlas alejando el router de la calle y de los vecinos. Tener un plano completo del edificio te será de gran ayuda. Por otro lado, aprovecha otros aparatos electrónicos y objetos metálicos: ambos interfieren con la señal WiFi y pueden actuar como un "escudo". Y si no aprovechas la velocidad del protocolo 802.11n, usa el b o el g: tienen menos alcance.

5- Usa un nombre de red anónimo, gracioso y pasivo/agresivo

Cada red WiFi tiene un nombre (SSID). Si no has tocado la configuración del router, el SSID será el que venga incluido de fábrica o uno generado al azar, como WLAN_123D o Linksys-G. Lo que quizá no sepas es que mantener el SSID por defecto es muy peligroso para tu red WiFi, pues das información valiosa sobre tu modelo de router.

Un ejemplo de SSID gracioso. El de arriba tampoco se queda corto (vía WTFWiFi)

Cambiar el nombre de tu punto de acceso (SSID) no hará que tu red WiFi esté a salvo, pero sí será un mensaje para quien explore

las redes que tiene a su alrededor. Le estarás diciendo a los potenciales parásitos que conoces tu router y que te has preocupado por hacer que tu red sea más segura.

Algunos SSID graciosos y que le quitarán a los demás las ganas de tantear tu red:

Virus_Detectado

Te estoy viendo

UnidadMovil_47

Buen intento, cowboy

Soy abogado

Seguro que se te ocurren más...

6- No descuides la seguridad intramuros

Por muy segura que sea la configuración del router, debes tener una segunda línea de defensa en la que refugiarte en caso de que alguien consiga acceder a tu red y tenga malas intenciones (o simplemente curiosidad). Si el cifrado de la conexión WiFi falla y no tienes un cortafuegos en tu PC, cualquiera podrá acceder a tus carpetas compartidas.

El muro más importante que debes levantar es el cortafuegos / firewall. Todos los sistemas operativos incluyen uno, y hay utilidades que facilitan su puesta a punto. Por otro lado, en nuestro especial sobre detección de intrusos en redes WiFi

recomendamos varias utilidades para detectar e identificar visitas inesperadas.

7- ¡Tampoco te pases con las medidas de seguridad!

Llenar tu router de contramedidas, en lugar de ser beneficioso, puede causarte problemas. Es lo que se conoce como el fenómeno "Me he quedado fuera de mi castillo". El filtrado de direcciones MAC es un ejemplo de medida de seguridad ineficaz y peligrosa, puesto que es tremendamente fácil quedar excluido de la propia red por un pequeño error.

Preocuparse es bueno, pero preocuparse demasiado...

O dicho de otra forma: no te vuelvas paranoico. El 99% de las personas que intentan entrar en redes WiFi solo quieren ver vídeos en YouTube y descargar el correo; usan herramientas semi-automáticas, y, si estas fallan, se dan por vencidos al instante y buscan otras redes más sencillas de hackear.

8- Apaga el WiFi si no vas a usarlo

La última recomendación es de sentido común: si no vas a conectar a tu red a través de una conexión WiFi, desactiva esa funcionalidad en tu router. Una red cableada es más segura, rápida y fiable que una inalámbrica.

Y si vas a estar fuera de casa por un largo periodo, apaga el router. Todavía no tenemos noticia de que alguien haya conseguido hackear un router apagado...