VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Febrero 2016

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- **Tu red inalámbrica**
- **Tus dispositivos**

Asegurando tu red doméstica

Resumen

Hace varios años las redes domésticas eran relativamente simples, por lo general no eran más que un punto de acceso inalámbrico y una o dos computadoras utilizadas para navegar por Internet, comprar en línea o jugar. Sin embargo, las redes domésticas se han vuelto cada vez más complejas. Ahora conectamos varios dispositivos a estas redes y los usamos para algo más que navegar por la web o consumir medios de comunicación. En este boletín abarcamos cómo se puede crear una red segura en el hogar para ti y tu familia.

Editor Invitado

Cheryl Conley dirige al equipo de Educación de Seguridad y Concientización en Lockheed Martin, aprovechando The I Campaign ™ que llega a más de 100 mil empleados. Esto incluye grupos enfocados a alianza y defensa de toda la empresa, además de un programa de phishing global. Sigue a Cheryl en Twitter como **@conleychera**.

Tu red inalámbrica

Casi toda red doméstica comienza con una red inalámbrica (comúnmente llamada red Wi-Fi) que te permite conectar de forma inalámbrica cualquiera de tus dispositivos a Internet, desde computadoras portátiles y tabletas hasta consolas de videojuegos y televisores. La mayoría de estas redes son controladas por un router, el cual es un aparato que tu proveedor de servicios instala en tu hogar para conectarte a Internet. Sin embargo, en algunos casos, tu red podría ser controlada por un sistema aparte llamado punto de acceso inalámbrico que se conecta a tu router. Independientemente de la red inalámbrica que uses, ambas funcionan de la misma manera por la transmisión de señales inalámbricas. Los diferentes dispositivos en tu casa se conectan a tu red inalámbrica a través de estas señales que les permiten conectarse a Internet, así como a cualquier otro dispositivo ajeno a tu red doméstica, por lo que asegurar tu red inalámbrica es una pieza clave para proteger tu hogar. Nosotros recomendamos seguir los siguientes pasos para resguardarla:

- Cambia la contraseña de administrador predeterminada del router o punto de acceso de tu red inalámbrica. La cuenta de administrador es lo que permite configurar los ajustes para tu red. El problema es que muchos routers o puntos de acceso inalámbricos se envían con un usuario y contraseña de administrador predeterminados, los cuales son conocidos y a menudo están publicados en Internet. Por eso, asegúrate de cambiar la contraseña de administrador a una contraseña única y segura que sólo tú conozcas.
- Modifica el nombre predeterminado de tu red inalámbrica (a veces llamada SSID). Este es el nombre que tus dispositivos verán cuando busquen una red inalámbrica local. Dale a tu red el nombre de algo único para que

Asegurando tu red doméstica

puedas identificarla fácilmente, pero asegúrate de que no contenga información personal. Configurar tu red como oculta no tiene mucho valor puesto que la mayoría de las herramientas de escaneo inalámbricos o cualquier atacante experto puede descubrirla fácilmente.

- Asegúrate de que sólo personas de confianza puedan conectarse y usar tu red inalámbrica y que esas conexiones estén cifradas; haz esto habilitando la seguridad más fuerte. Actualmente, la mejor opción es utilizar el mecanismo de seguridad llamado WPA2. Al habilitarla se necesita una contraseña para que la gente se conecte a tu red doméstica y una vez conectada sus actividades en línea se cifrarán. Verifica que no utilices métodos de seguridad obsoletos y más antiguos, como WEP, o que carezcas de algún tipo de seguridad, que sería una red abierta. Las redes abiertas permiten que cualquiera pueda conectarse a tu red inalámbrica sin ningún tipo de autenticación.

Para proteger tu red doméstica, asegura tu red inalámbrica, actualiza y protege con contraseña todos los dispositivos conectados a ella.

- Asegúrate que la contraseña que las personas utilizan para conectarse a tu red inalámbrica sea segura y diferente a la contraseña de administrador. Recuerda que probablemente sólo necesites introducir la contraseña una sola vez por cada uno de los dispositivos, ya que éstos pueden almacenarla y recordarla.
- Muchas redes inalámbricas son compatibles con lo que se llama una red de invitados (guest network). Esto permite a los visitantes conectarse a Internet pero protegiendo tu red doméstica, ya que no pueden conectarse a algún dispositivo de la misma. Si agregas una red de invitados, asegúrate de habilitar WPA2, así como una contraseña única para esa red.
- Desactiva WPS (WiFi Protected Setup) u otros mecanismos que permitan a un nuevo dispositivo conectarse a la red sin saber las opciones de contraseña y configuración.
- Si tienes dificultad recordando todas estas diferentes contraseñas, te recomendamos ampliamente que utilices un gestor de contraseñas para almacenarlas de forma segura.

¿No estás seguro de cómo hacer estos pasos? Pregunta a tu proveedor de servicios de Internet, consulta la documentación que acompaña a tu router o punto de acceso inalámbrico, o en su respectivo sitio web.

Tus dispositivos

El siguiente paso es saber lo que está conectado a tu red doméstica y asegurarte de que todos esos dispositivos son seguros. Esto solía ser simple cuando sólo había pocos dispositivos conectados. Sin embargo, en la actualidad con

Asegurando tu red doméstica

el Internet de las cosas, casi todo puede conectarse a la red doméstica, incluyendo televisores, consolas de juegos, monitores de bebés, altavoces, tu termostato o quizá incluso tu coche. Una manera fácil de descubrir lo que está en tu red doméstica es utilizar un escáner de red simple, como Fing. Estas aplicaciones, que se pueden instalar en tu computadora o dispositivo móvil, escanean tu red inalámbrica e informan de todos los dispositivos conectados a ella. Una vez que haya identificado todos los dispositivos, es necesario verificar que cada uno de ellos es seguro. La mejor manera de hacerlo es revisar que siempre se esté ejecutando la última versión de su sistema operativo/firmware; cuando sea posible, se debe permitir la actualización automática en ellos. Si alguno de tus dispositivos requiere una contraseña, utiliza siempre una que sea segura y única. Por último, no dejes de visitar el sitio web de tu proveedor de servicios de Internet, ya que pueden proporcionar herramientas gratuitas para ayudarte a proteger tu red doméstica.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Aumentar la seguridad de la red:	http://windows.microsoft.com/es-mx/windows/making-network-more-secure#1TC=windows-7
Consejos de seguridad para redes:	http://www.xatakahome.com/la-red-local/consejos-de-seguridad-para-redes-wifi-convierte-tu-red-en-una-fortaleza-inexpugnable
Aprende a asegurar tu WiFi en 7 pasos:	https://www.osi.es/es/actualidad/blog/2015/03/09/aprende-asegurar-tu-wifi-en-7-pasos
Frases de acceso:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_sp.pdf
Gestores de contraseña:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción: Denise Betancourt, Mario Vasquez, Katia Rodríguez