UNA RED WIFI CONTROLADA EVITA EL PASO DE *HACKERS*

Texto: Redacción Séptimo Día **Foto:** Lylibeth Coloma

NO HAY SISTEMA INFALIBLE, PERO SI SE ASESORA CON PERSONAL IDÓNEO ES POSIBLE DETENER ATAQUES CIBERNÉTICOS QUE BUSCAN ROBAR O DESTRUIR INFORMACIÓN EN CUENTAS PERSONALES Y CORPORATIVAS.

Un perjuicio que supera $ 1,2 millones provocó el hackeo (ataque cibernético) al sistema informático de la cuenta de la Agencia Nacional de Tránsito (ANT) del Ecuador, descubierto a inicios de este año.

Acciones similares se han registrado también en grandes organizaciones, como el FBI y la CIA, y en empresas mundialmente conocidas como la propia Google, Renault, entre otras. Y aunque se trate de un delito informático el hackeo se promociona libre e ilegalmente a través de la red, en Ecuador y el mundo.

Lo que hay que tener claro es que no hay sistema infalible, pero sí existen mecanismos que pueden frenar el ingreso de los piratas cibernéticos que están al acecho para, en la menor oportunidad, destruir o robar información privada y ocasionar grandes perjuicios, dicen especialistas.

Según datos del INEC, el 78,7% de la población ecuatoriana usó internet en 2016 y cada vez es más común el uso de redes wifi (Wireless Fidelity - soluciones informáticas que utilizan tecnología inalámbrica) en distintos sectores, permitiendo a los usuarios trasladarse a cualquier lugar sin perder la conexión. ¿Pero cuáles son los mayores riesgos que usuarios y empresas deben considerar para no poner en peligro la seguridad de su información o la de sus colaboradores?

Es importante recordar que en las redes inalámbricas el medio de transmisión (el aire) es compartido por todos los usuarios. Esto hace que la información sea más fácil de espiar que la que se transmite en una red tradicional (Ethernet), opina Rafael Bonilla Armijos, docente de la carrera de Computación de la Facultad de Ingeniería en Electricidad y Computación (FIEC) de la Espol.

"Las redes inalámbricas no deberían ser usadas para tener accesos a información sensitiva o a sistemas críticos de las empresas, sin usar medidas complementarias como VPN o canales encriptados".

La recomendación para evitar vulneraciones es usar el protocolo WPA2 (personal o empresarial) con una clave adecuada (al menos 14 caracteres aleatorios mezclando letras mayúsculas y minúsculas, números y símbolos) o portales captivos donde los usuarios deben presentar sus credenciales regulares (contraseñas) antes de ganar acceso a la red. "Pese a esto, en octubre de 2017 se descubrió una seria vulnerabilidad en WPA2 llamada KRACK, la cual ha acelerado los planes para reemplazar WPA2 por WPA3".

Lo mínimo que se puede hacer es asegurarse de que los archivos de *log* de los diferentes dispositivos de red que ofrecen acceso a la red inalámbrica estén activos. La tarea de estos *logs* es registrar todos los dispositivos que se unen a la red. También existen soluciones más "profesionales" mediante dispositivos de red especializados que permiten hacer un monitoreo y control de todo lo que pasa en una red inalámbrica.

Gabriel Ortega señala la vulnerabilidad de los routers y switch.

El académico destaca que no existe una tecnología segura que evite los ataques contra las redes inalámbricas. "De manera similar, tampoco podemos recomendar una marca de equipos en lugar de otra; todas en su momento han tenido uno o varios problemas de seguridad. Generalmente lo que se recomienda es seguir las mejores prácticas al momento de configurar y usar redes wifi".

Daniel Faour, gerente general de Casa del Cable, afirma que el problema es que usuarios (personal/corporativo) y técnicos no incluyen en el cerco de protección elementos que están conectados dentro de una empresa (como impresora, central telefónica, sensores, cámaras o controladores de temperatura).

"Se dedican a blindar la periferia: los servidores y *routers* para que los *hackers* no entren por la puerta ni brinquen la cerca. Pero hay un boquete por donde pueden pasar. Por eso también hay que controlar la seguridad este-oeste. El secreto es tener visibilidad y elementos seguros en tus redes". Sugiere tener cuidado con los puntos de red, no abrir correos maliciosos y que el técnico esté actualizado para poder tener un wifi gestionado (controlado).

Gabriel Ortega, especialista en Networking y Telecomunicación, explica que los hackeos no solo se producen con redes abiertas, sino también con aplicaciones que permiten introducirnos en redes autenticadas. "Muchas empresas siguen tratando sus redes wifi corporativas como una red doméstica que en casa solo configuramos con una contraseña y nada más".

Indica que existen métodos corporativos más seguros para saber qué usuarios se están conectando a la red. Y ahí hay que diferenciar cuál de ellos puede entrar a los datos internos y cuáles solo a internet. "Por ejemplo, una persona a quien se le concede acceso a internet a través de una red no controlada tendrá información de todos los servidores y en este punto empieza el peligro".

La tecnología hace que todo este tema de seguridad ya no sea un dolor de cabeza constante, sino que podemos tomar acciones más automatizadas, tener toda la visibilidad de lo que ocurre en la red.

"Lo que hacen los equipos es facilitar la forma en que tratamos a cada uno de nuestros usuarios, dispositivos, puntos de red. A todo lo que puede generar una pequeña vulnerabilidad le damos más visibilidad, control y tratamiento mucho más sencillo para que no sea un dolor de cabeza para el administrador de la red".

Esta tecnología es segura hasta que se vulnera, pero si ocurre aquello, el usuario recibe una alerta, lo que le permitirá tomar medidas correctivas. SD