Seguridad en la Red Inalámbrica

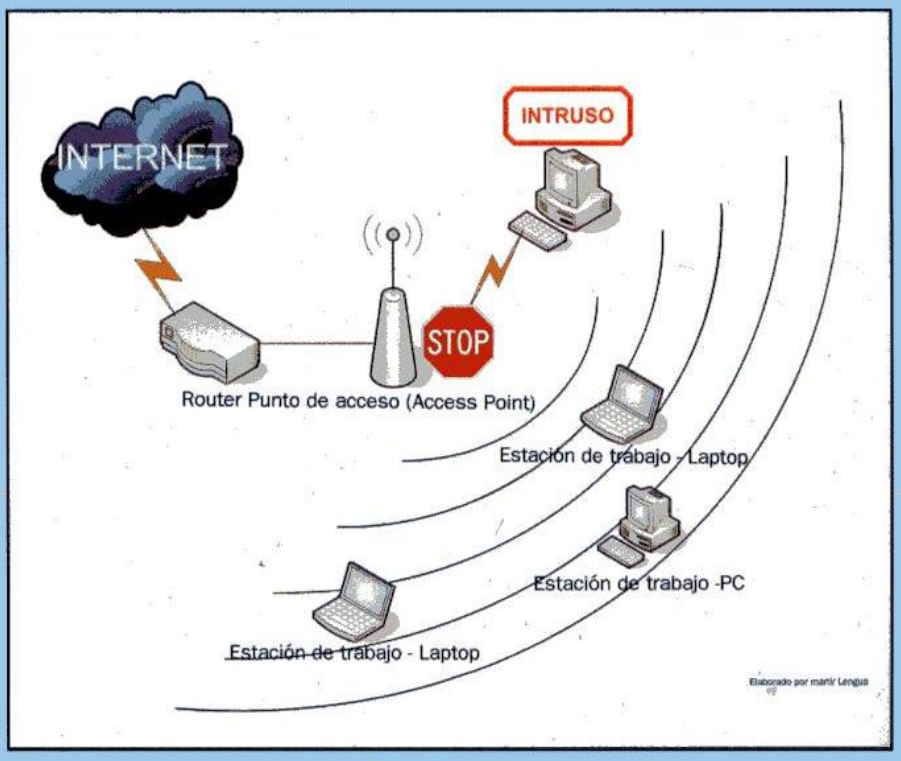
La tecnología de las redes inalámbricas, es en este momento una pieza clave para dotar servicios de Internet y ancho de banda a empresas y localizaciones donde la adquisición de infraestructuras de telecomunicaciones no es asequible desde el punto de vista económico. Esto significa e implica el crecimiento del uso de este medio de transmisión para conectarse a Internet, como así también para cometer delitos informáticos.

Una de las tantas ventajas que tiene una conexión inalámbrica es que la transmisión de datos es por medio de ondas, que cada estación de trabajo móvil remite esa señal y tendrá acceso a la información que está circulando dentro del mismo entorno, con la particularidad que no es necesario conectarse por medio de un cable de red, sino a través de ondas electromagnéticas.

Pero como todo servicio y/o aplicación informático(a) tiene sus vulnerabilidades y brechas de seguridad, es necesario tomar medidas estrictas para evitar cualquier tipo de eventualidad negativa. Así como un usuario en una empresa o una persona natural en su domicilio quieren ingresar a Internet usando su propia conexión inalámbrica, hay personas con fines inescrupulosos o por curiosidad que acceden clandestinamente a una red inalámbrica para tratar de encontrar o sacar alguna información importante que esté circulando en esa red.

Desde la perspectiva de un atacante, las redes inalámbricas son fantásticas ya que son un medio ideal para lanzar un ataque y apropiarse de activos importantes y valiosos para una empresa o persona natural.

En una red cableada tradicional, el control del acceso es sencillo y controlable, pero en las redes inalámbricas las reglas cambian por la imposibilidad de rastreo que las mismas ofrecen, incrementando el anonimato de un supuesto atacante.



Por lo tanto, es necesario asegurar una red inalámbrica ya sea por contraseñas fuertes y técnicas de encriptamiento de los datos que circulen en la red existente para contrarrestar cualquier tipo de ataque o acceso no deseado a la red.

Los métodos de ataques normales han tomado gran envergadura así como también han aparecido otros métodos de protección a este tipo de conexiones. A pesar de que siempre existen riesgos y vulnerabilidades, también existen soluciones y mecanismos de seguridad que pueden evitar un ataque a una red inalámbrica. Los productos de redes inalámbricas que podemos encontrar en el mercado peruano ofrecen tres mecanismos de seguridad para encriptar el tráfico y denegar acceso a personas no autorizadas, estos son: WEP, WPA-TKIP y WPA.

¿Pero qué mecanismo es mejor y qué recomendamos?

El uso de WEP con una llave de cifrado de cinco de caracteres (64 bit), letras mayúsculas y minúsculas, números, entre otros signos se rompen con la herramienta de seguridad «Aircrack» (ver imagen 01) en menos de un segundo. Romper WEP con una llave de cifrado de 13 caracteres (128 bit) tarda un poco más (Hasta 4 minutos depende de la

complejidad (ver imagen 02) de un llave complejo) pero sí es susceptible a ataques. Esto significa que una persona no autorizada, en caso de éxito en un ataque a una red wireless, no sólo tiene acceso a Internet sino tiene acceso a todas las computadoras y servidores con los datos que están ubicados en esa red, como también puede hacer ataques a otras redes desde la red hackeada y/o vulnerada. Esto generaría un problema jurídico o penal.

El protocolo de encriptación WPA-TKIP es más fuerte pero poco seguro como debería ser. En su anuncio actual los científicos alemanes, Erik Tews y Martín Beck, encontraron un camino eficiente para leer el tráfico protegido con WPA-TKIP. Pero todavía no hay oportunidad para entrar a la red o registrar al punto de acceso.

WPA2 es un protocolo de encriptación más seguro y se necesita un tratamiento fuerte para vulnerabilizarlo. WPA2 está usando, contrario a WEP y WPA-TKIP, el algoritmo AES, quien es mucho más seguro que WEP y WPA-TKIP que esta usando el algoritmo RC4. También es muy importante el nombre de la red inalámbrica (SSID). No tiene sentido pensar que sin el nombre de la red inalámbrica no se podrán realizar ataques, es un sofisma. Herramientas libres de seguridad como Kismet pueden detectar redes sin SSID y acceder a la red sin problemas.

¿Como es la situación en Lima? ¿Saben los usuarios sobre las medidas de seguridad?

Una vuelta con un auto y armado con una laptop en zonas concurrentes de San Isidro, Miraflores y Barranco, muestran que la gran mayoría no está usando estas medidas de seguridad. El 44.5% de usuarios de Internet, usando una red inalámbrica dentro de los distritos mencionados, no usa ningún mecanismo de seguridad, el 48% usa el protocolo WEP con 64 bits o 128 bits de cifrado, el 4.37% usa WPA-TKIP y solo el 2.5% usa el protocolo WPA2. En nuestra opinión, hay una obligación de empresas de telecomunicaciones para clarificar y dilucidar sobre las amenazas que nos rodean.

En general, FON PERÚ recomienda para el uso de una red inalámbrica en toda empresa/ entidad y porque no mencionar hasta en casa, restringir el acceso a un Access Point (Punto de Acceso) con una contraseña fuerte para el administrador a través de un protocolo de encriptación como WAP2 y con una llave de cifrado largo (hasta 63 caracteres y letras mayúsculas y minúsculas, números, entre otros signos). Elegir un nombre sin conclusión sobre el dueño de la red, la desactivación de configuración remota y no permitir la configuración del Access Point sobre el WLAN sino siempre sobre el cableado, apagar el Access Point u otros equipos inalámbricos cuando no se usan.

Disminuir el alcance del Access Point, actualizando el Firmware de los Access Points y dividiendo el Access Point con la red, con el uso de VLAN y Firewall dentro de las subredes.

Para empresas grandes con una gran cantidad de redes inalámbricas de Access Points, recomendamos el uso de las tecnologías de IPSEC, SSL y RADIUS, tecnologías de seguridad avanzadas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por: Ing. Christopher Hafer
Gerente General
FON PERU S.A.