ISSN 1998-5347

Product Review
Más espacio con el monitor LCD X224W+ de Hyundai

Apuntes
Cisco reconoce a Nexus Technology

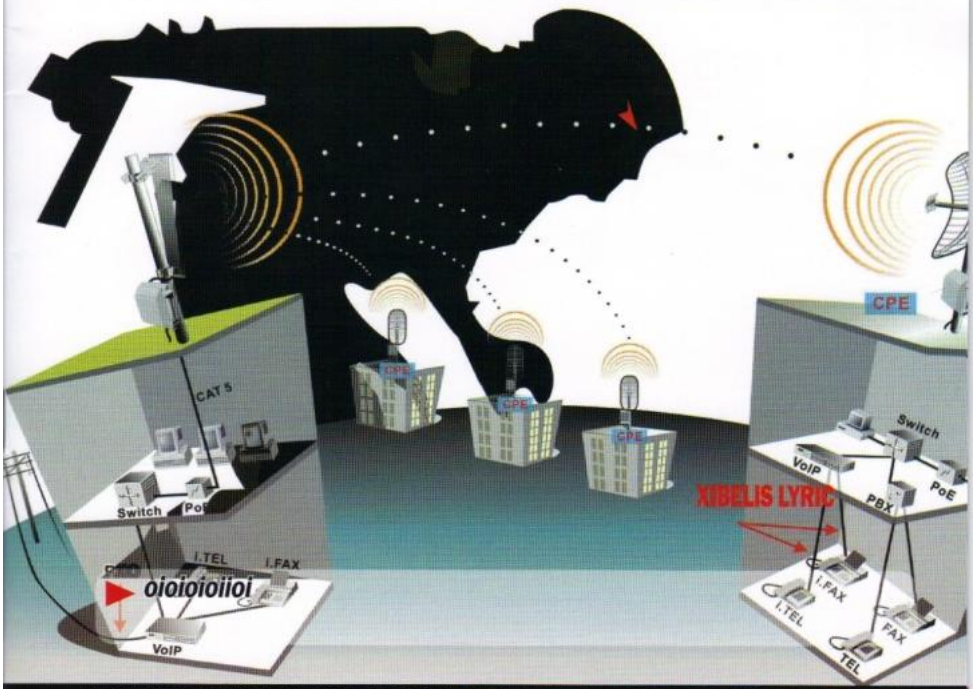
Entrevista
Ledda Valdivieso de Intel

canalTI

INFORMACIÓN PARA EL NEGOCIO TECNOLÓGICO

DISTRIBUCIÓN SEMANAL GRATUITA AÑO 5 • N° 198 • 17 DE AGOSTO DE 2009

Seguridad en la Red inalámbrica



PRODUCTOS PANDA SECURITY 2010 / LANZAMIENTO DE XIBELIS LYRIC POR SUMTEC

Seguridad en redes inalámbricas

Por
Christopher Hafer (*)

Una de las tantas ventajas que tiene una conexión inalámbrica es que la transmisión datos se realiza por medio de ondas que cada estación de trabajo móvil remite para acceder a la información que está circulando dentro del mismo entorno, con la gran ventaja de que ya no es necesario contactarse por medio de un cableado de red.

Pero como en todo servicio y/o aplicación informático existen 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 que por curiosidad acceden clandestinamente a una red inalámbrica para tratar de encontrar o sacar alguna información importante que esté circulando en ella.

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:

1.- WEP
2.- WPA
3.- WPA2.

¿Pero qué mecanismo es mejor y qué recomendamos?

El uso de WEP con una llave de cifrado de cinco caracteres (64 bit), letras mayúsculas y minúsculas, números, entre otros signos se rompen con la herramienta de seguridad <<Aircrack>> en menos de un segundo. Romper WEP con una llave de cifrado de 13 caracteres (128 bit) tarda un poco más, hasta 4 minutos dependiendo de la complejidad de una llave compleja pero sí es susceptible a ataques. Esto significa que una persona no autorizada, en caso de éxito en un ataque a una red wireles, no sólo tiene acceso a todas las computadoras y servidores con los datos que están ubicados en esa red, sino 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 es más fuerte pero no tan seguro como debería de ser. En su anuncio actual, los científicos alemanes Erick Tews y Martin Beck, encontraron un camino eficiente para leer el tráfico protegido con WPA. Pero todavía no hay oportunidad para entrar a la red o registrar al punto de acceso.

Sobre el WPA2

Este es un protocolo de encriptación más seguro y que necesita de un tratamiento fuerte para ser vulnerado. WPA2 está usando, contrariamente a WEP y WPA, el algoritmo AES, que es mucho más seguro que el de WEP y WPA, el RC4.

Aquí también es muy importante el nombre

de la red inalámbrica (SSID), aunque no tiene sentido pensar que sin el nombre de la red inalámbrica no se podrán realizar ataques, pues herramientas libres de seguridad como Kismet pueden detectar redes sin SSID y acceder a la red sin problemas.

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

UUna vuelta con un auto y armado con una laptop en zonas concurrentes de San Isidro, Miraflores y Barranco, muestran que la gran mayoría de redes no están usando estas medidas de seguridad. Estudios demuestran que el 44.5 % de usuarios de Internet, que usan una red inalámbrica dentro de los distritos mencionados, no emplea ningún mecanismo de seguridad. El 48 % usa el protocolo WEP con 64 bits o 128 bits de cifrado, el 4.37 5 usa WPA y sólo el 2.5 % usa el protocolo WPA2. En nuestra opinión, hay una obligación por parte de las empresas de telecomunicaciones para clarificar y dilucidar sobre las amenazas que nos rodean.

En general, recomiendo para el uso de una red inalámbrica en toda empresa o entidad, y por qué no, 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, letras mayúsculas y minúsculas, números, entre otros signos). Elegir un nombre sin conclusión sobre el dueño de la red, la desactivación de configuración del Access Point sobre el WLAN, sino siempre sobre el cableado, así como apagar el Access Point u otros equipos inalámbricos cuando no se usan. También se puede disminuir el alcance del Access Point a través de la actualización del 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 Point, 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.

(*) Gerente General de Fon Perú S.A.C.