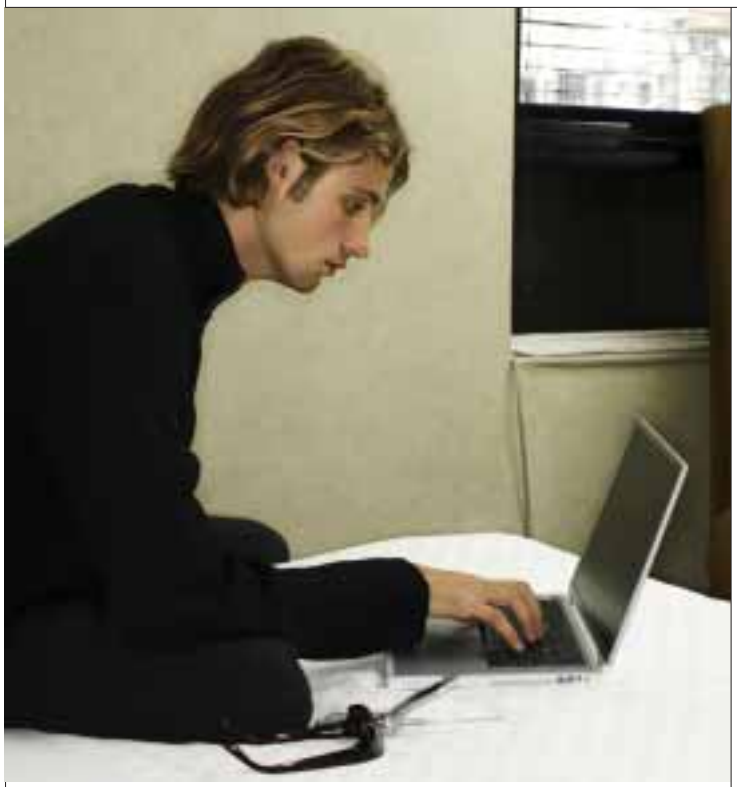
Asegure su red inalámbrica



Existen dos usos muy comunes a la redes inalámbricas:

- Como acceso a Internet en casa
- Como extensión de la red cableada (LAN)

ACCESO EN CASA

Regularmente, un acceso a Internet por ADSL y módem/router inalámbrico no ofrece mucho más que WEP para proteger. Como se ha visto, esta protección no es muy eficaz, pues aunque no se genere mucho tráfico, alguien con paciencia logrará obtener los 400,000 IV para crackear su llave WEP o incluso reinyectar paquetes con aireplay.

Una opción es reemplazar su equipo inalámbrico por uno que soporte WPA por lo menos. Los clientes de Microsoft Windows (zero configuration) soportan ahora WPA.

LINK

www.microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en

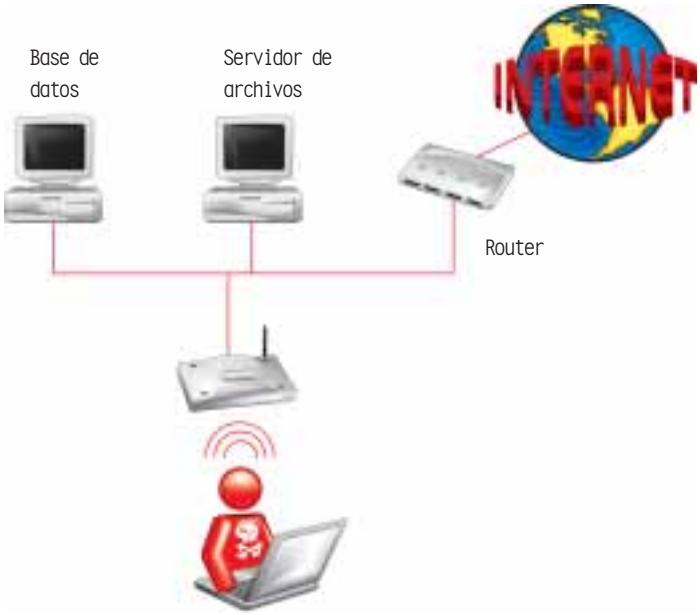
Como se verá, las opciones que se ofrecen a la empresas también pueden aplicar en la casa mediante un cierto costo.

EXTENSIÓN DE LA LAN

Las empresas no pueden dejar la problemática inalámbrica de lado, porque alguien que logra tener acceso a la red inalámbrica tiene acceso a toda la red vista desde dentro como un usuario conectado a la LAN.

Hoy todos estamos preocupados por los peligros desde afuera, pero ¿quién se preocupa de lo que hacen sus usuarios?, pues casi nadie porque son de "confianza". El grave problema es que alguien llegando por la red inalámbrica que acaban de estrenar será parte de estos usuarios de "confianza" ¡y podrá navegar sin problema a través de su infraestructura!

Red inalámbrica en muchas empresas:

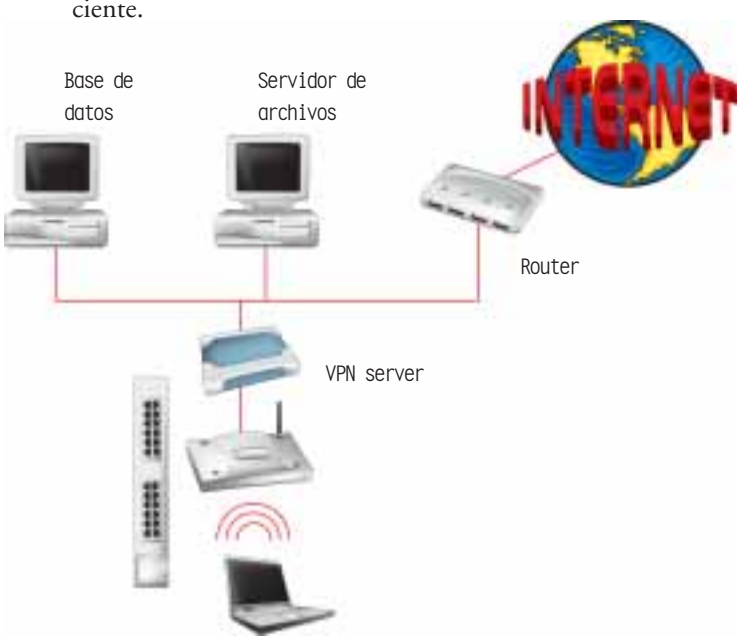


La primera cosa que que debe hacerse es tomar conciencia de este peligro y asegurar la red.

¿QUÉ PUEDE HACERSE PARA ELLO?

- 1.- **Manejar la ubicación de los AP**: no dejar, si posible, AP abiertos a la calle, si es posible bajar la potencia de emisión y comprobar el alcance.
- 2.- **Configurar el AP**: no dejar la configuracion de fábrica, poner una contraseña fuerte para la administración.
- 3.- **Deshabilitar broadcast SSID**: aunque no sea algo de seguridad, se protegerá de los "script-kiddies" que juegan con netstumbler.

• 4.- **Aplicar WEP 128**: si no puede autenticar y/o usar WPA, mejor esto que nada.
• 5.- **Autentificar los usuarios**: implementar WPA o mejor WPA2 que empieza a estar soportado por varios fabricantes.
• 6.- Autentificar los usuarios: implementar PEAP/EAP-TTLS en conjunto con un servidor RADIUS para el acceso a la red.
• 7.- **Cifrar**: la autenticación solamente brinda acceso al usuario pero no se preocupa por cifrar los datos, así que se debe implementar WPA o WPA2 adicionalmente. Si solamente tienen WEP a su disposición, una opción es usar IPSEC con un servidor de VPN/Firewall. Una máquina con Linux es suficiente.



• 8.- **Monitorear la red inalámbrica**: es una buena idea monitorear su red, para detectar rogue AP (AP que no son parte de su empresa), máquinas asociadas, y ataques potenciales. Varios programas permiten hacer esto, entre ellos:
• Airsnare [1]: verifica si no hay MAC desconocidas que se asocian
• WIDS, WIDZ [2]: IDS para ambientes inalámbricos, detectan ataques físicos (jamming)
• Netstumbler [3]: netstumbler permite monitorear la potencia de los AP
• Wifiscanner [4]: escaner de redes inalámbricas, tiene un modulo IDS.
• Airdefense [5]: lo mejor de lo mejor, producto comercial
• 9.- **Monitorear su red LAN**: un IDS monitorea el tráfico que transita en la red. Existen varios IDS que detectan ataques. Este punto no tiene que ver específicamente con el aspeto inalámbrico, pero siempre es bueno tener un IDS (¡y checar los logs!).
• 10.- **Plan de seguridad**: si es posible, en caso de no usar un modo de autenticación/encripción fuerte, planee una segmentación de la red a través de un firewall y monitoree el tráfico para detectar alguna intrusión.
• 11.- **Contraseñas fuertes**: no lo diremos suficientemente, pero una buena contraseña es un buen comienzo, así que no permita contraseñas sencillas (LEAP o WPA-PSK no son realmente vulnerables si se usan contraseñas fuertes). Esta es la problemática número uno de las empresas hoy...

Muchos dicen que una contraseña fuerte es una mezcla de números, letras, minúsculas y mayúsculas, que se vuelve una pesadilla para los usuarios. Hay una forma de hacer aceptar a los usuarios una contraseña fuerte sin que sea imposible de recordar.

Por ejemplo: "yomellamofabien" ¡es una buena contraseña! Por lo menos es mejor que "fabien".

CONCLUSIÓN

El corazón de la seguridad tiene tres conceptos:
• Autentificar: PEAP/EAP-TTLS + Radius
• Cifrar de forma eficiente: WPA/WPA2
• Monitorear

Muchas veces no se tiene la posibilidad de usar WPAo WPA2 ni tener un servidor Radius en casa, así que se puede instalar un IDS de cualquier forma o monitorear el tráfico por lo menos. En el caso empresarial se debe planear y dar la importancia necesaria al acceso inalámbrico ya que se instala, se pone la WEP key y se olvida para siempre, ¡lo que no hay que hacer!

Si tienen preguntas sobre esta serie de artículos serán bienvenidos en nuestro foro en: www.conthackto.com.mx

LINK

[1] Airsnare: home.comcast.net/~jay.deboer/airsnare/
[2] Wireless IDS: www.zone-h.org/en/download/category=18/
[3] Netstumbler: www.netstumbler.com
[4] WifiScanner: wifiscanner.sourceforge.net
[5] Airdefense: www.airdefense.net/