Metodología de Análisis de la Seguridad en redes Wi-Fi
Analysis Methodology of Security Wi-Fi networks

Juan Ceballos [1] Elías Bedoya [2]

[1] Programa de Ingeniería en Sistemas, Fundación Universitaria Tecnológico Comfenalco, Cartagena, Colombia.

[2] Coordinación de investigación, Programa de Seguridad e Higiene Ocupacional, Fundación Universitaria Tecnológico Comfenalco. Grupo CIPTEC, Cartagena, Colombia.

{jceballos,ebedoya}@tecnologicocomfenalco.edu.co

Resumen.

En la actualidad las redes Wi-Fi se han masificado enormemente. Su relativo bajo costo en la instalación y la gran movilidad que ofrecen las coloca como la primera opción al momento de crear una red de área local. El tema de la seguridad en este tipo de redes no se debe descuidar en ningún momento ya que su principal ventaja puede ser su gran debilidad: cualquier persona en el radio de cobertura podría acceder ilegalmente a la red si no se cuentan con parámetros adecuados de seguridad. El presente proyecto propone una metodología para el análisis de la seguridad de las redes Wi-Fi que además de cumplir con los estándares actuales, se adapte a las necesidades de diferentes tipos de usuarios de tal forma que se garantice la confiabilidad e integridad de la información que por ellas circula, de tal manera que después de examinar los protocolos y vulnerabilidades que existan, se ofrece una solución de cómo configurar una red Wi-Fi para diferentes tipos de usuarios: casa, micro, pequeña, mediana y gran empresa. Para desarrollar esta metodología, se establecieron unas actividades previas y unas fases de elaboración que incluyen esas actividades. Como toda metodología de análisis se debe hacer un examen inicial de la infraestructura tecnológica, las necesidades y tamaño de la red para luego pasar a detectar las posibles debilidades y subsanarlas.

Palabras clave: Redes Wi-Fi, seguridad en redes, protocolos, vulnerabilidades.

Abstract.

Currently, Wi-Fi networks have been massively multiplied. The relatively low installation cost and the great mobility they offer place them as the first choice when creating a local area network. The issue of security in this type of network should not be neglected at any time since its main advantage may be its great weakness: anyone within the radius of coverage could illegally access the network if they do not have adequate security parameters. The present project proposes a methodology for the analysis of the security of the Wi-Fi networks that besides complying with the current standards is adapted to the needs of different types of users in a such way that guarantee the reliability and integrity of the information that circulates through them, so that after examining the protocols and vulnerabilities that exist, offers a solution on how to configure a Wi-Fi network for different types of users: home, micro, small, medium and large company.

In order to develop this methodology, previous activities and elaboration phases that included these activities were established. Like all methodology of analysis, an initial examination of the technological infrastructure is needed, the needs and size of the network must be made to later detect the possible weaknesses and correct them.

Keywords: Wi-Fi networks, network security, protocols, vulnerabilities.

1 Introducción

En los últimos años el mundo se ha vuelto 'móvil'. Las personas necesitan conectividad en cualquier momento y en cualquier lugar, donde antiguos sistemas de interconexión cableados se han ido reemplazando por variadas tecnologías de interconexión inalámbricas: BlueTooth , WiMax , Wi-Fi. El presente trabajo se centra en la tecnología Wi-Fi conocida como el estándar más ampliamente difundido para crear redes de área local inalámbricas [1]. Conforme a lo anterior se puede apreciar que la implantación de este tipo de redes para interconectar equipos inalámbricamente y navegar por Internet es muy apetecida por los usuarios en el hogar y las empresas. El problema es que cada tipo de usuario de los antes mencionados tiene necesidades de interconexión diferentes y si a esto le sumamos que no se cuenta con unas nociones básicas de seguridad se puede llegar a comprometer seriamente la seguridad de la información, elemento vital y diferenciador en el mundo actual. El presente trabajo presenta una metodología para analizar la seguridad en las redes Wi-Fi de tal manera que después de examinar los protocolos y vulnerabilidades que existan se ofrece una solución de cómo configurar una red Wi-Fi para diferentes tipos de usuarios: casa, micro, pequeña, mediana y gran empresa. Además, se mostrará el impacto que genera en la competitividad de la organización tener una red Wi-Fi segura.

El problema de la seguridad es inherente a cualquier tipo de red. En las redes Wi-Fi se hace más palpable ya que en teoría al atacante solo le basta con estar en el radio de acción para emprender la acción delictiva. Si a lo anterior le sumamos que la instalación de una red Wi-Fi puede hacerse muy 'simple' ya que para muchos administradores de red la simple conectividad es suficiente, dejando de lado pasos que dejan huecos de seguridad que comprometen la integridad del sistema lo que desemboca en una continua alza de redes Wi-Fi inseguras [2]. Por esto, se debe contar con una metodología clara y un manual de buenas prácticas que dependiendo del tipo de usuario permita configurar una red Wi-Fi que cumpla con altos estándares de seguridad garantizando la integridad, confidencialidad y disponibilidad de la información que por ellas circula. Por lo anterior, se prevé desarrollar una metodología para el análisis de la seguridad de las redes Wi-Fi que además de cumplir con los estándares actuales se adapte a las necesidades de diferentes tipos de usuarios de tal forma que se garantice la confiabilidad e integridad de la información que por ellas circula.

Al desarrollar dicha metodología para analizar la seguridad en las redes Wi-Fi partiendo de su definición para luego detallar las vulnerabilidades que existen y la forma de evitarlas estudiando los diferentes protocolos que permiten conectarse a una red Wi-Fi, para de esta forma ofrecer una solución que se adapte a las necesidades de los usuarios de casa, de las micro, pequeñas, medianas y grandes empresas.

Para desarrollar una metodología de análisis de la seguridad en redes Wi-Fi se debe establecer unas actividades previas y unas fases de elaboración que incluyan esas actividades. Como toda

metodología de análisis se debe hacer un examen inicial de la infraestructura tecnológica, las necesidades y tamaño de la red para luego pasar a detectar las posibles debilidades y subsanarlas.

Las actividades necesarias para este proceso son:

- Revisión de los equipos de cómputo y la infraestructura Wi-Fi
- Adquisición de los equipos correspondientes
- Creación de una política de contraseñas a utilizar
- Configuración de los dispositivos de acceso y los métodos de autenticación y encriptación elegidos
- Configuración de los dispositivos que usarán la red Wi-Fi
- Prueba de conectividad
- Revisión de la política instaurada

El cada vez mayor auge que experimentan las redes Wi-Fi y las mejores tecnologías usadas hacen que este tipo de redes seas muy atractivas para diferentes tipos de usuarios. Además, la facilidad en su instalación reduce los costos asociados a tener una red de computadoras. El problema surge cuando no se tiene la suficiente información en materia de seguridad y se configuran redes totalmente expuestas que comprometen seriamente la integridad de los datos que por ellas circulan.

Por esto, el presente proyecto ofrece una metodología clara y precisa sobre como configurar una red Wi-Fi segura que además sea escalable y adaptable a la mayoría de usuarios que las usan. Es evidente que las necesidades en materia de conectividad varían mucho de un tipo de usuario a otro, pero lo que debe ser común a todos es una correcta política de seguridad que garantice que los recursos ofrecidos por la red solo sean utilizados por los usuarios correctos, teniendo en cuenta los costos asociados a la implantación de dicha política y haciendo uso de tecnologías estandarizadas, garantizando de este manera la confiabilidad e integridad de la información que por dichas redes circula.

2 Diseño de la metodología

La metodología que se propone se debe adaptar a cualquier tipo de empresa y usuario de casa que quiera construir una red Wi-Fi segura. Para ello cada una de las actividades descritas en el apartado anterior se deben tener claras para luego proceder a ejecutar la metodología en sí.

A modo de aclarar todo el concepto y establecer correctamente la ruta a seguir, a continuación, se describirán cada una de esas actividades y el alcance que tienen dentro del proyecto.

Actividad 1: Revisión de los equipos de cómputo y la infraestructura Wi-Fi

- *Descripción detallada:* Se revisarán cada uno de los equipos de cómputo que van a hacer uso de la red Wi-Fi para ver si cuentan con la configuración adecuada del sistema operativo y constatar que la tarjeta inalámbrica soporte el protocolo de autenticación requerido. También se inspeccionará la configuración de los dispositivos que brindan acceso con el fin de asegurarse que soporte el protocolo de autenticación que se utilizará.

- *Alcance:* El alcance de esta actividad es asegurarse que se cuenta con los requisitos mínimos en materia de hardware para poder implementar la solución propuesta.
-

Actividad 2: Adquisición de los equipos correspondientes

- *Descripción detallada:* En la primera actividad se hizo una revisión general del estado de los equipos de hardware y software que dan soporte a la red Wi-Fi. Si se nota alguna falencia en este paso se procede a la adquisición de los equipos necesarios para implementar la solución.
- *Alcance:* Si después de la revisión anterior se hace evidente la adquisición de nuevos equipos, esta actividad se asegura de que sean los adecuados.

Actividad 3: Creación de una política de contraseñas a utilizar

- *Descripción detallada:* La autenticación a una red Wi-Fi segura debe hacerse mediante contraseñas. Los dispositivos que brindan conectividad también deben tener contraseñas que impidan el acceso a personal no autorizado. En apartados anteriores se hizo referencia a un documento que propone una metodología para crear contraseñas seguras.
- *Alcance:* Crear unas contraseñas robustas de acuerdo a los estándares actuales sobre el uso y manipulación de contraseñas.

Actividad 4: Configuración de los dispositivos de acceso y los métodos de autenticación y encriptación elegidos

- *Descripción detallada:* De acuerdo a lo visto en capítulos anteriores, de los muchos protocolos que existen actualmente para la conexión segura a redes Wi-Fi, no todos son lo suficientemente eficientes. Esta actividad consiste en configurar los dispositivos de acceso con los protocolos más robustos que existen actualmente. También se configurará el método de autenticación de usuarios más adecuado.
- *Alcance:* Configurar adecuadamente el protocolo de encriptación y de autenticación para la transmisión de los datos y la autenticación de usuarios en la red Wi-Fi.

Actividad 5: Configuración de los dispositivos que usarán la red Wi-Fi

- *Descripción detallada:* Los computadores y/o dispositivos inalámbricos que usarán la red, deben contar con los mismos protocolos que se configuraron en el apartado anterior. En esta actividad se configurarán cada uno de esos equipos para que usen dichos protocolos y se conecten de manera segura a la red.
- *Alcance:* Garantizar la compatibilidad entre todos los dispositivos que harán uso de la red Wi-Fi.

Actividad 6: Prueba de conectividad

- *Descripción detallada:* Se hacen diferentes pruebas para ver si la red cumple su función. Las pruebas consisten en revisar si los diferentes equipos están interconectados y pueden acceder a la información que requieran, así como a Internet sin problemas.
- *Alcance:* Garantizar la conectividad a través de la red Wi-Fi configurada.

Actividad 7: Revisión de la política instaurada

- *Descripción detallada:* Se examina paso a paso cada actividad del proyecto.
- *Alcance:* Revisar si no se ha pasado nada por alto y que todo esté conforme al plan trazado.

2.1 Desarrollo de la metodología

Después de analizar cada una de las actividades y tomando como referencia las buenas prácticas estipuladas para la gestión de proyectos [3], construir una red Wi-Fi segura consta de las siguientes etapas:

- Inicio
- Planeación
- Ejecución
- Seguimiento y control
- Cierre

A continuación, se describirán cada una de estas etapas.

Fase 1: Inicio

Esta es la fase inicial del proyecto. Luego de detectar la necesidad de tener una red Wi-Fi segura, se procede a planificar todo el trabajo necesario para llegar a esa meta. Se debe tener claro el objetivo del proyecto y que la consecución del mismo requiere de un esfuerzo en tiempo y dinero. Cada usuario tiene unas necesidades diferentes pero la metodología que aquí se propone es fácilmente adaptable.

Fase 2: Planeación

Incluye las siguientes actividades, cada una con sus respectivas acciones:

- Revisión de los equipos de cómputo y la infraestructura Wi-Fi de la empresa
  Acciones:
  1. Verificar el alcance y las necesidades de la red Wi-Fi a configurar.
  2. Especificar los tipos de usuarios y los tipos de accesos que tendrán. Si se necesita conexión a Internet es necesario contratar el servicio con algún ISP del mercado.
  3. Verificar que los computadores que van a tener acceso a la red Wi-Fi cuenten con un adaptador de red inalámbrico. Este adaptador debe ser compatible con el protocolo de seguridad WPA2[4].
  4. Verificar que los Sistemas Operativos de los computadores estén actualizados y que tengan protección antivirus.
  5. Verificar que se cuenta con dispositivos de acceso modernos que sean compatibles con el protocolo de seguridad WPA2.

Fase 3: Ejecución

En esta fase se procede a configurar la red de conformidad con las siguientes actividades:

- Adquisición de los equipos correspondientes
  Acciones:
  1. Si la fase de planeación detectó que hacen falta equipos se procede a su adquisición. También si es necesario actualizar alguno se hace.
- Creación de una política de contraseñas a utilizar
  Acciones:
  1. Para garantizar la seguridad de la red Wi-Fi se necesita una política actual sobre el manejo de las contraseñas.
  2. Es recomendable usar contraseñas complejas de más de ocho caracteres que tengan combinación de letras y números.
  3. Estas contraseñas no deben quedar en un lugar desprotegido y su accesibilidad debe ser lo más restringida posible.
- Configuración de los dispositivos de acceso y los métodos de autenticación y encriptación elegidos
  Acciones:
  1. Cambiar las contraseñas por defecto de los dispositivos de interconexión. Deshabilitar administración inalámbrica y la administración remota de dichos dispositivos. Entre menos posibilidades de acceso haya, es mucho mejor la administración.
  2. El estándar IEEE 802.11[5] define las normas de funcionamiento de las redes Wi-Fi. Con esto se busca garantizar la conectividad e interoperabilidad de los diferentes dispositivos fabricados. A medida que la tecnología avanza se crean o mejoran protocolos existentes dando como consecuencia mayor seguridad y mayor velocidad, entre otras. Cuando un nuevo estándar es creado casi siempre se agrega una letra al nombre, por ejemplo 802.11g o 802.11n. La red debe operar con dispositivos actualizados.
  3. Cambiar el SSID por defecto.
  4. Habilitar filtro de direcciones MAC y configurarlo para que solo acepte las direcciones de los computadores que se quieren conectar.
  5. Establecer un método de encriptación de los datos y otro para la autenticación de los usuarios [6]. Este tópico es el pilar fundamental del proyecto. Existen muchos métodos de encriptación de datos, unos más seguros que otros, pero si se quiere contar con una red Wi-Fi que cumpla los estándares de seguridad existentes se debe escoger como método de encriptación de datos WPA2 con el algoritmo de cifrado AES. Utilizando este método se cuenta con una red Wi-Fi que cumple los requerimientos de seguridad del gobierno de los Estados Unidos de América. La autenticación de los usuarios depende del tipo de red que se quiere y de la capacidad de la empresa que la crea.
  6. Guardar todas las configuraciones y hacer una copia de seguridad de los archivos de configuración.

- Configuración de los dispositivos que usarán la red Wi-Fi
  Acciones:

1. Se instalan y configuran los dispositivos que usarán la red inalámbrica.
2. La configuración debe ser acorde a los parámetros definidos en fases anteriores.

Fase 4: Seguimiento y control

Hay que verificar que la política quede bien instaurada. En esta fase se revisa que la red Wi-Fi cumpla con los estándares propuestos. Eso se hace por medio de las siguientes actividades:

- Prueba de conectividad
  Acciones:
  1. Realizar pruebas locales de conectividad.
  2. Revisar que haya acceso a Internet (si se requiere) en cada dispositivo configurado.

- Revisión de la política instaurada
  Acciones:
  1. Empezar desde la primera actividad y repasar paso a paso la configuración aplicada.

Fase 5: Cierre

El proyecto se da por terminado cuando se logra configurar la red Wi-Fi de conformidad con los parámetros descritos en las fases anteriores.

2.1 Tipo y nivel de investigación

El tipo de investigación que se hará es la aplicada puesto que se tienen los conocimientos adecuados en materia de seguridad en las redes Wi-Fi y lo que se quiere es enfocarlo a diferentes tipos de usuarios con el fin de ofrecer una solución práctica y eficiente que se adapte a las necesidades particulares de cada uno.

El nivel de la investigación es explicativo ya que se quiere mostrar una relación de causa al describir el problema, mirar los factores que lo originan y ofrecer posibles soluciones.

2.2 Método y diseño de la investigación

Se utilizarán los siguientes métodos en la investigación realizada:

- Descriptivo
- Explicativo
- Deductivo
- Inductivo
- Análisis
- Síntesis

En cuanto al diseño de la investigación será experimental puesto que se está planteando una metodología de análisis de seguridad en redes Wi-Fi nueva apoyada en un análisis previo de los factores que hacen vulnerable una red Wi-Fi y con base en las necesidades de los usuarios plantear posibles soluciones.

2.3 Análisis de resultados según el tipo de usuario

En esta sección se ofrecerán soluciones concretas para cada tipo de usuario definido en el alcance del presente proyecto. La intención es que después de revisar la metodología propuesta y aplicar las buenas prácticas definidas, se pueda plantear una solución de cómo configurar una red Wi-Fi segura según las características del entorno.

Para configurar una red Wi-Fi por cada tipo de usuario se tendrán en cuenta los siguientes factores:

- Estabilidad
- Inversión
- Robustez
- Escalabilidad

Además, en los parámetros a utilizar para garantizar la integridad y confidencialidad de los datos están:

- Método de autenticación utilizado
- Método de encriptación utilizado

Entonces, para cada tipo de usuario se dará una ponderación (alta o baja) de cada uno de los factores y con base en eso se usará un método de autenticación y encriptación teniendo siempre presente la metodología planteada y el gran norte de todo: tener una red Wi-Fi que cumpla con los estándares actuales de seguridad que se adapte a las necesidades de los usuarios.

2.4 Hogar

- Estabilidad: Alta
- Robustez: Baja
- Inversión: Baja
- Escalabilidad: Baja

- **Autenticación:** En aras de minimizar costos el método de autenticación de usuarios para este tipo de redes Wi-Fi debe ser PSK (Pre Shared Key) por su relativo bajo costo puesto que cualquier punto acceso del mercado lo ofrece dentro de sus parámetros de configuración. Es preciso señalar la robustez de la contraseña a utilizar de acuerdo a los lineamientos expuestos en capítulos anteriores.
- **Encriptación:** El estándar actual más robusto y eficiente que existe para proteger los datos que circulan por una red Wi-Fi es utilizar el protocolo WPA2 con el algoritmo de cifrado AES. Hay que tener presente que este método de encriptación es relativamente nuevo y algunos

dispositivos antiguos no lo tienen implementado por lo que se deben aplicar las actualizaciones necesarias. En caso de que no sea posible una alternativa sería usar WPA TKIP, pero se hace la salvedad que este mecanismo hereda algunas fallas de WEP y su uso queda limitado a redes Wi-Fi de hogar sencillas que no transmitan información altamente sensible [7].

2.5 Pequeña empresa

- **Estabilidad:** Alta
- **Robustez:** Baja
- **Inversión:** Baja
- **Escalabilidad:** Baja

- **Autenticación:** En aras de minimizar costos el método de autenticación de usuarios para este tipo de redes Wi-Fi debe ser PSK (Pre Shared Key) por su relativo bajo costo puesto que cualquier punto acceso del mercado lo ofrece dentro de sus parámetros de configuración. Es preciso señalar la robustez de la contraseña a utilizar de acuerdo a los lineamientos expuestos en capítulos anteriores.
- **Encriptación:** El estándar actual más robusto y eficiente que existe para proteger los datos que circulan por una red Wi-Fi es utilizar el protocolo WPA2 con el algoritmo de cifrado AES. Hay que tener presente que este método de encriptación es relativamente nuevo y algunos dispositivos antiguos no lo tienen implementado por lo que se deben aplicar las actualizaciones necesarias y realizar las inversiones pertinentes.

2.6 Mediana empresa

- **Estabilidad:** Alta
- **Robustez:** Alta
- **Inversión:** Baja
- **Escalabilidad:** Alta

- **Autenticación:** Una mediana empresa está en constante crecimiento. Las inversiones hechas en etapas tempranas repercuten en ganancias o pérdidas más adelante. Por esto, no se debe dejar de lado la seguridad Wi-Fi, eso sí, sin incurrir en costos excesivos. Para autenticar a los usuarios los administradores de las redes Wi-Fi de las medianas empresas deben usar cualquier método descrito en el estándar 802.1x / EAP [8] que se adapte a las necesidades particulares de la organización.
- **Encriptación:** El estándar actual más robusto y eficiente que existe para proteger los datos que circulan por una red Wi-Fi es utilizar el protocolo WPA2 con el algoritmo de cifrado AES. Hay que tener presente que este método de encriptación es relativamente nuevo y algunos dispositivos antiguos no lo tienen implementado por lo que se deben aplicar las actualizaciones necesarias y realizar las inversiones pertinentes.

2.7 Gran empresa

- **Estabilidad:** Alta
- **Robustez:** Alta

- **Inversión:** Alta
- **Escalabilidad:** Alta

- **Autenticación:** Este tipo de empresas tiene los medios suficientes para hacer inversiones en materia de seguridad. El mecanismo de autenticación que se debe usar es un servidor RADIUS [8] que sirva de autenticador y pueda negociar contraseñas diferentes por cada tipo de usuario para de esta manera lograr un alto grado de fiabilidad y garantizar que los usuarios conectados son los que en verdad deben hacerlo. Obviamente implementar este mecanismo incurre en unos costos que a la larga terminan siendo una inversión con un rápido retorno ya que una gran empresa puede ser objeto constante de ataques de diferente índole.
- **Encriptación:** El estándar actual más robusto y eficiente que existe para proteger los datos que circulan por una red Wi-Fi es utilizar el protocolo WPA2 con el algoritmo de cifrado AES. Hay que tener presente que este método de encriptación es relativamente nuevo y algunos dispositivos antiguos no lo tienen implementado por lo que se deben aplicar las actualizaciones necesarias y realizar las inversiones pertinentes. Otro método dejaría la red insegura y una empresa siempre debe velar por proteger su principal activo: la información.

2.8 Cobertura

La cobertura de la investigación se especifica a continuación:

- Universo: Usuarios de redes Wi-Fi que se preocupan por la seguridad e integridad de la información.
- Muestra: La metodología propuesta se basa en le experiencia del investigador y es aplicada en los siguientes escenarios:
    - Wi-Fi en la casa: Como usuario de una red Wi-Fi en la residencia se tiene conocimiento de la forma como operan.
    - Wi-Fi en la micro y pequeña empresa: Como ingeniero desarrollador y encargado de la red interna de una pequeña empresa se conocen las configuraciones mínimas de seguridad con una buena relación costo – beneficio
    - Wi-Fi en la gran empresa: Como docente en dos grandes universidades de la región se ha indagado e investigado en las necesidades en materia de conectividad de este tipo de empresas.

De acuerdo a lo anterior, la experiencia en el área es extensa y además se cuenta con una muestra amplia que garantiza una correcta comprobación de la metodología planteada y su aplicabilidad práctica.

3 Conclusiones

Cuando se implementa o se adopta una tecnología es requisito indispensable conocer todas sus capacidades, limitaciones y los riesgos asociados. El conocimiento de los aspectos de seguridad asociados a las redes Wi-Fi garantiza la integridad, autenticidad y confidencialidad de la información que por ellas circula, lo que impacta enormemente en la competitividad de las empresas. Y es que el alto grado de madurez del que goza la tecnología Wi-Fi la hace candidata número uno para ofrecer conectividad a bajo costo y buen rendimiento.

Es por esto que la falsa concepción de inseguridad que rodeaban a las redes Wi-Fi ha quedado en el pasado. Actualmente las redes Wi-Fi pueden ser tan seguras como sus homologas cableadas siempre y cuando se apliquen las políticas de seguridad correctas, las cuales están estipuladas en el estándar IEEE 802.11i. Es más, en algunos se puede considerar a las redes Wi-Fi más seguras que las cableadas. Ejemplo de esto son empresas que proporcionan todos los mecanismos de seguridad a sus redes Wi-Fi, pero con solo conectar un cable al punto de enlace más cercano se puede acceder a todos los recursos de la red sin problemas.

Una de las grandes cosas a tener en cuenta para garantizar la seguridad en una red Wi-Fi es la elección de los algoritmos de encriptación y autenticación adecuados. Desafortunadamente muchos administradores de red pasan esto por alto utilizando el protocolo WEP que no ofrece ningún esquema de seguridad actualmente. El protocolo más seguro que su puede usar es el descrito en el estándar IEEE 802.11i o mejor conocido como WPA2. No existe a la fecha incidentes que hayan comprometido la seguridad de una red Wi-Fi que use dicho protocolo.

En lo referente al sector empresarial no se deben escatimar esfuerzos para mantener la infraestructura de conectividad segura. Como se demostró en capítulos anteriores las consecuencias por descuidar este aspecto pueden ser desastrosas. Es deber de toda empresa contar con alguien capacitado en esta área y tratar en lo posible de ofrecerle los medios adecuados para realizar su labor. Como punto final es necesario enfatizar en que no existe sistema 100% ya que la propia naturaleza del ser humano lo lleva a cometer errores (intencionada o no intencionadamente) que ponen en riesgo la seguridad. Lo que sí se puede hacer es minimizar dichos errores y en caso de que ocurran tomar las acciones respectivas.

Recomendaciones

Configurar una red Wi-Fi segura no es una tarea muy compleja, lo que se debe considerar siempre es el tipo de usuario y las necesidades particulares de conectividad para utilizar una u otra herramienta. Las siguientes recomendaciones son aplicables a cualquier entorno y suponen unas sugerencias prácticas para tratar de proteger al máximo la información que circula por una red Wi-Fi.

1. Antes de comenzar a configurar la red revisar si los dispositivos involucrados están actualizados y soportan los protocolos de seguridad exigidos.
2. Cambiar las configuraciones y contraseñas por defecto de los dispositivos de acceso ya que son de dominio público [9].
3. Utilizando siempre protocolos de encriptación y autenticación. Para encriptar los datos el estándar más robusto y eficiente que existe actualmente es el protocolo WPA2 con el algoritmo de cifrado AES. La autenticación depende del tipo de usuario: PSK para usuarios de casa y pequeñas empresas y cualquier método descrito en el estándar 802.1x / EAP para medianas y grandes empresas [10].
4. No confiar siempre en los dispositivos que se conectan a la red ya que la propia naturaleza de estas incentiva la ‘promiscuidad’ de los mismos, lo que puede comprometer las políticas de seguridad instauradas.

5. Por último, utilizar siempre el sentido común y entender que la naturaleza humana involucrada en lo que se hace conlleva a errores que deben subsanarse lo más pronto posible.

BIBLIOGRAFÍA

1. Li, H.,Xu, Z.,Zhu, H.,Ma, D.,Li, S.,Xing, K.: Demographics inference through Wi-Fi network traffic analysis. Proceedings - IEEE INFOCOM. Volume 2016-July, 27 July 2016, 35th Annual IEEE International Conference on Computer Communications Article number 7524528.
2. Fong, K.K.-K.ab. , Wong, S.K.S.:Wi-Fi adoption and security in Hong Kong. Asian Social Science Volume 12, Issue 6, June 2016, pp 1-22
3. Morabito, V.: Big data and analytics: Strategic and organizational impacts., Department of Management and Technology, Bocconi University, Milan, Italy . 2015, Pages 1-183
4. Yang, C., Gu, G.: Security in wireless local area networks. Wireless Network Security: Theories and Applications. 1 June 2013, Pages 39-58
5. Cruz Felipe, MR., Martínez, Reinier., Crespo, Y.: Análisis de la QoS en redes inalámbricas. Rev cuba cienc informat.7(1) (2013) 86-96
6. Stallings, W.: Cryptography and Network Security: Advance Encrypcion Standar. Prentice Hall. 5(2011) 148-174
7. Stallings, W.: Network Security Essentials: Wireless Network Security. Prentice Hall. 4(2011)197-204
8. Arana, JR., Villa, LA., Polanco, O.: Implementación del control de acceso a la red mediante los
9. protocolos de autenticación, autorización y auditoría. Iingeniería Eléctrica y Electrónica. 15(1) (2013) 127-137
10. Voutssas, M.: Preservación documental digital y seguridad informática. Investig. bibl (24)50 (2010)127-155.
11. Cabarcas, A., Puello, P., Martelo, RJ., Sistema de Información Soportado en Recuperación XML para Pequeñas y Medianas Empresas (PYME) de Cartagena de Indias, Colombia. Inf. tecnol. (26)2 (2015) 135-144