CONSULTORÍA PARA LA DETERMINACIÓN DE BRECHAS DE SEGURIDAD EN UNA RED INALÁMBRICA

Anabel Castillo Mora[1], Roberto Cabezas Cabezas[2], José Escalante[3]

[1]Ingeniera en Electrónica y Telecomunicaciones 2005
[2]Ingeniero en Electrónica y Telecomunicaciones 2005
[3]Director de Tópico, Ingeniero Eléctrico y Electrónico, Escuela Superior Politécnica del Litoral, 1996, Profesor de la ESPOL desde 1996., email: jescala@espol.edu.ec

RESUMEN

Las redes inalámbricas cuentan con una excelente acogida gracias a sus características de flexibilidad y movilidad. Su falencia se encuentra en su medio de transmisión. El aire es un medio abierto que permite que cualquier receptor tenga acceso a los datos transmitidos en una WLAN.

Existen muchos métodos para combatir los problemas de seguridad de las redes inalámbricas. El problema surge al momento de seleccionar la más adecuada. En este proyecto se realiza un análisis de los diferentes métodos de seguridad disponibles para las redes inalámbricas. Se realizó un caso de estudio en el cual se revisó las condiciones de seguridad de una red y se determinó e implementó un sistema de seguridad. Posteriormente se creó un procedimiento para realizar una consultoría que permita determinar las necesidades de seguridad de una WLAN para finalmente proponer tres soluciones que se ajustan a las necesidades de cada red.

La implementación de una de estas soluciones más la correcta administración de la red inalámbrica permitirá una seguridad efectiva que haga posible aprovechar las ventajas de las WLAN.

ABSTRACT

Wireless networks are widely used because of their flexibility and mobility. Their flaw lies in their transmission means. Air is an open medium that allows any receiver access to the data transmitted over a WLAN.

There are many methods to solve the security issues in wireless networks. The problem arises when choosing the most adequate solution. In this project there is an analysis of the different methods of security available for wireless networks. A study was done in which the security conditions of a network where revised and a security system was implemented. Then a procedure was created that would allow a survey that will let us determine the security needs of a WLAN and finally propose three solutions that will fit the security needs of each network.

Deploying one of these solutions along with the correct administration of the wireless network will permit a successful security that makes it possible to take advantage of the multiple qualities of a WLAN.

INTRODUCCION

Las redes inalámbricas de área local o WLAN (Wireless Local Area Networks) están transformando la forma de comunicarnos. No solo son más flexibles y escalables que las redes de área local cableadas, también nos permiten armar redes en lugares en donde el cableado es un limitante. Actualmente en el Ecuador la implementación de redes inalámbricas es un considerable segmento de las redes de comunicación. Sin embargo, además de sus diversas ventajas, las redes WLAN tienen un gran inconveniente, su vulnerabilidad a ataques de seguridad.

El objetivo de este proyecto es crear un procedimiento para evaluar el problema de inseguridad de las redes inalámbricas. Por medio de una consultoría se pretende determinar cuales son las brechas de seguridad en la implementación de una WLAN. Presenta sugerencias de posibles implementaciones que refuerzan la seguridad de la red logrando erradicar sus inseguridades.

CONTENIDO

Los avances más relevantes con respecto a la seguridad WLAN son:

- El WPA (Wi-Fi Protected Access) es un estándar de seguridad que resuelve los problemas de cifrado del WEP mediante actualizaciones de hardware.
- El estándar 802.1x con EAP sistema adaptado a las redes inalámbricas que ofrece control de acceso al medio y autenticación.
- Redes VPN que crean túneles de conexión segura.
- Sistemas propietarios.

Cada uno provee un nivel de seguridad que viene a un costo. Lo ideal sería implementar la seguridad más robusta para cada red pero lamentablemente esto implicaría fuertes gastos que no se justifican para la gran mayoría de redes inalámbricas pequeñas. Existe la necesidad de establecer un método que determine cuales son las fallas de seguridad. Este método debe evaluar las condiciones de la red y determinar cual es la implementación más adecuada.

Para crear un método general inicialmente se partió de un estudio. Así se logro una interacción con la tecnología inalámbrica y sus equipos. Esta fue indispensable para poder comprender la necesidad de seguridad inalámbrica.

El caso de estudio fue realizado en el laboratorio DELTA en el Instituto de Ciencias Humanísticas y Económicas de la ESPOL. En este se procedió a revisar las características de seguridad de su ubicación física y las configuraciones de sus puntos de acceso. Se determinó que cambios de seguridad se debieron realizar para aumentar el nivel de seguridad.

El reconocimiento de las características de seguridad se realizó con la ayuda del programa NetStumbler. Este software es una herramienta muy útil para el monitoreo de redes inalámbricas. Presenta información de la red incluyendo la razón señal a ruido de cada punto de acceso en las diferentes ubicaciones físicas. Con el se pudo medir la potencia de la señal fuera del laboratorio DELTA en donde una señal permitiría a intrusos ingresar a la red.

Inicialmente el laboratorio del caso de estudio no tenía ningún tipo de seguridad implementada. Como conclusión de los datos recolectados se pudo comprobar que existían tres partes importantes para definir el nivel de la seguridad necesaria:

1. Los riesgos que implica la ubicación física de la red.
2. El tipo de intrusos que pretendieran entrar a la red.
3. La clase de información que circula en la red.

Al finalizar nuestro análisis se implementó en el laboratorio un esquema de seguridad que no requería de ningún hardware adicional puesto que aunque la red estaba en una ubicación física abierta, los datos de la red y el tipo de intrusos que proyectaran entrar en la red no presentan un mayor riesgo.

El proyecto determina los pasos que se deben seguir para realizar una consultoría de red en cualquier WLAN. Estos pasos proyectan sistematizar y crear un método de consultoría que puede aplicarse para cualquier caso. Al final se determina cual es el nivel de seguridad requerido por la red y se procede a detallar los métodos de implementación para nivel básico, intermedio y avanzado de seguridad.

Lo primordial era determinar que información era necesaria para decidir cual implementación sugerir. Surgió la idea de una empresa consultora que se encargue de realizar una serie de estudios en la red inalámbrica y mediante un análisis pueda proponer, y si se da el caso implementar, un sistema de seguridad. Un consultor externo tiene el nivel de conocimiento necesario para implementar la solución más adecuada además de que provee un punto de vista externo e imparcial sobre todos los aspectos que conciernen la seguridad de la red inalámbrica.

Al momento de tomar una decisión sobre una implementación de seguridad de cualquier tipo el primer paso es realizar una evaluación de los riegos y vulnerabilidades de seguridad para comparar el costo de una posible brecha versus el costo de la implementación de posibles soluciones.

Se decidió realizar un proceso metódico en el cual se identifica, analiza y cuantifica los riesgos de seguridad en una red inalámbrica. Consta de tres etapas: evaluación de las condiciones actuales de la red, estudio de las vulnerabilidades de la red y estudio de los riesgos de la red. Para facilitar este procedimiento se crearon tres formularios (Figuras 1, 2 y 3) que se llenan en cada etapa del estudio.

Esta primera parte de la evaluación de seguridad requiere de la colaboración del administrador de la red inalámbrica. Se requiere las características de todos los router inalámbrico, punto de acceso y tarjeta de red inalámbrica que sea utilizada en la red. Es importante realizar una investigación de las especificaciones técnicas de los equipos y anexar esta información al formulario.

El objetivo del estudio de vulnerabilidades es examinar el sistema para encontrar debilidades que pueden ser explotadas y determinar las probabilidades de que alguien se aproveche de estas vulnerabilidades. Se determina en que puntos o locaciones la red de la empresa está abierta para intrusos. Este procedimiento requiere de la ayuda del programa NetStumbler.

Se debe incluir un plano del edificio en donde se encuentra la red y sus alrededores. En este gráfico es muy importante ubicar los puntos de acceso y hacer un estimado de su alcance.

Para medir de una manera adecuada el impacto de un riesgo se debe determinar los valores que se está tratando de proteger. Los bienes deben ser reconocidos y valorados. En el caso del estudio en una red WLAN, los valores que se desea proteger son los datos que se envían. A cada "dato" se le debe asignar un valor. El departamento gerencial debe estar involucrado en esta etapa del proceso. Esta etapa es muy importante para asegurarse que el alcance de las medidas de seguridad implementadas son las adecuadas para los riesgos asociados con la sensitividad de los datos en la WLAN.

Al finalizar todas las etapas del estudio el consultor poseerá toda la información necesaria para sacar conclusiones sobre el estado de seguridad de la red inalámbrica de la empresa. En este punto el trabajo del consultor consiste en determinar que tipo de seguridad requiere de acuerdo a la exigencia de la red, se deberá determinar si la WLAN requiere de una implementación de seguridad mínima, implementación de seguridad media o una implementación de seguridad avanzada. Esto se debe presentar a la compañía contratante mediante un informe que detalle los resultados de las etapas y especifique cual es el nivel de riesgo de la red.

En la figura 4 se tiene un diagrama de flujo que permite entender mejor el proceso de seleccionar la implementación adecuada. Los datos recolectados en el estudio nos presentarán la respuesta de las preguntas planteadas.

La seguridad mínima generalmente no se necesita ningún equipo adicional al de la red inalámbrica previamente establecida. Solo se requerirá de actualizaciones en algunos casos o quizá pequeños reajustes de hardware. Se aumenta la seguridad mediante creación de tablas MAC y métodos para controlar la señal.

Utiliza equipos adicionales, el principal es un servidor RADIUS que permita la implementación del PEAP para el funcionamiento del 802.1X. Se decidió utilizar una solución con Windows Server 2003 con componentes IAS. La ventaja de este servidor es que como producto Windows es utilizado ampliamente y conocido por la mayoría de administradores de red.

ESTADO ACTUAL DE LA RED

Equipos Inalámbricos Utilizados

Equipo	Marca	Tipo	Cantidad

Características

SSID	
Número de estaciones de trabajo	
Número de puntos de acceso	
Canal en el que trabaja	
Utiliza DHCP	

Seguridad

	Si	No
WEP		
SSID broadcast		
Clave de AP de fabrica		
Tablas MAC		

Otro tipo de seguridad ______________________________

Empresa	
Administrador de Red	
Consultor	
Fecha	

Figura 1. Formulario de Estudio de Condición Actual de la Red

EXTERIORES

PLANO

Puntos de Acceso intrusos detectados por NetStumbler

SSID	Canal	SNR

Observaciones:

Figura 2. Formulario de Estudio de Vulnerabilidades

TIPO DE DATOS

INTRANET

1 Información de Negocios
Valor estimado de pérdida

2 Información Corporativa
Valor estimado de pérdida

3 Información técnica y de desarrollo
Valor estimado de pérdida

4 Información de mercadeo
Valor estimado de pérdida

5 Información operacional y secretos de oficio
Valor estimado de pérdida

6 Información de recursos humanos
Valor estimado de pérdida

7 Información financiera
Valor estimado de pérdida

8 Código fuente
Valor estimado de pérdida

9 Información confidencial del cliente
Valor estimado de pérdida

10 Acceso a través de la red a otras empresas
Valor estimado de pérdida

Figura 3. Formulario de Estudio de Riesgos

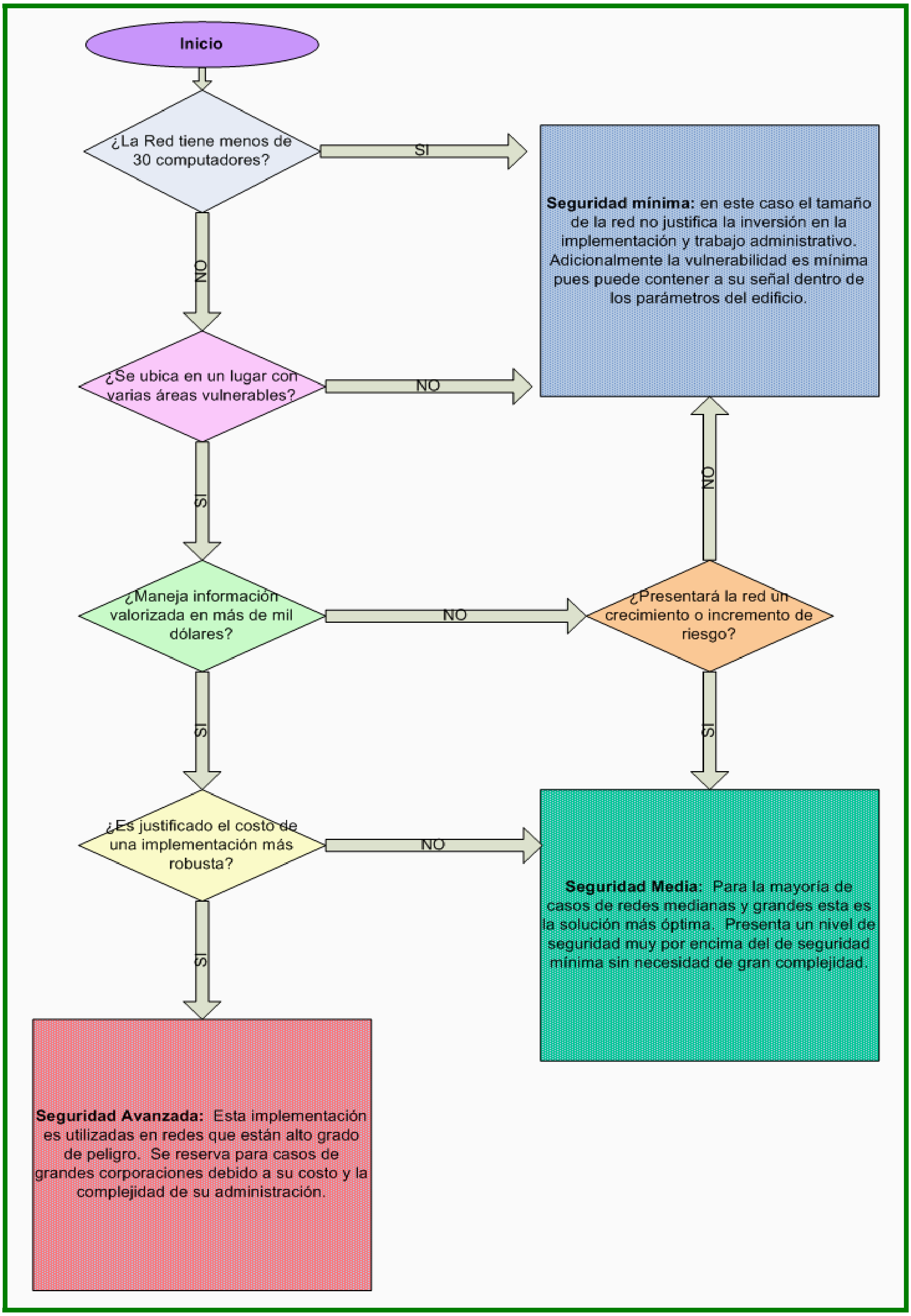

Figura 4. Diagrama de flujo para selección de la implementación de seguridad

La implementación de seguridad media de una WLAN proporciona un método más consistente de autenticación y autorización con el protocolo 802.1X.

El último nivel de seguridad se recomienda para empresas grandes con datos altamente sensibles. Se basa en tecnologías de VPN probadas y de confianza para proteger la confidencialidad de los datos enviados a través de Internet. Aunque la solución de seguridad intermedia puede ser suficiente para la mayoría de escenarios, se ha decidido poner a disposición esta implementación como una medida más definitiva que separa de manera más concisa la red inalámbrica de la red cableada.

Aunque las gateways VPN convencionales se pueden adaptar para ser usadas en la red WLAN para la solución utilizamos una gateway WLAN que provee funciones adicionales que permiten una mejor administración y monitoreo de la red inalámbrica.

CONCLUSIONES

Las facilidades de movilidad y escalabilidad que ofrece la tecnología inalámbrica la convierten en una opción insuperable para la implementación de redes LAN. Al evaluar sus virtudes no hay duda de que las redes inalámbricas son la mejor opción. Debido a que permiten la movilidad aumentan la productividad de los trabajadores significativamente. Convierten a una computadora portátil en una oficina móvil. Los costos de su implementación son menores a los de cableado y la extensión de la red con nuevos equipos anualmente tiene un costo mínimo.

La consultoría logra determinar cual es el nivel de inseguridad de la red. Permite que un consultor externo, imparcial, evalúe la red en los tres puntos que, basados en la experiencia del caso de estudio, consideramos los más relevantes.

El caso de estudio nos demostró que muchas veces una implementación muy compleja de seguridad no siempre es viable o necesaria. Como resultado de la consultoría se determina la magnitud de la necesidad de seguridad y se recomienda el tipo de implementación para cada caso. El gerente tiene la última palabra sobre la viabilidad de la implementación.

Al finalizar este proyecto pudimos determinar cuan importante es la seguridad en una red inalámbrica. Hace mucho tiempo dejó de ser opcional para convertirse en necesaria. La formación de una empresa de este tipo puede resultar un proyecto rentable pues la tecnología WLAN es un mercado en crecimiento. Aun con los costos adicionales para seguridad las redes inalámbricas siguen siendo una opción excelente para una empresa grande o en constante expansión.

REFERENCIA

a) Proyecto de Tópico

b) J. Rittinghouse y J. Ransome, Wireless Operational Security (Digital Press, 2004), Capítulos 8, 9 y 12.
c) C. Peikari y S. Fogie, Maximum Wireless Security (Sams, Diciembre 18, 2002), Capítulo 9 y 12.
d) George Ou, enero 2005, Wireless LAN Security Guide http://www.lanarchitect.net/Articles/Wireless/SecurityRating/