ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

Metodología de Seguridad en Redes T.A.M.A.R.A: Testeo, Análisis, Manejo de Redes y Acceso

María Fernanda Viteri M. [(1)], Pedro Orellana Zuñiga [(2)], Ignacio Marin-Garcia [(3)]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
viviteri@espol.edu.ec [(1)], porellana@espol.edu.ec [(2)], imaringa@fiec.espol.edu.ec [(3)]

Resumen

Debido a la necesidad de seguridad en los sistemas de información en las empresas ecuatorianas, hemos desarrollado una metodología, cuyo objetivo es asegurar aquellos recursos que estén vulnerables para un posible ataque por parte de personas internas o externas a la entidad, esto se logra poniendo en conocimiento de todas las personas que hacen uso de programas, sistemas o aplicaciones de propiedad de las empresas que la adopten, las consideraciones mínimas de seguridad para garantizar la integridad y buen recaudo de la información guardada, procesada, transmitida y propagada por estas aplicaciones.

Primero debemos observar que tipo de sistema queremos proteger: Sistema particular, pequeño, mediano o grande. Dependiendo del sistema, se aplicarán las políticas, en las cuales hemos tratado en lo posible de no usar términos técnicos ni complicados, esto es porque deseamos que sea legible para el usuario común.

Nos proveerá de recursos para mantenernos informados sobre lo que pasa en nuestra PC, nos permite conocer nuestro sistema operativo y así hacer uso de utilidades de seguridad. Nos permitirá saber qué hacer en caso de un ataque, ya sea en nuestra PC o en la de nuestra empresa. Es importante saber que hacer, ya que hay personas que piensan que nunca van a ser víctimas de fraude o ataques, pero están equivocadas, hay que recordar que en cuestiones de seguridad en redes todos podemos ser vulnerables.

Palabras Claves: *Integridad, vulnerabilidad, sistema, ataque.*

Abstract

Due to the need for security in information systems in the Ecuadorian companies, we have developed a methodology, which aims to ensure those resources that are vulnerable to a possible attack by insiders or outside the entity, this is achieved by placing in knowledge of all the people who make use of programs, systems or applications owned by the companies that adopt the minimum safety considerations to ensure the integrity and safekeeping of information stored, processed, transmitted and propagated by these applications.

First we see what kind of system we want to protect: System particular, small, medium or large. Depending on the system, the relevant policies, which we tried as much as possible not to use technical terms or complicated, this is because we want to make it readable for the average user.

We provide resources to keep us informed about what's happening in our PC, we can meet our operating system and thus make use of security utilities. We will know what to do in case of an attack, either on our PC or our company. It is important to know what to do, as there are people who think they will never be victims of fraud or attacks, but they are wrong, remember that network security issues can all be vulnerable.

Keywords: *integrity, vulnerability, system, attack.*

1. Introducción

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada una de las ramas que la componen.

Esta metodología está enfocada a cumplir con los cuatro puntos que caracterizan a un sistema "seguro", las cuales son: Integridad, Confiabilidad, Disponibilidad y no repudiación. Con nuestra propuesta, esperamos dar soluciones a empresas de pequeña, mediana y gran escala, con el fin de aumentar la seguridad en este tipo de organizaciones, así como también para asegurar aquellos recursos que estén dispuestos para un posible ataque por parte de personas internas o externas a la entidad.

2. Metodología de Seguridad "T.A.M.A.R.A"

Hemos creado esta metodología de Seguridad Informática denominada **"T.A.M.A.R.A: Testeo, Análisis y MAnejo de Redes y Accesos"** seleccionado por su origen **hebreo** y que significa **"Da protección, brinda seguridad"**, la cual se fundamenta en los principios básicos de seguridad: confidencialidad, disponibilidad, integridad, y no repudiación, en ésta tratamos la implantación de controles o mecanismos de seguridad, basados en las políticas generales de la empresa, particularmente en las políticas y procedimientos de seguridad, con lo que se busca minimizar las vulnerabilidades expuestas y aumentar la seguridad de la información.

2.1 Explicación de la Metodología

Primero observaremos que tipo de sistema queremos proteger: Sistema particular, pequeño, mediano o grande, Si el sistema es **particular** (Laptop o desktop que usamos en nuestra casa o en nuestra oficina y que no es de uso comercial ni público), lo que debemos verificar es si está o no conectada a internet, **si no hay una conexión a internet**, se deja a criterio personal las medidas de seguridad, pero se recomienda tener actualizada la base de firma de virus del antivirus que nos guste emplear o del que creamos es el mejor, las actualizaciones de la PC ayudan, como así también tener activado el firewall de Windows (si se usa este sistema operativo), a mas de los criterios de seguridad que tengan los usuarios de cada equipo. Pero por el contrario, **si hay una conexión a internet**, se citarán unas series de medidas que se consideran indispensables si hay una conexión a internet, las hemos denominado básicas y avanzadas. Las básicas son de implantación obligatoria y las avanzadas serán de implantación deseada. En el caso de ser un sistema **pequeño** (Llámese así al cibercafé de o a una pequeña red LAN) debemos tomar en cuenta las leyes y normas ecuatorianas para este nivel, ya que a medida que los sistemas se hacen más grandes necesitamos de éstas para no irrespetar las leyes y a la vez defendernos en caso de alguna irregularidad. Si el sistema es **mediano o grande** (Empresa con más de 20 estaciones de trabajo), con el fin incrementar la seguridad se hace necesario realizar un análisis de riesgos, para identificar aquellas brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la organización, así como facilitar la toma de decisiones sobre las formas de proteger sus bienes y los servicios que prestan a la comunidad.

Teniendo en cuenta los diferentes aspectos anteriormente mencionados, solo las empresas con suficiente capital podrían implementar una solución de seguridad que contemple todos los temas necesarios; por tal motivo se ha hecho necesaria la elaboración de ésta metodología de seguridad apropiada para las empresas que no poseen estos recursos, la metodología creada busca satisfacer esta necesidad, con el fin de brindar y mejorar los ambientes de seguridad a un bajo costo, dándole, de esta manera, un enfoque social.

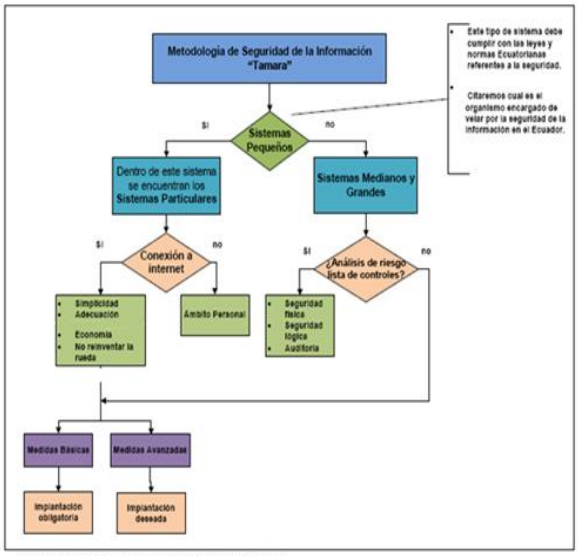

FIGURA 1 METODOLOGIA DE SEGURIDAD TAMARA

3. "T.A.M.A.R.A" en sistemas Medianos y Grandes

Como se mencionó en el primer capítulo, en los

sistemas medianos o grandes (La empresa donde trabajamos o cualquier otra), con el fin incrementar la seguridad se hace necesario realizar un análisis de riesgos, para identificar aquellas brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la organización, así como facilitar la toma de decisiones sobre las formas de proteger sus bienes y los servicios que prestan a la comunidad.

3.1 Análisis de riesgos

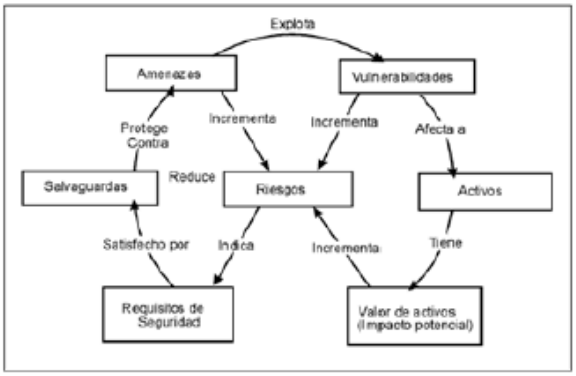

FIGURA 3.1 ANALISIS DE RIESGOS

Al crear una política de seguridad de la información, es importante entender que la razón para crear tal política es decir se debe entender cuáles recursos de la red vale la pena proteger y también entender que algunos recursos son más importantes que otros. Es decir se deberá identificar la fuente de amenaza de la que se protege a los recursos. El análisis de riesgos implica determinar lo siguiente: ¿Qué se necesita proteger?, ¿De quién protegerlo? Y ¿Cómo protegerlo? , los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida.

No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso. Hay que tener muy en cuenta que, al realizar el análisis de riesgo, se deben identificar todos los recursos (por más triviales que parezcan) cuya seguridad está en riesgo de ser quebrantada, ahora bien, ¿cuáles son los recursos? Los recursos que deben ser considerados al estimar las amenazas a la seguridad son:

Hardware: Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, Computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.

Software: Programas fuente, programas objeto, programas de diagnóstico, sistemas operativos.

Datos: Durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos.

Gente: Usuarios, personas para operar los sistemas.

Documentación: Sobre programas, hardware, sistemas, procedimientos administrativos locales.

3.2 Implementación del sistema de seguridad que minimiza los riesgos

Es conveniente citar en esta sección el área física y también la parte lógica (software, sistemas operativos etc.) para poder establecer las políticas y procedimientos de seguridad.

3.2.1 Área Física

La seguridad física es una de las vías fundamentales para minimizar los riesgos al interior del cuarto de servidores o de la empresa, podemos citar:

El Centro de Computo y/o la sala de maquinas de todas las agencias debe contar con sistemas de aire acondicionado, un detector de humos y un extintor.

También se tiene prohibido conectar a la red eléctrica de cómputo, cualquier dispositivo ajeno, por ejemplo (Electrodomésticos, Cargadores de baterías, etc.).

3.2.2 Seguridad Lógica

Dentro de las herramientas que se utilizan a diario en una organización se encuentra el sistema operativo, el cual controla el acceso y uso de los recursos de una maquina, siendo uno de los elementos más apetecibles para intentar explotar cualquier vulnerabilidad, por lo tanto, en un sistema operativo se debe contemplar: Identificación y autentificación de los usuarios, Control de acceso a los recursos del sistema, Monitorear las acciones realizadas por los usuarios, Auditoria de los eventos de posible riesgo, Garantía de integridad de los datos almacenados, Garantía de la disponibilidad de los recursos.

Una vez implementada la metodología y aseguradas todas las áreas que se tuvieran en cuenta en el plan de seguridad, se procede con la auditoria de sistemas, con el fin de verificar el éxito de la implementación y el buen desempeño de los sistemas de información, ya

que se determina si estos salvaguardan los activos, mantienen la integridad de los datos y utilizan eficientemente los recursos.

3.3 Impacto en la Organización

La implementación de políticas de seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. ¿Cómo pueden impactar si se implementan para hacer más seguro el sistema? En realidad, la implementación de un sistema de seguridad conlleva a incrementar la complejidad en las operaciones de la organización, tanto técnica como administrativa.

Por ejemplo, en el punto de seguridad administrativa (Área Física) se toman algunas medidas como deshabilitar los puertos USB, no se permitirá ingresar CDs etc. Esto va llevar que los usuarios tomen ciertas medidas de rechazo, ya que no podrán instalar ni almacenar nada si no es con la autorización del personal responsable, pero deben entender que estas son medidas de la empresa, para así poder lograr tener nuestra información segura sin que se produzcan infiltraciones.

3.3.1. Visibilidad del Proceso

La visibilidad es permitir el aporte de las personas de la organización y, dar a conocer las acciones tomadas. Es decir que, cuando se deben producir cambios en las políticas no es necesario que se decidan unilateralmente.

Es altamente deseable que se formen grupos de trabajo para discutir y/o conocer el alcance y el tipo de medidas a llevar a cabo. Luego, una vez tomada la decisión, se debe comunicar a los involucrados de los cambios realizados por medio de notas o boletines informativos

3.3.2 Implementación

La implementación de medidas de seguridad, es un proceso técnico-administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

También, como hemos mencionado anteriormente, es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Conclusiones y recomendaciones

1. Con esta metodología podemos brindar a más de seguridad, control y administración de los accesos a las empresas y a sus respectivas áreas tecnológicas.

2. Crear manuales de configuración y administración para todos los dispositivos que forman parte de la infraestructura de las redes: conmutadores, Puntos de Acceso, servidores de autenticación, servidores de Directorio Activo, administrador y monitor de la red inalámbrica WCS. Esto sirve para que las personas que los administren a futuro, tengan a mano las configuraciones y como dar seguridad a estos equipos y así nos podemos evitar algunos errores.

3. Informar a los usuarios de los servicios y beneficios que nos proveen las redes, así como de su funcionamiento; además solicitar que se enmarquen en las políticas de seguridad establecidas. También se debe dar capacitación técnica al administrador de la red alámbrica o inalámbrica, dentro y fuera de la empresa, para que éste pueda dar un mejor mantenimiento a las redes y un mejor soporte a los usuarios.

BIBLIOGRAFÍA:

[1] Garzón Daniel, Vergara Alejandro, Metodología de análisis y vulnerabilidades para empresas de mediana escala, Universidad Javeriana, Bogotá-Colombia 2006.

[2] Areitio J, Seguridad de la información: Redes informáticas y sistemas de la información, Paraninfo 2008, Madrid-España, Diciembre 2010

[3] Millán Ramón, Consultoría estratégica en tecnologías de la información, http://www.ramonmillan.com/tutoriales/cortafuegos_parte1.php>, Diciembre 2010.

[4] Cmac-Paita, Código de Buenas prácticas para la gestión de seguridad de la información, Piura-Perú 2009.