ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
Facultad de Ingeniera en Electricidad y Computación

Tema:

Auditoria de Redes Locales para empresas medianas y pequeñas.

Integrantes:

William Luis Cargua Freire [1]
Patricia Isabel Peñafiel Barrera[2]
Andrés Gilberto Wong Blacio[3]
Ing. Albert Espinal Santana[4]

[1]Licenciado en Sistemas de Información 2005; email: william.cargua@sasf.net

[2]Licenciado en Sistemas de Información 2005; email: patty_penafiel@yahoo.es

[3]Licenciado en Sistemas de Información 2005; email: andreswongb@homail.com

[4]Director de Tópico, Título de Pregrado: Ingeniero en Computación, ESPOL, Diciembre 1996. Título de Postgrado: Magister en Sistemas de Información Gerencial, ESPOL, Enero 2000. Profesor de la ESPOL desde: Octubre 1996

RESUMEN

La popularidad de Internet y la explosión de usuarios en todo el mundo, ha producido una creciente amenaza de ataques hacia los sistemas y la información de las organizaciones públicas y privadas, esto crea la necesidad de implementar en cualquier organización un esquema de seguridad informática. Por otra parte, el acceso remoto y la conexión a Internet permiten mejorar la comunicación a un nivel sin precedente, además de proveer una extensa fuente de información, adicionalmente abre las puertas a un gran universo de comunicación con los clientes y proveedores. No obstante, estas mismas oportunidades exponen a las redes locales a sufrir ataques, así como al uso inadecuado por parte de sus propios empleados.

La seguridad informática es muy importante y debido a esto se ha realizado un análisis de las vulnerabilidades de la red local de una empresa en Guayaquil, el mismo que se puede tomar como modelo a aplicar en empresas medianas o pequeñas. Basándose en el análisis realizado, se hicieron las sugerencias para los problemas encontrados y se definió un modelo de políticas de seguridad para su posible aplicación.

INTRODUCCIÓN

Las redes locales (LAN) tienen un papel importante en el funcionamiento de las empresas hoy en día. En vista de que muchas organizaciones carecen de estudios sobre las seguridades informáticas, se realizó el siguiente estudio cuyo fin es ayudar a las empresas a identificar su situación actual con respecto a las seguridades informáticas y sugerir los correctivos necesarios. Este estudio se compone de los siguientes puntos:

- Análisis del Estado actual de la red, incluyendo controles físicos y lógicos, detección de usuarios no autorizados, hardware de comunicaciones, tipos de tráfico de red, esquema de antivirus, acceso a Internet, esquema y pruebas de respaldo.

- Elaboración de un plan de respaldo y contingencia que garantice la disponibilidad de los recursos tanto en la parte de servidores y equipos de comunicación, enlaces de transmisión, aplicaciones y datos en general.

- Análisis de Políticas de seguridad actuales, que incluye verificación de políticas de claves, control de personal, perfiles de usuario, sistemas operativos de red, esquema de licencias de software.

- Análisis de protección de recursos informáticos y establecimiento de un plan de capacitación en las políticas de seguridad.

CONTENIDO

1. Situación actual.

El primer paso para realizar una auditoria de redes locales es identificar cual es la situación actual de la organización con respecto a las seguridades informáticas, realizando lo siguiente:

- **Inventario de hardware:** Consiste en realizar un diagrama de los componentes físicos de la red.
- **Inventario de software existente:** Elaboración de un listado de los programas instalados en cada máquina de la red.
- **Esquema de antivirus:** Se especifica el software antivirus utilizado en la empresa.
- **Esquema de respaldos:** Identificar la frecuencia y el medio con el que se realizan los respaldos de la información de la empresa, en caso de que se realicen.
- **Análisis de riesgos:** Realizar un análisis de los riesgos posibles a los que se encuentra expuesta la empresa, basándose en los puntos anteriormente mencionados en el estudio de la situación actual.

2. Solución propuesta y plan de contingencias

Como resultado del análisis hecho de la situación actual, se deben proponer las respectivas recomendaciones para cada una de los problemas encontrados, así como establecer un plan de contingencias que permita garantizar el funcionamiento de la red local en caso de suscitarse algún imprevisto. A continuación, se presenta un esquema genérico de las recomendaciones y plan de contingencias a implementar:

2.1 Recomendaciones contra la acción de virus

Es aconsejable tener un proveedor de software antivirus para las estaciones y otro diferente para el servidor, para reducir la probabilidad de que un virus que no este en la lista de actualización, se filtre en toda la red. También es necesario implementar un procedimiento para las actualizaciones automáticas de las definiciones de virus, labor que se debe realizar en horas en que no se degrade el performance del tráfico de red.

2.2 Recomendaciones contra accesos no autorizados

Es recomendable que los equipos más importantes de la empresa residan en un área accesible solo a personal autorizado, sean estos tanto servidores como equipos de comunicación. Es necesario controlar el acceso alas instalaciones como el acceso a las maquinas con sus debidos perfiles.

Se deben establecer políticas para el flujo de datos en la red, además de incluir sistemas de monitoreo de los accesos realizados a la red.

2.3 Recomendaciones para prevenir fallas en los equipos

Se recomienda realizar mantenimiento preventivo de los equipos, también contar con un sistema de alimentación emergente de electricidad y llevar un control del software instalado en las máquinas, teniendo un equipo de pruebas para las nuevas instalaciones de programas.

2.4 Recomendaciones de como realizar las actualizaciones de parches de seguridad

Como complemento a las sugerencias anteriores, es recomendable estar al día con la instalación de los diferentes parches de seguridad para el software de la empresa.

2.6 Plan de contingencias

El Plan de Contingencias o Emergencias, constituye el instrumento principal para dar una respuesta oportuna, adecuada y coordinada a una situación de emergencia causada por fenómenos destructivos de origen natural o humano. Como parte del plan de contingencias, tenemos:

2.6.1 Actividades previas al desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, las cuales nos asegurarán un proceso de recuperación con el menor costo posible

2.6.2 Actividades durante el desastre

Son todas las actividades a realizar en el momento que ocurre un siniestro, estas actividades deben estar previamente establecidas en el plan de emergencias de la empresa, donde se detallan entre otras cosas vías de salida o escape, plan de evacuación del personal, plan de puesta a buen recaudo de los activos, ubicación y señalización de los elementos contra el siniestro (extintores, etc.), lista de teléfonos de Bomberos / Ambulancia.

2.6.3 Actividades después el desastre

Después de ocurrido el siniestro o desastre es necesario realizar las actividades que se detallan en el Plan de contingencias establecido. Previo a su ejecución se deben tomar en cuenta los puntos que se detallan a continuación.

- Evaluación de daños.
- Priorización de actividades del plan de acción
- Ejecución de actividades
- Evaluación de resultados
- Retroalimentación del plan de acción

3. Políticas de seguridad

Desarrollar un sistema de seguridad significa "planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa". Los objetivos que se desean alcanzar luego de implantar un plan de políticas de seguridad son los siguientes:

- Establecer un esquema de seguridad con claridad y transparencia bajo la responsabilidad de la empresa en la administración del riesgo.
- Compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.
- Que la prestación del servicio de seguridad gane en calidad.
- Todos los empleados se convierten en interventores del sistema de seguridad.

CONCLUSIONES

Un estudio muestra que si un desastre causa que las compañías pierdan sus centros de datos por 10 o más días, 50 por ciento de esas compañías se declararán en bancarrota casi inmediatamente después de la perdida. Otro 43 por ciento lo hará dentro de un año de la perdida.

Esto demuestra la importancia de realizar un análisis de las vulnerabilidades de la redes locales, ya que si no se cuenta con medidas preventivas contra desastres, se corre el riesgo de comprometer seriamente la vida operacional de las empresas.

Por esta razón, concluimos que el esquema de auditoria mostrado en este artículo puede servir de base para las pequeñas y medianas empresas pongan en marcha un plan de seguridad, ya que ningún esfuerzo, sea este económico o humano, es demasiado cuando está en juego información confidencial y vital para el normal funcionamiento del negocio.

Fuente: www.phoneplusmag.com.

REFERENCIAS

a) Libros de consulta

1 MARTÍN ÁLVAREZ. L., Redes Informáticas: La base de las superautopistas de datos. Tower Communications SRL, 1994.

2 COBB, S., Manual de Seguridad para PC y Redes Locales. McGraw-Hill, 1995.

3 COX, N., Manley, C. T., Chea, F. E., Guía de Redes Multimedia. McGraw-Hill, 1996.

4 HUNTER, P., Local Area Networks: Making the Right Choices. Addison-Wesley, 1997.

5 PALMER-STEVENS, D., Guía de Redes de Área Local. Cabletron Systems Limited, 1998.

6 SIMIANI, M., Intranets, Empresa y Gestión Documental. McGraw-Hill, 2001.

7 MAXIMUM SECURITY: A Hacker's Guide to Protecting Your Internet Site and Network, Macmillan Computer Publishing. Mark Taber, 1998.

Ing. Albert Espinal Santana,

Director de Tesis

SUMMARY

Internet’s popularity and the growth of users all around the world has produced a growing menace of attacks to systems and public and private organizations’ information, this creates the necessity to implement in any organization an information security scheme. On the other half, remote access and Internet connection allow to increase communications to a never accessed level, besides giving a huge information source, also opening the doors to a great universe of communication between clients and vendors. However, these opportunities expose local nets to suffer attacks and wrong use by inner employees.

Information security is very important and because of this, an study has been done about local net vulnerabilities on an enterprise located in Guayaquil. This study can be taken as a model to apply on small-middle organizations. Over the analisis done, suggestions were made for the problems found and a security politics model was defined for its future posible application.