2011

Redes de Comunicación

Ing. Luis Müller

[UNIDAD IX – AUDITORIA EN SEGURIDAD]

Esta es una recopilación de la teoría referente a la asignatura Redes de Comunicación, a ser estudiada en clases con los alumnos, y que servirá como base para su aplicación también en clases en ejercicios prácticos.

Contenido

Auditoria aplicada a la seguridad en redes de computadores

El concepto de auditoría

Una **auditoría de seguridad** consiste en apoyarse en un tercero de confianza (generalmente una compañía que se especializada en la seguridad informática) para validar las medidas de protección que se llevan a cabo, sobre la base de la política de seguridad.

El objetivo de la auditoría es verificar que cada regla de la política de seguridad se aplique correctamente y que todas las medidas tomadas conformen un todo coherente.

Una auditoría de seguridad garantiza que el conjunto de disposiciones tomadas por la empresa se consideren seguras.

1. Introducción

La organización en la parte de las redes de comunicaciones de computadores es un punto de viraje bastante importante; es por ello, que uno de los modelos de red más conocidos, es el modelo OSI.

A grandes rasgos, el modelo OSI, dado por capas, está dividido en:

Capa física:

Se encarga de garantizar la integridad de la información transmitida por la red; por ejemplo, si se envía un 0, que llegue un 0.

Capa de enlace:

Garantiza que la línea o canal de transmisión, esté libre de errores.

Capa de red:

Determina como se encaminan los paquetes, de la fuente al destino. Igualmente, debe velar por el tráfico de la red, evitando al máximo las congestiones. Para ello, debe llevar un registro contable de los paquetes que transitan.

Capa de transporte:

Divide los datos en unidades más pequeñas y garantiza que tal información transmitida, llegue correctamente a su destino.

De igual forma, crea una conexión de red distinta para cada conexión de transporte requerida, regulando así el flujo de información.

Analiza también, el tipo de servicio que proporcionará la capa de sesión y finalmente a los usuarios de red.

Capa de sesión:

Maneja el sentido de transmisión de los datos y la sincronización de operaciones; es decir, si uno transmite, el otro se prepare para recibir y viceversa o Situaciones Commit, donde tras algún problema, se sigue tras último punto de verificación.

Capa de presentación:

Se encarga de analizar si el mensaje es semántica y sintácticamente correcto.

Capa de aplicación:

Implementación de protocolos y transferencia de archivos.

Lo anterior, nos permite describir 3 tipos de fallos en la seguridad de la red:

1. Alteración de bits: Se corrige por código de redundancia cíclico.
2. Ausencia de tramas: Las tramas se desaparecen por el ambiente o una sobrecarga del sistema; para ello, se debe tener un número de secuencia de tramas.
3. Alteración de la secuencia en la cual el receptor reconstruye mensaje.

Otro de los tipos de modelos de referencia más conocidos, es el TCP/IP, hoy día, con algunas variaciones, como el de encapsular varios protocolos, como el NetBIOS; el TCP/IP da replicación de los canales para posibles caídas del sistema.

Bajo ésta política, entonces se ha definido como clases de redes:

- Intranet = Red interna de la empresa.
- Extranet = Red externa pero directamente relacionada a la empresa.
- Internet = La red de redes.

El problema de tales implementaciones, es que por los puertos de estandarización pública de TCP/IP, se puede entrar cualquier tercero para afectar la red de la compañía o su flujo de información Tal cuestión, es recurrente sobretodo en el acceso de la red interna de la compañía a la Internet, para lo cual, y como medida de protección, se usan Firewall (cortafuegos) que analizan todo tipo de información que entra por Internet a la compañía, activando una alarma, en caso de haber algún intruso o peligro por esa vía a la red.

La compañía puede definir 2 tipos extremos de políticas de seguridad:

- Políticas paranoicas: Toda acción o proceso está prohibido en la red.
- Políticas promiscuas: No existe la más mínima protección o control a las acciones de los usuarios en la red.

No importa lo que haga la empresa, siempre va a haber un punto de fallo, para adelantarse a intrusos, entonces se han ideado algunas herramientas para probar la eficacia de las políticas de seguridad en red de la empresa, algunas de tales herramientas, son: SAFEsuite y COPS. Estas empiezan probando la fiabilidad de las contraseñas de usuario usando algunas técnicas de indagación como es el leer el tráfico de la red buscando en tal información sobre nombres de usuarios y contraseñas respectivas, probar la buena fe de los usuarios mandándoles mensajes de la administración solicitando su contraseña a una especificada por la herramienta o probando contraseñas comunes o por defecto en muchos sistemas.

2. Auditoria de comunicaciones:

Ha de verse:

- La gestión de red = los equipos y su conectividad.
- La monitorización de las comunicaciones.
- La revisión de costes y la asignación formal de proveedores.
- Creación y aplicabilidad de estándares.

Cumpliendo como objetivos de control:

- Tener una gerencia de comunicaciones con plena autoridad de voto y acción.
- Llevar un registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- Mantener una vigilancia constante sobre cualquier acción en la red.
- Registrar un coste de comunicaciones y reparto a encargados.
- Mejorar el rendimiento y la resolución de problemas presentados en la red.

Para lo cual se debe comprobar:

- El nivel de acceso a diferentes funciones dentro de la red.
- Coordinación de la organización de comunicación de datos y voz.
- Han de existir normas de comunicación en:
  - Tipos de equipamiento como adaptadores LAN.
  - Autorización de nuevo equipamiento, tanto dentro, como fuera de las horas laborales.
  - Uso de conexión digital con el exterior como Internet.

- Instalación de equipos de escucha como Sniffers (exploradores físicos) o Traceadores (exploradores lógicos).

- La responsabilidad en los contratos de proveedores.
- La creación de estrategias de comunicación a largo plazo.
- Los planes de comunicación a alta velocidad como fibra óptica y ATM (técnica de conmutación de paquetes usada en redes MAN e ISDN).
- Planificación de cableado.
- Planificación de la recuperación de las comunicaciones en caso de desastre.
- Ha de tenerse documentación sobre el diagramado de la red.
- Se deben hacer pruebas sobre los nuevos equipos.
- Se han de establecer las tasas de rendimiento en tiempo de respuesta de las terminales y la tasa de errores.
- Vigilancia sobre toda actividad on-line.
- La facturación de los transportistas y vendedores ha de revisarse regularmente.

3. Auditoria De La Red Física

Se debe garantizar que exista:

- Áreas de equipo de comunicación con control de acceso.
- Protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.
- Control de utilización de equipos de prueba de comunicaciones para monitorizar la red y el tráfico en ella.
- Prioridad de recuperación del sistema.
- Control de las líneas telefónicas.

Comprobando que:

- El equipo de comunicaciones ha de estar en un lugar cerrado y con acceso limitado.
- La seguridad física del equipo de comunicaciones sea adecuada.
- Se tomen medidas para separar las actividades de los electricistas y de cableado de líneas telefónicas.
- Las líneas de comunicación estén fuera de la vista.
- Se dé un código a cada línea, en vez de una descripción física de la misma.
- Haya procedimientos de protección de los cables y las bocas de conexión para evitar pinchazos a la red.
- Existan revisiones periódicas de la red buscando pinchazos a la misma.
- El equipo de prueba de comunicaciones ha de tener unos propósitos y funciones específicas.

- Existan alternativas de respaldo de las comunicaciones.
- Con respecto a las líneas telefónicas: No debe darse el número como público y tenerlas configuradas con retrollamada, código de conexión o interruptores.

4. Auditoria De La Red Lógica

En ésta, debe evitarse un daño interno, como por ejemplo, inhabilitar un equipo que empieza a enviar mensajes hasta que satura por completo la red.

Para éste tipo de situaciones:

- Se deben dar contraseñas de acceso.
- Controlar los errores.
- Garantizar que en una transmisión, ésta solo sea recibida por el destinatario. Para esto, regularmente se cambia la ruta de acceso de la información a la red.
- Registrar las actividades de los usuarios en la red.
- Encriptar la información pertinente.
- Evitar la importación y exportación de datos.

Que se comprueban si:

El sistema pidió el nombre de usuario y la contraseña para cada sesión:
En cada sesión de usuario, se debe revisar que no acceda a ningún sistema sin autorización, ha de inhabilitarse al usuario que tras un número establecido de veces erra en dar correctamente su propia contraseña, se debe obligar a los usuarios a cambiar su contraseña regularmente, las contraseñas no deben ser mostradas en pantalla tras digitarlas, para cada usuario, se debe dar información sobre su última conexión a fin de evitar suplantaciones.

- Inhabilitar el software o hardware con acceso libre.
- Generar estadísticas de las tasas de errores y transmisión.
- Crear protocolos con detección de errores.
- Los mensajes lógicos de transmisión han de llevar origen, fecha, hora y receptor.
- El software de comunicación, ha de tener procedimientos correctivos y de control ante mensajes duplicados, fuera de orden, perdidos o retrasados.
- Los datos sensibles, solo pueden ser impresos en una impresora especificada y ser vistos desde una terminal debidamente autorizada.

- Se debe hacer un análisis del riesgo de aplicaciones en los procesos.
- Se debe hacer un análisis de la conveniencia de cifrar los canales de transmisión entre diferentes organizaciones.
- Asegurar que los datos que viajan por Internet vayan cifrados.
- Si en la LAN hay equipos con modem entonces se debe revisar el control de seguridad asociado para impedir el acceso de equipos foráneos a la red.
- Deben existir políticas que prohíban la instalación de programas o equipos personales en la red.
- Los accesos a servidores remotos han de estar inhabilitados.
- La propia empresa generará propios ataques para probar solidez de la red y encontrar posibles fallos en cada una de las siguientes facetas:
  - Servidores = Desde dentro del servidor y de la red interna.
  - Servidores web.
  - Intranet = Desde dentro.
  - Firewall = Desde dentro.
  - Accesos del exterior y/o Internet.

5. Criptografía

La criptografía se define como " las técnicas de escrituras tales que la información esté oculta de intrusos no autorizados". Esto, no incluye el criptoanálisis que trata de reventar tales técnicas para descubrir el mensaje oculto.

Existen 2 tipos de criptoanálisis:

Diferencial:

Con variaciones de un bit en cada intento, trata de averiguar la clave de descifrado del mensaje oculto.

Lineal:

Se apoya en variaciones XOR entre cada par de bits, hasta que se logre obtener un único bit, parte de la clave.

Relacionado con esto, se ha desarrollado también la esteganografía, que bajo un camuflaje totalmente ajeno al mensaje a transmitir, se envía la información oculta.
Aunque el cifrado de información es una excelente técnica para proteger los datos, no debería convertirse en el desvelo de la compañía, pues existen otros tipos de debilidades más importantes para tratar por la

compañía, ello, además porque ya existen diferentes programas, hasta gratuitos, como algunas versiones de PGP, tales que toda la potencia informática del mundo, podría romperlos.

Algunos tipos de métodos de criptografía, son:

Transposición :

Invierte el orden de los caracteres en el mensaje. Por ejemplo, si se quiere cifrar "El perro de san Roque no tiene rabo " , colocándolo en un arreglo de columnas de tamaño n, con clave de descifrado k = n en secuencia con 5 columnas {3,2,5,1,4}, el mensaje cifrado quedaría = "osonea lr r ir ednu eo ere et p aqonb"

Tal mecanismo, se criptoanaliza con estudios de factibilidad de cierto tipo de tuplas.

DES:

Utiliza una clave de 56 bits para codificar bloques de 64 bits, por su escasa longitud de clave de acceso, es fácil de romper.

IDEA:

Surgió del DES, IDEA genera bloques de ciframiento de 64 bits con una clave de 128 bits, además usa diversas técnicas de confusión, como es el XOR, suma modulo 2^16 y producto (2^16)+1 . El problema de la criptografía de llave privada, es que en una red muy grande, en caso de que se decida cambiar la clave de desciframiento, hay que notificar a cada uno de los participantes en los procesos de transmisión de datos, corriéndose el peligro de que caiga la nueva clave en manos no autorizadas.. Es por ello, que se ha desarrollado la criptografía de llave pública, que consta de 2 tipos de llaves:

- Una que es pública y conocida por todos los miembros autorizados de la red.
- Una segunda, que es privada y solo la conoce su dueño y el paquete cifrado.

De esa forma, si es necesario cambiar las claves, se notifica por un mensaje cifrado a todos los participantes de la transmisión usando la llave pública.

RSA es un tipo común de transmisión encriptada por llave privada, opera por factorizaciones de los mensajes clave o registro por números primos de orden.

Consideraciones para Elaborar un Sistema de Seguridad Integral.

Como hablamos de realizar la evaluación de la seguridad es importante también conocer cómo desarrollar y ejecutar el implantar un sistema de seguridad.

Desarrollar un sistema de seguridad significa: "planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa."

Por lo cual podemos ver las consideraciones de un sistema de integral de seguridad.

Sistema Integral de Seguridad

Un sistema integral debe contemplar:

- Definir elementos administrativos
- Definir políticas de seguridad
- A nivel departamental
- A nivel institucional
- Organizar y dividir las responsabilidades
- Definir prácticas de seguridad para el personal:
  - Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extinguidores.

- Números telefónicos de emergencia

- Definir el tipo de pólizas de seguros
- Definir elementos técnicos de procedimientos
- Definir las necesidades de sistemas de seguridad para:
  - Hardware y software
  - Flujo de energía
  - Cableados locales y externos.
- Aplicación de los sistemas de seguridad incluyendo datos y archivos.
- Planificación de los papeles de los auditores internos y externos
- Planificación de programas de desastre y sus pruebas (simulación)
- Planificación de equipos de contingencia con carácter periódico.
- Control de desechos de los nodos importantes del sistema:
- Política de destrucción de basura copias, fotocopias, etc.
- Consideración de las normas ISO 1400

Etapas para Implementar un Sistema de Seguridad

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:

Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.

Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.

Elaborar un plan para un programa de seguridad. El plan debe elaborarse contemplando:

Plan de Seguridad Ideal (o Normativo)

Un plan de seguridad para un sistema de seguridad integral debe contemplar:

- El plan de seguridad debe asegurar la integridad y exactitud de los datos

- Debe permitir identificar la información que es confidencial

- Debe contemplar áreas de uso exclusivo

- Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles

- Debe asegurar la capacidad de la organización para sobrevivir accidentes

- Debe proteger a los empleados contra tentaciones o sospechas innecesarias

Donde:

Riesgo (roles, fraudes, accidentes, terremotos, incendios, etc.)

Medidas pre.. (Políticas, sistemas de seguridad, planes de emergencia, plan de resguardo, seguridad de personal, etc.)

Consideraciones para con el Personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una conciencia para obtener una autoevaluación de su comportamiento con respecto al sistema, que lleve a la persona a:

Asumir riesgos

Cumplir promesas

Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

Motivar

Se debe desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel empresarial, de cargo y individual.

Capacitación General

En un principio a los ejecutivos con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa. El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo.

Este proceso incluye como práctica necesaria la implantación la ejecución de planes de contingencia y la simulación de posibles delitos.

Capacitación de Técnicos

Se debe formar técnicos encargados de mantener la seguridad como parte de su trabajo y que esté capacitado para capacitar a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

Práctica y Cultura

Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión a nivel personal e institucional.

De ser posible realizar conferencias periódicas sobre: doctrina, familia, educación sexual, relaciones humanas, etc.

Etapas para Implantar un Sistema de Seguridad en Marcha

Para hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguiente 8 pasos:

1. Introducir el tema de seguridad en la visión de la empresa.

2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.

3. Capacitar a los gerentes y directivos, contemplando el enfoque global.

4. Designar y capacitar supervisores de área.

5. Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.

6. Mejorar las comunicaciones internas.

7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.

8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que el la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

Aumento de la productividad.

Aumento de la motivación del personal.

Compromiso con la misión de la compañía.

Mejora de las relaciones laborales.

Ayuda a formar equipos competentes.

Mejora de los climas laborales para los RR.HH.

Auditoría de seguridad de sistemas de información

Una **auditoría de seguridad informática** o **auditoría de seguridad de sistemas de información** (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales generalmente por Ingenieros o Ingenieros Técnicos en Informática para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Fases de una auditoría

Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos
- Identificación de los sistemas operativos instalados
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas preventivas.

Tipos de auditoría

Los servicios de auditoría pueden ser de distinta índole:

- Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
- Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- Test de intrusión. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.
- Auditoría de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización de los software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Estándares de Auditoría Informática y de Seguridad

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática.

Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas".

Adicional a este estándar podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001 analizado por maritee.