Autor:
Xombra
www.xombra.com

El mundo de la Informática Forense

(Capitulo II)

Actualmente la realidad competitiva de las empresas, hace imprescindible para ellas acoplarse a las tecnologías de seguridad de la información disponibles, por lo que es prioritario que las empresas tomen medidas para proteger su información estratégica tanto de ataques internos como externos y a todos los niveles.

En el capitulo anterior se expone en forma general lo crucial que es la informática forense dentro de la seguridad de una empresa o institución, se mostrarón algunas herramientas vitales en el área. Pero, la informática forense va mucho más allá de verificar e identificar la intrusión o ataque en los sistemas informáticos de una empresa, una labor importante es adiestrar y concientizar al personal involucrado dentro de la red organizativa y en indicar las medidas preventivas a seguir para evitar que la información de la empresa sea vulnerable.

En este capitulo nos centraremos en las normas y/o actividades que el profesional de la informática forense debe seguir para la correcta planificación preventiva de seguridad de una red corporativa.

A medida que la Internet crece, lo hace de igual manera el número de acciones incursivas ilegales contra la seguridad de las redes corporativas, por ello hay que preguntarse:

a) ¿Quien lleva a cabo estos incidentes?
b) ¿Que los posibilita?
c) ¿Que, quien y porqué los provoca?
d) ¿Como se evitan?
e) ¿como se producen?
f) ¿Que medidas se deben implementar?
g) ¿Se pueden realizar acciones juridicas legales?

Es necesario que las organizaciones concreten sus políticas de seguridad, con el objetivo de planificar, gestionar, y controlar aspectos tan básicos como:

• Definición de seguridad para los activos de información, responsabilidades y planes de contingencia: Se debe establecer que hay que proteger y como.

• Sistema de control de acceso: Se deben restringir y maximizar los permisos de acceso para que cierto personal pueda llegar a una determinada información, estableciendo quien puede acceder a una determinada información y de que modo.

• Respaldo de datos: Hacer copias de la información periódicamente para su posterior restauración en caso de pérdida o corrupción de los datos.

• Manejo de virus e intrusos: Establecer una política de actuación ante la presencia de de malware, spyware y virus evitando los riegos para la seguridad.

Las políticas y una estimación preliminar de los riesgos, observando y analizando los posibles

puntos débiles de la infraestructura organizativa de la red.

Se debe realizar una reunión presencial del personal gerencial y/o directivo para instruirles que:

a) Muchas veces el gasto en seguridad informática es considerado poco rentable.
b) Se debe valorar el coste que les supondría una pérdida de información frente al coste de protegerla
c) La inversión en las medidas de seguridad será más alta para aquellas aplicaciones que presenten mayor riesgo y un mayor impacto en el caso de ser suspendidas.
d) Las medidas de seguridad tomadas racionalmente, provocaran en las organizaciones beneficios tales como aumento de la productividad, aumento en la motivación e implicación del personal.

En la implantación de políticas de seguridad es importante la implicación de la alta dirección y su concienciación en la importancia que tienen las tecnologías y la protección de la seguridad en el éxito de las empresas. Otros requisitos previos a la implantación es establecer quien será el encargado de planificarla y aplicarla y la asignación de responsabilidades. El objetivo es conseguir que las medidas de seguridad den resultados a corto plazo pero con vigencia a largo plazo (no podemos cambiar la política de forma continua, para no crear confusión).

El desarrollo de políticas de seguridad debe emprenderse después de una evaluación de las vulnerabilidades, amenazas y riesgos. Una vez analizado el campo de trabajo, se debe empezar a establecer las medidas de seguridad del sistema pertinentes. Se ha de conseguir sensibilizar a toda la organización de la importancia de las medidas que se deben tomar para facilitar la aceptación de las nuevas instrucciones, leyes internas y costumbres que una implantación de un sistema de seguridad podría acarrear.

Es importante además de planificar, analizar e implantar sistemas y políticas de seguridad, establecer medidas de control, planes de contingencia y realizar auditorias sobre los sistemas implantados y su correcto cumplimiento. Auditar las políticas de seguridad instituidas en la empresa, tiene como objetivos analizar el nivel de cumplimiento de las políticas puestas en marcha, y detectar "agujeros" para evolucionar en las mismas.

Por último, se han de conocer las posibles incitaciones que pueden llevar a los usuarios del sistema a cometer "delitos" sobre la seguridad interna, para sugerir las soluciones a aplicar.

Análisis de riesgos

La información es un bien muy valioso para cualquier empresa. Garantizar la seguridad de la información es por tanto un objetivo ineludible e inaplazable especialmente del departamento de tecnología de la información. Multitud de amenazas ponen en riesgo la integridad, confidencialidad y disponibilidad de la información.

El análisis de riesgos es un estudio detallado de los bienes a proteger, "intangibles", las amenazas a las que están sometidos, posibles vulnerabilidades, contramedidas establecidas y el riesgo residual al que están expuestos.

Uno de los objetivos principales de establecer una política de seguridad es el de reducir al mínimo los riegos posibles, implementando adecuadamente las diferentes medidas de seguridad.. Cuando se establecen los riesgos dentro la organización, se debe evaluar su impacto a nivel institucional total.

Hay multitud de herramientas para llevar a cabo un análisis de riesgos. Una de las más importantes es MAGERIT ("Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas"): método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para

controlar estos riesgos.

Existen otras herramientas como las siguientes: MARION, CRAMM, BDSS, RISK, ARES, BUDDY SYSTEM, MELISA, RISAN, etc.

Reacción Y Prevención De Intrusiones

Las normas de Seguridad standard establecen que todos los archivos deben estar protegidos con unas medidas de seguridad, cuya intensidad variará en función de la naturaleza de los datos que se almacena en ellos. Además, las empresas deberán tomar precauciones control de acceso, asignación y cambio de contraseñas del personal, especificar las funciones y obligaciones del personal que accede al fichero, hacer copias de seguridad, etc.

El perito informático debe verificar el correcto funcionamiento de:

• Firewalls: Son programas que evitan que entren personas no autorizadas en el equipo y bloquean la entrada o salida de ficheros que considera sospechosos. A la hora de instalar uno hay que tener en cuenta la preselección del mismo, configurabilidad, actualizaciones y el análisis de los costos.
• IDS (Sistema de detección de intrusos: Alertan de la realización de ataques con éxito e incluso de ataques en progreso. Aspectos sobre un IDS a tener en cuenta:

a) respuesta
b) instalación
c) análisis de los eventos que suceden en la red
d) facilidad de administración
e) costo de expansión

• IRTS. Es un equipo de personas que llevan a cabo la gestión directa del incidente en el seno de una organización.
• Antivirus. Herramientas especializadas en detectar y eliminar virus y otras amenazas de un computador (Existen muchas empresas antivirus, las cuales cuentan con software para servidores).
• Software Anti-Spam. Filtra el correo, clasificando e identificando los mensajes indeseados.
• Análisis forense. Es muy importante a la hora de analizar los alcances de una intrusión en un computador. Referencia a capitulo I http://www.xombra.com/go_news.php?articulo=1942

Consideraciones Inmediatas para la Auditoria de la Seguridad

Las normas que se deben tener para elaborar la evaluación de la seguridad son:

a) Uso del computador: Se debe observar el uso adecuado del computador y su software que puede ser susceptible a:

• tiempo de máquina para uso ajeno
• copia de programas de la organización para fines de comercialización (copia pirata)
• acceso directo o telefónico a bases de datos con fines fraudulentos

b) Sistema de acceso: Para evitar los fraudes electrónicos se debe considerar de forma clara los accesos al computador de acuerdo a:

• nivel de seguridad de acceso
• empleo de las claves de acceso
• evaluar la seguridad contemplando la relación costo, ya que a mayor tecnología de acceso mayor costo

c) Cantidad y tipo de información: El tipo, calidad y cantidad de información que se introduce en los computadores debe considerarse como un factor de alto riesgo ya que podrían producir que:

• la información este en manos de algunas personas
• la alta dependencia en caso de pérdida de datos

d) Personal: Se debe observar este punto con mucho cuidado, ya que hablamos de las personas que están involucradas al sistema de información de forma directa y se deberá contemplar principalmente:

• la dependencia del sistema a nivel operativo y técnico
• evaluación del grado de capacitación operativa y técnica
• contemplar la cantidad de personas con acceso operativo y administrativo
• conocer la capacitación del personal en situaciones de emergencia

e) Medios de control: Se debe estimar la existencia de medios de control para saber cuando se produce un cambio o un hay fraude (intrusión) en el sistema. Se debe prestar atención con detalle el sistema debido a que podría generar indicadores que pueden actuar como elementos de auditoria inmediata, aunque esta no sea una especificación del sistema.

f) Rasgos del personal: Se debe ver muy cuidadosamente el carácter del personal relacionado con el sistema, ya que pueden surgir:

. malos manejos de administración
. malos manejos por negligencia
. malos manejos por ataques deliberados

g) Instalaciones: Es imperativo no olvidar las instalaciones físicas y de servicios, que significan un alto grado de riesgo. Para lo cual se debe verificar:

. la continuidad del flujo eléctrico
. efectos del flujo eléctrico sobre el software y hardware
. evaluar las conexiones con los sistemas eléctrico, telefónico, cable, etc.
. verificar si existen un diseño, especificación técnica, manual o algún tipo de documentación sobre las instalaciones

h) Control de residuos: Observar como se maneja la basura (temporales, entre otros tipos de ficheros o datos) de los departamentos de mayor importancia, donde se almacena y quien la maneja.

i) Establecer las áreas y grados de riesgo: Es vital crear una conciencia en los usuarios de la institución evaluada sobre el riesgo que corre la información y hacerles entender que la seguridad es parte de su trabajo. Para esto se deben dar detalles sobre los principales riesgos que acechan a la función informática y los medios de prevención que se deben tener, para lo cual se debe:

Para tener un impacto positivo dentro del resguardo de los datos y la seguridad integral dentro de una institución se deben llevar a cabo lo siguiente:

a) Definir elementos administrativos
b) Definir políticas de seguridad
c) A nivel departamental
d) A nivel institucional
e) Organizar y dividir las responsabilidades
f) Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
g) Definir prácticas de seguridad para el personal:
h) Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extintores.
i) Números telefónicos de emergencia
j) Definir el tipo de pólizas de seguros

k) Definir elementos técnicos de procedimientos
l) Definir las necesidades de sistemas de seguridad para:
m) Hardware y software
n) Flujo de energía
o) Cableados locales y externos
p) Aplicación de los sistemas de seguridad incluyendo datos y archivos
q) Planificación de los papeles de los auditores internos y externos
r) Planificación de programas de desastre y sus pruebas (simulación)
s) Planificación de equipos de contingencia con carácter periódico
t) Control de desechos de los nodos importantes del sistema:
u) Política de destrucción de basura copias, fotocopias, etc.

Interesantes artículos de consulta necesaria:

Apuntes sobre la inversión y gestión de la seguridad informática
http://www.virusprot.com/Art49.html

Inseguridad Informática: Un concepto dual en seguridad informática
http://www.virusprot.com/Art47.html

Administración de la TI y seguridad de la información
http://symantec.com/region/mx/enterprisesecurity/content/risks/LAM_3522.html

El valor de la información
http://www.xombra.com/go_news.php?articulo=1935

El cambiante panorama de las amenazas
http://symantec.com/region/mx/enterprisesecurity/content/risks/LAM_3902.html

Nivel de Inmadurez de los Sistemas de Detección de Intrusiones de Red (NIDS).
http://www.htmlweb.net/seguridad/nids/InmadurezdelosNIDS.pdf

Fuentes consultadas:
virusprot.com
symantec.com
cert.org.mx
activalink.net
htmlweb.net
eicar.org
forensicfocus.com
nod32-la.com
bulma.net