La Informática Forense Como Ciencia Sistemática

Montoya Choque Rafael Israel
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
leodraco20@gmail.com

RESUMEN

En este trabajo se pretende comprender a la informática forense como una ciencia sistemática que se basa en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y pruebas necesarias. En donde la escena del crimen es el computador y la red a la cual está conectado. Gran cantidad de documentos son elaborados digitalmente en computadores para ser a continuación impresos o copiados a otros computadores.

Palabras clave

Forense, probatorio, doloso, experticia, log, intrusiones, riesgos, normas.

1. INTRODUCCIÓN

Las nuevas leyes sobre delitos informáticos y la de firmas electrónicas y mensajes de datos abren procesalmente y definitivamente los medios probatorios informáticos. Las operaciones comerciales tienden claramente a reducir costos y ampliar mercados a través de las redes informáticas.

Ya se han producido algunas experticias en Venezuela, Argentina, Colombia y otros países de habla hispana uno de los más destacados es España, en las cuales se ha solicitado la determinación de la autenticidad e integridad por ejemplo de mensajes de e-mail pudiéndose relacionar con un remitente, dirección de correo, computador y hasta con una persona determinada e inclusive la relación entre estos elementos y los datos anexos (attachments) que se encontraban en el email almacenado previamente en el equipo en curso.

Es posible investigar (aún cuando internet permite el anonimato y el uso de nombres falsos) quien es el dueño de sitios web, quienes son los autores de determinados artículos y otros documentos enviados a través de redes o publicados en la misma. El rastreo depende en sí de quien y como realizó el ataque o cualquier otra acción, es posible buscar atacantes exteriores de sistemas e incluso se conocen casos donde se ha determinado la autoría de virus.

Son igualmente investigables las modificaciones, alteraciones y otros manejos dolosos de bases de datos de redes internas o externas, así como de cualquier sistema de redes, ataques internos. Por supuesto, para realizar esta fragosa tarea se debe poseer un conocimiento sólido (normalmente quienes hacen de Informáticos forenses han realizados ataques anteriormente o conocen el uso de herramientas, dispositivos y software de incursión en redes, por lo que tienen una idea de las posibles intrusiones por parte de terceros en un sistema).

La destrucción de datos y la manipulación de los mismos también pueden rastrearse. Los hábitos de los usuarios de los computadores y las actividades realizadas pueden ayudar a la reconstrucción de hechos, siendo posible saber de todas las actividades realizadas en un computador determinado.

2. RASTROS INFORMÁTICOS

Los archivos informáticos pueden guardar información sobre su autor, la compañía, fecha y otros datos de interés jurídico. Esta información es almacenada a espaldas del usuario pudiendo determinarse en algunos casos en que computador/estación fue redactado el archivo (esto es poco fiable, ya que cualquier otra persona pudo trabajar con la PC, falsificando la identidad del usuario propietario de la estación, pero es usado como base del procedimiento).

Las imágenes digitales y otros medios audiovisuales pueden estar protegidos no solo por derechos de autor (copyright) sino por las llamadas marcas de agua digitales que servirían para determinar el origen del archivo aunque hayan sido modificados para disfrazarlos y darle una apariencia distinta.

3. LABOR FORENSE

Ya son frecuentes las inspecciones judiciales sobre páginas Webs y archivos, tendientes a la fijación de hechos que ocurren dentro del vasto mundo electrónico digital.

La promoción, evacuación y control de estas experticias informáticas es especial y bajo las normas de naciente, pero desarrollada informática forense que se pone al servicio inmediato del derecho para afrontar nuevas tareas probatorias y lo más importante es que ya se puede contar en Venezuela, Argentina, Colombia y en otros países con este tipo de pericias útiles en los procesos judiciales del presente y del futuro.

El objetivo de un análisis forense informático es realizar un proceso de búsqueda detallada y minuciosa para reconstruir a través de todos los medios el log de acontecimientos que tuvieron lugar desde el mismo instante cuando el sistema estuvo en su estado integro hasta el momento de detección de un estado comprometedor.

Esa labor debe ser llevada a cabo con máxima cautela y de forma detallada, asegurándose que se conserva intacta, en la medida posible, la información contenida en el disco de un sistema comprometido, de forma similar que los investigadores policiales intentan mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles.

4. DE LOS EXPERTOS

Juan Carlos Guel, jefe del Departamento de Seguridad en Cómputo de la Dirección General de Servicios de Cómputo Académico y Coordinador del Equipo de Respuesta a Incidentes en Seguridad en Cómputo UNAM-CERT, señala: "informática o cómputo forense es un conjunto de técnicas especializadas que tiene como finalidad la reconstrucción de hechos pasados basados en los datos recolectados, para lo cual se procesa la información que pueda ser usada como evidencia en un equipo de cómputo".

En una entrevista realizada por virusprot al Doctor Jeimy J.Cano, Ingeniero de Sistemas y Computación Universidad de los Andes (Colombia) en el año 2002, y cito textualmente:"¿Cuánto se puede tardar en reunir las suficientes pistas que den con el autor de un ataque?

Es una pregunta complicada de responder, pues muchas veces el informático forense debe prepararse para fallar en identificar la persona real que cometió el ataque. Pues la versatilidad que ofrece Internet para enmascarar direcciones IP, correos electrónicos, entre otros aspectos, sugiere un gran conocimiento técnico y paciencia por parte de los atacantes, los cuales también consideran estrategias "anti-forenses" que limiten las investigaciones y la efectividad de las mismas. Luego, la recolección de pista puede ser demorada, algunos casos pueden llevar años en esta labor."

5. DE LAS HERRAMIENTAS

Las herramientas que utilizan los peritos forenses en materia de cómputo para dar con los intrusos, y saber a ciencia cierta qué hicieron en el sistema, se han desarrollado al paso del tiempo, para que nos ayuden en cuestiones de velocidad y faciliten identificar lo que realmente le pasó al sistema y qué es lo que le puede suceder, en su contra parte igualmente se han desarrollado herramientas bastantes sofisticadas en contra de los análisis forenses (herramientas y técnicas que intentan no dejar rastros, camuflarlos o borrarlos, de tal manera que se dificulte una posterior investigación.), tal como lo indica el Dr. Jeimi Cano.

De allí el personal que trabaje en la informática forense deberá poseer sólidos conocimientos técnicos y prácticos y conocer las herramientas de uso, estar al día en bugs (vulnerabilidades) de sistemas (Sistemas operativos, software y hardware)

El campo de la seguridad informática es inmensamente heterogéneo e interesante. Analizar un entorno atacado y comprometido es un desafiante ejercicio de aplicación de ingeniería inversa, para el cual es necesario tener gran conocimiento del funcionamiento de los sistemas involucrados, las técnicas de ataque y los rastros que dejan las mismas.

Se puede leer en diferente sitios web notas similares a estas: "Espero que los nuevos empleados tengan un mínimo de conocimientos de informática y software forense antes de que lleguen a la puerta", apunta Marc Kirby, detective inspector para la sección de informática forense de la británica Unidad Nacional de Crimen de Alta Tecnología (NHTCU)".

Debemos tener en cuenta que la prioridad es preservar lo más íntegramente posible las evidencias del crimen en un estado íntegro. Eso significa colocar el sistema fuera de servicio (offline) cuando todos los usuarios del sistema están presionando para volver a ponerlo on-line.

Sí el sistema, por parte del administrador, fue forzado a seguir funcionando, eliminando las posibles vulnerabilidades o cualquier otra supuesta vía de acceso al servidor, la investigación forense no podrá seguir el rumbo correcto ya que:

- Se eliminaría cualquier posibilidad de persecución del intruso en un futuro ya que se modifica la "escena del crimen" y no se podría calcular los daños estimados con un grado elevado de certeza.
- Hay muchas posibilidades de que se le pasó algo importante por alto al administrador y el intruso (o intrusos) siguen teniendo acceso al sistema. Por lo tanto es mejor sufrir un "downtime" de red, mientras que se realiza el análisis forense del sistema.

Se tiene que establecer una prioridad entre:

(a) Funcionamiento inmediato, teniendo presente que las huellas dejadas por el/los intruso(s) pueden haberse eliminado por descuido del administrador y su equipo, y que el servidor puede seguir teniendo puertas traseras bien ocultas. Esta opción permite estar operativo en poco tiempo.

(b) Investigación forense detallada. Esta opción supone un mayor tiempo de permanencia offline sí no existen planes de contingencia y procedimientos para el backup del servicio.

6. BASES DE LA INFORMÁTICA FORENSE

1. Experticias, Auditoria e Inspecciones en Computadores y Páginas Web.

2. Ubicación de origen de correos anónimos y archivos anexos.

3. Determinación de propietarios de Dominios .com .net .org y otros.

4. Pruebas de violación de derechos de autor.

5. Control preventivo y restricción de uso de computadores

e Internet.

6. Protección de información y derechos de autor.

7. Recuperación de data y archivos borrados intencionalmente o por virus.

8. Recuperación y descifrado de las claves.

Al realizar un análisis de informática forense es necesario tomar notas de lo que se hace con el disco duro, y a que hora, almacenándolo en una ubicación segura como por ejemplo una caja fuerte. Es recomendable que siempre que se trabaje con el medio original esté acompañado por un colega, para que conste a los efectos legales y el testimonio pueda ser confirmado por alguien con un nivel de conocimientos similar.

Las copias deben ser hechas bit-por-bit, es decir será necesario hacer imágenes del disco. La investigación debe ser llevada sobre una copia y nunca sobre el disco original. Se debe hacer tres copias del disco duro original. Sobre todas las copias y original se debe llevar acabo una verificación criptográfica - un checksum. En lo posible realizar dumps de memoria y almacenarlos al igual que los discos.

Es importante todos los hechos pertinentes al caso durante la preparación, recuperación y análisis de las pruebas sobre un ataque sean anotados para poder desarrollar un informe detallado de incidencia que se debe preparar una vez terminado el análisis. Este documento deberá servir como una prueba del incidente o compromiso. Siempre que se realiza cualquier apunte al cuaderno, el asistente debe tener completo conocimiento y entendimiento de lo que ha sido apuntado.

Antes de apagar el sistema, será útil recoger algunos ejemplos de aquella información que posiblemente no ha sido cambiada por los intrusos, como la organización de sistema de ficheros logs, el nombre del host, su dirección IP del fichero e información de algunos dispositivos.

El análisis de la comunicación de datos es realmente importante allí se trabajaran en dos actividades:

1. Intrusión en una red de computadoras o mal uso de la misma.

2. Interceptación de datos.

La intrusión en una red de computadoras o mal uso de la misma es la actividad de la informática forense principal cuando el análisis se hace sobre estructuras de esta naturaleza. Consiste en las funciones siguientes:

(a) Detección de la intrusión, (b) Detectar la evidencia, capturarla y preservarla; y (c) Reconstrucción de la actividad específica o del hecho en sí.

El descubrimiento de la intrusión generalmente involucra la aplicación de software especializado y en algunos casos hardware, para supervisar la comunicación de los datos y conexiones a fin de identificar y aislar un comportamiento potencialmente ilegal.

Este comportamiento incluye el acceso no autorizado, modificación del sistema en forma remota y el monitoreo no autorizado de paquetes de datos.

La captura de la evidencia y su preservación, generalmente tiene lugar después del descubrimiento de una intrusión o un comportamiento anormal, para que la actividad anormal o sospechosa pueda conservarse para el posterior análisis.

La fase final, la reconstrucción de la intrusión o comportamiento anormal, permite un examen completo de todos los datos recogidos durante la captura de la evidencia.

Para llevar a cabo con éxito estas funciones, el investigador forense debe tener experiencia en comunicación de datos y el apoyo de ingenieros y/o técnicos de software.

Antes de realizar un análisis se debe tener en cuenta la siguiente información:

a) sistema operativo afectado.

b) inventario de software instalado en el equipo

c) tipo de hardware del equipo

d) accesorios y/o periféricos conectados al equipo

e) si posee firewall

f) si esta en el ámbito del DMZ (Zona desmilitarizada)

g) conexión a internet

h) configuración

i) parches y/o actualizaciones de software

j) políticas de seguridad implementadas

k) forma de almacenamiento de la información (cifrada o no)

l) personas con permisos de acceso al equipo

m) el PC esta dentro del DMZ

n) existe IDS

o) cuantos equipos en red

6.1. Normas y/o actividades

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) ¿Cómo se evitan? (e) ¿Cómo se producen? (f) ¿Qué medidas se deben implementar? (g) ¿Se pueden realizar acciones jurídicas 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.

6.2. 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.

6.3. Reacción y prevención de intrusiones

Las normas de Seguridad estándar 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 en el 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 verificará el buen 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.

6.4. Consideraciones inmediatas para la auditoria de la Seguridad

Las normas que se deben tener para elaborar la evaluación de la seguridad se mencionan de forma somera, a continuación:

a) Uso del computador.

b) Sistema de acceso.

c) Cantidad y tipo de información.

d) Personal.

e) Medios de control.

f) Rasgos del personal.

g) Instalaciones.

h) Control de residuos.

i) Establecer las áreas y grados de riesgo.

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.

6. CONCLUSIONES

Después de todo el análisis que se ha detallado en el presente trabajo se tiene que para llevar a cabo un análisis forense se debe tener bien en cuenta el uso de normas, leyes y propiedades sobre como un perito forense debe actuar sobre la escena de crimen, como se detallaba, para poder realizar el uso de las herramientas mas adecuadas para realizar su labor; si recordamos una ciencia para ser ciencia debe cumplir ciertos aspectos para lograr ser considerada como ciencia y esos aspectos son que debe tener establecidas axiomas, leyes y teoremas que se cumplan dentro de su ámbito de aplicación de la ciencia, por tanto como la informática forense posee "axiomas" como lo es el enjuiciamiento al/los intruso(s) de un sistema, "leyes" como lo son las leyes sobre delitos informáticos que se definen en cada país y los "teoremas" que vendrían a ser las normas y políticas de seguridad que se deben contemplar para garantizar que los riesgos de intrusiones sean menores, por tanto es que se puede llevar a considerar a la informática forense como una ciencia sistematica.

8. REFERENCIAS

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

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

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

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

[5] Sistemas de Detección de Intrusiones de Diego González Gómez - http://www.dgonzalez.net/pub/ids/html/