Asegurándose contra delitos informáticos

Quispe Yujra Efraín
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
ybberf_15@yahoo.es

RESUMEN

El advenimiento y posterior desarrollo de las tecnologías de la información ha desembocado en numerosos avances para la mayoría de los ámbitos sociales. Este importante avance puede observarse en los múltiples cambios en la forma en la que la información es generada, transmitida y almacenada.

Por esta razón, y como ocurre en otros ámbitos, se hace necesaria la adaptación de determinadas disciplinas para que estas puedan tener efectividad en el nuevo entorno. La informática forense intenta satisfacer una necesidad, cada vez más importante, de reconstruir determinados hechos en función de un conjunto de evidencias digitales.

Palabras clave

Tecnologías de la Información, Reconstruir, evidencias digitales, informática forense.

1. INTRODUCCIÓN

El propósito de las técnicas informáticas forenses, es buscar, preservar y analizar información en sistemas de ordenadores para buscar evidencias potenciales de un delito. Muchos de las técnicas usadas por detectives en escenarios del crimen, tiene su contrapartida digital en la informática forense, aunque hay algunos aspectos únicos en la investigación basada en ordenadores.

Por ejemplo, simplemente abrir un archivo, cambia ese archivo – el ordenador recuerda la hora y fecha en el que fue accedido. Si un detective coge un ordenador y comienza a abrir archivos y ficheros, no habrá manera de poder decir si cambiaron algo. Si un caso de piratería informática llegara a juicio, no tendría validez como prueba al haber alterado y modificado el estado del sistema informático.

Algunas personas creen que usar información digital como una evidencia, es un mala idea. Si es tan fácil cambiar datos en un ordenador, ¿Cómo puede usarse como una prueba fiable? Muchos países permites pruebas informáticas en juicio y procesos, pero esto podría cambiar si se demuestra en futuros casos que no son de confianza. Los ordenadores cada vez son más potentes, por lo que los campos dentro de la informática forense tienen que evolucionar constantemente.

En lo tempranos días de la informática, era posible para un solo detective, navegar a través de los ficheros de un equipo ya que la capacidad de almacenamiento era mucho más baja. Hoy en día, los discos duros de un ordenador pueden contener gigabytes o incluso terabytes de información, por lo que la tarea de investigación puede ser compleja. Los expertos en informática forense deben encontrar nuevas maneras de buscar evidencias, sin tener que dedicar demasiados recursos en el proceso.

1.1. La mayoría de incidencias de seguridad tiene origen en el interior del propio negocio en mas de un 80%.

La labor de estos modernos detectives (informáticos) forenses es identificar, extraer y analizar las pruebas del delito informático, realizando una copia exacta del disco duro -la copia espejo- que contenga las huellas (digitales) del delito y que sirva como prueba en un juicio, acompañado de un exhaustivo informe pericial. La informática forense detecta la intrusión en el sistema, captura la evidencia de esta intrusión y reconstruye el historial del hecho cometido. Entre los comportamientos no autorizados que serán detectados por los investigadores, figuran las modificaciones remotas del sistema o la sustracción de paquetes de datos, por ejemplo.

De forma paralela al vertiginoso avance en tecnologías de la información en la última década, el fraude y la delincuencia informática han ido perfeccionando sus técnicas para derribar cada vez con menor esfuerzo las barreras de seguridad que han surgido con el cifrado de la información y las comunicaciones.

Ahora son los propios delincuentes los que recurren a los algoritmos criptográficos para cifrar sus operaciones, explotar las

vulnerabilidades de las aplicaciones o utilizar las herramientas de borrado para no dejar rastros. El análisis forense se verá así dificultado en multitud de ocasiones por las sofisticadas técnicas esteganográficas de ocultación de pruebas (algo muy frecuente en el caso de las imágenes de contenido ilícito), el gran volumen de datos a analizar -que obligará al forense a efectuar búsquedas restringidas basándose en fechas, formato o contenido para ganar

tiempo y eficacia- y las falsas pistas dejadas por el infractor para confundir a los auditores.

Para que las pruebas acumuladas por los informáticos forenses sean válidas en un proceso judicial (hay que tener en cuenta que, en muchos procesos, estas pruebas serán determinantes),

tanto las herramientas como los procedimientos utilizados deben garantizar la integridad de las evidencias y huir de cualquier modificación de las mismas, por mínima que sea. Un principio universal del análisis forense tal como destaca la Internacional Organization of Computer Evidence (IOCE)- establece que, independientemente de la metodología y persona que realice la investigación, el análisis forense debe conducir a un mismo resultado, claro y unívoco, respetando en todo momento la integridad de las evidencias digitales.

Si existiesen, las cajas fuertes de las empresas de todo el mundo no contendrían dinero en efectivo sino un bien mucho más valioso: la información en forma de bits. Para proteger esta información los millones de datos que dan razón de ser a un negocio-, en lugar de cajas fuertes, los expertos en seguridad lógica configuran complejas redes y sistemas de seguridad informática con los que se trata de preservar la integridad y confidencialidad de las comunicaciones.

Aunque los ataques externos pueden poner en serio peligro a una

empresa y a su rentabilidad e imagen en el mercado, la mayoría de incidencias de seguridad tienen su origen en el interior del propio negocio en más de un 80%, en forma de fugas de información, accesos no autorizados a recursos sensibles, etc.

Para combatir el sabotaje de información, las empresas disponen

de una sofisticada técnica denominada informática forense, llevada siempre a cabo por expertos, con el fin de proteger los datos y garantizar la seguridad informática de las corporaciones frente a los actos de competencia desleal, el fraude, el robo de información o el espionaje industrial.

1.2. Auditorias: tomar el pulso a la seguridad del negocio

La informática forense sirve también para descubrir y poner remedio a las causas de un incidente de seguridad en un determinado equipo o red. De este modo, los planes de actuación ante incidentes se vuelven más eficaces y, sobre todo, se vuelcan en la prevención, la mejor filosofía para reducir los daños de un incidente de este calibre y evitar que vuelvan a producirse.

Estrechamente ligada a la informática forense, y como estadio previo, una auditoría de seguridad eficaz permitirá certificar el correcto funcionamiento de las aplicaciones, redes (fijas e inalámbricas) y código fuente, así como la realización de test de intrusiones y gestión de identidades y accesos, para corroborar que ninguna puerta corporativa esté abierta al fraude. La auditoría de seguridad, normalmente a cargo de una consultora especializada, incluirá búsqueda de vulnerabilidades (formularios

inseguros, agujeros de los sistemas operativos, posibilidades de ataques de denegación de servicio a nivel de aplicación, etc.), control de acceso a los sistemas y aplicativos críticos de la compañía, nivel de adecuación a la política de seguridad y análisis de logs, entre otros.

1.3. La informática forense detecta la intrusión en el sistema, captura la evidencia de esta intrusión y reconstruye el historial del hecho cometido

Al contratar servicios de informática forense, las empresas no sólo ponen remedio a hechos consumados, sino que buscan también prevenir y corregir posibles deficiencias. Como medida preventiva, los profesionales del análisis forense ayudarán a la empresa a comprobar que los mecanismos y sistemas de protección que utilizan son eficaces, al tiempo que detectarán las vulnerabilidades y ofrecerán las soluciones más ajustadas a sus requisitos particulares. Cuando la infracción ya haya sido cometida, la informática forense recogerá las evidencias electrónicas y llegará hasta el origen del ataque o la alteración/destrucción de datos.

Las incidencias y ataques pueden convertirse en oportunidades para el negocio si desde la dirección de la empresa se plantean como un reto a la política de seguridad corporativa y se utilizan para mejorar los aspectos deficientes. El equipo técnico se enfrentará asimismo al reto de recuperación ante el desastre, de modo que puedan estar mejor preparados ante un próximo ataque y los daños causados sean lo menos cuantiosos posibles

1.4. La informática forense sirve también para descubrir y poner remedio a las causas de un incidente de seguridad en un determinado equipo o red

Ya que los delincuentes sí que están volcados en mejorar sus técnicas de ocultación de pruebas. Para muchos profesionales de la seguridad informática, este campo puede resultar enormemente atractivo, puesto que deberán agudizar como en ningún otro sus sentidos, para desmontar las técnicas de ataque y dejar al descubierto los rastros digitales. El investigador forense controlará no sólo las maniobras del atacante, sino que sabrá seguir sus rastros y demostrar los efectos que estas acciones han ocasionado en el sistema.

Los equipos de análisis forense son generalmente multidisciplinares, compuestos por expertos en derecho de las tecnologías de la información, que garanticen los requisitos jurídicos que se requerirán en un tribunal, y en técnicos avanzados en informática forense, que sepan igualmente respetar los procedimientos tecnológicos necesarios para no alterar las evidencias. Algunos informáticos forenses han protagonizado incluso ellos mismos ataques e incursiones a redes, debido a que un profundo conocimiento del enemigo es más que un requisito indispensable en este cambiante mundo del delito informático. El personal dedicado a estas tareas deberá asimismo poseer amplios conocimientos teóricos

y prácticos sobre sistemas operativos, programas y hardware, y actualizar continuamente sus nociones sobre vulnerabilidades y ataques.

3. UN INCIDENTE DE SEGURIDAD TIC

Es bueno recordar que la definición de incidente ha evolucionado, en el pasado, un Incidente de Seguridad en las TIC, era definido como cualquier suceso adverso que tenía como consecuencia una pérdida de la confidencialidad, de la integridad o de la disponibilidad de los datos o sistemas. Hoy en día, un Incidente de Seguridad TIC se entiende como la violación o la amenaza inminente de violación de las políticas de seguridad o los estándares o prácticas de la Organización.

Los procedimientos que emanen de este Plan deberán estandarizar las respuestas intentando minimizar los errores que se puedan producir especialmente aquellos debidos a la premura de tiempo y al stress de la situación, para ello el Plan definirá el Ciclo de Vida continuo de Respuesta ante Incidentes cubriendo cuatro fases:

1. Preparación
2. Detección y Análisis
3. Contención, Erradicación y Recuperación
4. Actividades Posteriores al Incidente

Es aquí donde la Informática Forense se convierte en la estrella. Informática Forense se puede definir como la rama de la Ciencia Forense que mediante un Método Científico, define el proceso de obtención de tanta información digital como sea posible sobre un Incidente para posteriormente analizarla y ser capaz de determinar lo que realmente sucedió durante el mismo, utilizando herramientas y tecnología que puedan ser aceptadas por un tribunal y probar su veracidad y exactitud con el propósito de presentar dicha información como Evidencias.

4. CONCLUSIONES

La informática forense se ocupa con la investigación de acontecimientos sospechosos relacionados con sistemas informáticos, el esclarecimiento de situaciones creadas y sus autores, a través de la identificación, preservación, análisis y presentación de evidencias digitales.

Los servicios de la informática forense, también se aplican a recuperar evidencias para su estudio y a la reconstrucción de determinados hechos con fines privados, empresariales.

La mejor manera en que el individuo puede estar preparado para situaciones de pérdida de información, ya sea accidentalmente o por intrusión, es la de tener un conocimiento mediano de lo que es informática forense para estar provisto de "armas" y herramientas potenciales para combatir esta batalla que normalmente está a favor de quien sabe más.

5. REFERENCIAS

[1]KSHETRI, N. (2006) The simple economics of cybercrime. IEEE Security & Privacy.

[2]SUNDT, C. (2006) Information security and the law. Information Security Technical

[3]CANO, J. (2006) Estado del arte del peritaje informático en Latinoamérica

[4]Alfa- REDI. Disponible en:http://www.alfa-redi.org/ar-dnt-documento.shtml?x=728