“Informática Forense”. La nueva profesión para cazar criminales.

Javier Leonardo Correa Valencia
Universidad Piloto de Colombia
Bogotá D.C.
Correo-e: saghet@gmail.com

Resumen. La información es el activo más valioso que tenemos en la sociedad actualmente. Esto es cada vez más importante para el desarrollo de la actividad empresarial y el éxito en la implementación de sistemas de información. Para proteger la información entra una nueva ciencia, la informática forense, que persigue objetivos de prevención y corrección, una vez que se ha producido una infiltración un sistema informático.

Abstract. Information is the most valuable asset we have in society today. This is increasingly important for the development of business and the successful implementation of information systems. To protect the information enters a new science, computer forensics, with aims of prevention and correction, once infiltration has occurred in the system.

I. Introducción

Hoy en día no están asociados, ni existe un censo, pero se los forenses informáticos se encuentran encaminados en proceso de formación. Están más adelante que la ley, que no contempla todos los delitos informáticos existentes, y se anticipan a jueces e investigadores que, con frecuencia, se apegan a procedimientos tradicionales para investigar delitos en los que interviene la tecnología y hasta en ocasiones el descuido de muchos usuarios.

Antiguamente eran diferentes las armas que se necesitaban para realizar un delito, ya que se utilizaban armas, bombas, cuchillos tal como nos lo muestra la ciencia ficción, hoy hacer ilícitos de robo es mucho más fácil y sencillo, se realiza, en la red y esta cobijado en muchos casos por el anonimato, atrás de una computadora y en el abrigo del hogar. Hoy en día cuando comienzan a desaparecer los saldos en las cuentas de un banco, o dentro de una organización comienzan a aparecer comportamientos extraños que retrasan o impiden el correcto trabajo de una organización, es cuando aparece la necesidad inminente de expertos que logren solucionar estos problemas y que de alguna manera realicen prevención, para que dichos comportamientos atípicos no vuelvan a suceder.

II. Evidencia Digital

La evidencia informática es única cuando se compara con otras formas de evidencia documental. En comparación de la evidencia en papel la evidencia computacional es muy traslúcida, ya una copia de un documento almacenado en un archivo es idéntica al original. Ahora bien, hay que reconocer otro aspecto relevante de la evidencia computacional, en cuanto al potencial de realizar copias no autorizadas de archivos, sin dejar rastro alguno de que se realizo una copia.

III. Análisis Forense Informático

[1] “Es la técnica de capturar, procesar e investigar información procedente de sistemas informáticos utilizando una metodología con el fin de que pueda ser utilizada en la justicia” La Informática Forense se encarga de analizar sistemas informáticos en busca de evidencia que colabore a esclarecer los hechos en una causa judicial o una negociación extrajudicial.

El flujo del procedimiento a realizar es el siguiente:

Figura 1

Proceso General

La primera etapa de un proceso general de levantamiento de evidencia digital parte de una solicitud de intervención desde un juzgado, seguido se realiza un plan de inteligencia, y del proceso de secuestro de la evidencia. Teniendo la evidencia digital en custodia se debe realizar las copias tanto de memoria volátil como de medio físico y se da inicio al proceso de cadena de custodia. Como parte final del proceso se debe llevar el análisis de la evidencia y la escritura y presentación del reporte final el cual busca esclarecer los actos criminales y si se quebraron leyes o globales (Sarbanes-Oxley, etc).

Proceso Específico

El primer paso a realizar es identificar qué computador puede contener evidencia digital, reconociendo la delicada naturaleza de los datos digitales.

La segunda gran tarea es preservar la evidencia contra daños accidentales o intencionales, usualmente esto se realiza efectuando como mínimo una copia o imagen espejada exacta del medio analizado. Dependiendo de los posibles escenarios frente al encuentro del pc se deben tomar o no los datos volátiles dado el caso en el que el equipo se encuentre encendido, con ello se busca el máximo de pruebas y evidencias para su posterior análisis. En cuanto a una imagen espejada, ésta es una copia sector a sector de la unidad original investigada, o también llamada una copia a bajo nivel o a nivel físico en un medio previamente esterilizado.

El tercer paso es analizar la imagen copia de la original, buscando la evidencia o información necesaria. En este paso se trata toda la evidencia en custodia tanto física como volátil, de preferencia por un experto diferente al encargado de realizar el levantamiento de la misma con el ánimo de tener una mejor objetividad en el momento del análisis. Finalmente una vez terminada la investigación se debe realizar el reporte de los hallazgos a la persona indicada para tomar las decisiones, quien puede ser un juez o un CEO.

Preservación de la Evidencia

El orden para la preservación de la evidencia debe darse de manera estricta ya que no de darse con la prioridad respectiva nos podemos arriesgar a perder parte vital en el levantamiento de la evidencia, el orden principal seria:

- Registros, caches, memoria de periféricos
- Memoria (Kernel, Fisica)
- Estado de las conexiones de red
- Procesos que se están ejecutando.
- Discos Rigidos.
- Disketes, archivos de backup
- CD-ROM`s, Impresiones.

Todo este tipo de evidencias siempre debe ser llevado a imágenes de las mismas con el fin de poder ser analizadas.

Evidencia Volátil

La evidencia volátil es aquella que desaparecerá rápido, es decir se perderá en el momento en que el equipo se apague o se ejecute determinado proceso, se trata entonces de las conexiones activas de red, procesos en la memoria, archivos abiertos, etc. Lo que se haga, técnicamente va a afectar la evidencia. En estos casos la evidencia a tomar son:

- Memoria swap y contenidos temporales.
- Conexiones de red actual, puertos abiertos, archivos relacionados con los puertos.
- Procesos, archivos abiertos por los procesos
- En lo posible se debe utilizar herramientas seguras para analizar el sistema.

Para hacer el levantamiento de la información de datos volátiles se deben utilizar herramientas conocidas y ampliamente utilizadas. Deben en lo posible de trabajarse con medios propios como CD-ROM, diskette, USB Drive para no alterar la metadata de la evidencia y siempre debe documentarse el procedimiento realizado para el alza de este tipo de información.

IV. Problemas Jurisdiccionales

Existen varios problemas en el momento de procesar un delito informático y varios de ellos, uno de ellos es ¿En dónde ocurrió el hecho?, éste es un factor muy importante ya que dada la naturaleza del delito pueden darse las penas del mismo, por ejemplo si dicho delito informático solo infringió las políticas internas de la compañía será entonces ella la encargada de tomar las medidas y penas o procedimientos necesarios para su corrección, hecho contrario en las cuales se afecten de manera directa los derechos a la intimidad de una persona, en la cual estará bajo la jurisdicción de la autoridad penal regional (fiscalías). Otro aspecto relacionado es ¿En dónde se encuentra el intruso? Esto se identifica con la finalidad de determinar si es un empleado interno o externo, además de ello se revisa si ¿El país donde ocurrió posee legislación que aborde los delitos informáticos?, al mismo tiempo que ¿El país donde nos encontramos posee legislación relacionada con éste tema?, lo cual es importante para establecer si el delito que se encontró realizando, está o no fuera de la legislación y además esclarecer, si existen penas o precedentes para su juzgamiento, lo que finalmente llevaría a decretar ¿En dónde se juzgaría el hecho?

Leyes contra delitos informáticos por país

Argentina

En Argentina se sancionó el 4 de junio del 2008 la Ley 26.388[2] (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

España

En España, los delitos informáticos son un hecho sancionable por el Código Penal (Ley-Orgánica 10/1995, de 23 de Noviembre/BOE número 281, de 24 de Noviembre de 1.995) [3] en el que el delincuente utiliza, para su comisión, cualquier medio informático. Éstos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) [4] que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

México

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal [5] sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001 [6].

Estados Unidos de América

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986[7]. En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

Colombia

En Colombia el 5 de enero de 2009 [8], el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

Ley 1273 (Delitos Informáticos)

La Ley 1273 de 2009 [8] creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos

legales mensuales vigentes. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello[9], durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

V. Conclusiones

Cuando se da un delitos informáticos en muchos casos se caracteriza por las dificultades técnicas que entraña descubrirlos muchas veces se utilizan técnicas avanzadas de enmascaramiento o también conocido como técnicas anti-forenses. Son delitos, que en la mayoría de los caos no se denuncian, para evitar la alarma social o el desprestigio por un fallo en la seguridad y a veces solo se exponen cuando una potencia ataca a a otra con fines terroristas como el caso ocurrido recientemente entre las coreas. Los afectados en muchos casos prefieren sufrir las consecuencias del delito e intentar prevenirlo para el futuro, antes que iniciar un procedimiento judicial. Esta situación dificulta enormemente el conocimiento preciso del número de delitos cometidos y la planificación de las adecuadas medidas legales sancionadoras o preventivas y desde el punto de vista técnico se pierden los escenarios forenses para verificar el que y el cómo se efectuó dichos hechos delictivos. Existen varios aspectos claves a intervenir en nuestra sociedad para que el delito informático sea tomado como un aspecto a tener en cuenta por todos y que tenga la importancia para que nunca tome desprevenido a nadie.

La carencia de cultura informática es un factor crítico en el impacto de los delitos informáticos hoy en día en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

Las nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre

el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

Sin duda alguna hoy en día la responsabilidad del auditor informático no abarca el dar solución al impacto de los delitos o en implementar cambios; sino más bien su responsabilidad recae en la verificación de controles, la evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los delitos informáticos.

Agradecimientos

Un agradecimiento a la Universidad Piloto y su equipo de docentes que me hicieron apasionar por el tema de seguridad informática y de manera particular en la informática forense, espero que desde el marco jurídico de la legislación colombiana pasando por técnicas anti-hacking hasta la reconstrucción forense aprendidas en el proceso formativo, para así mitigar delitos informáticos no sólo en el ambiente laboral sino en mi entorno personal y familiar, haciendo uso de técnicas electrónicas y de mi conocimiento como especialista para tomar las medidas necesarias en su detección, corrección y si es el caso, su debido proceso ante la justicia de los delincuentes informáticos.

Referencias

[1] Rodney McKennish, report, “1998 Donald Mackay Churchill Fellowship to Study Overseas Developments in Forensic Computing” (Australia)

[2] Código Penal Argentino, junio 24 de 2008. http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

[3] Legislación sobre delitos informáticos España http://delitosinformaticos.com/legislacion/espana.shtml

[4] Galaycosoft Ciberdelitos.

http://www.galaycosoft.es/ciberdelitos.html

[5] Código Penal Federal.

http://www.cem.itesm.mx/derecho/nlegislacion/federal/11/178.htm

[6] Ley especial contra los delitos informáticos.

http://www.redipd.org/documentacion/legislacion/common/legislacion/venezuela/13-leydelitosinformaticos.pdf

[7] Legislación y delitos informáticos estados unidos.

http://www.segu-info.com.ar/delitos/estadosunidos.htm

[8] Secretarias Senado Ley 1273 de 2009.

http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

[9] Revista Cara y Sello “2007 Delitos informáticos”

Perfil del Autor

Javier Leonardo Correa Valencia, profesional en Ingeniería de Sistemas Especialista en Seguridad Informática. Actualmente Gerente

de Tecnología en Textiles Velanex S.A. (Medias Samsara), experiencia en implementación de metodologías ITIL, implementación de servidores de seguridad sobre código abierto (Ipfire/Linux), experto dba SQL Server, CERTIFICACION: ITIL v3, CERTIFICACION: Microsoft® Certified Technology Specialist MCTS