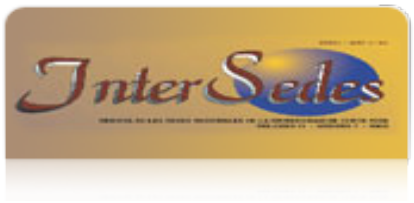

InterSedes: Revista de las Sedes Regionales
ISSN: 2215-2458
intersed@cariari.ucr.ac.cr
Universidad de Costa Rica
Costa Rica

Arias Chaves, Michael

PANORAMA GENERAL DE LA INFORMÁTICA FORENSE Y DE LOS DELITOS INFORMÁTICOS EN COSTA RICA

InterSedes: Revista de las Sedes Regionales, vol. VII, núm. 12, 2006, pp. 141-154
Universidad de Costa Rica
Ciudad Universitaria Carlos Monge Alfaro, Costa Rica

Disponible en: http://www.redalyc.org/articulo.oa?id=66612867010

Inter Sedes. Vol. VII. (12-2006) 141-154. ISSN: 1409-4746

PANORAMA GENERAL DE LA INFORMÁTICA FORENSE Y DE LOS DELITOS INFORMÁTICOS EN COSTA RICA

*Michael Arias Chaves**

Recepción: 2 de marzo de 2007 • Aprobación: 4 de mayo de 2007

RESUMEN

Este artículo da un vistazo general acerca de la informática forense, su definición y características principales. Además, muestra la importancia de que la informática forense sea puesta en práctica de manera efectiva, en conjunto con el apoyo que recibe de las herramientas tecnológicas. Finalmente, explica la aplicación que tiene esta ciencia en Costa Rica, así como la legislación existente en materia de delitos informáticos en el país.

Palabras claves: Informática forense, delito informático, auditoria informática, seguridad informática, tecnología y herramientas.

ABSTRACT

This paper gives a general look about the forensic computer science, its definition and main characteristics. Also, it shows the importance that the forensic computer science is put into practice in an effective way, together with the support that receives from the technology tools. Finally, explains the application that has this science in Costa Rica, as well the existent legislation for computer science crime in the country.

Key Words: Forensic computer science, computer science crime, computer science audit, computer science security, technology and tools.

* Profesor e investigador en el Departamento de Ciencias Naturales de la Sede de Occidente de la Universidad de Costa Rica.
[mike_arias@hotmail.com]

Introducción

Evidentemente el crecimiento en el uso de las computadoras desde que éstas aparecieron allá por el año de 1947, encabezadas por la máquina electrónica ENIAC (Electronic Numerical Integrator and Computer) considerada como la primera computadora digital electrónica de la historia, ha hecho palpable la necesidad de considerar el mundo en el que vivimos, el acceso a tecnología de punta requerida por las empresas y las personas a nivel mundial, la velocidad de transmisión de los datos, así como la seguridad de los mismos, ya que todo esto es muy diferente al trafico de información que se originaba y se transmitía hace poco más de medio siglo, donde el tener una computadora significaba un lujo y algo poco alcanzable.

Ante la gran cantidad de información que se maneja actualmente por medios electrónicos, y el valor tan alto que tiene ésta para las personas y organizaciones, es que la informática forense esta siendo considerada como una herramienta muy valiosa ante la necesidad de contar con algún método que facilite la obtención de pruebas digitales en los casos donde se cometan fraudes o crímenes que atenten contra los usuarios de la información, máxime en tiempos donde el uso de la Internet se ha expandido por todo el mundo, y donde día a día más negocios tradicionales pasan a formar parte de la gran red de redes a nivel mundial.

La informática forense aprovecha su enfoque científico, aprovechando una serie de fenómenos electromagnéticos con la idea de recolectar, analizar, verificar y validar todo tipo de información, ya sea información existente, o información que se consideraba como borrada de la computadora, para beneficio de quienes han sufrido ataques mal intencionados a sus sistemas informáticos y bases de datos.

Desarrollo

Informática Forense

Como una definición de lo que propiamente es este concepto, el FBI ha definido la siguiente descripción:

"…la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional." (López, Amaya, León, 2001, p. 2)

Se puede ampliar que a la informática forense se conoce como el conjunto de herramientas y técnicas que son necesarias para encontrar, preservar y analizar pruebas digitales frágiles, que son susceptibles de ser borradas o sufrir alteración de muchos niveles.

Bajo este concepto, se puede incluir a la informática forense como una herramienta muy importante a tomar en cuenta dentro de una auditoria informática, ya que sirve como un mecanismo para obtener pruebas contundentes que pueden ser tomadas en cuenta si comprobado algún crimen se procede a llevar a instancias mayores como los juicios penales.

Con frecuencia se escucha mencionar en las organizaciones el término de auditoria, sin muchas veces conocer su definición básica. El autor Carlos Muñoz Razo define la auditoría informática como:

"Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes" (Muñoz Razo, 2002, p. 19)

Como se puede apreciar, la informática forense se ajusta perfectamente como una herramienta muy valiosa para ser tomada en cuenta en la realización de una auditoría dentro de una compañía. Por medio de la informática forense se busca información en una computadora que puede estar almacenada en registros de acceso, registros específicos, modificación de archivos intencionalmente, eliminación de archivos y otras pistas que puede dejar un atacante a su paso. La idea entonces es poder erradicar esos ataques logrando una adecuada prevención una vez que el análisis forense se haya llevado a cabo y se generen resultados cuantificables.

¿Qué finalidad busca la informática forense?

Básicamente la importancia de la informática forense radica en identificar y determinar los perjuicios generados por el ataque(s) al que ha sido víctima una organización en particular. El poder cuantificar el nivel de daño recibido, e incluso, identificando a los responsables del crimen, se puede elevar la situación ante las autoridades respectivas como se mencionó anteriormente, con el fin de buscar justicia y que los responsables tengan su pena correspondiente al delito cometido. Posteriormente, y aprovechando la experiencia acumulada en ataques recibidos, es posible generar información que sirva como un historial para tomar acciones preventivas en un futuro.

Al utilizar la informática forense es posible investigar (incluso cuando Internet permite el anonimato y el uso de nombres falsos) quién es el dueño de algún sitio Web, quiénes son los autores de determinados artículos y otros documentos enviados a través de alguna red o publicados en la misma. El rastreo que se realiza trata de indagar quién es y cómo es que realizó el ataque o cualquier otra acción ilícita. Además, es posible buscar atacantes externos de sistemas e inclusive casos donde se ha determinado el contagio de virus.

Son igualmente investigables las modificaciones, alteraciones y otros manejos dolosos de bases de datos de redes internas o externas. Por supuesto, para realizar esta tarea se debe poseer un conocimiento sólido, por lo cual, normalmente quienes hacen de Informáticos forenses han realizado 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.

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* (registro) 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. Recordemos que los archivos informáticos pueden guardar información sobre su autor, la compañía, fecha, hora, entre otros datos que en el caso jurídico son de gran interés. Esta información resulta desconocida para una gran mayoría de usuarios, lo que permite determinar en algunos casos

en qué computadora 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 si se lleva a cabo un procedimiento legal).

Tecnología y herramientas de la mano con la informática forense

Las herramientas que utilizan los expertos 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. La idea es que las herramientas colaboren en cuestiones de velocidad y faciliten la identificación de lo que realmente le pasó al sistema y qué es lo que le puede suceder. Sin embargo, 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.

La IOCE (*International Organization On Computer Evidence*) define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.
4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

El objetivo de este artículo no es dar a conocer a fondo las herramientas de software que automatizan y permiten agilizar aún más el proceso de recolección y análisis de la información utilizada por los peritos, sin embargo, si se van a mencionar brevemente algunos de los medios existentes con ese fin.

Herramientas tecnológicas

De forma global**,** las herramientas tecnológicas que hay son muchas a nivel mundial. Su funcionalidad como se mencionó anteriormente viene a ser la de ayudar al perito que realiza una investigación a encontrar mejores pruebas y de una forma más exacta y precisa, y que a la postre, sirva como evidencia clara para el debido proceso penal.

De esta forma, es posible decir que las herramientas informáticas son una base esencial para colaborar en el análisis de las evidencias obtenidas en un proceso forense. Sin embargo, el poderlas aprovechar al máximo y obtener la confiabilidad deseada de sus resultados tiene que ver mucho con la formación y el conocimiento con que cuente el investigador o perito que haga uso de ellas.

Pasaremos entonces a mencionar algunas de las herramientas que con frecuencia son utilizadas en procesos de

informática forense, con la idea de que el lector pueda adquirir un conocimiento general sobre ellas y su involucramiento en el proceso de investigación forense en informática.

- ENCASE[1]. El software *EnCase* de la firma estadounidense *Guidance Software* es una de las herramientas clave que las fuerzas policiales que han empezado a utilizar técnicas de investigación cibernética. *EnCase* genera una imagen duplicada del disco duro que será utilizada como evidencia ante la justicia. Este sistema incluye mecanismos que salvaguardan la integridad del contenido original del disco.
  En el siguiente paso *EnCase* empieza a analizar la estructura de archivos del disco en busca de evidencias de actividades criminales. Esa herramienta penetra más allá del sistema operativo y busca en todos sitios donde encuentra datos. Esa búsqueda incluye espacios vacíos, espacios no asignados y los archivos "*swap*" de Windows donde se almacenan documentos borrados y otras posibles pruebas.
- FORENSIC TOOLKIT[2]: *Forensic Toolkit de AccessData* (FTK) ofrece a los profesionales encargados de controlar el cumplimiento de la ley y a los profesionales de seguridad la capacidad de realizar exámenes forenses informatizados completos y exhaustivos. FTK posee funciones eficaces de filtro y búsqueda de archivos. Los filtros personalizables de FTK permiten buscar en miles de archivos para encontrar rápidamente la prueba que se necesita. FTK ha sido reconocida como la mejor herramienta forense para realizar análisis de correo electrónico.

Estos dos, son algunas de las muchas herramientas disponibles en el mercado. En ambos casos, son herramientas licenciadas y cuyos costos están entre los 600 y los 4000 o 5000 dólares. Aparte de estas aplicaciones, existen varios programas que no gozan de tanto reconocimiento a nivel mundial, llamados *softwares* de código abierto, que a pesar de no tener tanto renombre si han venido siendo tomadas en cuenta con el fin de que poco a poco tomen mayor posicionamiento en la práctica de informática forense. Además, existen las herramientas a nivel de hardware que sirven también para bloquear discos duros, evitar que se copie información de ellos, entre otros, que colaboran paralelamente en este proceso. Finalmente, cabe mencionar que existen en los mercados de países más desarrollados, computadores especializados para poder realizar investigaciones forenses, en donde el costo de estos equipos puede estar cercano a los 10 mil dólares, según datos expresados por el Organismo de Investigación Judicial (OIJ[3]) .

Aplicación de la informática forense en Costa Rica

La informática forense es un tema bastante nuevo en nuestro país. En realidad, la computación forense en Costa Rica está iniciando, y hasta donde se tiene conocimiento es poco el avance que se ha logrado generar tanto en las empresas del sector privado como en el sector público nacional.

1. Se puede ampliar información en su sitio Web: http://www.encase.com/
2. Se puede ampliar información en su sitio Web: http://www.accessdata.com/
3. Institución costarricense encargada de los temas relacionados con asuntos judiciales del país.

En Costa Rica es el Organismo de Investigación Judicial (OIJ) el ente encargado de velar y supervisar los asuntos relacionados con este tema. El OIJ cuenta desde 1997 con la Sección de Delitos Informáticos, la cual es la encargada de investigar los delitos informáticos y otros actos delictivos en donde la informática fue utilizada para la comisión de éstos o pueda ser útil para esclarecer la verdad de los hechos.

Los delitos informáticos son actividades ilícitas que se cometen utilizando medios tecnológicos, tales como computadoras, sistemas de información, sistemas de comunicaciones, páginas de Internet, entre otros, en donde éstos medios informáticos son el fin del perpetrador, o en otros casos, son el medio por el cual se comete el delito[4].

Proceso para denunciar un acto delictivo

El OIJ ha establecido un proceso en particular con el fin de que si alguna persona o institución desea interponer alguna denuncia producto de un acto delictivo. Los pasos para llevar a cabo este proceso se pueden resumir como se muestra a continuación:

1. Poner la denuncia ya sea en forma verbal en la oficina del OIJ más cercana en donde se dio o verificó el hecho. Esta denuncia se puede hacer en cualquier oficina del país.
2. También, se puede poner la denuncia ante el Ministerio Público mediante una denuncia escrita.
3. En ambas opciones se puede aportar impresiones u prueba referente al hecho.

Los procesos de este tipo son abiertos mediante la denuncia presentada por los ofendidos y la fiscalía los tramita dependiendo del delito y pide la investigación a la Sección. Una vez allí, la Sección se basa en los informes remitidos y algunas diligencias policiales necesarias que se han realizado. Ellos hacen la investigación y la pasan al Ministerio Público. Una vez ahí, se toman las pruebas presentadas y se procede a hacer un análisis a nivel penal para ver si las documentos presentados son lo suficientemente probatorios para determinar que el caso denunciado realmente sucedió, y que además se pueda encontrar al verdadero culpable, ya que es posible que algún caso puede suceder que no se encuentre quién fue el que cometió el delito, y de ahí que algunos casos no se resuelven por este motivo.

Es importante resaltar que la Sección depende de las bitácoras que tienen las empresas en sus equipos para poder realizar una mejor investigación. En el caso de nuestro país, la mayoría de empresas no las manejan, excepto los bancos que sí tienen políticas definidas en ese sentido. “Hay que crear una cultura empresarial donde se haga hincapié en la necesidad y la importancia que conlleva contar con este tipo de bitácoras, tanto para las empresas públicas y privadas. Además, es requerido contar con políticas de usuarios bien definidas, con el fin de que en caso de algún delito, estas políticas ayuden a esclarecer los hechos”, comentó Erick Lewis, miembro de la Sección de Delitos Informáticos del OIJ.

Lewis también mencionó que algunos de los tipos de casos atendidos por esta sección son:

- El fraude informático.
- La alteración de datos y sabotaje informático.

4. Un delito informático es aquel delito que fue cometido utilizando un medio informático o tecnológico, hardware y software.

- La estafa.
- Producción y difusión de pornografía.
- Amenazas.
- Extorsiones.
- Entre otros.

"En realidad la computación forense en Costa Rica está iniciando, en este organismo[5] se han estado utilizando herramientas forenses desde hace unos 3 o 4 años, las cuales han venido a colaborar en obtener mejores resultados. En cuanto a limitaciones, las principales limitantes son por un lado la falta de conciencia de las empresas en registrar todas las actividades en sus equipos y almacenar dichos registros por períodos de tiempo largos; y por el otro, los altos costos que tienen las herramientas informáticas especializadas que existen", explicó Lewis.

Casos atendidos

El OIJ cuenta con estadísticas de una serie de casos que han sido denunciados ante esta instancia a través de los últimos diez años, considerando toda clase de delitos en general. En la siguiente tabla se resumen los delitos relacionados con la informática forense.

De estos casos reportados, el OIJ no maneja una cifra exacta de cuántos casos fueron resueltos y cuántos hay pendientes; sin embargo, la Sección de Delitos Informáticos indicó que la mayoría de los casos tratados antes del año 2005 ya fueron resueltos, mientras que de ese año a la fecha aún se encuentran abiertos, debido a que se encuentra en el debido proceso de resolución en el Ministerio Público.

Legislación

En cuanto a la legislación exclusiva para lo que son los delitos informáticos, la Sección de Delitos Informáticos se apoya en varios artículos del código penal de Costa Rica, así como en algunos otros reglamentos para hacerle frente a este tema.

La ley número 4573 es la principal ley utilizada para reprimir y sancionar los delitos informáticos. A esta ley se le

Tabla 1[6]
Estadísticas de delitos informáticos atendidos por la Sección de Delitos Informáticos del Organismo de Investigación Judicial.

Delito	1997-99	2000	2001	2002	2003	2004	2005	2006
Alteración de datos y sabotaje informático						2	2	4
Delito informático				4	4	1		
Fraude informático				2	10	8	15	56
Violación de comunicación electrónica				1	2	1	2	3

5. Organismo de Investigación Judicial.

6. Datos suministrados por la Sección de Delitos Informáticos del OIJ. Corte de los datos hecho al 22 de septiembre del 2006.

hicieron adiciones de varios artículos mediante la ley número 8148, con el fin fortalecer la ley en lo referente a delitos informáticos.

Las modificaciones hechas se pueden encontrar en los siguientes tres artículos tomados de la ley 8148[7] del código penal costarricense.

"***Artículo 196 bis.-*** **Violación de comunicaciones electrónicas.**

Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

"***Artículo 217 bis.-*** **Fraude informático.**

Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

"***Artículo 229 bis.-*** **Alteración de datos y sabotaje informático.**

Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."

En dichos artículos de la ley se establecen claramente las sanciones que se impondrán a aquellas personas que sean encontradas como culpables bajo uno o varios de los delitos citados anteriormente. Las penas van desde unos meses en prisión, hasta de uno a diez años de cárcel, siendo ésta la pena más elevada.

Además, la Sección de Delitos Informáticos se apoya en otras leyes especiales en donde se detallan artículos donde se castigan los delitos informáticos. Principalmente se apoyan en las siguientes leyes y reglamentos:

- Ley General de Aduanas, Capítulo II, Artículos 221 y 222.
- Ley de la Administración Financiera de la República y sus Presupuestos. Artículo 111.
- Ley de Derechos de Autor, Derechos Conexos.
- Otros reglamentos y manuales que algunas instituciones públicas han creado con el fin de regular el buen uso de los sistemas informáticos.

¿Qué tanto sabemos de seguridad informática?

Hoy en día se puede afirmar que Internet es tierra de nadie, debido a

7. La fecha de vigencia de esta ley es desde el 9 de septiembre del 2001.

su presencia mundial, una red mundial poco regulada y en donde se permite el anonimato. De ahí se puede derivar la pregunta ¿qué tan seguro es navegar por esta red?, pues sin duda alguna eso dependerá de los sitios Web que uno como usuario acceda.

Al igual que la tecnología ha venido a favorecer a todo el mundo en sus actividades diarias y los negocios, ésta también se vuelve amiga de los delincuentes cibernéticos, lo que les permite a ellos realizar secuestros de información, fraudes, robos y compras, todo esto y más, al alcance de un clic.

Las cifras relacionadas con seguridad informática tanto a nivel nacional como mundial son realmente sorprendentes. Según un artículo publicado en la revista *Summa* (Zueras, 2006), desde mediados del año 2006, la empresa Microsoft ha venido realizando una gira centroamericana llamada "*Envision Security Tour*". La idea de este tour es dar a conocer datos aterradores sobre la seguridad informática. En este artículo se señala que el 67% de los computadores del mundo no cumplen con los requisitos mínimos de seguridad.[8] Lo más interesante no está en ese dato, sino en el que el 80% de los usuarios cree que sí está protegido, de ahí la importancia de este tour organizado por la empresa norteamericana en hacer conciencia en los usuarios de la situación real en materia de seguridad.

Dentro del mismo articulo, Andrés Blanco, director de seguridad de Microsoft Caribe y Centroamérica, reconoce las debilidades presentadas por el último sistema operativo presentado por Microsoft (XP), y de los continuos "parches" que los usuarios deben de descargar de la página Web de la empresa[9] con el fin de cerrar las puertas a los eventuales ataques de los "*hackers*" o piratas informáticos. Blanco explica también que para este 2007 saldrá el nuevo sistema operativo llamado Windows Vista, en donde se ha reforzado la seguridad del mismo para beneficio de los usuarios. "Algunas de las mejoras son que este sistema operativo contará con un parental de control, encriptación del disco duro de manera total y segura, configuración para prohibir determinado tipo de dispositivos y filtro *"antiphising"*, explicó Blanco".

Precisamente, el *phising*[10] es una de las causas más frecuentes de estafas electrónicas a nivel mundial. Según la empresa de seguridad informática RSA, el *phising* es la causa del 98% de las estafas electrónicas. Dicho dato se resalta en un reporte emitido en el periódico La Nación publicado el 13 de agosto del año anterior (Fonseca, 2006). A esa fecha, existían 195 entidades financieras estadounidenses que habían sido objeto de este mal en sus sistemas solo en el mes de julio. En nuestro país no existen datos oficiales sobre la cantidad de personas estafadas mediante esta técnica, sin embargo, como se detalló anteriormente en la tabla 1, el fraude informático ha crecido desde el año 2002 hasta el año 2006. Para Jorge Rojas, director del OIJ, la mayoría de estos fraudes no se han reportado con características asociadas al *phising*, ya que en esos casos, los afectados no revelaron sus datos al estafador.

8. Contar con un firewall en uso y un antivirus activo y actualizado.

9. www.microsoft.com

10. Se le conoce como la pesca de *passwords* e información de los usuarios con fines delictivos por parte de los piratas informáticos que utilizan páginas Web falsas.

En otro artículo publicado también en *La Nación*, pero esta vez del día 10 de noviembre anterior (Vargas, 2006), revela que los *ticos* son vulnerables a "*hackers*" por se confiados. En dicha publicación se revela que el riesgo de robo informático en sistemas nacionales es cercano al 80%, y deja muy en claro lo mencionado anteriormente por el director de Microsoft del Caribe y Centroamérica, en el sentido de que las personas creen tener protegidas sus computadoras, cuando realmente no lo están. "La mayoría de los *ticos* son muy vulnerables porque no tienen la mentalidad de seguridad y tienen la idea de que no es con ellos, de que son demasiado pequeños para que algún "*hacker*" se meta en sus sitios", dijo Enrique Sánchez, reconocido *hacker* mexicano quien visitó el país para participar en un congreso de seguridad realizado por el Grupo Cesa.

Como parte del mismo articulo, el experto venezolano Carlos Meza de la empresa 3Com explica que una cantidad mayoritaria de empresas privadas, bancos y otras compañías ubicadas en nuestro país, utilizan solo tres herramientas para proteger sus datos. Esas herramientas son los *Firewalls* (98%), los antivirus (97%) y el dispositivo IDS[11] (69%). Meza explicó, "este trío de herramientas solo es capaz de prevenir el 20% de los ataques informáticos, lo que significa que hay un 80% de vulnerabilidad en nuestros sistemas".

No cabe duda que los sitios más tentadores para recibir ataques por parte de los piratas informáticos son los bancos y las entidades financieras, que son quienes más invierten en la seguridad de sus sistemas. A ellos se podrían sumar además los sitios de telecomunicaciones y los sitios turísticos. Abonado a ellos, los sitios Web del gobierno sufren significativamente en criterios de seguridad, debido principalmente a lo lento que es el proceso de las licitaciones con el fin de adquirir la adecuada seguridad que se necesita.

En el caso de los bancos, en una publicación hecha por el periódico nacional *El Financiero* (Cordero, 2006) acerca de fraudes informáticos hechos en el país, da cabida a un ejemplo muy marcado para aplicar los conceptos analizados de la informática forense. En dicha publicación queda de manifiesto esta grave situación relacionada con delitos informáticos provocados por medio del uso de Internet. En ese articulo se detalla en específico uno de los catorce fraudes informáticos que se han denunciado en los últimos dos años en el país. En dicho caso, una empresa de seguros fue victima del robo de ¢8 millones de una de sus cuentas mediante una transacción realizada por Internet. La situación se ha centrado en el sentido en que para los representantes del banco los procedimientos efectuados en dicha transacción no sufrieron ninguna violación en los sistemas, mientras que la posición del ente asegurador denuncia el movimiento de dinero sin la debida autorización de sus cuentas. Al ser la situación muy reciente (05 de mayo del año recién concluido), el caso se encuentra actualmente bajo investigación por el Organismo de Investigación Judicial (OIJ).

En todos los casos reportados, los bancos han reafirmado su posición de que los problemas que se han presentado no son un problema de ataques a sus sistemas informáticos, sino más bien un mal manejo de parte de los clientes de sus cuentas y descuidos con las claves, sobre todo tratándose de transacciones hechas "en línea"; dejando en claro que esos

11. Es un dispositivo de protección contra intrusos.

ataques son más comunes en muchos otros países como Japón por ejemplo.

Como se puede apreciar, la situación anterior representa un buen caso para aplicar los principios de la informática forense, con el fin de buscar las causas y los responsables directos de cada uno de los fraudes denunciados ante el OIJ. De ahí, que la informática forense que se pone al servicio inmediato del derecho para afrontar tareas probatorias como la expuesta en el caso de los bancos, y que conforme se vaya conociendo e implementando más en el país, sirve como una herramienta útil en los procesos judiciales del presente y del futuro.

Las tarjetas no se quedan atrás

Sin lugar a dudas, quienes utilicen tarjetas de crédito y débito también deben de tener mucho cuidado, ya que mediante la informática forense se ha podido determinar que también los usuarios de este tipo de tarjetas han sido víctimas de estafas. Aunque no fueron dadas por el OIJ cifras reales de estafas producto del uso de tarjetas de crédito, si se estima que son un número considerable y con tendencia a la alza, debido al auge del comercio electrónico, por lo cual los expertos recomiendan mucha cautela y cuidado al momento de realizar transacciones electrónicas por medio de Internet.

Consejos útiles a seguir

Ya sea como persona, o bien como empresa, es muy importante seguir algunos consejos que nos pueden ayudar a todos a evitar ser víctimas de robos, fraudes y sabotajes productos de medios informáticos. La informática forense brinda algunos de los siguientes consejos prácticos:

- No existe un sitio completamente seguro, todo se puede *hackear*. Lo importante es hacer conciencia de la importancia de tratar de contar con mecanismos de seguridad que ayuden a hacer menos vulnerable su sitio Web y/o computador.
- Se puede contar con dispositivos como el llamado *Tipping Point*, que es una plataforma de seguridad construida por *hackers* de 'sombrero blanco', quienes son los que invaden los sistemas con el fin de indagar en dónde es que están las fallas y tratar de corregirlas.
- Utilizar algoritmos de encriptación que protejan los datos que viajan por medio de la red.
- No prestar su computador(s) a personas desconocidas, puede ser objeto para que le instalen software que rastree el número de tarjeta personal e información privada. Cuide su computador como cuida su automóvil.
- Cambie los *passwords* de sus computadoras y pines de sus tarjetas con cierta frecuencia. No utilice datos evidentes que sean de fácil identificación para el *hacker*, como por ejemplo la fecha de nacimiento, iniciales del nombre, etc.
- No revele información privada por correo electrónico, tales como *passwords* o contraseñas, nombres de usuario y números de tarjeta.
- Ignore todos aquellos correos conocidos como *Spam* o correo no deseado, que provienen de remitentes desconocidos o de un tema dudoso.
- Mantenga actualizado todo el sistema de seguridad de su computadora, especialmente el antivirus y el *firewall*.

- Hacer conciencia por parte de las empresas, en registrar todas las actividades en sus equipos y almacenar dichos registros por periodos de tiempo largos.
- Siempre que navegue por Internet, busque la imagen de un candado amarillo en la parte inferior de las páginas Web que visita. Esta imagen, junto con la aparición de la línea *https* al inicio de la barra de direcciones del explorador que este utilizando para navegar, le da la seguridad de que usted se encuentra navegando por un sitio protegido y seguro.

Seguir estos consejos, entre muchos otros no significa que se estará libre de ser victima de un fraude o de un delito informático, sin embargo, le ayudará sustancialmente a mejorar la seguridad de su sitio Web y/o computador, y a cuidar la valiosa información con la que usted trabaja y que sin duda alguna es muy importante para usted.

Conclusión

El desarrollo de las nuevas tecnologías informáticas ha cambiado los medios de registro de la actividad intelectual humana. Las computadoras son esenciales en los negocios de hoy en día, y son parte del vivir cotidiano de las personas. En ellas se puede guardar información financiera, correspondencia interna, propiedad intelectual, listas de precios y otra información sensible, como registros de su compañía y empleados, de ahí la importancia enorme que tiene el lograr alcanzar un nivel de seguridad que permita gozar de plena tranquilidad para mantener su información segura, o bien, el poder realizar transacciones de negocios y personales sin ninguna desconfianza.

La función de la informática forense viene a jugar un papel fundamental en este apartado de la seguridad informática, siendo una herramienta muy importante a tomar en cuenta dentro de las auditorías que las empresas quieran aplicar en el seno de su organización, o bien, como una poderosa herramienta que colabore con investigaciones de carácter judicial. Esa labor debe ser llevada acabo 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 la misma forma que un investigador policial trata de mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles. Por tanto, la informática forense permite investigar un delito informático en busca de evidencia digital que permita recrear lo sucedido y plasmarlo dentro de un informe de manera que pueda ser tomada en cuenta como prueba dentro de un proceso legal; proceso que en nuestro país es llevado a cabo por medio de la Sección de Delitos Informáticos del OIJ.

El crecimiento en el uso a nivel mundial de Internet, la sustitución a la que ha sido objeto el correo de cartas en papel por el correo electrónico, las redes de informática que permiten nuevos tipos de publicaciones virtuales sin necesidad de imprimirlas, son claras señales de que la era digital se ha apoderado del mundo, por lo que día a día se ha visto y se seguirá viendo a las personas y compañías luchando por tener mejores niveles de seguridad de su información, abocando sus esfuerzos a más y mejores mecanismos tanto de autentificación como de autorización a nivel de servicios, que brinden mayor confianza en los usuarios.

Las leyes sobre delitos informáticos y mensajes de datos abren procesalmente los medios probatorios informáticos a favor de la lucha establecida para vencer la delincuencia cibernética tan difícil de probar debido a las características de anonimato y virtualidad manejadas en Internet, situación que puede ser atacada efectivamente con las técnicas utilizadas por los peritos en la informática forense, tales como el rastreo, la reconstrucción de datos, las inspecciones y la evaluación y control de la información recuperada.

Es evidente que a nivel mundial la mayoría de personas creen que están bien protegidas de posibles ataques cibernéticos, y como se pudo apreciar, en Costa Rica el exceso de confianza de los *ticos* los ha llevado a tener esa errónea idea de creer estar bien protegidos. En ese sentido, es necesario hacer conciencia, tanto en las personas como en las compañías, de tomar en cuenta los concejos que los expertos brindan, tales como registrar todas las actividades en sus equipos y almacenar dichos registros por periodos de tiempo largos, contar con herramientas tecnológicas de protección debidamente activadas y actualizadas como los *firewalls* y los antivirus, no revelar información personal por Internet y navegar por sitios seguros, entre muchas otras. El cumplir con estos consejos no indica que se estará a salvo, pero sin duda alguna permitirá alcanzar un mayor grado de protección ante posibles ataques malintencionados.

Por último, y en vías de un avance que pretende alcanzar la presidencia de la República encabezada por el señor presidente Oscar Arias con el proyecto "Gobierno Digital", es muy importante hacer hincapié en la necesidad de reforzar estos temas de seguridad concernientes a la informática forense y el apoyo económico que esta rama necesita. En dicho proyecto se pretende utilizar Internet como plataforma para prestar servicios públicos de una forma más eficiente, de manera de hacer menos problemático los diversos trámites que se deben de realizar al intentar utilizar un servicio público. El situar al país en una apertura tecnológica de este calibre sin duda alguna no solo necesita contar con la tecnología apropiada, sino que también se debe de tomar como ejemplo a naciones extranjeras que han implementado el mismo sistema con el fin de aprovechar de su experiencia en nuestro beneficio, sin olvidar que vivimos en un país con una cultura no tan acostumbrada a realizar sus transacciones por Internet, y en donde la capacitación, la seguridad y la confianza que brinde este programa, serán pilares fundamentales para el éxito de esta iniciativa, hoy en pañales.

Bibliografía

Arrieta Arias Esteban, 2006, "¿Paga con tarjeta?, no deje que le copien datos", *Al Día*, edición del viernes 8 de septiembre, 2006, p. 6.

Cordero Pérez Carlos, 2006, **"**Catorce fraudes informáticos en últimos dos años en el país", *El Financiero* Nº 566, edición del 22-28 de mayo.

Fonseca Pablo, 2006, "Circulan en Internet 634 correos para robarle dinero" *La Nación*, edición del domingo 13 de agosto, 2006, p.16A.

Muñoz Razo Carlos, 2002, *Auditoria en Sistemas Computacionales*, Primera Edición, México DF, Editorial Prentice Hall.

Vargas Alejandra, 2006, "Ticos son vulnerables a 'hackers' por ser confiados" *La Nación*, edición del viernes 10 de noviembre, 2006, p. 16A.

Zueras Daniel, 2006, "Seguridad informática, "Cerrar las puertas de la casa", *Revista Summa*, edición 146, julio 2006, p. 160.

Páginas Web

Asamblea Legislativa de la República de Costa Rica, "**Ley 4573**", recuperado el 24 de enero de 2007, en: http://www.inamu.go.cr/derechos/leyes/ley4573.doc

Asamblea Legislativa de la República de Costa Rica, "**Ley 8148**", recuperado el 24 de enero de 2007, en: http://www.asamblea.go.cr/ley/leyes/8000/8148.doc

Sitio Web de Informática Forense, recuperado el 10 de noviembre de 2006, en: www.ciencia-forense.com/Informatica_Forense.htm

López Óscar, Amaya Haver, León Ricardo, "*Informática forense: generalidades, aspectos técnicos y herramientas***"** recuperado 9 de noviembre de 2006 en: www.urru.org/papers/RRfraude/ InformaticaForense_OL_HA_RL.pdf

Entrevista

Arias, Michael, Entrevista sobre "La perspectiva de la Informática Forense en Costa Rica", realizada a Lewis Hernández Erick, miembro de la Sección de Delitos Informáticos del OIJ, San José, 15 de diciembre de 2006 y 25 de enero de 2007.