LINEAMIENTOS PARA ASEGURAR LA CONFIABILIDAD E INTEGRIDAD DE LA EVIDENCIA EN LA PYMES

Parada Arévalo José Alvaro
jose.parada@live.com
Universidad Piloto de Colombia

Resumen—En el presente artículo se plantean unos lineamientos de seguridad para que las empresas PYMES interesadas tengan una referencia clara de aplicar algunas de las mejores prácticas al momento de enfrentarse a un incidente de seguridad crítico y se maneje la situación de la mejor manera posible.

Índice de Términos—Cadena de custodia, Computación forense, Delito Informático, Evidencia digital, Incidente de seguridad, imagen forense.

I. INTRODUCCIÓN

Las pequeñas y medianas compañías son un motor bastante importante en el crecimiento económico sin importar al sector al que pertenezcan; al momento en que a una compañía se le presenten dificultades relacionados con la seguridad de la información puede que no represente un impacto considerable a la economía, pero si sumamos un gran número de empresas a las que se les presente este tipo de dificultad y carezcan de procedimientos y/o lineamientos para realizar un análisis sobre lo que origina los incidentes informáticos el sector se puede llegar a ver notablemente afectado, y aún más cuando los incidentes de seguridad ocurren y no se indaga sobre la causa de los mismos sin embargo este tipo de inconvenientes se puede llegar a manejar teniendo los lineamientos correctos sobre el manejo y análisis de los hechos y las evidencias teniendo en cuenta los mejores estándares utilizados nacional como internacionalmente.

II. NECESIDAD EN LAS COMPAÑÍAS

En el momento en que se presenta un incidente de seguridad en las pequeñas empresas, muchas de estas no tienen un alto conocimiento en informática forense, ni de las herramientas disponibles en el mercado o de uso libre para realizar la correcta toma de evidencia o el manejo del incidente, por otro lado se encuentran con soluciones muy costosas para su presupuesto. Al ver esta dificultad las compañías no tienen otra opción que dejar de lado el incidente presentado sin poder realizar un debido proceso de indagación o de ser necesario escalar con las entidades judiciales competentes debido a que muchas de estas empresas pymes no tienen un procedimiento adecuado que permitan asegurar la confiabilidad e integridad de la evidencia, y al momento en que las autoridades competentes deban realizar su intervención dada la magnitud del incidente se encuentran dificultades debido a que no se tuvo apoyo en algún procedimiento de manejo de evidencia inicial que permita identificar que la evidencia que están recibiendo es confiable e integra.

Por otro lado existen aún muchas compañías que aún creen que por ser una empresa de categoría pequeña o mediana no va a ser un blanco para los atacantes sin embargo se observa que Dado a que el acceso al servicio de internet ha aumentado desde el año 2002 de un 5% de la población a un 75% al año 2012 y en aumento debido a las grandes campañas por parte del gobierno y las facilidades económicas que ofrecen los diferentes operadores de servicios de internet.

Esto nos indica que el porcentaje de colombianos que hace uso de este servicio aumenta rápidamente así como también aumenta el riesgo de exposición a ser víctima de un delito informático, al momento en que se realiza la indagación en las diferentes entidades como la fiscalía o equipos de respuesta ante emergencias informáticas como el CSIRT-CCIT de Colombia para obtener información sobre

algunas de las estadísticas que manejan acerca de los eventos reportados por las diferentes empresas al momento de ser víctimas de un fraude informático no es fácil obtener respuesta,

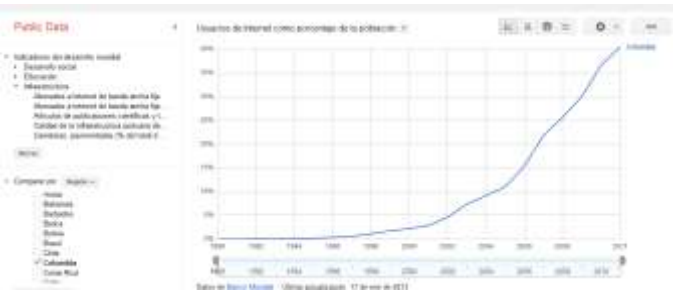

Figura 1.

posiblemente por el riesgo reputacional al que pueden exponer a las entidades al momento de publicar este tipo de información, por otro lado se encuentra la información que es publicada por diferentes medios tales como los portales web de algunas empresas de seguridad y algunos medios de comunicación nacionales, existen datos relevantes como "Delitos informáticos en Colombia dejan pérdidas por 400 millones de dólares anualmente (oct 2012) [1], lo cual se debe al poco interés de la seguridad por parte de los usuarios de diferentes dispositivos tecnológicos y se enfocan exclusivamente a su parte funcional, por otro lado se encuentran cifras como "el valle con el mayor número de delitos informáticos"[2], este departamento presenta 430 denuncias de delitos informáticos en los primeros 7 meses del año 2012.

El evento Ack Security Conference que se realizó en la ciudad de Manizales en marzo del año 2012 reunió a varios de los expertos en el tema de seguridad donde dan a conocer la siguiente cifra: "en promedio 187 denuncias mensuales por fraude electrónico se registran en Colombia"[3] siendo Colombia el que ocupa el tercer puesto en Latinoamérica en delitos informáticos después de Brasil y México, no se tiene cálculo de los fraudes electrónicos que padezcan las entidades bancarias ya que esto les generaría una muy mala imagen ante la comunidad.

Esto indica que no se están tomando las medidas adecuadas para proteger la información y existe mucha confianza por parte de las personas y empresas donde se cree que nunca serán víctimas de los delincuentes informáticos.

III. NORMATIVIDAD LEGAL

De acuerdo al nivel de afectación hacia la compañía sus directivos decidirán de acuerdo a sus normas y políticas internas escalar o no a entidades judiciales, al momento de que el incidente requiera ser escalado a un nivel superior, es decir, entablar una investigación judicial se debe tener en cuenta lo siguiente:

En el caso Colombiano la Ley 527 de 1999 del código penal, reglamenta la admisibilidad y fuerza probatoria de los mensajes de datos, e indica los criterios para valorar probatoriamente un mensaje de datos.

Ley 527. ART. 10. Admisibilidad y fuerza probatoria de los mensajes de datos. “Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del capítulo VIII del título XIII, sección tercera, libro segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original”.

Ley 527. ART. 11. Criterio para valorar probatoriamente un mensaje de datos. “Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente”.

Es decir, para que en Colombia un mensaje de datos tenga valor probatorio debe asegurarse: la confiabilidad en la forma en la que se generó; la confiabilidad en la forma en la que se conservó; y, la confiabilidad en la forma en la que se identifica al autor.

Además, la Corte Constitucional en la Sentencia No. C-662 de Junio 8 de 2000 consideró: "El proyecto de ley establece que los mensajes de datos se deben considerar como medios de prueba, equiparando los mensajes de datos a los otros medios de prueba originalmente escritos en papel. Al hacer referencia a la definición de documentos del Código de Procedimiento Civil, le otorga al mensaje de datos la calidad de prueba, permitiendo coordinar el sistema telemático con el sistema manual o documentario, encontrándose en igualdad de condiciones en un litigio o discusión jurídica, teniendo en cuenta para su valoración algunos criterios como: confiabilidad, integridad de la información e identificación del autor" [4]

IV. MEJORES PRACTICAS

Dentro de las mejores prácticas utilizadas internacionalmente se encuentran la RFC 3227 la cual ofrece unas recomendaciones para evitar alterar la evidencia al momento de manipularla: " Directivas principales durante la recopilación de Pruebas

Respetar a su sitio la política de seguridad y comprometer el manejo apropiado de incidentes y aplicación de la ley personal.

Captura de una imagen lo más exacta del sistema como sea posible.

Mantenga notas detalladas. Estas deben incluir fechas y horas. Si Posible generar una transcripción automática. (Por ejemplo, En el sistema Unix el 'script' puede ser usado, sin embargo la salida de archivo que genera no se deben a los medios de comunicación que es parte de las pruebas). Notas e impresos de salida debe ser firmado y fechado. Nota la diferencia entre el sistema y el reloj UTC. Para cada fecha y hora previstas, indicar si el tiempo UTC o local se utiliza.

Esté preparado para testificar (quizás años más tarde), que expone todas las acciones que tomó y en qué momento. Notas detalladas es Vital.

Minimizar los cambios a los datos en que se van a coleccionar. Esto no se limita a los cambios en los contenidos, así que debería evitar la actualización de archivo los tiempos de acceso o directorio.

Eliminar las vías externas para el cambio.

Cuando nos enfrentamos a una elección entre la recolección y el análisis que debe hacer primero la recopilación y el análisis posterior.

Aunque no es necesario afirmar, sus procedimientos deben ser aplicables. Al igual que con cualquier aspecto de una política de respuesta a incidentes, los procedimientos deben ser probados para garantizar la viabilidad, Especialmente en una crisis. Si es posible, los procedimientos deben ser automatizados por razones de velocidad y precisión. Sea metódico.

Por cada dispositivo, de adoptar un criterio que debe ser aprobado se ajusta a las directrices establecidas en el procedimiento de su recolección. La velocidad será con frecuencia de manera crítica, donde hay una serie de Dispositivos que requieren examen puede ser apropiado para difundir el trabajo entre su equipo para recoger las pruebas en paralelo. Sin embargo en un único sistema dado de recogida debe hacerse paso a paso.

Proceda de la volátil a la menos volátil (véase la Orden Volatilidad de abajo).

Usted debería hacer una copia a nivel de bits de los medios de comunicación. Si desea hacer el análisis forense debe hacer una copia a nivel de bits de su copia de las pruebas para ese fin, su análisis seguramente puede modificar los tiempos de acceso a los archivos. Evite hacer pruebas forenses en la copia.

2.1 Orden de Volatilidad

Al recoger las pruebas se debe proceder del volátil a los menos volátiles. Aquí tiene un ejemplo de orden de la volatilidad típico de un Sistema.

Registros, caché.
Tabla de enrutamiento, caché arp, el proceso de mesa, núcleo de las estadísticas, Memoria.
Temporal de los sistemas de archivos.
Disco.
Registro y supervisión remota de datos que es de interés para el Sistema en cuestión.
Configuración física, la topología de la red.
Los medios de comunicación de archivo.

2.2 Cosas de evitar.

Es demasiado fácil destruir las pruebas, sin embargo inadvertidamente.

No cierre hasta que haya concluido la recopilación de pruebas. Muchas pruebas se pueden perder y el atacante puede haber alterado el Inicio / apagado scripts / servicios para destruir las pruebas.

No confíes en los programas en el sistema. Ejecute sus pruebas recopilación de los programas de los medios de comunicación debidamente protegidos (véase a continuación).

No ejecute programas que modifiquen el tiempo de acceso de todos los archivos del sistema (por ejemplo, 'tar' o 'xcopy').

Al retirar las vías externas para el cambio en cuenta que simplemente desconectar o filtrado de la red puede desencadenar "Muerto interruptores" que detectan cuando están fuera de la red y Borrar pruebas.

2.3 privacidad

Respetar la intimidad normas y directrices de su empresa y Su jurisdicción legal. En particular, asegúrese de que no Con la información recogida a lo largo de las pruebas que está buscando Está disponible para cualquier persona a la que normalmente no tienen acceso a esta información. Esto incluye el acceso a los archivos de registro (que puede revelar patrones de comportamiento de los usuarios), así como los datos personales Archivos.

No inmiscuirse en la vida privada de personas sin un fuerte Justificación. En particular, no recopilan información de Zonas que normalmente no tienen acceso a la razón (como Expediente personal tiendas) a menos que usted tenga una indicación suficiente Que hay un incidente real.

Asegúrese de que tiene el respaldo de su empresa establecida Procedimientos en la toma de los pasos que hacer para reunir las pruebas de un Incidente.

3 El procedimiento de recogida.

Su colección procedimientos deben ser lo más detallado posible. Como es En el caso de su estado general de los procedimientos de Manejo de Incidentes, deben Ser inequívocos, y debe reducir al mínimo la cantidad de la toma de decisiones necesarias durante el proceso de recolección.

3.1 Transparencia

Los métodos utilizados para recopilar pruebas deben ser transparentes y Reproducible. Usted debe estar preparado para reproducir con precisión el Métodos que utilizó, y han probado los métodos independientes Expertos.

3.2 Colección Pasos

¿Dónde están las pruebas? Lista de lo que son los sistemas que participan en la Incidente y de la que se recogerán las pruebas.

Establecer lo que es probable que sea pertinente y admisible. Cuando En la duda abstente de recolección demasiado más que no Suficiente.

Para cada sistema, obtener la correspondiente orden de la volatilidad.

Eliminar las vías externas para el cambio.

Registro de la medida de que el sistema de reloj de la deriva.

Pregunta ¿qué otra cosa pueden ser las pruebas a medida que se trabaja a través de la Colección pasos.

Documento cada paso.

No se olvide de las personas involucradas. Tomar notas de que fue allí Y lo que se hace, lo que observó y la forma en que Reaccionado.

Cuando sea posible se deben tomar en cuenta la generación de comprobación y Criptográficamente la firma recogidas las pruebas, ya que esto puede hacer más fácil de mantener una fuerte cadena de pruebas. Al hacerlo, usted debe No alterar las pruebas.

4 El procedimiento de archivo

Las pruebas deben ser estrictamente garantizadas. Además, la Cadena de Custodia debe estar claramente documentada.

4.1 Cadena de Custodia

Usted debe ser capaz de describir claramente la manera en la se encontraron pruebas, Cómo se maneja y todo lo que sucedió a él.
Los siguientes deben ser documentados:

¿Dónde, cuándo y por quién fue descubierto y las pruebas Recogidos.
Dónde, cuándo y por quién fue manejado o las pruebas de examen.
¿Quién tiene la custodia de las pruebas, durante qué período. ¿Cómo sé que almacenan.
Cuando las pruebas cambiado custodia, el momento y la forma en que el Transferencia ocurrir (incluir números de envío, etc.)

4.2 Dónde y cómo Archivo

Si es posible de uso común los medios de comunicación (en lugar de alguna oscura de almacenamiento los medios de comunicación) deberían ser utilizados para el archivo.

Acceso a la prueba debería ser muy limitado, y debe ser claramente documentados. Debe ser posible detectar no autorizado acceso.
“[5]

Por otro lado el departamento de justicia de los estados unidos expone en uno de sus documentos "investigación en la escena del crimen electrónico" unos de sus lineamientos de seguridad para las investigaciones forenses donde se resaltan varios de los aspectos que se estudian en el presente proyecto tales como el manejo de la evidencia en la escena, encontrar fuentes potenciales de evidencia, identificación de dispositivos con valor probatorio, además del tratamiento de la evidencia como el procedimiento de embalaje transporte y almacenamiento, este documento se encuentra referenciado al finalizar el artículo, donde dentro de los parámetros más relevantes se encuentra la evaluación de la situación a la cual pueda estar expuesta a diferentes circunstancias que se exponen a continuación:
“Evaluar la situación:
Después de identificar el estado de alimentación del ordenador, siga los pasos que se indican a continuación para la situación más como su propio
Situación 1: El monitor está encendido. Se muestra un programa, aplicación, producto del trabajo, imagen, e-mail o sitio de Internet en la pantalla.
1. Fotografiar la pantalla y registrar la información representada.
2. Continúe con "Si el equipo está encendido"
Situación 2: El monitor está encendido y un protector de pantalla o imagen es visible.
1. Mueva el ratón un poco sin presionar ningún botón o girando la rueda. Tome nota de cualquier actividad en pantalla que hace que la pantalla para cambiar a la pantalla de inicio de sesión, el trabajo producto, u otra pantalla visible.
2. Fotografiar la pantalla y registrar la información representada.
3. Continúe con "Si el equipo está encendido"

Situación 3: El monitor está encendido, pero la pantalla está en blanco como si la pantalla está apagada.
1. Mueva el ratón un poco sin presionar ningún botón o girando la rueda. La pantalla cambiará de un espacio en blanco pantalla para la pantalla de inicio de sesión, el producto funciona, u otro visible mostrar. Tenga en cuenta el cambio en la pantalla.
2. Fotografiar la pantalla y registrar la información representada.
3. Continúe con "Si el equipo está encendido"

Situación 4a: El monitor se enciende off, la pantalla está en blanco.
1. Si el interruptor de alimentación del monitor esté en la posición de apagado, el monitor. La pantalla cambia de una pantalla en blanco a una pantalla de inicio de sesión, producto, u otra pantalla visible trabajar. Tenga en cuenta el cambio en la pantalla.
2. Fotografiar la pantalla y la información visualizada.
3. Continúe con "Si el equipo está encendido"
Situación 4b: El monitor se enciende off, la pantalla está en blanco.
4. Si el interruptor de alimentación del monitor esté en la posición de apagado, el monitor. La pantalla no cambia, sino que se mantiene blanco. Tenga en cuenta que no se produce ningún cambio en la pantalla.
5. Fotografiar la pantalla en blanco.
6. Continúe con "Si el equipo está apagado"
Situación 5: El monitor está on, la pantalla está en blanco.
1. Mueva el ratón un poco sin presionar ningún botón o girando la rueda; esperar una respuesta.
2. Si la pantalla no cambia y la pantalla permanece en blanco, compruebe que se está suministrando energía al monitor. Si la pantalla permanece en blanco, marque la caja de la computadora para las luces activas, escuche ventiladores moviéndose u otros indicadores que el equipo está encendido.
3. Si la pantalla se queda en blanco y la caja de la computadora hay indicios de que el sistema está encendido, vaya al "Si el equipo está apagado", por otro lado se mencionan aspectos para tener en cuenta al momento de realizar la recolección de la evidencia los diferentes tipos de camuflaje que pueden tener diferentes medios de almacenamiento como lo son las memorias USB

Figura 2.

Por lo cual se debe prestar bastante atención al momento de realizar la recolección ya que estos dispositivos se pueden confundir con otro elemento [6]

V. HERRAMIENTAS DE SOFTWARE

Si bien es cierto las herramientas licenciadas presentan mayor utilidad debido a que los desarrollos de las mismas son más completas lo cual les da un valor agregado sin embargo no se debe dejar de lado que algunas de las casas fabricantes que desarrollan aplicaciones costosas tienen versiones menos complejas y que nos permiten acceder a funcionalidades básicas pero efectivas, es el caso de **EnCase** el cual permite crear imágenes forenses de una manera comprimida por segmentos y realizar la validación hash y sha1 por cada uno de estos lo que nos garantiza que no se pueda dar una colisión de hash, por otro lado nos permite analizar información completa, o remanentes de la misma además esta aplicación en su versión de uso libre es reconocida en los estrados judiciales ya que es una de las herramientas informáticas que usan los peritos informáticos para realizar el estudio de las evidencias, por otro lado existen otras herramientas como **FTK Imager** que comparte varias de las funcionalidades de EnCase sin embargo esta herramienta tiene una característica especial que permite realizar el montaje de imágenes y permite su visualización así estas se encuentren ocultas, por otro lado una de las falencias que tiene esta aplicación es que no soporta una gran cantidad de formatos como si lo hace EnCase, también permite recuperar la SAM de Windows la cual contiene la información de acceso de los usuarios de sistema operativo y exportarla para luego poder ser montada

en otra ubicación y poder ser explorada, con la herramienta **OS forensics** es una herramienta eficaz que dentro de sus múltiples características permite realizar una exploración completa de los archivos de registro de Windows lo cual es una de las partes más sensibles del sistema operativo Windows y de donde se puede obtener información de gran importancia, por otro lado se debe tener en cuenta que de acuerdo a la situación a la que se encuentre expuesto el investigador forense se debe tener presente la adquisición de datos volátiles para esto se debe reunir las diferentes utilidades para obtener la mayor información como sea posible de la maquina dentro de los más importantes se encuentra el obtener el direccionamiento IP, tabla de enrutamiento, nombre de la máquina, procesos que se encuentren ejecutando en el instante que se inicia la investigación, la información de la fecha MAC time (Modificación, Acceso y Creación) de todos los archivos del sistema, realizar un volcado de memoria RAM, obtener el listado de archivos que fueron eliminados, entre otros datos que podamos recolectar y que el investigador decida que son importantes para el proceso de investigación que encabece.

VI. CONCLUSIONES

Se debe tener claridad sobre seguir el debido proceso en una investigación y no permitir que el mismo se contamine por razones que puedan generarse en personales únicamente profesionales.

El investigador debe cumplir con las leyes sobre el manejo de la evidencia digital y regirse a las normas de acuerdo al país donde se encuentre realizando esta actividad.

Se debe documentar de una manera muy organizada todos los eventos de caso con cualquier medio de fijación de tal manera que en el curso de la investigación se pueda acudir a estos eventos sin dejar pasar de lado algún tipo de información que pueda ser importante.

Cuando se realice la extracción de información se debe rotular, nombrar o maquillar de una manera nemotécnica que permita identificar fácilmente las evidencias y relacionarlas con el caso que se esté tratando.

Cuando se extraen imágenes forenses se debe realizar sobre medios esterilizados para impedir que se contamine la evidencia

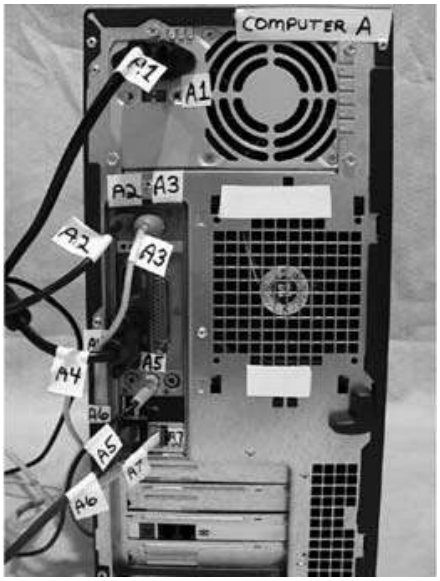

Figura 3.

Realizar la descarga de las aplicaciones forenses de su página oficial para minimizar el riesgo de infección o suplantación en las herramientas

VII. APENDICE

Datos volátiles: se identifican como la información o datos temporales que se almacenan en memoria RAM.

Imagen forense: copia exacta e inequívoca de información.

Figura 1: Aumento en el acceso al servicio de internet desde el año 2000.

Figura 2: Camuflaje de algunos de los medios de almacenamiento USB.

Figura 3. Ejemplo de etiqueta de una evidencia para este caso un PC

REFERENCIAS

[1] Información de estación de radio RCN de Colombia donde relaciona las pérdidas ocasionadas por los delitos informáticos disponible en linea < http://www.rcnradio.com/noticias/delitos-informaticos-en-colombia-dejan-perdidas-por-400-millones-de-dolares-anualmente >

[2] Información de estación de radio RCN de Colombia donde relaciona el departamento con mayor numero de delitos informáticos reportados, disponible en linea < http://www.rcnradio.com/noticias/el-valle-con-el-mayor-numero-de-delitos-informaticos-11195>

[3] Información de estación de radio Caracol de Colombia donde relaciona las denuncias reportadas por delitos informáticos disponible en línea < http://www.caracol.com.co/noticias/tecnologia/en-promedio-187-denuncias-mensuales-por-fraude-electronico-se-registran-en-colombia/20120313/nota/1653843.aspx>

[4] ACIS. Evidencia Digital en el Contexto Colombiano [en línea]. < http://www.acis.org.co/index.php?id=856> [Citado el 22 de enero de 2012]

[5] Norma internacional RFC 3227 disponible en línea < www.ietf.org/rfc/rfc3227.txt>

[6] Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition [en linea]. < www.ncjrs.gov/pdffiles1/nij/219941.pdf>

José Alvaro Parada Arévalo
Ingeniero de Sistemas enfocado al estudio de técnicas forenses, se desempeña en el área de seguridad informática en una entidad financiera colombiana apoyando las soluciones y mejoras en esta área.