Panel E – Herramientas forenses: lo que nuestros dispositivos dicen de nosotros

William Baker, Estados Unidos

Debido a la variedad de fuentes de datos, las técnicas forenses pueden ser utilizadas con varios propósitos: pruebas para iniciar un juicio, electronic discovery, violación de políticas internas, investigación criminal, incidentes de seguridad y recuperación de daños accidentales del sistema.

Prácticamente cada organización debe tener la capacidad de utilizar herramientas forenses, sin esta capacidad no es posible conocer cuando ocurrieron los incidentes, tales como una exposición de datos sensibles.

El NIST ha identificado diversas fases en su guía de técnicas forenses para respuesta a incidentes, citándose entre ellas:

- Recolectar datos relevantes: esto implica su identificación y etiquetado. Es necesario procesar los datos preservando su integridad.
- Examen forense: se trata del procesamiento de los datos recolectados usando una combinación de mecanismos automatizados y manuales.
- Análisis: de los resultados del examen utilizando métodos y técnicas legalmente justificados, para derivar información que responda a las preguntas que llevaron a la recolección y examen.
- Reporte: de los resultados del análisis. Implica describir acciones, explicar la selección de herramientas y procedimientos, asegurar las vulnerabilidades encontradas, formulando recomendaciones.

Las categorías de análisis pueden ser archivos, sistemas operativos,

tráfico de redes y aplicaciones.

Se exponen recomendaciones para el uso de herramientas forenses, que incrementan la eficiencia y efectividad de tales actividades:

- Las organizaciones deben asegurarse que sus políticas contengan enunciados claros.
- Las organizaciones deben crear y mantener procedimientos y guías con elementos forenses, conforme a las leyes y regulaciones.
- Las organizaciones deben asegurarse que sus políticas y procesos apoyen el uso razonable y apropiado de las herramientas forenses.
- Los asesores legales deben revisar cuidadosamente las políticas forenses y los procedimientos a alto nivel.
- Las organizaciones deben asegurarse que sus profesionales de tecnologías de la información están preparados para participar en actividades forenses.

Realizar actividad forense implica mantener la integridad de la fuente y el contenido de la información, esto es, mantener la cadena de evidencia. A su vez, se explicita que mantener la cadena de evidencia implica: control de datos forenses, grabar la generación de datos forenses, acceso a datos forenses y cambiar el manejo de datos forenses.

Las tecnologías asociadas a la criptografía como el sellado de tiempo o firmas pueden indicar la fecha en que se accedió a los datos, así como quién accedió y así como la eventual ocurrencia de modificaciones en algún punto de la cadena.

A continuación se hace referencia a los proyectos llevados a cabo por el NIST, y se indica que se está trabajando en el uso de herramientas forenses en

el ambiente de la nube, a los efectos de tener respuestas frente a la comisión de los delitos tanto en la nube o cuanto ante la verificación de un ataque a un servidor en la nube. La privacidad es un tema de importante consideración en mérito a que en la nube no se conoce cuál jurisdicción es la competente.

Finalmente se afirma que en la reconstrucción de archivos borrados, hay tres problemas básicos a enfrentar: identificar y ubicar los archivos que fueron borrados, la necesidad de una herramienta para recuperar los datos, por eso como el resultado depende de una herramienta, ésta debe funcionar correctamente y la falta de certeza reduce la confiabilidad de los archivos recuperados.

Monique Altheim, Bélgica,

La moderadora del panel, señala que hasta los datos borrados pueden ser recuperados, lo que es muy importante al momento de encontrar evidencia. La mayoría de las veces, la evidencia más importante es borrada como sucedió en el caso Enron.

Gustavo Betarte, Uruguay

La presentación se centra en un punto concreto que muestra el delicado equilibrio entre tecnología y privacidad. El uso de cualquier sistema digital deja trazas, información, que permite recuperar e identificar el tipo de actividad realizada.

El problema se presenta cuando esas trazas que permiten identificar la actividad del usuario no son intencionales, o el usuario ha intentado borrar la información porque va a hacer un uso compartido del equipo. Esos datos pueden ser utilizados por una investigación o para fines maliciosos.

Un punto importante es que preservar información en los repositorios digitales puede ser crítico para el desarrollo de ciertas actividades: por ejemplo

el “login”, para recuperarse después de la falla de un sistema, para analizar un incidente de seguridad transcurrido, para auditar el sistema.

Preservar intencionalmente información de las actividades desarrolladas por usuarios o por aplicaciones puede tener un buen propósito.

El problema es que mantener información que permita reconstruir la actividad desarrollada sobre un dispositivo puede plantear escenarios donde se verifique una problemática; por ejemplo la ley uruguaya en materia de protección de datos permite que el propietario de los datos pueda pedir que sean borrados de una base de datos. Mantener estos datos puede ser una amenaza para la privacidad.

La mayoría de los sistemas modernos preservan la historia sin intención. Hay varios artículos de investigación que demuestran lo difícil que puede llegar a ser remover trazas de actividad pasada.

En la historia reciente se han dado bastantes casos de problemas en que se han visto involucradas organizaciones por haber dejado datos remanentes en repositorios que fueron investigados por personas autorizadas. Por ejemplo el caso de los correos electrónicos de Enron, que fueron recuperados luego de borrarse e incluso fueron utilizados como elementos de prueba en un proceso judicial.

Es posible tener varios escenarios donde se verifique una retención de datos no intencional, permitiendo que ciertos datos permanezcan en una base, en un sistema. En este caso los analistas pueden recuperar datos de esos repositorios.

Hoy en día los sistemas se respaldan en bases de datos “embebidas” para ser usadas en repositorios, diseñadas para determinado tipo de información. Aún en el manejo de mails que se pretendan borrar, hay información asociada a ese mail que sigue quedando registrada en la base de datos, por ejemplo mail app de OS X. Otro ejemplo refiere a que Firefox permite aplicaciones que almacenan información de las sesiones en una base de datos SQLite; se trata de una modernización de las cookies.

Hay muchas formas de que queden datos remanentes en los repositorios digitales, con o sin intención y pueden ser recuperados por procesos forenses digitales, el problema es cuando lo hace un actor malicioso no autorizado. Éste sabe como borrar sus trazas; un usuario común es el que se ve más perjudicado.

Finalmente, se explica que el problema de la información remanente es tecnológico ya que se refiere al manejo de información en interfaces, donde los datos quedan disponibles.

Se concluye entonces que lo importante es desarrollar un adecuado equilibrio entre concientización, seguridad institucional y aplicación adecuada de herramientas tecnológicas.

En función de lo señalado la Sra. Altheim indica que el derecho al olvido es cada vez más ilusorio, ya que nunca se pueden borrar los datos.

Yoram Hacohen, Israel

Siendo que se trata del único regulador presente en el panel, es importante su señalamiento en el sentido de indicar que desde que se creó ILITA hace 6 años cuenta con capacidades forenses, con un laboratorio, afirmándose a su vez que, las autoridades de protección de datos que no cuentan con estas habilidades no pueden afrontar tal protección.

Si se pretenden realizar inspecciones es necesario entender el software usado, así como ser capaz de analizar las bases de datos, recolectar evidencia y mantener la cadena, todo en relación con la órbita administrativa, no penal. Considera que la mayoría de las autoridades de protección de datos ya tienen o están construyendo estas capacidades.

Para ello se necesitan cinco elementos: hardware adecuado para mantener la cadena, software adecuado para seguir los procedimientos certificado por NIST u otra organización que certifique, profesionales capaces

que sepan operar los dispositivos y conozcan la tarea forense, poderes jurídicos para aplicar las herramientas y procedimientos para aplicar esos poderes, para crear un caso y presentarlo en juicio.

Se comenta la historia de un alcalde en el norte de Israel que tenía discusiones con un auditor interno municipal, relatándose que llamó a una empresa que realizaba análisis forenses ya que sostenía que había infracciones de seguridad. La compañía forense copia todo el intercambio de archivos con el servidor de la municipalidad y se llevan el servidor al laboratorio. De la casilla de correo del auditor surgen conversaciones con periodistas. El alcalde enjuicia al auditor y en el juicio el auditor cuestiona la autorización para entrar en su cuenta personal. En ese momento interviene ILITA, ya que se analizan temas relativos a la privacidad. En este caso no era adecuado copiar todo el servidor ante la sospecha de un troyano. El caso terminó con una denuncia penal contra el alcalde y el director de la compañía forense por violación de la privacidad.

Lo importante es que cuando se hace trabajo forense se visualiza toda la imagen y si el analista no se limita al objeto que se debe verificar se está infringiendo la privacidad y en Israel esto puede configurar un acto delictivo. Esta es una herramienta muy poderosa que se debe usar con limitaciones.

Se plantea otro relato referido a la utilización de herramientas forenses en una investigación criminal. lLITA condujo una investigación por que la base de datos administrativa de toda la población fue robada del Ministerio del Interior y publicada en un sitio público desde donde se podía descargar. Los datos eran nombres, números de identificación, fechas de nacimiento, direcciones y datos de los padres. El criminal que subió la información al sitio ocultó sus datos usando “proxy”, nombres falsos. También una casilla de correo que cuando se consultó a Google se había creado desde Canadá, motivo por el cual Israel no tenía jurisdicción. Finalmente, se aplicó tecnología forense en sus equipos pudiendo conectar la identidad digital con una persona física. Toda la prueba contra esta persona se deriva del análisis de los datos recolectados. Por eso cuando se habla de cibercriminales las herramientas

forenses son las que llevan a las personas ante la justicia, sin estas herramientas no se los puede enjuiciar. También para las investigaciones administrativas hay que entender cómo funcionan los equipos.

Jeimy Cano, Colombia

Se afirma que todo lo expresado con anterioridad a su presentación adquiere un nivel exponencial cuando la referencia se realiza por computación en la nube. Ésta remite a una serie de elementos tales como procesos, sistemas de información, infraestructura tecnológica que están agrupados por proveedores que tienen servicios, tipos de información, aplicaciones, tipos de plataforma y operación sustentada en procedimientos.

Cloud computing evoluciona en la gestión de la tecnología de la información; se trata de un paso natural en la evolución para que pueda verificarse un tercero administrando la infraestructura. De acuerdo con la definición de computación en la nube del NIST hay tres tipos de servicios: infraestructura como servicio, -plataforma como servicio y software como servicio.

Cuando se habla de infraestructura como servicio el cliente controla las aplicaciones, middleware, base de datos, sistema operativo. Es como alquilar una máquina que tiene el proveedor y se trabaja en una máquina virtualizada. En este modelo el riesgo es la disponibilidad.

En el modelo de plataforma como servicio el cliente sólo controla la aplicación y el resto lo controla totalmente el proveedor. Los elementos claves son la disponibilidad y el control de acceso; a través de las aplicaciones se tiene acceso directo a los datos.

Cada modelo tiene su impacto en la protección de datos. En el primero, éste está relacionado con las prácticas del proveedor y el cliente. En el segundo modelo el proveedor se vuelve más importante, por lo que la seguridad de la información es un elemento crítico del mismo.

Finalmente en el modelo software como servicio, que es el modelo que muchas organizaciones eligen, el cliente controla los datos. Así, al controlar todo el proveedor, se puede otorgar mayor agilidad en el manejo. Pero el problema en este modelo es que como toda la infraestructura es alquilada, cuando termina el contrato hay que analizar cómo se entregan los datos y qué sucede con los datos remanentes que quedaron en la infraestructura.

Si se quieren analizar los riesgos de la nube, se puede tomar una pirámide cuya base es la disponibilidad, cuando se asegura ésta, hay que tener en cuenta el control de acceso que es la seguridad, luego se considera la calidad de la información y por último la agilidad. Esta última sólo se consigue si se dan los tres elementos anteriores.

En el caso que de la recepción de denuncias que impliquen actividades en la nube, se establece que Cloud Security Alliance está trabajando para lograr un criterio homogéneo para certificar proveedores, que deben contar con elementos que permitan apoyar a las autoridades nacionales e internacionales.

Analizando los retos del análisis forense en la nube, se debe indicar que éstos presentan tres dimensiones: técnica, organizacional y legal. En la dimensión organizacional se verifica la existencia de múltiples proveedores que deben relacionarse entre sí. En la dimensión técnica el problema de la nube es que no es posible conocer dónde está el equipo, no se sabe en qué momento se movieron los datos. El problema central es desarrollar un procedimiento estándar que sea reconocido en todos los países. La dimensión legal implica múltiples jurisdicciones, propietarios, tenencias y acuerdos de servicios.

En relación con la protección de datos en la nube hay una Directiva de la Unión Europea del 5 de mayo de 2012 que maneja dos claves: pérdida de control y pérdida de transparencia. El tema crítico de la nube es la seguridad, por lo que se considera que a mayor transparencia de los proveedores, mayor confianza de los clientes.

La pérdida de transparencia se produce porque hay muchos contratistas,

muchas locaciones geográficas y transferencias internacionales no consentidas. La pérdida de control refiere a la integridad, la disponibilidad y la confidencialidad. Para ello CEB Executive Board presenta un programa guía para cumplir con la protección de datos.

En este sentido, habría que revisar los estatutos de la organización, identificar las fuentes potenciales de responsabilidad, aplicar políticas de valoración de riesgos, diseñar controles y por último procesos de auditoría.

En la dimensión técnica debe existir un servicio forense del proveedor, el que debe ser auditado con una infraestructura especializada para poder proceder en ese sentido.

En la dimensión legal está el marco de la protección de datos.

Monique Altheim expresa que se ha puesto de manifiesto el uso de herramientas forenses en la nube para los negocios, sin embargo estos elementos son usados por agencias gubernamentales para combatir el crimen. Las investigaciones se pueden realizar de forma remota. Ahora bien, la policía no puede entrar en una casa sin una orden, pero tampoco puede entrar en una computadora sin una orden y esto las personas no lo saben y por otra parte, no es fácil acceder a esa orden.

Oscar Puccinelli, Argentina

Dentro de los posibles esquemas jurisdiccionales a considerar, esta temática se plantea en aquel esquema legal de multiplicidad de jurisdicciones. El problema se verifica en la faz práctica de aplicación de derechos que están reconocidos en el tratamiento de datos en la nube.

En consecuencia, para resolver esta temática se considera que deberían existir menos normas, más claras y que, además, no se superpongan o sean contradictorias. Es necesario ubicar las situaciones en el plano material de las responsabilidades.

Resolver estas asimetrías requiere de más principios generales, considerándose que una herramienta particularmente eficaz es el habeas data. También se requiere mayor independencia de los órganos de control de protección de datos y de acceso a la información pública, así como más participación ciudadana en el control.

Asimismo, es necesario avanzar en más cooperación global y regional, dado que los acuerdos regionales llevan a una solución global. En la medida que se observa y considera a la nube como una solución casi perfecta a los problemas informáticos de usuarios, proveedores y gobiernos, es necesario que los proveedores de software colaboren con la privacidad desde el diseño.

Se verifican nuevos riesgos generados por las nuevas herramientas; el problema es que desde el punto de vista jurídico, existen rezagos.

En Santa Fe se aprobó una Ley de “registro no llame”, pero probablemente pronto los teléfonos incluyan los metadatos necesarios para no tener que registrarlos, siendo la exclusión por defecto.

El marco jurídico está provisto por normas legales limitadas en el ámbito geográfico, temporal y las limitaciones de recursos humanos.

Los problemas de la investigación forense actual son: la adquisición de datos es más costosa, la cadena de custodia es más compleja, es imprescindible la cooperación de los proveedores de servicios en la nube, las herramientas forenses no son adecuadas para analizar datos en la nube y existen dificultades de acceso a las distintas jurisdicciones.

Las jurisdicciones deben balancear las necesidades de los usuarios con las de los proveedores de servicios. Los usuarios reclaman que los proveedores sean previsibles y tengan normativa uniforme. Muchos gobiernos colocan datos personales en la nube y eso tiene que ser objeto de regulación.

El problema, en definitiva, es que primero hay acciones judiciales contra

determinado programa y luego se da la reacción legislativa y esta legislación pronto queda obsoleta. Hoy en día, tanto la Directiva 95/46 como el Convenio 108 están en plena revisión porque son parcialmente efectivos. Los mayores avances a nivel legal se dan en los países tecnológicamente más avanzados.

En Latinoamérica todavía no se ha aprobado una convención sobre protección de datos, aunque hubo iniciativas. Es deseable que la Corte Interamericana instara a los países a implementar regulación en materia de protección de datos y de acceso a la información pública.

En Europa se aprobó una Convención sobre cibercrimen adoptada en Budapest en 2001 y se aplica también a Estados Unidos; la idea es unificar los tipos penales y las reglas procesales. Existen varias herramientas de cooperación en materia de cibercrimen que están dando sus frutos, pero pocos países forman parte.

Si bien la “Patriot Act” de 2001 es muy cuestionada, otros países como Australia, Alemania, Canadá, Dinamarca, Francia, Irlanda, Japón, España y Reino Unido tienen normas similares. Incluso en Alemania la agencia de investigación criminal puede instalar un “troyano federal” en los casos que involucren terrorismo o seguridad nacional, sin conocimiento del monitoreado y sin orden judicial.

En Latinoamérica una herramienta eficaz es el habeas data, una acción de garantía procesal constitucional, nacida en la Constitución de 1988 de Brasil. Generalmente el órgano de control tiene limitaciones presupuestales, por eso esta herramienta es usada por los particulares que concurren a la justicia para la protección de datos.