

CONSIDERACIONES FORENSES EN LA BANCA ELECTRÓNICA

Fuente: http://www.bormart.es/articulo_redseguridad.php?id=1234

De acuerdo con investigaciones recientes (“Análisis de tendencias en seguridad informática. Algunos referentes internacionales para revisar”, 2006, http://www.acis.org.co/fileadmin/Revista_96/investigacion.pdf), la seguridad de la información es un reto cada vez más complejo para las organizaciones. Grandes inversiones, largas horas de ajustes y monitoreo permanente son las características más sobresalientes de las empresas que gestionan, día a día, la seguridad informática. Sin embargo, el crecimiento de los fallos de seguridad, intrusiones y vulnerabilidades superan las expectativas de los encargados de la seguridad informática en las organizaciones.

Ante esta realidad, las organizaciones deben procurar la administración de la inseguridad de la información (<http://www.virusprot.com/Art47.html>), formulando umbrales de confianza que conforme a los recursos, características y negocios de las organizaciones, puedan estructurarse alrededor de la administración de riesgos establecida por la empresa. En este sentido, no es posible tener seguridad total, pues riesgo cero no existe.

Informática forense y banca ‘on-line’

En la banca electrónica el panorama no es diferente. La inseguridad de las infraestructuras de operación actuales establece un reto para la administración de la inseguridad pues la exposición permanente de dicha infraestructura, a diferentes ataques y fallos, exige de los encargados aprender y desaprender cada vez más, no para conocer cómo llevar los sistemas a mayores niveles de seguridad, sino para reconocer en las vulnerabilidades la forma de cómo el sistema falla y mejorar los umbrales confianza en los mismos.

Si la inseguridad es la constante en el mundo real e informático, la atención de incidentes debería ser la norma. En este sentido, los sistemas de información deberían ser diseñados y medidos en cuanto a la resistencia que tienen para enfrentar fallos y vulnerabilidades. En los términos que Bruce Schneier utiliza en su libro *Beyond fear. Thinking sensibly about security in an uncertain world* (página 51):

❖ ¿Cómo funciona el sistema?

❖ ¿Cómo no funciona el sistema?

❖ ¿Cómo reacciona ante un fallo o situación inesperada?

❖ ¿Cómo hacerlo fallar?

En este contexto, las aplicaciones, los dispositivos de hardware y las acciones de los usuarios son susceptibles de acciones que atenten contra la integridad, la disponibilidad y la confidencialidad de la información. Por tanto, la atención de incidentes debe ser la constante en todas las organizaciones, como la forma ordenada y coordinada para hacerle frente a la inseguridad. De manera complementaria aparece la computación forense o informática forense (http://www.acis.org.co/fileadmin/Revista_96/dos.pdf) como la disciplina técnico-legal, que procura el esclarecimiento de lo que ocurrió,

recabando las evidencias necesarias para explicar que ha pasado en una situación específica.

De acuerdo con recientes estudios realizados por organismos internacionales (nueva edición del CSI/FBI Computer Crime and Security Survey, disponible en <http://www.hispasec.com/corporate/noticias/110>), los sitios web, los virus y las vulnerabilidades son las fuentes y objetivos de los más importantes ataques actualmente en las organizaciones. Si esto es cierto, los sistemas que soportan la banca electrónica no son la excepción en esta tendencia. Por tanto, los ejercicios de administración de riesgos, pruebas de vulnerabilidades y aseguramiento de infraestructuras de cómputo deben ser la constante dentro de la gestión de seguridad de la información.

La banca electrónica, como la tendencia natural de la actividad bancaria en un mundo interconectado, debe afinar sus actividades para mantenerse preparada ante lo inesperado y los fallos propios de la inseguridad de la información, contando con profesionales entrenados en atención de incidentes e investigadores en informática forense, como la manera de enviarle un mensaje a todos sus clientes, donde se manifiesta que, a pesar de que los sistemas son susceptibles a vulnerabilidades y fallos, la organización está preparada para responder, perseguir y procesar a todos aquellos que atentan contra su infraestructura.

De igual forma, los usuarios y clientes de la banca electrónica, tienen un compromiso con ésta, como parte fundamental de la función de seguridad de la información. El cliente como primer custodio y “mecanismo de defensa” del sistema, debe notificar y apoyar a la banca electrónica para visualizar los posibles puntos de fallo que los encargados del tema no han identificado previamente. Es decir, debe establecerse una retroalimentación y comunicación de doble vía que permita tanto a los usuarios como a los encargados de la seguridad mantener el nivel de confianza requerido para operar y mantener los elementos propios de la banca electrónica.

Evidencia digital

Una vez se consuma un fallo, un delito o una conducta punible en el contexto de la banca electrónica, se hace necesario adelantar una investigación que permita determinar qué ha sucedido y las acciones correspondientes. Para adelantar estas diligencias técnicas y jurídicas, la evidencia digital es factor fundamental que sustenta las conclusiones que sobre el evento analizado se establezcan.

Por tanto, los investigadores forenses, utilizando las técnicas y los procedimientos autorizados, profundizan en la recuperación y análisis de la información disponible en los sistemas de archivo de las máquinas, el tráfico de red, los archivos de configuración, los diferentes medios de almacenamiento, entre otros, con el fin de identificar la evidencia relevante a los hechos analizados.

Sin embargo, se plantean una serie de retos tanto para los investigadores como para sus procedimientos cuando de evidencia digital se trata.

Buenas prácticas

A continuación algunas consideraciones sobre la evidencia digital que se deben revisar para contar con pruebas electrónicas más veraces y confiables las cuales puedan ser sopesadas y contrastadas ante un tribunal. Para ello, se detallan a continuación algunas buenas prácticas para la administración de la evidencia digital (<http://gecti.uniandes.edu.co/documentos.html>).

- ✗ Clasificar la información de la organización, de tal forma que se pueda establecer cuál es la evidencia más relevante y formal que se tiene. Para ello, las oficinas de archivo o documentación en conjunto con el área de tecnología deben adelantar un estudio de las características de la información que soporta decisiones administrativas y sus medidas tecnológicas de protección, almacenamiento y recuperación posterior.
- ✗ Determinar los tiempos de retención de documentos electrónicos, la transformación de éstos (cambios de formato) y la disposición final de los mismos.
- ✗ Diseñar los registros de auditoría de las aplicaciones, como parte fundamental de la fase de diseño de la aplicación. Este diseño debe considerar la completitud y el nivel de detalle (granularidad) de los registros.
- ✗ Utilizar medidas tecnológicas de seguridad informática para validar la autenticidad e integridad de los registros electrónicos. Tecnologías como certificados digitales, token criptográficos, entre otras, podrían ser candidatas en esta práctica.
- ✗ Asegurar la sincronización de las máquinas o dispositivos que generen la información, de tal manera que se pueda identificar con claridad la fecha y hora de los registros electrónicos.
- ✗ Contar con pruebas y auditorías frecuentes alrededor de la confiabilidad de los registros y su completitud, frente al diseño previo de los registros electrónicos.
- ✗ Diseñar y mantener un control de integridad de los registros electrónicos, que permita identificar cambios que se hayan presentado en ellos.
- ✗ Asegurar el área donde ocurrió el siniestro, con el fin de custodiar el área o escena del delito y así fortalecer la cadena de custodia y recolección de la evidencia.
- ✗ Registrar en medio fotográfico o video la escena del posible ilícito, detallando los elementos informáticos allí involucrados.
- ✗ Levantar un mapa o diagrama de conexiones de los elementos informáticos involucrados, los cuales deberán ser parte del reporte del levantamiento de información en la escena del posible ilícito.
- ✗ Validar y verificar la confiabilidad y limitaciones de las herramientas de hardware y software utilizadas para adelantar los análisis de los datos.
- ✗ Establecer el rango de tiempo de análisis y correlacionar los eventos en el contexto de los registros electrónicos recolectados y validados previamente.
- ✗ Mantener una copia de la cadena de custodia y de la notificación oficial para adelantar el análisis de los registros electrónicos.
- ✗ Incluir las irregularidades encontradas o cualquier acción que pudiese ser irregular durante el análisis de la evidencia.
- ✗ Preparar una presentación del caso de manera pedagógica, que permita a las partes

observar claramente el contexto del caso y las evidencias identificadas.

✗Detallar las conclusiones de los análisis realizados sustentados en los hechos identificados. Evitar los juicios de valor o afirmaciones no verificables.

✗Verificar y validar con pruebas que los resultados obtenidos luego de efectuar el análisis de los datos, son repetibles y verificables por un tercero especializado.

✗Auditar periódicamente los procedimientos de recolección y análisis de registros electrónicos, de tal manera que se procure cada vez mayor formalidad y detalles en los análisis efectuados.

✗Procurar certificaciones profesionales y corporativas en temas relacionados con computación forense, no como signos distintivos de la experiencia de la organización en el área, sino como una manera de validar la constante revisión y actualización del tema y sus mejores prácticas.

✗Si al preparar un reporte de un análisis de datos, considera que puede estar incompleto o no cuenta con las calificaciones y condiciones requeridas para efectuarlo, debe documentarlo en el informe o manifestar esta condición a la parte que ha solicitado sus servicios.

Reflexiones finales

La banca electrónica, en el contexto actual, debe ajustarse a la dinámica de los negocios y de las tecnologías de la información, no como una actualización permanente de mecanismos de seguridad, sino como una manera de repensar las relaciones con sus clientes, con los proveedores y con sus procesos internos de operación.

La inseguridad es una realidad que implica un cambio de estrategia en la administración de la seguridad. Un cambio que implica estar preparado para enfrentar los incidentes o imprevistos que son la constante en un mundo interconectado. Este cambio requiere una transformación cultural al interior de la banca electrónica, que implica reconocer: el nivel de inseguridad que se debe manejar, cómo los usuarios hacen parte de la cadena de protección, cómo los investigadores deben realizar su trabajo e identificar la evidencia relevante.

La computación forense en la banca electrónica es una disciplina auxiliar que le permite a la banca aumentar la formalidad de su operación y la confianza en sus clientes, pues saben que existe personal cualificado y entrenado para desarrollar investigaciones que develen la verdad sobre los posibles hechos “sospechosos” que sucedieron en las operaciones realizadas en línea.

La computación forense es una respuesta natural a las preguntas que todos los usuarios tienen cuando eventos no esperados suceden, una manera técnica-legal de afrontar las investigaciones, una forma de responder y comprender la inseguridad propia de la banca electrónica

Jeimy J. Cano

**Miembro investigador del Grupo de Estudios en Comercio Electrónico,
Telecomunicaciones e Informática (GECTI) de
la Universidad de los Andes (Colombia)**