Procedimientos en el lugar de los hechos: "el primero en responder" en la informática forense

"La respuesta más rápida es la acción".
Proverbio americano

David Eduardo Acosta, CISSP, CISM, CISA, OPST, CCNA Security, CHFI Instructor, BS25999 Lead Auditor, PCI QSA
Consultor en Seguridad de la Información

El 11 de Septiembre de 2001 fue una fecha que marcó para siempre la historia de EE.UU. y su impacto sigue latente en el mundo entero, ahora que se conmemora su décimo aniversario. En esa fecha, los bomberos de Nueva York reaccionaron de forma inmediata y se convirtieron en los héroes del suceso. A pesar de las pérdidas humanas, su acción inmediata fue contundente para evitar que el daño hubiera sido peor. Su trabajo fue sistemático y dirigido por entrenamientos previos, lo cual les permitió actuar de forma eficaz ante este incidente.

No tenemos que irnos tan lejos para ver cómo una acción rápida y eficiente posterior a una notificación puede salvar vidas: los paramédicos, los cuerpos de policía, las brigadas de apoyo civil, los militares, etc. son ejemplos claros de cómo se debe atender una emergencia. Cuando presenciamos un accidente o alguien se enferma en casa, por lo general, sabemos a quién llamar y tenemos en nuestra agenda telefónica datos de contacto en caso de problemas, con lo cual –en cierta forma– estamos preparados para actuar ante una potencial eventualidad.

Sin embargo, en el ámbito informático de una organización, esta preparación no siempre es la norma. Si se reporta una intrusión en los servidores, un robo de información clasificada, se detecta la presencia de una botnet o se está bajo un ataque de denegación de servicio, ¿realmente sabemos cómo actuar en ese momento, cómo determinar la severidad del incidente, cómo recolectar información para un análisis posterior y cómo conservar la evidencia siendo lo menos intrusivos posible? Y más importante aún: ¿sabemos hacerlo manteniendo la validez legal de las evidencias capturadas?

Este artículo describirá de forma general la figura del ***primero en responder*** ("first responder" en inglés) como elemento clave para desencadenar todo el procedimiento de respuesta a incidentes en una organización y su papel fundamental en la gestión de la cadena de custodia.

El rol del *Primero en Responder* en la gestión de incidentes

Un incidente de seguridad informática se puede definir como cualquier evento adverso en un entorno informático, que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información. Obviamente, ante cualquier acción siempre existirá una reacción y la reacción ideal en este caso consiste en la realización de una serie de pasos metodológicos: detectar, notificar, analizar, contener, erradicar, recuperar e investigar dicho incidente.

En cada una de estas fases pueden intervenir múltiples actores, desde el individuo que identifica un comportamiento sospechoso hasta aquel que realiza una investigación forense y presenta las evidencias ante una corte, en caso de ser necesario. Sin embargo, la garantía que toda la cadena sea efectiva desde el momento de la notificación recae en el primero en responder. Este rol, generalmente, es cubierto por la primera persona notificada, quien debe ser el primero en reaccionar ante dicha eventualidad. En muchos casos, puede ser un administrador de sistemas o un administrador de red, que debe contar con conocimientos y formación previa para poder gestionar eficientemente el incidente y determinar su causa raíz. La importancia de las labores del primero en responder radican en que, en muchos casos, sólo se tiene una oportunidad para realizar el proceso de atención al incidente y que, generalmente, los errores en esta fase son irreversibles. Es por ello que la persona que realice la primera respuesta debe contar con el conocimiento y las herramientas necesarias para poder gestionar de forma efectiva y eficiente el incidente, respetando siempre el escenario en el cual se presentó el suceso y obteniendo una evidencia que permita una investigación sin contratiempos, al mismo tiempo que intenta contener el impacto potencial del daño.

Dado que un incidente se puede presentar en cualquier momento, es importante que todo el personal de TI se encuentre formado y cuente con las herramientas necesarias para poder responder, independientemente que se trate de un incidente menor o de una investigación que pueda conllevar la intervención de las autoridades, de la forma adecuada. Puede presentarse el caso que la persona que detecte el incidente sea el mismo que realice la primera respuesta, con lo cual es importante que el personal técnico y administrativo de la organización sean parte de la cadena de respuesta a incidentes e informática forense.

Acciones a ejecutar en la primera respuesta

Uno de los principales enemigos en la respuesta a incidentes es el tiempo. Dada la volatilidad de la información y la fragilidad de la potencial evidencia (que puede ser fácilmente alterada, dañada o destruida), la acción inmediata es un factor clave en el proceso. Desde el momento de la notificación del incidente, las labores a realizar por el primero en responder (teniendo en cuenta que el tiempo corre en su contra) serán:

- Identificar la ubicación física y lógica del incidente, con el fin de securizar el entorno y minimizar cualquier potencial contaminación, así como aislar otros posibles elementos en la frontera que se puedan ver afectados.
- Identificar el problema aparente, intentando clasificarlo y perfilarlo con el fin de definir una estrategia de atención específica.
- Tratar de determinar los posibles actores involucrados.
- Entrevistar a los usuarios.
- Definir las herramientas a utilizar, en función del tipo de activos afectados.
- Obtención de evidencia e inicio del proceso de cadena de custodia.
- Establecer comunicación con otras áreas involucradas en el incidente para que activen sus planes de acción.

La figura del "primero en responder" es el elemento clave para desencadenar todo el procedimiento de respuesta a incidentes en una organización y para la gestión de la cadena de custodia.

- Entregar la evidencia obtenida bajo la cadena de custodia y documentar todo el procedimiento y sus actuaciones.

Como se puede concluir, de una ejecución metódica de los anteriores pasos se desprenderá una investigación satisfactoria.

Errores comunes en la primera respuesta

La respuesta a incidentes tecnológicos y la investigación informática forense son un trabajo que debe ser realizado por un equipo entrenado y equipado. Un equipo de investigación sin experiencia puede destruir la evidencia o modificarla haciéndola inadmisible ante una investigación o un juicio, con lo cual se reduce de forma drástica la posibilidad de una acción judicial o disciplinaria satisfactoria. Inclusive, se puede presentar el caso que la evidencia recolectada de forma no adecuada se pueda volver en contra de la organización y se preste para falsas acusaciones, contrademandas o impunidad.

Para evitar estos problemas, se deben evitar las siguientes acciones:

- Apagar o reiniciar el equipo: éste es el dilema del primero en responder. Cuando esto sucede, toda la información volátil se pierde: conexiones, estado de procesos y tiempos en los ficheros son modificados. Como norma, se recomienda aplicar la siguiente premisa: "Si está apagado, déjelo apagado. Si está encendido, déjelo encendido".
- Asumir que el equipo sospechoso es un entorno no confiable: siem-

Las acciones del "primero en responder" deben estar enmarcadas dentro de un programa global de gestión de incidentes de seguridad de la organización, dentro del cual deben existir roles y responsabilidades definidos.

pre se debe desconfiar de comandos del sistema y de la información facilitada por éstos en los equipos relacionados con el incidente y se debe evitar ejecutar programas que puedan modificar la integridad de la evidencia.

- Excluir evidencia: dado que el proceso de análisis es posterior a la obtención de evidencia, el primero en responder aún no cuenta con criterio suficiente para descartar potencial evidencia. Es por ello que se debe obtener y securizar la evidencia necesaria con base en la información obtenida hasta el momento.

El principio básico en toda acción del primero en responder es proteger la evidencia original y ser lo menos intrusivo posible. Muchas veces es mejor pedir soporte a algún experto que arriesgarse a improvisar con los procedimientos.

La caja de herramientas del primero en responder

Adicional a la formación y entrenamiento en respuesta a incidentes, el primer respondiente debe contar con una serie de herramientas que le permitan actuar de forma rápida y específica sobre cualquier activo sospechoso y securizar el escenario en el que se está desarrollando el incidente.

Dentro de estas herramientas y logística se encuentran (entre otros):

- Herramientas lógicas certificadas, legalizadas y reconocidas para la captura de información volátil y persistente en los activos sospechosos, teniendo en cuenta las diferentes plataformas operativas y equipos presentes en la red. Contar que no sólo los ordenadores y servidores pueden contener evidencia. Teléfonos móviles, dispositivos activos de red, reproductores de música, cámaras fotográficas, consolas de juegos, impresoras, fax, etc. pueden estar vinculados con el incidente y se debe contar con instrumentos para extraer dicha evidencia.
- Herramientas para la duplicación de evidencia.
- Dispositivos de almacenamiento masivo esterilizados (que no contengan datos remanentes de usos anteriores que puedan contaminar la evidencia a almacenar).
- Etiquetas, bolsas antiestáticas y cintas para embalar y proteger la evidencia y marcarla.
- Destornilladores, pinzas, cables, conectores y otros periféricos que puedan ser necesarios.
- Cámaras fotográficas o de videograbación, con el fin de obtener evidencia del estado físico del escenario del incidente.

En función de la experiencia y conocimiento del primero en responder, se puede ampliar este conjunto con herramientas básicas de análisis e investigación, teniendo presente que dichas acciones podrían llegar a modificar la evidencia original.

Siguientes pasos

Obtenida la evidencia y securizado el entorno afectado se debe proceder con las siguientes fases de la gestión de incidentes: erradicación, recuperación y retroalimentación (lecciones aprendidas) de forma paralela con el análisis forense, si se llegase a necesitar. Puede ser probable que la misma persona que fuera el primero en responder sea quien deba analizar la evidencia con el fin de desechar o comprobar hipótesis sobre el incidente y vincular a los actores involucrados, pero la recomendación es que siempre se actúe con la mentalidad que será un tercero quien deba analizar e interpretar esta evidencia, lo cual facilitará el proceso de redacción y descripción de todas las acciones realizadas y el enlace entre los componentes de la evidencia para que exista una congruencia entre todas las partes.

Palabras finales

Claramente, la actuación metodológica de una primera respuesta en la atención de incidentes (y no solamente incidentes informáticos) garantizará que el resto de actividades se desarrollen de forma correcta y se obtenga una conclusión válida que permita tomar una decisión como respuesta al suceso analizado.

Algunos consejos finales al primero en responder:

- Proteger la continuidad del negocio. A pesar del incidente, la organización debe continuar operando.
- Tenga siempre presente que sus acciones tendrán un impacto sobre el resto de etapas del proceso de gestión de incidentes.
- Guardar la calma. Las acciones racionales deben primar sobre las acciones emocionales. A pesar que el tiempo está en su contra, la experiencia y la formación previa son factores diferenciales para controlar el estrés.
- Pruebe de forma periódica sus conocimientos y habilidades. Defina "juegos de guerra" o escenarios hostiles hipotéticos ante los cuales haya que responder y revise las estrategias que se tomarían ante tal situación. Documente el proceso y retroalimente la metodología con los resultados.
- Mantenga actualizado y disponible el kit de herramientas y logística en caso de que ocurra un incidente.

Las acciones del primero en responder deben estar enmarcadas dentro de un programa global de gestión de incidentes de seguridad de la organización, dentro del cual deben existir roles y responsabilidades definidos. La acción conjunta y coordinada de cada componente garantiza que la actividad se desarrolle de forma satisfactoria y afecte lo menos posible al negocio.