UNIDAD 3

INVESTIGACIÓN DE INCIDENTES DE CIBERSEGURIDAD

Se conoce como gestión de incidentes de seguridad de la información a un conjunto ordenado de acciones enfocadas a prevenir, en la medida de lo posible, la ocurrencia de ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible. El proceso de gestión de incidentes consta de diferentes fases y, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea.

RECOPILACIÓN DE EVIDENCIAS

Una vez que se han tomado las medidas iniciales para contener el problema, cuidando de no destruir información valiosa, es momento de comenzar con los procedimientos de toma y preservación de evidencias. Este paso resulta importante, tanto por si finalmente es necesario judicializar el incidente, como para poder analizar correctamente el origen y determinar el impacto real del problema.

Los aspectos más importantes a tener en cuenta durante este proceso aparecen estandarizados en la RFC 3227[1]. Estos son los puntos más importantes relacionados con dicho proceso:

Principios durante la recolección de evidencias

- Capturar una imagen del sistema tan precisa como sea posible.

[1] https://tools.ietf.org/html/rfc3227

- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad (de mayor a menor).
- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.
- Orden de volatilidad El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información. Es por ello que se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.
  De acuerdo a esta escala se puede crear la siguiente lista en orden de mayor a menor volatilidad:
  - Registros y contenido de la caché.
  - Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
  - Información temporal del sistema.
  - Disco
  - Logs del sistema.
  - Configuración física y topología de la red.
  - Documentos.
- Acciones que deben evitarse Se deben evitar las siguientes acciones con el fin de no invalidar el proceso de recolección de información ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan ser utilizados en un juicio en el caso de que sea necesario:
  - No apagar el ordenador hasta que se haya recopilado toda la información.

- No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido.
- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

- Consideraciones sobre la privacidad
  - Es muy importante tener en consideración las pautas de la empresa en lo que a privacidad se refiere. Es habitual solicitar una autorización por escrito de quien corresponda para poder llevar a cabo la recolección de evidencias. Este es un aspecto fundamental ya que puede darse el caso de que se trabaje con información confidencial o de vital importancia para la empresa, o que la disponibilidad de los servicios se vea afectada.
  - No hay que entrometerse en la privacidad de las personas sin una justificación. No se deben recopilar datos de lugares a los que normalmente no hay razón para acceder, como ficheros personales, a menos que haya suficientes indicios.

Procedimiento de recolección

El procedimiento de recolección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

- Transparencia Los métodos utilizados para recolectar evidencias deben de ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido testados por expertos independientes.
- Pasos
  - ¿Dónde está la evidencia? Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.
  - Establecer qué es relevante. En caso de duda es mejor recopilar mucha información que poca.
  - Fijar el orden de volatilidad para cada sistema.
  - Obtener la información de acuerdo al orden establecido.
  - Comprobar el grado de sincronización del reloj del sistema.

  - Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.
  - Documentar cada paso.
  - No olvidar a la gente involucrada. Tomar notas sobre qué gente estaba allí, qué estaban haciendo, qué observaron y cómo reaccionaron.

El procedimiento de almacenamiento

- Cadena de custodia Debe estar claramente documentada y se deben detallar los siguientes puntos:
  - ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
  - ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
  - ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?
  - En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el intercambio, incluyendo número de albarán, etc.
- Dónde y cómo almacenarlo Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.

Herramientas necesarias

Existen una serie de pautas que deben de ser seguidas a la hora de seleccionar las herramientas con las que se va a llevar a cabo el proceso de recolección:

- Se deben utilizar herramientas ajenas al sistema ya que éstas pueden haberse visto comprometidas, principalmente en los casos de malware.
- Se debe procurar utilizar herramientas que alteren lo menos posible el escenario, evitando el uso de herramientas de interfaz gráfico y aquellas cuyo uso de memoria sea grande.
- Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un dispositivo de sólo lectura (CDROM, USB, etc.).
- Se debe preparar un conjunto de utilidades adecuadas a los sistemas operativos con los que se trabaje.

- El kit de análisis debe incluir los siguientes tipos de herramientas:
    - Programas para listar y examinar procesos.
    - Programas para examinar el estado del sistema.
    - Programas para realizar copias bit a bit.

A la hora de enfrentarse a un incidente de seguridad hay que tener muy claro las acciones que se deben realizar, siendo muy meticuloso y detallando en todo momento dicho proceso de manera minuciosa. Así mismo, se debe realizar el proceso procurando ser lo menos intrusivo posible con el fin de preservar el sistema en su estado original, y siguiendo las pautas indicadas en alguna de las metodologías o guías anteriormente indicadas o similares.

Finalmente, se debe tener presente que los requisitos o pautas a seguir a la hora de realizar un análisis forense digital que vaya a derivar en un proceso legal varían dependiendo del país, ya que no existe una legislación común. De todas formas, se debe tender a seguir las indicaciones establecidas en alguna metodología como el RFC 3227 con el fin de que dicho proceso sea realizado de una manera rigurosa.