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 durnate este proceso aparecene 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 como se explicará más adelante.
- 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.

ANÁLISIS DE EVIDENCIAS

La fase de análisis no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder proceder a elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrontarse al incidente. Como ya se ha explicado nunca se debe trabajar con datos originales y se debe respetar cada una de las

leyes vigentes en la jurisdicción donde se lleve a cabo la investigación. Los resultados que se obtengan de todo el proceso han de ser verificables y reproducibles, así que en cualquier momento debemos poder montar un entorno donde reproducir la investigación y mostrarlo

a quién lo requiera. Es importante también disponer de una documentación adicional con información de diversa índole, por ejemplo:

- Sistema operativo del sistema.
- Programas instalados en el equipo.
- Hardware, accesorios y periféricos que forman parte del sistema.
- Datos relativos a la conectividad del equipo:

o Si dispone de firewall, ya sea físico o lógico.

o Si el equipo se encuentra en zonas de red especiales, por ejemplo, DMZ. o Si tiene conexión a Internet o utiliza proxies.

- Datos generales de configuración que puedan ser de interés para el investigador para ayudar en la tarea.

Para ayudar al desarrollo de esta fase del análisis forense podemos centrarnos en varias subfases o puntos importantes que generalmente siempre deben realizarse. Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuentas las diversas particularidades que nos podamos encontrar. No será lo mismo analizar un equipo con sistema operativo Windows o con Linux. Tampoco será lo mismo un caso de intrusión en el correo electrónico de alguien o un ataque de denegación de servicio a una institución. De igual forma no actuaremos con los mismos pasos en un caso de instalación de un malware que destruya información de una ubicación de disco o un malware que envíe todo lo que se teclea en un equipo.

En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

Preparar un entorno de trabajo

Antes de empezar el análisis propiamente, se debe preparar un entorno para dicho análisis. Es el momento de decidir si se va a hacer un análisis en caliente o en frío.

En caso de un análisis en caliente se hará la investigación sobre los discos originales, lo que conlleva ciertos riesgos. Hay que tomar la precaución de poner el disco en modo sólo lectura, esta opción sólo está disponible en sistemas operativos Linux pero no en Windows. Si se opta por esta opción hay que operar con sumo cuidado pues cualquier error puede ser fatal y dar al traste con todo el proceso, invalidando las pruebas.

Si se opta por un análisis en frío, lo más sencillo es preparar una máquina virtual con el mismo sistema operativo del equipo afectado y montar una imagen del disco. Para ello previamente habremos creado la imagen a partir de las copias que se hicieron para el análisis. En este caso podremos trabajar con la imagen, ejecutar archivos y realizar otras tareas sin tanto cuidado, pues siempre cabe la opción de volver a montar la imagen desde cero en caso de problemas.

La opción del análisis en frío resulta muy atractiva pues en caso de malwares se podrán ejecutar sin miedo, reproducir lo que ocurre y desmontar la imagen sin que la copia original resulte afectada. De este modo tal vez se pueda ir un poco más allá en la investigación y ser un poco más agresivo.

Existen varios programas gratuitos para crear y gestionar máquinas virtuales, eación de la línea temporal

Sea cual sea el tipo de análisis que se va a llevar a cabo, el primer paso suele ser crear una línea temporal dónde ubicar los acontecimientos que han tenido lugar en el equipo desde su primera instalación.

Para crear la línea temporal, lo más sencillo es referirnos a los tiempos MACD de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen por qué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.

Para empezar, lo mejor es determinar la fecha de instalación del sistema operativo, para ello se puede buscar en los datos de registro. Además la mayoría de ficheros del sistema compartirán esa fecha. A partir de aquí puede ser interesante ver qué usuarios se crearon al principio, para ver si hay discrepancias o usuarios fuera de lo común en últimos instantes del equipo. Para ver esta información también es útil acudir al registro del sistema operativo.

Teniendo ya los datos iniciales del sistema, ahora se puede proceder a buscar más información en los ficheros que se ven “a simple vista”. Lo importante es localizar que programas fueron los últimos en ser instalados y qué cambios repercutieron en el sistema. Lo más habitual es que estos programas no se instalen en los lugares habituales, sino que se localicen en rutas poco habituales, por ejemplo en archivos temporales o mezclados con los archivos y librerías del sistema operativo. Aquí se puede ir creando la línea temporal con esos datos.

Alternativamente es útil pensar que no todos los archivos están a la vista. Se puede encontrar información en archivos normales, pero también en temporales, ocultos, borrados o usando técnicas como la esteganografía, no se puede obviar ninguna posibilidad.

Habitualmente los sistemas operativos ofrecen la opción de visualizar los archivos ocultos y también las extensiones. Es útil activar estas opciones para detectar posibles elementos ocultos y extensiones poco habituales que nos resulten extrañas.

Para los archivos borrados se utilizaran programas especiales capaces de recuperar aquellos datos que se hayan eliminado del disco pero sobre los cuales aún no se haya sobrescrito nada. Es posible que el atacante elimine archivos o registros varios en afán de esconder lo que ha ocurrido, si estos no han sido sobrescritos se podrán recuperar y se podrán situar en la línea temporal relacionándolos con el conjunto de sucesos. Para recuperar información oculta mediante esteganografía también se deberán usar programas concretos. Es posible que el atacante ocultara información sobre otros archivos, tales como imágenes o audio para enviarlos posteriormente o tenerlos almacenados sin llamar la atención. Habitualmente hallaremos más información en ubicaciones ocultas que en los lugares más habituales.

Con todos estos datos se debería poder crear un esbozo de los puntos clave en el tiempo tales como la instalación del sistema, el borrado de determinados archivos, la instalación de los últimos programas, etcétera.

Determinar cómo se actuó

Para determinar cómo se actuó es importante llevar a cabo una investigación sobre la memoria del equipo. Es interesante realizar un volcado de memoria para la obtención de

cierta información. Con programas destinados a tal fin podremos ver que procesos se están ejecutando en el momento concreto y también aquellos que hayan sido ocultados para no levantar sospechas. Con esta información podremos saber qué ejecutables inician los procesos en ejecución y qué librerías se ven involucradas. Llegados aquí se puede proceder a realizar volcados de los ejecutables y de dichas librerías para poder analizar si contienen cadenas sospechosas o si, por lo contrario, son archivos legítimos. Sabiendo los procesos que se ejecutan y su naturaleza podemos obtener pistas de cómo se actuó para comprometer el equipo.

menudo nos deberemos fijar en procesos en ejecución aparentemente inofensivos, habituales y legítimos en los sistemas operativos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos. Para ello deberemos observar que muchas veces estos se encuentran sin un proceso padre, cuando lo más habitual es que dependan de otros. En otras ocasiones simplemente se camuflan con nombres muy parecidos a otros para pasar desapercibidos.

Ciertos programas también nos darán información sobre las cadenas del ejecutable en cuestión. Con ellas podremos ver si mutan su contenido cuando se ejecutan en memoria y cuál es su contenido. En ocasiones, cierta información de las cadenas nos puede dar pistas muy valiosas, como por ejemplo, cadenas dónde encontrar logs, o enlaces a direcciones de Internet. También nos puede dar pistas sobre el tipo de malware al que nos enfrentamos. Si por ejemplo encontramos cadenas con alfabetos o teclas concretas del teclado, es probable que nos encontremos ante un keylogger.

Finalmente, otra práctica interesante para determinar cómo se actuó es leer la secuencia de comandos escrita por consola. Para ello procederemos con el volcado de memoria y podremos obtener dicha información. De este modo podremos leer que comandos se hicieron por consola y sabremos si se ejecutó algún proceso de este modo. Debemos excluir nuestras propias instrucciones pues seguramente aparecerán los comandos del volcado de memoria que se hicieron en su momento.

3.5.4. Identificación de autores

Para poder realizar una identificación del autor o autores del incidente, otra información importante que nos puede dar el volcado de memoria son las conexiones de red abiertas y las que están preparadas para enviar o recibir datos. Con esto podremos relacionar el posible origen del ataque buscando datos como la dirección IP en Internet.

Hay que actuar con prudencia puesto que en ocasiones se utilizan técnicas para distribuir los ataques o falsear la dirección IP. Hay que ser crítico con la información que se obtiene y contrastarla correctamente. No siempre se obtendrá la respuesta al primer intento y posiblemente en ocasiones sea muy difícil averiguar el origen de un incidente.

Es interesante recapacitar en los distintos perfiles de atacantes que se pueden dar hoy día en este ámbito para intentar mimetizarse y entender quién pudo ser el autor.

Por un lado podemos encontrar organizaciones y criminales que actúan por motivaciones económicas. Su finalidad es robar cierta información, ya sea empresarial o personal, para una vez obtenida venderla o sacar un rendimiento oneroso de la información.

Por otro lado está quién sólo busca acceder a sistemas por mero prestigio y reconocimiento en su ambiente cibernético. Accediendo a sistemas mal configurados y publicando datos que prueben su fechoría incrementará su notoriedad y se dará a conocer más en las redes.

En este punto es importante analizar dos vertientes. En caso que se esté realizando un peritaje con fines inculpatorios, o sea, judiciales, se deberá intentar resolver quién es el autor o al menos aportar pistas fiables para que otros investigadores puedan llevar a cabo otras investigaciones de otros ámbitos.

En cambio, si es con fines correctivos lo más interesante seguramente será obviar esta fase y proceder con el estudio del impacto causado y estudiar las mejoras que se pueden implantar para evitar episodios similares.

INVESTIGACIÓN DEL INCIDENTE

Tras la evaluación inicial, la comunicación y la contención, tenemos que determinar qué sistemas, equipos e información han podido verse comprometidos. Esto será de utilidad para identificar los activos afectados y tomar las acciones que se consideren oportunas para valorar los daños y evitar que vuelva a suceder. En función de los activos afectados, la metodología de actuación variará y como cada caso es diferente, se debe intentar seguir las siguientes recomendaciones:

- Determinar qué tipo de ataque se ha sufrido, como puede ser un ransomware, robo de información confidencial o acceso no autorizado a la página web. En este punto, al conocer más detalle de los activos afectados, podemos darnos cuenta del alcance real del ataque y clasificarlo de forma diferente que lo hicimos en la fase inicial.
- Determinar el punto de origen o vector de ataque que se ha utilizado. Puede ser el correo electrónico corporativo, una memoria USB infectada con malware, etc.
- Identificar si el ataque ha sido dirigido en particular contra la empresa o si por el contrario, se trata de un ataque aleatorio. Los incidentes provocados por situaciones relacionadas con comunicaciones genéricas e impersonales, a través de correos electrónicos, o debidos a vulnerabilidades no parcheadas de la web corporativa, es muy probable que sean ataques aleatorios. Por el contrario, si el ataque cuenta con información personal de la víctima o sobre el software utilizado por la empresa, es muy posible que el ataque sea dirigido.
- En base al tipo de ataque sufrido y el vector utilizado, se identificarán los activos que hayan podido verse comprometido

a comunicación será una parte fundamental del proceso de respuesta. Es importante que únicamente tengan conocimiento de lo sucedido aquellas personas o departamentos que puedan ser de ayuda en la solución del mismo. La reputación de una empresa es algo que no tiene precio y una fuga de información en estos momentos podría tener consecuencias mucho más negativas que el propio incidente. Por esa razón, únicamente el personal designado a dar respuesta debe estar en conocimiento de lo sucedido. También debe nombrarse un responsable que será el encargado de coordinar la respuesta. Este coordinador, será el encargado de realizar las comunicaciones oportunas con el personal externo como proveedores, soporte técnico, Fuerzas y Cuerpos de Seguridad del Estado, Agencia Española de Protección de Datos en caso de que se hayan visto comprometidos datos personales o INCIBE-CERT a través de su servicio de respuesta a incidentes. Este tipo de comunicaciones comúnmente se realizan por medio de correo electrónico o por teléfono.

En la actualidad las empresas se encuentran en el punto de mira de los ciberdelincuentes y son un objetivo ya que, sobre todo las pymes, microempresas y autónomos en ocasiones no cuentan con las medidas adecuadas para poder repeler, gestionar y resolver un incidente de ciberseguridad. En este contexto cobra especial importancia el reporte de este tipo de problemas para interceptar a tiempo casos de fraude, nuevas tipologías de malware, fugas de información, etc.
En Protege tu empresa contamos con un equipo especializado en el análisis y gestión de incidencias de seguridad y fraude electrónico: INCIBE-CERT. Este equipo opera de forma continuada **24 horas al día, 7 días a la semana**. En INCIBE-CERT participan activamente agentes de la Oficina de Coordinación Cibernética del Ministerio del Interior, lo que permite trasladar de una forma muy ágil los casos constitutivos de delito telemático a las unidades técnicas de las Fuerzas y Cuerpos de Seguridad del Estado.
Si has tenido un incidente o has sido víctima de un caso de fraude electrónico puedes reportarlo a INCIBE-CERT a través de dirección incidencias@incibe-cert.es o mediante el formulario de contacto, detallando en el mismo la información de contacto y una descripción lo más completa posible del incidente. Recuerda que cuanta más información del incidente nos remitas, más sencillo será para nosotros gestionarla de manera efectiva. Si la incidencia contiene información sensible, te recomendamos que la envíes cifrada con PGP.

- Claves públicas PGP

Una vez reportado el incidente a través del correo indicado, nuestros técnicos de INCIBE-CERT se encargarán de evaluarlo y ofrecerte soporte para su mitigación y resolución tanto en sus aspectos técnicos como en la denuncia ante otras entidades.
¿Has sido víctima de un incidente? ¡Repórtalo! A continuación te indicamos cómo hacerlo.

- **Fraude**
- Ransomware
- Botnet
- Denuncia tu incidente

Si te has visto afectado por un caso de fraude electrónico, puedes reportarlo al equipo de respuesta a incidentes de INCIBE-CERT, **aportando**:

- Una descripción detallada del incidente y tus datos de contacto.
- El **correo sospechoso** junto con sus **cabeceras y ficheros adjuntos**.

De esta forma, el equipo de respuesta a incidentes identificará mejor tu caso y te ayudará a resolverlo. Antes de seguir cualquiera de los procedimientos recuerda que nunca debes abrir los adjuntos de un correo malicioso, pues podrían provocar la infección del equipo.

Impacto causado

El impacto causado se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que nos dé un importe económico. Aun así para estos cálculos puede servir ayudarse de métodos como BIA (Business Impact Analysis) que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

A la larga cualquier incidente ocurrido devengará en unos gastos económicos que habrá que cuantificar en función de los ítems afectados tras el suceso. En ocasiones el coste económico resultará de tener que reemplazar una máquina o dispositivo que ha quedado inservible tras un ataque o bien las horas de empleado de tener que reinstalar el sistema. En este caso, el cálculo no supone mayor dificultad y se resuelve fácilmente.

En otras ocasiones, por ejemplo, los daños pueden deberse al robo de una información de secreto industrial en el que habrá que cuantificar no sólo qué supone reponer el sistema

sino, a la larga, en qué se verá afectada la empresa. Los datos robados pueden ser para publicar cierta información sobre la empresa y poner en la opinión pública datos con intenciones de crear mala imagen, lo cual supone un daño incalculable y muy elevado para la empresa.

El impacto no sólo se puede calcular en base económica. Como ya se ha comentado al inicio de esta sección también existen otros factores, es el caso del tiempo de inactividad. Si el incidente ha supuesto paralizar la producción de una planta automatizada de fabricación esto supone muchas horas en que la producción es nula, por lo tanto no se trabajará. Evidentemente, a la larga también supondrá un problema económico pues no se podrán servir los pedidos pendientes de los clientes. Si la paralización afecta a una oficina, tal vez no se pare la producción de bienes pero sí el trabajo de los empleados que verán retrasado todo su trabajo.

Una vez concluido todo el proceso, documentado debidamente y cuando la actividad haya vuelto a la normalidad, llegará el momento de recapitular y hacerse varias preguntas:

- ¿Qué ha fallado para que se produjera el incidente?
- ¿Qué política de seguridad no ha funcionado?
- ¿Qué hay que mejorar para que no vuelva a suceder? ¿He informado a los empleados de lo que ha ocurrido? ¿Es necesario formar a los empleados para que sepan cómo actuar en estos casos?
- ¿La gestión del incidente fue correcta?
- ¿Qué pasos se pueden mejorar para hacer la gestión del incidente más fluida?
- En caso de tener que hacer el incidente público, ¿la comunicación con los medios fue correcta y fluida?
- ¿Se realizó un ejercicio de transparencia con la opinión pública o por el contrario las comunicaciones fueron opacas?
- Si el incidente afectó a información privada de clientes o proveedores, ¿se realizó la comunicación en tiempo y forma?

Gestionar un incidente de manera correcta no se reduce únicamente a restaurar los sistemas y servicios afectados o aplicar las medidas de seguridad necesarias para que no vuelva a suceder. Tan importante es recuperar la actividad cotidiana de la organización como documentar correctamente todo lo sucedido, valorar los daños o revisar las políticas de la empresa. Con estas «lecciones aprendidas» estaremos mejor preparados para detener un incidente similar.

INTERCAMBIO DE INFORMACIÓN DEL INCIDENTE CON PROVEEDORES U ORGANISMOS COMPETENTES

Con todos los datos recopilados tras un incidente tenemos que recapitular y ver qué ha pasado. Debemos informar a todos de lo que ha pasado, tomar buena nota y elaborar instrucciones precisas para que no vuelva a suceder.

La última fase de un análisis forense queda para redactar los informes que documenten los antecedentes del evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto que se ha derivado de todo el incidente.

Para ello se redactarán dos informes, a saber, el informe técnico y el ejecutivo. En esencia en ambos informes se explican los mismos hechos pero varía su enfoque y el grado de detalle con que se expone el asunto.

En el informe ejecutivo se usará un lenguaje claro y sin tecnicismos, se debe evitar usar terminología propia de la ciencia e ingeniería y expresiones confusas para gente no ducha en el tema. Hay que pensar que el público lector de estos informes serán jueces y gerentes que seguramente estén poco relacionados con el tema y además tengan poco tiempo para dedicarle. Se les debe facilitar la tarea al máximo.

En el informe técnico, por el contrario, el público final será técnico y con conocimientos de la materia que se expone. Aquí se detallarán todos los procesos, los programas utilizados, las técnicas, etcétera. Debemos crear un documento que pueda servir de guía para repetir todo el proceso que se ha realizado en caso necesario.

El informe ejecutivo

Entrando más en detalle en este tipo de informes, cabe destacar que será un resumen de toda la tarea que se ha llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, al menos comparado con el informe técnico, éste deberá contener al menos los siguientes apartados:

- Motivos de la intrusión.

o ¿Por qué se ha producido el incidente? o ¿Qué finalidad tenía el atacante?

- Desarrollo de la intrusión.

o ¿Cómo lo ha logrado?

o ¿Qué ha realizado en los sistemas? - Resultados del análisis.

o ¿Qué ha pasado?

o ¿Qué daños se han producido o se prevén que se producirán? o ¿Es denunciable?

o ¿Quién es el autor o autores?

- Recomendaciones.

o ¿Qué pasos dar a continuación?

o ¿Cómo protegerse para no repetir los hechos?

3.6.2. El informe técnico

El informe técnico será más largo que el anterior y contendrá mucho más detalle. Se hará una exposición muy detallada de todo el análisis con profundidad en la tecnología usada y los hallazgos. En este caso se deberá redactar, al menos:

Antecedentes del incidente.

o Puesta en situación de cómo se encontraba la situación anteriormente al

incidente.

- Recolección de datos.

o ¿Cómo se ha llevado a cabo el proceso?

o ¿Qué se ha recolectado?

[?] Descripción de la evidencia.

o Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etc.

[?] Entorno de trabajo del análisis.

o ¿Qué herramientas se han usado? o ¿Cómo se han usado?

[?] Análisis de las evidencias.

o Se deberá informar del sistema analizado aportando datos como las

características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.

[?] Descripción de los resultados.

o ¿Qué herramientas ha usado el atacante?

o ¿Qué alcance ha tenido el incidente?

o Determinar el origen del mismo y como se ha encontrado.

[?] Dar la línea temporal de los hechos ocurridos con todo detalle.

[?] Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.

[?] Dar unas recomendaciones sobre cómo proteger los equipos para no repetir el incidente o sobre cómo actuar legalmente contra el autor.

L

MEDIDAS DE CONTENCIÓN DE INCIDENTES

Contención de daños y minimización de los riesgos

Actuar rápida y eficazmente puede reducir considerablemente los efectos de un incidente. El tiempo es un factor diferencial, ya que un incidente de nivel bajo si se prolonga en el tiempo, podría convertirse en un problema mucho más grave. Cada ataque tiene una naturaleza diferente, aunque las siguientes **prioridades** deberían estar presentes en todo tipo de ataque:

- Proteger la seguridad de las personas, esta debe ser la máxima prioridad.
- Proteger cualquier tipo de información valiosa para la empresa como información personal de clientes, proveedores o el plan de negocio. En caso de que se haya realizado una clasificación de la información se puede optar por proteger aquella marcada con un determinado nivel de criticidad.
- Proteger los equipos y sistemas de la organización, aunque minimizando el tiempo que estos se encuentran detenidos. Puede darse el caso que parar los procesos y servicios de la organización sea perjudicial para la misma, pero a la larga es más probable que sea peor no detener los sistemas afectados.

Además de estas prioridades, hay que **contener el daño** que se pudiera causar a la organización lo antes posible. Para ello se deberán tener en cuenta lo siguientes aspectos:

- Ya que la gran mayoría de los escenarios requieren desconectar todos los equipos de la red o varios de ellos hay que tener en cuenta el impacto que puede tener, en especial cuando se cuenta con acuerdos a nivel de servicio en el que se garantiza un mínimo de disponibilidad.
- Determinar la vía utilizada por el atacante para comprometer la seguridad de la organización y tomar medidas para proteger ese canal de entrada para que la organización no vuelva a ser atacada por esa vía.
- Clonar los discos de los equipos afectados o cambiarlos por unos nuevos, estas pruebas serán de gran utilidad para determinar que ha hecho el atacante en la red de la empresa. También hay que cambiar las credenciales de acceso de todos los usuarios.

Estos son solo los primeros pasos, en las próximas semanas conocerás cómo responder y recuperarse de un incidente. También a valorar los daños y tomar las medidas necesarias para que no vuelva a suceder.

Es hora de reinstalar los equipos afectados y restaurar las copias de seguridad si las tuviéramos. Hacer copias de seguridad periódicas off-line y almacenarlas en otra ubicación distinta a la de los equipos afectados será en algunos casos la única forma de recuperar los datos y equipos afectados.

Un incidente de seguridad se puede presentar sin ser detectado. En estos casos, algunas copias de seguridad almacenadas podrían estar afectadas y tendremos que identificar cuál de ellas tenemos que restaurar. Para saber qué copia utilizar, es de suma importancia identificar en qué momento se produjo el ataque. Para determinarlo puede ser de utilidad contar con software de integridad de archivos u otras herramientas de seguridad como IDS, IPS, UTM, etc. Para recuperar los sistemas y los activos afectados se debe utilizar una copia de seguridad **previa al incidente**. Es vital para la empresa disponer de varias copias de seguridad y utilizar aquella sobre la que tengamos la seguridad de que sus archivos no se han visto comprometidos.