Investigación de los incidentes de ciberseguridad (Incidentes de ciberseguridad)

Procesos para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de información en eso consiste la gestión de incidentes de seguridad.

Se conocen como gestión de ciberincidentes 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

Las evidencias son información que, por sí misma, o en combinación con otra información, se utiliza para probar algo.

Se trata de una fase inicial en la que toda entidad debe estar preparada para cualquier suceso que pudiera ocurrir. Una buena anticipación y entrenamiento previo es clave para realizar una gestión eficaz de un incidente, para lo que hace falta tener en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología.

Más información

- https://www.jesusninoc.com/02/28/seguridad-informatica-con-powershell/#Artefactos
- https://www.jesusninoc.com/02/28/seguridad-informatica-con-powershell/#Crear_un_fichero_de_volcado_de_memoria_de_un_proceso

---

Análisis de evidencias

El objetivo de esta fase es identificar o detectar un ciberincidente para lo cual es importante realizar una monitorización lo más completa posible. Teniendo en cuenta la máxima de que no todos los eventos o alertas de ciberseguridad son ciberincidentes.

Investigación del incidente

Los incidentes son cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio.

Intercambio de información del incidente con proveedores u organismos competentes

Mediante el sistema de ventanilla única se informa de un incidente, la información solicitada en cada caso, en función de la naturaleza del afectado, deberá ser remitida de acuerdo al cauce establecido por su autoridad competente o CSIRT de referencia.

Funcionamiento del sistema de ventanilla única:

1. El sujeto afectado enviará un correo electrónico (o ticket) al CSIRT de referencia (INCIBE-CERT o CCN-CERT) notificando el incidente.
2. El CSIRT de referencia, dependiendo del incidente, pone en conocimiento del mismo al organismo receptor implicado o la autoridad nacional competente:
    - Si afecta a la Defensa Nacional, al ESPDEFCERT
    - Si afecta a Infraestructura Crítica de la Ley PIC 8/2011, al CNPIC
    - Si afecta al RGPD, a la AEPD.
    - Si es un incidente de AAPP bajo el ENS de peligrosidad MUY ALTA o CRÍTICA, al CCN-CERT
    - Si es un incidente de obligatorio reporte según el RD Ley 12/2018, a la autoridad nacional competente correspondiente.
        - RGPD: se remite la URL del portal de la AEPD.
        - BDE: se remite la plantilla de notificación .XLS del BDE.
        - PIC: se remite la plantilla de notificación .XLS del CNPIC.
        - ENS: se remite la plantilla de notificación .DOC a CCN-CERT.
        - NIS: se remite la plantilla de notificación de la autoridad nacional competente.
3. El Organismo receptor implicado o autoridad nacional competente se pone en contacto con el sujeto afectado para recabar datos del incidente.
4. El sujeto afectado comunica las datos necesarios al organismo receptor implicado o autoridad nacional competente.
5. Si procede, desde la Oficina de Coordinación Cibernética (CNPIC) se pone la información a disposición de las Fuerzas y Cuerpos de Seguridad del Estado y Ministerio Fiscal para iniciar la investigación policial y judicial (art. 14.3 RD Ley 12/2018).

Medidas de contención de incidentes

En el momento que se ha identificado un ciberincidente la máxima prioridad es contener el impacto del mismo en la organización de forma que se puedan evitar lo antes posible la propagación a otros sistemas o redes evitando un impacto mayor, y la extracción de información fuera de la organización.

Ésta suele ser la fase en la que se realiza el triage que consiste en evaluar toda la información disponible en ese momento realizar una clasificación y priorización del ciberincidente en función del tipo y de la criticidad de la información y los sistemas afectados. Adicionalmente se identifican posibles impactos en el negocio y en función de los procedimientos se trabaja en la toma de decisiones con las unidades de negocio apropiadas y/o a los responsables de los servicios.

Las medidas de mitigación dependerán del tipo de ciberincidente, ya que en algunos casos será necesario contar con apoyo de proveedores de servicios, como en el caso de un ataques de denegación de servicio distribuido (DDoS), y en otros ciberincidentes puede suponer incluyo el borrado completo de los sistemas afectados y recuperación desde una copia de seguridad.

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en ciberincidentes.

Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización.