CAPITULO 4
Gestión de Incidentes

Jenny Torres, PhD.

Gestión de Incidentes

Definición

- Es un evento, anomalía o interrupción de un servicio de seguridad de la información, inesperado o no deseado, que tienen una probabilidad significativa de comprometer las operaciones de un sistema y de amenazar la seguridad de la información del mismo.

Gestión de Incidentes

- Se aplica enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.
- Se establece procedimientos para manejar eventos y debilidades en la seguridad de información de una manera efectiva.
- Se aplica proceso de mejora continua en respuesta para monitorear, evaluar y gestionar los incidentes.

Gestión de Incidentes

- **Incidente de seguridad.** Podría definirse como cualquier hecho o evento que podría afectar la seguridad personal o la seguridad de una organización. Estos amenazan el buen funcionamiento de cualquier organización y violan implícita o explícitamente las políticas de seguridad.

- **Incidente de seguridad informático.** Se le denomina un incidente de seguridad informática a cualquier evento que sea considerado una amenaza para la seguridad de un sistema.

Gestión de Incidentes

Principales Incidentes Informáticos

- Instalación de software malicioso
- Acceso sin autorización al sistema o a datos personales
- Interrupciones indeseadas
- Denegación de servicios
- Uso desautorizado de las bases de datos
- Cambio en el hardware, firmware o software del sistema

Gestión de Incidentes

Clasificación

- Se denominan incidentes **automáticos** a los incidentes producidos por programas de cómputo tales como virus, gusanos y troyanos.

- Los incidentes **manuales** son aquellos incidentes en los que de manera intencional se ataca un sistema utilizando, por ejemplo, escaneo de vulnerabilidades, inyección SQL o ingeniería social, aunque bajo ciertas circunstancias, también se pueden realizar de forma automática.

Gestión de Incidentes

Procedimiento

- Debe incluir:
  - Procesos de retroalimentación para obtener resultados después de haber tratado el problema
  - Reporte de eventos de seguridad que contenga acciones realizadas
  - Indicar detalles importantes y no ejecutar acción propia sino reportarla

Gestión de Incidentes

Comunicación de debilidades en seguridad

- Todos los empleados que son usuarios de los sistemas y servicios de información deben comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.
- Los empleados no deben intentar probar debilidades sospechadas de seguridad, podría causar daño al sistema
- Los reportes deben ser fáciles, accesibles y disponibles

Gestión de Incidentes

Identificación de responsabilidades y procedimientos

- Los procedimientos deben comprender:
  - Análisis e identificación de la causa de incidente
  - Contención
  - Planificación e implementación de la acción correctiva para evitar
  - recurrencia
  - Comunicación con afectados o implicados
  - Reporte de acción de autoridad apropiada

Gestión de Incidentes

Proceso

- Un procedimiento bien documentado para la gestión de respuesta a incidentes garantiza la rápida recuperación del sistema y la pronta restauración de las operaciones normales de la organización.
- La International Organization for Standardization (ISO) ha propuesto un mecanismo de respuesta a incidentes como parte de la serie de estándares ISO 27000 para el manejo de seguridad de la información
- Este mecanismo establece un framework que permite identificar los posibles ataques y las técnicas de mitigación asociadas a estos
- Este framework es esencial para no solo responder a los incidentes, sino también asegurar la infraestructura tecnológica.

Gestión de Incidentes

Proceso

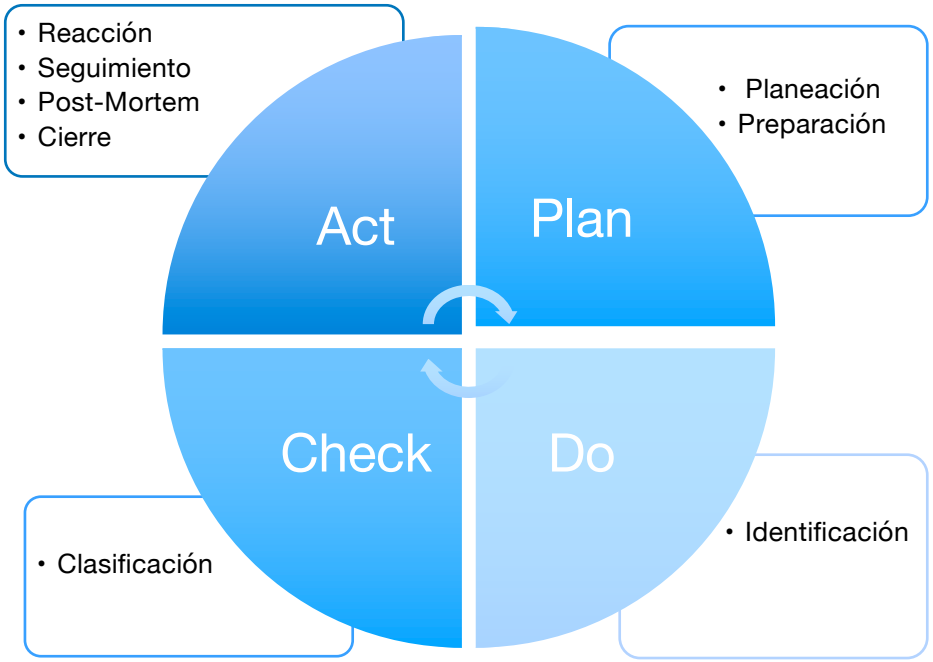
- Este framework o Sistema de Gestión de Seguridad de la Información (SGSI) propone un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos informáticos basándose en la evaluación de riesgos y en los niveles de tolerancia que la organización pudiese tener (BS ISO/IEC, 2009).

- La efectiva integración de la respuesta a incidentes dentro de la organización requiere una clara metodología que integre las funciones de la organización, los activos, los departamentos y sus respectivas responsabilidades (Bhaiji, 2008)

- El framework de respuesta a incidentes debe ser abordado holísticamente, es decir abordar la solución de cada incidente integrando a todos las disciplinas involucradas.

Gestión de Incidentes

Proceso



Gestión de Incidentes

Fase 1. Planeación y Preparación

- El aspecto más importante de la respuesta a un incidente es la preparación preventiva de modo que se pueda estar preparado para eventos que puedan ocurrir.
- Definir los roles y responsabilidades del CSIRT
- Pedir apoyo de los altos niveles de mando de la organización
- Investigar los incidentes que pueden ocurrir y detallar cómo pueden ser manejados
- Clasificar los incidentes en categorías y niveles
- Desarrollar acciones preventivas
- Probar las acciones preventivas para asegurar la efectividad del mecanismo de respuesta
- Definir acciones proactivas junto con las herramientas de respuesta
- Validar las acciones proactivas en escenarios de prueba controlados

Gestión de Incidentes

Fase 1. Planeación y Preparación

- Identificar los posibles afectados y establecer canales de comunicación efectivos para alertarlos
- Establecer canales de comunicación con los proveedores de Intenet (ISPs) para bloquear y eventualmente rastrear al infractor
- Definir las instrucciones que deberán seguir los usuarios afectados durante el incidente
- Entrenar al personal del CSIRT en cada incidente identificado
- El último aspecto es el más importante ya que los miembros del CSIRT no tienen un plan de seguridad y un procedimiento. Además no están adecuadamente entrenados en el uso efectivo de las herramientas. Un aspecto adicional a considerar es la dependencia y confianza en los proveedores, los cuales son contactados cuando surgen brechas de seguridad, sin considerar que éstos no son responsables del mantenimiento y la solución de problemas de la infraestructura en general, únicamente están para facilitar y proveer los dispositivos.

Gestión de Incidentes

Fase 2. Identificación

- Luego de que un incidente es detectado y reportado, el CSIRT debe analizar detalladamente el mismo para identificar el proceso de resolución predefinido que debe ser aplicado. Para ello, la organización debería entender el tipo de ataque y el daño que haya causado.
- Para ayudar a la identificación de incidentes, es recomendable establecer pistas de auditoría en los sistemas críticos tales como:
  - Carga de CPU
  - Registros de Actividad del Sistema
  - Alertas SNMP
  - Monitorear Protocolos e Interfaces
  - Monitorear Interrupciones de Procesador
  - Monitorear Caídas de Ancho de Banda debido a saturaciones de peticiones HTTP
  - Mantener Estadísticas de Tráfico de la Red

Gestión de Incidentes

Fase 3. Clasificación

- Una vez que el procedimiento de resolución a un incidente haya sido identificado, el mismo debe ser clasificado de acuerdo a las categorías y niveles definidos en la fase 1.
- Para ayudar a la clasificación de incidentes, se pueden utilizar herramientas de clasificación como:
  - Network Traffic Analizer - NetFlow
  - http://www.solarwinds.com/products/network-traffic-analyzer/
  - Cisco Network-Based Application Recognition - NBAR
  - http://www.cisco.com/en/US/products/ps6616/products_ios_protoco l_group_home.html
  - Cisco Modular QoS Client
  - http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/f t3level.html

Gestión de Incidentes

Fase 4. Reacción, Seguimiento, Post-Mortem y Cierre

- Reaccionar ante un incidente informático es aplicar los procedimientos para rápida y flexiblemente contener y erradicar el mismo, seguido de un restablecimiento completo de los sistemas del negocio para asegurar que las respuestas adoptadas han sido efectivas.
- Para hacer esto, el CSIRT debe hacer un seguimiento de la resolución al incidente mediante acciones como:
  - Preparar un reporte detallado para informar a la administración y al personal que se ha manejo un incidente de inicio a fin, con un resultado eventualmente exitoso
  - Recolectar evidencia del mal uso de equipos o infraestructura deben ser recolectados asegurando su integridad y proveniencia
  - En este último paso, es donde prácticamente la Gestión de Respuesta a Incidentes se enlaza con las Prácticas de Computación Forense de modo que se pueda proveer y dar seguimiento óptimo a un evento ilegal dentro de la organización.

Gestión de Incidentes

Fase 4. Reacción, Seguimiento, Post-Mortem y Cierre

- Es necesario que el CSIRT, junto con los involucrados en el proceso de identificación, revise los componentes técnicos y de personal que produjeron el incidente para tomar acciones efectivas de modo que el sistema de información comprometido sea reforzado para reducir el riesgo de recurrencia del incidente. Este análisis se lo conoce como Post-Mortem.
  - Evaluar el Riesgo del Incidente
  - Revisar las Políticas de Seguridad
  - Identificar Tendencias y Patrones del Incidente
  - Identificar opciones para reforzar o reponer los Controles de Seguridad
  - Establecer acciones internas o externas de ser requerido; e.g., acciones legales
  - Basándose en los hallazgos del análisis post-mortem, la organización debe acordar acciones de cierre del incidente, como por ejemplo: Establecer una nueva política interna de seguridad.

Gestión de Incidentes

Fase 4. Reacción, Seguimiento, Post-Mortem y Cierre

- Reasignar la custodia del activo
- Desarrollar campañas de concientización
- Implementar parches o nuevas contra medidas
- Implementar procesos disciplinarios o legales, de ser necesario
- Revisar la responsabilidad de la organización en cuanto a sus objetivos y necesidades para asegurar un efectivo proceso de gestión de respuesta a incidents.

- A más de lo anterior, toda la información del incidente debe ser archivada y mantenida para referencia futura. Esto incluye no solo el reporte del incidente, sino toda la información colateral generada durante el proceso. Por ejemplo, llamadas telefónicas, email, correspondencia, registros de sistema, etc. De este modo, la evaluación final del daño puede ser remitida a la administración central de la organización para restitución de los mismos si es que se cuenta con una póliza de seguro.

Gestión de Incidentes

Fase 4. Reacción, Seguimiento, Post-Mortem y Cierre

- Estas acciones de cierre son importantes ya que puede haber una gran posibilidad de que una gran cantidad de la información utilizada sea olvidada o mal interpretada, produciendo la repetitiva ejecución de tareas de **identificación, clasificación y de seguimiento**.

- Adicionalmente, en las fases previas del proceso es inviable determinar si el procesamiento de los intrusos es viable y si el incidente como tal va a tener repercusiones legales. Al mantener registros de información, se puede obtener la evidencia necesaria para establecer o no acciones legales, si el caso se mueve a esa dirección.

- Finalmente, si la respuesta a un incidente informático lleva a la investigación forense del mismo, las prácticas de computación forense deben ser adoptadas para obtener información y evidencia admisible en la corte para uso de las autoridades competentes.

Referencias

- ISO 27000, disponible en : http://www.iso27000.es
- Computer Emergency Response Team. Available at: http://www.cert.org
- Maiwald Eric, Fundamentos de Seguridad en Redes, McGrawHill, Segunda Edición, México 2005.
- Garfinkel Simson, Web Security, Privacy & Commerce.
- Tipos de delitos informáticos reconocidos por las Naciones Unidas. Disponible en http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm