Plan: gestión de incidentes de seguridad

Autor: Graciela Martínez
Edición: Área de Comunicaciones
Área: Área de Tecnología

Noviembre 2023

lacnic
www.lacnic.net

Objetivo

El objetivo de este documento es compartir un breve resumen de las etapas básicas para la definición de un plan general para implementar la gestión de incidentes de seguridad en una organización. Tener este plan definido colabora en la respuesta efectiva ante la ocurrencia de un incidente de seguridad.

Etapa de preparación

- Establecer el CSIRT
- Desarrollar un Plan para la respuesta a incidentes de seguridad: Identificar, asesorar, mitigar y recuperar
- Establecer un mecanismo para el reporte de incidentes de seguridad, tanto para la comunidad objetivo como para otras partes interesadas
- Definir la taxonomía de los incidentes y su nivel de severidad
- Definir el procedimiento para el triage de los reportes recibidos
- Definir un plan de comunicación para las partes interesadas internas y externas, que incluya voceros autorizados y que contemple la imagen de la organización
- Capacitar al Staff para que sepan identificar posibles amenazas y cómo reportar incidentes de seguridad.
- Crear un inventario de activos críticos

Etapa de Identificación

- Detectar eventos e incidentes: implementar sistema de monitoreo, centralizar logs, implementar sistemas de detección de intrusos

Etapa de contención y erradicación

- Identificar el/los sistema/s afectados y tomar medidas efectivas lo antes posible para evitar daños mayores
- Analizar si corresponde realizar notificaciones legales
- Iniciar la documentación correspondiente, manteniendo el orden de los hechos en una línea de tiempo
- Preparar las comunicaciones, comunicar a los posibles afectados y a toda persona que corresponda
- Investigar el incidente de seguridad para determinar las causas que permitieron el ataque, la dimensión del daño ocasionado, evaluar posible compromiso de otros sistemas y analizar posibles vulnerabilidades no detectadas hasta el momento
- Erradicar la causa del incidente (Ejemplo: eliminar malware, aplicar patches, cambiar contraseñas, evaluar la efectividad de la trazabilidad de eventos, realizar análisis forense donde y cuando corresponda, buscar artefactos para su posterior análisis etc.)
- Documentar las razones del incidente, las acciones realizadas y todo hecho que sea relevante para la correcta comprensión del mismo

Etapa de recuperación

- Restaurar los sistemas afectados a medida que se vayan corrigiendo.
- Restaurar datos de respaldos de acuerdo al plan de la organización (si fuera necesario)
- Implementar nuevos controles y medidas que se hayan identificado en el proceso de investigación

Etapa de evaluación post-incidente

- Revisar la documentación generada durante las etapas previas y completar con la información que se entienda necesaria para que sirva de futura referencia
- Documentar las lecciones aprendidas:
    - Fortalezas como debilidades de la gestión del incidente
    - Evaluar si corresponde elaborar un plan de capacitación de acuerdo a la característica del incidente analizado
    - Evaluar si corresponde una actualización del plan de gestión

Plan de Comunicación

Es muy importante tener un Plan de Comunicación definido y acordado en la organización. Durante la gestión de un incidente es necesario realizar las comunicaciones pertinentes de acuerdo al mismo.

A grandes rasgos se deben tener en cuenta los siguientes aspectos:

- Comunicar a la interna de la organización durante todas las etapas de la gestión del incidente, de acuerdo a la necesidad de saber de cada rol
- Comunicar a todas las partes interesadas externas a la organización de acuerdo a las regulaciones vigentes y la necesidad de saber de las mismas
- Definir cómo se va a gestionar la intervención de la prensa si fuera necesario
- En caso que corresponda realizar:
    - Las notificaciones legales
    - Las denuncias ante agencias del orden

- Una vez concluida la gestión del incidente de seguridad, realizar un informe ejecutivo del mismo para elevar a la Dirección de la organización, y al Directorio si corresponde. Este informe es independiente de las comunicaciones que se hayan realizado durante las distintas etapas de su gestión.