INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 11

23 DE NOVIEMBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado. 2
Preparación 2
Identificación 3
Contención 3
Mitigación 4
Recuperación 4
Actuaciones post-incidente 4

Enunciado.

REALIZA LA GESTIÓN DEL CIBERINCIDENTE INDICADO SIGUIENDO LAS FASES DADAS POR EL INCIBE:

1º.- Preparación.

2º.- Identificación.

3º.- Contención.

4º.- Mitigación.

5º.- Recuperación.

6º.- Actuaciones post-incidente.

Preparación

Desarrollo de un Plan de Respuesta a Incidentes (PRI):

- Identificación de Roles y Responsabilidades:

Determinar quiénes son los responsables de qué aspectos durante un incidente.

- Equipo de Respuesta a Incidentes:

Crear un equipo capacitado y con roles asignados para la gestión de incidentes.

- Procedimientos y Protocolos:

Establecer protocolos claros para la notificación, escalada y resolución de incidentes.

Formación y Ejercicios:

- Capacitación del Personal:

Brindar formación continua al personal para que estén preparados para detectar y responder a incidentes.

- Simulacros y Ejercicios:

Realizar ejercicios simulados para poner a prueba la efectividad del PRI y la capacidad de respuesta del equipo.

Implementación de Controles de Seguridad:

- Revisión y Reforzamiento:

Evaluar y mejorar las medidas de seguridad existentes para reducir las vulnerabilidades.

- Actualizaciones de Políticas:

Mantener actualizadas las políticas de seguridad de la información.

Identificación

Monitoreo Continuo:

- Sistemas y Redes:

Implementar sistemas de monitorización para la detección de actividad inusual.

- Alertas Tempranas:

Configurar alertas que notifiquen sobre eventos sospechosos.

Detección de Intrusiones:

- Herramientas de Detección:

Utilizar sistemas de detección de intrusiones (IDS) para identificar patrones anómalos.

- Análisis de Tráfico:

Analizar el tráfico de red en busca de comportamientos maliciosos.

Análisis de Logs:

- Registro y Análisis:

Mantener registros detallados de eventos y realizar análisis periódicos para identificar actividades sospechosas.

- Integración de Herramientas de SIEM:

Utilizar sistemas de gestión de eventos e información de seguridad (SIEM) para centralizar y analizar los registros.

Contención

Aislamiento de Sistemas Afectados:

- Desconexión Rápida:

Desconectar sistemas comprometidos de la red para evitar la propagación.

- Segmentación de Red:

Implementar segmentación de red para limitar el impacto en caso de un incidente.

Implementación de Contramedidas:

- Bloqueo de Tráfico Malicioso:

Configurar reglas de firewall para bloquear tráfico asociado con el incidente.

- Aplicación de Políticas de Seguridad:

Reforzar las políticas de seguridad para prevenir futuras amenazas similares.

Mitigación

Remediación de Sistemas:

- Eliminación de Malware:

Realizar análisis antivirus y antimalware para eliminar código malicioso.

- Restauración desde Reservas:

Restaurar sistemas desde copias de seguridad verificadas.

Actualizaciones y Parches:

- Gestión de Vulnerabilidades:

Implementar actualizaciones de seguridad para corregir vulnerabilidades conocidas.

- Revisión de Configuraciones:

Verificar y corregir configuraciones inseguras en sistemas y aplicaciones.

Recuperación

Restauración de Datos y Sistemas:

- Priorización de Servicios:

Restaurar primero los servicios críticos para minimizar el tiempo de inactividad.

- Verificación de Integridad:

Verificar la integridad de los datos y sistemas restaurados.

Análisis Posterior:

- Evaluación de Respuesta:

Analizar la efectividad de la respuesta y determinar áreas de mejora.

- Registro de Lecciones Aprendidas:

Documentar las lecciones aprendidas para mejorar futuras respuestas.

Actuaciones post-incidente

Análisis de Lecciones Aprendidas:

- Revisión de Procedimientos:

Evaluar cómo los procedimientos de respuesta podrían mejorarse.

- Capacitación Adicional:

Identificar necesidades de formación adicional basadas en el incidente.

Informe Post-Incidente:

- Documentación Detallada:

Crear un informe completo del incidente, incluyendo acciones tomadas y resultados.

- Recomendaciones para Mejoras:

Ofrecer recomendaciones para evitar incidentes similares en el futuro.

Mejora Continua:

- Actualización de Políticas:

Modificar políticas y procedimientos según las lecciones aprendidas.

- Evaluación Periódica:

Revisar y actualizar periódicamente el PRI y los protocolos de respuesta.