INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 23

8 DE FEBRERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.

Realiza la Gestión del Incidente solicitado siguiendo las siguientes fases :

1º.- Preparación.-

Afecta a todos los activos.-

2º.- Identificación.-

Afecta solamente al equipo con el IDS/IPS.-

3º.- Contención.

Afecta solamente al equipo con el IDS/IPS.-

4º.- Mitigación.-

Afecta a todos los activos.-

5º.- Recuperación.-

Afecta a todos los activos.-

6º.- Actuaciones post-incidente.-

Activos Informáticos :

1º.- CPD1 : Expedientes académicos + laborales .-

2º.- CPD2 : Moodle Centros (Aula Virtual) + Página Web .-

3º.- Equipos Equipo Directivo +Admon + Sala de Profesoras/es + Ordenadores Departamentos +Ordenador Profesor Aula.-

4º.- Ordenadores de Laboratorio.-

5º.- Elementos de red .-

GESTIÓN DE INCIDENTE-- ANÁLISIS DE PAQUETES (SNIFFING)

Preparación

- Identificación de activos: Realiza un inventario detallado de todos los activos informáticos, incluyendo servidores en CPD1 y CPD2, estaciones de trabajo, dispositivos de red, etc.

- Planificación de respuesta a incidentes: Desarrolla un plan detallado que incluya roles y responsabilidades del equipo de respuesta a incidentes, procedimientos de notificación, escalado de incidentes y coordinación con partes externas como proveedores de servicios y agencias de aplicación de la ley.

- Configuración de sistemas de detección: Asegúrate de que los sistemas de detección de intrusiones (IDS/IPS) estén configurados correctamente para monitorear y detectar actividades maliciosas en la red.

- Capacitación del personal: Proporciona entrenamiento regular al personal sobre prácticas de seguridad, procedimientos de respuesta a incidentes y herramientas de seguridad utilizadas.

Identificación

- Monitoreo de eventos: Utiliza los registros de eventos de los sistemas y los datos recopilados por los IDS/IPS para identificar patrones o actividades sospechosas en la red.

- Análisis de anomalías: Utiliza herramientas de análisis de seguridad para identificar comportamientos anómalos en la red, como tráfico inusual, intentos de acceso no autorizados o comunicaciones sospechosas.

- Investigación de alertas: Investiga todas las alertas generadas por los sistemas de detección de intrusiones para determinar la naturaleza y el alcance del incidente.

Contención

- Aislamiento de sistemas comprometidos: Desconecta los sistemas comprometidos de la red para evitar que el incidente se propague a otros activos.

- Implementación de controles de acceso: Refuerza los controles de acceso para limitar el acceso a los sistemas afectados solo a personal autorizado mientras se investiga el incidente.

- Bloqueo de tráfico malicioso: Utiliza reglas de firewall u otras herramientas de seguridad para bloquear el tráfico malicioso y prevenir ataques adicionales.

Mitigación

- Eliminación de amenazas: Elimina cualquier malware o software malicioso presente en los sistemas comprometidos.

- Aplicación de parches de seguridad: Instala parches de seguridad y actualizaciones de software para cerrar cualquier vulnerabilidad que haya sido explotada durante el incidente.

- Restauración de servicios: Restaura los servicios afectados a su estado operativo normal y verifica que funcionen correctamente.

Recuperación

- Restauración de datos y sistemas: Restaura los datos y sistemas afectados desde copias de seguridad verificadas para garantizar la integridad de la información.

- Pruebas de seguridad: Realiza pruebas de seguridad adicionales para verificar que los sistemas restaurados estén libres de vulnerabilidades y sean seguros.

- Actualización de documentación: Actualiza la documentación de seguridad y los registros de incidentes con los detalles del incidente y las acciones tomadas durante la respuesta.

Actuaciones post-incidentes

- Análisis de lecciones aprendidas: Realiza una revisión exhaustiva del incidente para identificar las causas subyacentes y las lecciones aprendidas.

- Mejoras en políticas y procedimientos: Actualiza los procedimientos de respuesta a incidentes y las políticas de seguridad según sea necesario para prevenir incidentes similares en el futuro.

- Capacitación y concientización: Proporciona entrenamiento adicional al personal sobre las lecciones aprendidas durante el incidente y promueve la conciencia de seguridad en toda la organización.