INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 20

30 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

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 INCIDENTES: CONFIGURACIÓN DE MALWARE.

1. Preparación:

- **Instalación de software de detección de intrusiones (IDS/IPS):** Asegúrate de que todos los equipos, especialmente aquellos que almacenan datos críticos como CPD1 y CPD2, tengan instalado y configurado un IDS/IPS para detectar y prevenir intrusiones.

- Copias de seguridad: Realiza copias de seguridad regulares de los datos almacenados en CPD1 y CPD2, así como de los sistemas y archivos críticos en los equipos, incluyendo los servidores de Moodle y la página web. Asegúrate de que estas copias de seguridad estén actualizadas y almacenadas en un lugar seguro y fuera del alcance de posibles amenazas**.**

2. Identificación:

- Monitoreo de IDS/IPS: El equipo encargado del monitoreo del IDS/IPS debe estar atento a cualquier actividad inusual o potencialmente maliciosa en la red. Esto puede incluir intentos de intrusión, tráfico anómalo o patrones de comportamiento sospechosos.

- Análisis de eventos: Una vez que se detecte un evento sospechoso, el equipo debe analizarlo detenidamente para determinar la naturaleza del incidente, su origen, su impacto potencial en los activos y la forma en que se propaga a través de la red.

3. Contención:

- Aislamiento de la amenaza: Una vez identificado el incidente, el equipo debe tomar medidas para contener la amenaza y evitar que se propague a otros activos. Esto puede implicar la desconexión del equipo comprometido de la red, la desactivación de cuentas de usuario comprometidas o el bloqueo de direcciones IP sospechosas.

- Restricción de accesos: Limita el acceso a los activos afectados y restringe los privilegios de usuario para evitar daños adicionales mientras se investiga y se resuelve el incidente.

4. Mitigación:

Implementación de medidas correctivas: Una vez contenida la amenaza, el equipo debe implementar medidas correctivas para mitigar el impacto del incidente y prevenir futuros ataques similares. Esto puede incluir la aplicación de parches de seguridad, actualización de software, cambios de contraseñas y reconfiguración de sistemas afectados para cerrar las brechas de seguridad.

5. Recuperación:

- Restauración de datos: Utiliza las copias de seguridad previamente realizadas para restaurar los datos y sistemas afectados a un estado seguro y funcional. Asegúrate de que las copias de seguridad estén libres de malware antes de restaurarlas.

- Pruebas de integridad: Verifica la integridad de los datos restaurados y realiza pruebas exhaustivas para asegurarte de que los sistemas y servicios afectados estén funcionando correctamente después de la restauración.

6. Actuaciones post-incidente:

- Análisis de lecciones aprendidas: Realiza una revisión exhaustiva del incidente para identificar las causas subyacentes, las deficiencias en los controles de seguridad y las lecciones aprendidas. Documenta los hallazgos y utiliza esta información para mejorar los procedimientos y políticas de seguridad.

- Capacitación y concienciación: Proporciona capacitación adicional al personal sobre las lecciones aprendidas del incidente, incluyendo prácticas de seguridad recomendadas, procedimientos de respuesta a incidentes y señales de advertencia de posibles amenazas.

- Actualización de políticas y procedimientos: Actualiza los procedimientos de respuesta a incidentes y las políticas de seguridad en función de las lecciones aprendidas del incidente, asegurándote de que estén alineados con las mejores prácticas de seguridad y las necesidades específicas de la organización.