INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 37

11 DE ABRIL 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 INCIDENTE—Denegación Distribuida de Servicio DDoS

Preparación

- Se identifican los activos críticos, como los CPD (Centros de Procesamiento de Datos) que contienen expedientes académicos y laborales, Moodle Centros (Aula Virtual) y la página web en CPD2, los equipos informáticos del equipo directivo, administrativo, profesores, departamentos, y laboratorios, así como los elementos de red.

- Se establecen roles y responsabilidades para el equipo de gestión de incidentes, designando quién liderará la respuesta, quién será responsable de la comunicación, quién gestionará la recuperación de datos, entre otros.

- Se implementan herramientas de detección, como sistemas de detección de intrusiones (IDS) o sistemas de prevención de intrusiones (IPS), para monitorear la red en busca de actividad sospechosa.

- Se realizan copias de seguridad regulares de los datos críticos para garantizar su disponibilidad en caso de un incidente.

Identificación

- El equipo con el IDS/IPS monitorea constantemente la red en busca de actividad inusual o sospechosa que pueda indicar un incidente de seguridad.

- Se utilizan firmas de amenazas, análisis de comportamiento y otros métodos para identificar posibles intrusiones o violaciones de seguridad.

- Se registran y documentan todas las alertas generadas por el IDS/IPS para su análisis posterior.

Contención:

- Una vez que se detecta un incidente, el equipo con el IDS/IPS toma medidas inmediatas para contenerlo y evitar que se propague.

- Esto puede incluir la desconexión de sistemas comprometidos de la red, el bloqueo de direcciones IP sospechosas o la implementación de políticas de seguridad más estrictas en los firewalls.

Mitigación

- Una vez que el incidente está contenido, se implementan medidas para mitigar su impacto y evitar futuros ataques.

- Esto puede incluir la aplicación de parches de seguridad, actualizaciones de software, cambios en la configuración de red y fortalecimiento de las políticas de seguridad.

Recuperación

- Se restauran los sistemas afectados a un estado seguro y se recuperan los datos perdidos, si es necesario.

- Esto implica la reinstalación de sistemas operativos, la restauración de copias de seguridad y la validación de la integridad de los datos recuperados.

- Se lleva a cabo una exhaustiva revisión para garantizar que todos los sistemas estén completamente funcionales y libres de malware.

Actuaciones post-incidentes

- Se realiza un análisis detallado del incidente para comprender su causa raíz y determinar las lecciones aprendidas.

- Se actualizan los procedimientos y políticas de seguridad según sea necesario para prevenir incidentes similares en el futuro.

- Se proporciona capacitación adicional al personal involucrado en la gestión de incidentes para mejorar la respuesta ante futuros incidentes.

- Se documenta exhaustivamente el incidente y las acciones tomadas para referencia futura y para cumplir con requisitos regulatorios o de cumplimiento.