INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 25

15 DE FEBRERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

observación y grabación del tráfico de redes.

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: INGENIERÍA SOCIAL.

Preparación

Realiza una revisión exhaustiva de la configuración de seguridad de todos los activos informáticos:

- Verifica que los firewalls estén correctamente configurados para filtrar el tráfico no autorizado y bloquear los intentos de acceso no autorizados.

- Asegúrate de que los sistemas IDS/IPS estén activos y configurados para detectar y alertar sobre actividades sospechosas.

Asegúrate de tener procedimientos de respuesta a incidentes documentados y accesibles para todo el personal relevante:

- Define claramente los roles y responsabilidades de cada miembro del equipo de respuesta a incidentes.

- Establece canales de comunicación efectivos para coordinar la respuesta al incidente.

Realiza copias de seguridad de los datos críticos almacenados en los activos informáticos:

- Programa copias de seguridad regulares y verifica que sean almacenadas de forma segura fuera del sitio.

Identificación

Utiliza el IDS/IPS para identificar patrones o comportamientos anómalos en el tráfico de red que puedan indicar una observación y grabación no autorizadas:

- Configura alertas para detectar tráfico sospechoso, como patrones de acceso inusualmente altos o tráfico hacia destinos no autorizados.

Analiza los registros del IDS/IPS para determinar la naturaleza y el alcance del incidente:

- Examina los registros de eventos para identificar los sistemas afectados y los métodos de ataque utilizados.

Contención

Una vez identificado el tráfico sospechoso, implementa medidas para contener el incidente y evitar que se propague a otros activos informáticos:

- Aísla los sistemas comprometidos o afectados del resto de la red utilizando VLANs o segmentación de red.

- Bloquea el tráfico sospechoso en los firewalls para evitar una mayor propagación del incidente.

Mitigación

Implementa soluciones para mitigar los efectos del incidente y restaurar la seguridad de los activos informáticos afectados:

- Aplica parches de seguridad y actualizaciones en los sistemas afectados para cerrar posibles brechas de seguridad.

- Restablece contraseñas y credenciales de acceso comprometidas para evitar accesos no autorizados futuros.

Recuperación

Restaura los sistemas afectados a un estado seguro y funcional utilizando las copias de seguridad disponibles:

- Realiza una restauración completa de los sistemas afectados utilizando las copias de seguridad más recientes.

- Verifica la integridad de los datos restaurados y realiza pruebas exhaustivas para garantizar que los sistemas funcionen correctamente.

Actuaciones post-incidentes

Realiza una evaluación exhaustiva del incidente para identificar las causas subyacentes y las lecciones aprendidas:

- Realiza entrevistas con el personal involucrado para recopilar información sobre la cadena de eventos que condujeron al incidente.

- Analiza los informes de incidentes para identificar áreas de mejora en los controles de seguridad y los procedimientos de respuesta a incidentes.

Actualiza los procedimientos de respuesta a incidentes en base a las lecciones aprendidas:

- Incorpora nuevas medidas de seguridad y controles de acceso para prevenir incidentes similares en el futuro.

- Proporciona formación adicional al personal relevante sobre las mejores prácticas de seguridad informática y la detección de amenazas.