INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 18

11 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

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

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: SERVIDOR C&C.

1. Preparación:

- Auditorías de seguridad: Realizar auditorías periódicas en los Centros de Procesamiento de Datos (CPD) para identificar posibles vulnerabilidades y evaluar la eficacia de los controles de seguridad.

- Inventario de activos: Mantener un inventario actualizado de todos los activos informáticos, incluidos servidores, equipos, software y elementos de red, clasificando su importancia para la continuidad del negocio.

- Equipo de respuesta: Establecer un equipo de respuesta a incidentes que incluya representantes de cada área, desde administradores de sistemas hasta personal de seguridad informática.

- Protocolos de comunicación: Desarrollar protocolos claros de comunicación interna y externa para garantizar una respuesta rápida y coordinada ante un incidente.

2. Identificación:

- Configuración de IDS/IPS: Ajustar la configuración de los sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS) para identificar patrones de tráfico y comportamientos sospechosos específicos de cada CPD.

- Análisis de registros: Implementar sistemas de monitoreo de registros para analizar los eventos del sistema y detectar actividades inusuales o signos de intrusiones.

- Herramientas de análisis de amenazas: Utilizar herramientas avanzadas de análisis de amenazas para identificar y categorizar la presencia de malware, exploits o comportamientos maliciosos en los activos informáticos.

3. Contención:

- Aislamiento del equipo con IDS/IPS: Desconectar el equipo que tiene el IDS/IPS de la red para prevenir la propagación de la amenaza y permitir un análisis más detenido de la situación.

- Desconexión de sistemas afectados: Tomar medidas para desconectar físicamente o aislar lógicamente los sistemas afectados, evitando que la amenaza se propague a otros activos.

- Reglas de firewall adicionales: Implementar reglas de firewall específicas para bloquear el tráfico malicioso conocido y reducir aún más la superficie de ataque.

4. Mitigación:

- Aplicación de parches y actualizaciones: Realizar una evaluación de vulnerabilidades en todos los activos y aplicar parches de seguridad y actualizaciones para corregir las debilidades identificadas.

- Análisis forense: Utilizar herramientas de análisis forense para comprender cómo se llevó a cabo el incidente, identificar el vector de ataque y mejorar las defensas en consecuencia.

- Mejora de políticas de seguridad: Actualizar las políticas de seguridad, incluyendo la gestión de contraseñas y políticas de acceso, con base en las lecciones aprendidas durante el incidente.

5. Recuperación:

- Restauración desde copias de seguridad: Utilizar las copias de seguridad previamente realizadas para restaurar los sistemas afectados a un estado anterior al incidente.

- Validación de sistemas: Verificar la integridad de los sistemas restaurados mediante pruebas exhaustivas para garantizar que no se hayan comprometido durante el incidente.

- Monitoreo continuo: Implementar un monitoreo activo después de la recuperación para detectar cualquier signo de actividad maliciosa residual o intentos de reintroducir la amenaza.

6. Actuaciones post-incidente:

- Análisis forense exhaustivo: Realizar un análisis forense detallado para entender completamente la cadena de eventos durante el incidente, identificar puntos débiles y ajustar las medidas de seguridad en consecuencia.

- Actualización de procedimientos: Modificar y mejorar los procedimientos de respuesta a incidentes basándose en las lecciones aprendidas durante el análisis post-incidente.

- Formación y concienciación: Proporcionar formación adicional al personal, destacando los aspectos clave del incidente y promoviendo prácticas seguras.

- Comunicación interna y externa: Informar internamente sobre los resultados del análisis post-incidente y, si es necesario y permitido, comunicar externamente sobre el incidente, siguiendo las regulaciones y normativas aplicables.