INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 27

3 DE MARZO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.

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-- EXPLOTACIÓN DE VULNERABILIDADES CONOCIDAS

Preparación

- Revisión de políticas de seguridad de contraseñas: Evaluar y actualizar las políticas de seguridad de contraseñas en todos los activos informáticos. Esto podría incluir requerir contraseñas robustas, cambiarlas regularmente y evitar el uso de contraseñas compartidas.

- Copias de seguridad: Realizar copias de seguridad completas y verificadas de los datos críticos almacenados en los Centros de Procesamiento de Datos (CPD) y otros activos informáticos.

- Configuración de sistemas de detección de intrusiones: Asegurarse de que los sistemas de detección de intrusiones (IDS/IPS) estén configurados y actualizados en el equipo designado para monitorear y responder a posibles intentos de vulnerar credenciales.

- Capacitación del personal: Proporcionar capacitación regular al personal sobre prácticas de seguridad de contraseñas, reconocimiento de intentos de vulnerar credenciales y procedimientos de respuesta a incidentes.

Identificación

- Utilizar el equipo con IDS/IPS para monitorear continuamente el tráfico de red en busca de actividades sospechosas, como intentos de inicio de sesión fallidos, escaneo de puertos o tráfico malicioso.

- Registrar y analizar cualquier actividad sospechosa para determinar la naturaleza y el alcance del intento de vulnerar credenciales.

Contención

- Configurar el IDS/IPS para bloquear o limitar el tráfico de red asociado con los intentos de vulnerar credenciales.

- Aislar los sistemas comprometidos del resto de la red para evitar la propagación del ataque y minimizar el daño potencial.

Mitigación

- Cambiar inmediatamente las contraseñas comprometidas en todos los activos afectados, utilizando contraseñas seguras y únicas.

- Aplicar parches de seguridad y actualizaciones en todos los sistemas afectados para corregir cualquier vulnerabilidad conocida que haya sido explotada durante el incidente.

- Realizar una evaluación exhaustiva de vulnerabilidades en todos los sistemas para identificar y remediar posibles puntos débiles que podrían ser explotados en futuros intentos de vulnerar credenciales.

Recuperación

- Restaurar los sistemas comprometidos desde copias de seguridad verificadas y limpias para asegurar la integridad de los datos y la infraestructura.

- Implementar medidas adicionales de seguridad, como la autenticación multifactorial, para fortalecer la seguridad de los sistemas y prevenir futuros intentos de vulnerar credenciales.

- Revisar y reforzar las políticas de seguridad de contraseñas y acceso para garantizar una protección adecuada de los activos informáticos.

Actuaciones post-incidentes

- Realizar un análisis forense completo para identificar la causa raíz del incidente y recopilar evidencia para futuras acciones legales o de seguimiento.

- Documentar todas las acciones tomadas durante el incidente, incluidas las decisiones de respuesta y las lecciones aprendidas.

- Comunicar el incidente y las medidas correctivas a las partes interesadas relevantes, incluido el personal y los usuarios afectados, para mantener la transparencia y la confianza en el sistema de seguridad.

- Programar sesiones de entrenamiento y concienciación adicionales sobre seguridad informática para el personal con el fin de mejorar la preparación y la respuesta ante futuros incidentes de seguridad.