INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 15

14 DE DICIEMBRE DE 2023

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 INCIDENTE: CONTENIDO INADECUADO.

Fases dadas por el Incibe.

1. Preparación:

- Desarrollar un plan de respuesta a incidentes:

Identificar roles y responsabilidades específicos para cada activo.

Establecer protocolos de comunicación interna y externa para cada área del centro.

Documentar procedimientos detallados para cada activo en caso de incidente.

- Identificar y asignar roles y responsabilidades:

Designar responsables específicos para la seguridad de cada activo.

Asignar tareas y funciones a los responsables designados.

- Establecer mecanismos de comunicación interna y externa:

Configurar canales de comunicación específicos para cada área afectada.

Establecer protocolos de notificación interna y externa para cada activo.

- Implementar medidas de seguridad proactivas en todos los activos:

Actualizar regularmente el software y firmware de todos los sistemas.

Implementar firewalls, sistemas de detección de intrusos y otras soluciones de seguridad en cada activo.

Realizar auditorías de seguridad periódicas y evaluaciones de vulnerabilidad específicas para cada activo.

2. Identificación:

- Configurar y mantener el IDS/IPS:

Implementar sistemas IDS/IPS específicos para cada CPD y área de equipos.

Configurar y monitorear el tráfico de red de cada activo.

Analizar activamente las alertas generadas por los IDS/IPS en cada CPD y área de equipos.

- Recopilar y analizar alertas:

Investigar todas las alertas generadas por los IDS/IPS de cada CPD y área de equipos.

Diferenciar entre falsos positivos y verdaderos positivos en cada activo.

Documentar y priorizar incidentes para la siguiente fase, específicamente para cada activo.

3. Contención:

- Tomar medidas para aislar o contener el incidente:

Identificar y aislar el CPD o área de equipos afectada para prevenir la propagación del incidente.

Desconectar el activo afectado de la red si es necesario.

Iniciar la respuesta de emergencia según lo definido en el plan para cada activo.

- Bloquear o mitigar la actividad maliciosa:

Utilizar el IDS/IPS y sistemas de firewall específicos para bloquear el tráfico malicioso en cada CPD y área de equipos.

Implementar contramedidas específicas para detener la actividad del atacante en cada activo.

4. Mitigación:

- Aplicar parches de seguridad o soluciones temporales:

Identificar y aplicar parches específicos para cada sistema y aplicación en los CPDs y áreas de equipos afectadas.

Actualizar las firmas de detección en los IDS/IPS de cada activo para proteger contra variantes conocidas.

- Actualizar políticas de seguridad y reforzar medidas preventivas:

Revisar y ajustar las políticas de seguridad para cada activo según las lecciones aprendidas.

Reforzar las medidas de seguridad específicas para cada área, como el monitoreo continuo, la autenticación de dos factores y el cifrado.

5. Recuperación:

- Restaurar sistemas desde copias de seguridad:

Verificar la integridad de las copias de seguridad específicas para cada CPD y área de equipos.

Restaurar sistemas y datos afectados desde copias de seguridad validadas en cada activo.

Monitorear los sistemas restaurados para detectar cualquier anomalía.

- Realizar análisis post-mortem:

Evaluar la efectividad de las acciones tomadas durante el incidente para cada CPD y área de equipos.

Identificar áreas de mejora en los procedimientos y políticas específicas para cada activo.

Documentar el incidente y las lecciones aprendidas, considerando la naturaleza única de cada activo.

6. Actuaciones post-incidente:

- Documentar el incidente, acciones tomadas y lecciones aprendidas:

Crear un informe detallado del incidente para cada activo, incluyendo el alcance, la duración y las acciones tomadas.

Registrar cualquier impacto financiero o reputacional específico para cada área.

- Realizar análisis forense:

Analizar evidencia forense específica para cada CPD y área de equipos para comprender cómo ocurrió el incidente y si hay datos comprometidos.

Identificar el origen y las tácticas utilizadas por el atacante en cada activo.

- Implementar mejoras en políticas, procedimientos y medidas de seguridad:

Actualizar el plan de respuesta a incidentes para cada activo con base en las lecciones aprendidas.

Realizar revisiones periódicas del plan específico para cada área y realizar simulacros de incidentes.

Implementar mejoras continuas en las medidas de seguridad y en la preparación para incidentes futuros, considerando la diversidad de activos.