INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 33

21 DE MARZO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

uso para propósitos inadecuados, incluyendo acciones con ánimo de lucro.

Ejemplo: uso de correo electrónico para participar en estafas.

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--Compromiso de Aplicaciones.

Preparación

- Realización de una evaluación exhaustiva de los activos informáticos: Se debe llevar a cabo una evaluación detallada de cada activo informático mencionado, incluyendo servidores, sistemas de red, equipos individuales y aplicaciones, para identificar posibles vulnerabilidades y puntos débiles que podrían ser explotados para actividades maliciosas con fines de lucro.

- Desarrollo de políticas y procedimientos de seguridad: Es fundamental contar con políticas y procedimientos claros para manejar incidentes de seguridad. Esto incluye la definición de roles y responsabilidades, los pasos a seguir en caso de incidentes y la documentación adecuada de las políticas de seguridad.

- Capacitación del personal: Todos los empleados deben recibir capacitación regular sobre seguridad cibernética, incluyendo la identificación de posibles amenazas, prácticas de seguridad recomendadas y cómo responder ante incidentes de seguridad.

Identificación

- Utilización de IDS/IPS: Los sistemas de detección y prevención de intrusiones (IDS/IPS) deben estar configurados para monitorear de manera proactiva la red en busca de actividades sospechosas, como intentos de acceso no autorizado, transferencias de archivos inusuales o comportamiento anómalo en el tráfico de red.

- Monitoreo de registros de actividad: Se deben revisar regularmente los registros de actividad del correo electrónico, sistemas de archivos y otras plataformas digitales en busca de patrones de comportamiento sospechoso que puedan indicar actividades maliciosas con fines de lucro, como el envío masivo de correos electrónicos fraudulentos o intentos de phishing.

Contención

- Aislamiento de sistemas comprometidos: Una vez que se detecta un incidente, es crucial aislar rápidamente los sistemas afectados para evitar que la actividad maliciosa se propague a otros activos informáticos. Esto puede implicar desconectar los sistemas comprometidos de la red o bloquear el acceso a los recursos afectados.

- Bloqueo de acceso: Se deben tomar medidas para bloquear el acceso de los atacantes a los sistemas comprometidos, como cambiar contraseñas o desactivar cuentas comprometidas.

Mitigación

- Corrección de vulnerabilidades: Se deben tomar medidas correctivas para abordar las vulnerabilidades que permitieron el incidente de seguridad, como la aplicación de parches de seguridad, la actualización de software obsoleto y la configuración adecuada de firewalls y sistemas de detección de intrusiones.

- Refuerzo de medidas de seguridad: Además de abordar las vulnerabilidades específicas que condujeron al incidente, se deben tomar medidas adicionales para reforzar la seguridad en general, como la implementación de autenticación multifactor, la encriptación de datos sensibles y la segmentación de la red.

Recuperación

- Restauración de sistemas: Una vez que se ha mitigado el incidente y se han corregido las vulnerabilidades, se pueden restaurar los sistemas afectados a un estado seguro y funcional. Esto puede implicar la restauración desde copias de seguridad limpias y la verificación de la integridad de los datos.

- Cambio de contraseñas y análisis adicionales: Es recomendable cambiar todas las contraseñas afectadas y realizar análisis adicionales para asegurarse de que no haya persistencia de amenazas en los sistemas comprometidos.

Actuaciones post-incidentes

- Análisis de lecciones aprendidas: Se debe realizar una revisión exhaustiva del incidente para identificar las lecciones aprendidas y las áreas de mejora en los procesos y políticas de seguridad existentes.

- Actualización de políticas y procedimientos: Basándose en el análisis post-incidente, se deben actualizar las políticas y procedimientos de seguridad para abordar las debilidades identificadas y mejorar la preparación y respuesta ante futuros incidentes de seguridad.

- Capacitación adicional del personal: Se deben programar sesiones de capacitación adicionales para educar al personal sobre las lecciones aprendidas del incidente y reforzar la importancia de seguir las políticas y procedimientos de seguridad establecidos.