Ejercicios de Análisis de Incidentes de Seguridad (Casos Reales)

Objetivo: Desarrollar la capacidad de análisis de incidentes, identificar las vulnerabilidades y proponer medidas de seguridad preventivas basadas en la realidad.

Estructura de la Respuesta (Para los tres ejercicios)

Los alumnos deben seguir la siguiente estructura para cada caso:

1. **Resumen de la Noticia:** Breve descripción del incidente, la empresa/organización afectada, la fecha del suceso y la fuente.
2. **Vulnerabilidad/Fallo de Seguridad (Causa Raíz):** Identificar el principal error técnico, humano o de proceso que permitió el incidente.
3. **Medidas de Prevención Propuestas (La Solución):** Enumerar y explicar *qué* debería haberse implementado para evitar el ataque o mitigar gravemente su impacto.

Ejercicio 1: Fuga de Datos y Petición de Rescate (Doble Amenaza)

Tipo de Incidente: Filtración masiva de datos sensibles seguida de extorsión (Ransom/Extorsión).

Instrucción:

Busca una noticia reciente (últimos 3 años) sobre una empresa o entidad que haya sufrido una brecha de datos donde los atacantes hayan robado información y, posteriormente, hayan solicitado un rescate (o hayan amenazado con publicarla/venderla).

Enfoca tu análisis en: ¿Qué medidas de protección de datos (cifrado, control de acceso, segmentación de red) habrían impedido el robo de la información, incluso si el atacante lograba acceder al sistema?

Preguntas guía para el alumno:

- ¿Qué tipo de información sensible fue expuesta? (Ej: datos personales, secretos comerciales, credenciales).

- ¿Qué sistemas de detección de intrusiones o gestión de eventos (SIEM) podrían haber alertado a la empresa antes de la extracción masiva de datos?
- Si los datos sensibles hubieran estado cifrados "en reposo" y "en tránsito", ¿habría esto inutilizado la información robada, minimizando la extorsión? Explica por qué.

Ejercicio 2: Multa de la AEPD por Mal Uso de Datos (Cumplimiento Legal)

Tipo de Incidente: Incumplimiento del Reglamento General de Protección de Datos (RGPD) o de la LOPDGDD que resulta en una sanción de la Agencia Española de Protección de Datos (AEPD).

Instrucción:

Busca una noticia sobre una sanción impuesta por la AEPD a una gran empresa (ej. sector telecomunicaciones, banca, o e-commerce) debido a un mal manejo o tratamiento inadecuado de los datos de sus clientes. Esto podría ser por no garantizar el derecho de acceso, por una cesión incorrecta de datos o por una seguridad insuficiente.

Enfoca tu análisis en: ¿Qué obligaciones del RGPD se han incumplido? ¿Qué políticas de privacidad, evaluaciones de impacto (EIPD) o medidas técnicas organizativas (MTO) son obligatorias para prevenir este tipo de infracciones?

Preguntas guía para el alumno:

- Identifica el artículo o principio del **RGPD** que la empresa ha violado.
- ¿Cómo una **Auditoría de Seguridad Periódica** y una correcta **Gestión de Consentimientos** (si aplica) habrían evitado la multa?
- Propón una **Medida Organizativa** (procedimiento, formación de empleados) y una **Medida Técnica** (configuración de sistemas) para garantizar la correcta gestión de los datos de clientes en esa situación.

Ejercicio 3: Ataque de Ransomware y Paralización Operativa (Disponibilidad)

Tipo de Incidente: Ataque de *ransomware* que cifra los sistemas de una empresa, afectando gravemente su capacidad de operar.

Instrucción:

Busca una noticia sobre una empresa (PYME o gran corporación) que haya sido víctima de un ataque de ransomware y haya tenido que paralizar sus operaciones (producción, servicios al cliente, etc.) durante un periodo significativo.

Enfoca tu análisis en: ¿Qué medidas de *hardening*, sistemas de respaldo y protocolos de recuperación deberían haber estado en vigor para restaurar las operaciones sin tener que pagar el rescate?

Preguntas guía para el alumno:

- ¿Cómo pudo el *ransomware* penetrar en la red (ej. correo de *phishing*, escritorio remoto no protegido, vulnerabilidad de software)?
- Describe la **Estrategia de Copias de Seguridad (Backup)** que debe tener la empresa, mencionando específicamente la **regla 3-2-1** y la importancia del almacenamiento *offline* o inmutable.
- Si la empresa hubiera tenido un **Plan de Continuidad de Negocio (BCP)** y un **Plan de Recuperación ante Desastres (DRP)**, ¿cuánto tiempo estimas que se habría reducido el tiempo de inactividad? Justifica tu respuesta.