EJERCICIO: Problema para la materia de Seguridad de la Información utilizando Aprendizaje Basado en Problemas (ABP).

Donde desarrollarán un proyecto donde den soluciones efectivas a este ejemplo. Usen su gran ingenio y el trabajo en equipo.

Título del Problema:

Respuesta y Fortalecimiento de Seguridad en una Empresa Industrial tras un Ataque Informático

Escenario:

La empresa **INDUSTRIAS MECATRONIX S.A. de C.V.**, dedicada a la manufactura automatizada de componentes electrónicos, sufrió un ataque informático que comprometió sus sistemas de producción y gestión de inventario. El incidente ocurrió a través de un ataque de ransomware que cifró archivos críticos, paralizando la cadena de producción y afectando el control de calidad de sus productos.

El departamento de TI detectó que la intrusión ocurrió debido a una vulnerabilidad en un servidor desactualizado y la falta de un sistema adecuado de detección de intrusos. A raíz de este ataque, la empresa perdió datos valiosos, tuvo retrasos en la entrega de productos y sufrió un daño en su reputación ante clientes y socios comerciales.

La directiva de la empresa ha solicitado un plan de respuesta y fortalecimiento de la seguridad de la información para evitar futuros ataques y garantizar la continuidad del negocio.

Retos para los estudiantes:

Los alumnos deberán analizar el ataque, identificar vulnerabilidades, evaluar los riesgos y proponer un plan de acción para mitigar futuras amenazas.

Deben responder a las siguientes preguntas clave:

1. ¿Cómo pudo haberse prevenido el ataque?
2. ¿Qué vulnerabilidades fueron explotadas y cómo se pueden corregir?
3. ¿Cuáles son las mejores prácticas para mejorar la seguridad de la empresa?
4. ¿Cómo garantizar la continuidad de las operaciones en caso de otro ataque?
5. ¿Qué medidas se pueden implementar para concienciar a los empleados sobre ciberseguridad?

Propuestas de Solución:

1. **Implementación de un Sistema de Respuesta ante Incidentes (CSIRT)**

- Establecer un equipo de respuesta a incidentes de seguridad (CSIRT) encargado de gestionar ataques futuros.
- Definir un protocolo de acción en caso de ciberataques, incluyendo copias de seguridad, aislamiento de sistemas comprometidos y comunicación con las autoridades.

2. **Refuerzo de la Seguridad en la Red y Sistemas**
    - Implementar firewalls avanzados y sistemas de detección de intrusos (IDS/IPS) para monitorear y bloquear actividades sospechosas.
    - Aplicar segmentación de red para evitar la propagación de malware dentro de la infraestructura de la empresa.
    - Configurar registros detallados de auditoría para detectar accesos no autorizados.
3. **Política de Actualización y Gestión de Parches de Seguridad**
    - Desarrollar un plan de mantenimiento y actualización periódica de todos los sistemas y software utilizados en la empresa.
    - Implementar herramientas de gestión de parches automatizados para cerrar brechas de seguridad.
4. **Capacitación en Ciberseguridad para el Personal**
    - Realizar campañas de concienciación en seguridad informática y entrenamientos regulares sobre buenas prácticas en ciberseguridad.
    - Simular ataques de phishing para evaluar la preparación del personal y reforzar la educación sobre la identificación de amenazas.
5. **Implementación de una Estrategia de Respaldo y Recuperación**
    - Establecer copias de seguridad automáticas y cifradas en servidores externos o en la nube con acceso restringido.
    - Probar regularmente los planes de recuperación ante desastres para garantizar que los datos puedan restaurarse en caso de un ataque exitoso.

Conclusión

Este problema se pretende que los estudiantes apliquen sus conocimientos en seguridad informática dentro de un contexto industrial realista. A través del aprendizaje basado en problemas, desarrollarán habilidades críticas para identificar, analizar y mitigar amenazas cibernéticas en entornos empresariales.