Laboratorio 4 - Ciberseguridad en el sector comercio electrónico

Estudiante: Hernan Andres Gutierrez Anillo

Estructura del Laboratorio:

Pequeña Empresa de Comercio Electrónico
Perfil: Una empresa pequeña que vende productos en línea y almacena información de tarjetas de crédito.

1. Identificación de Activos Críticos
Explicación: Se introdujo el concepto de "activos críticos" dentro de una empresa de comercio electrónico. Estos son los recursos que deben protegerse para evitar pérdidas graves. Los activos críticos en una tienda online incluyen bases de datos, servidores web, información de clientes y, particularmente, los datos de tarjetas de crédito.

Ejercicio Grupal: Como grupo, discutimos qué activos consideramos más importantes. En nuestra empresa, los activos críticos serían:

-Base de datos de clientes: Contiene información personal y financiera.

-Servidores de la página web y plataformas de pago.

-Sistemas de gestión de inventarios.

Discusión: Clasificamos estos activos en términos de criticidad:

-Base de datos de clientes: De alta criticidad, ya que contiene información sensible.

-Servidores de la página web: De alta criticidad, ya que son esenciales para la venta online.

-Sistemas de gestión de inventarios: De media criticidad, ya que aunque son importantes, no representan un riesgo inmediato para la seguridad financiera.

Resultado: Estos activos deben recibir protección prioritaria, con medidas como cifrado de datos y acceso restringido.

2. Análisis de Amenazas y Riesgos
Explicación: Se discutieron diferentes tipos de amenazas cibernéticas que afectan a las empresas de comercio electrónico, como el phishing, malware, ransomware y DDoS. También se explicó cómo los ataques pueden afectar cada uno de los activos de la empresa.

Ejercicio Grupal: Junto con mi grupo, analizamos las amenazas que podrían afectar los activos críticos que identificamos previamente. Estas amenazas fueron:

-Phishing: Puede afectar a los empleados al intentar obtener acceso a credenciales de sistemas críticos.

-Malware/Ransomware: Puede cifrar las bases de datos de clientes y servidores, haciendo que los datos sean inaccesibles.

-DDoS (Denegación de Servicio Distribuida): Puede afectar la disponibilidad del sitio web, lo que impediría a los clientes realizar compras.

Discusión: Priorizamos las amenazas en función del riesgo que representan:

-Phishing: Alto riesgo debido a la posibilidad de acceso a cuentas administrativas.

-Ransomware: Alto riesgo debido al daño potencial a las bases de datos y la pérdida de datos sensibles.

-DDoS: Riesgo medio, ya que aunque afecta la disponibilidad, se puede mitigar con servicios de protección DDoS.

3. Formación del Equipo de Respuesta a Incidentes
Explicación: Se discutió la necesidad de un equipo de respuesta a incidentes bien estructurado. Los roles principales incluyen:

-Responsable de comunicaciones: Encargado de informar a empleados y clientes.

-Técnico de sistemas: Encargado de analizar el incidente y aplicar soluciones técnicas.

-Legal: Encargado de gestionar la comunicación con entidades regulatorias y clientes.

-Responsable de recuperación de datos: Encargado de restaurar los sistemas a su estado normal.

Ejercicio Grupal: Se asignaron roles dentro de nuestro equipo simulado:

-Comunicaciones: Yo me encargué de las comunicaciones, y elaboré un plan para notificar a los clientes y empleados sobre el incidente.

-Técnico de sistemas: Un compañero se encargó de analizar el incidente, con especial énfasis en cómo contenerlo.

-Legal: Otro miembro del grupo gestionó la parte legal, asegurando que cumpliéramos con las regulaciones sobre protección de datos.

Discusión: Creamos una lista de contactos de emergencia que incluiría a todos los miembros del equipo y personas clave dentro de la empresa.

4. Desarrollo de Procedimientos de Detección
Explicación: Se habló sobre la importancia de la detección temprana de incidentes, utilizando herramientas como el monitoreo de logs, la detección de anomalías y sistemas de alertas en tiempo real.

Demostración: Se mostró cómo revisar los logs de seguridad y cómo detectar patrones sospechosos, como intentos de acceso no autorizado.

Ejercicio Grupal: Diseñamos un procedimiento básico para la detección de incidentes en nuestra empresa. Este procedimiento incluiría:

Monitoreo de logs de acceso y actividad del servidor.

Configuración de alertas automáticas cuando se detecten actividades inusuales.

Revisión periódica de patrones de tráfico web para detectar ataques DDoS.

5. Elaboración del Plan de Contención
Explicación: Se explicó que la contención de un incidente es vital para evitar que se propague y cause más daño.

Ejercicio Grupal: Junto con el equipo, diseñamos un plan de contención que incluiría:

-Aislamiento de sistemas afectados: Desconectar los servidores comprometidos.

-Desactivación temporal de accesos: Limitar el acceso a las bases de datos.

-Notificación al equipo de respuesta: Informar inmediatamente al equipo de incidentes para activar el plan de acción.

6. Plan de Recuperación y Continuidad del Negocio
Explicación: Se presentó un enfoque estructurado para la recuperación, que incluye la restauración de datos desde copias de seguridad y la reactivación de los sistemas afectados.

Ejercicio Grupal: Elaboramos un plan de recuperación que incluiría:

-Restauración desde copias de seguridad periódicas.

-Notificación a los clientes sobre el incidente y el estado de la recuperación.

-Pruebas regulares de restauración para asegurar la integridad de los datos.

7. Conclusiones y Preguntas
Recapitulación: Durante el taller, aprendimos sobre la importancia de identificar activos críticos, las amenazas que podrían afectarlos y cómo estructurar un plan de respuesta ante incidentes.