Sesión #4 Ciberseguridad en el sector comercio electrónico

Nombre de la Empresa: "Café y Tradición Online"
Descripción: Es una pequeña empresa en línea ubicada en Valledupar, Colombia, que se dedica a la venta de productos relacionados con el café, como granos de café orgánico, cafeteras, accesorios para baristas y productos autóctonos del país.
Almacenamiento de Información: Ofrecen pagos en línea y almacenan de manera segura la información de las tarjetas de crédito de sus clientes para facilitar las futuras compras.

Objetivo del taller:

1. Concienciar sobre la importancia de la **ciberseguridad** en el comercio electrónico, protegiendo la información confidencial de los clientes y la reputación de la empresa.
2. Identificar los riesgos cibernéticos y las posibles vulnerabilidades en sistemas que manejan datos sensibles.
3. Implementar buenas prácticas para el manejo seguro de la información financiera, como el uso de protocolos de cifrado, sistemas de detección de fraudes y el cumplimiento de normativas legales como PCI DSS.

Paso 1: **Identificación de Activos Críticos**

Objetivo: Identificar los activos esenciales que deben ser protegidos para garantizar la continuidad y la seguridad de la empresa.

Actividades Detalladas:

1. **Explicación:**
    - Los activos críticos son aquellos recursos, tanto físicos como digitales, indispensables para el funcionamiento y éxito de la empresa. Protegerlos asegura la continuidad del negocio y la confianza de los clientes.
    - Resalta la importancia de proteger activos como las bases de datos de clientes, información financiera, infraestructura tecnológica y el sitio web.
2. **Ejercicio Grupal:**
    - Divide a los participantes en pequeños grupos.
    - Solicita que enumeren los activos clave de "Café y Tradición Online". Algunos ejemplos relevantes podrían incluir:
        - **Bases de datos de clientes**: Contiene información personal y financiera de los clientes.
        - **Sitio web de comercio electrónico**: Es la principal plataforma de ventas.

        - **Servidor de almacenamiento**: Donde se guarda la información crítica, como pedidos y transacciones.
        - **Sistemas de pago**: Procesos y datos relacionados con las tarjetas de crédito.
        - **Marcas y patentes**: Protege la identidad comercial de la empresa.
    - Cada grupo presenta sus resultados en una pizarra o documento colaborativo.

3. **Discusión:**
    - Clasifica los activos listados según su nivel de criticidad (por ejemplo, **alto**, **medio**, **bajo**) y prioridad para ser protegidos. Esto podría estructurarse como:
        - Nivel Alto: Bases de datos de clientes y sistemas de pago.
        - Nivel Medio: Servidores y sitio web.
        - Nivel Bajo: Materiales de marketing o accesorios físicos de baja sensibilidad.

Paso 2: **Análisis de Amenazas y Riesgos**

Actividades Detalladas:

1. **Explicación:**
    - Amenazas cibernéticas: "Son eventos o acciones malintencionadas que pueden comprometer la seguridad de los activos críticos de una empresa."
        - **Phishing:** Intentos de suplantación de identidad para robar datos de clientes.
        - **Malware:** Software malicioso que podría infectar los servidores o bases de datos.
        - **Ransomware:** Ataques que bloquean el acceso a los datos a menos que se pague un rescate.
        - **DDoS:** Ataques de denegación de servicio que podrían paralizar el sitio web.

2. **Ejercicio Grupal:**
    - Activos críticos previamente identificados, como:
        - Bases de datos de clientes.
        - Servidores de almacenamiento.

        - Sistemas de pago en línea.
        - Sitio web de comercio electrónico.
    - Solicita que, para cada activo crítico, los participantes identifiquen posibles amenazas específicas. Ejemplo:
        - Amenaza para la base de datos de clientes: Phishing dirigido a empleados para acceder a información sensible.

3. **Discusión:**

- Analiza con los participantes el impacto financiero y reputacional de cada amenaza si llegara a materializarse.
- Discute posibles medidas para mitigar estos riesgos, como formación en ciberseguridad, uso de firewalls, y sistemas de respaldo.

Paso 3: **Formación del Equipo de Respuesta a Incidentes**

Objetivo: Definir los roles y responsabilidades necesarias para responder de manera efectiva a incidentes de seguridad cibernética.

Actividades Detalladas:

1. **Explicación:**
    - Presenta los objetivos de un equipo de respuesta a incidentes (ERI): "Un ERI está diseñado para identificar, gestionar y mitigar incidentes de seguridad, asegurando la rápida recuperación y minimizando el impacto en la empresa."
    - Describe las funciones principales dentro de un equipo:
        - **Responsable de Comunicaciones:** Se encarga de informar a las partes interesadas internas y externas, incluyendo empleados, clientes y medios de comunicación.
        - **Especialista Técnico de Sistemas:** Encargado de contener el incidente y restaurar los sistemas afectados.
        - **Representante Legal:** Gestiona los aspectos legales relacionados con el incidente, como el cumplimiento normativo y la interacción con las autoridades.
        - **Director de Respuesta (Líder del Equipo):** Coordina al equipo, toma decisiones clave y asegura el progreso de las acciones.
        - **Relaciones con Clientes:** Brinda información y soporte a los clientes afectados.
2. **Ejercicio Grupal:**

- Formación de un ERI:
    - Divide a los participantes en pequeños grupos y asigna a cada grupo la tarea de definir roles específicos para un equipo simulado en "Café y Tradición Online".
    - Proporciona escenarios hipotéticos de incidentes, como una filtración de datos de clientes o un ataque ransomware, para que identifiquen cómo responder según los roles asignados.
- Asignación de roles:
    - **Yordin:** Líder del equipo.
    - **Yordin:** Técnico de sistemas.
    - **Jorge Ivan:** Responsable de comunicaciones.
    - **Rigoberto:** Representante legal.
    - **Jorge Ivan:** Relaciones con clientes.

3. **Discusión:**
    - Pide a los grupos que compartan un listado de contactos clave de emergencia, que podría incluir:
        - Proveedor de servicios tecnológicos.
        - Consultores en ciberseguridad.
        - Representante legal externo.
        - Autoridades locales o nacionales (como la Policía Cibernética en Colombia).
    - Discute las responsabilidades de cada rol en un plan de respuesta a incidentes, y asegúrate de que haya un consenso sobre los pasos a seguir en caso de crisis.

Paso 4: **Desarrollo de Procedimientos de Detección**

Actividades Detalladas:

1. **Explicación:**
    - **Detección de incidentes**:
      La detección temprana permite identificar actividades sospechosas o posibles amenazas antes de que afecten los activos críticos de la empresa.
    - Explica herramientas y técnicas clave para la detección de incidentes:
        - **Monitoreo de logs:** Registros de actividad en sistemas, aplicaciones y redes que sirven para identificar patrones anómalos.
        - **Sistemas de detección de anomalías:** Software que utiliza algoritmos para detectar comportamientos inusuales, como accesos no autorizados.
        - **Alertas proactivas:** Configuración de sistemas de monitoreo que envían notificaciones cuando se detecta un incidente potencial.
        - Ejemplos de herramientas: SIEM (Security Information and Event Management), sistemas de monitoreo como Splunk o SolarWinds.
2. **Demostración:**

    Ejemplo:

        - Accede al servidor de la empresa ficticia y habilita el registro de actividades (logs).
        - Configura parámetros básicos de detección, como alertas para accesos en horarios inusuales o intentos repetidos de inicio de sesión fallidos.
        - Explica cómo interpretar los logs y cómo identificar eventos anómalos, como direcciones IP desconocidas o cambios no autorizados en configuraciones.
3. **Ejercicio Grupal:**
        - Identificar los puntos clave de monitoreo (sitio web, bases de datos, sistemas de pago).
        - Establecer una periodicidad para revisar los logs (diaria, semanal, según el nivel de actividad).
        - Configurar alertas automáticas para eventos críticos.
        - Definir cómo se comunicarán los incidentes detectados al Equipo de Respuesta a Incidentes.

Paso 5: **Elaboración del Plan de Contención**

Actividades Detalladas:

1. **Explicación:**
    - **La importancia de la contención:**
      La contención es crucial durante un incidente de seguridad para evitar que se propague y cause mayores daños. Actuar rápidamente puede proteger los activos críticos, preservar evidencia para análisis posteriores y garantizar la continuidad del negocio.
    - Medidas comunes de contención:
        - Aislar sistemas afectados para evitar la propagación de malware.
        - Desconectar redes comprometidas para mitigar accesos no autorizados.
        - Implementar controles temporales mientras se desarrolla una solución completa.
2. **Ejercicio Grupal:**
    - Divide a los participantes en pequeños grupos y pídeles que creen un plan de contención básico para la empresa ficticia "Café y Tradición Online". Algunas acciones clave a incluir en el plan podrían ser:
        - **Detección Inicial:** ¿Cómo identificar un incidente rápidamente? (Por ejemplo, monitoreo de alertas o informes de anomalías).
        - **Aislamiento de Sistemas:** ¿Qué sistemas deben desconectarse primero? (Bases de datos, servidores de pago, sitio web).
        - **Notificación:** ¿Quién debe ser informado dentro del Equipo de Respuesta a Incidentes? Establece un flujo de comunicación claro.
        - **Medidas Temporales:** Uso de herramientas de respaldo para mantener operaciones críticas mientras se resuelve el problema.
    - Cada grupo puede presentar un borrador de su plan de contención.
3. **Discusión:**
        - ¿Qué medidas son más efectivas para minimizar el impacto?
        - ¿Hay pasos adicionales que deberían incluirse, como contacto con proveedores externos o autoridades?

Paso 6: **Plan de Recuperación y Continuidad del Negocio**

Actividades Detalladas:

1. **Explicación:**
    - Mejores prácticas para recuperación de datos y continuidad del negocio:
        - **Copias de seguridad:** Mantener respaldos actualizados y almacenarlos en ubicaciones seguras, preferiblemente externas o en la nube.
        - **Restauración efectiva:** Implementar procedimientos claros para restaurar datos críticos de manera rápida y eficiente.
        - **Notificación a clientes:** Comunicar de forma transparente los incidentes y las acciones tomadas para proteger su información.
        - **Planes de redundancia:** Configurar sistemas alternativos para mantener las operaciones durante interrupciones (por ejemplo, usar una plataforma secundaria para ventas).
2. **Ejercicio Grupal:**
    - Solicitar a los participantes que elaboren un plan básico de recuperación para "Café y Tradición Online" que contemple los siguientes puntos:
        - **Identificación de datos críticos:** ¿Qué datos deben recuperarse primero? (Ejemplo: bases de datos de clientes y sistemas de pago).
        - **Fuente de recuperación:** Uso de copias de seguridad o sistemas alternativos para restaurar los datos.
        - **Procedimientos:** Paso a paso para llevar a cabo la recuperación (ejemplo: desconectar sistemas afectados, realizar análisis de seguridad, restaurar datos, probar sistemas restaurados).
        - **Comunicación:** Crear un mensaje para clientes afectados, explicando las acciones tomadas y asegurando la continuidad del servicio.
3. **Discusión:**
    - Se simula un escenario de recuperación, como una filtración de datos en "Café y Tradición Online".
        - Los grupos deben aplicar sus planes de recuperación al escenario simulado y evaluar los resultados.

        - Discute qué aspectos funcionaron bien y cuáles podrían mejorarse. Pregunta:
            - "¿Cómo podríamos reducir los tiempos de recuperación?"
            - "¿Qué pasos adicionales podríamos incluir para fortalecer la continuidad del negocio?"

Paso 7: **Conclusiones y Preguntas**

Actividades Detalladas:

1. **Recapitulación:**
    - Resumen de los temas tratados:
        - **Identificación de Activos Críticos:** Cómo clasificar y priorizar los activos esenciales de la empresa.
        - **Análisis de Amenazas y Riesgos:** Evaluación de las amenazas más probables y su impacto.
        - **Formación del Equipo de Respuesta:** Importancia de roles claros y comunicación eficiente.
        - **Procedimientos de Detección:** Estrategias para la detección temprana de incidentes.
        - **Plan de Contención:** Medidas para limitar el impacto de los ataques.
        - **Plan de Recuperación y Continuidad del Negocio:** Proceso para restaurar datos y mantener operaciones activas.
2. **Preguntas y Respuestas:**
        - Resolver dudas sobre los conceptos abordados.
        - Compartir ideas o puntos que consideren clave en sus negocios reales o hipotéticos.
        - Proponer temas que les gustaría explorar más a fondo en el futuro.
3. **Cierre:**
    - Gracias por compartir sus ideas y energía durante este taller. Espero que los conceptos aprendidos les sean útiles para reforzar la seguridad de sus negocios.
    - Entrega material complementario, como:
        - Resúmenes del taller.
        - Guías de buenas prácticas de ciberseguridad.

- Recursos en línea o contactos útiles para consultas futuras.