Laboratorio 4: Ciberseguridad en el sector comercio electrónico

Paso 1: Identificación de Activos críticos

Actividades:

- **Concepto de Activos Críticos**

Son aquellos recursos que, si se ven comprometidos, pueden afectar seriamente la operación, la reputación y la viabilidad de la empresa.

- **Activos Críticos Identificados:**
  - **Base de Datos de Clientes:** Contiene datos personales y financieros.
  - **Servidor Web:** Hospeda el sitio de comercio electrónico.
  - **Sistema de Procesamiento de Pagos:** Conecta con pasarelas de pago como Stripe, Mercado Pago o PayPal.
  - **Backups (copias de seguridad):** Aseguran la recuperación ante incidentes.
  - **Cuentas Administrativas:** Permiten acceso a sistemas críticos.

- **Clasificación por Nivel de Criticidad**

1. Base de Datos de Clientes (Muy crítico)
2. Sistema de Procesamiento de Pagos (Muy crítico)
3. Servidor Web (Crítico)

4. Backups (Crítico)

5. Cuentas Administrativas (Crítico)

Paso 2: Análisis de Amenazas y Riegos

Actividades:

- Explicación:
  - **Phishing:** Robo de credenciales administrativas por medio de clonación de sitios legítimos falsos.
  - **Malware/Ransomware:** Encriptación de la base de datos o información importante de la empresa para posteriormente pedir dinero para rescatarla.
  - **Ataques DDoS:** Derribo del sitio web por medio de peticiones masivas a la página web volviéndola inaccesible prohibiendo la disponibilidad del sitio.
  - **Explotación de Vulnerabilidades:** Acceso no autorizado al servidor por medio de fallos en la seguridad del sitio.
- **Evaluación de Riesgos**
  - **Base de Datos de Clientes:** Riesgo alto de fuga de información sensible.
  - **Servidor Web:** Riesgo de indisponibilidad que afectaría las ventas del negocio.
  - **Sistema de Pagos:** Riesgo de fraude financiero y sanciones legales por si se presenta algún robo a algún cliente por nuestra culpa.
- **Prioridad de Mitigación:**
  - Proteger base de datos de clientes y sistema de pagos.

Paso 3: Formación del equipo de Respuestas a incidentes

Actividades:

- Explicación:

¿Qué es un Equipo de Respuesta a Incidentes?

Es un grupo organizado de personas responsables de preparar, detectar, analizar, contener, erradicar y recuperar frente a incidentes de seguridad informática que afectan a una organización en este caso el e-commerce.

El objetivo principal es minimizar el impacto de los incidentes, restaurar rápidamente las operaciones normales, **y** proteger los activos críticos de la empresa.

Miembros:

- **Responsable de Comunicaciones:** Se encarga de la comunicación interna y externa durante el incidente (ej. clientes, proveedores, autoridades). (Luis Silva)
- **Coordinador de Respuesta (Líder):** Dirige el equipo, toma decisiones críticas y mantiene informada a la dirección. (Cristian Cañate)
- **Técnico de Sistemas:** Apoya con la contención técnica: aislamiento de sistemas, recuperación de servidores. (Oscar)
- **Responsable Legal:** Evalúa el impacto legal, cumplimiento de normativas, y redacta notificaciones si es necesario
- **Coordinador de Seguridad:** Monitorea los sistemas, detecta incidentes y realiza el análisis forense. (Compañero)

- **Especialista de Soporte Técnico:** Ayuda en restaurar sistemas afectados y aplicar parches de seguridad.
- **Documentador:** Registra todo lo sucedido para análisis posterior, lecciones aprendidas y reportes formales.

Contactos de Emergencia

- Equipo interno de TI.
- Soporte técnico del proveedor de hosting.
- Autoridades regulatorias de protección de datos.

Paso 4: Desarrollo de procedimientos de detección

Actividades:

Descripción de herramientas y técnicas para monitorear Logs, detección de anomalías, y sistemas de alertas:

Para identificar incidentes de seguridad, es fundamental utilizar herramientas de **monitoreo**, **detección de anomalías** y **sistemas de alertas automáticas**. Estas herramientas permiten analizar los eventos que ocurren en los sistemas (como intentos de acceso, cambios de configuración o comportamientos inusuales) y generar alertas si se detecta algo anómalo.

Herramientas Comunes:

Herramienta	Función Principal
SIEM (Security Information and Event Management)	Centraliza, analiza y correlaciona logs de diferentes sistemas. (Ejemplo: Splunk, ELK Stack)
IDS/IPS (Sistema de Detección/Prevención de Intrusiones)	Detecta y bloquea tráfico sospechoso en redes. (Ejemplo: Snort, Suricata)
Monitorización de Logs (Syslog, Logwatch)	Revisa archivos de logs en busca de actividades anómalas.
Alertas Automatizadas (Fail2Ban, Wazuh)	Bloquea automáticamente IPs sospechosas o genera alertas ante eventos específicos.

Técnicas de Detección

Análisis de logs: Revisar registros de accesos, cambios de archivos, actividad de red.

Detección de anomalías: Identificar comportamientos que se desvían de los patrones normales (ej., inicio de sesión desde un país no habitual).

Correlación de eventos: Relacionar múltiples actividades sospechosas para detectar ataques más complejos (ej., escaneo de puertos seguido de intento de login).

Procedimiento Propuesto para la Empresa de E-Commerce

1. **Definir los logs a monitorear:**

   - Logs de accesos al servidor (auth.log).
   - Logs del servidor web (Apache/Nginx).
   - Logs de base de datos (MySQL, PostgreSQL).
   - Logs del firewall o IDS.

2. **Frecuencia de revisión:**

   - Revisión automática diaria (resumen).
   - Revisión manual semanal de logs críticos.

3. **Detección de anomalías:**

   - Crear alertas para más de 5 intentos de acceso fallido desde una misma IP en menos de 10 minutos.
   - Detectar cambios en archivos de configuración importantes (integridad de archivos).

4. **Herramientas para utilizar:**

   - **Fail2Ban** para bloqueo automático de IPs sospechosas.
   - **Logwatch** para resumen diario de eventos importantes.
   - **Snort** o **Wazuh** para detección avanzada de intrusiones.

5. **Acciones ante detección de incidentes:**

   - Notificar al equipo de respuesta a incidentes.
   - Aislar el sistema si se detecta actividad maliciosa confirmada.

- Registrar todos los eventos para posterior análisis.

Paso 5: Elaboración del Plan de Contención

Actividades:

¿Qué es la Contención en un Incidente de Seguridad?

Esta es el conjunto de acciones rápidas y planificadas que se toman para limitar el alcance y minimizar **los daños** de un incidente de seguridad, **antes** de que el incidente pueda propagarse a otros sistemas o afectar de manera más grave la infraestructura de la empresa.

¿Cuándo se realiza? inmediatamente después de detectar el incidente, pero antes de erradicar completamente la amenaza.

Acciones Inmediatas en Caso de Incidente

- Aislar el servidor afectado desconectándolo de la red.
- Cambiar contraseñas de acceso a los sistemas críticos.
- Notificar al equipo de respuesta a incidentes.
- Preservar los registros del sistema para análisis forense.

Objetivo: Limitar el daño y evitar propagación a otros sistemas.

Paso 6: Plan de Recuperación de recuperación y continuidad del negocio

Proceso de Recuperación:

Supongamos que sufrimos un ataque a nuestro e-commerce, esto es lo que haríamos para la recuperación y continuidad de nuestro negocio:

- Se restauraría los sistemas afectados desde backups verificados.
- Validaríamos la integridad de los datos antes de reactivar los servicios.
- Realizaríamos pruebas de seguridad antes de volver a operar de forma segura.

Continuidad del Negocio

- Mantener una copia de seguridad diaria automatizada.
- Tener proveedores alternativos para servicios críticos (ej. hosting y pasarela de pagos).
- Plan de comunicación transparente a clientes en caso de incidentes que afecten su información.

Objetivo: Minimizar la interrupción del servicio y restaurar la confianza de los clientes.

By: Luis Silva, Cristian Cañate, Oscar y el otro compañero