Laboratorio 4 – Ciberseguridad en el Comercio Electrónico

Integrantes:
anderson Smith iriarte Quintana

Roberto Carlos González Ferrer

Paso 1: Identificación de Activos Críticos

Activos Críticos Identificados:

Activo	Justificación	Nivel de Criticidad
Base de datos de clientes	Contiene información personal y financiera sensible	Alto
Sitio Web	Es el canal principal de ventas	Alto
Servidor web	Aloja la plataforma y APIs	Alto
Sistema de pago	Maneja transacciones con tarjeta de crédito	Alto
Backups en la nube	Soporte para recuperación ante fallos	Medio
Infraestructura de red interna	Permite la operación del negocio	Medio

Para mi la priorización de proteger la base de datos y el sitio web ya que una brecha puede significar pérdida financiera, legal y de confianza del cliente.

2. Análisis de Amenazas y Riesgos

Amenaza	Activo afectado	Riesgo	Probabilidad	Impacto
Phishing	Base de datos de clientes	Robo de credenciales	Alta	Alta
Ransomware	Servidor web, backups	Secuestro de información	Media	Alta
DDoS	Plataforma e-commerce	Inaccesibilidad al sitio	Alta	Media
Inyección SQL	Sistema de pago, BD	Acceso no autorizado	Media	Alta

Considero que el phishing y ataques DDoS se consideran los más probables, pero SQL injection y ransomware tienen impacto crítico si se ejecutan con éxito y no se mitigan.

3. Formación del Equipo de Respuesta a Incidentes

Rol	Responsable	Funciones
Coordinador General	Anderson Iriarte	Liderar la respuesta, coordinar acciones
Técnico de Sistemas	Roberto Gonzáles	Identificar y mitigar vulnerabilidades
Comunicación Externa	Sharith Minota	Manejo de prensa y usuarios
Legal y Cumplimiento	Oscar Parra	Contacto con autoridades, análisis legal

Contactos de Emergencia:

- Soporte hosting: soporte@empresa.com
- Equipo legal: legal@empresa.com

4. Procedimientos de Detección

Herramientas usadas:

- ***Fail2ban*:** Para bloqueo automático de IPs sospechosas
- ***AuditD*:** Para monitoreo de logs
- ***ClamAV*:** Antivirus en el servidor
- ***Snort*:** Detección de intrusos

Procedimiento Básico:

1. Revisión diaria de logs de acceso y error
2. Alertas y politicas automáticas configuradas en el servidor
3. Escaneo de integridad de archivos cada semana

5. Plan de Contención

Pasos del plan:

1. Aislamiento del sistema comprometido
2. Desconexión temporal de la red afectada
3. Notificación inmediata al equipo de incidentes
4. Activación de plan de respaldo si se compromete la disponibilidad
5. Análisis de logs y evidencias

6. Plan de Recuperación y Continuidad del Negocio

Proceso propuesto:

- **Recuperación:**
    - Restauración desde backups en la nube (retención diaria y semanal)
    - Escaneo de archivos restaurados
- **Continuidad:**
    - Activación de sitio alterno o versión mínima del e-commerce
    - Comunicación con clientes sobre el estado
    - Revisión de brechas para evitar recurrencias

Simulación: Se simula una infección de ransomware y se prueba el tiempo de restauración desde backup (2 horas aprox.)

7. Conclusiones y Preguntas

Conclusiones del taller:

- La ciberseguridad es un aspecto vital en la continuidad del comercio electrónico.
- La prevención, detección temprana y respuesta rápida son claves para minimizar daños.
- El equipo debe estar entrenado y actualizado en los procedimientos de seguridad.

8. Evaluación del Taller

Retroalimentación:

- El taller fue útil para aterrizar conceptos de seguridad en escenarios reales.
- Se recomienda hacer simulaciones más frecuentes con escenarios variados.
- Sugerencia: incluir herramientas automatizadas tipo SIEM en futuras sesiones.