Sesión #4 Ciberseguridad en el sector comercio electrónico

JULIANA TORRES AARÓN

Título del Laboratorio: Ciberseguridad en el sector comercio electrónico

Objetivos del Laboratorio:

1. Fortalecer la Seguridad de la Información y Protección de Datos Sensibles
2. Preparar a la Empresa para Responder Eficazmente ante Incidentes de Seguridad:
3. Diseñar las pautas para un Plan de Recuperación y Continuidad del Negocio
    - **Paso 1: Identificación de Activos Críticos**

Objetivo: Identificar los activos más críticos de la empresa que deben ser protegidos.

Actividades:

Explicación breve:

Los activos críticos son elementos fundamentales para la operación del negocio. Si son comprometidos, pueden causar daños financieros, legales o reputacionales.

Ejercicio grupal:

En grupos, los participantes deben listar los activos más importantes de su organización, tales como:

Plataforma web de ventas (e-commerce)

1. Base de datos de clientes Contiene: nombres, correos electrónicos, direcciones, datos de pago.
2. Información de tarjetas de crédito Procesada o almacenada.
3. Servidores y sistemas que alojan la web y base de datos
4. Cuentas de acceso administrativo: Usuarios con privilegios elevados.
5. Correos electrónicos corporativos: Para atención al cliente y comunicaciones internas.
6. Sistemas de respaldo (backups)

Discusión grupal:

- Clasificación por nivel de criticidad, considerando:
  Base de Datos de Clientes (Muy crítico)
  Sistema de Procesamiento de Pagos (Muy crítico)
  Cuentas Administrativas (Crítico)
  Servidor Web (Crítico)
  Backups (Crítico)Cuentas Administrativas (Crítico)

2. Análisis de Amenazas y Riesgos

Objetivo: Identificar amenazas probables y evaluar los riesgos para cada activo crítico.

Actividades:

Phishing (suplantación de identidad)

Malware (software malicioso)

Ransomware (secuestro de datos)

DDoS (ataques de denegación de servicio)

1. Base de Datos de Clientes

- Nivel de criticidad: Muy crítico
- Amenazas comunes: Robo de datos, acceso no autorizado, ransomware
- Impacto potencial: Pérdida de confianza del cliente, sanciones legales por incumplimiento de normativas, daño reputacional grave
- Probabilidad de ocurrencia: Alta

2. Sistema de Procesamiento de Pagos

- Nivel de criticidad: Muy crítico
- Amenazas comunes: Intercepción de pagos, malware financiero, fraude electrónico
- Impacto potencial: Robo de dinero, filtración de información financiera, consecuencias legales y regulatorias severas
- Probabilidad de ocurrencia: Alta

3. Cuentas Administrativas

- Nivel de criticidad: Crítico
- Amenazas comunes: Phishing, fuerza bruta, escalamiento de privilegios
- Impacto potencial: Control total del sistema por parte de atacantes, pérdida de datos, sabotaje o instalación de malware
- Probabilidad de ocurrencia: Media-Alta

4. Servidor Web (Plataforma de E-commerce)

- Nivel de criticidad: Crítico
- Amenazas comunes: DDoS, explotación de vulnerabilidades, defacement del sitio
- Impacto potencial: Inaccesibilidad del sitio, pérdida de ventas, daño a la reputación corporativa
- Probabilidad de ocurrencia: Media

5. Sistemas de Backups (Respaldos)

- Nivel de criticidad: Crítico
- Amenazas comunes: Ransomware, corrupción de datos, eliminación accidental o intencional
- Impacto potencial: Imposibilidad de recuperar datos, prolongación del impacto del incidente, incremento de pérdidas
- Probabilidad de ocurrencia: Media

3. Formación del Equipo de Respuesta a Incidentes (ERI)

Objetivo: Definir roles y responsabilidades claras para actuar frente a incidentes.

Actividades:

• Explicación:

¿En qué consiste un Equipo de Respuesta a Incidentes?

Se trata de un conjunto estructurado de personas encargadas de preparar, identificar, investigar, controlar, eliminar y recuperar frente a eventos de seguridad que afecten a una organización, en este caso una plataforma de comercio electrónico.

Su propósito fundamental es reducir al mínimo el impacto del incidente, restaurar las operaciones habituales lo antes posible y salvaguardar los recursos clave de la empresa.

Integrantes del equipo:

• Encargado de Comunicaciones:

Administra la información que se transmite tanto dentro de la empresa como hacia el exterior durante la gestión del incidente (clientes, proveedores, entidades oficiales). (Juliana Torres)

• Líder del Equipo de Respuesta:

Coordina todas las acciones del equipo, toma decisiones clave y mantiene actualizada a la alta dirección. (Nayid Castellar)

• Especialista en Sistemas:

Proporciona soporte técnico, ejecuta acciones de aislamiento de equipos afectados y ayuda en la recuperación de servidores.

(Un compañero que no me acuerdo el nombre)

• Asesor Legal:

Analiza los riesgos legales involucrados, asegura el cumplimiento normativo y elabora comunicaciones legales si corresponde.

• Responsable de Seguridad Informática:

Supervisa la infraestructura tecnológica, identifica anomalías y lleva a cabo análisis técnicos del incidente.

• Soporte Técnico Especializado:

Participa en la restauración de servicios y aplica actualizaciones o correcciones necesarias para evitar nuevas vulnerabilidades.

• Relator del Incidente:

Se encarga de documentar todos los hechos relevantes, para generar reportes, evaluar la respuesta y extraer aprendizajes futuros.

Contactos de Emergencia:

• Área interna de tecnología (TI)

• Soporte del proveedor de alojamiento web

• Entidades responsables de la protección de datos personales

4. Desarrollo de Procedimientos de Detección

Objetivo: Establecer mecanismos para detectar incidentes tempranamente.

Actividades:

- Herramientas clave: SIEM (Security Information and Event Management): Centraliza, analiza y correlaciona logs de diferentes sistemas (Ejemplo: Splunk).
- Monitoreo de logs: Revisa archivos de logs en busca de actividades anómalas.

- Detección de anomalías-sistemas de alertas (IDS/IPS, SIEM): Detecta y bloquea tráfico sospechoso en redes (Ejemplo: Snort,

5. Elaboración del Plan de Contención

Objetivo: Minimizar el impacto de un incidente mediante acciones inmediatas.

Actividades:

Crear un plan de contención que contemple:

- Aislamiento de sistemas afectados
- Corte de accesos o red si es necesario
- Notificación al ERI

6. Plan de Recuperación y Continuidad del Negocio

Objetivo: Restablecer operaciones y servicios tras un incidente.

Actividades:

Buenas prácticas para recuperación:

1. Restaurar desde backups
2. Verificación de integridad de datos
3. Comunicación con clientes y partes interesadas

Ejercicio grupal:

Elaborar un plan de recuperación incluyendo:

Pasos para restaurar servicios

1. Verificación de backups
2. Roles responsables
3. Tiempo estimado de recuperación