LABORATORIO 4 TALENTO TECH

CIBERSEGURIDAD

Juan Sebastián Rondón Garcés

UNIVERSIDAD POPULAR DEL CESAR

VALLEDUPAR

2025

Paso 1: Identificación de activos críticos

Base de datos de clientes: Es uno de los activos más valiosos, ya que permite personalizar la experiencia de compra. Además, la pérdida o filtración de estos datos puede resultar en robo de identidad, fraude financiero y daños irreparables a la reputación de la empresa.

Sitio web y plataforma de comercio electrónico: Si el sitio web se cae o es hackeado, puede interrumpir las ventas, lo que afectaría directamente los ingresos. Además, si se modifican o se roban datos del sitio (como las páginas de pago), puede perjudicar la confianza de los usuarios.

3. **Sistemas de pago (Pasarelas de pago):** El compromiso de estos sistemas puede permitir el robo de fondos y dañar la relación con los clientes si se detecta que sus datos no están seguros.

4. **Cuentas de administración (usuarios y contraseñas):** El acceso no autorizado a estas cuentas podría permitir a un atacante modificar precios, robar datos de clientes, o incluso cerrar el negocio de forma temporal.

Paso 2: Análisis de Amenazas y riesgos

Base de datos de clientes: Accesos no autorizados, Si un atacante obtiene acceso a la base de datos, puede robar información extremadamente valiosa como datos personales, números de tarjetas de crédito, direcciones, y otros detalles sensibles. Esto puede resultar en fraude, robo de identidad y un daño irreversible a la reputación de la empresa.

Cuentas administrativas: Las cuentas administrativas tienen acceso completo a los sistemas y datos críticos. Si un atacante obtiene acceso a estas cuentas, puede

modificar, robar o destruir datos importantes, o incluso tomar control total del sistema, comprometiendo toda la infraestructura del negocio.

Sitio web y plataforma de comercio electrónico: DDOS, Un ataque DDoS puede inundar el sitio web con tráfico masivo, dejándolo fuera de servicio. Esto interrumpe las operaciones de la tienda en línea, impide que los clientes compren y puede generar pérdidas económicas directas debido a la inaccesibilidad del sitio.

Sistemas de pagos: El malware puede interceptar las transacciones de pago o robar información sensible de las tarjetas de crédito de los clientes mientras están siendo procesadas. Esto puede resultar en pérdidas financieras y en un daño a la confianza de los clientes.

Paso 3: **Formación de equipos de respuestas a incidentes**

Leidy García – Técnica de Sistemas

Responsabilidad: Detectar y contener incidentes técnicos.

Carlos Gonzales – Responsable Legal

Responsabilidad: Gestionar las implicaciones legales y notificación de brechas.

Sofia Rodríguez– Responsable de Comunicaciones

Responsabilidad: Gestionar la comunicación interna y externa.

Enrique Ortega – Responsable de TI/Infraestructura

Responsabilidad: Recuperar sistemas y restaurar servicios afectados.

Angie Sánchez – Proveedor de Servicios de Seguridad Cibernética

Responsabilidad: Asistencia técnica en incidentes graves.

Laura Jiménez – Responsable de Seguridad

Responsabilidad: Evaluar riesgos y aplicar medidas de mitigación.

Paso 4: Desarrollo de procedimientos de detección

- Paso 1: Utilizar herramientas para como el visor de eventos para centralizar y analizar logs
- Paso 2: Analizar actividades inusuales como accesos fuera de hora y cambios de archivos
- Paso 3: Realizar escaneo de vulnerabilidades para ver procesos críticos
- Paso 4: Monitorear constantemente que todo esté en perfecto estado

Paso 5: Elaboración Del Plan de Contención

Aislamiento de manera inmediata: Desconectar temporalmente la base de datos del servidor público si se detecta un acceso no autorizado y quitar accesos a usuarios sospechosos.

Si el sitio está comprometido, redirigir a una página de mantenimiento mientras se investiga. Informar a los bancos asociados y bloquear transacciones sospechosas.

Otra cosa que se puede hacer es cambiar las contraseñas y bloquear los accesos no autorizados y activar la autenticación doble-factor si no esta habilitado, incluso si el

incidente es grave otra opción a tomar seria desconectar los servidores afectados de la red principal y restringir el acceso externos hasta que todo esté en perfecto estado

Paso 6: Plan de recuperación y continuidad del negocio

- Una vez ha pasado el incidente se pueden usar copias de seguridad recientes, y verificar que las copias de seguridad estén en buen estado (integridad) antes de restaurar
- Revisar que los datos restaurados no estén contaminados o alterados y verificar que todo funciona perfectamente
- Limpiar los dispositivos comprometidos y volver a instalar los software desde fuentes verificadas si es necesario
- Finalmente aplicar parches de seguridad antes de poner el servidor en línea para que no se vuelva a repetir el mismo incidente

Paso 7: Conclusiones y Preguntas

Contar con un buen plan de seguridad ayuda a proteger los activos más importantes de la empresa y a reaccionar rápido ante cualquier incidente. Identificar riesgos, tener un equipo preparado, detectar amenazas a tiempo y saber cómo contener y recuperar los sistemas afectados es clave para mantener el negocio en funcionamiento, es decir es importante identificar vulnerabilidades, en caso de comportamientos inusuales aplicar medidas de seguridad inmediatas y también si termina sucediendo un incidente grave hacer las medidas necesarias para la recuperación y verificar que todo este en perfecto estado, además esto servirá de experiencia para que no se vuelvan a repetir las mismas situaciones, mejorando así la seguridad del sistema