Dilan Aragón

Roberto Blanco

Rubén Ariza

Laboratorio 4 Ciberseguridad

Objetivo:

Sensibilizar sobre la importancia de la ciberseguridad y capacitar en la identificación, análisis y respuesta ante incidentes de seguridad en el entorno del comercio electrónico.

Paso 1

1. ¿Qué es un activo crítico en una empresa de comercio electrónico?

   /R. Es un recurso esencial para el funcionamiento y seguridad del negocio, cuya pérdida o compromiso afectaría gravemente la operación. Ejemplos: base de datos de clientes, sistema de pagos, sitio web.

2. Menciona tres activos críticos que debe proteger una tienda en línea.

   /R.
   - - Base de datos de clientes
   - - Plataforma de pagos
   - - Sitio web de ventas

3. ¿Cómo se clasifica un activo según su nivel de criticidad?

   /R. Se evalúa su importancia con base en el impacto de su pérdida y la probabilidad de que sea atacado. Se clasifica como: Alta, Media o Baja criticidad.

Paso 2

1. ¿Qué es una amenaza cibernética?

   /R. Es cualquier posible evento malicioso que pueda dañar, robar o interrumpir los activos digitales de la empresa.

2. Menciona cuatro amenazas comunes en comercio electrónico.

   /R.

   - Phishing
   - Malware
   - Ransomware
   - Ataques DDoS

3. ¿Qué factores se consideran para evaluar el riesgo de un activo?

   /R. La probabilidad de que sea atacado y el impacto que tendría dicho ataque.

Paso 3

1. ¿Cuál es el propósito de un equipo de respuesta a incidentes?

   /R. Coordinar y ejecutar acciones para responder rápidamente a incidentes de seguridad y mitigar su impacto.

2. Menciona tres roles dentro del ERI – asignar roles.

   /R.

Nombre	Rol Asignado	Funciones Principales
Dilan	Coordinador de Incidentes	Lidera la respuesta, toma decisiones clave, organiza y dirige al equipo.
Roberto	Técnico de Sistemas	Analiza logs, contiene el incidente, apoya la restauración de sistemas.
Rubén	Responsable de Comunicaciones	Informa a clientes, medios y autoridades; mantiene la imagen de la empresa.
Dilan	Representante Legal	Garantiza el cumplimiento normativo y maneja implicaciones legales del incidente.
Roberto	Responsable de Seguridad (CISO)	Supervisa herramientas de ciberseguridad y actualiza políticas y controles preventivos.

3. Crear un listado de contactos de emergencia y responsabilidades

/R.

Nombre	Cargo/Rol	Correo De Contacto	Responsabilidad Principal
Dilan	Coordinador / Legal	dilan@empresa.com	Dirige la respuesta y maneja los temas legales
Roberto	Técnico / CISO	roberto@empresa.com	Contención técnica y supervisión de seguridad
Rubén	Comunicaciones	ruben@empresa.com	Comunicación con clientes y medios externos

Paso 4

1. Explicación:
   La detección temprana de amenazas es clave en la ciberseguridad. Para lograrlo, se utilizan herramientas que permiten:
   - **Monitoreo de logs**: Registros de eventos del sistema, red y aplicaciones.
   - **Sistemas de detección de intrusos (IDS**): Detectan accesos no autorizados.
   - **Análisis de comportamiento**: Identifican actividades anómalas.
   - **Alertas automatizadas**: Notifican eventos críticos en tiempo real.

2. Demostracion:

   # Ver logs del sistema en tiempo real

   tail -f /var/log/syslog

   # Buscar errores críticos

   grep "CRITICAL" /var/log/syslog

   # Ver accesos al sistema

   cat /var/log/auth.log

3. Diseñar un procedimiento básico de monitoreo para su empresa

   /R.

Paso	Actividad	Responsable
1	Configurar el monitoreo de logs del servidor web	Roberto
2	Implementar alertas por correo para errores críticos	Dilan
3	Revisar logs de acceso diariamente	Rubén
4	Detectar cambios sospechosos en archivos del sistema	Roberto
5	Generar un informe semanal de incidentes detectados	Dilan
6	Reunión semanal de revisión de alertas y actualización del plan	Rubén

Paso 5

1. Explicar la importación de la contención en la respuesta a incidentes.
   /R
   La **contención** es una etapa crítica en la respuesta a incidentes. Su propósito es **limitar la propagación** del ataque y **preservar la integridad de los sistemas**. Una respuesta rápida y organizada puede evitar pérdidas mayores y facilitar la recuperación.
2. Crear un plan de contención que incluye el aislamiento de sistemas afectados, desconexión de redes, y notificación al equipo de respuesta.
   /R

Paso	Acción	Responsable
1	Detectar y confirmar el incidente	Coordinador (Roberto)
2	Aislar los sistemas comprometidos (servidores, endpoints, etc.)	Técnico de Sistemas (Roberto)
3	Desconectar los sistemas afectados de la red	Técnico de Sistemas (Roberto)
4	Notificar al equipo de respuesta y al CISO	Responsable de Comunicaciones (Rubén)
5	Activar canales seguros para la coordinación	Coordinador (Dilan)
6	Documentar todas las acciones tomadas para análisis posterior	Todos los involucrados

3. Revisión de los plenes elaborados y retroalimentación.
   /R
   Durante esta etapa se revisan los planes desarrollados por cada grupo o equipo, se identifican posibles debilidades (por ejemplo, falta de notificación o demoras en el aislamiento), y se brindan recomendaciones para mejorar su efectividad en futuros incidentes.

Paso 6

1. Presentar las mejores prácticas para la recuperación de datos y la continuidad del negocio tras un incidente.
   /R
   - Realizar **copias de seguridad periódicas** (diarias o semanales).
   - Almacenar respaldos en **ubicaciones seguras** (físicas y en la nube).
   - Tener un **plan documentado** de recuperación ante desastres.
   - Priorizar la recuperación de los **servicios más críticos**.
   - Mantener canales de **comunicación con clientes y stakeholders**.
   - Realizar **pruebas de restauración** regularmente para validar el plan.
2. Elaborar un plan de recuperación, incluyendo restauración desde copias de seguridad y notificación a clientes.
   /R

Paso	Acción	Responsable
1	Confirmar la integridad de las copias de seguridad	Técnico de Sistemas (Roberto)
2	Restaurar los sistemas críticos desde respaldo	Técnico de Sistemas (Roberto)
3	Verificar el funcionamiento correcto del sistema restaurado	Coordinador (Dilan)
4	Notificar a los clientes sobre la restauración y tiempo estimado	Comunicaciones (Rubén)
5	Evaluar la causa raíz y actualizar el plan de prevención	Responsable de Seguridad (Roberto como CISO)
6	Documentar todo el proceso de recuperación para auditoría	Todos los involucrados

3. Simulación de un escenario de recuperación y evaluación de la respuesta.
   /R
   Se realiza una **simulación de recuperación**, evaluando la rapidez, efectividad y comunicación interna/externa. Se discuten oportunidades de mejora, tiempos de respuesta y se plantean nuevas medidas para reducir el tiempo de inactividad en el futuro.