Fase 3.1 - Plan de respuesta a incidentes y certificación

Introducción

Este plan tiene como objetivo estabelcer un marco claro y estructurado para responder de manera eficiente a futuros incidentes de seguridad. Basado en la guía del NIST SP 800-61, se enfoca en las fases clave: **Preparación, Identificación, Contención, Erradicación, Recuperación y Lecciones Aprendidas.**

---

1. Preparación

Formación de un equipo de respuesta a incidentes (CSIRT):

- Miembros clave: Administradores de red, expertos en ciberseguridad, personal de TI, y responsables legales.
- Roles definidos: Líder de incidente, analista forense, coordinador de comunicaciones.

Políticas y procedimientos:

- Actualizar y documentar políticas de seguridad.
- Realizar simulacros periódicos de incidentes.
- Implementar herramientas como SIEM para monitoreo en tiempo real.

Inventario actualizado:

- Catalogar sistemas, servicios y usuarios críticos.
- Mantener un registro de configuraciones y credenciales.

2. Identificación

- **Detección del incidente:**
  - Monitorear logs y alertas generadas por herramientas como chkrootkit, rkhunter y sistemas de detección de intrusiones (IDS).
  - Identificar actividades inusuales, como inicios de sesión sospechosos, transferencias masivas de datos, o cambios en configuraciones.
- **Confirmación del incidente:**
  - Analizar evidencias usando herramientas forenses.
  - Determinar el alcance y la naturaleza del incidente.

---

3. Contención

- **Contención a corto plazo:**
  - Desconectar sistemas comprometidos de la red.
  - Detener servicios afectados (por ejemplo, `systemctl stop`).
  - Bloquear direcciones IP sospechosas con `iptables` o `ufw`.

- **Contención a largo plazo:**
  - Crear entornos aislados (sandbox) para analizar malware.
  - Implementar parches y configuraciones temporales para mitigar riesgos.

---

4. Erradicación

- **Eliminación de amenazas:**
  - Identificar y eliminar archivos maliciosos y backdoors.
  - Deshabilitar cuentas de usuario no autorizadas.
  - Corregir configuraciones vulnerables en servicios como SSH y FTP.

- **Análisis forense:**
  - Realizar un escaneo completo del sistema con herramientas avanzadas.
  - Revisar logs históricos para identificar el punto de acceso inicial.

5. Recuperación

- **Restauración del sistema:**
  - Reconstruir sistemas comprometidos a partir de respaldos seguros.
  - Asegurarse de que los servicios esenciales funcionen correctamente antes de reconectarlos a la red.

- **Pruebas de integridad:**
  - Verificar que no queden remanentes de malware.
  - Confirmar la funcionalidad de las medidas de seguridad implementadas.

---

6. Lecciones Aprendidas

- **Evaluación post-incidente:**
  - Documentar el tiempo de respuesta, impacto y medidas efectivas.
  - Identificar áreas de mejora en el plan de respuesta.

- **Actualización del plan:**
  - Ajustar políticas y procedimientos según los hallazgos del incidente.
  - Implementar soluciones permanentes para prevenir incidentes similares.

6. Recomendaciones Extra (opcionales pero muy recomendables)

- **Fortalecer la configuración de seguridad:**
  - Deshabilitar `PermitRootLogin` y `PasswordAuthentication` en SSH.
  - Utilizar claves SSH y acceso restringido por IP.

- **Implementar un firewall avanzado:**
  - Bloquear puertos innecesarios y restringir accesos externos.

- **Capacitación de empleados:**
  - Sensibilizar sobre phishing y mejores prácticas de seguridad.

- **Auditorías regulares:**
  - Revisar configuraciones y realizar pruebas de penetración periódicas.

Con este plan, la organiazción estará mejor preparada para responder de manera eficiente a incidentes de seguridad, minimizando su impacto y mejorando continuamente su postura de ciberseguridad.