Fase 3.4 - Sistema de Gestión de Seguridad de la Información (SGSI)

Introducción

Este Sistema de Gestión de Seguridad de la Información (SGSI), conforme a ISO 27001, establece un marco completo para gestionar la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos críticos. Está diseñado considerando los hallazgos y mejoras implementadas en el sistema comprometido durante todas las fases anteriores del proyecto.

---

1. Análisis de Riesgos

El análisis de riesgos es un componente esencial para identificar amenazas y vulnerabilidades. Se ejecutaron los siguientes pasos:

1.1 Identificación de Activos Críticos

Hardware y software:

- Máquina virtual Debian (IP: 192.168.1.137).
- Servicios: OpenSSH, Apache, MariaDB.

Información crítica:

- Logs del sistema (`/var/log/auth.log`, `/var/log/syslog`).
- Configuraciones sensibles (`/etc/ssh/sshd_config`).
- Bases de datos y credenciales.

1.2 Identificación de Amenazas

- Accesos no autorizados a través de SSH debido a configuraciones inseguras (e.g., `PermitRootLogin` habilitado).
- Explotación de puertos abiertos innecesarios (HTTP, FTP).
- Malware detectado en rutas críticas (`/home/debian/.local/share/orca`).
- Posibilidad de escalación de privilegios y acceso a cuentas administrativas.

Fase 1:

- Accesos no autorizados a través de credenciales débiles detectadas con fuerza bruta (`hydra`).
- Archivos y procesos sospechosos identificados (`speech-dispatcher`, scripts en `/opt/`).

Fase 2:

- Puertos filtrados pero potencialmente explotables (FTP y HTTP).
- Configuración insegura en SSH (`PermitRootLogin yes`, `PasswordAuthentication yes`).

1.3 Evaluación de Impacto

Cada amenaza se clasifica por su impacto potencial:

1. **Compromiso de credenciales:** Alto riesgo (afecta la integridad y confidencialidad).
2. **Procesos sospechosos:** Riesgo medio (posibles puertas traseras).
3. **Puertos abiertos innecesarios:** Riesgo bajo-medio (aumenta la superficie de ataque).

1.4 Tratamiento del Riesgo

Se impelmentaron las siguientes medidas:

1. Configuración reforzada de SSH (deshabilitar `PasswordAuthentication` y `PermitRootLogin`).
2. Cierre de puertos no esenciales con `iptables`.
3. Actualización y mantenimiento regular del sistema.
4. Creación de políticas claras de respaldo y recuperación.

2. Políticas de Seguridad

Las políticas de seguridad establecen las reglas fundamentales del SGSI:

2.1 Política de Protección de Logs

Almacenamiento seguro: Los registros críticos deben estar protegidos contra modificaciones no autorizadas.

- Implementar herramientas como **auditd** para monitorear accesos.
- Restringir permisos de acceso a `/var/log/`.

Retención: Mantener los logs durante un mínimo de 6 meses para auditorías y análisis forenses.

2.2 Política de Gestión de Servicios

- **Eliminación de servicios innecesarios:** Como parte de la fase 1, se deshabilitaron `CUPS`, `Apache`, y `speech-dispatcherd`.

- **Actualización constante:** Mantener versiones seguras y actualizadas de servicios esenciales.

2.2 Política de Respuesta a Incidentes

- Clasificar los incidentes en niveles de severidad.
- Documentar incidentes y asegurar una comunicación fluida con el equipo de respuesta (CSIRT).

2.2 Política de Respaldo y Recuperación

- Respaldos automatizados diarios y semanales.
- Almacenamiento en ubicaciones seguras fuera del servidor principal.

2.3 Política de Gestión de Incidentes

- Respuesta a incidentes basada en el NIST SP 800-61.
- Documentación de cada incidente y análisis de lecciones aprendidas.

2.4 Política de Monitoreo Continuo

- Uso de SIEM para monitorear eventos de seguridad.
- Revisiones semanales de logs en `/var/log/` y `/etc/ssh/`.

2.5 Política de Capacitación

- Formación periódica en ciberseguridad para el personal.
- Simulaciones de ataques para evaluar la preparación.

3. Controles Técnicos Implementados

3.1 Configuración Segura de SSH

Se aplicaron ajustes clave tras identificar configuraciones inseguras:

- Deshabilitación de `PermitRootLogin` y `PasswordAuthentication`.
- Uso obligatorio de claves SSH.
- Restricción de accesos mediante la directiva `AllowUsers`.

3.2 Cierre de Puertos No Necesarios

- Bloqueo de puertos HTTP (80) y FTP (21) con `iptables`.
- Permitido únicamente el puerto 22 para SSH, con acceso limitado por IP.

3.3 Escaneos de Seguridad

- Herramientas como `chkrootkit` y `rkhunter` implementadas para detectar y eliminar amenazas como rootkits y malware.
- Escaneos regulares para identificar scripts maliciosos y procesos sospechosos.

3.4 Implementación de Backups Incrementales

- **Estrategia:** Respaldos diarios y semanales con herramientas como `rsync`.
- **Pruebas de restauración:** Simulaciones mensuales para garantizar la integridad y la eficacia de los backups.

3.5 Prevención de Fugas de Datos (DLP)

- Implementar políticas que restrinjan transferencias de datos críticos.
- Monitoreo de dispositivos externos conectados al servidor.

4. Gestión de Vulnerabilidades

4.1 Proceso de Escaneo

- Escaneos regulares con herramientas como `Nmap` y `OpenVAS`.
- Identificación y corrección de vulnerabilidades encontradas en servicios y configuraciones.

4.2 Gestión de Contraseñas

Hallazgo: Fuerza bruta exitosa en la cuenta `debian` (contraseña: `123456`).

Acción: Se implementó una política de contraseñas seguras:

- Rotación obligatoria cada 90 días.

---

5. Respuesta a Incidentes

5.1 Análisis Forense

- Revisiones manuales y automatizadas de los logs del sistema (`last`, `lastlog`).
- Identificación de accesos sospechosos y manipulación de archivos.

5.2 Contención y Erradicación

- Deshabilitación de servicios no esenciales y eliminación de scripts maliciosos detectados.
- Configuración del firewall para mitigar futuras escalaciones.

---

6. Monitoreo y Mejora Continua

Un SGSI eficaz requiere monitoreo constante y ajustes según las lecciones aprendidas.

6.1 Indicadores de Rendimiento

- **Reducción de tiempo de respuesta:** Objetivo de mitigar incidentes críticos en menos de 1 hora.
- **Incremento en la seguridad:** Disminuir intentos de acceso no autorizado mediante bloqueos IP automáticos.

6.2 Simulaciones

- Pruebas regulares para verificar que las configuraciones implementadas funcionan según lo esperado.
- Ejecución de ejercicios de fuerza bruta simulada para comprobar la robustez de las credenciales.

6.3 Actualizaciones y Parches

- Automatización de actualizaciones con `unattended-upgrades`.
- Verificación de compatibilidad y estabilidad tras cada actualización.

Conclusión

Este sistema es adaptable y escalable, asegurando la protección de activos críticos y mejorando continuamente. Si se implementa de manera estricta, reducirá drásticamente el riesgo de futuros incidentes y garantizará la continuidad operativa en la empresa.