PROYECTO FINAL

Plan de Respuesta a Incidentes y SGSI

Ramón Tirado Fernández

ÍNDICE

1. Plan de Respuesta a Incidentes (Basado en NIST SP 800-61)

Objetivo: Establecer un protocolo estructurado para identificar, contener, erradicar y recuperarse de incidentes de seguridad, basado en el ataque descrito en los informes.

Fases del Plan:zz

1.1. Preparación

- **Equipo de Respuesta a Incidentes (CSIRT):**
  - Roles definidos (Líder de Respuesta, Analistas Forenses, Administradores de Sistemas, Comunicación).
  - Contactos de emergencia (interno/externo).
- **Herramientas:**
  - Monitoreo continuo (SIEM, IDS/IPS).
  - Copias de seguridad automatizadas y cifradas.
- **Documentación:**
  - Inventario de activos críticos (servidores, bases de datos, aplicaciones).
  - Políticas de acceso y autenticación (MFA, SSH sin root, contraseñas fuertes).

1.2. Detección y Análisis

- **Identificación del Incidente:**
  - Alertas de logs (SSH, FTP, Apache).
  - Herramientas: chkrootkit, rkhunter, WPScan.
- **Análisis Forense:**
  - Revisión de procesos sospechosos (ps aux, crontab).
  - Auditoría de permisos (/var/www/html, wp-config.php).

- **Clasificación:**
    - Severidad alta (acceso root no autorizado, malware en procesos como orca).

1.3. Contención

- **Contención Inmediata:**
    - Aislamiento del servidor comprometido de la red.
    - Bloqueo de IP maliciosa (iptables -A INPUT -s 192.168.0.134 -j DROP).
    - Deshabilitar servicios vulnerables (FTP anónimo, XML-RPC en WordPress).
- **Contención a Largo Plazo:**
    - Parcheo de vulnerabilidades (apt upgrade).
    - Eliminación de backdoors (ej. scripts PHP maliciosos).

1.4. Erradicación

- **Eliminar Compromisos:**
    - Reinstalación de servicios afectados (Apache, MySQL).
    - Cambio de credenciales (MySQL, SSH, WordPress).
    - Eliminación de archivos sospechosos (/usr/bin/orca, shell.php).
- **Hardening:**
    - Restricción de permisos (chmod 750 /var/www/html).
    - Deshabilitar cuentas innecesarias (DROP USER 'user'@'localhost').

1.5. Recuperación

- **Restauración:**
    - Recuperación desde backups limpios (verificar integridad).
    - Pruebas de funcionalidad (WordPress, FTP, SSH).

- **Monitoreo Post-Incidente:**
    - Análisis de logs para detectar reintentos de ataque.

2. Sistema de Gestión de Seguridad de la Información (SGSI - ISO 27001)

Objetivo: Alinear las prácticas de seguridad con ISO 27001 para proteger la confidencialidad, integridad y disponibilidad de la información.

Componentes del SGSI:

2.1. Análisis de Riesgos

- **Identificación de Activos:**
    - Servidores (Debian, Apache, MySQL), datos (BD WordPress), usuarios.
- **Evaluación de Riesgos:**
    - Acceso no autorizado (SSH/FTP), inyección SQL, malware.
    - Matriz de riesgos (probabilidad vs. impacto).

2.2. Políticas de Seguridad

- **Controles ISO 27001 Aplicables:**
    - A.9 (Control de Acceso):
        - MFA para SSH y WordPress.
        - Política de mínimos privilegios (sudo restringido).
    - A.12 (Seguridad Operacional):
        - Actualizaciones automáticas (unattended-upgrades).
        - Monitoreo con herramientas como Fail2Ban.
    - A.13 (Protección de Datos):
        - Cifrado de backups y datos sensibles (LUKS, SSL/TLS).

2.3. Implementación de Controles

- **Protección de Datos:**
  - Backups diarios en ubicación externa (3-2-1 rule).
  - Cifrado de wp-config.php y bases de datos (ALTER USER ... IDENTIFIED BY 'nueva_contraseña').
- **Protección de Servicios:**
  - Deshabilitar FTP anónimo (anonymous_enable=NO).
  - Configuración segura de Apache (Options -Indexes).

2.4. Auditoría y Mejora Continua

- **Revisiones Periódicas:**
  - Auditorías internas cada 6 meses.
  - Simulacros de incidentes (ej. ataques de fuerza bruta).
- **Indicadores de Desempeño (KPI):**
  - Tiempo de detección/containment (<1 hora).
  - Número de vulnerabilidades parcheadas/mes.

2.5. Documentación

- **Manual del SGSI:**
  - Procedimientos para respuesta a incidentes.
  - Registros de capacitación del personal.

3. Recomendaciones Finales

- **Formación:**
  - Entrenar al personal en concienciación de phishing y buenas prácticas.
- **Automatización:**
  - Desplegar herramientas como CIS-CAT para hardening automático.
- **Resiliencia:**
  - Plan de continuidad del negocio (BCP) para ataques críticos.

4. Conclusión:

La combinación del plan NIST SP 800-61 y el SGSI (ISO 27001) mitigará riesgos futuros, asegurando una respuesta rápida y una gestión proactiva de la seguridad. La prioridad es la prevención mediante controles técnicos y la cultura organizacional.