Plan de Respuesta a Incidentes

Objetivo:

Elaborar un plan detallado de respuesta a incidentes de seguridad basado en las mejores prácticas de la guía NIST SP 800-61 y aplicar medidas correctivas de manera efectiva para evitar futuros ataques. Este plan cubre las fases de identificación, contención, erradicación y recuperación ante un incidente de seguridad.

1. Identificación del Incidente

- Detectar la presencia de incidentes mediante herramientas de monitoreo continuo (e.g., SIEM).
- Establecer un protocolo de reportes internos donde los empleados puedan informar sobre incidentes de seguridad.
- Usar herramientas de análisis forense como nmap y Wireshark para confirmar la naturaleza del incidente.
- Alertas automáticas que notifiquen a los equipos de seguridad sobre anomalías detectadas.

2. Contención

- Aislar los sistemas afectados para evitar la propagación del ataque (desconectar redes comprometidas).
- Evaluar el alcance del ataque y priorizar la contención de servicios críticos.
- Registrar todas las acciones tomadas durante esta fase para garantizar la trazabilidad.

3. Erradicación

- Eliminar cualquier software malicioso encontrado en los sistemas.

- Reparar las vulnerabilidades explotadas por el atacante.
- Restablecer contraseñas y credenciales comprometidas.
- Verificar que los sistemas afectados estén completamente libres de amenazas.

4. Recuperación

- Restaurar los datos desde los respaldos más recientes.
- Asegurar que los sistemas y servicios restaurados funcionen correctamente y sin amenazas.
- Monitorear de cerca los sistemas durante un período post-restauración para detectar posibles recurrencias.
- Mantener a la gerencia informada sobre el estado de la recuperación.

Conclusión

Un plan efectivo de respuesta a incidentes es crucial para minimizar el impacto de los ataques y garantizar la continuidad de los servicios. La identificación temprana, la contención rápida, la erradicación de amenazas y la recuperación de sistemas críticos son pasos fundamentales para mitigar los riesgos de seguridad.