El Incidente Crítico

Paso 1: Identificar el Vector de Ataque Inicial. ¿Qué ataque recibimos?

Phishing

1. Diagnostico:

Se alerto una técnica de ciberdelincuencia que consiste en engañar a las personas para que revelen información personal, como contraseñas y números de tarjetas de crédito, haciéndose pasar por una entidad legítima, en este caso, una red social.

Paso 2: Analizar los Logs del Sistema para Encontrar Evidencias de Actividad Maliciosa

2.1 Recolección de Logs:

Logs de autenticación

- Intentos de inicio de sesión: Identifica intentos fallidos o múltiples en poco tiempo desde una misma IP.
- Credenciales comprometidas: Rastrea si las cuentas afectadas han iniciado sesión desde ubicaciones geográficas inesperadas.

Logs de servidor web

- URLs accedidas: Examina las páginas visitadas en el servidor, especialmente aquellas que contienen formularios sensibles.
- Solicitudes HTTP sospechosas: Filtra peticiones que incluyen parámetros anómalos.

Logs de correo electrónico

- Correos enviados/recibidos: Busca patrones inusuales, como correos no autorizados enviados desde cuentas internas.
- Enlaces y adjuntos: Analiza los correos en busca de enlaces a dominios desconocidos o adjuntos maliciosos.

2.2 Análisis de la Actividad Maliciosa:

1. Logs de autenticación

Actividad:

- Busca múltiples intentos fallidos de inicio de sesión en un corto periodo de tiempo (posible ataque de fuerza bruta).
- Identifica inicios de sesión desde ubicaciones geográficas inusuales o fuera del horario laboral típico.

- Rastrea el uso de credenciales legítimas en sistemas a los que normalmente no acceden los usuarios.

Herramientas de Análisis:

- **Splunk:** Ideal para visualizar patrones de autenticación y anomalías.
- **ELK Stack (Elasticsearch, Logstash, Kibana):** Una poderosa suite para analizar y graficar datos.
- **Azure Sentinel:** Especial para entornos en la nube y con capacidades de detección avanzada.

2. Logs de servidor web

Actividad:

- Revisa las solicitudes HTTP sospechosas que incluyan parámetros o comandos fuera de lo normal (posibles intentos de inyección SQL o XSS).
- Identifica patrones de acceso a páginas específicas que puedan usarse para recopilar datos sensibles.
- Examina respuestas de error (como códigos 401 o 403) que podrían denotar intentos de acceso indebido.

Herramientas de Análisis:

- **Wireshark:** Excelente para examinar el tráfico y analizar solicitudes específicas.
- **AWStats:** Ayuda a detectar accesos extraños en logs de servidores.
- **Nmap con scripts NSE:** Permite evaluar posibles vulnerabilidades en servidores comprometidos.

3. Logs de correo electrónico

Actividad:

- Analiza el historial de correos enviados para detectar si se han enviado mensajes no autorizados desde cuentas legítimas.
- Examina los enlaces y dominios incluidos en los correos para identificar URLs maliciosas.
- Rastrea intentos de acceso a buzones de correo desde direcciones IP desconocidas.

Herramientas de Análisis:

- **Microsoft Exchange Admin Center:** Ofrece herramientas de auditoría específicas para entornos de Exchange.
- **Mimecast:** Especializado en monitoreo de seguridad de correo.
- **PhishTool:** Diseñado para analizar correos sospechosos y sus metadatos.

Paso 3: Determinar el Alcance del Compromiso y los Sistemas Afectados

3.1 Identificación de Sistemas Comprometidos:

Revisión de los sistemas interconectados

Actividad:

- Inspeccionar conexiones con otros sistemas para determinar si el compromiso se ha propagado.
- Identificar y aislar dispositivos potencialmente afectados para prevenir la expansión del daño.

Acciones clave:

- Utilizar herramientas como Network Mapping (por ejemplo, Nmap) para detectar relaciones entre sistemas.
- Desactivar temporalmente conexiones no esenciales.

Evaluación del impacto en la infraestructura crítica

Disponibilidad

En este caso lo que se debería de analizar es:

- Comprobación de servicios caídos o interrumpidos.
- Identificar sistemas y aplicaciones críticas que han quedado fuera de servicio.

Ejemplo: Monitorear servidores web y bases de datos esenciales para verificar tiempos de inactividad.

Integridad

En este caso lo que se debería de analizar es:

Validar si los datos almacenados en sistemas comprometidos fueron alterados o corrompidos.

Inspeccionar logs para cambios no autorizados en archivos y configuraciones.

Ejemplo: Comparar los hash de archivos sensibles con respaldos para verificar modificaciones.

Confidencialidad

En este caso lo que se debería de analizar es:

- Evaluar si datos sensibles han sido accedidos, robados o expuestos.
- Revisar logs de acceso y tráfico para detectar brechas de datos.

Ejemplo: Identificar accesos no autorizados a información confidencial mediante herramientas de monitoreo.

Paso 4: Proponer Medidas de Contención Inmediatas:

4.1 Medidas de Contención Inmediatas

- **Actividad:**
    - Aislar sistemas comprometidos: Desconectar temporalmente los dispositivos afectados de la red para evitar la propagación del ataque.
    - Bloquear accesos sospechosos: Revocar credenciales de usuarios potencialmente comprometidos e implementar autenticación multifactor.
    - Actualizar reglas del firewall y IDS/IPS: Ajustar configuraciones para bloquear el tráfico malicioso.

4.2 Plan de Recuperación

- **Actividad:**
    - Restaurar desde respaldos seguros: Asegurarse de que las copias de seguridad no estén comprometidas antes de la restauración.
    - Actualizar software y parches: Instalar actualizaciones de seguridad en todos los sistemas para eliminar vulnerabilidades conocidas.
    - Realizar un análisis forense: Investigar el origen del ataque y documentar sus métodos para futuras mitigaciones.

4.3 Comunicación

- **Actividad:**
    - Informar a los responsables internos: Comunicar la situación al equipo de TI, gerentes de seguridad de la información (CISO) y alta dirección.
    - Notificar a las partes afectadas: Avisar a empleados, clientes, o socios comerciales cuyas credenciales o datos puedan estar comprometidos.
    - Colaborar con las autoridades: Enviar un reporte del incidente a entidades regulatorias o legales si es necesario (por ejemplo, cumplimiento de GDPR o regulaciones locales).