Plantilla de Respuesta a Incidentes de Ransomware

Nombre y Apellidos: IVANA SÁNCHEZ PÉREZ

Escenario asignado:

El Acceso Remoto Comprometido

- **ESCENARIO: Son las 8:15 AM de un viernes. Eres la administradora de sistemas de "Gestoría Integral Global". Te dispones a realizar el mantenimiento semanal del servidor de aplicaciones principal, al que accedes por Escritorio Remoto (RDP). Al intentar conectar, tus credenciales de administrador son rechazadas. Tras varios intentos, consigues acceder con una cuenta local y te encuentras con un fondo de pantalla cambiado que exige un "pago para recuperar el acceso al servidor" y una nota de rescate en el escritorio que detalla los daños.**

He decidido utilizar el método NIST SP 800-61 para estructurar el procedimiento de respuesta al incidente. Pienso que esto aportará más claridad, alineación con la guía.

---

1. Identificación del Incidente

- **Tipo de Incidente: Rasomware desplegado a través del protocolo de Escritorio Remoto (RDP)**
- **Sistemas Afectados Confirmados:**
  - **Servidor principal de aplicaciones (nombre pendiente de confirmación – servidor afectado por RDP).**
  - **Posiblemente, servidores o estaciones de trabajo conectados a la misma red también se hayan expuesto (se determinará tras el análisis forense)**
- **Indicadores de Compromiso (IoCs) Observados:**
  - **Rechazo de credenciales administrativas por parte del servicio RDP.**
  - **Acceso autorizado únicamente mediante una cuenta local.**
  - **Fondo de pantalla modificado con instrucciones de rescate.**
  - **Nota de rescate visible en el escritorio especificando daños y demanda de pago.**
  - **Posibles logs de acceso remoto sospechosos (pueden incluir intentos de fuerza bruta, accesos desde IPs externas no habituales).**
  - **Potencial cifrado y/o inaccesibilidad de archivos críticos del servido**

---

2. Acciones de Contención Inmediatas

- **Acción de Contención 1 (Máxima Prioridad):**
  - **Descripción: Desconectar el servidor afectado de la red para evitar propagación del ransomware y pérdida de datos adicionales**
  - **Justificación: Esta medida es esencial para contener la amenaza y evitar que el malware se expanda lateralmente a otros sistemas de la organización. También previene comunicaciones externas con los servidores de los atacantes**
- **Acción de Contención 2:**
  - **Descripción: Realizar una copia forense (snapshot o imagen del sistema) del servidor comprometido en su estado actual.**
  - **Justificación: Permite conservar pruebas para el posterior análisis forense, ayudando a entender cómo se produjo el ataque y facilitando la investigación**
- **Acción de Contención 3:**
  - **Descripción: Cambiar inmediatamente todas las contraseñas de cuentas con privilegios de administrador, credenciales críticas (incluyendo cuentas RDP) y deshabilitar cuentas comprometidas.**
  - **Justificación: Evita que los atacantes sigan teniendo acceso persistente a la infraestructura incluso tras aislar el servidor, y neutraliza el uso de credenciales robadas para ataques adicionales**

---

3. Plan de Erradicación y Recuperación

- **Paso 1: Erradicación:**
  - **Eliminar por completo la máquina virtual o formatear el servidor físico afectado.**
  - **Identificar y corregir la vulnerabilidad que permitió el acceso inicial, por ejemplo:**
    - **Revisión de los logs de acceso remoto/RDP, auditoría de cuentas utilizadas.**
    - **Analizar posibles exploits sobre servicios expuestos (puertos abiertos de RDP sin protección, falta de MFA o credenciales débiles).**
  - **Realizar un escaneo profundo con herramientas especializadas antes de restaurar cualquier sistema.**

- **Paso 2: Recuperación:**
  - **Reinstalar el sistema operativo del servidor desde una imagen limpia y actualizada o plantilla verificada.**
  - **Restaurar los archivos de la aplicación y los datos únicamente desde la última copia de seguridad fiable y verificable, anterior al incidente.**
  - **Cambiar todas las contraseñas de servicio y claves de API implicadas.**
  - **Verificar que los backups no estén infectados antes de hacer la restauración**

- **Paso 3: Verificación y Puesta en Marcha:**

    - **Aplicar todos los parches y actualizaciones de seguridad antes de volver a conectar el servidor a la red o internet.**
    - **Realizar un escaneo de vulnerabilidades completo al servidor restaurado y comprobar que no hay rastros de la amenaza.**
    - **Habilitar y revisar los logs de seguridad, activar la monitorización reforzada y alerta de anomalías en las primeras horas tras la recuperación.**
    - **Confirmar que el acceso remoto requiere credenciales robustas y, si es posible, MFA habilitado**

- **Paso 4: Lecciones Aprendidas (Post-Incidente):**

    - **Análisis de causa raíz:**
        - **El incidente se originó por exposición insegura de acceso remoto por RPD sin MFA y con credenciales reutilizables o débiles.**
        - **Falta de medidas de protección perimetral y políticas de control de accesos robustas.**
    - **Mejoras a implementar:**
        - **Restringir el acceso a RDP únicamente mediante VPN y a direcciones IP autorizadas.**
        - **Habilitar autenticación multifactor (MFA) para cualquier acceso remoto.**
        - **Imponer una política estricta de gestión y rotación de contraseñas.**
        - **Realizar backups frecuentes y almacenarlos en ubicaciones aisladas (offline o inmutables).**
        - **Configurar firewalls para limitar el acceso al puerto RDP y monitorizar ataques de fuerza bruta.**
        - **Revisar periódicamente las configuraciones de seguridad y ejecutar simulacros de respuesta a incidentes.**
        - **Capacitar al personal en prácticas seguras y detección de amenazas.**
        - **Realizar auditorías de seguridad periódicas**