5 DE ABRIL DE 2024

# ACTIVIDAD 4.2 PRIMERAS CONTENCIONES

INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARÍN
CETI

**Contenido**

**Investiga y haz una propuesta de una primera medida de contención para cada uno de los siguientes tipos de incidentes:**

1. **Virus detectado en el PC de un empleado.**

La primera medida de contención podría ser aislar la máquina afectada de la red para evitar la propagación del virus a otros sistemas.

2. **Servidor C&C.**

Una medida inicial podría ser bloquear la comunicación con el servidor C&C para interrumpir el control que el atacante tiene sobre los sistemas comprometidos.

3. **Sniffing.**

Claramente la medida de contención más importante sería implementar el cifrado de datos en tránsito para proteger la información sensible.

4. **Intento de intrusión.**

Al detectar un intento de intrusión la medida de contención inicial podría ser reforzar las políticas de seguridad, como fortalecer contraseñas y habilitar la autentificación de dos factores.

5. **Compromiso de una cuenta con privilegios.**

La medida de contención inicial podría ser revocar o limitar los privilegios de la cuenta afectada hasta que se pueda realizar una investigación más completa.

6. **DoS.**

Implementar técnicas de mitigación de DoS, como la limitación de la tasa (cantidad de tráfico de red permitido a un solo usuario, dirección IP o conexión), para minimizar el impacto de ataque.

7. **Pérdida de datos.**

En caso de producirse una pérdida de datos, la contención inicial sería la restauración de los datos a partir de copias de seguridad.

**8. Phishing.**

Al detectar un intento de phishing, podríamos alertar a los usuarios sobre el intento de phishing y aconsejarles que no hagan clic en enlaces sospechosos o proporcionen información personal.

**Bibliografía**


- Virus detectado en el PC de un empleado
- Servidor C&C
- Sniffing
- Intento de intrusión
- Compromiso de una cuenta con privilegios
- DoS
- Pérdida de datos
- Phishing