15 DE ABRIL DE 2024

RESPUESTA A INCIDENTES

INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

ENUNCIADO

En esta actividad se te pide investigar qué acciones pueden resultar adecuadas y cuáles no para el siguiente caso:

Una empresa tiene varios servidores. Los empleados de la empresa acceden a ellos a través de SSH, empleando un usuario y contraseña. Hoy ha saltado una alarma en el SIEM de la empresa debido a que se han producido sucesivos intentos fallidos de inicio de sesión en diversas cuentas de empleados. Como primera medida de contención se ha pensado en bloquear la IP del atacante. Al hacerlo, automáticamente se ha seguido sufriendo el mismo ataque pero desde una IP distinta. Probablemente el atacante tenga una herramienta para cambiar de proxy. ¿Qué acciones podríamos tomar?

Vamos a intentar cubrir acciones para las 4 metas de ciberresiliencia:

1. **Anticipar:**

Para la anticipación podríamos instalar un sistema de prevención de intrusiones (IPS) o un sistema de detección de intrusiones (IDS). Estos sistemas ayudan a detectar y prevenir ataques de fuerza bruta y otros tipos de amenazas de seguridad. Además, podrías considerar el uso de un servicio de reputación de IP para identificar y bloquear el tráfico sospechoso.

2. **Resistir:**

En lugar de bloquear la IP del atacante, podríamos implementar un límite de intentos de inicio de sesión fallidos, después del cual se bloquearía temporalmente el acceso. También podríamos implementar una autenticación de dos factores (2FA) para añadir una capa adicional de seguridad.

3. **Recuperar:**

Sería importante tener un plan de recuperación. Que podría incluir la restauración de los sistemas a partir de copias de seguridad seguras, la revisión de los registros para entender la naturaleza del ataque y la implementación de medidas para prevenir futuros ataques.

4. Evolucionar:

Para prevenir futuros incidentes, podríamos considerar la implementación de políticas de seguridad más estrictas, como la obligatoriedad de contraseñas más fuertes y la formación regular de los empleados en seguridad informática. También podrías considerar la migración a la autenticación basada en claves en lugar de contraseñas para el acceso SSH.