9 DE MAYO DE 2024

PRIMERAS CONTENCIONES

INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARIN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

Documenta alguno de los incidentes que has investigado en la práctica 4.2, indicando:

Incidente: Compromiso de una cuenta con privilegios.

1. Las causas del incidente.
    - Falta de autentificación multifactor (MFA). La cuenta comprometida no estaba protegida con MFA, o que la hizo más vulnerable a ataques de phishing.
    - La contraseña no seguía una buena política de contraseñas seguras y estaba siendo reutilizada en múltiples servicios.
    - Falta de monitorización constante y detección temprana, esto permitió al atacante mantener acceso no autorizado durante un período prolongado.
2. Cómo se detectó el incidente.
    - Anomalías en los registros de acceso: El equipo de seguridad notó patrones inusuales en los registros de acceso, como intentos de sesión desde ubicaciones u horas inusuales.
    - Alertas del sistema de detección de intrusiones: Los sistemas de detección generaron alertas sobre comportamientos sospechosos, como intentos repetidos de autenticación fallidos o acceso a recursos sensibles.
3. La forma de mitigar el incidente.
    - Implementando la autenticación multifactor (MFA) en todas las cuentas privilegiadas para agregar una capa adicional de seguridad.
    - Fortalecer las medidas de seguridad, incluido el uso de contraseñas seguras y únicas, así como la educación sobre la importancia de la seguridad de la información.
    - Mejorar el seguimiento y la detección mediante la implementación de sistemas de seguimiento proactivos y la revisión periódica de los registros de actividad.

4. El proceso de recuperación del incidente.
    - Bloquear la cuenta comprometida y revocarle los privilegios.
    - Investigación exhaustiva para determinar el alcance del compromiso y los datos afectados.
    - Restablecer credenciales y contraseñas de todas las cuentas afectadas.
    - Notificar a los afectados, como usuarios o clientes, si fuera necesario.
5. Lecciones aprendidas.
    - La importancia de la autenticación multifactor para proteger cuentas privilegiadas.
    - La necesidad de mantener estrictas medidas de seguridad, incluidas contraseñas seguras y monitoreo activo de la actividad de los usuarios.
    - La importancia de una respuesta rápida y una buena comunicación durante y después del incidente.