[Publish] - 5. Asegurar que la política de contraseñas de IAM esté configurada para expirar las contraseñas en 90 días o menos

El hallazgo de seguridad **"Asegurar que la política de contraseñas de IAM esté configurada para expirar las contraseñas en 90 días o menos"** se enfoca en un control de seguridad basado en el tiempo, diseñado para limitar el riesgo de credenciales comprometidas. Incluso las contraseñas más fuertes pueden ser expuestas a través de ataques de phishing, malware o filtraciones de datos en otros sitios.

Al forzar un cambio de contraseña periódico (por ejemplo, cada 90 días), se reduce significativamente la ventana de tiempo durante la cual una contraseña robada puede ser utilizada por un atacante. Si una credencial se ve comprometida, su utilidad para el actor malicioso expira automáticamente. Esta es una práctica estándar requerida por muchos marcos de cumplimiento, como PCI DSS y SOC 2.

Análisis de las Cuentas Reportadas

Las siguientes cuentas de AWS han sido identificadas por no tener una política de expiración de contraseñas o por tener un período de expiración mayor a 90 días.

Tipo	Nombre (Número de Cuenta)
Account	002670977573
Account	005344269008
Account	174771279728
Account	398984081329
Account	498798756906
Account	613703092215
Account	890342916428
Account	996126991518

Preguntas para tu Equipo (Acción Requerida)

Implementar este cambio afectará directamente a todos los usuarios de IAM que inician sesión en la consola. Es crucial gestionar esta transición adecuadamente.

1. **Plan de Comunicación:** ¿Cómo se notificará a los usuarios de IAM en estas cuentas sobre el nuevo requisito de cambio de contraseña cada 90 días? Es importante comunicar el cambio con anticipación para evitar confusiones y una sobrecarga en el equipo de soporte técnico.
2. **Impacto en Usuarios:** ¿Están los usuarios preparados para este cambio? Forzar la rotación de contraseñas puede ser un inconveniente si no se comunica la razón de seguridad detrás de esta medida.

Consideraciones de Costo

No hay **ningún costo directo** asociado con la configuración de la política de expiración de contraseñas en IAM. Esta es una característica de seguridad fundamental que AWS proporciona sin cargo alguno.

Cómo Solucionarlo: Actualizar la Política de Contraseñas

Puedes actualizar la política de contraseñas para cada cuenta directamente desde la Consola de Administración de AWS.

1. Inicia sesión en la **Consola de Administración de AWS** para la cuenta que deseas modificar.
2. Navega al servicio de **IAM (Identity and Access Management)**.
3. En el panel de navegación izquierdo, elige **Configuración de la cuenta (Account settings)**.
4. En la sección **Política de contraseñas (Password policy)**, haz clic en **Editar**.
5. Marca la casilla **Habilitar vencimiento de contraseña (Enable password expiration)**.
6. En el campo **Período de vencimiento de la contraseña (días)**, introduce un valor de **90** o menos.
7. **(Opcional pero recomendado)** Considera habilitar la opción **Permitir que los usuarios cambien su propia contraseña** para que puedan gestionarla ellos mismos antes de que expire.
8. Haz clic en **Guardar cambios**.
9. Repite este proceso para cada una de las cuentas identificadas.

Recomendación

Se recomienda que se implemente una política de expiración de contraseñas de 90 días en todas las cuentas listadas. Esta es una medida de seguridad básica que reduce drásticamente el riesgo asociado con credenciales comprometidas a largo plazo. Al mismo tiempo, aprovecha la oportunidad para revisar y fortalecer otras configuraciones de la política de contraseñas, como la longitud mínima y la complejidad.

Referencias

Set an account password policy for IAM users - AWS Identity and Access Management