[Publish] - 9. Habilitar el cifrado para el flujo de entrega de Kinesis Firehose

El hallazgo de seguridad **"Habilitar el cifrado para el flujo de entrega de Kinesis Firehose"** se enfoca en proteger los datos que Firehose entrega a su destino final (como un bucket de S3, Redshift o Elasticsearch). Kinesis Firehose es un servicio para capturar, transformar y cargar flujos de datos de manera confiable.

Si el cifrado del lado del servidor no está habilitado, los datos que Firehose escribe en el destino se almacenan en texto plano. Esto crea un riesgo de seguridad, ya que cualquier persona con acceso de lectura al destino podría ver la información sensible contenida en los flujos de datos.

Habilitar el cifrado asegura que los datos se cifren automáticamente antes de ser guardados en el destino, protegiéndolos en reposo y garantizando que solo las entidades autorizadas con acceso a la clave de cifrado puedan leerlos.

Análisis de los Flujos de Entrega Reportados

Los siguientes flujos de entrega (delivery streams) de Kinesis Firehose han sido identificados por no tener habilitado el cifrado del lado del servidor.

Tipo	Nombre del Flujo de Entrega	Número de Cuenta
KinesisFirehose	deliverystream/AWSAccelerator-LoggingStack-000316901759-us-east-1--Sz4626zb8rNM	000316901759
KinesisFirehose	deliverystream/AWSAccelerator-LoggingStack-000316901759-us-west-2--FdisgesJjZfl	000316901759

Observación Clave: Los nombres sugieren que estos flujos son parte de una solución de registro centralizada (`AWSAccelerator-LoggingStack`). Los registros a menudo contienen información sensible, lo que hace que el cifrado sea aún más crítico.

Preguntas para tu Equipo (Acción Requerida)

Para habilitar el cifrado de manera correcta, es necesario tomar una decisión sobre la gestión de las claves.

1. **¿Qué clave de KMS se debe utilizar?** Existen dos opciones:
   - **Una clave gestionada por AWS (`aws/s3`)**: Es la opción más sencilla y no tiene costo de almacenamiento de llave.
   - **Una Llave Gestionada por el Cliente (CMK)**: Proporciona un control más granular sobre los permisos y la auditoría de la llave. ¿Existe ya una CMK designada para esta solución de logging?

Consideraciones de Costo

- **Costo de la Función de Cifrado:** No hay un cargo adicional por parte de Kinesis Firehose por habilitar el cifrado.
- **Costo de AWS KMS:**
  - Si usas una **clave gestionada por AWS**, no hay costo adicional.
  - Si usas una **Llave Gestionada por el Cliente (CMK)**, se aplicará el costo estándar de **$1 USD al mes por la llave**, más un costo muy bajo por las solicitudes a la API que Firehose hará a KMS para usar la llave.

Conclusión sobre Costos:

Habilitar el cifrado es una medida de seguridad muy rentable. Usando la clave predeterminada de AWS, no hay costo adicional. Usando una CMK, el costo es mínimo y se justifica por el nivel superior de control y auditoría.

Cómo Solucionarlo: Habilitar el Cifrado en el Flujo de Entrega

Puedes habilitar el cifrado editando la configuración del flujo de entrega. Este cambio no suele requerir tiempo de inactividad.

1. **Navegar al Flujo de Entrega de Firehose:**
   - Ve a la consola de **Amazon Kinesis**.
   - En el panel de navegación izquierdo, selecciona **Data Firehose**.
   - Haz clic en el nombre del flujo de entrega que deseas modificar.
2. **Editar la Configuración del Destino:**
   - Desplázate hasta la sección de detalles del destino (ej. **Detalles del destino de Amazon S3**).
   - Haz clic en **Editar**.
3. **Habilitar el Cifrado del Lado del Servidor:**

- En la configuración del destino, busca la sección de **Cifrado del lado del servidor (Server-side encryption)**.
- Marca la casilla para **Habilitar** el cifrado.
- Selecciona la **Clave de KMS** que deseas utilizar, ya sea la clave predeterminada de S3 o una CMK de tu elección.
- Guarda los cambios.

4. **Repetir:** Realiza este proceso para el otro flujo de entrega identificado.

Recomendación

Se recomienda que se habilite el cifrado del lado del servidor para ambos flujos de entrega de Kinesis Firehose. Dado que estos flujos parecen estar manejando datos de registro, es fundamental proteger esta información en reposo. El uso de la clave gestionada por AWS (`aws/s3`) es una solución excelente y sin costo que soluciona inmediatamente el hallazgo de seguridad.

Refrencias

Data protection in Amazon Data Firehose - Amazon Data Firehose