[Publish] - 13. Buckets de CloudTrail Públicos

El hallazgo de seguridad **"Buckets de CloudTrail Públicos"** identifica una de las vulnerabilidades de seguridad más graves posibles en un entorno de AWS. Los registros de AWS CloudTrail son la pista de auditoría definitiva de tu cuenta; documentan cada acción, cada cambio y cada acceso. Hacer público el bucket de S3 que almacena estos registros es equivalente a publicar un registro detallado de todas las actividades de tu infraestructura en internet.

Exponer estos registros permite a cualquier persona en el mundo:

- **Analizar tu Infraestructura:** Entender qué servicios usas, cómo están configurados y con qué frecuencia cambian.
- **Identificar Patrones y Posibles Debilidades:** Un atacante puede estudiar los registros para encontrar errores de configuración, usuarios con demasiados permisos o patrones de actividad que puedan ser explotados.
- **Obtener Nombres de Usuario y Roles:** Los registros contienen los nombres de los principales (usuarios y roles) que realizan acciones, lo que facilita los ataques dirigidos.
- **Cubrir sus Huellas:** Aunque no pueden modificar los registros existentes, pueden saber exactamente qué se está registrando para intentar evadir la detección en futuros ataques.

No existe ningún escenario legítimo en el que un bucket que almacena registros de CloudTrail deba ser público.

Análisis de los Recursos Reportados

El siguiente trail de CloudTrail ha sido identificado por estar almacenando sus registros en un bucket de S3 que es accesible públicamente.

Tipo	Nombre del Trail	Número de Cuenta
CloudTrail	trail/ValesElectronicos	002670977573

Preguntas para tu Equipo (Acción Requerida)

Dado que este es un hallazgo crítico, la acción debe ser inmediata. No se necesita deliberación sobre si el bucket debe ser público o no; no debe serlo. Las preguntas para el equipo son para entender el origen del problema y prevenir su recurrencia:

1. **Análisis de Causa Raíz:** ¿Cómo llegó este bucket a tener una configuración pública? ¿Fue un error manual, un script de automatización defectuoso o una política de bucket incorrecta?

2. **Revisión de Permisos:** ¿Quién o qué tiene permisos para cambiar la configuración de acceso de este bucket? Es necesario revisar las políticas de IAM para limitar esta capacidad.

Consideraciones de Costo

No hay **ningún costo directo** asociado con hacer que un bucket de S3 sea privado. La configuración de seguridad es una característica fundamental de AWS y es gratuita.

El verdadero costo de no solucionar este hallazgo de inmediato es el **riesgo incalculable de una brecha de seguridad**. La información contenida en los registros de CloudTrail puede ser el punto de partida para un ataque sofisticado y dirigido contra tu infraestructura.

Cómo Solucionarlo: Bloquear el Acceso Público Inmediatamente

La forma más rápida y efectiva de remediar este hallazgo es utilizando la función de Bloqueo de Acceso Público de S3.

1. **Identificar el Bucket de S3:**
   - Navega a la consola de **CloudTrail**.
   - Selecciona el trail `ValesElectronicos`.
   - En la configuración del trail, identifica el nombre del bucket de S3 de destino.
2. **Habilitar el Bloqueo de Acceso Público en el Bucket:**
   - Navega a la consola de **Amazon S3** y selecciona el bucket identificado.
   - Ve a la pestaña **Permisos**.
   - En la sección **Bloquear acceso público (configuración del bucket)**, haz clic en **Editar**.
   - Selecciona **Bloquear todo el acceso público** y luego haz clic en **Guardar cambios**. Esto anulará cualquier política de bucket o ACL que esté permitiendo el acceso público.
3. **Revisar y Eliminar la Política Pública (Opcional pero recomendado):**
   - En la misma pestaña de **Permisos**, revisa la **Política del bucket**.
   - Identifica y elimina la declaración (`Statement`) que permite el acceso público (aquella con `"Principal": "*"` o `"Principal": {"AWS": "*"}`).
   - Guarda la política corregida.

Recomendación

1. **Acción Inmediata:** Remedia este hallazgo con la máxima prioridad siguiendo los pasos descritos anteriormente. El bucket que contiene los registros de CloudTrail debe ser privado sin excepción.
2. **Prevención a Nivel de Cuenta:** Para evitar que esto vuelva a ocurrir, se recomienda evaluar el habilitar el **Bloqueo de Acceso Público a nivel de cuenta** en la consola de S3. Esta es la

mejor práctica y actuará como una salvaguarda para todos los buckets en la cuenta, previniendo futuras exposiciones accidentales.

Referencias

Examples of Amazon S3 bucket policies - Amazon Simple Storage Service