Grupo N°06

Resolución a escenarios en AWS

Desarrollo de Soluciones en la Nube

Integrantes

- Guzman Gutierrez Lin Abigail
- Mamani Mamani, Franco Nilver
- Pisconte Chuctaya, Santiago Joel
- Qquelcca Fernandez, Roman Rivaldo
- Quispe Maqque, Abel

Escenario 06

Configuración Incorrecta de Firewall

- Descripción: Se detecta que el firewall de una instancia EC2 está configurado para permitir conexiones desde cualquier dirección IP, lo que representa un riesgo de seguridad. o Instrucciones para el Grupo:
- ¿Qué debe hacer el cliente para mejorar la configuración del firewall?
- ¿Qué herramientas de AWS podrían ayudar a auditar y corregir configuraciones de seguridad?

Acciones para mejorar la configuración del firewall

Restringir las reglas de acceso

Definir rangos de IP específicos

Aplicar principios de menor privilegio

Implementar acceso mediante VPC o AWS Systems Manager

Solución 01

Mejorar de la configuración del firewall

- **Revisión de las Reglas de Seguridad en el Grupo de Seguridad de EC2:** Debe restringirse el acceso a la instancia para permitir solo las direcciones IP necesarias. Es recomendable aplicar la regla de "principio de menor privilegio":
  - Acceso SSH: permitir solo desde IP específicas (por ejemplo, la IP de la oficina o IP estáticas confiables).
  - Acceso HTTP/HTTPS: si es una aplicación web, restringir a rangos de IP necesarios o permitir tráfico solo por ciertos puertos.
- **Desactivar reglas de acceso innecesarias:** Remover reglas de entrada que no sean estrictamente necesarias para el funcionamiento de la instancia.

AWS VPC

¿Qué es VPC?

- Definición simple
- Red virtual aislada en AWS
- Control total sobre el entorno de red
- Base de la seguridad en red

Componentes Clave de VPC

- Security Groups
- Network ACLs
- Subredes (públicas/privadas)
- Internet Gateway
- Route Tables

Implementación de la Solución

- Crear subredes específicas
- Configurar Security Groups restrictivos
- Establecer Network ACLs
- Definir rutas seguras

La implementación de la solución de seguridad mediante AWS VPC resolverá el problema de la configuración incorrecta del firewall en la instancia EC2, eliminando el acceso indiscriminado (0.0.0.0/0) y estableciendo un control de acceso granular. Como resultado, solo el tráfico autorizado podrá acceder a las instancias a través de Security Groups específicos y Network ACLs, proporcionando una doble capa de seguridad.

Acciones de Responsabilidad Afectiva

Comunicación Clara: Explicar al cliente los riesgos de una configuración abierta del firewall en términos no técnicos, destacando la posible exposición de sus datos.

Educación y Empatía: Ofrecer una sesión educativa para explicar las mejores prácticas en seguridad de firewall, ayudando al cliente a comprender la importancia de aplicar restricciones.

Soporte Continuo: Garantizar disponibilidad para resolver cualquier duda y guiar en la implementación de medidas de seguridad.

Seguimiento y Mejora Continua

1. Revisión Periódica: Implementar revisiones regulares de la configuración de seguridad para adaptarse a nuevos desafíos y actualizar las políticas de seguridad.
2. Reportes de Estado de Seguridad: Generar reportes periódicos que informen al cliente sobre el estado de la seguridad de sus instancias, brindando transparencia y manteniendo una comunicación de confianza.

Actualizar la Configuración del Firewall:

- Limitar el acceso únicamente a direcciones IP necesarias, o en su defecto, definir rangos específicos de IP confiables.
- Configurar reglas en el grupo de seguridad de AWS EC2 para restringir las conexiones de entrada a puertos específicos y bloquear el acceso desde "0.0.0.0/0", que permite el acceso desde cualquier parte.

Uso de Herramientas de AWS para Auditoría y Seguridad:

- AWS Security Hub: Detecta configuraciones incorrectas y proporciona recomendaciones de seguridad en tiempo real.
- AWS Config: Permite auditar y monitorear los cambios en la configuración, asegurando que las reglas de seguridad se cumplan.
- AWS Trusted Advisor: Ofrece asesoramiento sobre las mejores prácticas y alerta sobre configuraciones de seguridad incorrectas.
- Amazon CloudWatch y CloudTrail: Monitorean y registran la actividad de la instancia, proporcionando alertas en caso de intentos de acceso no autorizado.

Implementar Autenticación Multi-factor (MFA):

- Reforzar la seguridad mediante autenticación adicional para acceder a las instancias y configuraciones sensibles.