Caso de Estudio: Cifrado Fuerte, Configuración Débil

Contexto:

Una startup ha implementado rápidamente una arquitectura en AWS para lanzar su producto mínimo viable (MVP). El sistema expone un servicio de catálogo de productos accesible vía API.

A continuación, se describe la arquitectura actual implementada por el equipo técnico:

Amazon API Gateway

- Expone el endpoint /catalog al público.
- Se protege únicamente mediante una **API Key**.

AWS Lambda

- Es invocada por API Gateway para consultar productos en una tabla DynamoDB.
- También envía notificaciones por correo mediante Amazon SES.
- Tiene habilitado CloudWatch Logs.

AWS IAM Role asignado a Lambda

- Utiliza las políticas administradas: AmazonDynamoDBFullAccess y AmazonSESFullAccess.

AWS CloudTrail

- Está habilitado, pero solo registra eventos en la región us-east-1.

No se ha habilitado AWS WAF ni ningún otro sistema de protección adicional.

Instrucciones para análisis:

En grupos pequeños:

1. **Analiza la arquitectura actual.**
   ¿Qué elementos te parecen inseguros o mal diseñados desde el punto de vista de buenas prácticas de seguridad en la nube?
2. **Detecta al menos 4 problemas o vulnerabilidades.**
   Algunos pueden ser evidentes, otros requieren una mirada crítica.

3. **Propón un rediseño seguro**, manteniendo la simplicidad del entorno (no hace falta escalar demasiado). Tu propuesta debe considerar al menos:
    - Mejorar la autenticación de la API.
    - Aplicar el principio de menor privilegio.
    - Ampliar la trazabilidad de eventos.
    - Añadir protecciones frente a tráfico anómalo o abusivo.
4. **Representa gráficamente el antes y el después** (opcional).
   Puedes usar herramientas como Draw.io, Canva, Figma o simplemente hacer un esquema a mano y tomarle foto.

Preguntas guía

1. ¿Qué problemas de seguridad podrían ocurrir si la API Key se filtra?
2. ¿Por qué no es buena idea usar políticas de acceso completo (FullAccess) en Lambda?
3. ¿Qué limitaciones tiene CloudTrail si solo está activado en una región?
4. ¿Qué beneficios traería usar un sistema como Cognito o un Lambda Authorizer?
5. ¿Qué tipo de reglas podrías aplicar con AWS WAF?