Ciberseguridad

Conocé cómo proteger las APIs correctamente

Concientización

Ciberseguridad

Primero, ¿qué son las APIs?

Las APIs (Interfaces de Programación de Aplicaciones) son los “puentes” que permiten que distintas aplicaciones y sistemas se comuniquen entre sí. Cada vez que haces un pago con una app, rastreas un pedido o inicias sesión en un sitio con tu cuenta de Google, hay una API trabajando detrás. Pero hay un problema: las APIs mal protegidas pueden convertirse en la puerta de entrada de los atacantes.

Concientización

Ciberseguridad

1. Autenticación Rota

Las APIs necesitan verificar quién está accediendo a ellas, pero muchas veces no lo hacen bien. Si una API no exige credenciales seguras, cualquier persona con acceso a la URL de la API podría entrar y ver información sin restricciones.

Consejos:

- Usa **OAuth 2.0**, un sistema de autenticación moderno que da permisos sin compartir contraseñas.
- Implementa **tokens** de acceso con **expiración**
- Habilita autenticación multifactor (**MFA**), que agrega una segunda capa de seguridad

Concientización

2. Fallas en la autorización

Autenticación y autorización no son lo mismo. La autenticación verifica quién eres, pero la autorización decide qué puedes hacer. Si una API permite que un usuario vea datos que no le corresponden, hay un problema de autorización.

Consejos:

- Implementa **controles de acceso** basados en roles, para que cada usuario solo vea lo que le corresponde.
- Verifica en cada solicitud que el usuario tenga **permisos correctos.**
- Usa un **API Gateway**, un sistema que ayuda a filtrar y gestionar quién accede a qué información.

Ciberseguridad

3. Robo de Credenciales y API Keys Expuestas

Muchas APIs usan claves (keys) de acceso para identificarse, pero si esas claves se exponen en internet, cualquiera puede usarlas para acceder a los sistemas.

Consejos:

- **Nunca** guardes claves en el código fuente. Usa variables de entorno o herramientas seguras
- Implementa **rotación automática** de claves, para cambiar las credenciales con frecuencia y evitar que sean reutilizadas.
- **Usa tokens** en lugar de claves fijas, para que cada usuario tenga un permiso limitado y temporal.

Concientización

Ciberseguridad

SEGUINOS Y UNITE AL DISCORD PARA SEGUIR APRENDIENDO

Guardar

Compartir

Seguir

Concientización