LWsystems
OPEN SOURCE IT-Lösungen

Schnelltest: Wie sicher sind Ihre APIs?

Beantworten Sie die folgenden Fragen, um eine erste Einschätzung der API-Sicherheit Ihres Unternehmens zu erhalten.

1. API-Transparenz
- Haben Sie eine Liste aller in Ihrem Unternehmen genutzten APIs?
- Wissen Sie, welche sensiblen Daten über Ihre APIs fließen?

2. Authentifizierung und Zugriffssicherung
- Sind API-Zugriffe durch OAuth2 oder eine vergleichbare Methode gesichert?
- Sind API-Schlüssel hinreichend lang und kryptisch?
- Werden API-Schlüssel sicher gespeichert und regelmäßig erneuert?

3. Schutz vor Angriffen
- Ist eine Rate-Limiting-Funktion für API-Zugriffe aktiviert?
- Werden verdächtige API-Zugriffe automatisch erkannt und blockiert?
- Führen Sie regelmäßig Sicherheitsübungen und Penetrationstests für Ihre APIs durch?

4. Datenverschlüsselung und Kommunikation
- Werden alle API-Daten über HTTPS/TLS verschlüsselt?
- Sind sensible Informationen innerhalb der API-Kommunikation verschlüsselt?

5. Monitoring und Wartung
- Ist ein API-Logging und Monitoring eingerichtet?
- Werden API-Logs regelmäßig ausgewertet, um ungewöhnliche Aktivitäten zu erkennen?
- Sind automatische Updates und Sicherheitspatches für Ihre APIs aktiviert?

Ergebnisbewertung

0-5 Punkte: Hohe Sicherheitsrisiken! Ihre APIs sind anfällig für Angriffe.
Handeln Sie umgehend und setzen Sie grundlegende Schutzmaßnahmen um.

6-10 Punkte: Mittleres Risiko. Sie haben bereits einige Sicherheitsvorkehrungen getroffen, aber es gibt noch Verbesserungsbedarf.

11-13 Punkte: Gute Sicherheit! Ihre API-Schutzmechanismen sind solide, sollten aber regelmäßig überprüft und optimiert werden.

Empfehlung: Nutzen Sie Open-Source-Sicherheitslösungen wie OWASP ZAP oder Kong API Gateway, um Ihre API-Sicherheit weiter zu verbessern!