LWsystems
OPEN SOURCE IT-Lösungen

Checkliste zur API-Sicherheit für Unternehmen

1. Sichtbarkeit und Bestandsaufnahme
☐ Welche APIs werden im Unternehmen genutzt?
☐ Gibt es eine zentrale Dokumentation aller APIs?
☐ Welche Daten fließen über diese APIs?

2. Authentifizierung und Zugriffskontrolle
☐ Sind API-Schlüssel sicher gespeichert und regelmäßig erneuert?
☐ Wird OAuth 2.0 oder eine andere starke Authentifizierung verwendet?
☐ Sind Zugriffsrechte nach dem „Least Privilege"-Prinzip vergeben?

3. Schutz vor Missbrauch und Angriffen
☐ Sind Ratenbegrenzungen (Rate Limiting) aktiv?
☐ Ist API-Logging aktiviert, um Angriffe frühzeitig zu erkennen?
☐ Werden verdächtige API-Zugriffe überwacht und automatisch blockiert?

4. Datenverschlüsselung und sichere Kommunikation
☐ Werden alle API-Anfragen über HTTPS/TLS verschlüsselt?
☐ Sind sensible Daten innerhalb der API-Kommunikation verschlüsselt?
☐ Gibt es Schutzmechanismen gegen Man-in-the-Middle-Angriffe?

5. Sicherheitsupdates und Wartung
☐ Werden API-Sicherheitsupdates regelmäßig eingespielt?
☐ Gibt es einen festen Prozess für API-Sicherheitsüberprüfungen?
☐ Werden regelmäßig Schwachstellen-Scans durchgeführt?

6. Notfallplan und Reaktionsstrategie
☐ Gibt es einen klar definierten Notfallplan bei API-Hacks?
☐ Sind alle relevanten Mitarbeiter auf API-Sicherheitsrisiken geschult?
☐ Werden API-Backups erstellt und getestet?

Tipp: Nutzen Sie Open-Source-Tools wie OWASP ZAP oder Kong API Gateway, um die Sicherheit Ihrer APIs zu verbessern.

Fazit: API-Sicherheit ist keine einmalige Aufgabe, sondern (wie IT-Sicherheit im Allgemeinen) ein fortlaufender Prozess. Nutzen Sie diese Checkliste regelmäßig, um Ihre Systeme abzusichern!