Einleitung

Die nachfolgende Checkliste ist eine grobe Orientierung unserer durchzuführenden Checks bei einem Software-Gutachten. Hierbei handelt es sich um einen Rahmen, den wir in einem Vollgutachten überprüfen.

Die genau zu prüfenden Bestandteile und Umsetzungen sind von Projekt zu Projekt unterschiedlich, da auch der Aufbau unterschiedlich sein kann. Diese Checkliste zeigt die für uns wichtigsten Punkte bei der Entwicklung einer Webanwendung oder einer App mit Web-Backend.

1. Rahmenbedingungen

☐ Liegen Angebote und Verträge des Dienstleisters vor?
☐ Wurde eine Kosten-Nutzen-Abschätzung durchgeführt?
☐ Welche Frameworks wurden verwendet (Aufwand-Nutzen)?
☐ Besteht Zugriff zu den Repositories?
☐ Besteht Zugriff zum Ticketsystem zur Nachvollziehbarkeit?

2. Architektur & Technologie

☐ Ist die Softwarearchitektur dokumentiert (Diagramme, Schichten, Datenflüsse)?
☐ Wird eine saubere Trennung von Backend, Frontend, Datenbank und Infrastruktur umgesetzt?
☐ Ist die Architektur skalierbar (horizontale/vertikale Skalierung, Cloud-Readiness)?
☐ Werden gängige Standards (REST, GraphQL, gRPC) korrekt eingehalten?
☐ Ist die Codebasis modular und erweiterbar?

3. Infrastruktur & Deployment

☐ Werden Container (Docker) eingesetzt, und sind Images schlank & sicher gebaut?
☐ Existieren Kubernetes-Manifeste oder Helm-Charts für reproduzierbare Deployments?
☐ Ist ein CI/CD-Prozess vorhanden und automatisiert (Build, Tests, Deployments)?

4. Cloud & Kosten

☐ Falls Cloud verwendet wird: Gibt es eine Analyse der Cloud-Kosten (Compute, Storage, Datenverkehr)?
☐ Sind Autoscaling und Ressourcenlimits korrekt gesetzt?
☐ Werden unnötige Services vermieden (Kostenfallen)?
☐ Existiert ein Monitoring der laufenden Kosten?

5. Sicherheit

☐ Werden API-Zugriffe über Authentifizierung/Autorisierung (z. B. OAuth2, JWT) abgesichert?
☐ Ist HTTPS/TLS überall verpflichtend (Cert-Manager, Let's Encrypt)?
☐ Werden Secrets sicher verwaltet (Vault, K8s-Secrets, kein Hardcoding)?
☐ Ist ein Schwachstellenscan für Dependencies vorhanden (Snyk, OWASP, Trivy)?
☐ Wie aktuell sind genutzte Drittanbieter-Bibliotheken? Sind diese von Schwachstellen betroffen?
☐ Ist ein Berechtigungskonzept für Rollen/Nutzer dokumentiert oder gibt es ein dynamisches Berechtigungssystem?

6. Daten & Persistenz

☐ Ist die Datenbankwahl sinnvoll (SQL vs. NoSQL)?
☐ Gibt es ein Backup- und Restore-Konzept?
☐ Ist die Datenmigration (Schemaänderungen) automatisiert?
☐ Werden personenbezogene Daten nach DSGVO behandelt (Löschung/Archivierung)?

7. Qualitätssicherung & Tests

☐ Sind Unit-Tests und Integrationstests vorhanden und wie hoch ist die Test Coverage?
☐ Existieren End-to-End-Tests (z. B. Cypress, Playwright, Appium)?
☐ Läuft ein automatischer Testprozess in CI/CD?
☐ Gibt es Last-/Performancetests?
☐ Sind Mocks und Stubs für externe Systeme vorhanden?
☐ Existieren Coding Guidelines und werden diese überprüft (z.B. mit SonarQube)?

8. Monitoring & Betrieb

☐ Werden Logs zentral gesammelt (z. B. ELK, Loki)?
☐ Gibt es ein Metrik-Monitoring (Prometheus, OpenTelemetry)?
☐ Ist Grafana für Dashboards und Visualisierung im Einsatz?
☐ Gibt es Alerts/Benachrichtigungen bei Ausfällen oder Grenzwertüberschreitungen?
☐ Werden SLIs/SLOs/SLAs definiert und überwacht?

9. Wartung & Weiterentwicklung

☐ Ist die Dokumentation aktuell und vollständig (Architektur, API, Betrieb)?
☐ Gibt es einen definierten Update-Prozess (z. B. für Dependencies, Security Patches)?
☐ Ist der Prozess für Feature-Requests und Bugfixes klar geregelt?
☐ Gibt es einen Plan für Skalierung bei steigender Nutzerzahl?

10. Nutzerperspektive & Usability

☐ Ist die User Experience konsistent und getestet (UX-Design, Prototypen)?
☐ Gibt es Feedback-Mechanismen (z. B. Telemetrie, Nutzerumfragen)?
☐ Sind Accessibility-Standards berücksichtigt?

Erstellung des Gutachtens

Wenn Sie einen unabhängigen Gutachter für Ihr durchgeführtes Software-Projekt suchen, fragen Sie bei uns gern an. Wir haben bereits mehrere Projekte begutachtet und haben durch unsere jahrelange Projekterfahrung bereits viele Umsetzungen durchführen, aber auch begleiten dürfen.

Wir bieten die Erstellung von Vollgutachten oder zeitlich terminierten Gutachten an. In beiden Fällen berechnen wir nach tatsächlichem Stundenaufwand. Um einen groben Rahmen vorzugeben, sollte gesagt sein, dass ein Gutachten innerhalb von 10 Stunden bereits ein gutes erstes Bild über die Gesamtqualität liefert. Ein Vollgutachten ist in etwa 40 bis 50 Stunden erstellt.

Alexander Hähnel, Geschäftsführer

CodeGuides GmbH

+49 (0) 3375 2510 343

info@codeguides.de