Risikomanagement

Risikoarten

Fachliches Risiko
- Vertriebsrisiko: Die App lässt sich nicht gut vertreiben (1)
- Finanzrisiko: Keine Investoren für die App & kein Vertrieb der App (2)

Strategien zur Mitigation:
- zu (1) Marktanalyse durchführen (lassen) oder Marketing outsourcen (a)

Inhärentes Risiko
- Angriffe auf IT-Infrastruktur: Beeinträchtigung des Services durch Einschränkung der Server-Performance (u.a. DDoS) (3)
- Angriffe auf Nutzerdaten: Ungewollte Veröffentlichung sensibler Daten (“Data-Leaks”) (4)
- Mithören des Datenverkehrs von dritten (5)
- Ausfall der IT-Infrastruktur: Ausfall der Infrastruktur von Drittanbietern (6)
- Verzögerung im Entwicklungsablauf aufgrund fehlender technischer Kenntnisse über verwendeten Services (7)

Strategien zur Mitigation:
- zu (3) DDoS-Protection (z.B. Cloudflare) (b)
- zu (3) Mehr Serverinfrastruktur für mehr kumulierte Serverleistung (c)
- zu (5) Verschlüsselung des Datenverkehrs zwischen Server und Client mittels End-to-End Verschlüsselung (d)

Wesentliches, bedeutendes oder relevantes Risiko
- Verfügbarkeit der verwendeten APIs: Ausfall der Spotify API, Google Books API & Amazon Product Advertising API: Schadenshöhe skaliert exponentiell mit der Ausfallzeit (8)

Maximal akzeptables Risiko
- Infrastruktur: Ausfall jeglicher Infrastruktur, der die Kundenzufriedenheit und das Geschäftsergebnis nur marginal negativ beeinflusst (9)

Compliance Risiko
- Verstoß gegen API-Richtlinien (10)
- Verstoß gegen Werbe-Gesetze (11)
- Verstoß gegen die Datenschutzrichtlinien (gerade bei internationaler Verbreitung des Produkts) (12)
- Nichteinhalten von etablierten UX-Praktiken oder ähnlichem bei der App-Entwicklung (13)
- Verletzung von Produkt Patenten bei der Programmierung der Software (14)

Erkennungsrisiko und Bewertungsrisiko
- Nichterkennen von Risiken aufgrund fehlender fachlicher Kenntnisse zu allen Komponenten des Produkts (15)

- Verzögerung beim Einholen von Genehmigungen (16)
- Unterschätzen der anfallende Kosten (17)
- Fehleinschätzung der Produktakzeptanz/Nachfrage aufgrund fehlender (Markt-) Analysen (18)

Strategien zur Mitigation:

- zu (15) Weiterbildung zu den benötigten Technologien, Konsultation mit erfahreneren Entwicklern (e)
- zu (18) Marktanalyse durchführen (lassen) oder Marketing outsourcen (f)

Kontrollrisiko

- DDoS-Protection schützt nur gegen die Auswirkungen einer Attacke (19)

Restrisiko

- nach (a) Fehleinschätzung des Marktes, Nichterreichen von Kunden (20)
- nach (b) Eingesetzter DDoS Protection Service schützt nicht ausreichend gegen Attacken, (21)
- nach (c) Performance der Infrastruktur wird eingeschränkt (22)
- nach (d) Mithören des Datenverkehrs durch Security-Lücken oder Brute-Force Entschlüsselung (23)
- nach (e) geringeres Risiko auf eine nicht ausreichende Produktentwicklung durch fehlendes Know How (24)
- nach (f) siehe (20)

Klassifikation der Risiken

Schadens-höhe					
Sehr hoch	6, 23	4, (5)	(1)		(15)
Hoch		2, 8, 12, 20	(3)		
Mittel	11	10	14, 19		(18)
Gering	24	9 , 16, 22	13, 17	7	
Unbedeutend					
	Sehr Unwahrscheinlich	Eher Unwahrscheinlich	Eher Wahrscheinlich	Wahrscheinlich	Sehr Wahrscheinlich

Eintritts-wahrscheinlich-keit

Legende (Tizian)

- Sehr Geringes Risiko
- Geringes Risiko
- Hohes Risiko
- Sehr Hohes Risiko
- Bestandsgefährdendes Risiko

x siehe Risiko (oben)

(x) Risiko kann durch bereits definierte Strategien zur Mitigation vermindert werden