# Anforderungsanalyse

## Identifikation der Sicherheitsanforderungen für die Anwendung

Die Anwendung muss sicherstellen, dass sensible Daten und Benutzerkonten vor unbefugtem Zugriff geschützt sind. Dazu ergeben sich folgende Sicherheitsanforderungen:

1. Kernanforderungen
   1. JWT-Authentifizierung
      1. Implementierung sicherer JWT-Token mit angemessener Ablaufzeit (z. B. exp-Claim).
      2. Verwendung einer sicheren Signaturalgorithmus wie RS256 oder HS256.
      3. Validierung und Verifizierung von JWTs auf Serverseite, um gefälschte Tokens zu verhindern.
   2. Kontextbasierte MFA
      1. Entscheidung über die Anforderung von MFA basierend auf dynamischen Faktoren wie:
         1. Standort (IP-basierte Geolokation)
         2. Geräteerkennung (User-Agent, Device-ID)
         3. Login-Zeitpunkt (ungewöhnliche Zeiten oder -Muster)
         4. Historische Daten (z. B. bisherige Login-Verhaltensweisen)
         5. weitere Faktoren
2. Datenintegrität und Datenschutz
   1. Verschlüsselung sensibler Daten (z. B. Benutzerpasswörter) in der Datenbank mit Algorithmen wie z.B bcrypt
   2. TLS (HTTPS) zur Sicherung der Datenübertragung
   3. Sicherstellung, dass JWT-Tokens nur über gesicherte Kanäle versandt werden
3. Prävention von Sicherheitsrisiken
   1. Schutz vor Token-Diebstahl
      1. Schutz vor Cross-Site Scripting (XSS), um das Auslesen von Tokens zu verhindern
      2. Token im HttpOnly-Cookie oder alternativ lokal speichern, aber mit klaren Sicherheitsrichtlinien
   2. Schutz vor Brute-Force- und Credential-Stuffing-Angriffen
      1. Ratenbegrenzung und Sperrmechanismen bei fehlgeschlagenen Anmeldeversuchen
   3. Schutz vor Replay-Angriffen
      1. Einbindung eines Nonce-Systems oder eines Claims wie jti (JWT ID)
   4. CORS-Schutz
      1. Konfiguration, um Zugriff nur von autorisierten Ursprüngen zuzulassen

## Analyse der Benutzerbedürfnisse hinsichtlich Funktionalität und Benutzerfreundlichkeit

1. **Benutzergruppen:**
   1. **Endbenutzer:** Personen, die sich anmelden und auf personalisierte Inhalte zugreifen.
   2. **Administratoren:** Personen, die die Sicherheitsrichtlinien und Benutzerzugänge verwalten.
2. **Funktionalitätsanforderungen:**
   1. **Benutzerfreundliches Login-System:**
      1. Minimaler Aufwand für Benutzer während regulärer Logins (MFA nur bei verdächtigem Verhalten).
      2. Möglichkeit zur Speicherung vertrauenswürdiger Geräte.
   2. **Selbstverwaltung:**
      1. Benutzer können verlorene Geräte oder Tokens über ein sicheres Portal zurücksetzen.
   3. **Dashboard für Sicherheitsübersicht:**
      1. Anzeige der letzten Anmeldungen und verdächtigen Aktivitäten für den Benutzer.
3. **Benutzerfreundlichkeit:**
   1. **Intuitives Interface:**
      1. Leicht verständliche Benachrichtigungen und Anweisungen bei MFA-Anforderungen.
   2. **Schnelle Authentifizierung:**
      1. Minimale Verzögerung durch MFA-Prozesse (Push-Benachrichtigungen, OTPs oder biometrische Optionen).
   3. **Barrierefreiheit:**
      1. Unterstützung für unterschiedliche Geräte und Plattformen (Mobile, Desktop).
   4. **Transparenz:**
      1. Benutzer sollten verstehen, warum MFA verlangt wird (z. B. “Verdächtige Aktivität erkannt”).

### Untersuchung potenzieller Risiken und Schwachstellen in der Anwendung

1. **Technische Risiken:**
   1. **Token-Manipulation:**
      1. Gefährdung durch unsichere JWT-Signaturen.
      2. Verwendung schwacher Algorithmen oder unsicherer Schlüssel.
   2. **Angriffe auf die MFA-Mechanismen:**
      1. Abfangen von OTP-Codes durch Phishing oder SIM-Swapping.
      2. Umgehung von MFA durch Schwachstellen in der Logik.
   3. **Fehlkonfigurationen:**
      1. Ungesicherte Endpunkte, die Tokens ausgeben oder verifizieren.
2. **Benutzerrisiken:**
   1. **Phishing-Angriffe:**
      1. Nutzer könnten durch gefälschte Login-Seiten getäuscht werden.
   2. **Unzureichende Sicherheitspraktiken:**
      1. Benutzer verwenden unsichere Passwörter oder deaktivieren MFA.
3. **Organisatorische Risiken:**
   1. **Fehlerhafte Entscheidungslogik für MFA:**
      1. Falsch positive oder negative Entscheidungen können die Benutzererfahrung beeinträchtigen.
   2. **Skalierbarkeit:**
      1. Steigende Nutzerzahlen könnten die Leistungsfähigkeit der MFA-Entscheidungslogik beeinträchtigen.

# Fazit

Die Anforderungsanalyse hebt hervor, dass eine Balance zwischen Sicherheit und Benutzerfreundlichkeit entscheidend ist. Die JWT-Authentifizierung muss robust gegen Manipulation und Missbrauch sein, während die MFA-Entscheidungslogik dynamisch, präzise und datenschutzkonform arbeitet. Potenzielle Schwachstellen und Risiken sollten durch sichere Entwicklungspraktiken, regelmäßige Penetrationstests und eine klare Benutzerkommunikation minimiert werden.