## **Daten zur Verhaltensanalyse**

Um das Benutzerverhalten zu analysieren und zu bestimmen, ob MFA erforderlich ist, können Sie folgende Daten erfassen:

* **Anmeldehistorie:**
  + Zeitstempel der Anmeldungen (z.B. Uhrzeit und Datum).
  + Häufigkeit der Anmeldungen von verschiedenen Geräten oder Standorten.
* **Geräteinformationen:**
  + Typ des verwendeten Geräts (z.B. Desktop, Tablet, Smartphone).
  + Betriebssystem und Browser-Version.
* **Standortdaten:**
  + IP-Adresse des Benutzers (kann zur Geolokalisierung verwendet werden).
  + Geografische Informationen (z.B. Stadt oder Land).
* **Verhalten während der Sitzung:**
  + Tippmuster (z.B. Geschwindigkeit und Muster beim Eingeben von Passwörtern).
  + Mausbewegungen oder Touchscreen-Interaktionen.
* **Nutzungshäufigkeit:**
  + Wie oft der Benutzer auf bestimmte Funktionen oder Ressourcen zugreift.
  + Welche spezifischen Aktionen in der Anwendung durchgeführt werden.

## **Arten von Multi-Faktor-Authentifizierung**

Es gibt mehrere Arten von MFA, die Sie projektspezifisch implementieren können:

1. **Wissen (Something You Know):**
   * **Passwort:** Der Benutzer gibt ein Passwort ein.
   * **PIN:** Eine zusätzliche persönliche Identifikationsnummer.
2. **Besitz (Something You Have):**
   * **Einmalpasswort (OTP):** Ein temporäres Passwort, das per SMS oder E-Mail gesendet wird.
   * **Hardware-Token:** Physische Geräte, die einen Code generieren (z.B. RSA SecurID).
   * **Smartphone-App:** Authentifizierungs-Apps wie Google Authenticator oder Authy, die zeitbasierte OTPs generieren.
3. **Biometrie (Something You Are):**
   * **Fingerabdruck:** Verwendung eines Fingerabdruckscanners.
   * **Gesichtserkennung:** Biometrische Authentifizierung durch Gesichtserkennungstechnologie.
   * **Stimmerkennung:** Verwendung der Stimme zur Authentifizierung.

4. **Adaptive MFA:**

* + Diese Methode passt die Anforderungen an die MFA basierend auf dem Kontext an. Beispielsweise könnte das System zusätzliche Faktoren anfordern, wenn:
    - Der Benutzer sich von einem neuen Gerät anmeldet.
    - Die Anmeldung von einem unbekannten Standort erfolgt.
    - Verdächtige Aktivitäten erkannt werden (z.B. mehrere fehlgeschlagene Anmeldeversuche).

## **Vorhandene Frameworks und Bibliotheken**

Es gibt mehrere Tools und Frameworks, die Ihnen bei der Analyse des Benutzerverhaltens helfen können:

* **Google Analytics:** Ein weit verbreitetes Tool zur Verfolgung von Benutzeraktivitäten auf Webseiten. Es bietet umfassende Berichte über Nutzerinteraktionen, Verweildauer auf Seiten und Abbruchraten.
* **Hotjar:** Bietet Heatmaps, Aufzeichnungen von Benutzersitzungen und Umfragen. Mit Heatmaps können Sie sehen, wo Benutzer klicken oder scrollen, während Aufzeichnungen Ihnen zeigen, wie Benutzer mit Ihrer Anwendung interagieren.
* **Piwik PRO:** Eine datenschutzfreundliche Alternative zu Google Analytics, die detaillierte Einblicke in das Nutzerverhalten bietet. Es ermöglicht die Analyse von Website-Interaktionen und das Tracking von Konversionen.
* **Mixpanel:** Fokussiert sich auf die Analyse von Nutzerinteraktionen und bietet Funktionen zur Verhaltensanalyse in Echtzeit. Es ermöglicht Ihnen, spezifische Aktionen zu verfolgen und A/B-Tests durchzuführen.
* **Segment:** Eine Customer Data Platform (CDP), die es Ihnen ermöglicht, Daten aus verschiedenen Quellen zu zentralisieren und für Analysen zu nutzen.

## **Anwendung: Finanzmanagement-App**

**Kontext:**

Eine Finanzmanagement-App, die Benutzern hilft, ihre Ausgaben zu verfolgen, Budgets zu erstellen und Überweisungen durchzuführen. Die App verarbeitet sensible Daten wie Bankkontoinformationen und persönliche Finanzen.

## **Szenarien für die Nutzung von MFA**

1. **Szenario 1: Anmelden von einem neuen Gerät**
   * **Verhalten:** Ein Benutzer meldet sich zum ersten Mal von einem neuen Gerät an.
   * **MFA-Methode:** **SMS- oder E-Mail-Verifizierung**
     + Der Benutzer erhält einen einmaligen Code (OTP) per SMS oder E-Mail, den er eingeben muss, um den Anmeldevorgang abzuschließen.
   * **Begründung:** Diese Methode stellt sicher, dass nur der rechtmäßige Benutzer Zugriff auf das Konto hat, auch wenn jemand anderes das Passwort kennt.
2. **Szenario 2: Hohe Transaktion**
   * **Verhalten:** Der Benutzer versucht, eine große Geldüberweisung durchzuführen.
   * **MFA-Methode:** **Biometrische Authentifizierung (Fingerabdruck oder Gesichtserkennung)**
     + Der Benutzer muss seine biometrischen Daten zur Bestätigung der Transaktion verwenden.
   * **Begründung:** Bei großen finanziellen Transaktionen ist es wichtig, sicherzustellen, dass der Benutzer tatsächlich der Kontoinhaber ist. Biometrie bietet eine zusätzliche Sicherheitsebene.
3. **Szenario 3: Verdächtige Anmeldeaktivität**
   * **Verhalten:** Ein Benutzer meldet sich von einem unbekannten Standort oder einer verdächtigen IP-Adresse an.
   * **MFA-Methode:** **Adaptive MFA mit zusätzlichen Sicherheitsfragen**
     + Der Benutzer wird aufgefordert, zusätzliche Sicherheitsfragen zu beantworten (z.B. „Was ist der Name Ihres ersten Haustiers?“).
   * **Begründung:** Diese Methode hilft dabei, potenziell unbefugte Zugriffe zu verhindern, indem zusätzliche Informationen angefordert werden.
4. **Szenario 4: Regelmäßige Anmeldungen**
   * **Verhalten:** Der Benutzer meldet sich regelmäßig von seinem vertrauten Gerät an.
   * **MFA-Methode:** **Push-Benachrichtigung über eine Authentifizierungs-App**
     + Der Benutzer erhält eine Push-Benachrichtigung auf sein Mobilgerät und muss diese bestätigen.
   * **Begründung:** Diese Methode ist benutzerfreundlich und schnell für regelmäßige Anmeldungen, während sie dennoch eine zusätzliche Sicherheitsebene bietet.
5. **Szenario 5: Kontoänderungen**
   * **Verhalten:** Der Benutzer versucht, seine Kontoeinstellungen zu ändern (z.B. Passwort ändern oder E-Mail-Adresse aktualisieren).
   * **MFA-Methode:** **Zwei-Faktor-Authentifizierung (2FA) mit Hardware-Token**
     + Der Benutzer muss einen physischen Hardware-Token verwenden (z.B. YubiKey), um die Änderungen zu bestätigen.
   * **Begründung:** Hardware-Token bieten eine sehr hohe Sicherheit und sind besonders wichtig für kritische Änderungen im Konto.

## **Integration von MFA mit JWT**

1. **JWT-Generierung und MFA-Anforderung:**
   * Bei der Anmeldung eines Benutzers generiert das System zunächst ein JWT, das grundlegende Informationen über den Benutzer enthält.
   * Wenn das System erkennt, dass MFA erforderlich ist (z.B. aufgrund verdächtiger Anmeldeaktivitäten oder spezifischer Benutzerverhalten), wird der Benutzer aufgefordert, einen zusätzlichen Authentifizierungsfaktor bereitzustellen (z.B. einen OTP-Code oder eine biometrische Bestätigung).
2. **MFA-Validierung:**
   * Nach der Eingabe des MFA-Codes durch den Benutzer wird dieser Code validiert. Wenn der Code korrekt ist, wird ein neues JWT generiert, das die MFA-Bestätigung widerspiegelt.
   * Dieses neue JWT kann zusätzliche Claims enthalten, die bestätigen, dass die MFA erfolgreich war (z.B. ein mfa\_verified-Claim).
3. **Token-Scopes und Berechtigungen:**
   * Sie können unterschiedliche Scopes für verschiedene Aktionen definieren. Beispielsweise könnte ein Scope für "Überweisungen" eine MFA-Anforderung auslösen, während der Scope für "Kontostand anzeigen" dies nicht tut.
   * Bei einer Anfrage an die API prüft das System den Scope im JWT und entscheidet basierend darauf, ob zusätzliche MFA erforderlich ist.
4. **Adaptive MFA:**
   * Implementieren Sie adaptive MFA, bei der das System dynamisch entscheidet, ob MFA erforderlich ist oder nicht, basierend auf dem Benutzerverhalten und Kontextinformationen (z.B. Standort, Gerät).
   * Wenn ein Benutzer von einem neuen oder verdächtigen Standort aus auf sein Konto zugreift, könnte das System automatisch eine MFA-Anforderung auslösen.
5. **Token-Validierung:**
   * Bei jeder API-Anfrage überprüft das System das JWT auf seine Gültigkeit und stellt sicher, dass alle erforderlichen Scopes und Claims vorhanden sind.
   * Wenn das JWT gültig ist und die MFA-Bestätigung vorliegt, wird der Zugriff auf die angeforderten Ressourcen gewährt.

## **1. Eigenanteil durch Implementierung von MFA**

* **Entwicklung der MFA-Logik:** Die Implementierung von MFA erfordert eine eigene Logik, um zu entscheiden, wann und wie MFA angewendet wird. Dies beinhaltet das Erstellen von Algorithmen zur Analyse des Benutzerverhaltens und zur Bestimmung der Notwendigkeit von MFA.
* **Integration verschiedener MFA-Methoden:** Sie müssen verschiedene MFA-Methoden (z.B. SMS, E-Mail, biometrische Authentifizierung) in Ihre Anwendung integrieren. Dies erfordert sowohl Backend- als auch Frontend-Entwicklung.
* **Benutzeroberfläche:** Die Gestaltung einer benutzerfreundlichen Oberfläche für die MFA-Anforderungen ist ein kreativer und technischer Eigenanteil. Dies umfasst das Design von Formularen und Interaktionen, die den Benutzern helfen, die MFA einfach zu durchlaufen.
* Diese Integration erfordert fundierte Kenntnisse in der Softwareentwicklung, Sicherheit und Benutzererfahrung. Daher erfüllt Ihr Projekt die Anforderungen Ihres Professors hinsichtlich eines signifikanten Eigenanteils an der Entwicklung.