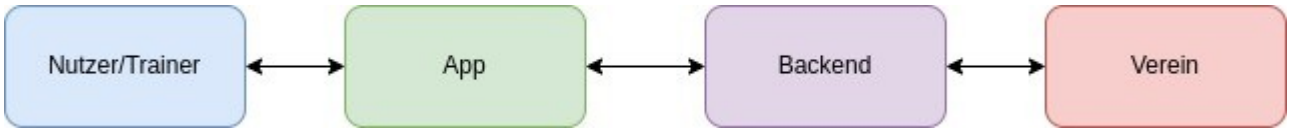
Sicherheitsanalyse FitXchange:

1. Die App basiert auf einer Basis des Datenaustausches. Der Datenaustausch erfolgt zwischen dem Nutzer und der App, sowie zwischen der App und dem Sportverein (Hochschulsport, VHS usw.). Aufgrund dieses Vorganges, müssen ausgetauschte Daten DSGVO konform sein und ausreichend Sicherheit vorweise, damit sensible Nutzerdaten nicht in die Öffentlichkeit gelangen können.



Stakeholders:

→ Hochschule Fulda bzw. Hochschulsport
→ Volkshochschule
→ Nutzer/Trainer

Assets:

→ Nutzerdaten

Die Datenaustausch erfolgt in beide Richtungen, vom Nutzter bis zum Verein und umgekehrt.

1. Vertraulichkeit:
   • Bedrohung: Abfangen der Kommunikation oder lesen der Daten auf einer externen Festplatte
   • Mechanismus: Verschlüsselung der Daten
2. Integrität:
   • Bedrohung: Andern der Kommunikation oder starten unerwünschter Programme auf einem Rechner
   • Mechanismus: Checksumme (z.B. CRC32) oder kryptographische Hashfunktion
3. Authentizität:
   • Bedrohung: Senden einer eMail unter falschem Namen
   • Mechanismus: Fingerabdruckscanner
4. Verfügbarkeit:
   • Bedrohung: Uberlasten eines Servers mit vielen Anfragen
   • Mechanismus: Redundante Auslegung der Infrastruktur
5. Autorisierung:
   • Bedrohung: Login unter einem anderen Benutzernamen
   • Mechanismus: Passwortabfrage
6. Verbindlichkeit:
   • Bedrohung: Käufer*in zahlt für Produkt, Verkäufer*in leugnet Erhalt der Zahlung und verweigert Ubergabe des Produktes
   • Mechanismus: Digitale Signaturen oder Loggen von Events zum Vorzeigen gegenüber einer vertrauenswürdigen dritten Partei

(Auszug aus IT-Sicherheit Vorlesung – Prof. Dr. Zohner)

	Vertraulichkeit	Integrität	Authentizität	Verfügbarkeit	Autorisierung	Verbindlichkeit
Nutzerdaten	X	X		X	X	

Aus der Architektur und auf Basis der Sicherheitsanalyse wurde es festgestellt, dass Vertraulichkeit, Integrität, Verfügbarkeit und Autorisierung unabdingbar ist. Dazu folgen entsprechende Sicherheitsmaßnahmen:

Sicherheitsmaßnahmen

Der Kommunikationsfluss muss mit aktuellsten Sicherheitsmechanismen abgesichert werden. Für die App wurde die Sprache “flutter” benutzt. Diese bietet auch eine eigene Bibliothek mit der Möglichkeit der Implementierung von TLS(Transport Layer Security) 1.2. Im Fall vom fitXchange muss diese auch genutzt werden, damit die Daten über einen sicheren TLS Kanal zwischen zwei Endpunkten fließen. Somit gewärleistet TLS die **Authentizität**, **Integrität** und **Vertraulichkeit** der Daten.

Der Aufbau von der App erfolgt anhand von Nutzter Konten. Jeder Nutzter muss ein eigenes Konto anlegen, mit dem dieser sich anmelden soll. Die Passwörter werden nicht im Backend im Klartext gespeichert, sondern mittels dem neuesten SHA-256 hash Verfahren. Damit werden nur Passwort hashes verglichen und nicht Klartext-Passwörter. Somit kann, falls die Kommunikation abgefangen werden sollte, der Angreifer mit den Hashes nichts anfangen. Hiermit wird auch die **Autorisierung** der Daten gewährleistet.

Damit die App auch zu jedem Zeitpunkt sicher verfügbar ist, muss die Architektur redundant ausgestellt werden. Falls ein Server ausfällt, kann ein anderer die Aufgaben übernehmen. Mit diesem letzten Schritt wird auch die **Verfügbarkeit** gewährleistet.

DSGVO

Die App “fitXchange” wird sicherheitskonform gemäß der DSGVO Daten übermitteln. Es werden keine weiteren Daten von Nutzern (außer Email und Passwort) in der Datenbank gespeichert. Diese Daten werden noch dazu mittels SHA-256 gehasht. Der Nutzer von unserer App muss somit die DSGVO Voraussetzungen annehmen. Diese werden bei dem Datenaustausch und/oder auch bei der Datenspeicherung in Zukunft durchgesetzt.