Konzept M183

# Was gilt es zu erreichen?

Im Rahmen der Projektarbeit im Modul 183, möchte ich in eine bereits bestehende EJS-Applikation um eine 2FA Anmeldemöglichkeit erweitern.

# Was besteht bereits?

Zurzeit besteht eine mehr oder weniger simple CRUD-Applikation, bei welcher man verschiedene Arten von Daten eingeben kann, welche dann in einer MongoDb abgespeichert/ mutiert werden.

# Grobe Umsetzungsidee

Dies soll einerseits aus einer herkömmlichen Passworteingabe bestehen, welches einen Wissens-Faktor darstellt. Das Passwort soll auf heute entsprechende Sicherheitsstandards (Min. 14. Zeichen, Kleinbuchstaben, Grossbuchstaben, Zahl und Sonderzeichen) überprüft werden. Zudem soll es einen zweiten Teil geben, welcher einen Habens- oder sogar Seins-Faktor benötigt. Dieser soll ergänzend zum Wissens-Faktor zusätzliche Sicherheit erzeugen. Zudem soll nach Abschluss eines erfolgreichen Logins eine Session gestartet werden. XSS soll ebenfalls abgedeckt werden, so, dass man vor erfolgreichem Login, sich nicht via URL auf der Website navigieren kann.

# Potenzielle Umsetzungsideen

## SSO (Single Sign On)

Bei der SSO, werden Anmeldedaten eines anderen Services verwendet, um diese ebenfalls für die zu registrierende Website zu verwenden. Dabei werden Daten von einem Server angefragt, nachdem der Benutzer dies mit dessen Anmeldedaten bewilligt hat.

Diese Umsetzungsidee wäre umsetzbar, jedoch wären die Daten ausserhalb der eigenen Kontrolle und zusätzliche Sicherheit wie regelmässiges Ändern des Passwortes wäre nur schwer forcierbar/ voraussetzbar.

Vorteile:  
+ Grösserer Komfort für Nutzer, weil weniger Passwörter  
+ Geringeres Risiko für erfolgreiche Attacken  
+

Nachteile:  
- Gewisser Implementierungsaufwand  
- Starke Abhängigkeit von Unternehmen mit Anmeldedaten des Nutzers  
-

## TOTP (Time-based one-time password)

Beim TOTP wird mittels QR-Code auf einem Gerät ein Zahlencode dargestellt, welcher sich in einem bestimmten zeitlichen Abstand ändert. Durch Eingabe dieses TOTP kann der Benutzer auf seine Authentizität überprüft werden, bzw. auf den Besitz dessen Verifizierungsgerätes.

Dessen Implementation sollte problemlose machbar sein, zudem können potenzielle Informationen sehr einfach auf der MongoDb-Datenbank ergänz werden.

Ob man Daten eventuell verschlüsselt bzw. gehashed ablegen möchte lässt man zum jetztigen Zeitpunkt erst einmal offen. Potenzielle Daten könnten ohne Problem in der MongoDb abgespeichert werden.

Vorteile:  
+ Dauernde Änderung des TOTP-Passwortes  
+ Mehr Sicherheit dank zweitem Authentifizierungsfaktor  
+

Nachteile:  
- Abfangen des einmaligen geheimen Schlüssels macht Authentifizierung nutzlos  
- Benötigt Authentifizierungsgerät (eventuell für Personen 65+ nicht mehr sehr verständlich)  
- Erhöhter Aufwand für Nutzer

## FIDO2/ Passkeys

Fido2 bzw. die Verwendung von Passkeys wäre die wohl mit Abstand sicherste und modernste Methode. Dabei wird mittels eines Hardware Devices und biometrischen Daten des Benutzers dessen Authentizität überprüft, nachdem dieser seine Anmeldedaten eingegeben hat.

Diese Methode ist zwar ziemlich sicher, deren Implementation wäre jedoch mit dem grössten Aufwand verbunden. Einerseits da wenig oberflächliches Vorwissen vorhanden wäre, andererseits, da man sich einen solchen Hardwarekey besorgen müsste und damit die Implementation nach und nach testen müsste.

Vorteile:  
+ Heute ziemlich sicher  
+ Schüssel in Besitz des Benutzers  
+ Grosses Potenzial in Zukunft

Nachteile:  
- Komplex  
- Kostenaufwändig  
- Zurzeit nur kleinen Anwendungsbereich

# Entscheid

Für die Umsetzung der 2FA-Implementierung im Modul M183 möchte ich eine simple Passwortanmeldung, mit gewissen Passwortanforderungen, sowie ein TOTP implementieren. Zudem wäre das Ziel, eine simple XSS-Verhinderung zu implementieren.

Ich habe mich für diese Methode entschieden, da es heutzutage eine weitverbreitete, akzeptierte Methode ist und für deren eher geringe Komplexität eine hohe Sicherheit bietet. Zudem stellt es neben dem Wissens-Faktor des herkömmlichen einen Habens-Faktor dar, welcher den zweiten Authentifizierungsfaktor darstellt und somit die Sicherheit durchaus erhöht.  
Das herkömmliche Passwort möchte ich beibehalten, da dies aus meiner Sicht nach wie vor zu einer Standardlogin dazugehört und für einen Durchschnittsbenutzer auch dazugehört. Man könnte es durch andere Methoden ersetzen, jedoch besteht dann die Möglichkeit, dass es diesen, aufgrund fehlenden Verständnisses, verunsichert und das Vertrauen gegenüber der Website mindert. Zudem ist für TOTP bereits ein gewisses Vorwissen vorhanden ist, welches mir die Implementierung erheblich erleichtern wird.