**Autentificare, Autorizare și Login**

**Autentificarea** este procesul prin care o aplicație verifică identitatea utilizatorului. Scopul este să se asigure că utilizatorul este cine pretinde că este.

Username și parolă: metoda clasică.

Autentificare cu doi factori (2FA): utilizarea unui cod trimis pe telefon sau e-mail.

Biometrie: recunoașterea facială sau amprentă.

SSO (Single Sign-On): utilizatorul se autentifică o singură dată pentru a accesa mai multe aplicații.

**Autorizarea** este procesul de a decide ce resurse și acțiuni poate accesa un utilizator după autentificare.

Exemple:

Un utilizator „admin” are acces la setările aplicației, pe când un utilizator obișnuit nu.

Restricționarea accesului la anumite funcționalități în funcție de rolul utilizatorului.

**Login-ul** reprezintă procesul de conectare la o aplicație, implicând de obicei autentificarea utilizatorului. Este punctul de acces inițial pentru orice sistem securizat.

**Cum se realizează login-ul într-o aplicație?**

Interfață de login: Utilizatorul introduce credențialele (e.g., nume de utilizator și parolă) într-un formular.

Validare: Serverul validează datele primite prin compararea lor cu cele stocate într-o bază de date securizată.

Autentificare: Dacă datele sunt corecte, serverul generează un token (e.g., JWT) sau o sesiune activă.

Metode suplimentare de securitate

Autentificare cu doi factori (2FA): Adaugă un strat suplimentar de protecție printr-un cod unic (OTP) trimis pe telefon sau printr-o aplicație precum Google Authenticator.

Autentificare biometrică: Utilizarea amprentei, recunoașterii faciale sau vocale pentru a asigura identitatea utilizatorului.

Parole puternice și politică de schimbare a parolei: Cerințe stricte pentru parole (e.g., lungime minimă, caractere speciale) și schimbarea lor periodică.

Protecție împotriva atacurilor brute-force: Limitarea numărului de încercări de login și blocarea contului după un număr specific de încercări eșuate.

HTTPS și criptare: Toate comunicațiile dintre utilizator și server sunt criptate pentru a preveni interceptarea datelor.

Monitorizare și alerte: Detectarea și notificarea activităților suspecte, cum ar fi autentificările de pe dispozitive necunoscute sau din locații neașteptate.

Aceste măsuri combinate asigură un nivel ridicat de securitate pentru aplicații și protejează datele utilizatorilor.

Un aspect esențial al securității parolelor este utilizarea unui algoritm de criptare unidirecțională, adică fără un mecanism de decriptare. Aceasta înseamnă că, odată criptată, parola nu mai poate fi recuperată înapoi într-o formă lizibilă, chiar și în cazul în care cineva reușește să acceseze datele criptate. Această abordare reduce semnificativ riscurile asociate cu breșele de securitate.

Un exemplu de metodă mai puțin sigură este criptarea simetrică, cum ar fi algoritmul Vigenere Cipher, care folosește o cheie pentru criptare și aceeași cheie pentru decriptare. Dacă un atacator ajunge să descopere cheia folosită, poate cu ușurință să decripteze toate parolele, având acces la informațiile sensibile. De aceea, se recomandă utilizarea unor algoritmi de criptare unidirecționali, precum bcrypt sau Argon2, care sunt concepuți să fie imposibil de inversat, chiar dacă algoritmul este cunoscut. Aceste metode adaugă un strat suplimentar de protecție, prevenind expunerea parolelor în cazul unei breșe de securitate.

A screenshot of a computer

Description automatically generated