# **7.b** Vesse össze a Microsoft és az IBM által nyújtott eszközöket felhasználó- és hozzáférés menedzsment szemszögből!

# Felhasználó és hozzáférés kezelés

* Identity and Access Management (IAM)
* Segítségével azonosítják, hitelesítik és engedélyezik a felhasználók hozzáférését az adatokhoz, alkalmazásokhoz és szolgáltatásokhoz.
* **Négy** A**-ből tevődik össze:**
  + Adminisztráció
    - **Felhasználó/Identitás kezelés**
  + Autentikáció – Ki vagy?
    - **Hozzáférés kezelés**
  + Autorizáció – Mit akarsz csinálni?
    - **Hozzáférés kezelés**
  + Audit
    - Azt a célt szolgálja, hogy megbizonyosodjunk arról, hogy biztosan jól csináltuk az **Adminisztráció**-t, **Autentikáció-**t, **Autorizáció**-t.

## IAM rendszer problémák, megoldások

### Megfelelő hozzáférés a megfelelő személyek számára

* **Probléma**
  + A felhasználók rendelkeznek nem szükséges jogokkal.
* **Megoldás**
  + Biztosítja, hogy a felhasználók a számukra nem szükséges bizalmas információk elérésének lehetővé tétele nélkül hozzáférjenek azokhoz az erőforrásokhoz, amikre szükségük van.

### Akadálytalan munkavégzés

* Fontos a felhaszálói élmény.
* **Problémák**
  + Többszöri bejelentkezések és jelszavak bekérése.
* **Megoldás**
  + Single-Sign-On (SSO) bevezetése, amivel csak egyszer kell bejelentkezni a felhasználóknak.

### Adatbiztonsági incidensek elleni védelem

* **Probléma**
  + Adatbiztonsági incidensek kockázata
  + Feltörések
* **Megoldás**
  + További biztonsági réteget ad hozzá a bejelentkezési folyamathoz.

### Adattitkosítás

* **Probléma**
  + Bizalmas adatok nincsenek védve.
* **Megoldás**
  + Titkosítás használata, például AES, RSA vagy SHA megoldásokkal.
  + Használhatunk titkosítást az adatok tárolására, adatátvitelkor vagy a hitelesítő adatokhoz.

# Identity

* Öntudat, identitás
* Hitelesítési információk olyan csoportja, amik a rendszer egy adott egyedét egyértelműen meghatározzák.

# User provisioning

* Felkészülés, szolgáltatás
* Felhasználói fiókok létrehozása és jogosultságaik beállítása cél erőforrásokon.

# IBM központ felhasználó menedzsment = IBM Tivoli

* A felhasználók a rendszerrel kapcsolatos jogosultságainak kezelése.
* A szervezetbe történő belépéstől a kilépésig.
* Előnyei:
  + A felhasználók csak olyan alkalmazásokat, adatokat érhetnek el, amikhez joguk van.
  + A jogosultságok menedzselése folyamatosan és centralizált.
  + A jogosultságot központilag azonnal le lehet tiltani, ha szükséges.

# Integrált jogosultság kezelés

* A felhasználók a jogosultságuk szerint különböző felhasználói azonosítókkal és jelszavakkal elérhető más rendszereket, alkalmazásokat, adatokat egy központi jelszóval elérik.
* Képes a más rendszerek, alkalmazások, adatok eléréséhez szükséges jelszavak automatikus generálására, a bejelentkezési és azonosítási folyamatok elvégzésére.
* Előnyei:
  + Csak egy jelszóval tud belépni a felhasználó.
  + Könnyű kezelhetőség, automatizálhatóság.
  + Minimalizálja a problémák, tévedések lehetőségét.

# Identity Manager működési modellje „Role Based”

* A felhasználó felelősségi körnek megfelelő szerepkörhöz rendelés.
* A szerepkör tagjainak erőforráshoz rendelése.
* Provisioning Policy attribútumokat is meghatározhat.
  + Felhasználó lemezterület kvóta
  + Csoport-tagság

# Microsoft

* Active Directory és csoportházirendek.
* Felhasználók központi menedzselése
  + Jelszó jogosultságok
  + Csoportok
  + Szervezetek
* A csoportházirendekkel az AD csoportjaihoz rendelhetünk jogosultság-gyűjteményeket, amik az adott csoport tagjaira lesznek érvényesek.
  + Adott felhasználónál egy adott jogosultság felüldefiniálható.