Adattárház biztonság és a felhő

Adattárház alapok biztonsági szemmel I.

- Az adattárház egy tárgy/témaorientált, integrált, tartós és időfüggő adatok gyűjteménye, melynek **egyetlen célja** van: a menedzsment döntéseinek támogatása.
- A benne lévő információk:
  - Mindig valamilyen tárgyhoz vagy témához köthetőek (ügyfelek, rendelések..)
  - Mindig valahonnan, más rendszerekből jönnek
  - Összesítődnek és egységesülnek valamilyen üzleti dimenzió (termék, régió) alapján
  - Mindig meghatározott időben töltődnek be (napi, heti, havi..)
  - Időbélyeggel látjuk el őket
  - Meghatározott időre, tartósan tárolódnak
  - Nem változnak az idő múlásával

Adattárház alapok biztonsági szemmel II.

Adatok köre
- Meghatározás és feltárás
- Besorolás

Felhasználók
- Top-down megközelítés
- Funkció szerinti bontás

Forrásrendszerek
- Hatás és ellenhatás

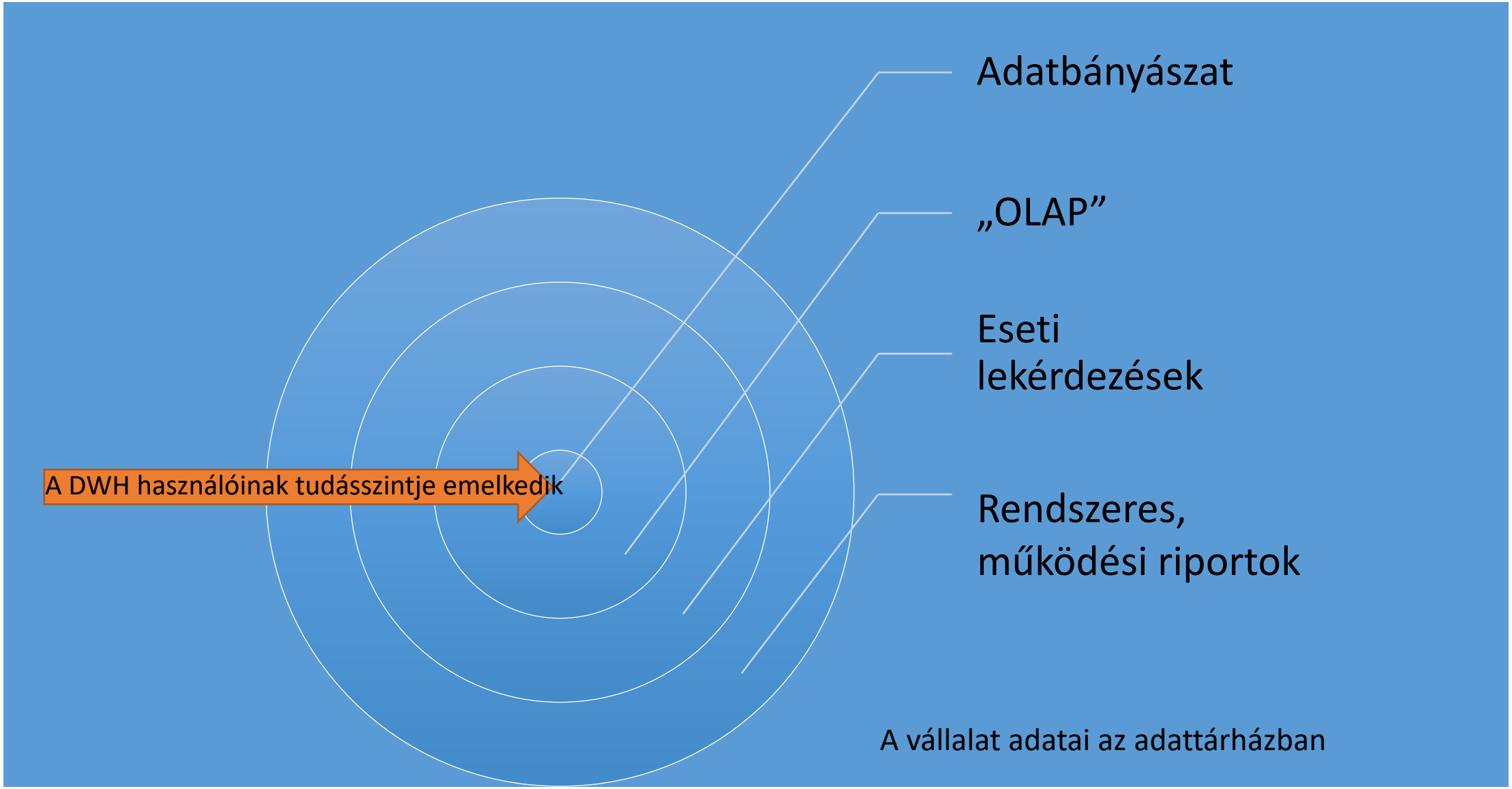
Hálózatok
- Bizalmasság
- Integritásvédelem

Kulcsmozzanatok
- Az adatok kinyerése
- Adat-transzformáció
- Riportkészítés és disztribúció

Auditálhatóság
- Ki, mit, mikor, honnan-hova, mivel

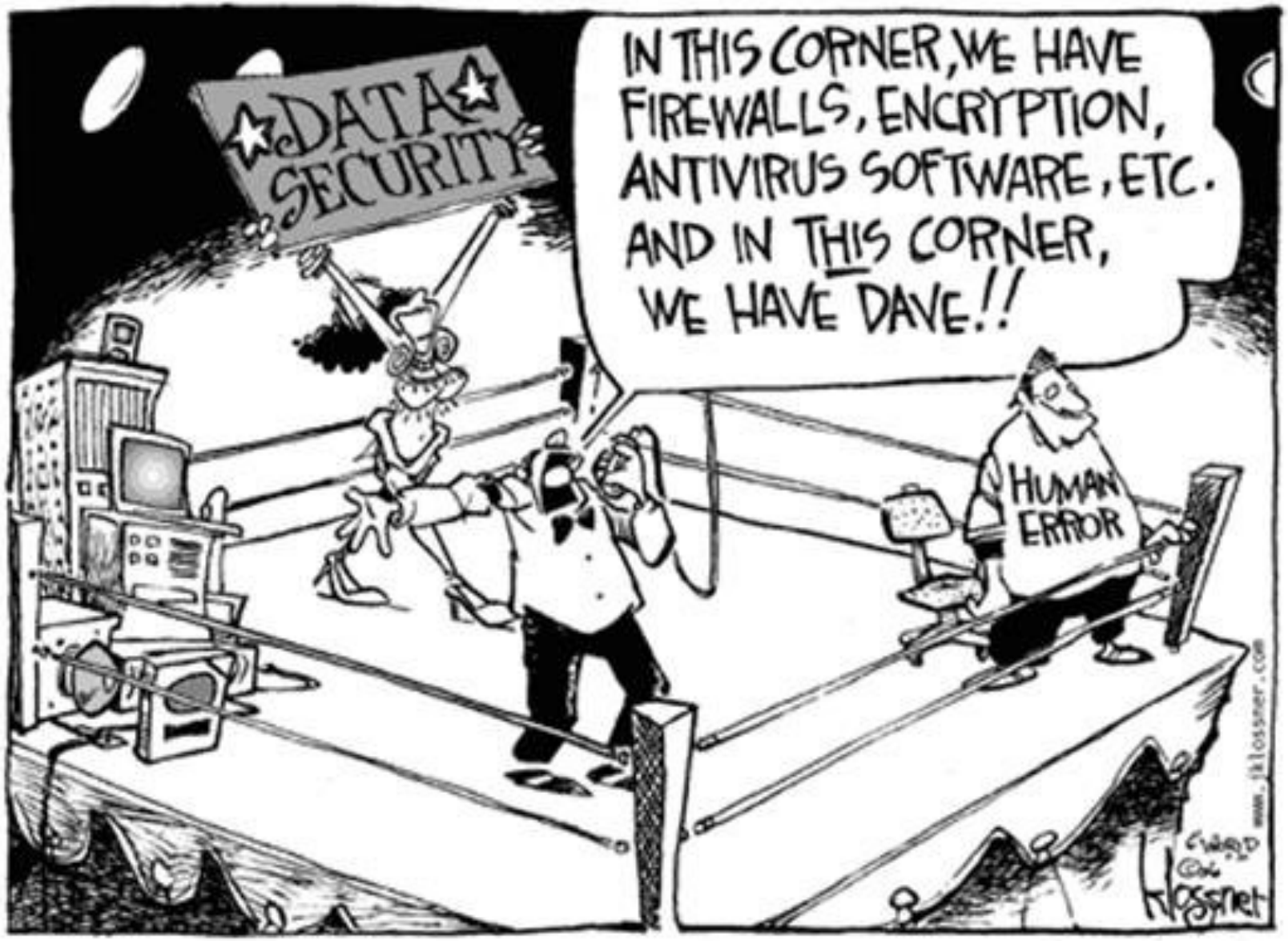
Infrastruktúra és performancia
- Még nem elég biztonságos, de már használhatatlan

Felhasználói kockázatok



Biztonsági megközelítés I.

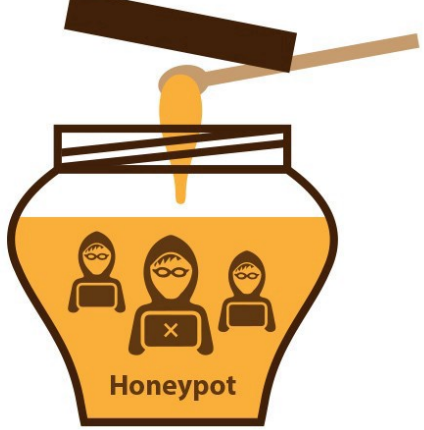
- Az Ember
  - Rendszeres tréningek
  - Kötelező gyakorlatok
  - Vizsgák
  - Játékok
  - Specifikus Adattárház oktatások



Biztonsági megközelítés II.

- Fizikai biztonság: elfelejteni a legkönnyebb, nagyot bukni rajta az egyik legegyszerűbb
  - Adatközponti kontrollok
  - Biztonsági protokollok
- Szoftveres védelem és technikák
  - Jelszószéf
    - Dokumentáció!?
  - Titkosítás: *szinte* minden feltörhető, de azért AES és FIPS
    - Performancia hatások? 
  - Adatszegmentáció és particionálás
    - Adatklasszifikáció
  - Adattovábbítási csatorna védelme: SSL, tunneling…

Biztonsági megközelítés III.



- Szoftveres védelem és technikák
  - Honeypot
  - E-mail biztonság
  - Központi jogosultságkezelés
    - RBAC
    - Least Privilige Principle
    - Rigorózus felülvizsgálatok
    - KPI és KRI set-ek
  - **Desktop** biztonság
    - Adatszivárgás elleni védelem
  - Hálózatbiztonság
    - Hálózati szegmentáció
  - Multi-layer védelmi szintek és más, jó gyakorlaton alapuló biztonsági módszertan követése
  - Rendszeres öntesztelés és önfeltörés

Irány a felhő – de miért?

- Túl nagy, és még annál is nagyobb
- Túl komplex, túl sokba kerül
- Senki nem érti már a logikákat és a lekérdezéseket
- Performancia és rendelkezésre állási problémák
- Kötelező feladatok
  - Adatduplikáció
  - Jelentési kötelezettségek
- Üzleti hatékonyságnövelés
  - Hibrid modellek
  - Szinte végtelen slákázhatóság
  - Széleskörűbb automatizálhatóság
  - Több tesztelési lehetőség
  - Viszonylag egyszerű migráció

Felhőbiztonság – EU módra

Exit stratégia

Adatbiztonság

Üzleti hatáselemzés

Üzletmenet folytonosság

Tanúsítványok és minősítések

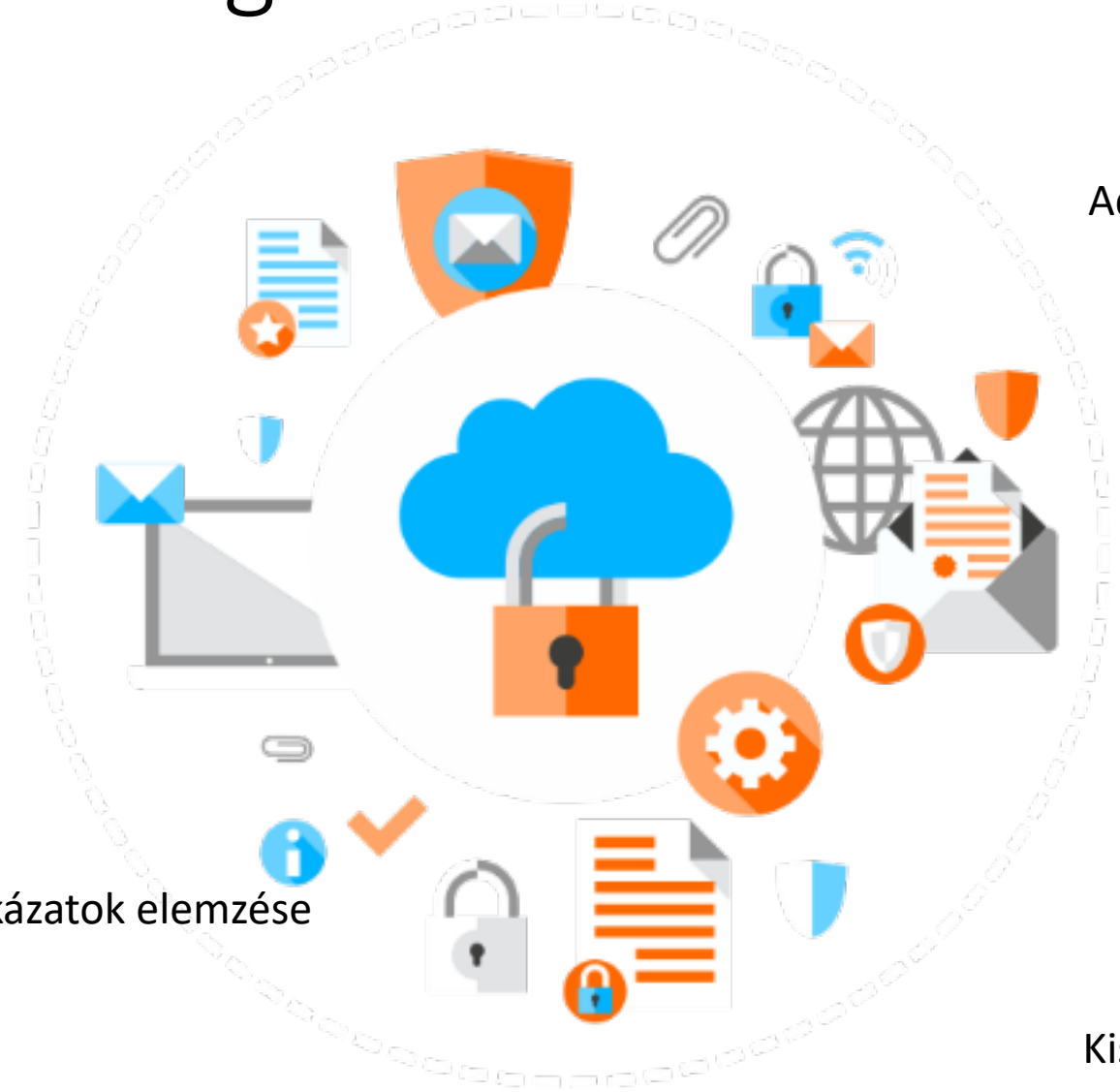
Adatvédelem

Jogi megfelelés

Biztonsági kockázatok elemzése

Kiszervezési kötelezettségek

Adattárolási keretek



Felhőbiztonság a gyakorlatban

- A kontroll elengedésének első döbbenete után..
- Régi kontrollok: adapt or die
  - Az új környezetre való transzformáció
  - Testreszabás
- Új kontrollok
  - Új eszközök
  - Cloud-specifikus use case-ek
  - Integráció - API
  - Automatizálás – Robotok
  - Optimalizálás
  - Szabályozás és módszertan újragondolás