Felhőtlen biztonság

TDK-konferencia
2013.11.27.

Dr. Horváth Attila

Országos Tudományos és Kutatási
Alapprogram PD-109740

A projekt:

IT- és hálózati sérülékenységek áttételes gazdasági-társadalmi hatásai

- Növekvő digitális konvergencia
- Az adatok, infrastruktúra és szolgáltatások koncentrációja
- Magán/Üzleti/Kormányzati
- Az IKT kritikus szerepe
- Rendszer szintű sérülékenységek
- Az elsődlegesen technológiai problémák és döntések gazdasági és társadalmi hatásvizsgálata
  - Pénzügyi és közgazdasági megközelítés szükséges

Gyorsan terjedő felhőszolgáltatások

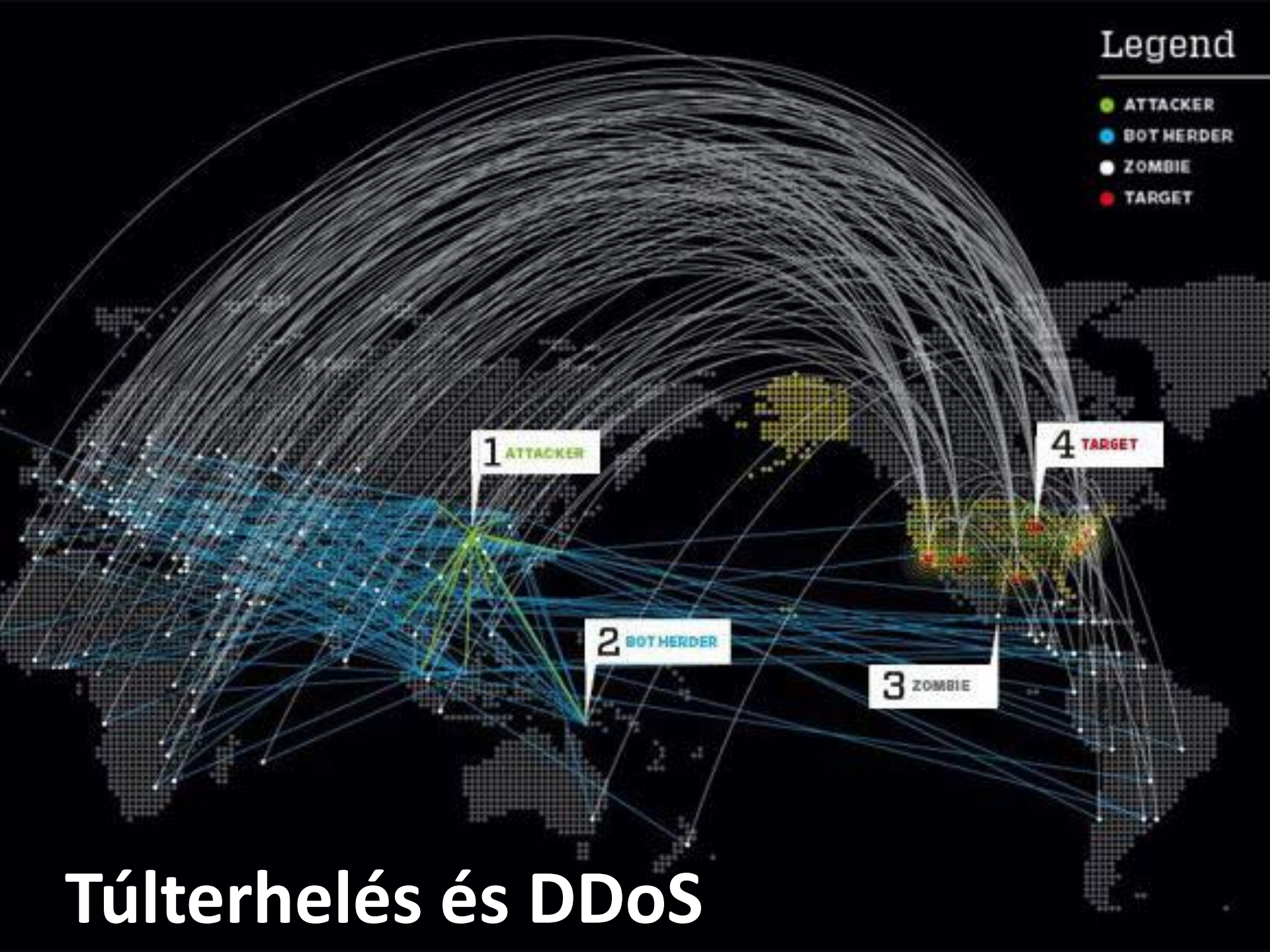
- IDC: a felhőszolgáltatások éves növekedési üteme Nyugat-Európában 35%, 2015-re 15 mrd euros üzletág lesz
- Gartner: a vállalatok 33% már használ SaaS típusú szolgáltatásokat Business Intelligence célokra
- At&T: a vállalatok 37%-a használja a felhőt, hogy javítsa az üzletmenet-folytonosságot
- Forrester: IaaS penetráció:
  - 18% a technológiai iparban (további 25% tervezi);
  - 10% a kormányzati szektorban (további 5% tervezi)

A kiszolgált ügyfelek

- Google: >500 millió android aktiváció évente,
    - US General Services Administration, Essilor, Ispen, BBVA Spain, Capgemini, SNL Financials, Salesforce.com, Essence, The Guardian, LSI Logic, The Telegraph
- Amazon Cloud
  - Az észak-amerikai teljes internetforgalom 1%-a átmegy rajta
  - Az internetezők harmada naponta látogat olyan oldalakat, amelyek az az Amazon felhőszolgáltatásain futnak
    - Zynga, Animoto, Reddit, MySpace, Netflix, Dropbox, airbnb, Ericssons, European Space Agency, HootSuite, IBM, Mahindra Satyam, Newsweek, UniCredit, Spiegel.Tv, PBS, Yelp, IMDB, Linden Labs, FourSquare, SmugSmug, Alexa, The Guardian, Farmville, Sitepoint, EventBrite.
- Rackspace (>200k ügyfél)
    - Transport of London, Virgin Trains, UK MoD, NHS Direct, Fiverr, Pitchfork, The Register, the Royal Navy, and TweetPhoto
- …

A Felhő-szolgáltatások kritikusak


Védelem a természeti katasztrófáktól

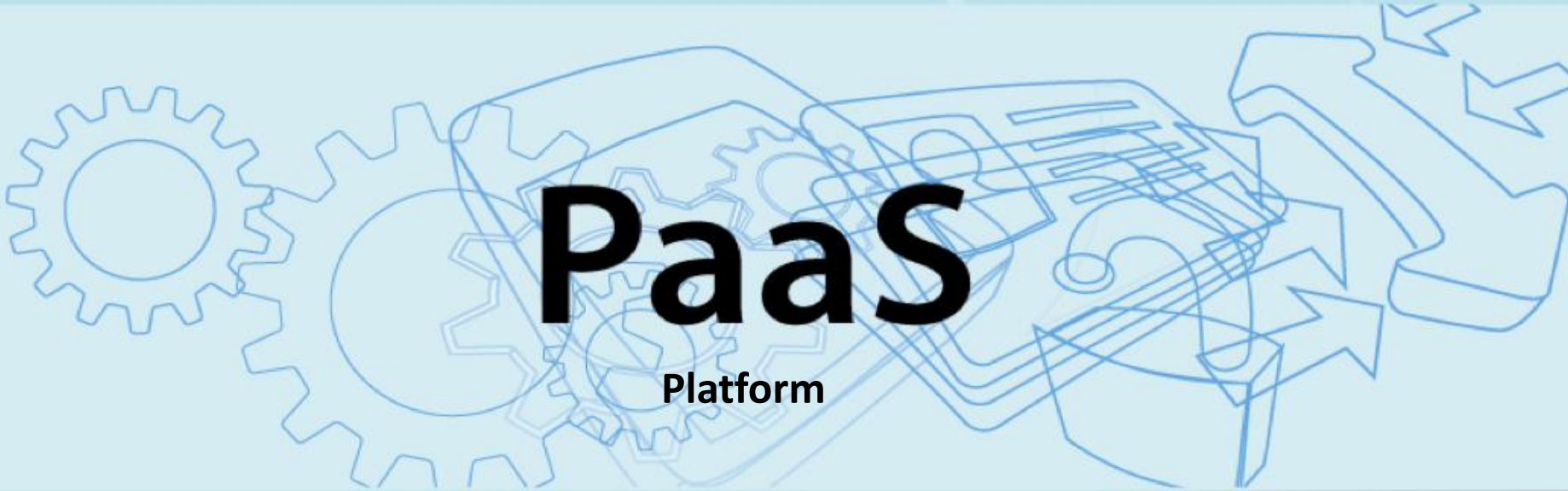


Túlterhelés és DDoS

Koncentrált kiber-támadások

SaaS

Szoftver



PaaS

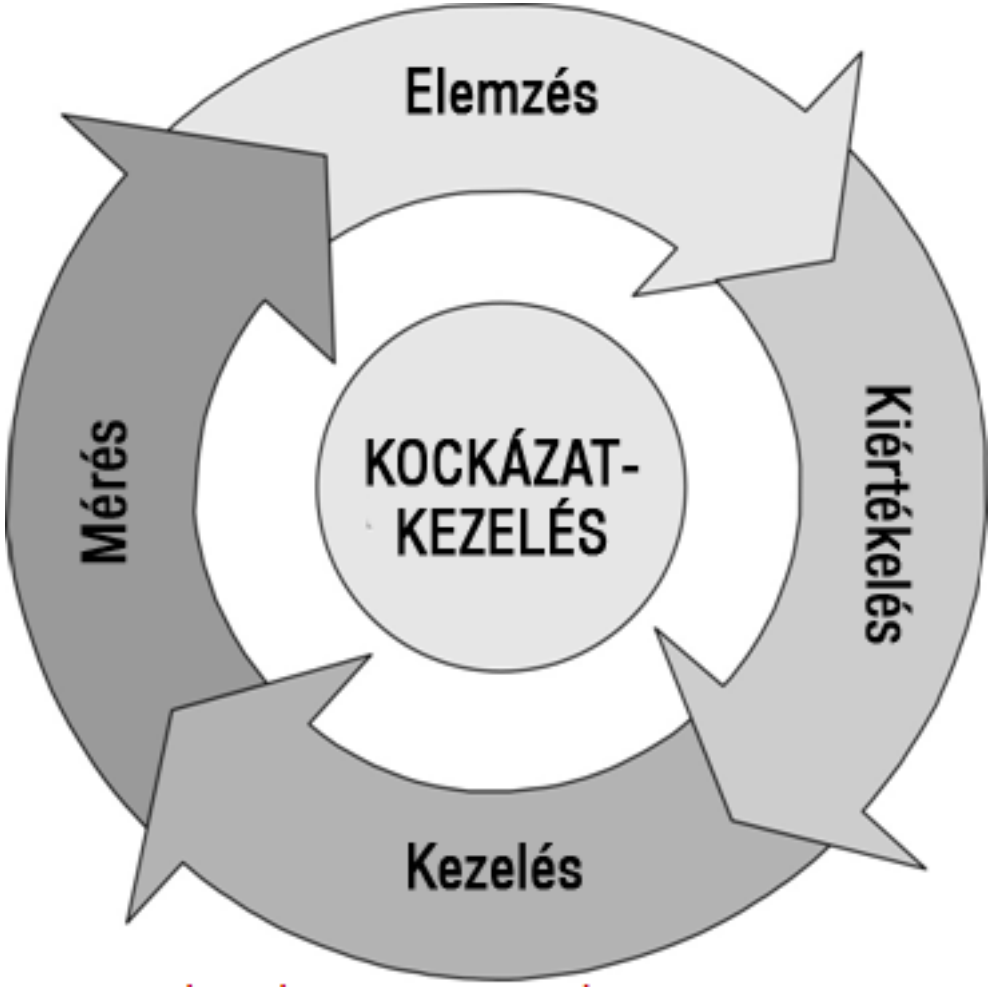
Platform

IaaS

Infrastruktúra

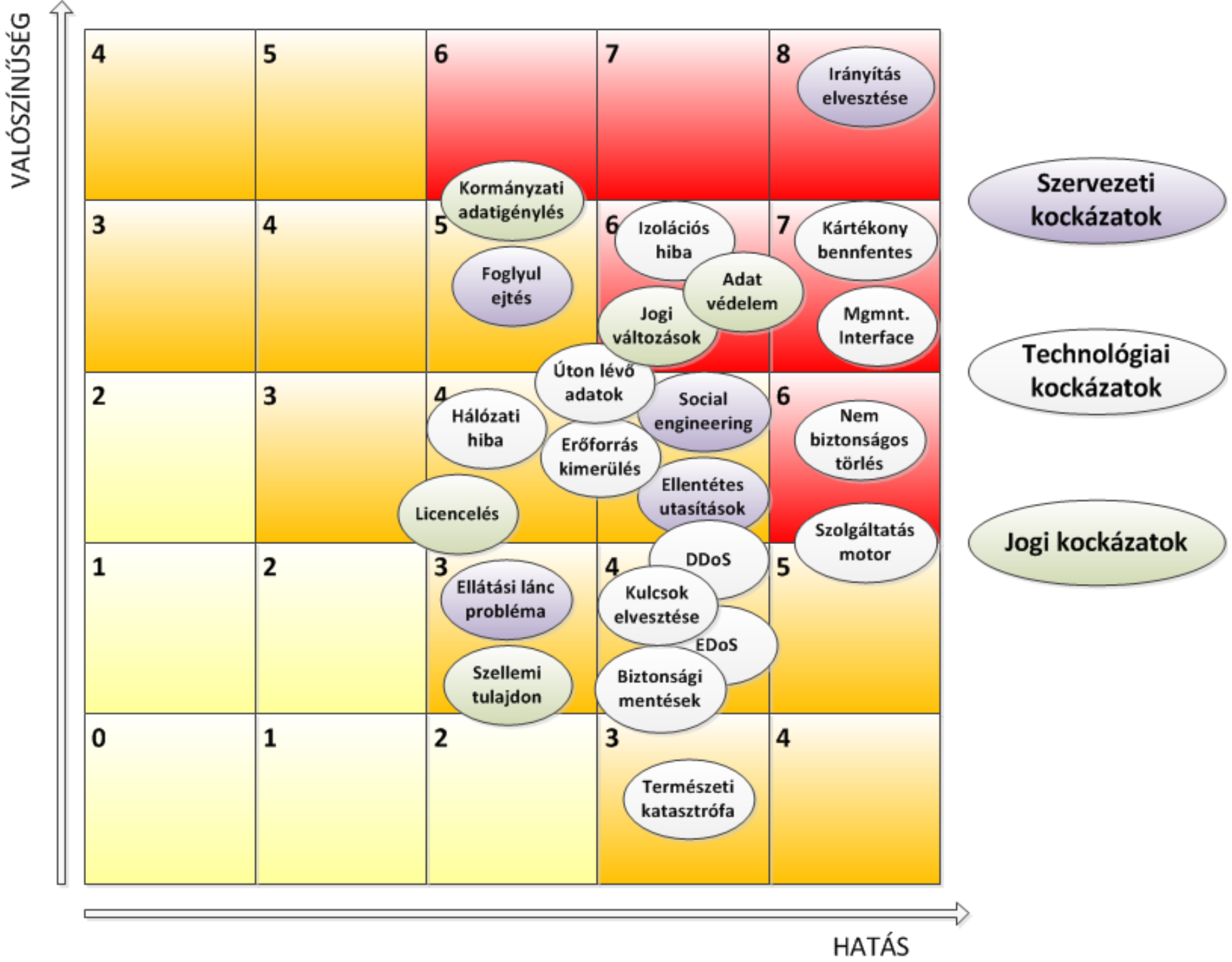
Adminisztratív- és jogi viták

Kockázat kezelés



Fókusz

- Először a legkritikusabb szolgáltatások
  - IaaS &PaaS
- A felhőtől való függőségek
  - A kritikus infrastruktúra része
  - Azonos szint az energia-ellátással és a kommunikációs csatornákkal
- Átláthatóság javítása - feltérképezés
  - Critical operators and critical services
  - Rugalmasság vs. Kölcsönhatások és tovagyűrűző hibák
  - Más, egyébként függetlennek látszó területeket is érint


VALÓSZÍNŰSÉG
HATÁS
4
5
6
7
8
Irányítás elvesztése
3
4
5
Kormányzati adatigénylés
Foglyul ejtés
6
Izolációs hiba
Adat védelem
Jogi változások
7
Kártékony bennfentes
Mgmnt. Interface
2
3
4
Hálózati hiba
Licencelés
Úton lévő adatok
Social engineering
Erőforrás kimerülés
Ellentétes utasítások
6
Nem biztonságos törlés
Szolgáltatás motor
1
2
3
Ellátási lánc probléma
Szellemi tulajdon
4
DDoS
Kulcsok elvesztése
EDoS
Biztonsági mentések
5
0
1
2
3
Természeti katasztrófa
4
Szervezeti kockázatok
Technológiai kockázatok
Jogi kockázatok

BIZTONSÁGI INTÉZKEDÉSEK

Best practice-ek

- Nincsenek még igazi felhő-biztonsági szabványok
- A legjobb biztonsági szint a BP-eken keresztül érhető el
- Tudásmenedzsment: a tapasztalatcsere támogatása és elősegítése
- Folyamatos fejlesztés
- Veszélyesek a kőbe vésett szabályok
  - Szabályozók vagy ön-szabályozás?

Logikai redundancia

- A fizikai redundancia már megvalósult
  - Különálló adatközpontok katasztrófa esetére
- A támadások inkább a szoftver-sérülékenységeket aknázzák ki
  - Ha ugyanaz a szoftver fut minden központban…
- Kulcs a logikai redundancia
  - A védelem különböző rétegei
  - Elkülönített rendszerek különböző logikai struktúrákkal
    - Tranzakciók kereszt-ellenőrzése
    - Behatolás-érzékelés

Szabványosítás

- A standard API-k használata elsőrendű fontosságú
- Ezzel elkerülhetők egy adott szolgáltató vagy platform típushibái
- Megkönnyíti a szolgáltató-váltást
- Szükséghelyzetben a terhelés megosztható több szolgáltató között
  - Kiesés
  - Rendszerhiba
  - Jogi vagy adminisztratív problémák
  - Stb.

Monitoring, audit, tesztek és gyakorlatok

- Gyakori audit
  - Belső és külső tesztelők
- Túlhangsúlyozott a külső auditorok általi tanúsíttatás
  - A felhő-biztonság túl komplex és változó ahhoz, hogy „egyszer egy évben” – típusú audittal jól felmérhető lenne.
- Folyamatos monitorozás, auditok, tesztek és gyakorlatok szükségesek

INCIDENSEK JELENTÉSE

Kötelező jelentéskészítés

- Megérteni a hatást
- Megtalálni a fókuszt
- Jelentési küszöb?
- Adathiány
  - Biztonsági prioritások?
  - Hatékonytalan és hatástalan

Jogi következmények

- „Lopakodó” támadások – Nehéz felfedezni
- Nyomok eltűntetése
- Nem kerülnek jelentésre a menedzsment és hatóságok felé
- Félelem a megtorlástól és/vagy jogi következményektől
- Ösztönző eszközökkel javítani a jelentési hajlandóságot

KÖSZÖNÖM A FIGYELMET!

Dr. Horváth Attila

ahorvath@bkf.hu