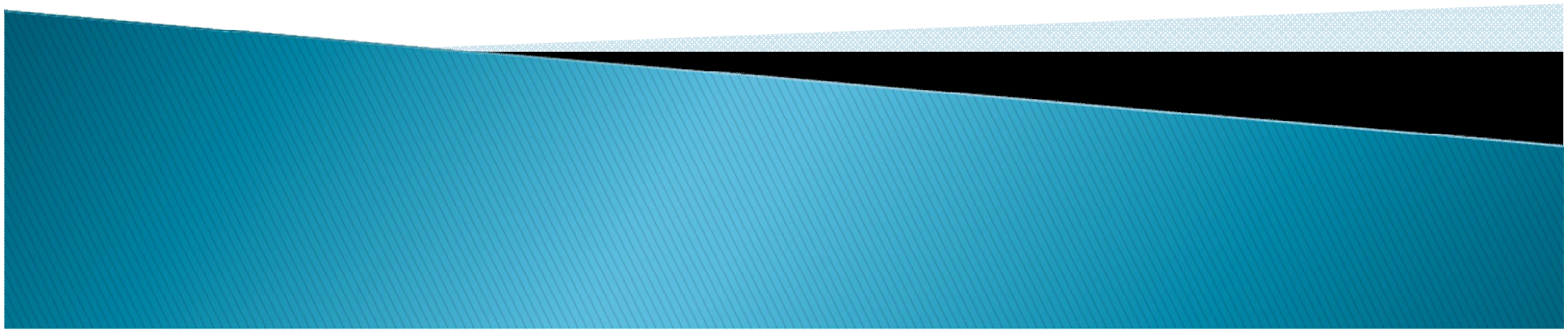
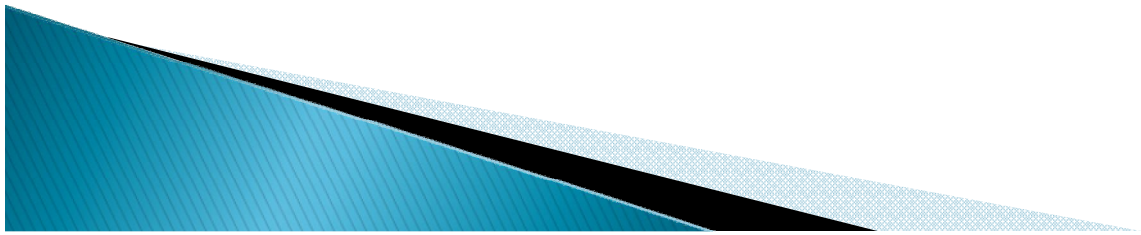
E-közigazgatási alkalmazásfejlesztések biztonsági tapasztalatai

Krasznay Csaba
ZMNE doktorandusz



Miért?

- Adódik a kérdés, hogy miért kell kiemelten foglalkozni egy funkcionálisan jól működő rendszer esetén a biztonsággal?
- Válasz: mert e-közigazgatási rendszerek esetén nemzeti kritikus információs infrastruktúrákról beszélünk
- Okok (prioritási sorrendben):
  - Belső visszaélések
  - Külső, nem szervezett támadások elkerülése (hackertámadások)
  - Külső, anyagi motivációból elkövetett támadások (szervezett alvilág)
  - Külső, ideológiai alapon nyugvó támadások (kiberterrorizmus)
  - Külső, országok közötti konfliktusok miatti támadások (kiberhadviselés)

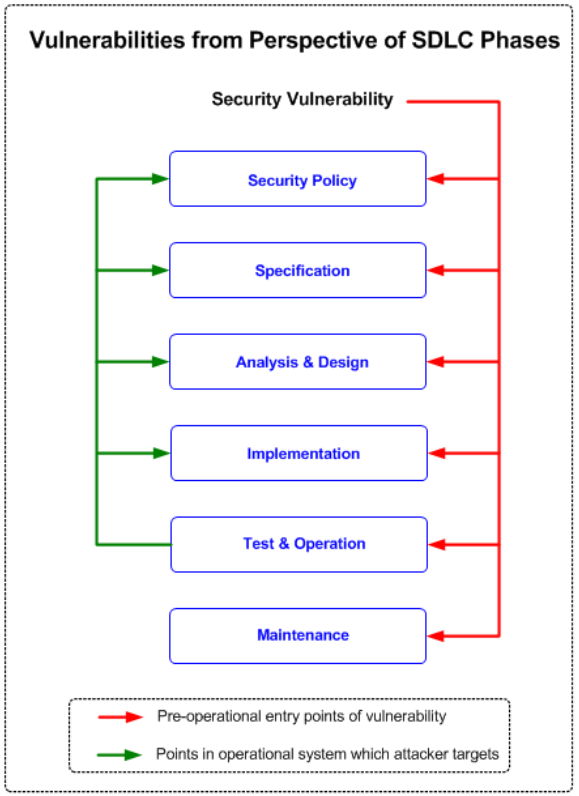


Általános helyzet

- Elmondható, hogy az államigazgatás felismerte a fejlesztés biztonságának fontosságát.
- A mozgásteret a szabályrendszer nagyjából kijelöli.
- Az ördög azonban a részletekben rejlik!
- Fejlődő területről van szó, nem csak hazánkban, hanem külföldön is!
- A következőkben a legégetőbb problémákról lesz szó.

Az ideális modellek

Microsoft SDL



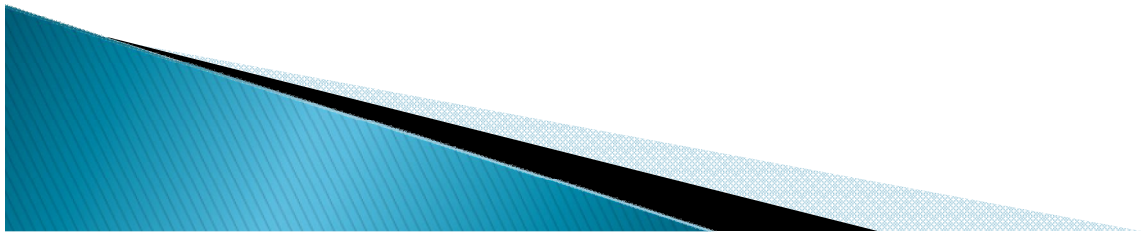
OWASP CLASP

NIST SP 800-64

Szerepkörök, felelősségek

A megrendelő

- Az EKOP-on belüli alkalmazásfejlesztésekben a biztonság kiemelt szerepet kapott
- A projektek elindulása után azonban sokszor felmerültek azok a hatásköri kérdések, melyekre a pályázat nem tért ki.
- Így elsősorban az, hogy kinek a feladata az alkalmazáshoz kapcsolódó kockázatelemzés elkészítése, a biztonsági besorolások elvégzése.
- Általánosságban elmondható, hogy nem pontosan tisztázott, hogy a kiírás/tervezés során milyen alapdokumentumokat kell átadnia a megrendelőnek, melyekből a fejlesztő már konkrét biztonsági rendszert tud tervezni.

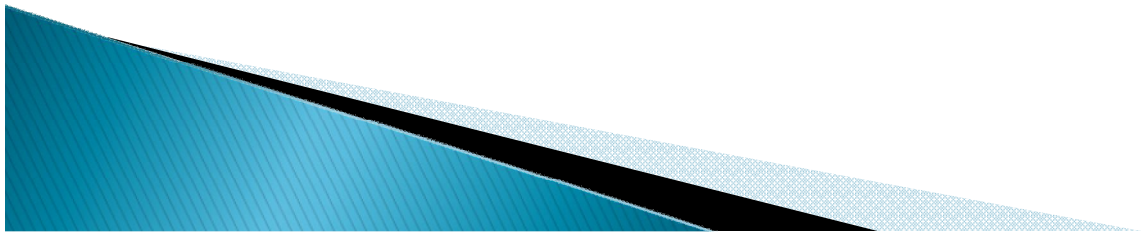


A szállító

- A biztonságos alkalmazásfejlesztés annyira új tudományterület, hogy nagyon kevés szakember foglalkozik a fejlesztőcégeknél ezzel a témával.
- A fejlesztő és a megrendelő/minőségbiztosító közötti láncban két biztonsággal foglalkozó szerepkört hasznos beilleszteni:
  - a security architektet, akinek a feladata az adott technológiai platformra magas szinten meghatározni a biztonsági követelményeket (technológiai tudás)
  - a belső biztonsági auditort, aki a szabályozási követelmények teljesülését és a megfelelő fejlesztési folyamatokat követeli meg (auditori tudás).

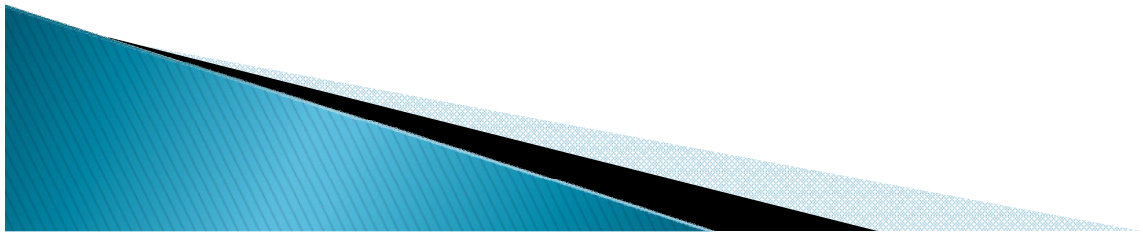
A minőségbiztosító

- A biztonsági minőségbiztosító hasznos segítséget jelent mind a megrendelő, mint a szállító oldal részére.
- Nem tisztázott azonban, hogy hatásköre meddig terjed ki, azaz mekkora belelátása lehet a fejlesztési folyamatokba.
- Érezhetően nincs egységesen elfogadott auditori gyakorlat, melynek kialakulása gördülékenyebbé tehetné az átadás/átvételi folyamatokat.



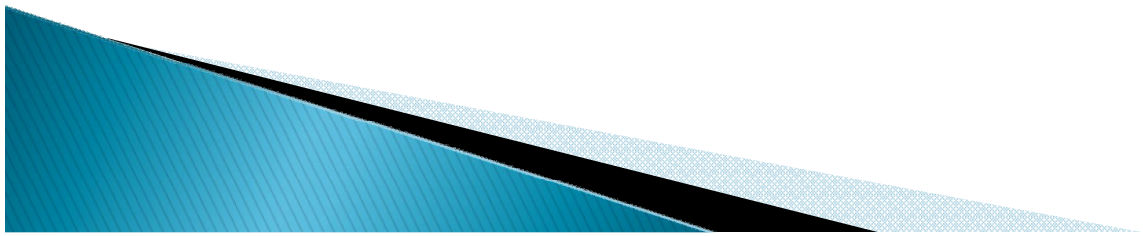
Funkcionális és garanciális követelmények

- A KIB 28. ajánlás az egyes biztonsági szintekhez pontosan meghatározza a funkcionális követelményeket.
- Ezek azonban eléggé magas szintűek ahhoz, hogy konkrét esetben (pl. mit naplózzon a rendszer) ne lehessen egyértelmű választ adni.
- A gyakorlatban az látható, hogy elsősorban az authentikációs, authorizációs és naplózási kérdésekre valamilyen egységes ajánlást kell kidolgozni
- Kicsit távolabbról nézve, a KIB 28. ajánláskötetet egy olyan élő halmazzá kell tenni, melyben folyamatosan jelenhetnek meg jógyakorlatok vagy műszaki ajánlások, melyek a jelenlegi rendszert kiegészítik.
- Ugyanez mondható el a fejlesztési folyamatokra is, pl. a sebezhetőségvizsgálat egységes módszertanának kidolgozása még várat magára.



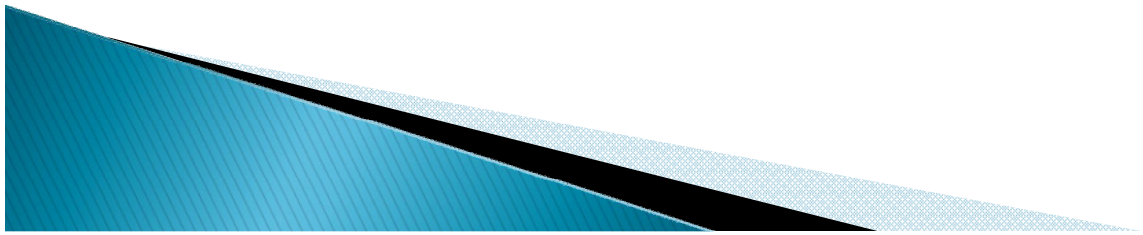
Az értékelési elvek

- Az EKOP projektek egy része előírta a CC EAL4 megfelelést.
- Ezen szabvány sikeres alkalmazásához azonban számos peremfeltétel hiányzik, így annak eldöntése
  - hogy az ISO szabvány, vagy a magyar értelmezésnek megfelelő MIBÉTS az irányadó,
  - pontosan milyen tartalmi és formai követelmények fogadhatók el,
  - milyen könnyítésekkel lehet esetlegesen élni, stb.
- Nagyon hiányzik a rendszerből egy olyan „vének tanácsa” jellegű testület, melyhez értelmezési kérdésekkel lehet foglalkozni.
- Ennek hiánya okozza azt a paradoxont, hogy ugyanabból a szabványból dolgozva a különböző minőségbiztosítók különböző következtetéseket vonnak le.



Összefoglalás

- Egy út elején járunk, ahol nagyon fontos a visszacsatolás, a további kutatás.
- A biztonságot már tervezési fázisban be kell „építeni” a rendszerbe, ezért nyilvánvaló problémákat a lehető leghamarabb meg kell oldani!
- Vegyük tudomásul: a rendszerfejlesztés teljes költségének 10-20%-a biztonsági jellegű kell, hogy legyen.



Köszönöm a figyelmet!

- E-mail: csaba@krasznay.hu
  Web: www.krasznay.hu