

# A magyar közigazgatás az informatikai biztonság szemszögéből

Póserné Oláh Valéria  
[poserne.valeria@nik.bmf.hu](mailto:poserne.valeria@nik.bmf.hu)

ROBOTHADVISELÉS 8  
TUDOMÁNYOS KONFERENCIA

# Miről lesz szó?

- Informatikai biztonsági intézkedések régen és ma
- A szabályozók szükségessége, hiányosságai
- A 195/2005. (IX. 22.) Korm. rendelet problémái

# Informatikai biztonsági intézkedések

Régen	Ma
Koncentráció fizikai védelemre Illetéktelenek kizárása a gépteremből <b>Egyetlen veszélyforrás a fizikai meghibásodásból, v. felhasználó figyelmetlenségéből adódó adatvesztés</b> Rendszeres mentés	Fizikai védelem, szabályzatok Illetéktelenek kizárása a gépteremből, hálózatból <b>Rengeteg veszélyforrás</b> (humán, host, hálózati, alkalmazás) (Automatizált)mentés, log elemzés Dinamikus weboldalak, -alkalmazások

# A SZABÁLYOZÓK

- Nemzetközi szinten: Az informatikai biztonság megteremtésével **nemzetközi szervezetek, nemzetközi szabványok** foglalkoznak.
- Nemzeti szinten: az **Alkotmány**, az **adatvédelmi törvény**, az egyes **országos szervek működéséről szóló törvények** adatkezelési előírásai, az **ITB ajánlásai** a mérvadók.
- Egy része kötelező érvényű (NATO és EU tagságunk), mások ajánlások.

# A SZABÁLYOZÓK hiányosságai

- Legfelső szinten többé-kevésbé megszülettek, nem teljes körűek.
- Léteznek a részletekre vonatkozó ajánlások, szabványok,
  - ▶ Az alsóbb szinteken az implementációk gyakran nem, vagy csak részlegesen jönnek létre.

# A SZABÁLYOZÓK hiányosságai

- Pl. a rendőrségnél léteznek szabályozások, mint:
  - ▶ adatvédelemmel kapcsolatos,
  - ▶ építészeti, műszaki,
  - ▶ iratkezelési,
  - ▶ elektronikus adathordozók kezelésére vonatkozó,
  - ▶ mentési szabályzatok,
  - ▶ katasztrófa tervek.
- Nincsenek egységes keretbe foglalva, aktualizálva.
- Okok: humánerőforrás problémák (személyi állomány csökken, a megfelelő képességekkel nem rendelkeznek, külső auditáló szakemberek bevonása a bizalmasság megsértését

# A SZABÁLYOZÓK szükségessége

- A közigazgatás területén a rögzített adatok több mint **90 %-a személyes adat v. személyes adathoz kötődik.**
- 2009-től az összes közfeladatot ellátó szervezetnek kötelező lesz a minősített elektronikus iratkezelő szoftvertermékek használata azok számára is, akik eddig nem is gondolkodtak elektronikus iratkezelésben.
- Az adatok védelme: **technika védelem** + meg kell óvni a szervezet tagjaitól is **különböző szabályok felállításával** és betartatásával.

# A 195/2005. (IX. 22.) Korm. rendelet

- 195/2005. (IX. 22.) Korm. rendelet: Az elektronikus ügyintézés lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról (különösen a biztonsági követelményekkel foglalkozó V. fejezet).

# A 195/2005. (IX. 22.) Korm. rendelet észrevételek

- 15. § (1): **a műszaki lehetőségeknek megfelelően** biztosítani kell, hogy az egyszer már azonosított ügyfél vagy hatóság helyébe jogosulatlan harmadik személy ne léphessen.
  - ▶ Mi a minimális műszaki lehetőség?
  - ▶ Könnyen lehet hivatkozni a feltételek hiányára.

# A 195/2005. (IX. 22.) Korm. rendelet észrevételek

- 16. § (1): az informatikai célrendszer működése szempontjából meghatározó folyamat valamennyi eseménye **naplózás**át írja elő.

▶ Naplók ellenőrzése, feldolgozása, elemzése?

# A 195/2005. (IX. 22.) Korm. rendelet észrevételek

- 20. § (1): **a célrendszer** vírusokkal és más rosszindulatú programokkal szembeni **arányos védelmét** követeli meg.
  - ▶ Kell, hogy minden munkaállomáson legyen megfelelően konfigurált és naprakész adatbázissal rendelkező vírusvédelem?

# A 195/2005. (IX. 22.) Korm. rendelet észrevételek

- 22. § (1): csak a külön jogszabályban meghatározott párbeszédre épülő elektronikus ügyintézésre kötelező az **elektronikus dokumentumok megfelelő rejtjelezési eljárás használata**. Egyéb esetekben **az ügyfél külön kérésére biztosíthatja** a hatóság azt.
- Az ügyfelek nagy része nem is tudja, hogy van ilyen lehetőség és mit is takar az.

# A SZEMLÉLETMÓD

- A döntéshozásban, a kivitelezésben és az üzemeltetésben résztvevők hozzáállása, szemléletmódja megfelelő legyen.

# A SZEMLÉLETMÓD

- Krasznay Csaba és Szigeti Szabolcs 2006 októberi tanulmánya (az Ügyfélkapu biztonságossága)
- Az Országgyűlés 2007.10.29-i ülésén a MeH EKK államtitkára:
  - ▶ „A hackerek számára is nyitott az ügyfélkapu, mint minden magyar állampolgár számára természetesen, szabályosan a hackerek is használhatják; ha megpróbálják hackelni, annak következményei vannak. **Nyilvánvalóan tettek már kísérletet, és ön sem tud beszámolni arról, hogy sikeres lett volna egyetlenegy kísérlet is. Azt tudom tehát kijelenteni felelősen, hogy az ügyfélkapu természetesen biztonságos**, biztosítja azt, hogy a magyar állampolgárok és a magyar vállalkozások nyugodtan, minden behatástól mentesen bevallhassák adataikat.”

# A SZEMLELETMÓD

- Az Ügyfélkapu a manapság egyre divatosabb támadási célpontok közé sorolható,
- Felmérések szerint drasztikusan növekednek a webalkalmazások elleni támadások (Gartner: a hacker támadások 75 %-a az alkalmazás rétegből kerül ki).
- Oka: a hagyományos támadások a hálózati rétegből, az operációs rendszer rétegből indultak, ezért itt építették ki a védelmet először, annyira megnehezítették a hekkerek dolgát, hogy inkább máshol (a kisebb ellenállás irányában) próbálkoznak, ami ma az alkalmazás réteg.

# A SZEMLÉLETMÓD

- Jelentős szerepet játszhat:
  - ▶ az oktatás,
  - ▶ a különböző továbbképzések,
  - ▶ a pedagógusok nevelő munkája, alap-, közép- és felsőfokon.

# ÖSSZEGLZÉS

- A felsőszintű **törvények**, előírások, ajánlások is mutatnak **hiányosságokat**
- A megfelelő **implementációk** az alsóbb szinteken **nem, vagy csak részben jönnek létre.**
- Reményeim szerint **javítani fog** a helyzeten a június 13-án ismertetett, december 31-ig lezáródó, az Államreform Operatív Program (ÁOP) **„Elektronikus közigazgatási keretrendszer kialakítása”** című e-közigazgatási keretrendszer projekt, melynek keretében elkészülő **szabványok, eljárásrendek és követelmények** iránymutatóul szolgálhatnak a magyar közigazgatás intézményei számára.

# ÖSSZEGZÉS

- A hatékony működéshez **elengedhetetlen az informatikai biztonság egységes értelmezése**, informatikai biztonsági **célok** és a megvalósításukhoz vezető **út**, a szükséges **feladatok** meghatározása, és **végrehajtásuk figyelemmel kísérése**, az esetleges változások figyelembe vétele érdekében legalább évente egyszeri felülvizsgálata.
- Ennek következetes kivitelezéséhez elengedhetetlenül szükség van **egyértelmű, pontosan megfogalmazott törvényi szabályozásra**, mert mivel az ajánlások nem kötelező érvényűek, számonkérésük sem lehetséges.

# ÖSSZEGZÉS

- A megfelelő informatikai biztonsági kultúra kialakítása nélkül alkalmazhatjuk a legkorszerűbb védelmi technológiákat, csupán szélmalom harcot vívunk.
- A megfelelő szemléletmód kialakulása hosszabb folyamat, törvényi szabályzásokkal, előírásokkal nem megvalósítható.

Köszönöm a figyelmet!