MINISZTERELNÖKI HIVATAL

Informatikai biztonsági elvárások

dr. Dedinszky Ferenc
kormány-főtanácsadó
informatikai biztonsági felügyelő

2008. július 2.

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Tartalom

Átfogó helyzetkép

Jogszabályi alapok és előírások

Ajánlások, a MIBA tartalma

Az Informatikai biztonsági felügyelő feladat- és hatásköre

Az önkormányzatok IT biztonságáról

Elvárások és lehetséges megoldások

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Átfogó helyzetkép

Informatikai biztonság vs. információbiztonság

- **Információbiztonság** – a „hagyományos” esetben régóta szabályozott, bevált eljárásrendek, módszerek léteznek
- **Informatikai biztonság** – az utóbbi időkig kötelező érvényű szabályzás nélkül „szájhagyomány útján” terjedt
  - A ’80-as években készült a KSH kiadványa (nagygépes környezetre)
  - A 90-es években az ITB ajánlásokat adott ki

A helyi informatikai vezetőkön múlt, hogy

- készítenek-e és milyen informatikai biztonsági szabályzatokat
- figyelembe veszik-e, és milyen mértékben a biztonsági követelményeket
- az informatikai biztonság általában kimerült a mentések megoldásában, és – az utóbbi években – a vírusvédelemben

A leggyakoribb kifogás:

„a biztonsági fejlesztésekre már nem jutott elegendő forrás”

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Jogszabályi alapok

A magyar közigazgatásra érvényes
alapvető informatikai biztonsági jogszabályok:

- **195/2005. (IX. 22.) Korm. rendelet** *az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról*
- **84/2007. (IV. 25.) Korm. rendelet a** *Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről*

Figyelembe veendő jogszabályok:

- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Avtv.)
- 2001. évi XXXV. törvény az elektronikus aláírásról (Eat.)
- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (Ket.)
- 193/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól (Ekr.)
- 194/2005. (IX. 22.) Korm. rendelet a közigazgatási hatósági eljárásban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről
- 182/2007. (VII. 10.) Korm. rendelet a központi elektronikus szolgáltató rendszerről

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Jogszabályi előírások

- **A 195/2005. (IX. 22.) Korm. rendelet** általában a közigazgatási elektronikus szolgáltatásokra vonatkozóan
  - szabályozza az informatikai biztonság közigazgatási szintű irányításának rendjét, az informatikai biztonságért felelős miniszter feladat- és hatáskörét
  - rendelkezik az „alapdokumentumok”: informatikai biztonsági politika; informatikai biztonsági szabályzat; katasztrófa-terv elkészítéséről
  - rendelkezik – a miniszter számára – ajánlások kiadásáról

- **A 84/2007. (IV. 25.) Korm. rendelet** a Központi Rendszerhez csatlakozó szervezetek számára, és a KR-en szolgáltatásokhoz
  - meghatározza az egységes informatikai biztonsági követelményrendszert
  - az Informatikai Katasztrófa-elhárítási Terv alapelveit
  - a szolgáltatások igénybe vételének biztonsági feltételeit

2008. június 30-ig kell a dokumentumokat a rendelet előírásaival összhangba hozni (vagy elkészíteni)!!!

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Ajánlások

- **ITB 8. számú ajánlás: Informatikai biztonsági módszertani kézikönyv (1994.) –** 1991-es angol és német dokumentumok alapján
- **ITB 12. számú ajánlás: Informatikai rendszerek biztonsági követelményei (1996.) –** 1992-es dokumentumok alapján
- **ITB 16. számú ajánlás: Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana (1997.)** – 1996-os dokumentumok alapján

IHM: MIBÉTS – nem jutott el az elfogadásig

Átdolgozásuk, korszerűsítésük elkészült:

Magyar Informatikai Biztonsági Ajánlások (MIBA)
A Közigazgatási Informatikai Bizottság elfogadta
(szerkesztés alatt, megjelenés előtt áll)

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

A MIBA tartalma

Az ajánláscsomag nyitó kötete az infokommunikációs biztonság szükségességéről, helyéről és szerepéről, és az önálló kötetek tartalmáról rövid összefoglaló

Önálló kötetekben:

- a **szervezeti szintű informatikai biztonságról (IBIR – Informatikai Biztonság Irányítási Rendszere) – informatikai vezetőknek, informatikai biztonsági felelősöknek**
- **az informatikai biztonsági dokumentumok tartalmi követelményei (IBIK – Informatikai Biztonság Irányítási Követelményei)**
- **az informatikai biztonság szervezeti szintű vizsgálatának (ellenőrzésének) formái és eljárásai (IBIV - Informatikai Biztonság Irányításának Vizsgálata)**

- **a technológiai szintű informatikai biztonságról a** MIBÉTS (Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma)
  - Külön kötetekben: megbízóknak, vezetőknek, fejlesztőknek, értékelőknek

- **a kis szervezetek, különösen az önkormányzatok informatikai biztonsági felkészülésének támogatására külön kötet!**

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Informatikai biztonsági felügyelő

• A 195/2005. (IX. 22.) Korm. rendelet 5. § (1) bekezdése szerint ***a közigazgatási szervek informatikai biztonságának felügyeletét a közigazgatási informatikáért felelős miniszter látja el az általa kinevezett informatikai biztonsági felügyelő útján***

• A Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről szóló 84/2007. (IV. 25.) Korm. rendelet 4. § (1) bekezdése szerint ***a közigazgatási informatikáért felelős miniszter a közvetlen irányítása alá tartozó informatikai biztonsági felügyelőt nevez ki, vagy bíz meg***.

ELEKTRONIKUSKORMÁNYZAT-KÖZPONT

Az IBF feladatai, hatás- és jogköre

A 195/2005. (IX. 22.) Korm. rendelet szerint:

1. **Jóváhagyja a biztonsági irányelvet, szabályzatot és eljárásrendet (biztonsági kockázat, illetve a jóváhagyás megtagadása esetén *kezdeményezheti a szolgáltatás felfüggesztését!!!*)**
2. **Ajánlásokat ad ki**
3. **Ellenőrzi az eljárási és biztonsági követelményeknek való megfelelőséget, a biztonságirányítási rendszer működtetésének megvalósítását**
4. **Véleményezi az eljárási cselekmények biztonsági osztályba sorolását**
5. **Állást foglal a Központi Rendszerhez csatlakozni kívánó szervezetek és szolgáltatások biztonságáról**
6. **Jelentések fogadása:**
   - ***Az üzemeltető szervezet* félévente tájékoztatást nyújt** az informatikai biztonsági eljárásrendek működéséről**;**
   - **I. és II. kategóriájú biztonsági esemény esetén haladéktalanul jelentést tesz az informatikai biztonsági felügyelőnek**
7. **Beavatkozás:** Az eljárási és biztonsági követelmények nem teljesülése esetén felhívja a hatóságot, hogy a jogszabályban foglaltaknak megfelelő működést állítsa helyre

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Az informatikai biztonság irányítási rendszere

• **A *hatóság*** köteles az informatikai célrendszer **informatikai biztonsági követelményeiért általánosan felelős személyt** és az informatikai célrendszer **üzemeltetéséért önállóan felelős személyt kinevezni**

• **Az *üzemeltető szervezet*** az üzemeltetést megvalósító szervezeti egységétől **független**, az üzemeltető szervezet vezetőjének közvetlen irányítása alá tartozó **informatikai biztonsági felelőst** jelöl ki, aki személyesen felel a biztonsági követelmények megvalósulásáért, és **e feladatának ellátása körében nem utasítható**

• **A *szolgáltató szervezet*** a szolgáltatást működtető szervezeti egységétől **független**, a szolgáltató szervezet vezetőjének közvetlen irányítása alá tartozó **informatikai biztonsági felelőst** jelöl ki, aki személyesen felel a biztonsági követelmények megvalósulásáért, és **e feladatának ellátása körében nem utasítható**

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Önkormányzati IT biztonság

- **Menedzsment biztonsági intézkedések**
  - kockázatfelmérés
  - tervezés, beszerzés
  - audit
- **Üzemeltetési biztonsági intézkedések**
  - fizikai és környezeti védelem
  - személyzettel kapcsolatos biztonság (kiválasztás, képzés)
  - konfiguráció kezelés, adathordozó védelem, karbantartás
  - üzletmenet-folytonosság
- **Műszaki biztonsági intézkedések**
  - azonosítás, hitelesítés, hozzáférés-ellenőrzés
  - naplózás, elszámoltathatóság
  - rendszer- és információ-sértetlenség
  - rendszer- és kommunikáció védelem
  - reagálás a biztonsági eseményekre

ELEKTRONIKUSKORMÁNYZAT-
KÖZPONT

Elvárások és lehetséges megoldások

Ellenőrzés:

- Jogszabályokban előírt dokumentumok, eljárásrendek megléte (IBSZ, katasztrófaterv stb.)
  - Ajánlásokban előírt követelmények szerinti tartalom
  - Eljárásrendek működőképessége
  - Jogszabályban előírt felelősök kinevezése

Megoldási lehetőségek:

- önálló kidolgozás és/vagy belső felelős személy kinevezése
- megbízás a kidolgozásra és belső vagy külső informatikai biztonsági felelős személy (szervezet) megbízása

Az elektronikus szolgáltató szervezet felelőssége nem átháríthatóó!!!

MINISZTERELNÖKI HIVATAL

Köszönöm a figyelmet!

Dr. Dedinszky Ferenc
kormány-főtanácsadó
informatikai biztonsági felügyelő
Miniszterelnöki Hivatal

ELEKTRONIKUSKORMÁNYZAT-KÖZPONT