KÖZIGAZGATÁSI INFORMATIKAI BIZOTTSÁG

25. számú Ajánlása

Magyar Informatikai Biztonsági Ajánlások (MIBA)

1.0 verzió

2008. június

Közigazgatási Informatikai Bizottság
25. számú Ajánlása

Készült a
Miniszterelnöki Hivatal megbízásából

Készítették:

25/1 – Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK)
(*Muha Lajos PhD, CISM*)

25/1-1 – Informatikai Biztonság Irányítási Rendszer (IBIR)
Összeállította: *Muha Lajos PhD, CISM*
Közreműködött: *Berkes Zoltán, Déri Zoltán, Krasznay Csaba CISA, CISM, CISSP, Muha Lajos PhD, CISM*

25/1-2 – Informatikai Biztonság Irányítási Követelmények (IBIK)
Összeállította: *Muha Lajos PhD, CISM*
Közreműködött: *Déri Zoltán, Lobogós Katalin, Muha Lajos PhD, CISM, Sneé Péter, Váncsa Julianna PhD*

25/1-3 – Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)
Összeállította: *Muha Lajos PhD, CISM*
Közreműködött: *Balázs István CSc, Déri Zoltán, Lobogós Katalin, Muha Lajos PhD, CISM, Nyíry Géza CSc, CISM, Sneé Péter, Váncsa Julianna PhD*

25/2 – Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)
1-4. segédletet
Összeállította: *Balázs István*
Közreműködött: *Balázs István, Staub Klára, Szabó István*
5. segédletet
Összeállította: *Balázs István*
Közreműködött: *Balázs István, Farkas Gábor, Endrődi Zsolt, Juhász Judit*

25/3 – Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX)
Összeállította: *Szigeti Szabolcs CISA, CISM, CISSP*
Közreműködött: *Krasznay Csaba CISA, CISM, CISSP, Muha Lajos PhD, CISM, Rigó Ernő, Szigeti Szabolcs CISA, CISM, CISSP*

A bevezetőt írta, és az ajánlást kiadásra előkészítette:
dr. Dedinszky Ferenc

Az ajánlás a Közigazgatási Informatikai Bizottság (KIB)
Jogi és Műszaki Szabályozási Albizottsága észrevételei alapján véglegesített tartalommal
a KIB tagjainak 2008. május-júniusi elektronikus távszavazása alapján
került elfogadásra

A Közigazgatási informatikai Bizottság 25. számot viselő ajánlássorozata az Informatikai Tárcaközi Bizottság 1994-1996. között kiadott 8. (Az informatikai biztonság módszertani kézikönyve) 12. (Az informatikai rendszerek biztonsági követelményeiről) és 16. számú (A Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertanáról) című ajánlásait váltja fel – kiegészített, átdolgozott és a korábbinál bővebb tartalommal. A korábbi ajánlások az elmúlt több, mint 10 évben tartalmilag megállták a helyüket, és megállapításaik túlnyomórészt ma is érvényesnek tekinthetők. Ugyanakkor az elmúlt időszakban az informatika olyan fejlődésen ment keresztül, amelyek indokolják a biztonsággal összefüggő ajánlásoknak az időközben bekövetkezett változásokat figyelembe vevő új, egységes szerkezetű, és az informatikai biztonság minden lényeges területét átfogó kiadását.

Az ajánlások tartalmilag úgy lettek összeállítva, hogy a jelenleg hatályos jogszabályok (195/2005. (IX. 22.) és a 84/2007 (IV. 25.) Korm. rendeletek) által előírt rendelkezéseknek a közigazgatási szervezetek meg tudjanak felelni. Az ajánláscsomag tartalmazza mindazokat az információkat, amelyek jogszabályok által előírt dokumentumok összeállításához, az eljárásrendek kialakításához, valamint a biztonságos elektronikus szolgáltatások megvalósításához szükségesek. Az ajánlássorozatba foglaltak alapján valósul meg az elektronikus szolgáltatást működtető/üzemeltető szervezetek biztonsági értékelése/tanúsítása, valamint a szolgáltatások auditálása. Az ajánlássorozat kiadásának időpontjában előkészületben van az informatikai biztonságról szóló törvény-tervezet, amely rendelkezik arról, hogy a közigazgatási szervek csak auditált elektronikus szolgáltatást működtethetnek. A törvény megfelelő felkészülési időt ad az auditálás végrehajtására, de javasolt, hogy a most fejlesztés alatt álló e-szolgáltatások már az ajánlás figyelembe vételével készüljenek el, illetve javasolt a már működő szolgáltatásoknak az ajánlás szerinti átvizsgálása, és szükség esetén a hiányosságok felszámolása.

Az elektronikus szolgáltatásoknak az ajánlássorozat szerinti biztonsági követelményeknek és előírásoknak a megfeleltetése azért különösen fontos, mert – örvendetesen – egyre jobban nő a közigazgatási szervek által indított szolgáltatások száma, amelyek egyre több közigazgatási ügy elektronikus úton történő elintézését teszik lehetővé. E szolgáltatások jelentős része – a szükséges azonosítás következtében, illetve a továbbított adatok tartalma miatt – tartalmaz vagy a személyiségi jogok, vagy az üzleti titok körébe sorolható olyan adatokat, amelyek védelme különös fontosságú. Ha az esetlegesen elégtelen biztonsági megoldások miatt a szolgáltatások során tárolt, továbbított és feldolgozásra kerülő információk illetéktelenek számára hozzáférhetővé, módosíthatóvá vagy törölhetővé válnak, vagy egy váratlanul bekövetkező esemény következtében a tárolt adatok helyreállíthatatlanul megsérülnek, akkor az nemcsak jelentős erkölcsi és anyagi károkkel járna, hanem az elektronikus közigazgatási szolgáltatások egész rendszerébe vetett bizalom rendülne meg.

A biztonsági követelmények biztosítása, és ezek ellenőrzése többletköltséget jelent az elektronikus közigazgatási szolgáltatást nyújtók számára, azonban ezek a költségek nem összevethetők azokkal az erkölcsi és anyagi károkkal, amelyek e költségek elhagyása esetén jelentkeznének. Az elektronikus szolgáltatások iránti bizalom megszűnése esetén a feleslegessé váló közigazgatási informatikai fejlesztések miatt több tízmilliárdos kár keletkezne. Különösen fontos annak a tételnek a széleskörű belátása, hogy az információbiztonság területén minden egyes elkerült kár nyereségnek felel meg. Az ajánlás célja az egységes elveken nyugvó, a nemzetközi szabványokhoz és ajánlásokhoz igazodó hazai előírások biztosítása az informatikai biztonság megteremtéséhez és fenntartásához.

Magyar Informatikai Biztonsági Ajánlások (MIBA)

A Magyar Informatikai Biztonsági Ajánlások (**MIBA**) című ajánlássorozat fő célja, hogy biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő.

A nemzetközi szabványokhoz és ajánlásokhoz igazodva a MIBA **három fő rész**ből áll:

- A **Magyar Informatikai Biztonsági Keretrendszer (MIBIK)** szervezeti szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBIK a biztonságos informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szól.
- A **Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)** technológiai szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBÉTS célközönsége az informatikai rendszer kialakításáért, fejlesztéséért felelős vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését és tanúsítását végző szakemberek köre.
- Az **Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)** olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel.

A **MIBIK** az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR)**,** amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK), amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányítás Vizsgálata (IBIV), amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

A **MIBÉTS** az ISO/IEC 15408:2005 és ISO/IEC 18045:2005 nemzetközi szabványokon, illetve a nemzetközi legjobb gyakorlatokon és nemzeti sémákon alapul. Keretet biztosít arra, hogy az informatikai termékek és rendszerek tekintetében a biztonsági funkciók teljessége és hatásossága értékelésre kerüljön. Értékelési módszertana alkalmas az operációs rendszerek, hardverek (pl. hálózati eszközök, tűzfalak, behatolás észlelők, intelligens kártyák), szoftver-alkalmazások (pl. különböző programnyelveken megírt kritikus alkalmazások) speciális biztonsági szempontjainak értékelésére. Ezzel a MIBÉTS a megbízható harmadik felek által végzett biztonsági ellenőrzés és audit egységes szempontrendszerét alkotja meg.

Az **IBIX** elsődleges célja, hogy segítséget nyújtson az informatikai biztonság megfelelő szintjének kialakításához önkormányzati és más informatikai szempontból kis méretű környezetben. Javasolt az anyag azon szervezetek számára, ahol a szervezet méreténél fogva nem áll rendelkezésre külön emberi és egyéb erőforrás az informatikai rendszerek biztonságának kialakítására és üzemeltetésére, hanem ezt „házon belül” kell megoldani.

Az ajánlások alkalmazása

Az ajánlások alkalmazásánál a következő alapelvek segítenek:

- A nagyobb szervezetek az informatika-biztonsági irányításában, működtetésében a MIBIK ajánlásait fokozatosan vezessék be;
- A nagyobb szervezetek az informatikai termék és rendszer beszerzéseik során az azonos tulajdonságú termékek vagy rendszerek közül – a közbeszerzési törvény előírásainak figyelembe vétele mellett – részesítsék előnyben a nemzetközi (CC, Common Criteria) vagy hazai (MIBÉTS) séma szerint értékelt és tanúsított termékeket, rendszereket;
- A kisebb szervezetek informatikai fejlesztéseik során az IBIX ajánlás szerinti szervezeti követelményeket érvényesítsék, valamint végeztessék el az ott megfogalmazott technológiai beállításokat.

Egy szervezeten belül az informatikai biztonság megteremtéséhez és fenntartásához az ajánlásokhoz kapcsolódó részletes segédletek adnak konkrét segítséget, a következő módon:

Feladat	Szükséges lépések	A MIBA felhasználandó dokumentumai
Az informatikai rendszer(ek) biztonságának megteremtése és fenntartása	Az Informatikai Biztonság Irányítási Rendszer létrehozása és működtetése	MIBIK ajánlás: IBIR
Új informatikai alkalmazás bevezetése	Védelmi követelmények megfogalmazása, Informatikai Biztonsági Szabályzat (IBSZ) elkészítése, meglévő aktualizálása	MIBIK ajánlás: IBIK
Új informatikai alkalmazást megvalósító termék vagy rendszer kiválasztása	A védelmi követelmények alapján az alkalmazás biztonság-kritikusságának felmérése, szükség esetén a védelmi (biztonsági) követelményeknek megfelelő, értékelt és tanúsított termékek kiválasztása	MIBÉTS ajánlás: 1. számú segédlet: Modell és folyamatok
Biztonság-kritikus termék és rendszer technológiai szempontú értékeltetése és tanúsíttatása	Amennyiben nincs megfelelően értékelt termék, vagy a termék egy olyan komplex rendszerben kerül alkalmazásra, melynek egységes értékelése is szükséges, a termék vagy a rendszer technológiai szempontú értékeltetése és tanúsíttatása	MIBÉTS ajánlás: 2. számú segédlet: Útmutató megbízóknak
Biztonság-kritikus termék és rendszer technológiai szempontú értékelése és tanúsítása (szervezeten kívüli feladat)	A technológiai szempontú értékelésben és tanúsításban érintett külső résztvevők (fejlesztő, vizsgáló laboratórium, tanúsító szervezet) végrehajtják az értékelést és tanúsítást	MIBÉTS ajánlás: 3., 4. és 5. számú segédletek (Útmutató fejlesztőknek, Útmutató értékelőknek, Értékelési módszertan)
A beszerzett termékek és rendszerek biztonságos üzemeltetése	A biztonsági szabályozók és a termék által teljesített (értékelt) biztonsági funkciók feltételrendszerének összhangba hozása	MIBIK ajánlás: IBIK
A rendszerek és adatok minősítése, a hiányosságok megállapítása	Kockázatelemzés, belső ellenőrzések elvégzése, külső audit megrendelése és elfogadása	MIBIK ajánlás: IBIV