HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Muha Lajos
muha.lajos@zmne.hu

Fleiner Rita
fleiner.rita@nik.uni-obuda.hu

ADATBÁZISOK BIZTONSÁGÁNAK KEZELÉSE A KÖZIGAZGATÁSBAN

Absztrakt

A publikáció az adatbázis biztonság szabályozásával foglalkozik. A szerzők bemutatják az adatbázis-biztonság szabályozását a magyar közigazgatásban és az Egyesült Államok haderejében. A publikáció az említett szabályozók alapján javaslatot tesz a magyar szabályozás megvalósítására.

The publication studies the regulation of database security. Authors describes regulation of database security in the hungarian government and the US Armed Forces. The authors proposed a base of database security regulation in the hungarian government.

***Kulcsszavak**: adatbázis-biztonság, adatbázis-biztonság szabályozása, Adatbázis-biztonsági útmutató, közigazgatás, Egyesült Államok Védelmi Minisztériuma ~ database security, database security regulation, ,, Database Security Guide, government, Department of Defense*

BEVEZETÉS

Az elektronikus közszolgáltatásoknak, illetve a közigazgatási szerv informatikával támogatott folyamatainak szükséges és alapvető feltétele az adatok, nyilvántartások elektronikus tárolása, mely leggyakrabban adatbázisok segítségével valósul meg. Az áttekinthetően és hatékonyan működő központi adatbázisok megléte az elektronikus közigazgatás alapvető eleme. Az adatbázisok biztonságának megsértése (működésképtelenné tétele, meghamisítása, a tárolt adatok jogtalan megismerése) az adott informatikai rendszer és az általa nyújtott szolgáltatás biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázis-biztonság megvalósítása és ennek szabályozása, támogatása.

Technológiai szempontból biztonságosan kifejlesztett (például egy magas Common Criteria szerinti minősítést elnyert) adatbázis-kezelő rendszer biztonságos működésének számos technikai és eljárásbeli feltétele van. Az adatbázis környezet telepítésekor, konfigurációjakor és működtetésekor számtalan szükséges beállítást és eljárást kell figyelembe venni, követni ahhoz, hogy az adatbázis-kezelő rendszer védve legyen már ismert támadási módszerektől. A biztonságos beállítások mellett olyan eljárásokkal is szükségszerű körültekintően eljárni, mint például a mentési, helyreállítási, audit és jogosultság beállítás folyamatok. Továbbá az adatbázis-kezelő rendszer az informatikai rendszer egyéb összetevőivel (operációs rendszer, hálózat, adatbázist elérő alkalmazások) is szoros kapcsolatban áll, ezek biztonsága nem kezelhető elkülönítve, mivel az informatikai rendszer egy komponensének nem biztonságos működése kihathat a vele együttműködő összetevőre.

A hazai közigazgatási informatika védelmére készült 223/2009. (X. 14.) Korm. rendelet, valamint a KIB 25. és 28. számú ajánlásai az informatikai védelem átfogó, komplex szabályozását nyújtják, de még emellett is szükséges az informatika egyes részterületeinek védelmét részterületi védelmi rendszabályokkal, útmutatókkal, ajánlásokkal elősegíteni, különös tekintettel a működés kritikus területeken. A közigazgatási informatika védelemben fontos részterület az elektronikus adatok tárolását és kezelését megvalósító adatbázis-kezelő rendszerek, illetve az azokban tárolt információk védelme, melynek jövőbeni szabályozásának kérdéseit, lehetőségeit vizsgálják a szerzők jelen cikkükben.

Az Egyesült Államok Védelmi Minisztériuma (Department of Defense, DoD) az informatika különböző részterületeinek védelméhez részletes szabályozó dokumentumokat dolgozott ki. Jelen publikációban feltárjuk a hazai informatika biztonság jelenlegi szabályozási rendszerét, megvizsgáljuk a DoD által kidolgozott szabályozókat, különös tekintettel az Adatbázis-biztonság Technikai Megvalósítási Útmutatóra, majd elemezzük a hazai adaptáció lehetőségeit, korlátait, illetve javaslatot fogalmazunk meg a magyar adatbázis-biztonsági szabályozás rendszerére.

A KÖZIGAZGATÁSI INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSA ADATBÁZISOK SZEMSZÖGÉBŐL

Az elektronikus közigazgatás biztonságát elsősorban a 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról [1] határozza meg, támogatva a Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásával. A kormányrendelet hatálya kiterjed az elektronikus közszolgáltatásokra, azok működtetőire, üzemeltetőire, az elektronikus közszolgáltatások nyújtásában részt vevő szervezetekre és személyekre, valamint az elektronikus közszolgáltatások igénybe vevőire.

A 223/2009. kormányrendelet a közszolgáltatást végző informatikai rendszerek személyi, szervezeti és műszaki követelményeit tartalmazza. A kormányrendelet főbb előírások a következők:

- Az elektronikus közszolgáltatásoknak meg kell valósítaniuk a bizalmasság, sértetlenség, törvényes adatkezelés és kockázatarányos védelem elveit.

- Az elektronikus közigazgatási rendszerek biztonsági felügyeletét a kormány informatikai biztonsági felügyelője látja el.

- A magyar kritikus információs infrastruktúra védelméért a Nemzeti Hálózatbiztonsági Központ a felelős.

- Az érintett szervezeteknek információbiztonsági irányítási rendszert kell létrehozniuk. Ezen belül meg kell valósítani a minőségbiztosítást és szabályzati rendszert kell létrehozni.

- A kritikus rendszereket naplózni, menteni és archiválni kell.

- Meg kell oldani az ügyféltámogatást.

- Speciális esetekben az üzemeltetés kiszervezhető, de ilyenkor is be kell tartani a biztonsági előírásokat.

- Vírusvédelmet kell megvalósítani.

- Adattovábbítás során kriptográfiai megoldásokat kell használni az üzenetek titkosítására.

- A hozzáférés-védelmet mind logikai, mind fizikai szinten gondosan meg kell tervezni és valósítani.

- Az üzemeltetés biztonságai elveinek kialakítása során a legjobb gyakorlatokra kell alapozni.

- Az elektronikus közszolgáltatásokat biztonsági auditnak kell alávetni az erre felhatalmazott szervezet által.

Ezek mellett még a központi rendszer biztonsági szabályozása is megtalálható a jogszabályban.

A Közigazgatási Informatikai Bizottság (a továbbiakban: KIB) 2008-ban adta ki a 25. számú, majd rövidesen a 28. számú ajánlását. A KIB 25. számú ajánlása a Magyar Informatikai Biztonsági Ajánlások (MIBA) címet viseli. Ez tulajdonképpen egy ajánlássorozat, amelynek fő célja, hogy nemzetközi szabványokhoz és ajánlásokhoz igazodva biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő. A MIBA három fő részből áll:

- A **Magyar Informatikai Biztonsági Keretrendszer (MIBIK)** [2] 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 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) [3]**,** amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK) [4], 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) [5], amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

• A **Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)** [6] 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. 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), szoftveralkalmazások (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 **Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)** [7] olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel. 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.

A KIB 28. számú ajánlása [8] egy Követelménytár, amely az elektronikus közigazgatás fejlesztéséhez és üzemeltetéséhez szükséges szabványokat, követelményeket és előírásokat tartalmazza. Az *IT biztonsági követelmények*, és a *Termékek, szolgáltatások értékelésének, auditjának előkészítése* a 25. számú ajánlásra épülve, azt kiegészítő vagy végrehajtását támogató előírásokat tartalmaz, illetve a Egyéb követelmények, ajánlások számos biztonsági szabványt mutat be.

Az *IT biztonsági követelmények* részei:

- Biztonsági tervezési útmutató;
- IT biztonsági követelményrendszer - biztonsági szintek követelményei;
- IT biztonsági Követelményrendszer érvényesítésének módja;
- IT Biztonsági Politika követelményei;
- IT biztonsági stratégia követelményei;
- IT Biztonsági szabályzatok követelményei;
- IT biztonsági szintek és biztonsági kategorizálási minta;
- Közigazgatási Operatív Programok IT biztonsági környezete, követelményrendszere;
- Szabályzatmenedzsment rendszer követelményei;
- Útmutató az IT biztonsági szintek meghatározásához.

Termékek, szolgáltatások értékelésének, auditjának előkészítése rész tartalma:

- IT biztonsági értékelő labor koncepció;
- Létező tanúsítások megfeleltetése - Technikai leírás;
- Összetett termékekre vonatkozó értékelési módszertan;

- Rendszerekre vonatkozó értékelési módszertan;
- Termékekre vonatkozó értékelési módszertan;
- Útmutató akkreditorok számára;
- Útmutató rendszer-értékelők számára;
- Útmutató rendszer-integrátorok számára;
- Útmutató tanúsítók számára.

A KIB 25. számú ajánlása IBIR kötete meghatározza, hogy, hogy a közigazgatási informatikai rendszerek biztonsági szabályozása milyen elemekből álljon.

- **Informatikai Biztonsági Politika (IBP)**: „Az Informatikai Biztonsági Politika kinyilvánítja a menedzsment biztonság iránti elkötelezettségét, a biztonsági célt, valamint magas szintű biztonsági elvárásokat fogalmaz meg, amelyek a biztonsági cél elérését szolgálják, és amelyeket érvényesíteni kell a védelmi intézkedések specifikálása során."

- **Informatikai Stratégia**: „Az Informatikai Biztonsági Stratégia célja, hogy a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét (középtávú, hosszú távú)."

- **Informatikai Biztonsági Szabályzat (IBSZ)**: „Az Informatikai Biztonsági Szabályzat rögzíti az IBIR működéséhez, működtetéséhez szükséges folyamatokat, megadja az érintett szereplők (pl.: információbiztonsági vezető, üzemeltető, rendszergazda, fejlesztési vezető, adatgazda stb.) feladatait, felelősségeit, hatásköreit. Rögzíti az információfeldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológiafüggetlen tudjon maradni."

- **Informatikai Felhasználói Szabályzat (IFSZ)**: „A dokumentum részletesen szabályozza a felhasználók kötelességeit az informatikai eszközök használata során, meghatározza azokat a peremfeltételeket, melyek között a felhasználó kapcsolatot létesít az informatikai osztállyal, vagy az adatgazdákkal. A szabályzat részletesen kifejti a felhasználó által elvégezhető és tiltott tevékenységeket, megadja a számonkérés formáját és módját, rögzíti a biztonsági események jelentésével kapcsolatos kötelezettségeket."

- **Eljárásrend gyűjtemény**: „Az eljárásrend gyűjteménybe tartozó végrehajtási utasítások olyan alacsony szintű szabályzatok, amelyek részletesen, rendszer specifikusan rögzítik azokat a tevékenységeket, melyeket az informatikai biztonsági szabályzat rendszer függetlenül megkövetel."

A KIB 25. és 28. számú ajánlása szerint (legalább) három, a bizalmassági követelményeket előtérbe helyező szinten kell az informatikai rendszerek védelmét megvalósítani: a kiemelt szint, amely a minősített adatokat feldolgozó rendszerek, a fokozott, amely a belső használatú, bizalmas információkat kezelő rendszerek, valamint az alap, amely a széles körben, interneten keresztüli hozzáférést biztosító rendszerek védelmi szintje.

Bár a közigazgatás informatikai rendszerei igen jelentős mértékben adatbázis rendszerek, ennek ellenére az adatbázisok biztonságára vonatkozó specifikus előírást a hazai jogszabályok és ajánlások nem tartalmaznak.

AZ AMERIKAI MODELL

A következőkben bemutatjuk az Amerikai Egyesült Államok Védelmi Minisztériuma (a továbbiakban: DoD) által kidolgozott és alkalmazott adatbázis-biztonsági szabályozás rendszerét, majd ennek alapján következtetéseket vonunk le a lehetséges hazai adaptációra.

A DoD az USA hadereje adatbázisainak védelme érdekében adatbázis-biztonság megvalósítását szabályozó dokumentumokat dolgozott ki. A dokumentumok nyilvánosak és bármely szervezet számára hasznosíthatóak, így a civil szféra is szabadon felhasználhatja.

Fontosnak tartjuk kiemelni, hogy az említett DoD adatbázis-biztonsággal foglalkozó szabályozása egy nagyobb egységnek, az Egyesült Államok haderején belüli teljes informatikai rendszerre vonatkozó, az informatikai védelem megvalósításával és ellenőrzésével foglalkozó **Informatikai Védelmi Direktívának** [9, 10] és az erre épülő **Informatikai Védelmi Megvalósítási Utasításnak** [11] a része, melyek. Az említett dokumentumok meghatározzák az informatikai biztonság alapvető szintjét, a megvalósítandó ellenőrzési célok együttese formájában. Az előírt ellenőrzési célok a rendszerek működésbiztonsági kategóriáitól és bizalmassági szintjeitől függően kerülnek meghatározásra.

A **működésbiztonsági kategória** az informatikai rendszerek által kezelt információknak a DoD célkitűzéseinek, különösen a harci küldetéseknek megvalósításában betöltött jelentőségét tükrözi. A szabályozóban három kategória van meghatározva [10, 19. o.] Az **információk bizalmassági szintje** az informatikai rendszerek elfogadható hozzáférési követelményeinek (személyi biztonsági ellenőrzések és háttérvizsgálatok, hozzáférési engedélyek, tudnia-kell szabályozások, összekapcsolási ellenőrzések és engedélyek) és felhasználói hozzáférési módszereinek (intranet, Internet, vezeték nélküli kapcsolat) meghatározására szolgál. A védelmi minisztérium három bizalmassági szintet használ: minősített, bizalmas és nyílt. [11, 16. o.]

A különböző rendszer-összetevőkre vonatkozó részletes informatikai biztonsági ellenőrzési célokat, az alkalmazandó védelmi rendszabályokat, eljárásokat biztonsági beállítási (konfigurációs), vagy megvalósítási útmutatók rögzítik. Az Egyesült Államok hadereje esetében ezeket a Védelmi Informatikai Rendszerek Ügynöksége (Defenese Information Systems Agency, DISA), valamint a Nemzetbiztonsági Ügynökség (National Security Agency, NSA) készíti el és bocsátja ki.[14]

A DISA által kidolgozott **Biztonsági Technikai Megvalósítási Útmutató** (Security Technical Implementation Guide, STIG) segédeszköz a DoD informatikai rendszerek védelme minőségének növeléséhez. Az egyes útmutatók az adott informatikai rendszerösszetevő ismert biztonsági komponenseit, sérülékenységeit és a DoD informatikai védelmi politika által tárgyalt, ezekhez kapcsolódó kérdéseket tartalmazzák.

A DISA útmutatókhoz, az azokban foglaltak ellenőrzéséhez általában rendelkezésre állnak biztonsági ellenőrző listák és a biztonsági készenlétet ellenőrző szkriptek. Mindkettő lényegében azt ellenőrzi, hogy a vizsgált rendszer (rendszer-összetevő) megfelel-e az útmutatóban előírt követelményeknek (ellenőrzési céloknak), vagyis megfelelően van-e telepítve és konfigurálva, illetve megfelelően van-e felügyelve, kezelve.

Az informatikai rendszer biztonságos működésének ellenőrzését nyolc csoportba sorolják be, melyek a következők [11, 48-49. o.]:

1. Biztonság tervezése és konfigurálása
2. Azonosítás és hitelesítés
3. Alrendszer és eszközrendszer
4. Alrendszer határvédelem
5. Fizikai és környezeti biztonság
6. Személyi biztonság
7. Működésfolytonosság
8. Sebezhetőség és incidenskezelés

Az adatbázis rendszerekre – mint az informatikai rendszer egyik összetevőjére – is rendszer specifikus módon kidolgoztak biztonsági útmutatókat és biztonsági ellenőrzési listákat. Ezen dokumentumokban szereplő irányelvek betartása olyan biztonsági környezetet eredményez, mely teljesíti vagy felülmúlja a 2. működésbiztonsági kategóriába (MAC II.) sorolt, bizalmas adatokat kezelő információs rendszerek biztonsági szintjét.

Az **Adatbázis-biztonság Technikai Megvalósítási Útmutatója** [12] az adatbázis-kezelő rendszerek biztonságára vonatkozóan nyújt általános útmutatást gyártó független módon, illetve a DoD informatikai rendszerének részét képező adatbázis rendszerekre fogalmaz meg kötelezően betartandó biztonsági követelményeket. A biztonsági követelményeket csoportokba szedve tárgyalja a dokumentum, amiket egy általános leírással vezet be, majd az adott követelmény csoporthoz összegyűjti az oda tartozó ellenőrzési pontokat, de csak azokat, melyek általánosan érvényesek minden adatbázis-kezelő termékre. A következő példával szemléltetjük a leírtakat:

- **Biztonsági követelmény csoport neve**: Rendszer könyvtárak kezelésének ellenőrzése
- **Biztonsági követelmény csoport általános leírása**: Az adatbázis-kezelő rendszer és a vele kapcsolatos alkalmazások fájljai, könyvtárai megfelelő védelem hiányában sérülékenyek lehetnek jogosulatlan módosításokkal szemben. A jogosulatlan módosítás negatív hatással bírhat az adatbázis-kezelő rendszer és az alkalmazások adatainak integritására és elérhetőségére.
- **Biztonsági követelmény csoporthoz tartozó termék független ellenőrzési pont:** Az adatbázis-kezelő szoftver egy felhatalmazott alkalmazás tulajdonos tulajdonában van.

Az adatbázis rendszerekre vonatkozó általános biztonsági követelményeket az általános informatikai rendszerekre vonatkozó csoportosítás alapján gyűjti össze és tárgyalja. A fentiekben ismertetett nyolc pont szerint, abból az adatbázis rendszerekre önmagában nem releváns 5. és 6. pontokat kihagyva a következő csoportosítás szerint épül fel:

1. Biztonság tervezése és konfigurálása,
2. Azonosítás és hitelesítés,
3. Alrendszer és eszközrendszer,
4. Alrendszer határvédelme,
5. Működésfolytonosság,
6. Sebezhetőség és incidenskezelés.

Az általános követelményeket megfogalmazó Útmutató ellenőrzési pontjainál megtaláljuk azt a szerepkört, aki az adott ellenőrzési pont betartásáért felel. Az Útmutató a következő négy szerepkört használja: informatikai biztonsági menedzser, informatikai biztonsági munkatárs, adatbázis adminisztrátor, adatbázis szerver operációs rendszer adminisztrátor. Minden ellenőrzési ponthoz tartozik sérülékenységi kategória, mely a sérülékenység súlyosságának fokát jelzi az adott követelmény be nem teljesülése esetén. A következő kategóriákat határozták meg:

- 1. kategória: olyan sérülékenységet jelent, ami a támadónak közvetlen hozzáférést ad az adatbázis rendszerhez, ott superuser hozzáférést eredményez.
- 2. kategória: olyan sérülékenységet jelent, ami olyan információt nyújt a támadó számára, ami nagy valószínűséggel az adatbázis rendszerhez történő hozzáférés megszerzéséhez vezethet.
- 3. kategória: olyan sérülékenységet jelent, ami olyan információt nyújt a támadó számára, ami az adatbázis rendszer megsértésének lehetőségét hordozza magában.

Az Útmutatóhoz tartozó **Adatbázis-biztonsági Ellenőrző Lista** [13] gyártó specifikusan nyújt a biztonsági követelmények teljesítéséhez segítséget. Az Útmutató általános követelményeihez adatbázis-kezelő rendszerfüggő követelményeket fogalmaz meg - szintén **ellenőrzési pontoknak** nevezve el -, melyek gyakorlatilag egy konkrét biztonsági követelményt, annak részletes megvalósítási eljárását és ellenőrzési módját írják le. Az Oracle, MS SQL, DB2 adatbázis-kezelő rendszerekhez speciálisan elkészített ellenőrző listák jöttek létre, illetve a többi típust egy platform független módon megfogalmazott ellenőrző lista támogatja. Az adatbázis rendszerek automatikusan megvalósítható biztonsági auditját szkriptek segítségével is támogatják, ezek viszont kizárólag a DoD szervei számára elérhetőek.

JAVASLAT A MAGYAR SZABÁLYOZÁS KIEGÉSZÍTÉSÉRE

A következőkben az adatbázis-biztonság szabályozásának lehetőségeit tekintjük át a magyar közigazgatáson belül. Abból indulunk ki, hogy egyrészt a hazai informatikai biztonság szabályozásában már sok fontos lépés történt, ezt a cikk első felében már felvázoltuk Másrészt a jelenleginél szigorúbb és részletesebb hazai központi szabályozás szükséges az informatika egyes részterületeinek védelme tekintetében (különös tekintettel a működés kritikus területeken), ezen belül a publikációban az adatbázis rendszerek védelmére koncentrálunk. A magyar szabályozásban e tekintetben jelenleg egy hiányzó láncszemet érzékelünk. Célunk a nemzetközi szabványokhoz és a hazai KIB 25. számú ajánláshoz igazodó adatbázis-biztonság megteremtéséhez és fenntartásához szükséges lépések megfogalmazása.

Az Egyesült Államok Védelmi Minisztériuma által kidolgozott informatikai biztonsági és ennek részét képző adatbázis-biztonsági szabályozás egy nagyon precízen felépített rendszert alkot, aminek egyes részeit kívülálló szervezetek is felhasználják a saját informatikai védelmük tervezésére, megvalósítására. A hazai közigazgatáson belüli informatikai védelem szempontjából is például szolgálhat az amerikai modell oly módon, hogy fel kell tárni, mik a hazai adaptációra alkalmas részei, illetve mi az, ami a magyar viszonyok között nem alkalmazható. Az amerikai modell vizsgálata kapcsán annak két fontos tulajdonságát mindenképp célszerű szem előtt tartani:

(1) Az adatbázis-biztonsági szabályozás a teljes informatikai biztonsági szabályozás keretein belül helyezkedik el, annak struktúrájához és terminológiájához illeszkedik,

(2) Az adatbázis-biztonsági szabályozás két nagyobb egységből áll. Egyrészt egy általános adatbázis-biztonsági útmutatóból, másrészt a konkrét adatbázis-kezelő rendszerekhez kidolgozott ellenőrzési listákból.

A leendő magyar adatbázis-biztonsági szabályozásnak keretet kell, hogy jelentsen a már meglévő hazai informatikai biztonsági szabályozás, de ez nem lesz olyan szoros kapcsolat, mint az amerikai modell esetén. Gyakorlati szempontból ez azt is jelenti, hogy egy adatbázis-biztonsági útmutató vagy adatbázis-biztonsági ellenőrző lista szerkezetét tetszőlegesen fel lehet építeni, ennek nem kell egy már adott struktúrához igazodnia.

A magyar közigazgatásban jelenleg nincs és valószínűen még sokáig nem is lesz egy olyan központi szerv, mely fel tudná vállalni azt a feladatot, hogy a jelentősebb adatbázis-kezelő rendszerek esetében adatbázis-biztonsági ellenőrző listákat állít fel és tart karban. Ugyanakkor egy általános adatbázis-biztonsági útmutató kiadását célszerű lenne a magyar elektronikus kormányzat számára kiadni, majd az erre épülő, termékfüggő adatbázis ellenőrzési listák elkészítését az adatbázis üzemeltetők feladatául lehetne kijelölni.

Az általános adatbázis-biztonsági útmutató és az adatbázis ellenőrzési listák a KIB 25. számú ajánlása IBIR kötetében meghatározott informatikai biztonsági szabályozási szintek közül az Eljárásrend gyűjtemények körébe tökéletesen beilleszkedik. Azonban önmagában egy jó eljárásrend kiadása még kevés[1]. Használatát elő kell írni. Szintén elő kell írni, hogy a külső és belső informatikai biztonsági auditok során az alkalmazását vizsgálni kell.

Javaslatunk szerint a magyar szabályozásnak tartalmaznia kellene az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági követelményeket, gyártó független módon megfogalmazva. A szabályozás hatálya alá eső szervezetnek (azaz, aki megfelelően kritikus adatbázist üzemeltet) a biztonsági követelményeket át kell fogalmaznia konkrét biztonsági elemek, ellenőrzési pontok halmazává, ami a saját adatbázis-kezelő rendszerére és az aktuális működési környezetre érvényes. Ebből épülne fel a szervezet adatbázis biztonsági szabályzata.

Az adatbázis-biztonsági útmutatót kiadó központi szerv feladatába tartozna továbbá az alá tartozó szerveken történő felügyelet gyakorlása. A központi szerv feladat lenne annak ellenőrzése, hogy a kritikus adatbázisokat üzemeltető szervek létrehoztak-e ellenőrzési listát és elvégzik-e ennek alapján a biztonsági vizsgálatot. Elő kell írni központilag, hogy milyen gyakran kell a szervezetben a biztonsági szabályozás alapján az ellenőrzést lefolytatni, annak eredményét dokumentálni kell és külső audit során a biztonsági szabályzat meglétét és az annak való megfelelés dokumentumát be kell mutatni. A központi szerv javaslatokat, segítséget nyújthat abban, hogy a termékfüggő adatbázis ellenőrző listákat milyen forrásokra támaszkodva tudják az üzemeltető szervezetek elkészíteni.

Az **Adatbázis-biztonsági útmutató** tehát az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági követelményeket tartalmazza gyártó független módon megfogalmazva. Az amerikai modellel ellentétben - ahol az Útmutatót egy előre megadott felépítést követ – a magyar szabályozás felépítése követheti az adatbázis-kezelő rendszer és a tárolt adatok védelmének középpontba állítását. Az általános útmutató szerkezetének eltervezésekor érdemes figyelemmel lenni arra, hogy az üzemeltetők által elkészítendő ellenőrző lista alapjául is szolgálhasson a választott struktúra.

[1] Nagyon jó példája ennek a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának 12. számú ajánlása [15]. Igen széles körben kötelezően használtak, kivéve a közigazgatást, amely számára készült.

A következőkben megvizsgáljuk, hogy az adatbázis biztonsági követelményeket milyen szempontok szerint lehet csoportosítani, rendszerezni. A biztonsági követelményeket csoportosíthatjuk aszerint, hogy az a védendő objektum mely részelemének védelméért felelős. Az adatbázis rendszer védendő objektumának meghatározásakor elsőként kell említeni az adatbázisban tárolt adatok védelmét, illetve az adatbázis-kezelő rendszer védelmét. Ugyanakkor ezek közvetlen kapcsolatban állnak az informatikai rendszer más részelemeivel, melyek biztonsága szorosan kihat az adatbázis biztonságra is. Itt meg kell említeni az adatbázis-kezelő rendszer számítógépének operációs rendszerét, a hálózatot és az adatbázist elérő alkalmazásokat, de ezeknél az informatikai rendszer elemeknél csak az adatbázis biztonságra kiható biztonsági követelmények meghatározására szorítkozunk.

A védendő objektum-elemekhez kötődő követelményeket megkülönböztethetjük aszerint, hogy:

1. az adatbázis-kezelő rendszer biztonságos működéséhez köthető,
2. az adatbázisban tárolt objektumokkal kapcsolatos,
3. az adatbázis-kezelő rendszer gépének operációs rendszeréhez kötődik,
4. az adatbázis-kezelő rendszerrel érintkező hálózati kommunikációval függ össze vagy
5. az adatbázisokat elérő alkalmazásokkal kapcsolatos.

Javasoljuk, hogy két fő kategóriát állapítsunk meg:

(1) az adatbázis-kezelő rendszer védelmét és

(2) a tárolt adatok védelmét.

Az operációs rendszer, a hálózat és az alkalmazások védelmét az (1) pont alá, mint annak alkotóelemeit helyezzük be.

A biztonsági követelmények egy másik típusú rendszerezése az adatbázis rendszerek biztonságos működtetéséhez kapcsolódó különböző folyamatokra, eljárásokra épül. Az adatbázis-kezelő rendszerek működésével kapcsolatos folyamatokhoz sorolhatjuk a teljesség igénye nélkül a következőket:

1. adatbázis-kezelő rendszer telepítése és biztonsági frissítése,
2. adatbázismentés és helyreállítás,
3. adatbázis audit, log elemzés,
4. felhasználó azonosítás,
5. jogosultság kezelés,
6. incidenskezelés és
7. egyéb eljárások.

(Az utolsó egy olyan kategória, melybe az előző kategóriák egyikébe sem elhelyezhető elemek tartoznának például az éles és fejlesztői környezetek szétválasztásának kritériuma).

Az adatbázis rendszerek biztonsági követelményeinek rendszerezéséhez az előző két módszer ötvözésére épülő, hierarchikus felépítést javasolunk. Három fő kategóriát különböztetünk

meg; kettőt a védendő objektum részelemei alapján, illetve harmadikként a működtetési folyamatokat, eljárásokat, azaz:

(1) az adatbázis-kezelő rendszer védelme,

(2) az adatbázisban tárolt adatok védelme,

(3) működtetési folyamatok, eljárások.

Ezekbe, mint alkategóriák helyezzük el az operációs rendszer, a hálózat és az alkalmazások védelmét, a különböző működtetéssel kapcsolatos részfolyamatokat, illetve az egyéb összetartozó követelmény csoportokat. A következő táblázatban foglaljuk össze az adatbázis biztonsági útmutató egy lehetséges felépítését:

Fejezet címe	Fejezet alcímei
Adatbázis-kezelő rendszer biztonsága	• Adatbázis-kezelő rendszer konfigurációs követelményei • Operációs rendszer biztonsága - Adatbázis-kezelő rendszer program könyvtárának és fájljainak védelme - Adatbázis adatfájljainak védelme - Adatbázis rendszerrel kapcsolatos operációs rendszer szintű felhasználók beállításai • Hálózati biztonság - Listener védelme - Port védelem - Az adatbázis-kezelő rendszer külső interfészeinek és ezeken áramló információknak a védelme - Külső objektumok elérése és külső eljáráshívás - Tükrözés, elosztott rendszerek, database link - Távoli hozzáférés adminisztrációs feladatok elvégzésekor • Adatbázist elérő alkalmazások biztonsági beállításai
Adatbázisban tárolt adatok biztonsága	• Adatbázis objektumok védelme hozzáférés szabályozással - Általános elvek - Objektum privilégiumok - Rendszer privilégiumok • Adatbázis szerepkörök - Adatbázis adminisztrátori szerepkör - Alkalmazás fejlesztői szerepkör - Adatbázis alkalmazás felhasználói szerepkör - Adatbázis alkalmazás adminisztrátori szerepkör • Adatok védelme titkosítással - Hálózaton - Adatbázisban
Működtetési folyamatok,	• Ügyrendi, biztonsági és egyéb eljárások szabályzatok • Adatbázis-kezelő rendszer telepítése és biztonsági fris-

eljárások	sítése - Adatbázis-kezelő rendszer telepítésének és frissítésének tesztelése - Az adatbázis-kezelő rendszer frissítése - Az adatbázis-kezelő rendszer elkülönítése, a nem használt komponensek eltávolítása • Felhasználók azonosítása, hitelesítése, bejelentkezése - Adatbázis felhasználók - Csoportos azonosítás és hitelesítés - Egyéni azonosítás és hitelesítés - Inaktív felhasználók - Jelszavak tárolása és tulajdonságai - Tokenekre és tanúsítványokra vonatkozó szabványok - Adatbázis rendszerekbe történő belépések • Adatbázis audit, log elemzés - Általános követelmények - Az audit tartalma - Audit nyomvonal, monitorozás, elemzés és jelentés • Éles és teszt környezetek szétválasztása • Adatbázismentés és helyreállítás

1.táblázat. Adatbázis biztonsági útmutató szerkezeti felépítése

FELHASZNÁLT IRODALOM

[1] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról

[2] *Muha Lajos*: Magyar Informatikai Biztonsági Keretrendszer (MIBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[3] *Berkes Zoltán, Déri Zoltán, Krasznay Csaba, Muha Lajos*: Informatikai Biztonsági Irányítási Rendszer (IBIR), Budapest: Miniszterelnöki Hivatal, 2008.

[4] *Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna*: Informatikai Biztonság Irányítási Követelmények (IBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[5] *Balázs István, Déri Zoltán, Lobogós Katalin, Muha Lajos, Nyíri Géza, Sneé Péter, Váncsa Julianna*: Informatikai Biztonság Irányításának Vizsgálata (IBIV), Budapest: Miniszterelnöki Hivatal, 2008.

[6] *Balázs István, Szabó István*: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)), Budapest: Miniszterelnöki Hivatal, 2008.

[7] *Krasznay Csaba, Muha Lajos, Rigó Ernő, Szigeti Szabolcs*: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX), Budapest: Miniszterelnöki Hivatal, 2008.

[8] e-Közigazgatási Keretrendszer Kialakítása projekt (2008): A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár, IT biztonsági műszaki követelmények

[9] DoD Directive 8500.1, Information Assurance (IA). – USA Department Of Defense, 2002.10.24.

[10] DoD Directive 8500.01E, Information Assurance (IA). – USA Department Of Defense, 2007.04.23.

[11] DoD Instruction 8500.2, Information Assurance (IA) Implementation. – USA Department Of Defense, 2003.06.06

[12] Database Secrity Technical Implementation Guide, Version 8, Release 1, 19 September 2007, Developed by DISA for the DoD

[13] Database Security Checklist, Version 7, Release 2.2, 30 October 2006, Developed by DISA for the DoD

[14] *Munk Sándor, Fleiner Rita*: Az adatbázis-biztonság szabályozása és megvalósítása az Egyesült Államok haderejében, Bolyai Szemle, XVIII. évfolyam 4. szám., 2009.

[15] *Bodlaki Ákos, Csernay Andor, Mátyás Péter, Muha Lajos, Papp György, Vadász Dezső*: Informatikai Rendszerek Biztonsági Követelményei (Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság ajánlása; 12.), Miniszterelnöki Hivatal, Budapest, 1996.