HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

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

Munk Sándor
munk.sandor@zmne.hu

AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁSÁNAK ALAPJAI A MAGYAR KÖZTÁRSASÁGBAN

Absztrakt

A publikáció az adatbázis biztonság szabályozásával foglalkozik. Ennek érdekében a szerzők megvizsgálják az adatbázis-biztonságot érintő informatikai biztonsággal kapcsolatos szabályozó dokumentumok típusait, bemutatják az adatbázis-biztonság és az informatikai biztonság szabályozási rendszerének jelenlegi szereplőit; végül feltárják a magyar adatbázis biztonsági szabályozó rendszer lehetséges felépítésének lehetőségeit.

The publication studies the regulation of database security. The authors examine the different types of regulatory documents related to information security and database security, describe the different actors of the hungarian information security regulation and finally outline the possible design of the hungarian database security regulation.

***Kulcsszavak**: adatbázis-biztonság, informatikai biztonság, adatbázis-biztonság szabályozása, közigazgatás ~ database security, information security, database security regulation, government*

BEVEZETÉS

Az informatikai biztonság az informatikai rendszer olyan állapota, amelyben az informatikai rendszerben kezelt adatok, valamint a rendszer elemei a fenyegetések ellen a megkívánt mértékben védettek. Az adatbázis-biztonság az informatikai biztonság részterülete, az adatbázis-kezelő rendszerek és az adatbázisokban tárolt adatok olyan állapota, amelyben ezek a fenyegetések ellen a megkívánt mértékben védettek.

A publikációban az adatbázis-biztonság állami szabályozásának kereteit és lehetőségeit vizsgáljuk a magyar viszonyok között. Az informatikai biztonság állami szabályozása a közigazgatás szereplőire és a kritikus infrastruktúrákra vonatkozóan lehet kényszerítő eszköz, ugyanakkor a magán szféra szereplői (saját döntés alapján) felhasználhatják szervezetük informatikai biztonságának biztosítására.

Konkrétan adatbázis-biztonságra vonatkozó szabályozó nem létezik, ezért egy tágabb terület, az informatikai rendszerek biztonságára kiterjedő állami szabályozást tanulmányozzuk és feltárjuk ezek adatbázis-biztonságot érintő vonatkozásait. Mivel a magyar törvényeknek és rendeleteknek összhangban kell állniuk a velük kapcsolatos Európa Uniós szabályozásokkal, a publikációban kizárólag a magyar szabályozókat vizsgáljuk.

Jelen publikáció alapvető célja, hogy megvizsgálja a közigazgatás informatikai rendszerein belül az adatbázis-biztonság szabályozásának lehetőségeit, kereteit. Ennek érdekében a publikáció:

- elemzi adatbázis-biztonságot érintő informatikai biztonsággal kapcsolatos szabályozó dokumentumok típusait, rendeltetését, tartalmát, célközönségét;
- rendszerezi az adatbázis-biztonság és az informatikai biztonság szabályozási rendszerének jelenlegi szereplőit;
- feltárja a magyar adatbázis biztonsági szabályozó rendszer lehetséges felépítését.

ADATBÁZIS ÚTMUTATÓK HELYE AZ INFORMATIKAI BIZTONSÁG DOKUMENTUMAINAK KÖRÉBEN

A következőkben megvizsgáljuk az informatikai biztonságot és a kritikus infrastruktúrákat érintő magyar jogszabályokat és a közigazgatásra vonatkozó ajánlásokat, majd kiemeljük ezek adatbázis-biztonságot érintő aspektusait.

Jogszabályok

Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény [1] határozza meg a központi elektronikus szolgáltató rendszer útján nyújtott elektronikus közszolgáltatások alapelveit, szabályait, használatának feltételeit. A törvény az elektronikus közszolgáltatások biztonságáról általános alapelveket fogalmaz meg, leírja például, hogy az elektronikus közszolgáltatás nyújtónak biztosítania kell az alkalmazott informatikai és kommunikációs rendszerek műszaki megfelelőségét és biztonságos működésének feltételeit. A törvényben felhatalmazást kap a Kormány arra, hogy rendeletben állapítsa meg a központi rendszer működtetésével, valamint szolgáltatásainak igénybevételével összefüggő részletes informatikai-biztonsági, adatbiztonsági követelményeket. Ennek kapcsán jött létre a 223/2009. (X. 14.) Kormányrendelet.

A 2009. évi LX. törvény felhatalmazása alapján létrejött *223/2009. (X. 14.) Kormányrendelet az elektronikus közszolgáltatás biztonságáról* [2] a közszolgáltatást végző informatikai rendszerek személyi, szervezeti és műszaki követelményeit tartalmazza - a következőkben szintén ismertetett - KIB 25. és 28. ajánlásokkal összhangban. A kötelező

erővel bíró rendelet hatálya az elektronikus közszolgáltatásokra, azok működtetőire, üzemeltetőire, és igénybe vevőire terjed ki és kimondottan informatikai biztonsági szempontokat tárgyal.

A rendeletben találunk az adatbázis rendszer – mint az informatikai rendszer részrendszere - biztonságát érintő követelményeket, előírásokat is. A kormányrendelet adatbázis-biztonságot is érintő főbb előírásai a következők:

- Az elektronikus közszolgáltatásoknak a rendszerben tárolt adatokra nézve meg kell valósítaniuk a bizalmasság, sértetlenség, rendelkezésre állás és kockázatarányos védelem elveit.
- Az elektronikus közigazgatási rendszerek biztonsági felügyeletét a közigazgatási informatikáért felelős miniszter látja el, aki a feladat ellátására az irányítása alá tartozó informatikai biztonsági felügyelőt jelöli ki.
- A magyar kritikus információs infrastruktúra védelméért a Nemzeti Hálózatbiztonsági Központ a felelős. Az elektronikus közszolgáltatás alapját képező Központi rendszer a kritikus infrastruktúra része, védelmét a kritikus infrastruktúrára vonatkozó, nemzetközileg kialakult biztonsági követelményeknek megfelelően kell kialakítani.
- Az elektronikus közszolgáltatást működtető szervezetnek információbiztonsági irányítási rendszert kell létrehozniuk. Ezen belül meg kell valósítani a minőségbiztosítást és szabályzati rendszert kell létrehozni. A rendelet a KIB 25. és 28. ajánlásokkal összhangban lévő dokumentáltsági követelményeket fogalmaz meg. A rendelet kimondja a következőket:

  „a tárolt és kezelt adatok biztonsága érdekében szolgáltatásműködési szabályzatot kell készíteni, meg kell határozni a rendszer működéséért felelős, az adatgazda, az adatkezelő, illetőleg az adatfeldolgozó, az üzemeltető és az igénybe vevők jogait és kötelezettségeit, valamint az adatkezelés, adattovábbítás és adatszolgáltatás eljárásrendjét”

  „az informatikai rendszerben forgalmazott adatok illetéktelen személy által történő megismerhetőségének megakadályozását elektronikus úton kell biztosítani az adatok keletkezési helyétől azok végső tárolási helyéig bezárólag, beleértve az adatok nyilvános hálózaton történő forgalmazását is”
- A kritikus rendszereket naplózni, menteni és archiválni kell.
- Adattovábbítás során kriptográfiai megoldásokat kell használni az adatok 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.
- Az elektronikus közszolgáltatás egyes elemeit biztonsági osztályokba kell sorolni, meg kell határozni az egyes biztonsági osztályokhoz tartozó védelmi szinteket és biztonsági követelményeket. A szolgáltatást nyújtó szervezetnek a biztonsági osztályba sorolást és a meghatározott védelmi szinteket az informatikai biztonsági tervében meg kell jelenítenie.

Informatikai rendszerekben tárolt és kezelt adatokra vonatkozóan számos, különböző vonatkozásokkal bíró törvény és kormányrendelet foglalkozik. Említést érdemelnek a

személyes adatok védelmével, a közérdekű adatok nyilvánosságával, illetve a minősített adatok kezelésével foglalkozó jogszabályok [3], [4], [5], [6]. Ezek az adatbázis-biztonság témáját csak nagyon távolról érintik, részletesebb vizsgálat a publikáció kereteibe nem fér bele.

Mivel a közigazgatás informatikai rendszerei a kritikus információs infrastruktúra részét alkotják, a kritikus infrastruktúra hazai szabályozását is vizsgálnunk kell. A magyar kormány a Kritikus Infrastruktúra Védelem Európai Programja hatására kiadta a *2080/2008 (VI. 30.) Korm. Határozatot a Kritikus Infrastruktúra Védelem Nemzeti Programjáról* [7], mely mellékletként a hazai Zöld könyvet is tartalmazza. A határozat általánosságokban tárgyalja a kritikus infrastruktúra fogalmait, a különböző ágazati hatáskörbe tartozó kritikus infrastruktúra védelmi tevékenységek feladatait és kereteit. A határozat a kritikus infrastruktúrákat 10 ágazatba és azon belüli alágazatokba sorolja, az ágazatokhoz kormányzati szerepkörrel bíró felelősöket rendel. A közigazgatási szolgáltatások alágazat a Jogrend – Kormányzat ágazat részeként szerepel a dokumentumban. Az informatikai biztonság témáját a határozat csak nagyon felületesen érinti.

Ajánlások

A következőkben a kormányzati informatikai rendszerek biztonságos működését elősegítő, de jogi értelemben nem kötelező erejű ajánlásokkal foglalkozunk. A Közigazgatási Informatikai Bizottság (a továbbiakban: KIB) az elektronikus közszolgáltatások biztonságos működésének elősegítése céljából adta ki 2008-ban a 25. számú és 2009-ben a 28. számú ajánlásait [8], [9]. A kötelező erejű 223/2009. (X. 14.) Korm. rendelet az ajánlásokkal összhangban született meg. 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)* [10] 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) [11], amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK) [12], 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) [13], amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

A *Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)* [14] 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)* [15] 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* [9] egy Követelménytár, amely az elektronikus közigazgatás fejlesztéséhez és üzemeltetéséhez szükséges szabványokat, követelményeket, előírásokat és információs anyagokat tartalmazza, az ajánlás webes felületen megjelenő segédeszköznek is tekinthető. Az *IT biztonsági követelmények*, és a *Termékek, szolgáltatások értékelésének, auditjának előkészítése* a 25. számú ajánlásra épülve, azt kiegészítő vagy végrehajtását támogató előírásokat, mintákat és követelményeket tartalmaz, illetve az *Egyéb követelmények, ajánlások* számos biztonsági szabványt, módszertant 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.

Dokumentumok értékelése, összegzése

Az informatikai biztonsággal kapcsolatos jogszabályokból és ajánlásokból az adatbázis-biztonság szabályozására nézve a következő pontokat tartom fontosnak kiemelni.

- Jelen pillanatban kimondottan adatbázis-biztonság szabályozásával jogszabályok és ajánlások nem foglalkoznak. Az elektronikus közszolgáltatás biztonságát szabályozó 223/2009. számú kormányrendeletnek vannak adatbázis-biztonságot érintő előírásai, a rendelet egy esetleges adatbázis-biztonság szabályozás számára a kereteket adja meg. A jövőben megszülethet a szükséglet arra –például a kritikus infrastruktúrák védelmének szabályozása kapcsán-, hogy jogszabályi vagy ajánlási szinten is megjelenjen az adatbázis-biztonság szabályozása.

- Az adatbázis-biztonság szabályozásának szervezeti szintjén a rendszabályoknak illeszkedniük kell a szervezet informatikai biztonsági szabályzatainak, dokumentumainak rendszerébe. A közigazgatási informatikai rendszerek szervezeti szintű biztonsági szabályozásának elemeit a 223/2009. számú kormányrendelet is tartalmazza, a KIB 25. számú ajánlás IBIR kötete pedig részletesen meghatározza a következők alapján:

  - *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 információ-feldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológia független tudjon maradni.” Az Informatikai Biztonsági Szabályzat nagyobb szervezeteknél kétszintű legyen. A szervezeti szintű IBSZ tartalmazza az általánosan és mindenre érvényes részletesebb szabályokat, míg a rendszer-specifikus szabályokat a rendszerszintű IBSZ tartalmazza.

  - *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.”

Az adatbázis-biztonsági rendszabályok a fenti szabályozási dokumentumok közül az Eljárásrend gyűjtemények körébe beilleszthetők. Bizonyos esetekben – például kritikus adatbázisokat üzemeltető szervezetek esetén – az Informatikai Biztonsági Szabályzatban is szükséges lehet egy részt az adatbázis rendszerek biztonsági szabályozására fordítani. Önmagában azonban egy jó eljárásrend kiadása még kevés, használatát elő kell írni. Szintén elő kell írni, hogy a külső és belső informatikai biztonsági auditok során az alkalmazását vizsgálni kell.

- A jogszabályokban és a szervezeti szintű szabályzatokban megtalálható, az adatbázis rendszerek biztonságos üzemeltetésével kapcsolatos előírásoknak (például mentés, naplózás, audit) összhangban kell lenniük az adatbázis-biztonsági rendszabályokban meghatározott előírásokkal.
- Az adatbázis-biztonsági rendszabályok követelményeinek függniük kell a tárolt adatok, illetve az adatbáziskezelő-rendszer biztonsági kategóriájától. Tehát az adatbázis-biztonság szabályozásának megvalósításánál az informatikai rendszerek és a feldolgozott információk biztonsági szintjeinek osztályozását figyelembe kell venni.

A KIB 25. és 28. számú ajánlása szerint (legalább) három szinten kell az informatikai rendszerek védelmét megvalósítani: (1) kiemelt szint, mely a minősített adatokat feldolgozó rendszereket jelenti, (2) fokozott szint, mely a belső használatú, bizalmas információkat kezelő rendszerekre vonatkozik, valamint (3) az alap szint, mely a széles körben, interneten keresztüli hozzáférést biztosító rendszerek védelmi szintje. A KIB 28. számú ajánlásban megtalálható IT biztonsági szintek megállapításának módja a következő három lépésből áll össze:

1. lépés: A tárolt adatok biztonsági kategóriájának megállapítása

A három biztonsági célra (bizalmasság, sértetlenség, rendelkezésre állás) külön-külön meg kell állapítani a biztonsági szintet, melynek lehetséges értékei: nem értelmezhető, alacsony, fokozott, kiemelt. (A nem értelmezhető szint csak a bizalmasság biztonsági célra vonatkozhat.)

2. lépés: Az informatikai rendszer biztonsági kategorizálása a biztonsági célok alapján

Az informatikai rendszert kell besorolni a bizalmasság, sértetlenség és rendelkezésre állás biztonsági célok alapján biztonsági osztályok (alacsony, fokozott, kiemelt) egyikébe. Az informatikai rendszerek biztonsági kategorizálásakor meg kell vizsgálni a rendszerben tárolt, feldolgozott, továbbított minden információ típus biztonsági kategorizálását, és ezen információk alapján kell megállapítani a rendszerhez rendelt biztonsági kategóriát. A három biztonsági célra (bizalmasság, sértetlenség, rendelkezésre állás) vonatkozóan külön-külön meg kell határozni a rendszerszintű biztonsági kategóriát, az egyes információ típusokra kapott legmagasabb értékek megállapításával.

3. lépés: Az informatikai rendszer biztonsági kategorizálása

A teljes informatikai rendszerre kell megállapítani egy biztonsági kategóriát. Az alacsony biztonsági kategóriájú rendszerben mindhárom biztonsági cél szerinti biztonsági kategória alacsony szintű. A fokozott biztonsági kategóriájú rendszerben legalább az egyik biztonsági cél fokozott szintű, és nincs fokozottnál erősebb szintű biztonsági cél. Végül a kiemelt biztonsági kategóriájú rendszerben legalább az egyik biztonsági cél szerinti biztonsági kategória kiemelt szintű.

A 223/2009. (X. 14.) Kormányrendelet is kimondja, hogy az adatokat érzékenységük és kritikusságuk szempontjából osztályozni kell. Az alkalmazásokat és az infrastruktúra elemeit a kezelt adatok biztonsági osztályával összhangban kell besorolni biztonsági osztályokba. A fejlesztők és üzemeltetők a biztonsági besorolásnak megfelelő adminisztratív és technikai védelmet kell, hogy kialakítsanak. A rendelet által előírt osztályozás nem teljesen egyezik a

KIB ajánlásokban található osztályozási rendszerrel, három helyett öt kategória használatát írja elő, melyek a következők:

(1) Különlegesen védendő (minősített) adatok, amelyekhez a belső és külső hozzáférés csak erősen korlátozva, szigorúan ellenőrizve és dokumentálva engedélyezhető,

(2) Érzékeny adatok, amelyekhez a belső és külső hozzáférést korlátozni, a hozzáférést naplózni kell,

(3) Belső adatok, amelyekhez a külső hozzáférés nem lehetséges, belső hozzáférés korlátozása nem kritikus,

(4) Nyilvános, közhiteles adatok, ahol a rendelkezésre állás és a megváltoztathatatlanság biztosítása kritikus,

(5) Általános kezelésű adatok.

ADATBÁZIS BIZTONSÁGI ÉS AZ INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSI RENDSZERÉNEK SZEREPLŐI

Mint azt korábban már bemutattuk, az adatbázis biztonság önmagában általában nem képezi szabályozás tárgyát, vagy az informatikai biztonság, illetve a kritikus információs infrastruktúrák védelmének részeként jelennek meg adatbázis biztonsági szabályozási elemek, vagy ezen szabályozások előírásai érvényesítendőek, adaptálhatóak az adatbázis biztonság területére. Ennek megfelelően a következőkben az informatikai biztonság és a kritikus információs infrastruktúra védelem szabályozási rendszerének felépítését vizsgáljuk meg, bemutatva annak szereplőit, feladat- és hatásköreit (feltárva az esetleges adatbázis biztonsági sajátosságokat). A szabályozási rendszer két nagy szférára (szintre) osztható, amelyből az első a kormányzati szintű szabályozás, a második az intézményi szintű szabályozás. Ez utóbbit részben – meghatározott körben – a kormányzati szabályozás írhatja elő, más része az intézmények (szervezetek) saját döntésének függvénye.

A kormányzati szintű szabályozási rendszer szereplői

Az informatikai szakterületi feladatok a Magyar Köztársaságban kormányzati szinten két nagy területre oszthatóak:

- - a közigazgatási informatika fejlesztése: a közigazgatás működésének javítása, az e-közigazgatás fejlesztése (cél: az állampolgárok minél magasabb szintű kiszolgálása);
- - az informatikai szolgáltatások körének, elérhetőségének bővítése: az informatika társadalmi, gazdasági, kulturális, oktatási, stb. célú alkalmazásának támogatása (cél: az információs társadalom kialakulásának elősegítése).

A kormányzati szintű szabályozási rendszer szereplői két nagy csoportba sorolhatóak. Az elsőbe a jogszabályok[1] előkészítésében érintett szereplők, a másodikba az ajánlások kidolgozásában részt vállaló szereplők sorolhatóak. A kormányzati szabályozási rendszer szereplői más szempontból csoportosíthatóak az állami vezetőkre (miniszterek, államtitkárok, helyettes államtitkárok), az irányításuk alatt álló minisztériumi (pld. főosztály-) vezetőkre és más szerepkörökre, illetve különböző kormányzati irányítás alatt álló, vagy kormányzati megbízás alapján feladatot ellátó bizottságokra, szervezetekre és hatóságokra.

A jogszabályok előkészítése a szakmailag illetékes miniszter feladata. A miniszterek feladat- és hatáskörét legmagasabb szinten a miniszterek feladat- és hatáskörét szabályozó kormányrendelet [16], valamint az egyes törvények képezik. Az állami vezetők feladat- és hatásköre az informatikai biztonságot átfogó módon nem tartalmazza. 2010 óta az e-

[1] Törvény, kormányrendelet, miniszterelnöki rendelet, miniszteri rendelet és más rendeletek.

közigazgatásért a *közigazgatási és igazságügyi miniszter*, a postaügyért, az audiovizuális politikáért, az informatikáért, a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért és az elektronikus hírközlésért pedig a *nemzeti fejlesztési miniszter* felelős. [16, 2. és 84. §] A nemzeti fejlesztési miniszter feladatai között – a közigazgatási intézményekre és az állami, vagy részben állami tulajdonban lévő társaságokra vonatkozóan – szerepel az informatikai biztonsági előírások megfelelőségének, betartásának ellenőrzése, valamint az informatikai biztonságért felelős vezetőkkel kapcsolatos jogok.

Az informatikai és ezen belül az adatbázis-biztonsági kérdésekhez szorosan kapcsolódó, a személyes adatok, illetve a minősített adatok védelmének szabályozási feladatai a *közigazgatási és igazságügyi miniszter* feladat- és hatáskörébe tartoznak.

A kritikus információs infrastruktúrákhoz kapcsolódó feladatok önállóan szintén nem jelennek meg, a kormányrendeletben egyedül a *belügyminiszter* kritikus infrastruktúra védelmi kormányzati koordinációs feladata, valamint a katasztrófák elleni védekezéssel kapcsolatos feladatkörében az infrastruktúra kritikus elemeivel kapcsolatos jogszabály-előkészítési és rendeletalkotási joga szerepel.

A miniszterek feladat- és hatáskörének megvalósítási rendjét, ezen belül a további állami vezetők (államtitkárok, helyettes államtitkárok) feladat- és hatáskörét, valamint az alapvető minisztériumi szervezeti egységek (főosztályok) feladatait az egyes minisztériumok Szervezeti és Működési Szabályzatai rögzítik. Eszerint az informatikához kapcsolódó miniszteri feladatkörök megvalósítása a Közigazgatási és Igazságügyi Minisztériumban a közigazgatási államtitkár irányítása alatt az *e-közigazgatásért felelős helyettes államtitkár*, a Nemzeti Fejlesztési Minisztériumban az *infokommunikációért felelős államtitkár* és irányításával a *kormányzati informatikáért*, illetve a *hírközlésért és audiovizuális médiáért felelős helyettes államtitkárok* feladata. [17, 61. §; 18, 21. §] Az államtitkári feladatok között informatikai biztonsághoz kapcsolódóak nem találhatóak.

A *Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala* a közigazgatási és igazságügyi miniszter – illetve egyes tevékenységek tekintetében a belügyminiszter, illetve a nemzeti fejlesztési miniszter – irányítása alatt álló központi hivatal, amelynek alaprendeltetése országos alapnyilvántartások vezetése, a közigazgatás korszerűsítésében való részvétel, ügyfélbarát közigazgatási eljárások kidolgozása, valamint az elektronikus közszolgáltatások továbbfejlesztése. Feladatai között szerepel a közreműködés a közigazgatási informatikai biztonsági politika kialakításában. [19, 6.2.a.14]

Az elektronikus közszolgáltatások biztonságáról szóló kormányrendeletben meghatározásra kerül a közigazgatási informatikáért felelős miniszter irányítása alatt működő *informatikai biztonsági felügyelő*, amelynek feladata az elektronikus közszolgáltatást nyújtó rendszerek eljárási és biztonsági követelményeknek való megfelelőségének felügyelete, ellenőrzése. [20, 5-6. §] Az informatikai biztonsági felügyelő feladatkörében azonban szabályozási feladatok nem szerepelnek.

Ugyanezen kormányrendeletben jelenik meg a közigazgatási informatikáért felelős miniszter felügyelete és az informatikai biztonsági felügyelő ellenőrzése alatt álló *nemzeti hálózatbiztonsági központ*, amelynek alaprendeltetése – a magyar kritikus információs infrastruktúrák védelme, valamint a központi rendszeren megvalósuló kommunikáció biztonsága, a vírus- és más támadások káros hatásainak korlátozása érdekében – a központi rendszer szolgáltatásait az Interneten keresztül érő támadások elleni védelem. Nevesített feladatai közé tartozik az informatikai és a hálózatbiztonságra, valamint a kritikus információs infrastruktúrák védelmére vonatkozó stratégiák és szabályozások előkészítésében történő részvétel.

A Nemzeti Hálózatbiztonsági Központot a kormány és más szervezetek által 2009-ben alapított *Puskás Tivadar Közalapítvány* működteti, az Országos Informatikai és Hírközlési

Főügyelet ügyeleti rendszerével párhuzamosan. Az elektronikus közigazgatás kialakítása és fejlesztése érdekében a központ feladatai közé tartozik a részvétel a közigazgatási informatikai biztonsági politika, az ellenőrzési rendszer és a megvalósításához szükséges alapfeltételek, valamint szabályozás kidolgozásában. [21, 16. o.]

A *Nemzeti Biztonsági Felügyelet* a közigazgatási és igazságügyi miniszter irányítása alatt álló, a Közigazgatási és Igazságügyi Minisztérium szervezeti keretében önálló feladattal és hatósági jogkörrel rendelkező szervezet, amelynek rendeltetése a minősített adatok védelmének hatósági felügyelete, kezelésük hatósági engedélyezése és felügyelete, valamint a nemzeti iparbiztonsági hatósági feladatok ellátása. A felügyelet konkrét szabályozási feladatokkal nem rendelkezik.

A *Közigazgatási Informatikai Bizottság* a kormány által 2007-ben létrehozott kormánybizottság [22], amelynek rendeltetése a szolgáltató állam kiépítésének meggyorsítása, az állampolgárbarát, gazdálkodóbarát közigazgatás megvalósítása, az informatika eredményeinek a közigazgatás egészében való terjesztése. A bizottság feladatkörébe tartozik többek között a közigazgatási informatikához kapcsolódó informatikai műszaki, biztonsági előírásokra vonatkozó szabályozások kezdeményezése, ajánlások elfogadása. [22, 5.c] A Közigazgatási Informatikai Bizottság és jogelődjei eddig hat informatikai biztonsági témájú ajánlást (ajánláscsomagot) fogadtak el.[2]

A *Kormányzati Koordinációs Bizottság* a kormány által a katasztrófavédelmi törvény felhatalmazása alapján 1999-ben létrehozott bizottság, amelynek rendeltetése a katasztrófák következményeinek felszámolására való felkészülés, a megelőzés és a végrehajtás feladatainak tárcák közötti koordinációja. A bizottságot 2010-től a belügyminiszter vezeti, tevékenységét a belügyminisztérium és az Országos Katasztrófavédelmi Főigazgatóság támogatja.

A kormány 2008-ban a KKB javaslatára fogadta el Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló Zöld Könyvet [23] és elrendelte a hazai infrastruktúra létfontosságú elemeinek védelméről szóló szabályozási koncepció összeállítását. 2010 őszére volt tervezve egy kritikus infrastruktúra védelmi törvény elfogadása, erre azonban nem került sor.

A bemutatott – esetenként potenciális – szereplők, illetve feladat- és hatáskörük alapján ***összegzésképpen*** a következők fogalmazhatóak meg. Az informatikai biztonság átfogó szabályozása nem szerepel a magyar kormányzati szabályozásban, helyette más – szűkebb – megközelítésű biztonsági szakterületek, mindenekelőtt a személyes adatok védelmének, a minősített adatok védelmének, illetve az elektronikus közszolgáltatások biztonságának szabályozásaival találkozhatunk. Ezek törvények és kormányrendelet formájában kerültek kiadásra. A kör a jövőben várhatóan bővülni fog a kritikus információs infrastruktúrák védelméhez kapcsolódó szabályozásokkal. A szabályozásokhoz kapcsolódóan az alapvető szerepet a jogszabályt előkészítő, feladat- és hatáskör szerint illetékes állami vezetők és minisztériumok játsszák.

Az eltérő megközelítésű, de az informatikai biztonsági kérdések esetében egymáshoz szorosan kapcsolódó szabályozások még ugyanazon minisztérium esetében sem állnak egymással teljes összhangban. Számos példa mutatható eltérő fogalmakra, kifejezésekre, értelmezésekre, eltérő elvekre és megoldásokra. Az aktuális jogszabályok fogalomrendszere nem egyezik meg a nemzetközi szabványok és bevált gyakorlatok alapján kidolgozott Magyar Informatikai Biztonsági Ajánlásokkal sem. Mindez a különböző jogszabályok hatálya alá tartozó tevékenységek – pld. minősített és személyes adatokat is kezelő közigazgatási

[2] ITB 8. (Inf. bizt. módszertan), ITB 12. (Inf. rsz. biztonsági követelményei), ITB 16. (Common Criteria), KIB 25. (Magyar Inf. Bizt. Ajánlások), KIB 26. (elektronikus azonosítás), KIB 28. (E-közigazgatási keretrendszer Követelménytár).

informatikai rendszerek – esetében megnehezíti az informatikai biztonság irányítását és megvalósítását.

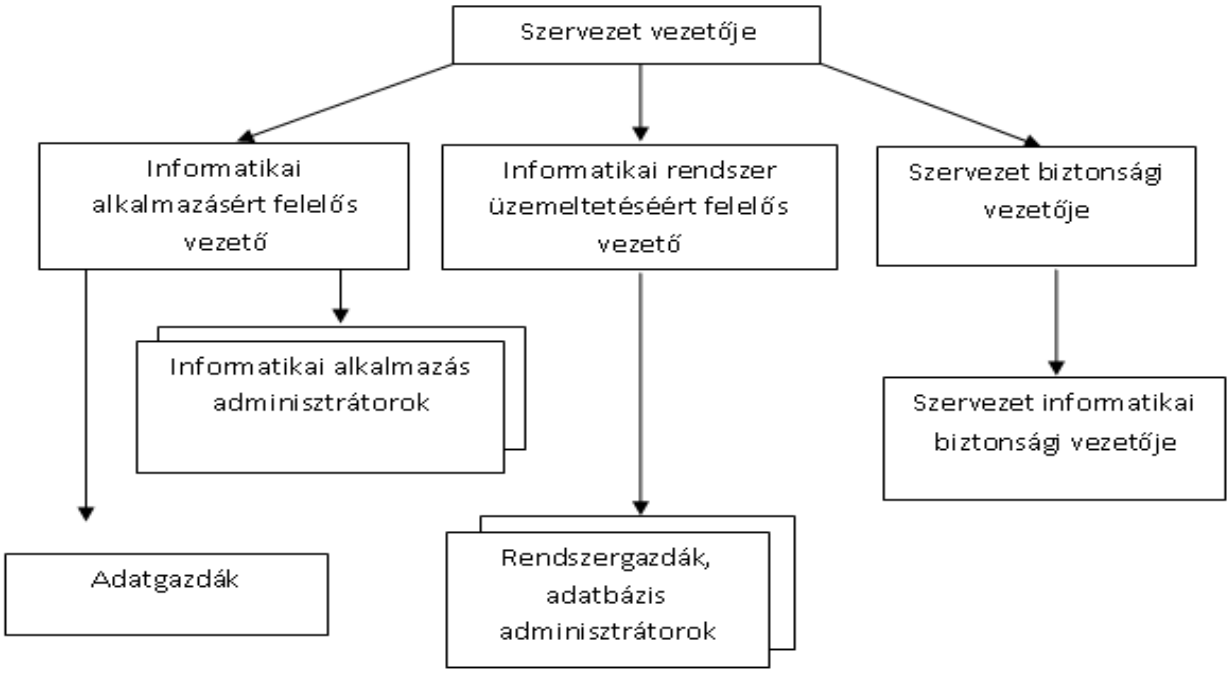
Az informatikai biztonság kormányzati szabályozása, valamint bármely szervezet informatikai biztonsági tevékenysége során felhasználható ajánlások kidolgozásának alapvető szereplője a Közigazgatási Informatikai Bizottság, amely összetétele alapján hosszú távon is megfelelő eszköze a széles körben hasznosítható dokumentumok megvitatásának és elfogadásának, ezzel a korszerű nemzetközi megoldások honosításának. Az ajánlások kidolgozásában – amire kormányzati, vagy szakmai kezdeményezésre, kormányzati fejlesztési tervek, programok, illetve megbízási szerződések keretében kerülhet sor – különböző állami, piaci és civil szervezetek vehetnek részt.

Az informatikai biztonságnak az átfogó nemzeti biztonságon belül, a közigazgatási informatikában és az információs társadalom építésében előre láthatóan egyre növekvő jelentősége miatt, az eredményes és hatékony, egymással harmonizáló megoldások érdekében megítélésünk szerint szükség lenne az informatikai biztonsággal kapcsolatos különböző szabályozások összehangolására, egy ezzel kapcsolatos koordinációs feladatkör megfogalmazására és ennek – a jelenlegi helyzetben – a közigazgatási és igazságügyi miniszterhez rendelésére. Mindezt a jelenlegi szabályozási területek, hatóságok és háttérintézmények önállóságának megtartásával célszerű megvalósítani.

Az intézményi szintű szabályozási rendszer szereplői

A 223/2009. (X. 14.) Kormányrendeletben is követelményként jelenik meg, hogy a szervezeten belül a biztonsági feladatok ellátására és ellenőrzésére azonosítható szerepköröknek kell rendelkezésre állniuk. Az adatbázis-biztonság szabályozása kapcsán megjelenő feladatokat társítani kell az informatikai biztonság szervezeti struktúrájában megjelenő különböző szerepkörökhöz. A következőkben ezek áttekintését végezzük el.

Az informatikai rendszer biztonságával kapcsolatos szerepköröket és ezek egy lehetséges kapcsolatrendszerét a következő ábra szemlélteti (a nyilak a közvetlen alá-fölé rendeltségi viszonyt jelzik).



1.ábra. Szervezeti szerepkörök az informatikai biztonság területén

Szervezet vezetője

Felelősségi körébe tartozik az elektronikus információvédelem gyakorlati megvalósítása, az elektronikus információvédelemre vonatkozó jogszabályok és előírások betartása, betartatása. Feladatkörébe tartozik a szervezet informatikai biztonságának személyi, szervezeti és pénzügyi feltételeinek megteremtése, a biztonsággal kapcsolatos felelősségi körök szabályozása, az informatikai biztonsági politika és stratégia kidolgoztatása, illetve megvalósítása. Rendszeresen kell ellenőriznie a bevezetett intézkedések betartását, hatékonyságát és gazdaságosságát [24].

Biztonsági Vezető

A szervezeten belül a biztonság komplex kezeléséért felelős. Gondoskodik az informatikai biztonságra vonatkozó jogszabályok, illetve az informatikai biztonságpolitika, az informatikai stratégia és az Informatikai Biztonsági Szabályzat végrehajtásáról, e körben szabályozási koncepciókat, szabályzat tervezeteket készít, a szakterületek megkeresésére vagy saját hatáskörben szakmai állásfoglalást ad ki.

Az informatikai biztonság szempontjából véleményezi a szervezet szabályzatait és szerződéseit. Irányítja és ellenőrzi az Informatikai Biztonsági Vezető munkáját [12].

Informatikai Biztonsági Vezető (Informatikai Biztonsági Felelős)

Felelős a szervezet informatikai rendszerével kapcsolatos biztonsági feladatok kezeléséért. A szervezet által üzemeltetetett, illetve annak adatait feldolgozó informatikai rendszerek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtése és fenntartása, ennek tervezése, szervezése, irányítása, koordinálása és ellenőrzése. Nagyobb szervezeteknél munkáját a vezetése alatt álló Informatikai Biztonsági Munkatársak segíthetik.

Jogosult az ellenőrzési tevékenysége során, a szervezet tulajdonában vagy használatában lévő dokumentumba, adatbázisba, számítógépes adathordozó tartalmába való betekintésre, az informatikai és távközlési eszközök vizsgálatára. Az informatikai biztonsági vezető szerepköre összeférhetetlen az informatikai rendszerért felelős vezető funkciójával, sőt annak alárendeltségében, tőle függő viszonyban sem lehetnek [12].

Feladatai közé többek között az alábbiak tartoznak:

- Felméri és elemzi az informatikai biztonsággal összefüggő veszélyforrásokat, meghatározza a kockázatkezelés módszerét.
- Kidolgozza az informatikai biztonság elérésére, illetve fenntartására vonatkozó szabályokat, utasításokat, terveket és irányelveket.
- Részt vesz:
  - a rendkívüli események kezelésére szolgáló tervek elkészítésében, azok naprakészen tartásában;
  - a fizikai biztonsági feltételek kialakításában, követelményeinek meghatározásában;
  - az informatikai biztonság szempontjából fontosnak minősített munkakörök betöltési szabályainak, feltételeinek meghatározásában;

- Szakmai szempontból közvetlenül irányítja a szervezet informatikai biztonsági tevékenységét.
- Ellenőrzi az informatikai biztonsági előírások végrehajtását.

Az informatikai alkalmazásért felelős vezető

Felelős az általa felügyelt informatikai rendszer egészének alkalmazásáért, bevezetésének és használatának megszervezéséért, illetve továbbfejlesztéséért és a kapcsolódó eljárási rend kialakításáért. Felelős továbbá a szervezet Informatikai Biztonsági Szabályzatának saját szervezeti egységét érintő részének elkészítésért és az abban foglaltak betartásáért.

Adatgazda

Felelős a számára meghatározott adatok meglétéért (beszerzéséért és előállításáért), hitelességéért és azok időben történő biztosításáért. Az adatgazda viseli a jogi és pénzügyi felelősséget az adatokért, ő tekinthető az adatok jogi értelemben vett tulajdonosának. Feladata a rendszerben tárolt adatok, információk osztályozása és védelme, a hozzáférés engedélyezése, tiltása. A hozzáférés engedélyezési jogkörét a kinevezett jogosultságigény engedélyezőkön keresztül gyakorolja.

Az adatgazda a nyilvántartó rendszerek esetében nem informatikus, hanem egy felhasználó, aki általában a leginkább érintett funkcionális terület vezetője (számlavezetés, könyvelés, stb.). Az informatikai kiszolgáló alkalmazásoknak (pl. Windows domain rendszer, Active Directory, adatátviteli hálózat vezérlő alkalmazás, naplógyűjtő és elemző alkalmazás stb.) adatgazdája informatikus [25].

Informatikai rendszer üzemeltetéséért felelős vezető

Felelős a szervezet informatikai rendszereinek rendeltetésszerű, előírt követelményeknek megfelelő működéséért. Felelős továbbá a szervezet Informatikai Biztonsági Szabályzatának saját szervezeti egységét érintő részének elkészítésért és az abban foglaltak betartásáért.

Általános rendszergazda, adatbázis adminisztrátor

A rendszergazda feladata az informatikai rendszer folyamatos üzemeltetése, beleértve az incidensek elhárítását, az adat- és rendszermentések szabályok szerinti elkészítését és tárolását, szükség esetén az adat visszaállítás végrehajtását, a karbantartási tevékenységek végrehajtását, a változások élesítését az üzemi környezetben; az üzemeltetői hozzáférési jogok beállítását az informatikai rendszereken a biztonsági felelős utasításainak betartásával.

Az adatbázis adminisztrátor feladata az adatbázis-kezelő rendszer által biztosított menedzsment feladatok kezelése, a rendszer folyamatos üzemeltetése a szabályzatokban szereplő feladatok elvégzésével.

A szervezeten belül el kell határolni az informatikai rendszert kezelő, fejlesztő, üzemeltető szerepeket a felhasználói funkcióktól. Az intézmény informatikai szervezeti egysége vezetőjének, a nagyobb és fontos alkalmazási területek vezetőivel egyeztetve a fontos alkalmazásokhoz rendszergazdákat kell kijelölniük, pontosan meghatározva feladataikat és felelősségüket. El kell különíteni a fejlesztői környezetet az alkalmazói környezettől, külön kell szabályozni a fejlesztői, működtetői és adminisztrációs hozzáférési jogköröket.

Az előbbiekben áttekintett szerepkörök közül az adatbázis-biztonságot szabályozó dokumentumokban szerepet kapnak a következők: az Informatikai Biztonsági Vezető, a

beosztásában lévő Informatikai Biztonsági Munkatársak, az Adatgazda, az általános rendszergazda és az adatbázis adminisztrátor.

A MAGYAR ADATBÁZIS BIZTONSÁGI SZABÁLYOZÓ RENDSZER FEJLESZTÉSÉNEK IRÁNYAI

A következőkben az adatbázis-biztonság szabályozó rendszerének fejlesztési 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. A magyar szabályozásban e tekintetben jelenleg egy hiányzó láncszemet érzékelünk. Célunk a nemzetközi szabványokhoz és a hazai jogszabályokhoz illeszkedő adatbázis-biztonság megteremtéséhez és fenntartásához szükséges lépések megfogalmazása.

További elemzésre és megfontolásra érdemes javaslat a jelenlegi Nemzeti Hálózatbiztonsági Központ bázisán, vagy azt magában foglaló megoldással egy Nemzeti Informatikai Biztonsági Központ kialakítása, amelynek feladatköre a hálózatbiztonság mellett kibővülne a közigazgatási informatikai rendszerek és a kritikus információs infrastruktúrák teljes körű informatikai védelmének koordinációs és egyes konkrét feladataival. A központ közigazgatási és igazságügyi, illetve nemzeti fejlesztési miniszterek irányítása alatt állhatna, egyben – ágazati résztvevőként – együttműködne a kritikus infrastruktúra védelem feladatait megvalósító, várhatóan a katasztrófavédelmi szervezetrendszer részét képező szervezettel.

Az adatbázis-biztonság szabályozását megítélésünk szerint az informatikai biztonság szabályozó rendszerének integráns részeként, a jelenleginél mélyebb tartalommal és az előzőekben bemutatott önálló dokumentumokkal szükséges megvalósítani, az átfogó informatikai biztonságért felelős miniszter feladat- és hatáskörében. Mindezt a Közigazgatási Informatikai Bizottság által elfogadott adatbázis-biztonsági ajánlások támogatnák, az adatbázis-biztonság felügyeletével és megvalósításával kapcsolatos konkrét feladatok pedig célszerűen a Nemzeti Informatikai Biztonsági Központ feladatkörébe tartoznának.

Javaslatunk szerint az adatbázis-biztonsági szabályozásnak egy többszintű rendszert kellene alkotnia. A szabályozás egyik részét képezné a szervezet és tevékenység független általános adatbázis-biztonsági útmutató, mely rendszabályok rendezett listája lenne és egy kormányzati központi szerv adná ki. Az általános adatbázis-biztonsági útmutató keretszabályozást jelentene, az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági követelményeket szervezet, tevékenység és termék független módon tartalmazná. A dokumentum mintaként szolgálna a szervezetek számára a saját adatbázis-biztonsági útmutató elkészítéséhez, mely már szervezet és tevékenység specifikusan tartalmazná a követelményeket, előírásokat. A dokumentumban lehetne egy termékfüggő adatbázis ellenőrzési lista elkészítését az adatbázis üzemeltetők feladatául kijelölni.

Az útmutató önmagában nem egy kötelező erejű jogszabály lenne, helyét magyar viszonylatban a KIB ajánlások között tudnánk elképzelni. Használatát viszont meghatározott szervezetek számára egy kormányrendelet elrendelhetné.

A szabályozás másik része szervezet specifikus dokumentumokból állna. A szabályozás hatálya alá eső szervezetnek ki kellene dolgoznia a saját általános adatbázis biztonsági útmutatóját az előző pontban leírt útmutató adaptációjával. Ebben az adatbázis rendszerre vonatkozó követelményeket saját szervezetére vonatkoztatva kellene megfogalmazni. Továbbá a szervezetnek az általános biztonsági követelményeket át kellene fogalmaznia

konkrét biztonsági elemek, ellenőrzési pontok halmazává, ami a saját adatbázis-kezelő rendszerére és az aktuális működési környezetre érvényes, ez lenne a szervezet adatbázis-biztonsági ellenőrző listája. Ebből a két dokumentumból épülne fel a szervezet adatbázis biztonsági szabályzata.

A szervezet általános adatbázis biztonsági útmutatóját a szervezeti szintű informatikai biztonság szabályozás részének a következő dokumentumok közé lehetne beilleszteni:

- Nagyobb szervezetek esetén a rendszerszintű Informatikai Biztonsági Szabályzatok közé
- Egyszintű Informatikai Biztonsági Szabályzat esetén annak egy fejezetének
- Eljárásrendek közé

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. A rendszer specifikus adatbázis-biztonsági ellenőrző listákat a szervezet készíti el a saját környezetére vonatkoztatva, a szervezet biztonsági dokumentumainak rendszerében az Eljárásrendek kategóriájába sorolható be.

Ha az általános adatbázis-biztonsági útmutató bizonyos szervezetek számára kötelező erővel bíró szabályozás részeként jelenne meg, akkor szükség lenne egy központi szervezetre – például az előzőekben javasolt Nemzeti Informatikai Biztonsági Központra -, melynek feladatába tartozna az alatta álló szerveken a felügyelet gyakorlása. A központi szerv feladat lenne annak ellenőrzése, hogy a kritikus adatbázisokat üzemeltető szervek létrehoztak-e szervezeti szintű általános adatbázis-biztonsági útmutatót és ellenőrzési listát, illetve elvégzik-e ennek alapján a biztonsági vizsgálatot. Elő kellene írni központilag, hogy milyen gyakran kell a szervezetben a biztonsági szabályozás alapján az ellenőrzést lefolytatni, annak eredményét dokumentálni kell és külső audit során az adatbázis-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.

Felhasznált irodalom

[1] 2009. évi LX. törvény az elektronikus közszolgáltatásról

[2] 223/2009. (X. 14.) Kormányrendelet az elektronikus közszolgáltatás biztonságáról

[3] A1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

[4] 2009. évi CLV. törvény a minősített adat védelméről

[5] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[6] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[7] 2080/2008 (VI. 30.) Korm. Határozatot a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[8] A KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA) http://www.ekk.gov.hu/hu/kib/KIB-25-0_MIBA_v1_vegl.pdf

[9] 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

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

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

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

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

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

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

[16] 212/2010. (VII. 1.) Korm. rendelet az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről.

[17] 17/2010 (VIII. 31.) KIM utasítás a Közigazgatási és Igazságügyi Minisztérium Szervezeti és Működési Szabályzatáról.

[18] 9/2011. (II. 15.) NFM utasítás a Nemzeti Fejlesztési Minisztérium Szervezeti és Működési Szabályzatáról.

[19] 42/2011 (IV. 20.) KIM utasítás a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala Szervezeti és Működési Szabályzatáról.

[20] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról.

[21] A Puskás Tivadar Közalapítvány Szervezeti és Működési Szabályzata (módosításokkal egységes szerkezetben). – Puskás Tivadar Közalapítvány Kuratóriuma, 2009.11.27.

[22] 1026/2007. (IV. 11.) Korm. határozat a közigazgatási informatikai feladatok kormányzati koordinációjáról.

[23] 2080/2008 (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[24] Póserné Oláh Valéria A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei, Hadmérnök II. Évfolyam 4. szám, 2007.

[25] A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről