10.17625/nke.2012.005

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM
Katonai Műszaki Doktori Iskola

Fleiner Rita

Az adatbázis-biztonság szerepe és megvalósításának feladatai a kritikus információs infrastruktúrák védelmében

Doktori (PhD) értekezés

Dr. Munk Sándor nyá. ezredes, egyetemi tanár
Dr. Muha Lajos mk. alezredes, főiskolai tanár
Témavezetők

Budapest, 2011

TARTALOMJEGYZÉK

BEVEZETÉS 4

1 AZ ADATBÁZIS-BIZTONSÁG, MINT AZ INFORMATIKAI BIZTONSÁG RÉSZE 9

1.1 AZ ADATBÁZIS-BIZTONSÁG FOGALMA, HELYE ÉS KAPCSOLATRENDSZERE AZ INFORMATIKAI BIZTONSÁGON BELÜL 9
1.1.1 ADATBÁZIS-BIZTONSÁG ÉRTELMEZÉSÉNEK ALAKULÁSA 10
1.1.2 ADATBÁZIS-BIZTONSÁG ÉS INFORMATIKAI BIZTONSÁG KAPCSOLATRENDSZERE 16
1.1.3 ADATBÁZIS-BIZTONSÁG HELYE, SZEREPE 20

1.2 ADATBÁZIS RENDSZEREK ARCHITEKTÚRÁI 24
1.2.1 MAGAS FOKÚ RENDELKEZÉSRE ÁLLÁS ADATBÁZISOK SZEMPONTJÁBÓL 27

1.3 AZ ADATBÁZIS-BIZTONSÁGOT VESZÉLYEZTETŐ FENYEGETÉSEK ÉS TÁMADÁSOK 31
1.3.1 SZEMPONTRENDSZEREK AZ ADATBÁZIS FENYEGETÉSEK OSZTÁLYOZÁSÁHOZ 31
1.3.2 JELLEGZETES ADATBÁZIS FENYEGETÉSEK A TÁMADÁS PONTJA SZERINT 35

1.4 KÖVETKEZTETÉSEK 40

2 AZ ADATBÁZIS-BIZTONSÁG ÉS SZEREPE A KRITIKUS INFRASTRUKTÚRA VÉDELEMBEN 42

2.1 A KRITIKUS INFRASTRUKTÚRÁK BIZTONSÁGÁNAK ALAPJAI 42
2.1.1 INFRASTRUKTÚRÁK 44
2.1.2 KRITIKUS INFRASTRUKTÚRÁK 45
2.1.3 KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK 48
2.1.4 KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK TÁMADÁSAI 50
2.1.5 KRITIKUS INFRASTRUKTÚRÁK VÉDELMI FELADATAI 53
2.1.6 KRITIKUS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK KÉRDÉSEI 55

2.2 ADATBÁZISOK SZEREPE A KRITIKUS INFRASTRUKTÚRÁKBAN 60
2.2.1 ADATBÁZISOK HELYE, SZEREPE KRITIKUS INFRASTRUKTÚRÁKBAN 60

2.3 KRITIKUS ADATBÁZISOK ÉS AZONOSÍTÁSUK 68

2.4 KÖVETKEZTETÉSEK 71

3 AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁS KERETEI A MAGYAR KÖZIGAZGATÁSBAN 73

3.1 ADATBÁZISOK A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁSBAN 74
3.1.1 A MAGYAR ELEKTRONIKUS KORMÁNYZAT FELÉPÍTÉSE 74
3.1.2 KRITIKUS ADATBÁZISOK A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁSBAN 80

3.2 AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁSÁNAK HELYZETE A MAGYAR KÖZIGAZGATÁSBAN 86
3.2.1 ADATBÁZIS ÚTMUTATÓK HELYE AZ INFORMATIKAI BIZTONSÁG DOKUMENTUMAINAK KÖRÉBEN 86
3.2.2 ADATBÁZIS-BIZTONSÁGI ÉS AZ INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSI RENDSZERÉNEK SZEREPLŐI 95
3.2.3 EGY LEHETSÉGE MODELL: ADATBÁZIS-BIZTONSÁG AZ USA HADEREJÉBEN 101

3.3 KÖVETKEZTETÉSEK 105

4 AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁS FEJLESZTÉSÉNEK IRÁNYAI A MAGYAR KÖZIGAZGATÁSBAN 108

4.1 ADATBÁZIS-BIZTONSÁGI ÚTMUTATÓK ALAPJAI 108
4.1.1 INFORMATIKAI BIZTONSÁGI ÚTMUTATÓK, KONTROLLOK 109

4.1.2 ADATBÁZIS-BIZTONSÁGI ÚTMUTATÓK, KONTROLLOK 114
4.2 ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁSÁNAK ALAPJAI 118
4.3 ÁLTALÁNOS ADATBÁZIS-BIZTONSÁGI ÚTMUTATÓ 122
4.4 KÖVETKEZTETÉSEK 142
ÖSSZEGZETT KÖVETKEZTETÉSEK 143
ÚJ TUDOMÁNYOS EREDMÉNYEK 145
AJÁNLÁSOK 145
ÉRTEKEZÉSSEL KAPCSOLATOS PUBLIKÁCIÓIM 146
FELHASZNÁLT IRODALOM 146
ÁBRAJEGYZÉK 154
TÁBLÁZATJEGYZÉK 154

BEVEZETÉS

A legtöbb szervezet számára a különböző formában tárolt információk, adatok biztonsága egyre kritikusabb feladattá válik. Az adatbázisokban, fájlkezelő rendszerekben vagy egyéb helyeken tárolt bizalmas adatok védelme az üzleti siker szempontjából kiemelkedő szereppel bír és napjainkban az informatikai szakemberek számára nagyon komoly kihívást jelent.

Az érzékeny adatokat védő informatikai megoldások olyan üzletágak esetén jelentek meg és váltak keresetté először, melyeknek meg kellett felelniük különböző, meglehetősen szigorú állami és iparági szabályozásoknak (például SOX, Basel II, HIPAA, PCI), melyek bevezetésére egy-egy törvénysértés vagy látványos hiba nyomán került sor. 2002-2003 körül világszerte számos tőzsdei gazdálkodó szervezetnél találtak olyan visszaéléseket, amelyek az adatkezelés hiányosságaira voltak visszavezethetőek, ezért elsőként az Egyesült Államokban majd az Európai Unióban is olyan jogi kényszerek jelentek meg, amelyek részletesen szabályozzák a tőzsdén megjelenő cégek adatkezelésének módját. Később a gazdaság más területein is szigorú előírások jelentek meg. A szabályozások az érintett cégeket arra kényszerítik, hogy megfelelő megoldásokat vezessenek be a bizalmas adatok kiszivárgásának megakadályozására. Ezek között a pénzügyi szektort, a bankszférát és az egészségügyet emelném ki, melyek rengeteg védendő, személyes adatot kezelnek, mint például hitelkártyaszámok, társadalombiztosítási számok vagy betegadatok.

Az utóbbi években nyilvánosságra került számos olyan eset, melyekben bizalmas információk, ügyféladatok szivárogtak ki adatlopás, hacker támadás vagy hűtlen kezelés miatt. Egy-egy ilyen incidens az érintett szervezet számára sok hatással jár együtt. Jelentősen ronthatja a vállalat, illetve az általa képviselt márka hírnevét, a kártérítési kötelezettség extra költségeket vonhat maga után, a meghamisított adatok és rendszerek visszaállítása időveszteséggel és többletmunkával párosul és sok esetben még jogi pereskedések, bírósági eljárások is következményként lépnek fel. Ma már az adatok védelmének kérdése a vállalatok és szervezetek általánosan elfogadott feladata lett.

Tudományos probléma

A fejlett XXI. századi társadalmak egyre nagyobb mértékben függenek a különböző (energetikai, kommunikációs, informatikai, közlekedési, ellátási, stb.) infrastruktúráktól és ezek az infrastruktúrák maguk is kölcsönösen függenek egymástól. A társadalmi, gazdasági és hétköznapi élet működési folyamatai egyre inkább veszélyeztetettek a legfontosabb – kritikusnak nevezett - infrastruktúrák működésének, szolgáltatásainak megszakadása esetén.

A kritikus infrastruktúrák működése napjainkban már szinte elképzelhetetlen az informatika eszközeinek, rendszereinek, alkalmazásainak támogatása nélkül. Ez az informatikai támogatás részben önálló információs infrastruktúrák révén, részben önmagukban kritikus infrastruktúrát nem alkotó, támogató összetevők révén jelenik meg. A támogató informatikai rendszerek jelentős részének működésében lényeges, esetenként kiemelt szerepet játszanak különböző adatbázisok is.

Adatbázisok számos kritikus infrastruktúrában megtalálhatóak és ezek közül sok esetben biztonságuk megsértése az adott kritikus infrastruktúra biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázis-biztonság és szabályozásának kritikus infrastruktúra védelem szempontjából vett vizsgálata.

Az elektronikus közigazgatásnak szükséges és alapvető feltétele az adatoknak, nyilvántartásoknak elektronikus tárolása, mely leggyakrabban adatbázisok segítségével valósul meg. Ezért az elektronikus közigazgatás területén fontos feladat az adatbázis-biztonság megvalósítása, ennek szabályozása, támogatása és ellenőrzése.

A hazai közigazgatási informatika védelmére készült KIB 25. és 28. ajánlások az informatikai védelem átfogó, komplex szabályozását nyújtják, emellett azonban szükség van az informatika egyes részterületeinek védelmét részterületi védelmi rendszabályokkal, útmutatókkal, ajánlásokkal elősegíteni, különös tekintettel a működés kritikus területeken. A közigazgatási informatika védelemben fontos részterület az adatbázis-kezelő rendszerek, illetve az azokban tárolt adatok védelme, melynek szabályozása hazánkban jelenleg még nincs kidolgozva.

Az előzőekben felvázolt problémák kapcsán kutatási területemnek az adatbázis-biztonság területét választottam. A kutatás során foglalkoztam az adatbázis-biztonság általános kérdéseivel, megvizsgáltam az adatbázis-biztonság és a kritikus információs infrastruktúra kapcsolatrendszerét, illetve az adatbázis-biztonság állami szabályozásának lehetőségeit. Az informatikai biztonság - és ennek részterülete az adatbázis-biztonság- állami szabályozása a közigazgatás szereplőire és a kritikus infrastruktúrákra vonatkozóan lehet kényszerítő eszköz. Mivel az elektronikus közigazgatás kritikus információs infrastruktúrának minősül, értekezésemben az adatbázis-biztonság szabályozási lehetőségeinek és kereteinek a magyar közigazgatáson belül végeztem el. A minősített információkat feldolgozó informatikai rendszerek, adatbázisok biztonsági kérdései a Nemzeti Biztonsági Felügyelet hatókörébe tartoznak, ennek a témának a tárgyalását nem tekintettem értekezésem tárgyának.

Kutatási témám választásában szerepet játszott, hogy az informatika biztonság területével a hollandiai egyetemi tanulmányaim óta foglalkozom. Munkám során részt vettem a hazai elektronikus közigazgatás megvalósítását elősegítő tanulmányok elkészítésében, a kritikus infrastruktúra kérdéseivel pedig a Zrínyi Miklós Nemzetvédelmi Egyetemen folyó kutatások kapcsán ismerkedtem meg. Az Óbudai Egyetemen adatbázis kezeléssel és adatbázis-biztonsággal kapcsolatos előadásokat és labor gyakorlatokat vezetek.

Kutatási hipotézisek

Kutatómunkám megkezdésekor abból indultam ki, hogy az adatbázisok a kritikus információs infrastruktúrákban fontos szerepet töltenek be, biztonságuk megsértése az adott kritikus információs infrastruktúra biztonságát fenyegeti. Feltételeztem, hogy lényeges kérdés az adatbázis-biztonságnak és szabályozásának kritikus infrastruktúra védelem szempontjából vett vizsgálata. Továbbá szükség van az informatika egyes részterületeinek – így az adatbázis rendszereknek - védelmét részterületi védelmi rendszabályokkal, útmutatókkal, ajánlásokkal elősegíteni, különös tekintettel a működés kritikus területeken.

Kutatásom célkitűzései

Kutatási célomnak az adatbázis-biztonság szerepének, fenyegetettség rendszerének és szabályozási lehetőségeinek elemzését, illetve kidolgozását jelöltem meg, különös tekintettel az adatbázisok kritikus infrastruktúra védelemben és azon belül az elektronikus közigazgatásban betöltött szerepére nézve.

A kutatási cél elérése érdekében a következő részcélok megvalósítását tűztem ki:

- Az adatbázis-biztonság alapjainak és az adatbázis-biztonság különböző értelmezéseinek feltárása. Az adatbázisokat tartalmazó informatikai rendszerek architektúráinak elemzése, illetve az adatbázis fenyegetések különböző formáinak rendszerezése.
- Az adatbázisok előfordulásának, helyének, szerepének és azonosítási lehetőségeinek elemzése, rendszerezése és értékelése a különböző kritikus infrastruktúra szektorokban.
- Az adatbázis-biztonság szabályozás jelenlegi helyzetének, kereteinek feltárása a magyar közigazgatásban.
- Az adatbázis-biztonság szabályozás fejlesztési irányainak és dokumentumainak meghatározása a hazai elektronikus közigazgatásban.

Alkalmazott kutatási módszerek

Széleskörű irodalomkutatást végeztem nemzetközi és hazai szakkönyvek, folyóiratok, kutatási munkák és az interneten található információk tanulmányozásával. Áttekintettem a kutatásom témáját érintő hazai és nemzetközi jogszabályokat, törvényeket, ajánlásokat. A források felhasználásával elemzéseket hajtottam végre, következtetéseket és ajánlásokat fogalmaztam meg.

Személyes beszélgetéseket, interjúkat folytattam a kutatási témám különböző területein dolgozó szakértőivel, illetve részt vettem több, a témával foglalkozó konferencián, szakmai napon. A szerzett információk és tapasztalatok feldolgozásával, értékelésével és elemzésével hasznosítottam az elhangzottakat a kutatásom folyamán. A kutatási célok elérése érdekében a munkám során felhasználtam a rendszerezést, a kritikai adaptációt, más kutatások másodelemzését, az összefüggéseknek az analízis és szintézis módszereivel való feldolgozását.

Értekezésem szerkezete

A doktori értekezésem négy fejezetből áll. Az első fejezetben elemeztem az adatbázis-biztonság különböző értelmezését és a fogalomban idők során bekövetkezett változásokat, feltártam az informatikai biztonság és az adatbázis-biztonság kapcsolatrendszerét, meghatároztam az adatbázis-biztonság helyét, szerepét az informatikai biztonságon belül és az általam alkalmazott adatbázis-biztonság fogalom értelmezését. Továbbá elemeztem az adatbázisokat tartalmazó informatikai rendszerek architektúráit és komponenseit, feltártam az adatbázis sérülékenységek különböző formáit és rendszereztem az adatbázis fenyegetéseket.

A második fejezetben összefoglaltam a kritikus infrastruktúrák fogalmi kérdéseit, támadási módszereit és védelmi lehetőségeit; elemeztem a kritikus infrastruktúrák azonosításának kérdéseit. Feltártam, rendszereztem és általánosságban értékeltem az adatbázisok előfordulását, helyét és szerepét a különböző kritikus infrastruktúra szektorokban. Bevezettem a kritikus adatbázis fogalmát; feltártam a kritikus adatbázisok azonosításának lehetőségeit.

A harmadik fejezetben elemeztem a magyar elektronikus kormányzat felépítését és ebben az adatbázisok helyét, szerepét. Elemeztem az informatikai biztonság szabályozását a magyar közigazgatásban, megállapítottam ebben az adatbázis-biztonság szabályozásának hiányát. Végül bemutattam az USA haderejében kifejlesztett adatbázis-biztonsági szabályozást, mint egy létező modellt.

A negyedik fejezetben elemeztem az adatbázis-biztonsági útmutatók és ellenőrzési listák felépítését, szerepét és ajánlást tettem a hazai adatbázis-biztonság szabályozásának rendjére és fejlesztési irányaira. Végül bemutattam egy közigazgatásban hasznosítható általános adatbázis-biztonsági útmutatót.

Értekezésem írása során rengeteg segítséget kaptam a környezetemtől. Szeretném külön megköszönni

- témavezetőimnek, prof. dr. Munk Sándornak és dr. Muha Lajosnak a folyamatos szakmai és emberi támogatást, és
- családomnak a kitartást, türelmet és sok fizikai és lelki segítséget.

1 AZ ADATBÁZIS-BIZTONSÁG, MINT AZ INFORMATIKAI BIZTONSÁG RÉSZE

BEVEZETÉS

Napjainkban az informatikai szolgáltatások jelentős része adatbázisokban tárolt információk kezeléséhez, rendelkezésre bocsátásához kapcsolódik. Az informatikai rendszerek jelentős részének működésében lényeges szerepet játszanak különböző adatbázisok. Az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az adatbázis-kezelő rendszerek biztosítják, melyek több felhasználós, hálózatos környezetben működnek.

A fejezet célja meghatározni az adatbázis-biztonság fogalmát az informatika biztonság rendszerének keretein belül, elemezni az adatbázisokat tartalmazó informatikai rendszerek architektúráit és rendszerezni az adatbázis-biztonságot fenyegető sebezhetőségeket, támadási módszereket. A felvázolt kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Elemeztem az adatbázis-biztonság különböző értelmezéseit és a fogalomban az idők során bekövetkezett változásokat; feltártam az informatikai biztonság és az adatbázis-biztonság kapcsolatrendszerét és meghatároztam az adatbázis-biztonság helyét, szerepét az informatikai biztonságon belül.
- Elemeztem az adatbázisokat tartalmazó informatikai rendszerek architektúráit és komponenseit;
- Rendszereztem az adatbázis fenyegetések különböző formáit és jellegzetes adatbázis fenyegetéseket gyűjtöttem össze.

1.1 AZ ADATBÁZIS-BIZTONSÁG FOGALMA, HELYE ÉS KAPCSOLATRENDSZERE AZ INFORMATIKAI BIZTONSÁGON BELÜL

A következőkben a téma alapozásaként az adatbázis-biztonság fogalmának, helyének és szerepének vizsgálatát végzem el [FR1] publikációm alapján. Ezen belül bemutatom az adatbázis-biztonság eddigi értelmezéseit és a fogalomban idők során bekövetkezett változásokat, fejlődéseket; feltárom az informatikai biztonság és az adatbázis-biztonság kapcsolatrendszerét; elemzem az adatbázis-biztonság helyét, szerepét, jelentőségét az informatikai biztonságon belül; végül ismertetem az általam alkalmazott adatbázis-biztonság fogalom értelmezését.

1.1.1 ADATBÁZIS-BIZTONSÁG ÉRTELMEZÉSÉNEK ALAKULÁSA

Az adatbázisok története szorosan összefügg az adatmodellek és az adatbázis-kezelő rendszerek történetével. Az adatbázis rendszerek folyamatos fejlődése hatással van az adatbázis-biztonsághoz tartozó fogalmak értelmezésére. Edgar F. Codd 1969-ben, az IBM munkatársaként kidolgozta a mai napig is legnépszerűbb és legelterjedtebb adatbázis típus logikai modelljét, a relációs adatmodellt. Ez az első adatmodell, amelyben már élesen szétválik a logikai és a fizikai adatbázis. Az adatbázisok magas szintű tervezésének fejlődésében egy másik jelentős időpont 1976, amikor is Peter Chen ismertette az egyed-kapcsolat adatmodellt, mely szoros kapcsolatban áll a relációs modellel és a gyakorlatban ma is elterjedt módszere az adatbázisok magas szintű tervezésének.

Az adatbázis-kezelő rendszerek jelenlegi, korszerű formái csak az 1960-as évek közepén kezdtek el kialakulni, azóta viszont folyamatosan fejlődnek. Az IBM-nél az 1970-es évek közepén Codd relációs modelljéhez kötődően kifejlesztették a System-R - ma DB2 - nevű adatbázis-kezelő szoftvert. Közben a CIA-nél is elindult egy Orákulum – angolul Oracle – nevű projekt, melynek célja egy olyan adattár létrehozása volt, amely a CIA minden felmerülő kérdését gyorsan, hatékonyan, és aránylag olcsón meg tudja válaszolni. A projekt egy idő után a CIA-nél véget ért, de a munka az 1977-ben alapított Relational Software Inc. (RSI, 1982-től Oracle Corp.) keretein belül folytatódott. 1978-ban elkészült az Oracle nevű adatbázis-kezelő rendszer első verziója, melynek lekérdező nyelve már az SQL elődjére, a SEQUEL-re alapult. 1986-ban az SQL, mint a relációs adatbázisok lekérdezőnyelve az Egyesült Államokban is, és Európában is szabványossá vált.

Napjainkban adatbázis-kezelő rendszer alatt több felhasználós, hálózatos környezetben működő, az adatbázisokhoz való hozzáférést, a felhasználói folyamatok zavartalan működését biztosító szoftveralkalmazást értünk. Adatbázisnak nevezzük valamely adatmodell szerint tárolt adatok halmazát, melyet az adatbázis-kezelő rendszer kezel. Az adatbázisokban koncentráltan található adatok biztonsága és védelme a kezdetektől fogva fontos feladat volt, azonban az adatbázisok elérési módjainak kiszélesedésével és a felhasználói kör kibővülésével új problémák, kihívások jelentek meg. Ezek a folyamatok hatással voltak az adatbázis-biztonság és védelem fogalmainak megváltozására is.

Adatbázis-biztonsággal kapcsolatos fogalmak az angol nyelv esetében több kifejezés formájában is előfordulnak. Ezek közé tartoznak a ’database security’, ’database assurance’, melyeket adatbázis-biztonságnak fordítunk, illetve a ’database protection’, magyarul adatbázis védelem.

Kutatásomban az adatvédelem kérdéskörét elkülönítettem az adatbázis-biztonság vizsgálatától. Az adatvédelem a személyes adatok védelmével, biztonságával kapcsolatos fogalom, mellyel az Adatvédelmi törvény [1] foglalkozik részletesen. Eszerint az adatvédelem a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozása, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. Az informatikai szaknyelv is elfogadta azt, hogy az adatvédelem az Adatvédelmi törvény által meghatározott adatok csoportjára vonatkozik.

Az adatbázis-biztonság fogalmának értelmezésekor nem szorítkoztam az adatok csak egy bizonyos csoportjára, az informatikai rendszerekben, azon belül adatbázis rendszerekben tárolt adatok egészének védelmét, biztonságát vizsgáltam. (Értekezésemben többször használom az érzékeny - vagy más szóval különleges, szenzitív - adat fogalmát. Érzékeny adatnak azokat a személyes adatokat nevezzük, melyek az ember személyiségét mélyebben érintik, sérelmüket nehezebben viseljük, ezért ezek az adatok fokozott védelemre tarthatnak számot. A magyar jog szerint különleges adat a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos, illetve lelkiismereti meggyőződésre vonatkozó adat. A szenzitív adatok egy másik csoportját az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó adatok alkotják [2].) A következőkben több forrás áttekintésével megvizsgálom az adatbázis-biztonság fogalmának értelmezéseit.

Először megvizsgálom néhány több kiadást megélt, felsőoktatásban is használt adatbázis témájú szakkönyvet. C. J. Date: An Introduction to Database Systems című könyvében [3] 27 fejezet közül egyet a biztonság témájának szentel, ahol az adatbiztonság fogalmát tisztázza elsőként. Véleménye szerint a biztonság az adatok védelmét jelenti a jogosulatlan felhasználók elől. Az adatbázis-kezelő rendszer rendelkezik biztonsági alrendszerrel, mely a hozzáférési kéréseket mindig egyezteti a rendszer katalógusában található biztonsági megszorításokkal, ezáltal biztosítva a biztonságos működést. Adatbázis-biztonság témakörébe tartozó problémákat, feladatokat vet fel és elemez, melyek közé az adatokhoz való hozzáférés szabályozása (access controll), azaz adatbázis felhasználók jogosultságainak beállítása, statisztikai adatbázisok biztonsági problémái (azaz megengedett lekérdezésekkel nem megengedett információkhoz megszerzésének kérdésköre), adatok titkosítása és nézetek definiálása tartoznak.

Elmasri, Navathe: Fundamentals of Database Systems című könyv [4] adatbázis-biztonság címet viselő fejezete azokat a technikákat tekinti át, melyek a különböző fenyegetések ellen

védik az adatbázisokat. A fenyegetések az adatok integritásának, rendelkezésre állásának és megbízhatóságának sérülését eredményezhetik. C. J. Date könyvében tárgyalt témák mellett a szerzők az adatbázis-kezelő rendszerek működésének biztonságát is felvetik. A támadás célpontja lehet az adatvagyon vagy pedig az azt kezelő informatikai rendszer. Az adatbázis-kezelő rendszer feladatának tekinti a támadás megelőzésének illetve felfedésének feladatán túl a támadó elszigetelését, a sérülés kiértékelését, a rendszer újra konfigurálását, az adatok és a rendszer funkciók sérülésének kijavítását és a hiba jövőbeni kiküszöbölését.

Az adatbázis-biztonság felsőfokú oktatásban való megjelenésének lehetőségeit tárgyaló cikkekben megtalálhatjuk azokat a témaköröket, melyeket a szerzők a témába illőnek találnak. Ezek közé tartoznak például az adatbázisok konzisztenciáját biztosító megszorítások (például az elsődleges és idegen kulcs megszorítások), a sor szintű biztonság, az adatokhoz való hozzáférés szabályozásának lehetőségei, a hitelesítés, a többszintű biztonság, a közvetett következtetés (inference), az adatbázisban tárolt adatok titkosítása és az adatbázis audit [5]. Adatbázis-biztonság oktatási tematikában egyre inkább teret nyer az adatbázis-kezelő rendszerek megfelelő karbantartása, a szoftver aktuális frissítéseinek telepítése. Hangsúlyossá válik a tradicionális adatbázis-biztonsági témák mellett–amik magának az adatbázisnak a biztosításáról szólnak - új területek tárgyalásának igénye, melyet a webes és hálózatos elérések számának növekedése, a bonyolult és heterogén kliens-szerver architektúrák kialakulása és az alkalmazás szerverek elterjedése váltott ki. Az új területek közé tartoznak a következők: operációs rendszer és adatbázis-kezelő rendszer biztosítása, alkalmazás biztosítása és sql injekció, többszintű biztonság, adattárházak, adatbányászat, statisztikai biztonság és adatbázis-biztonsági politikák készítése [6], [7].

Az adatbázis-biztonság fogalmát az indiai CERT szervezet a következőképpen határozza meg [8]: „*Adatbázis-biztonságnak nevezzük azokat a rendszereket, folyamatokat és eljárásokat, melyek megvédik az adatbázist az előre nem tervezett tevékenységektől. A nem tervezett tevékenységek körébe soroljuk a jogosultságokkal rendelkező felhasználók visszaéléseit, a rosszindulatú támadásokat, vagy nem szándékos hibákat, melyeket jogosultságokkal rendelkező felhasználók vagy folyamatok követnek el. Az adatbázis-biztonság része egy tágabb szakterületnek, az informatikai biztonságnak.”*

Az adatbázis-biztonság tárgykörének vizsgálata kapcsán érdemes megvizsgálni az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutató [9] tartalmát. Az adatbázisban tárolt adatok védelmét az adatbázis-kezelő rendszer által nyújtott védelmi lehetőségeken keresztül vizsgálja meg, tehát ebben a szemléletben az adatok

biztonsága és az azokat kezelő informatikai rendszer biztonsága egymástól elválaszthatatlan fogalomként jelenik meg.

A bemutatott értelmezések alapján is látható, hogy az adatbázis-biztonság értelmezése az idők folyamán megváltozott, kibővült. A szűkebb típusú értelmezés szerint az adatbázis-biztonságot a tárolt adatok biztonsága jelenti, ezen belül az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, ez a hozzáállás az adatbázis-kezelő rendszerekről nem tesz említést. Ez a szemléletmód az adatbázis-kezelő rendszerek első megjelenésétől kezdve megfigyelhető. A rendszerek fejlődésével és elterjedésével egy tágabb típusú értelmezés is megjelent, mely a tárolt adatokat és az ezeket kezelő adatbázis-kezelő rendszert tekinti a biztonság védendő objektumának. Az adatbázis-biztonságnak ezt a megközelítését találhatjuk meg az előzőleg hivatkozott USA Védelmi Minisztériuma hozzáállásában.

Az adatbázis-biztonság alanyának meghatározása mellett szólni kell a védendő tulajdonságok halmazáról is, amik természetesen konkrét alkalmazások és környezetek esetén eltérőek lehetnek. A biztonsági tulajdonságok elemzését az informatikai biztonság területén megtalálható tulajdonságok vizsgálatán keresztül érhetjük el, majd értelmezhetjük adatbázis-biztonságra vonatkozóan. A biztonság védendő tulajdonságai között három alapkategóriát mindig megtalálunk a magyar és a nemzetközi szakirodalom egyaránt, ezek a következők: bizalmasság (confidentiality), sértetlenség (integrity), rendelkezésre állás (availability). Ezek mellett még egyéb tulajdonságok is léteznek, mint például a letagadhatatlanság (non-repudation), hitelesség (authenticity), elszámoltathatóság vagy követhetőség (accountability vagy auditability), megbízhatóság (reliability) és garancia (assurance). A Közigazgatási Informatikai Bizottság által készített Magyar Informatikai Biztonsági Ajánlásokban [10] a következő meghatározásokat találjuk.

- Bizalmasság: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.
- Sértetlenség: Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.
- Rendelkezésre állás: Az informatikai rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időtartamra használható.

Látható, hogy ezen értelmezés a sértetlenség jelentésébe beleolvasztja a letagadhatatlanság és hitelesség tulajdonságokat anélkül, hogy megnevezné őket. Egy másik szintén kormányzati

dokumentumban [11] olvashatjuk a következőket: „*A sértetlenség fogalmába – jelen dokumentum megközelítése szerint – beleértendő az információk letagadhatatlansága és hitelessége is.*” Ezen tulajdonságok értelmezése a dokumentum szerint a következő:

- Letagadhatatlanság: Olyan biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az informatikai rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően.
- Hitelesség: A hitelesség az entitás olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz.

Az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Kormányrendeletben [12] a sértetlenséget szintén kibővített tartalommal definiálják a következő módon: biztosítandó, hogy *„a rendszerben kezelt adat tartalma és tulajdonságai az elvárttal megegyezzenek - ideértve a bizonyosságot abban, hogy az elvárt forrásból származik és a származás megtörténtének bizonyosságát is -, továbbá a rendszerelemek a rendeltetésüknek megfelelően használhatóak legyenek*.”

Az ISO/IEC 27001:2005-ös szabvány [13] elsődlegesen a bizalmasság, sértetlenség és rendelkezésre állás tulajdonságait emeli ki, de szól arról, hogy egyéb jellemzők is fontosak lehetnek, mint például a már említett letagadhatatlanság és hitelesség, emellett viszont szól még az elszámoltathatóság és megbízhatóság tulajdonságokról is. Az elszámoltathatóság az entitások (például felhasználók) tevékenységeinek nyomon követhetőségét jelenti az adott entitás felelősségének megállapíthatósága érdekében. A megbízhatóság több mutatóval jellemzett működőképességet jelent.

Adatbázis-biztonság nézőpontjából a bizalmasság annak biztosítása, hogy az adatok csak az arra jogosultak számára legyenek elérhetőek, a bizalmasság elvesztése az adatok illetéktelenek általi hozzáférését, megismerését jelenti. A sértetlenség azt jelenti, hogy a tárolt adatot, illetve az adatbázis-kezelő rendszert csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak és nem törölhetők. A rendelkezésre állás annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek a szükséges adatokhoz. A rendelkezésre állás megsértése azt jelenti, hogy az adatokhoz, illetve az adatbázis-kezelő rendszerhez való hozzáférés egy adott időtartamra nézve megsérül, vagy teljes mértékben megszűnik.

Az adatbázisok védelme szempontjából a bizalmasság, sértetlenség és rendelkezésre állás biztosításának követelménye mindenképp fontos szerepet játszik. A letagadhatatlanság és a hitelesség biztonsági kritériumait adatbázisokkal kapcsolatban ritkán említik, ezeket szokás a

sértetlenség biztonsági tulajdonság részének is tekinteni. A letagadhatatlanság az a biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az adatbázis-kezelő rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően, ezt auditálhatóságnak vagy elszámoltathatóságnak is szokták hívni. A hitelesség az adat forrásának, eredetének a valódiságát jelenti.

Az adatbázis-biztonság általam használt értelmezése

Továbbiakban az **adatbázis-biztonság alanyának** mind az adatbázisban tárolt adatokat, mind az azokat kezelő adatbázis-kezelő rendszereket tekintem.

Az **adatbázis-biztonság védendő tulajdonságai** közé elsődlegesen a bizalmasságot, sértetlenséget és rendelkezésre állást sorolom. Az utóbbi időben, a törvényi szabályozásoknak köszönhetően kialakult egy újabb védendő tulajdonság is, amit elszámoltathatóságnak vagy más néven auditálhatóságnak nevezünk.

Adatbázis-biztonság nézőpontjából a bizalmasság annak biztosítása, hogy az adatok csak az arra jogosultak számára legyenek elérhetőek, a bizalmasság elvesztése az adatok illetéktelenek általi hozzáférését, megismerését jelenti. A sértetlenség azt jelenti, hogy a tárolt adatot, illetve az adatbázis-kezelő rendszert csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak és nem törölhetők. A rendelkezésre állás annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek a szükséges adatokhoz. A rendelkezésre állás megsértése azt jelenti, hogy az adatokhoz, illetve az adatbázis-kezelő rendszerhez való hozzáférés egy adott időtartamra nézve megsérül, vagy teljes mértékben megszűnik. A letagadhatatlanság és a hitelesség biztonsági kritériumai adatbázisokkal kapcsolatban ritkábban merülnek fel. A letagadhatatlanság az a biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az adatbázis-kezelő rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően, ezt adatbázisok esetében ma inkább auditálhatóságnak hívják. A hitelesség az adat forrásának, eredetének a valódiságát jelenti.

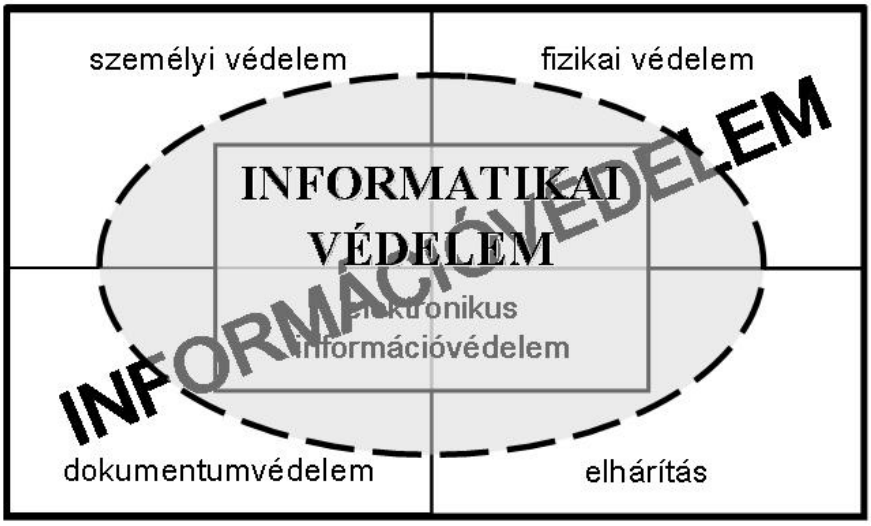
Összegzésképpen a bizalmasságot, sértetlenséget és rendelkezésre állást mindenképp a védendő tulajdonságok közé sorolom. Bár az auditálhatóság és hitelesség biztonsági tulajdonságok ritkábban jelennek meg az elvárások között, véleményem szerint létjogosult az adatbázis- biztonság védendő tulajdonságai között említeni őket. Fontosnak tartom ugyanakkor kiemelni, hogy ezek a védendő tulajdonságok konkrét adatbázis alkalmazások és környezetek esetén eltérőek lehetnek.

1.1.2 ADATBÁZIS-BIZTONSÁG ÉS INFORMATIKAI BIZTONSÁG KAPCSOLATRENDSZERE

A következőkben az informatikai biztonság és az adatbázis-biztonság kapcsolatát vizsgálom meg, melyhez szükséges néhány fogalom tisztázása is.

Az informatikai biztonság és az információbiztonság kifejezéseket még ma is gyakran összekeverik, felcserélik, egymás szinonimájaként használják. A két fogalom helytelen használata mögött az angol terminológia nem-egyértelműsége jelentős szerepet játszhat, ugyanis az angol nyelvben az 'information security' kifejezés írja le mind az informatikai biztonságot, mind pedig az információbiztonságot. Az angol dokumentumok magyar nyelvre történő fordításakor feltétlenül figyelembe kell venni a szövegkörnyezetet, ami alapján a helyes magyar terminológiát megválaszthatjuk.

Az információbiztonság és informatikai biztonság jelentését Muha Lajos [14] a következőképpen fogalmazza meg: *„Az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ezzel szemben például az informatikai biztonság „csak" az informatikai rendszerekben kezelt adatok, és az azt kezelő rendszer védelmét jelenti"*. Továbbá az információvédelem és informatikai védelem kapcsolatát vizsgálja a NATO védelmi előírására [15] alapozva, mely szerint *„Az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása, az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából"*. Az informatikai védelmet az információvédelemnél szűkebb, de önállóan is működtethető szakterületként jellemzi, amibe csak az informatikai rendszer védelme szempontjából szerepet játszó információvédelmi részterületek tartoznak. A két fogalom kapcsolatát Muha Lajos a következő ábrával szemlélteti:



1. ábra: Információvédelem és informatikai védelem kapcsolata [14]

Az informatikai rendszer fogalmának értelmezésére szintén különböző megközelítések léteznek. A NATO szabályozókat megvizsgálva például a következő releváns fogalmakkal találkozunk: ’information system’, ’communication system’ és ’communication and information system’ [16]. Általában az informatikai rendszer egységesen elfogadott sajátossága, hogy információs tevékenységeket támogat, összetevőit technikai eszközök, programok, adatok, illetve szükség esetén a működtető személyzet alkotják, illetve eleget tesz a rendszer fogalom követelményeinek is. Tehát nem nevezhető informatikai rendszernek egy egyedi eszköz vagy akár több, egymással kapcsolatban nem álló eszköz összessége sem [17].

A legszűkebb értelmezés a számítógépes rendszereket, egy ennél bővebb a számítógépes és kommunikációs rendszereket, a legtágabb pedig az információ feldolgozással kapcsolatos rendszereket sorolja ide. A továbbiakban informatikai rendszer alatt az információs tevékenységet támogató eszközök, programok, adatok, valamint a működtető személyek együttesét értjük [17]. Az informatikai rendszer a következő elemekből épül fel [18]:

1. az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra;
2. hardver;
3. szoftver;
4. kommunikációs eszközök és hálózat;
5. adathordozók;
6. dokumentumok és dokumentáció;
7. személyek.

Az informatikai biztonság és az informatikai védelem egymáshoz szorosan kapcsolódó fogalom. Az informatikai biztonságnak a szakirodalomban megtalálható meghatározásai

különböző nézőpontból közelítik meg a fogalmat, az eltérő hangsúlyok jöhetnek többek közt (1) a védelem, (2) a biztonság, mint állapot, (3) a biztonság ellenőrzése és (4) a védendő tulajdonságok oldaláról [19].

Az említett különböző hangsúlyok megjelennek például a hálózati munkacsoport egyik releváns RFC dokumentumában [20], melyben az informatikai biztonság fogalmát három pontban foglalják össze. A meghatározás magában foglalja egyrészt azokat az intézkedéseket, melyek az informatikai rendszer védelmére irányulnak, másrészt az informatikai rendszernek azt az állapotát, mely a védelmére létrehozott és fenntartott intézkedések hatására jön létre, harmadrészt pedig a rendszer erőforrásainak olyan állapotát, mely mentes a jogosulatlan hozzáférésektől, a jogosulatlan vagy véletlen változtatásoktól, tönkretételektől és veszteségektől.

Az ISO 27001:2005-ös szabványban [13] ’information security’ fogalom alatt az információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését értik, megjegyezve azt, hogy még egyéb tulajdonságok védelmére is szükség lehet, mint a hitelesség, elszámoltathatóság, letagadhatatlanság és megbízhatóság.

A témánkat érintő, egy másik széles körben elterjedt szabványban, a NIST 800-30-ban [21] informatikai biztonságon az informatikai rendszer tulajdonságát és működési folyamatait értik, melyek logikailag és fizikailag átszövik a rendszert. Az öt biztonsági cél pedig a sértetlenség, rendelkezésre állás, bizalmasság, elszámoltathatóság és garancia (mely az előző négy kritérium teljesítésére vonatkozik).

Az Amerikai Egyesült Államok hadseregében a biztonság alapfogalma a 'security' (biztonság, védelem) helyett az 'assurance' (garancia, garantált védelem) kifejezésre épül. Az ’information assurrance’ fogalmát következőképpen határozzák meg: mindazon intézkedések összessége, amelyek rendeltetése az információk és az informatikai rendszerek megóvása és védelme, rendelkezésre állásuk, sértetlenségük, hitelességük, bizalmasságuk és letagadhatatlanságuk biztosításával, beleértve az informatikai rendszerek helyreállítására irányuló védelmi, figyelési/észlelési és reagálási képességeket is [22].

Munk Sándor által javasolt biztonság alapmodellje [23] szerint az informatikai biztonság meghatározásához szükséges feltárni a biztonság alanyát, ennek sebezhetőségeit, védendő tulajdonságait és a fenyegetéseit. Az informatikai rendszer biztonságát fenyegetések veszélyeztetik, ami alatt olyan potenciálisan káros, vagy meg nem engedett hatást értünk, mely a védendő rendszer valamely összetevőjét károsan, egy megengedett mértéknél jobban

befolyásolja. A fenyegetések bekövetkezését az informatikai rendszer hiányossága vagy gyengesége, azaz sebezhetősége teszik lehetővé. A veszélyeztetés jellegét tekintve megkülönböztetünk fizikai, információs vagy tudati szinten jelentkező hatást [23].

Az informatikai biztonság értelmezése tekintetében Magyarországon a következő meghatározás terjedt el: Az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos [14].

Teljes körű védelem esetén a védelmi intézkedések a rendszer összes elemére kiterjednek. A védelem zárt, ha az figyelembe veszi az összes releváns fenyegetést. Folyamatos a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul. Kockázattal arányos a védelem, ha egy kellően nagy időintervallumot vizsgálva a védelem költségei arányosak a potenciális kárértékkel. A védelem akkor kielégítő mértékű, ha rá akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a kockázat az érintett fél számára még elviselhető szintű vagy annál kisebb [18].

Célszerű a biztonságot egy állapotként, a védelmet pedig tevékenységek rendszereként értelmezni. Az informatikai védelem az informatikai biztonság kialakítására és fenntartására - a biztonság összetevőinek érvényesülésére - irányuló tevékenységek és rendszabályok összessége [24]. A védelem feladatai közé tartozik a megelőzés, az észlelés, a reagálás és az esemény- vagy válságkezelés [14].

Napjainkban egy szervezeten belül az informatikai biztonság gyakorlata a következő alapintézkedéseket tartalmazza [10]:

1. az informatikai biztonságpolitika dokumentumainak elkészítése;
2. az informatikai biztonság felelősségeinek kiosztása;
3. informatikai biztonságtudatosság, képzés és oktatás;
4. helyes adatfeldolgozás az alkalmazásokban;
5. műszaki sebezhetőség kezelése;
6. működésfolytonosság irányítása;
7. az informatikai biztonsági incidensek menedzsmentje.

Ha az informatikai biztonság meghatározását megvizsgáljuk, akkor észrevesszük, hogy az két alapterületet foglal magában. Egyrészről az informatikai rendszerben kezelt adatok

sértetlenségének, bizalmasságának és rendelkezésre állásának elvesztését kívánja megakadályozni. Másrészről pedig magának az informatikai rendszernek a megbízható működését jelenti, ami magába foglalja a rendszer elemeinek sértetlenségét és azok rendelkezésre állását. Az informatikai biztonságot veszélyeztető fenyegetések elsősorban az adatok biztonságát veszélyeztetik, de gyakran nem közvetlenül, hanem az azokat kezelő rendszerelemeken keresztül érvényesülnek.

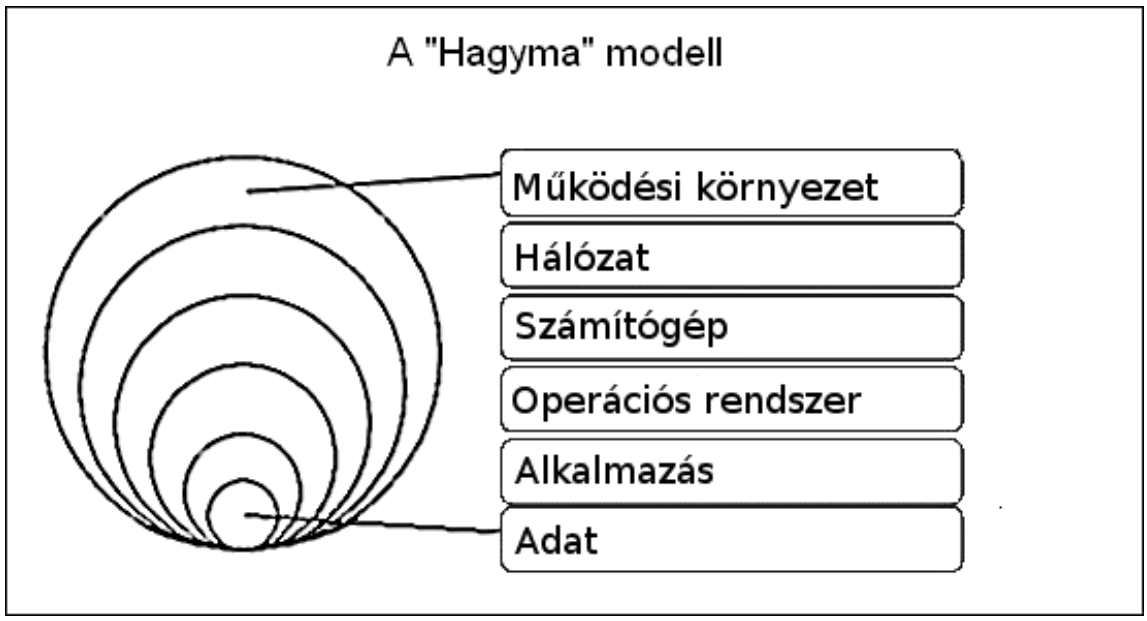
Ha az informatikai biztonság és az adatbázis-biztonság kapcsolatát szeretnénk feltárni, akkor meg kell vizsgálnunk mindkét esetben a biztonság alanyát, illetve annak védendő tulajdonságait. Az informatikai biztonság alanya az informatikai rendszer és az abban kezelt adatok halmaza, az adatbázis-biztonság esetében pedig az adatbázis-kezelő rendszer és az adatbázisokban tárolt adatok. Az informatikai rendszerek által kezelt adatok egyik leggyakoribb tárolási módját az adatbázisok alkotják, az adatbázis-kezelő rendszerek pedig az informatikai rendszerek részét képezik, vagyis az adatbázis-biztonság alanya az informatikai biztonság alanyának a része. Az előző fejezetben felvázolt adatbázis-biztonságot érintő tulajdonságok – sértetlenség, rendelkezésre állás, bizalmasság, auditálhatóság, hitelesség – az informatikai biztonság esetében is lényeges szerepet játszanak. Ebből az is következik, hogy az adatbázis-biztonságot érintő sérülékenységek, illetve fenyegetések az informatikai biztonságra is lényeges hatással vannak. Ezek alapján megállapíthatjuk, hogy az adatbázis-biztonság az informatikai biztonság részét képezi, köztük rész-egész viszony áll fenn.

1.1.3 ADATBÁZIS-BIZTONSÁG HELYE, SZEREPE

Az informatikai rendszerek fejlődésével, elterjedésével az informatikai biztonság szakterülete is bővül, fejlődik, egyre több speciális részterülete alakul ki. Az informatikai rendszerek biztonságának kialakításában mára a ’mélységi védelem’ (angolul defense in depth) stratégiája egy meghatározó iránnyá vált, melyben a védelmet több rétegbe szervezve kívánják elérni (ez az elv megtalálható például az USA haderejének informatikai védelmi direktívájában is [22]). A rétegek kategorizálása több szempontrendszerre épülve történhet, például az informatikai rendszerek különböző komponenseinek vezérfonala alapján.

Ha az alábbi ábrán található ’hagyma modell’ szerint vizsgáljuk az informatikai biztonságot, akkor megkülönböztethetünk adatbiztonságot, operációs rendszer biztonságot, alkalmazás biztonságot, hálózat biztonságot és működési környezet biztonságot. Mivel az informatikai rendszerekben az adatok tárolására az egyik legelterjedtebb módszer az

adatbázisokban történő tárolás, a ’hagyma modell’ szerinti informatikai biztonság legbelső területének részét képezi az adatbázisokban tárolt adatok biztonsága.



2. ábra: Az informatikai biztonság hagyma modellje [25]

Az adatbázis-biztonság az informatikai biztonság részét képzi, csakúgy, mint a hálózat biztonság, operációs rendszer biztonság, alkalmazások biztonsága vagy a fizikai biztonság. Az adatbázis-biztonságot az informatikai rendszer többi elemével egységben, csak komplex módon lehet megvalósítani, ugyanakkor célszerű és létjogosult, mint az informatikai biztonság egy különálló területét kezelni, ami hangsúlyosan érvényes a kritikus információs infrastruktúra védelem tekintetében.

Az előbbi gondolatot támasztja alá az USA Védelmi Minisztériuma által kiadott, a vezérlő rendszerek biztonságával foglalkozó egyik dokumentum is [26], melyben az informatikai biztonságot érintő egyik legkritikusabb támadási módszerként elemzik a vezérlő rendszerek adatbázisait érintő támadásokat. A következőket olvashatjuk: *„Adatbázis alkalmazások a vezérlő rendszerek és a kapcsolódó naplózó rendszerek alkalmazás komponenseinek egyik leglényegesebb elemét adják.” „Az adatbázisokban található információ értékes célponttal bír a támadók számára. Az értékes adatokat tartalmazó adatbázisokba való behatolás messzire kiható következményekkel járhat, különös tekintettel a vezérlő rendszerek környezetében, ahol az adat pontosság és integritás kritikus mind az üzleti, mind a működési döntési folyamatokban.”*

Az adatbázis-biztonság és védelem az adatbázis-kezelő rendszerek megjelenése és elterjedése utáni években egészen mást jelentett, mint manapság. A hagyományos adatbázis

védelem a hitelesítés (authentication), jogosultság kiosztás (authorization) és hozzáférés szabályozás (access control) köré csoportosul. Ezek megfelelő használata ma is a biztonságos működés szükséges feltétele. Az adatbázisok elterjedésével, elérésük módjának kiszélesedésével, illetve a különböző támadási módszerek megjelenésével az adatbázis-biztonság fogalomköre is tágult. A támadások számának növekedésével és a törvényi szabályozások bevezetésével a biztonsági megoldások bővültek. Új igények, szükségletek jelentek meg az adatbázis-biztonsági megoldások területén, mint például az adatbázisokban történő adattitkosítás, a felhasználók hitelesítésének és jogosultság kiosztásának a komplex informatikai rendszeren belüli egységes kezelése, az adatok biztonsági besorolását figyelembe vevő jogosultság kiértékelés, az adatbázis rendszerek monitorozása vagy a kiváltságos felhasználók jogainak korlátozása.

Az adatbázis-biztonság megvalósulásához kiemelt figyelmet kell fordítani az informatikai rendszer adatbázis rendszerekkel összefüggő összetevőinek biztonságára is. A hálózat, az adatbázis szervert futtató gép operációs rendszerének és az azon futó egyéb alkalmazásoknak (web szerver, alkalmazás szerverek, címtár szerver) megfelelő védelme szorosan összefügg az adatbázis-biztonsággal. Az adatbázist elérő alkalmazások jelentik az adatbázisok felé az egyik legnagyobb támadási felületet. Az adatbázis-biztonság és az informatikai biztonság egyéb részterületeinek szoros kapcsolatának hangsúlyozását megtalálhatjuk az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutatóban [9] is.

Feltehetjük a kérdést, hogy van-e létjogosultsága az adatbázis-biztonsággal, mint az informatikai biztonság egy meghatározott területével külön foglalkozni vagy pedig ezt az informatikai biztonság helyes kezelésével automatikusan úgyis elérjük? Mivel az adatbázis-kezelő rendszerek és az adatbázisok az informatikai rendszer egy elhatárolható részét képzik - a több rétegű architektúra modellben például egy speciális réteget alkotnak -, védelmüket egy külön egységet kezelve célszerű megtervezni és biztosítani. Ezt alátámasztja egyrészt az, hogy léteznek kimondottan az adatbázisok ellen irányuló támadási módok, másrészt pedig az informatikai biztonságot komplex módon érintő incidensek súlyos következményekkel járhatnak az adatbázisokban tárolt adatok biztonságára nézve. A következőkben néhány kritikus infrastruktúrával kapcsolatos biztonsági incidensen keresztül megvizsgálom azok adatbázisokat érintő hatását.

2009 decemberében számítógépes támadás érte az amerikai Nemzeti Légügyi és Űrhajózási Hivatalának (NASA) két alrendszerének informatikai központját. A támadók adminisztrációs felületeteket hackeltek meg, valószínűen demonstrációs célból. A

megtámadott oldalakról készült képernyőfotókból megállapítható volt, hogy a hackerek súlyos módosításokat is végrehajthattak volna a rendszerben, amire azonban nem került sor. A támadást SQL injekciós módszerrel hajtották végre [27]. Feltételezhető, hogy a NASA informatikai rendszere erős informatikai védelemmel rendelkezik, támadások számára nem képvisel könnyű célpontot, mégis a fenti eset bekövetkezhetett. A támadás módszere arra enged következtetni, hogy a támadóknak súlyos adatbázisokat érintő módosításokat is lehetőségükben állt végrehajtani.

2009. január 19. és február 7. között két olyan incidens következett be az elektronikus kormányzatot támogató Központi Elektronikus Szolgáltató Rendszer működésében, melynek adatbázist érintő vonzata is volt [28]. A hibák utáni biztonsági ellenőrzések során megállapították, hogy az incidensek visszavezethetőek a nem kellő gondossággal letesztelt programmódosítások éles üzembe állítására, a változáskezeléssel kapcsolatos – informatikai biztonság körébe tartozó – szabályok és eljárásrendek személyi mulasztás miatt bekövetkezett figyelmen kívül hagyására.

Az első incidens során az Országos Egészségbiztosítási Pénztár (OEP) informatikai rendszere az egészségügyi szolgáltatóknál és a gyógyszertárakban olyan állampolgárok esetében is rendezetlen jogviszonyt jelzett vissza hibásan, akik ténylegesen érvényes biztosított jogviszonnyal rendelkeznek. Az incidens során nem az alapadatok, hanem a feldolgozás során újra számított adatok sérültek meg. A megsérült adatokat tartalmazó adatbázisok újraszámlálása és ellenőrzése jelentette a helyreállítás időigényének jelentős részét.

A második incidens során az ügyfélkapu beléptetési moduljának átmeneti tárában (cache) keletkezett olyan üzemzavar, amely a hiba időszakában az ügyfélkapun belépett felhasználók egy része esetében a kapcsolatok keveredését okozta. A hiba oka az új program verzió hibás konfigurációs beállítása okozta. A hiba következtében felhasználók saját adataival nem tudtak belépni az ügyfélkapun, ugyanakkor a bejelentkezési kísérlet eredményeként másik – szintén bejelentkezni szándékozó - felhasználónak az adataival beléptek az Ügyfélkapu belső felületére. A hiba következtében a felhasználó hozzáférhetett a másik felhasználónak a Központi Rendszer által biztosított tartós tárához, törölhette annak ügyfélkapus regisztrációját, letölthette a más címére érkezett visszaigazolásokat, üzeneteket vagy átmehetett valamely szakrendszer szolgáltatásaihoz (például az APEH rendszerébe) és a szakrendszer által engedélyezett szolgáltatásokat igénybe vehette. Ez utóbbi következmény

például az APEH adatbázisaiban tárolt adatok módosítását és megismerését tette lehetővé, ami a legsúlyosabb biztonsági incidenst jelenti.

Ezek a példák is szemléltetik az informatikai biztonság és az adatbázis-biztonság szoros kapcsolatát, a kimondottan adatbázis-biztonságot érintő támadások jelentőségét a teljes informatikai biztonságra, illetve tetszőleges informatikai biztonsági incidens súlyos következményeit az adatbázis-biztonságra.

1.2 ADATBÁZIS RENDSZEREK ARCHITEKTÚRÁI

A következőkben a kritikus adatbázisokat tartalmazó informatikai rendszerek architektúrájának elemzését végzem el [FR2] publikációm alapján. Ismertetem a többrétegű architektúrák modelljeit, komponenseit és bemutatom a kritikusság szempontjából egyik leglényegesebb biztonsági célt, a magas fokú rendelkezésre állást megvalósító rendszerek felépítését.

Az adatbázis kezelő rendszerek architektúrájában jelentős változás, fejlődés figyelhető meg [29]. A kezdetekre a legegyszerűbb felépítés az egygépes megvalósítás jellemző, ahol az adatbázis és az azt feldolgozó program ugyanazon a gépen található, az adatbázist egy adott időben csak egyetlen program használja.

A **file-szerver** architektúrában az adatbázis állományok már átkerülnek egy központi szerverre, ami csak az adatok tárolásáért felelős és egy időben több program is elérheti ezt a hálózaton keresztül. Ha a felhasználó adatműveletet akar végrehajtani, akkor az adatrekordoknak el kell jutniuk a felhasználóhoz a hálózaton. Ez nagy adatforgalommal jár, ami a hálózat túlterheléséhez vezethet.

A **kliens-szerver** architektúra esetén két egységet különböztetünk meg. Az adatok közvetlen kezeléséért az adatbázis-szerver a felelős, míg az ügyfél program feladata a felhasználóval való kapcsolattartás és az üzleti logika által megkívánt feladatok végrehajtása. A hálózaton a feldolgozandó adatoknak csak a szükséges része utazik a szervertől a kliensig. Az adatfeldolgozást a szerver végzi a kliens parancsai szerint, a parancsokat SQL nyelvben adjuk meg.

A **többrétegű (angolul multi-tier) adatbázis architektúrában** a kliens nem közvetlenül az adatbázis-szerverhez, hanem a középen elhelyezkedő alkalmazás szerverhez kapcsolódik. Az alkalmazás szerver végzi el az üzleti logika által megkívánt számításokat, feldolgozásokat és hajtja végre az adatbázis-szerverrel a kommunikációt. A kliens az alkalmazás szervertől

kapja a szükséges adatokat, feladata csak a felhasználóval való kapcsolattartás (vékony kliens). A modern rendszerekre ez a felépítés jellemző, ezért a következőkben erre koncentrálunk.

A következőkben a kritikus adatbázisokat tartalmazó informatikai rendszerek felépítését vizsgálom. Feltételezem, hogy a rendszert sok felhasználó használja és az adatbázisok hálózati összeköttetés útján érhetők el. Napjainkban ezekre a rendszerekre gyakori a többrétegű architektúra szerinti felépítés, bár elterjedőben van egy új modell, a szolgáltatás orientált architektúra is. A réteg egy funkcionálisan elkülönített hardver és szoftver komponenst jelent, a legtisztább estben önálló számítógépre telepítve. A rendszerek egyik jelentős csoportját alkotják a webes alkalmazások, ahol a rétegeknek speciális elnevezéseik vannak. A következő rétegek különböztethetőek meg:

A **megjelenítési réteg** (felhasználói felület, kliens, user interface) felelős a felhasználói felületért és a felhasználóval való kapcsolattartásért, az architektúra legtetején helyezkedik el. A kliens felületnek felhasználóbarátnak, ugyanakkor elronthatatlannak kell lennie. Webes alkalmazások esetén ezt a réteget a böngésző jeleníti meg, mely HTTP protokollon keresztül kapcsolódik a web szerverhez.

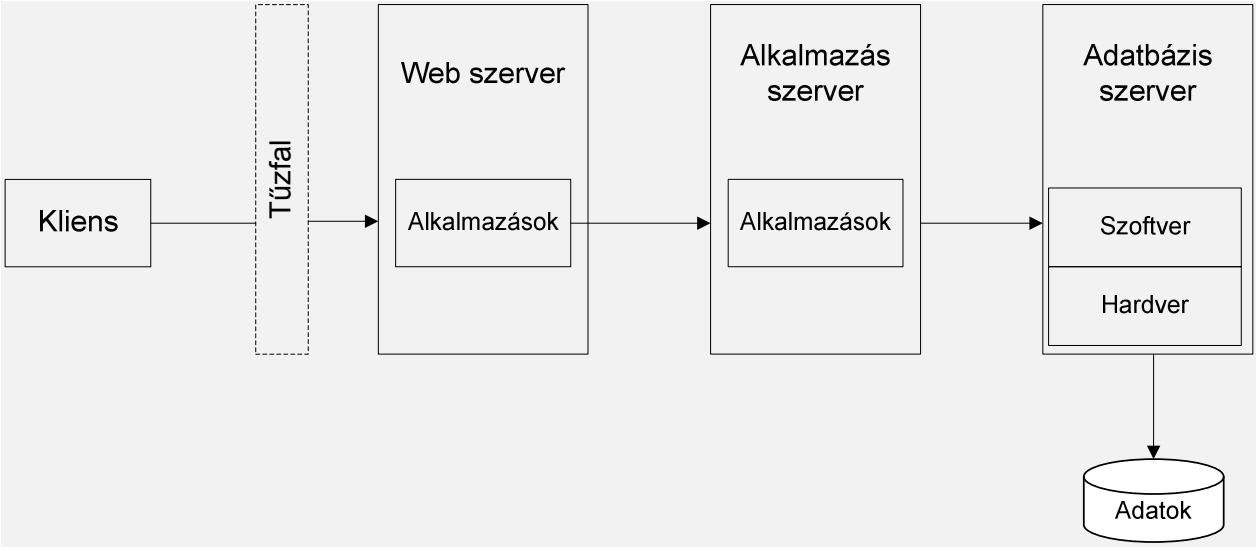
A **távoli elérés kiszolgáló réteg** felelős a felhasználói felülettel való kapcsolattartásért. A kliens kéréseit továbbítja az alkalmazás réteg felé, illetve az onnan érkezett válaszokat küldi vissza a kliensnek. Leggyakrabban ez a réteg képezi a választóvonalat a szervezet megbízható belső hálózata és a megbízhatatlan külső hálózat (például az internet) között. Webes alkalmazások esetében ez a réteg a web szervert, a HTTP forgalom kezelésével kapcsolatos részt jelenti, melyet tűzfallal védenek.

Az **alkalmazás réteg** (alkalmazás logika, üzleti logika) felelős az alkalmazás által megfogalmazott feladatok végrehajtásáért, az egy szinttel lejjebb elhelyezkedő adatbázis rétegtől a szükséges adatok megszerzéséért, illetve ezen adatok módosításának, törlésének kezdeményezéséért. Ennek a rétegnek a feladatát egy vagy több alkalmazás szerver látja el. Ezek a biztonságos belső hálózatban találhatók, méghozzá a web szerver és az adatbázis szerverek között.

Az **adatbázis réteg** a többrétegű architektúra legalsó szintjén található, az adatok fizikai eléréséért, feldolgozásáért felelős. E réteg feladata például az adatbázis állományok nyitása, zárása, új adat felvitele, törlése, módosítása, indexek kezelése, zárolási konfliktushelyzetek

feloldása. Ez a réteg az adatok alkalmazásoktól független tárolásáért felelős. Ebben a rétegben kaphatnak helyet az adatbázisok, adatbázis szerverek, fájl szerverek, különböző háttértárak.

Az adatbázisokat tartalmazó rendszerek felépítése nagyon összetett és változatos lehet. Az alábbi ábra egy olyan részstruktúrát mutat be, mely bonyolultabb rendszerekben is építő elem lehet. Ezt a struktúrát szem előtt tartva végeztem el a fenyegetések rendszerezését.

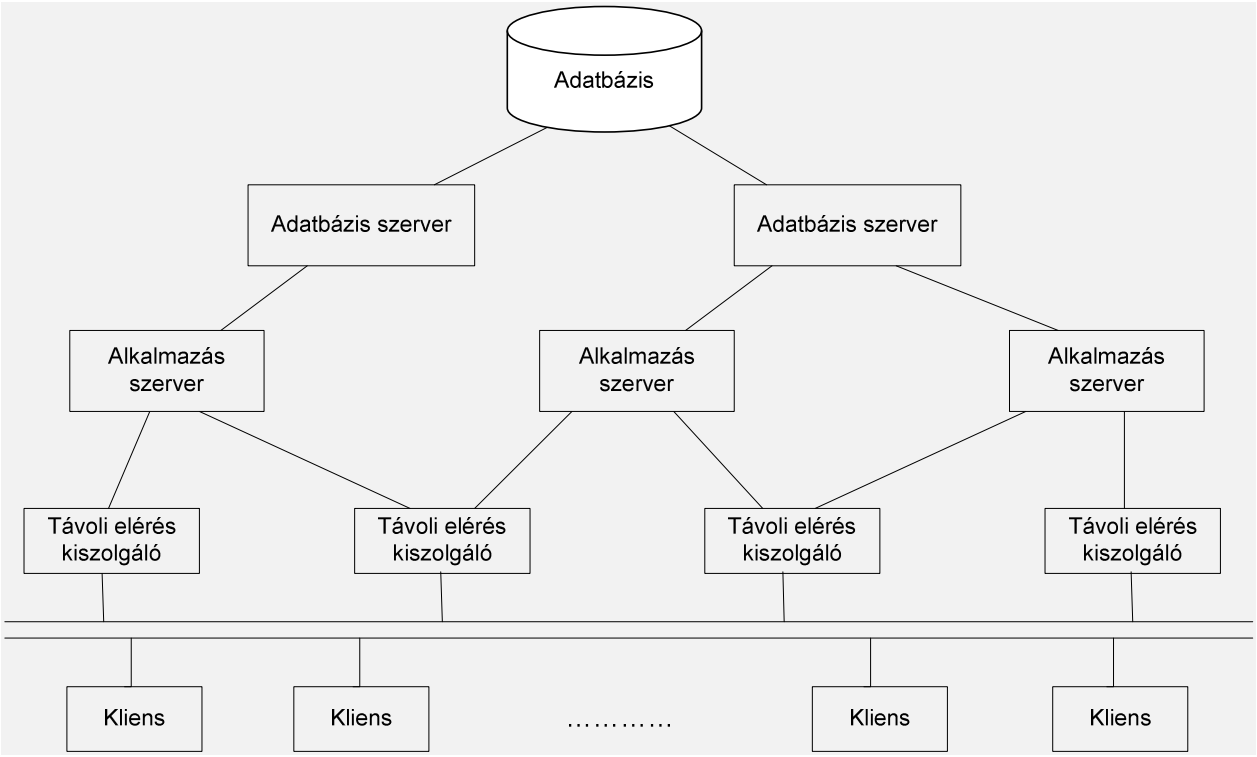


3. ábra: Adatbázisokat tartalmazó rendszerek architektúrája [30]

Az architektúrában a kliens nem közvetlenül fordul az adatbázis-kezelő rendszerhez, hanem egy alkalmazást használ, ami az adatbázis adataihoz való hozzáférést is elvégzi. Az ábrán egy tűzfal látható a web szerver előtt, a gyakorlatban azonban az architektúra több pontján is előfordulhat. Gyakran az adatbázis-kezelő rendszereket futtató számítógépeket is tűzfal védelemmel látják el. A kliens tehát a web szerveren, alkalmazás szerveren és adatbázis szerveren keresztül éri el az adatokat. Az adatbázis szerver esetén a hozzá tartozó platformot is ábrázoltam, amit hardver és szoftver részekre osztottam fel.

A 3. ábrán látható felépítés egy javasolt architektúra tervet mutat be. A rétegek fizikai és logikai szétválasztása a sérülékeny pontok helyes kezelését és az érzékeny adatok védelmét segíti. Vannak azonban olyan helyzetek, amikor a fenti architektúra módosított változatát lehet, illetve célszerű használni. Előfordulhat, hogy a web szervert és az alkalmazás szervert fizikailag ugyanarra a gépre kell, illetve célszerű helyezni. Léteznek olyan informatikai rendszerek, melyek a külső, megbízhatatlan hálózattól teljesen szeparáltan működnek, tehát az összes réteg a megbízható tartomány része. Máskor egy proxy szerver segítségével történik a külső és a belső hálózat elválasztása. A proxy szerver fogadja a kliensek kéréseit és továbbítja ezeket az azonos gépen elhelyezkedő web/alkalmazás szerver felé.

A hatékonyság és a biztonságos működés érdekében a nagy rendszerek esetén egy-egy réteg feladatát több szerver látja el párhuzamosan. A következő ábra ezt a megvalósítást szemlélteti:



4. ábra: A 4-rétegű architektúra több-szerveres környezetben [31]

A struktúra persze módosulhat, ha például több adatbázis szerver kommunikál egymással, gondoljunk az osztott adatbázis rendszerekre, vagy a magas rendelkezésre állás biztosítására kiépített fürtözött vagy tükrözött struktúrákra.

1.2.1 MAGAS FOKÚ RENDELKEZÉSRE ÁLLÁS ADATBÁZISOK SZEMPONTJÁBÓL

A vizsgált informatikai rendszerek kritikus adatbázisokat tartalmaznak, ebből kifolyólag az adatbázis réteg egyik lényeges követelménye lesz a rendelkezésre állás biztosítása. Informatikai rendszerek rendelkezésre állásán azt az időarányt értjük, amellyel egy definiált időintervallumon belül a rendszer a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható. A definíciót csak javítható (azaz meghibásodás esetén visszaállítható) rendszerek esetén értelmezzük. A rendelkezésre állás (availability, A) kiszámításának módja:

$$A = (MTBF)/(MTBF + MTTR),$$

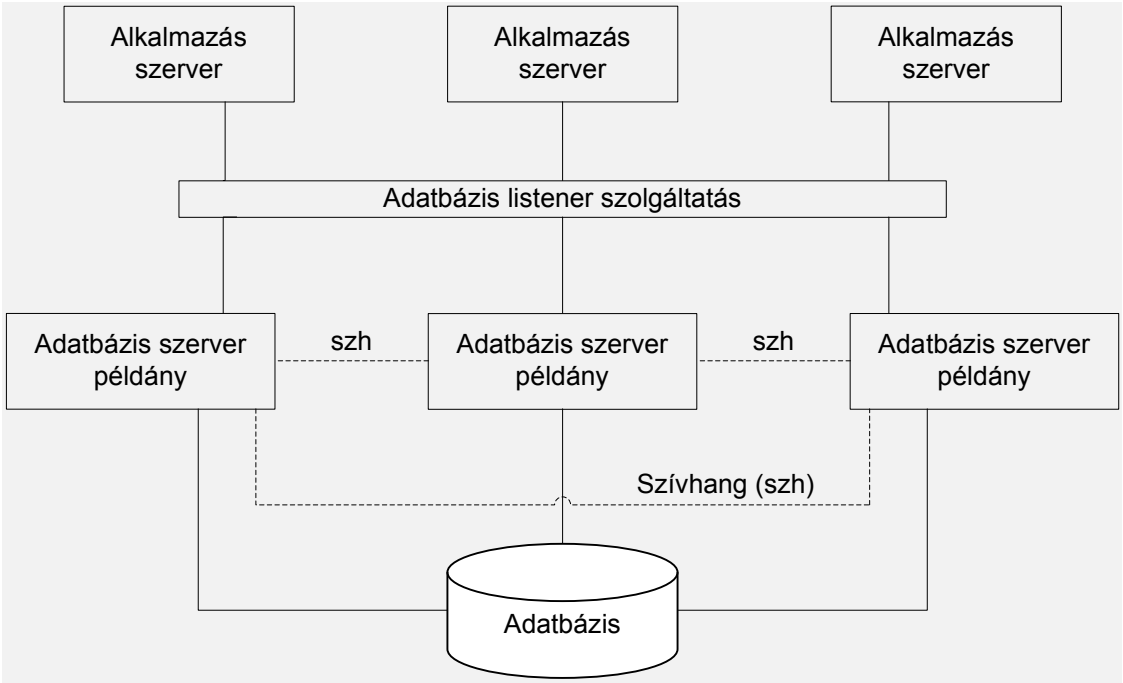
ahol MTBF a meghibásodások közötti átlagos idő (Mean Time Between Failures), MTTR

pedig a visszaállítás átlagos ideje (Mean time to repair). Magas fokú rendelkezésre állás esetén az arány (A) egyhez közeli érték (pl. 99%).

Adatbázis rendszerek tekintetében a magas fokú rendelkezésre állás biztosítása az adatok mentése és a rendszerek meghibásodásának kivédése köré csoportosul. Az adatbázis-kezelő rendszerek fejlett mentési és helyreállítási eszközökkel rendelkeznek, melyek az adatok védelmének szükséges eszközei. Többféle biztonsági mentési technika létezik, ezek közé tartoznak a teljes mentés, a részleges mentés és ennek két alapvető fajtája az inkrementális és a differenciális mentés.

Értekezésemben az adatbázis-biztonságot a kritikus infrastruktúra védelem szempontjából tanulmányozom. A kritikus infrastruktúrákban az elsődleges biztonsági cél a kritikus infrastruktúra által biztosított szolgáltatások hosszútávú rendelkezésre állása. Természetesen a többi biztonsági kategória (pld. bizalmasság, sértetlenség) sem hanyagolható el, többek között azért is, mert a kritikus infrastruktúra támadása, a rendelkezésre állás megakadályozása kiindulhat egy másik biztonsági tulajdonság megsértéséből. Terjedelmi korlátok miatt értekezésemben a hosszútávú elsődleges biztonsági célt szem előtt tartva, az adatbázisok magas fokú rendelkezésre állásának biztosítását, módszereit tekintem át.

Adatbázis szerverek fürtözése (database cluster) a szerverpéldányok meghibásodása ellen nyújt védelmet, az adatbázisok adatait tároló periféria meghibásodása ellen nem. Fürtözés esetén az adatbázis szerverpéldányokat (csomópontok, node-ok) kapcsolunk össze privát hálózaton keresztül, ezek fizikailag nincsenek egymástól messze és ugyanazt az adatbázis állományt érik el, mely külön periférián, diszken helyezkedik el. Ha az egyik csomópont meghibásodik, egy másik veszi át a szerepét. Az adatbázis szerver fürtözésének alapja egy üzemelés figyelő („létfenntartó") szolgáltatás, a szívhang (heartbeat), mely a fürtben található csomópontok egészségi állapotát ellenőrzi. Ha a főkiszolgáló kiesik (meghibásodás vagy tervezett leállítás, pl. karbantartás miatt), akkor a kiszolgálást a másodkiszolgáló veszi át, az adatbázis réteg listener szolgáltatását értesítvén arról, hogy mostantól ő az elsődleges kiszolgáló. Tehát, ha az alkalmazás rétegből kapcsolatot kezdeményeznek az adatbázis réteg felé, akkor az adatbázis listener szolgáltatás már a működő adatbázis szerverpéldányhoz irányítja a kapcsolatot. A főkiszolgáló visszaállítása után, az új adatok visszakerülnek rá, a szolgáltatást újra átveszi, míg a másodkiszolgáló készenlétben vár [32]. A következő ábra az adatbázisok fürtözésének felépítését szemlélteti:

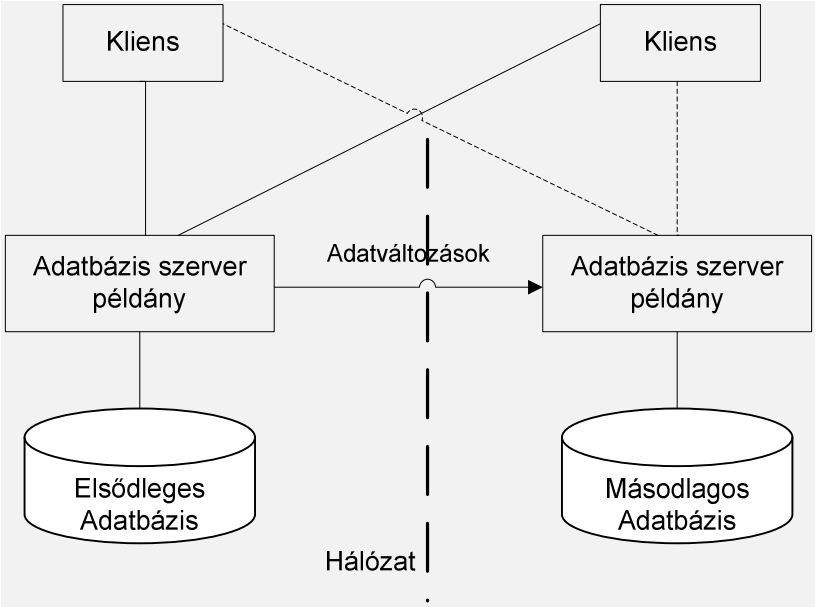


5. ábra: Adatbázis szerverek fürtözése [33]

Adatbázisok tükrözése (database replication) során a fő cél az adatállományok sérülésének kivédése, az adatvesztés elkerülése, például katasztrófák hatására bekövetkezett veszteségek esetén. A rendszer egy éles (elsődleges) és egy vagy több készenléti (másodlagos) adatbázis szerverből - szerverpéldányból és adatbázis állományból - áll, amik földrajzilag eltérő helyeken lehetnek, egymás közötti kommunikációjuk hálózati összeköttetés útján biztosított. A készenléti adatbázisokat kezdetben az elsődleges adatbázis-biztonsági másolatából hozzák létre. A már létrehozott készenléti adatbázist a tükrözés automatikusan és folyamatosan szinkronban tartja az elsődleges adatbázissal, biztosítva, hogy tranzakció szinten az elsődleges adatbázis teljes mértékben konzisztens másolata maradjon. Ehhez az elsődleges adatbázis tranzakciós ismétlési adatait (az adatbázison elvégzett, még nem véglegesített műveleteket, Oracle rendszerben redo logokat) folyamatosan továbbítja a tartalék rendszernek, amely ezeket az ismétlési naplókat alkalmazza a készenléti adatbázis adataira.

Egyes tükrözési megvalósításokban van egy szemtanú szerver, mely figyeli, hogy az elsődleges adatbázis rendelkezésre áll-e. Amennyiben nem érhető el az elsődleges adatbázis, illetve adatbázis szerverpéldány a szemtanú automatikusan kezdeményezi a tüköradatbázis kinevezését elsődleges adatbázissá, az elsődleges adatbázist pedig átkapcsolja készenléti üzemmódba Az adatbázis-tükrözés szemtanú nélküli kiépítése esetén nincs automatikus átállás, azaz hiba esetén manuálisan kell ezt végrehajtani. Az adatbázis-tükrözéshez kliensoldali támogatás is tartozhat, az ügyfelek kapcsolati beállításai között megadhatjuk a

tükörszerver nevét. Az elsődleges szerverrel való kapcsolat lezárását vagy elvesztését követően az újrakapcsolódás során az ügyfélalkalmazás az általunk megadott tükörszerverre kapcsolódik, amennyiben nem érhető el az elsődleges szerver [34], [35], [36]. A következő ábra az adatbázisok tükrözésének felépítését szemlélteti:



6. ábra: Adatbázis szerverek tükrözése [34]

A tükrözési technikák különböző adatvédelmi üzemmód alapján működhetnek, ugyanis egyes esetekben az adatvesztés elkerülése a fő cél, máskor viszont az adatbázis maximális teljesítménye a követelmény és a kisebb adatvesztések nem lényegesek.

Maximális védelem biztosítása esetén az adatváltozások azonnal továbbítódnak az elsődleges adatbázisból a készenléti adatbázisba, és az elsődleges adatbázisban a tranzakciók mindaddig nem véglegesítődnek (commit), amíg a változás adatai a készenléti adatbázisban rendelkezésre nem állnak. Ha hiba esetén a készenléti adatbázis leáll, az elsődleges adatbázisban is leáll a feldolgozás. Ez a működési mód biztosítja a legmagasabb szintű adatvédelmet.

Maximális rendelkezésre állás biztosítása esetén az adatváltozások azonnal továbbítódnak az elsődleges adatbázisból a készenléti adatbázisba, azonban ha a készenléti adatbázis elérhetetlenné válik (például mert megszakad a hálózati kapcsolat), a feldolgozás az elsődleges adatbázisban tovább folytatódik. A hiba elhárítását követően a készenléti adatbázis automatikusan újra szinkronizálódik az elsődleges adatbázissal.

Maximális teljesítmény biztosítása esetén az elsődleges adatbázis feldolgozza a tranzakciókat, de az adatváltozások aszinkron módon (késleltetve) továbbítódnak a készenléti adatbázishoz. Az elsődleges adatbázis véglegesítési mechanizmusa nem vár addig az írási

műveletek elvégzésével, amíg a készenléti adatbázis visszaigazolja a változási adatok sikeres fogadását. Ha egy készenléti rendszer elérhetetlenné válik, a feldolgozás az elsődleges adatbázisban folytatódik, és az esemény gyakorlatilag nem befolyásolja az elsődleges adatbázis teljesítményét. Ez az üzemmód kevésbé szigorú adatvédelmet biztosít az elsődleges adatbázis számára, de nagyobb a teljesítménye, mint a maximális rendelkezésre állási üzemmódé.

1.3 AZ ADATBÁZIS-BIZTONSÁGOT VESZÉLYEZTETŐ FENYEGETÉSEK ÉS TÁMADÁSOK

Az adatbázisok megfelelő védelmének biztosításához ismernünk kell az adatbázisok biztonságát veszélyeztető fenyegetések különböző formáit. Általános értelemben a fenyegetés olyan potenciálisan káros, vagy meg nem engedett hatás, amely a védendő objektumot károsan, egy megengedett mértéknél jobban befolyásolja. A fenyegetés érintheti a védendő objektum létét, érdekeit, állapotát, működését, vagy valamely tulajdonságát. A fenyegetések bekövetkezését a különböző sebezhetőségek teszik lehetővé. A sebezhetőség a biztonság alanyának egy olyan tulajdonsága, hiányossága, vagy gyengesége, amely lehetőséget teremt egy fenyegetés megvalósulására [23].

Értekezésemben az adatbázisok információs jellegű, a kibertérből érkező fenyegetéseit vizsgálom, nem térek ki a fizikai jellegű támadásokra (pld. kábelek elvágása). A következőkben kategorizálási szempontrendszereket állítok fel az adatbázis fenyegetéseinek osztályozásához, majd a támadási pontok szerint jellegzetes adatbázis fenyegetéseket gyűjtök össze [FR3], [FR4], [FR5] publikációim alapján.

1.3.1 SZEMPONTRENDSZEREK AZ ADATBÁZIS FENYEGETÉSEK OSZTÁLYOZÁSÁHOZ

Az adatbázisok az architektúra legutolsó pontján, tűzfalak védelmével ellátva helyezkednek el, ezért sokáig ezek védelme az informatika biztonsági feladatok között nem szerepelt prioritásként. Mára a helyzet megváltozott. Egyrészt a webes alkalmazások elterjedtével támadásuk könnyebbé vált, a behatolók ellen kevésbé vannak elrejtve, másrészt integritásuk megsértése bizonyos esetekben helyreállíthatatlan vagy nagyon problémásan helyreállítható helyzetet teremtene, illetve törvényi előírások is létrejöttek az adatok védelme érdekében. Egyre elterjedtebb igény, szükség jelentkezik vállalati szinten adatbázis-biztonsági terv készítésére az adatvagyon védelme érdekében. A védelem megtervezéséhez fontos ismerni, hogy milyen veszélyek ellen lehetnek az adatbázisokat kitéve.

Adatbázis veszélyek és a Common Criteria

A Common Criteria (rövidítve CC) [37], [38], [39] az informatikai termékek és rendszerek biztonsági értékelésének követelményrendszere, melynek 2.0 változatát nemzetközi szabványként fogadták el ISO-IEC 15408 számon és ezt magyar szabványként (MSZ ISO/IEC 15408:2003) honosították. Az informatikai rendszer CC szerinti biztonsági értékelésekor Védelmi Profilokat (angolul Protection Profile) definiálnak, melyek az értékelendő rendszer - esetünkben az adatbázis-kezelő rendszer – elvárt biztonsági követelményeit írják le termék független módon megfogalmazva. Egy típusfeladatra - például az adatbázis-kezelő rendszer működésére – több védelmi profil is készíthető, melyek szakemberek által elbírált, hitelesített dokumentumok. Értekezésemben fontosnak tartom kiemelni az USA kormányzata által kiadott adatbázis-kezelő rendszerekre vonatkozó védelmi profilt [40], mely a következő CC terminológiájú fenyegetésekkel számol (azaz ezeket célozza meg kivédeni):

- T.ACCIDENTAL_ADMIN_ERROR: Az adatbázis adminisztrátor által nem szándékosan okozott, biztonsági rést okozó telepítési vagy konfigurációs hiba.
- T.MASQUERADE: Felhasználó vagy processz egy másik felhasználó személyazonosságának álcázásával jogosulatlan hozzáférést szerez az adatokhoz vagy az adatbázis-kezelő rendszerhez.
- T.POOR_DESIGN: Az adatbázis-kezelő rendszer követelmény specifikációjában vagy tervében lévő véletlen hiba, mely által okozott hiányosságot kártékony program vagy felhasználó kiaknázhat.
- T.POOR_IMPLEMENTATION: Az adatbázis-kezelő rendszer tervének implementációja folyamán okozott véletlen hiba, mely által okozott hiányosságot kártékony program vagy felhasználó kiaknázhat.
- T.POOR_TEST: Az adatbázis-kezelő rendszer biztonsági funkcióinak helyes működését bizonyító tesztelést elégtelenül vagy egyáltalán nem végezték el. Ennek következtében kialakult helytelen működés felfedezése biztonsági sérülékenységet jelenthet.
- T.RESIDUAL_DATA: Felhasználó vagy processz jogosulatlan hozzáférést szerezhet adatokhoz adatbázis erőforrások egyik felhasználótól a másikhoz történő átrendelésével.
- T.TSF_COMPROMISE: Rosszhiszemű felhasználó vagy processz konfigurációs adatok jogosulatlan hozásférését érheti el.
- T.UNAUTHORIZED_ACCESS: Felhasználó, az adatbázis rendszer biztonsági politikája által nem biztosított, jogosulatlan hozásférést eszközölhet ki felhasználói adatokhoz.

- T.UNIDENTIFIED_ACTIONS: Felhatalmazott adminisztrátor jogosulatlan hozzáféréseket hibásan azonosít vagy kezel.

A dokumentum a lehetséges fenyegetéseket a következő feltételezések mellett tárgyalja:

- A.NO_EVIL: Az adminisztrátorok nem ellenségesek, megfelelően képzettek és követik az adminisztrátori útmutatót.
- A.NO_GENERAL_PURPOSE: Az adatbázis-kezelő rendszer működéséhez, adminisztrálásához és támogatásához szükséges szolgáltatásokon kívül más, általános célú program nem fut az adatbázis-kezelő rendszer gépén.
- A.PHYSICAL: A megfelelő fizikai biztonság biztosított az adatbázis-kezelő rendszer által érintett IT vagyontárgyaknak és a tárolt, feldolgozott és továbbított adatoknak.

Adatbázis fenyegetések rendszerezési szempontjai

A következőkben értekezésemben bemutatom az adatbázis fenyegetések különféle rendszerezéseit. A célom olyan rendszerezési kategóriák felállítása, melyek segítségével számba vehetők, áttekinthetők az adatbázis fenyegetések. Olyan kategorizálási szempontokat kerestem, melyek egyértelmű besorolást tesznek lehetővé.

Osztályozni lehet a fenyegetéseket a támadó adatbázishoz való viszonya szerint. Adatbázis fenyegetések esetén vizsgálható, hogy külső vagy belső támadás zajlott-e le. Komoly felmérések, tanulmányok készültek annak kimutatására, hogy ezek közül melyik a gyakoribb probléma egy szervezet esetében. Több tanulmány egész magas százalékot hoz ki a belső fenyegetések javára. A belső-külső kategóriák jelentésének meghatározása nem is olyan egyszerű, mint első ránézésre hinnénk. Belső támadásnak definiálom az adatbázist üzemeltető személyek által elkövetett támadást, melyben a támadó a számára megadott jogosultsággal él vissza, azokat nem rendeltetésszerűen használja.

Kategorizálni lehet egy támadást az elkövető indíttatása szerint, azaz a kivitelezője elkövetheti ezt szándékosan vagy véletlen folytán.

A támadásokat kategorizálni lehet aszerint, hogy mely biztonsági tulajdonság sérülését okozhatja. Azaz a bizalmasság, a sértetlenség vagy a rendelkezésre állás biztonságát veszélyezteti-e. A sértetlenség és rendelkezésre állás esetén megvizsgálható, hogy az adatokon történt meg a negatív kölcsönhatás vagy pedig az adatbázis-kezelő rendszert érintette. Például a rendelkezésre állás megsértése esetén az adatok megsemmisítése miatt vagy pedig az adatbázis-kezelő rendszer megváltoztatása miatt vált az adatbázis

elérhetetlenné. A sértetlenség megsértésekor szintén megvizsgálható, hogy az adatokon vagy az informatikai rendszerben történt meg az illetéktelen módosítás. Egy fenyegetés több biztonsági tulajdonság megsértését kiválthatja, így egyszerre több kategóriához is hozzárendelhető.

Végül az adatbázis fenyegetések vizsgálhatóak a lehetséges támadás architektúrában elfoglalt helye szerint is. Fontos, hogy csak az adatbázisban tárolt adatokat vagy az adatbázis-kezelő rendszer működését veszélyeztető fenyegetések rendszerezése a feladat.

Az adatbázis-biztonság helyzetét mérő kockázat elemzések egyik célja annak azonosítása, hogy a szervezet adatvagyonát hol veszélyeztetik a támadások leginkább. Ebből a nézőpontból tekintve ennek a csoportosításnak a jelentősége nagy. Az adatbázisokat veszélyeztető fenyegetések az architektúra négy pontjáról indulhatnak. Ennek alapján megkülönböztethetőek a hálózat, az alkalmazások, a platform és az adatbázisok sérülékenységeire építő fenyegetések.

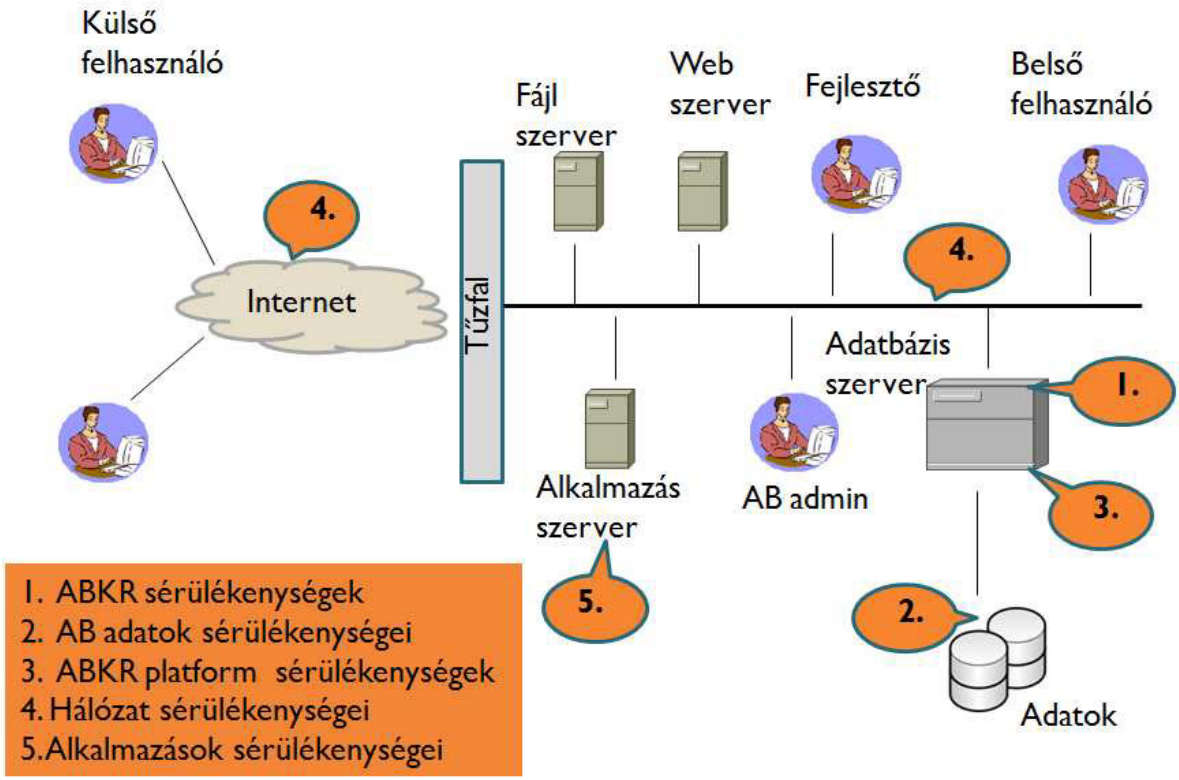
Hálózati fenyegetésének tekintem azokat a lehetséges támadási módokat, melyek az adatbázis szerverek, illetve adatbázis állományokat tartalmazó háttértárak közötti kommunikáció támadására alapulnak, vagy pedig a hálózat tetszőleges pontján lépnek fel és az adatbázisok rendelkezésre állását vagy sértetlenségét támadják meg. Az adatok bizalmasságának hálózati úton való támadása már nem tartozik a rendszerezésem tárgyába.

Az alkalmazásokban rejlő sebezhetőségek, programozási hiányosságok az adatbázis fenyegetések egy fontos csoportját jelentik, ebbe a kategóriába eső támadások különös tekintettel a webes alkalmazások használatának elterjedésével váltak gyakorivá.

A platform fenyegetései alatt a hálózatba kötött adatbázis szerverek és felhasználói számítógépek hardver és szoftver komponenseinek sebezhetőségeit értem. Mivel csak az információs úton történő támadásokat vizsgálom, az operációs rendszer és egyéb rendszerprogramok hibáit kihasználó fenyegetések tartoznak ebbe a kategóriába, különös tekintettel az adatbázis szervereket futtató platformok sebezhetőségeire.

Az adatbázisok felőli támadási pont az adatbázis-kezelő rendszerben, illetve a tárolt adatokban rejlő sérülékenységeket kihasználó fenyegetések induló pontja.

Az adatbázisokat tartalmazó informatikai rendszert és a támadások architektúrában elfoglalt helyeit szemlélteti az alábbi ábra:



7. ábra: Informatikai rendszer és az adatbázis sérülékenységek [készítette a szerző]

1.3.2 JELLEGZETES ADATBÁZIS FENYEGETÉSEK A TÁMADÁS PONTJA SZERINT

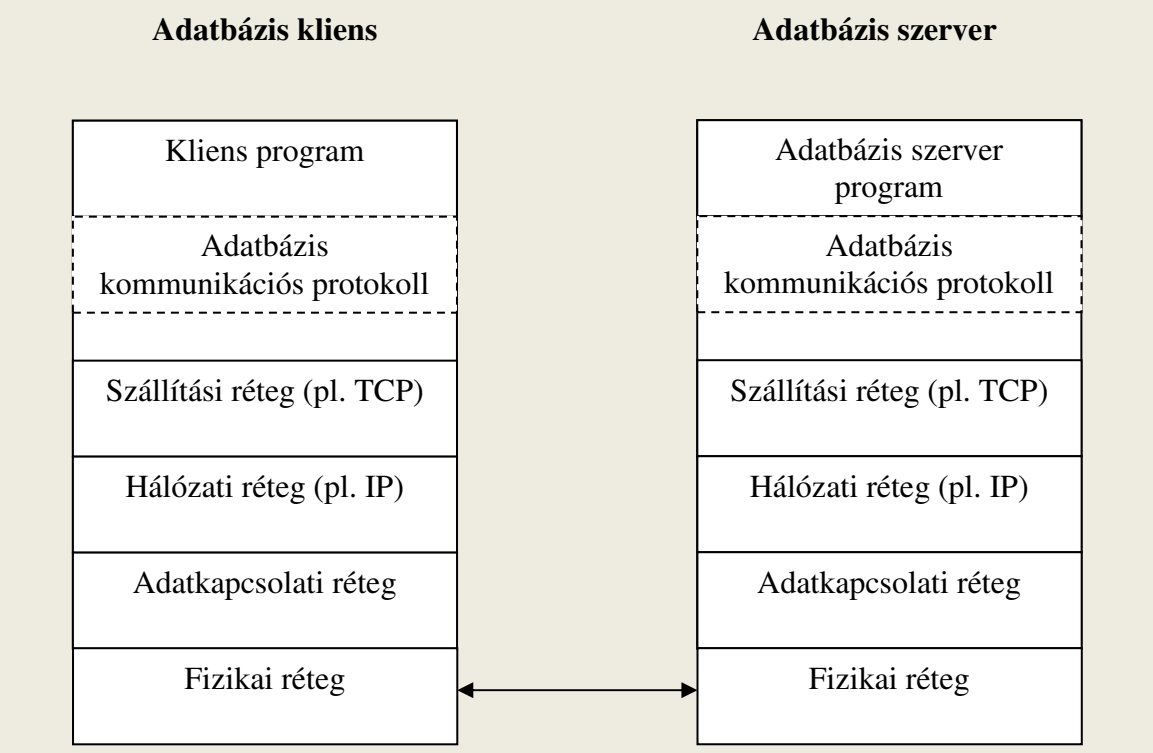
Hálózati infrastruktúra sebezhetőségei

A hálózati fenyegetések kategóriájába tartoznak az OSI modell szerinti hálózati-szállítási réteg lehetséges támadásai, illetve az adatbázis-kezelő rendszer hálózati protokolljának támadásai. A támadások technikái épülhetnek a hálózati adatforgalom lehallgatására, beékelődéses (man in the middle) támadási módszerre (melyet például a forráscím meghamisításával lehet megvalósítani), szolgáltatás megtagadása típusú támadásra (például a SYN csomagok elárasztásának módszerével), de akár a puffer túlcsordulásos hiba kihasználására is.

A hálózati adatforgalom lehallgatásának veszélye megjelenik az adatbázisok magas rendelkezésre állásának megvalósításánál (adatbázis tükrözés, fürtözés), ahol adatbázis szerverek kapcsolódnak hálózaton keresztül. Az adatbázis szerverek közötti adatforgalom titkosítás nélkül (vagy gyenge titkosítással) áramlása esetén az adatok lehallgathatóak, ezzel pedig adatbázisok tartalma kerülhet illetéktelenül támadók birtokába.

Pár évvel ezelőtt az adatbázis szerverek elleni új támadási vektor jelent meg, méghozzá az adatbázisok kommunikációs protokolljában rejlő sebezhetőségekre építve [41]. A támadás

mindhárom biztonsági tulajdonság megsértését okozhatja. Az adatbázisok kommunikációs (vagy más néven hálózati) protokolljai az OSI modellben a hálózati-szállítási réteg és az alkalmazás réteg között helyezkednek el az alábbi ábra szerint:



8. ábra: Az adatbázis kommunikációs protokoll elhelyezkedése [készítette a szerző]

Az SQL adatbázis lekérdező nyelv a kliens-szerver kommunikációhoz szükséges folyamatokat nem definiálja, ezeket az adatbázis-kezelő rendszer hálózati protokollja látja el. Például a kliens kapcsolat (client session) létrehozása, a parancsok (autentikáció, lekérdezés, kontroll információ) klienstől szerverhez való eljuttatása, az adatok és a lekérdezés státuszának klienshez való eljuttatása az adatbázis hálózati szoftverének a feladata.

Az adatbázisok hálózati szoftvereit (nem szükségszerűen, de a gyakorlat alapján) az adatbázis-kezelő rendszerek gyártói fejlesztik (például Oracle esetében Oracle Net-nek hívják), kódjaik általában nem nyilvánosak és számos sebezhetőséget hordoznak magukban. Bejelentett kommunikációs protokoll sebezhetőségek alapultak az üzenet struktúrájának elrontására, mező méret megváltoztatására, mező tartalmának manipulálására, illetve az üzenet sorszámának meghamisítására.

A támadás kivitelezéséhez a támadónak vagy egy saját programot kell írnia, amivel a manipulált üzeneteit elküldi a szervernek és feldolgozza a kapott választ addig a pontig, amíg a káros hatás bekövetkezik vagy pedig egy TCP proxy segítségével be kell ékelődnie a kliens

és a szerver közé, és ebben a pozícióban az elkapott üzeneteket megfelelően módosítva kell továbbítania. TCP proxy a kliens-szerver kommunikációba ékelődik be, a TCP csomagokat megjeleníti, változtatás nélkül továbbítja, illetve szükség esetén módosítva küldi tovább.

Alkalmazások sebezhetőségei

Az alkalmazásokban rejlő sebezhetőségek, programozási hiányosságok az adatbázis támadások egy fontos csoportját jelentik, melyek mögött elsősorban a felhasználói inputok ellenőrzésének hiánya áll. Sérülékenységet jelent még a hibaüzenetek nem megfelelő kezelése, az adatbázis elérések nem megfelelő megvalósítása és a naplózás hiánya is.

A felhasználói inputok ellenőrzésének hiánya puffer túlcsordulásos, SQL injekciós, illetve XSS (cross-site scripting) támadásra adhat lehetőséget. Mindhárom támadási módszerrel kiváltható a rendelkezésre állás, a sértetlenség illetve a bizalmasság megsértése.

Alkalmazások a felhasználók számára megjelenített hibaüzeneteikben adatbázisra, illetve az adatbázis szerverre jellemző információkat fedhetnek fel, ami támadások felépítéséhez ad segítséget, ezáltal sérülékenységi pontot jelent.

Egy adott alkalmazás az adatbázis szervert mindig egy (esetleg több) adatbázis felhasználó nevében éri el. Ha az alkalmazás tulajdonosként vagy superuserként csatlakozik az adatbázishoz, sérülékenységet jelent, mivel bármilyen utasítást és lekérdezést lefuttathat, pl. a szerkezeti módosítást (táblák megszüntetése) vagy táblák komplett törlése. Mindig a lehető legkevesebb jogosultsággal rendelkező, az alkalmazás számára önálló és testreszabott felhasználókat kell használni. Ekkor, ha a behatoló meg is szerez valamilyen jogosultságot (hitelesítési információt), akkor is csak akkora változást tud okozni, mint az alkalmazás maga.

Az alkalmazás szintjén történő adatbázis lekérdezések, hozzáférések naplózásának hiánya szintén sérülékenységet okozhat a rendszerben, hisz az adatbázis szerver naplóiban az alkalmazás számára az adatbázis elérésre létrehozott felhasználók jelennek csak meg (általában ezek száma a tényleges felhasználók számának töredéke). Nyilvánvalóan a naplózás nem tud megakadályozni egyetlen ártalmas próbálkozást sem, de segítséget nyújthat annak felderítésében, hogy melyik alkalmazás és ki által lett kijátszva.

A puffer túlcsordulásnál a program egy fix hosszúságú tömböt (puffert) foglal le a memóriában, majd a tömb írásakor nem ellenőrzi annak határait. A támadó a lefoglalt tömböt túlírva (túl hosszú bemenet segítségével) felülírhat a program működése szempontjából lényeges memóriarészeket, így kártékony kódokat futtathat le. Puffer túlcsordulást kiváltó

sérülékenység felléphet az alkalmazás szintjén például az SQL kérések túlméretezésével, vagy a dinamikus SQL lekérdezés számára túlméretezett input megadásával [42].

Az adatbázisokat érintő fenyegetések közül az SQL injekciós technika mindenképp az egyik vezető helyet foglalja el. A támadásnál az alkalmazás által előállítandó, tervezett tartalmú, dinamikusan szerkesztett SQL utasításba illesztenek káros tevékenységeket megvalósító kódot. Az alkalmazás a felhasználótól bekért paraméterek segítségével állítja elő az SQL szerverhez eljuttatandó lekérdezést. A támadó a paraméter értékének olyan kártékony karaktersorozatot ad meg, ami megváltoztatja az eredeti lekérdezés szintaktikáját, ezáltal az egészen más feladatot valósít meg, mint az eredeti elképzelés [FR3].

XSS támadás jelenti napjainkban a webes alkalmazások leggyakoribb megsértését. A támadó a felhasználó böngészőjében futtathat le tetszőleges kódot (például javaszkriptet), miközben a felhasználó egy megbízható webhelyhez kapcsolódik. Igazából a felhasználót sebzi meg a támadás, a web alkalmazás, mint közvetítő közeg segítségével. A támadó munkafolyamat (session) azonosítókat tud a felhasználó gépéről megszerezni, ezáltal a felhasználó nevében be tud lépni az alkalmazáson keresztül az adatbázis rendszerbe. A session azonosítók megszerzésére építő támadást munkamenet-eltérítésnek (session hijacking) nevezik. Az XSS támadás különösen veszélyes az adatbázis rétegre nézve, ha a támadáshoz használt web alkalmazás a felhasználó által megadott adatokat az adatbázis rétegen belül tárolja, ekkor a támadó az adatbázisba tud illetéktelenül beleírni [43].

Platformok sebezhetőségei

A platformok fenyegetéseihez hozzájárulnak a hálózatba kötött szerver és felhasználói számítógépek szoftver komponenseinek sebezhetőségei. Az adatbázisok biztonságára nézve az adatbázis-kezelő rendszert futtató számítógép operációs rendszerének és az itt található állományoknak a nem megfelelő védelme biztonsági rést jelent.

A Blaster féreg például a Windows XP, Windows 2000 operációs rendszerek puffer túlcsordulásra épülő sérülékenységét használta ki, amivel megfertőzött gépeket, köztük adatbázis szervereket is elérhetetlenné tett [44].

Az adatbázis-kezelő rendszer gépén lévő állományok megfelelő védelméről is gondoskodni kell. Titkosítatlanul tárolt adatbázis mentések és futtatható állományok jogosulatlan hozzáférése is biztonsági rést jelent.

Gyakori példa, hogy felhasználók adatbázis-kezelő rendszerbe való belépésekor lefut egy login szkript, mely a rendszer szükséges beállításait elvégzi. Ha ezt a login fájlt illetéktelenek

elérik és módosítani tudják, akkor teljes hozzáférést szerezhetnek az adatbázishoz, amit az alábbi példa szemléltet:

```
------------------login.sql----------------------------
set term off
create user hacker identified by hacker;
grant dba to hacker;
set term on
------------------login.sql----------------------------
```

Adatbázisok sebezhetőségei

Az adatbázis-kezelő rendszer szoftverei és a tárolt adatok is hordozhatnak sérülékenységeket. A biztonságos működéshez elsődleges feladat az adatbázis-kezelő rendszer biztonságos telepítése, megerősítése és folyamatos felügyelete, ezt angolul „database hardening”-nek nevezik. Az adatbázis-kezelő rendszerek telepítésekor gyakran, automatikus módon, ismert nevű felhasználók jönnek létre, mely a támadás számára egy jó kiindulási pont. Ugyanis a felhasználónév birtokában a támadónak „csak” a jelszót kell kitalálnia (ami gyakorta nem erős, azaz könnyen megfejthető). A telepítéskor automatikusan létrejövő táblák, tárolt eljárások is sérülékenységi pontot jelenthetnek. Célszerű ezeket törölni, és szükség esetén más névvel magunknak létrehozni.

A szerverekre vagy anonim kapcsolattal vagy autentikáció után lehet kapcsolódni. A támadó a hitelesítési mechanizmus és információk lehallgatásával, megszerzésével illetéktelenül tud az adatbázis szerverre bejutni.

Gyenge konfigurációs paraméterek használata, szoftver hibák, az adatbázis tárolt eljárásaiban található puffer túlcsordulásra, illetve SQL injekcióra épülő sérülékenységek, felhasználói hibák, elavult verziójú programok használata és biztonsági frissítések feltöltésének hiánya kártékony kód lefuttatását, vírusok, trójaiak és férgek rendszerbe való bejutását eredményezheti, illetve szolgáltatás megtagadása típusú támadásra ad lehetőséget. Például az SQL Slammer féreg a Microsoft SQL szerverének puffer túlcsordulásra épülő sérülékenységét használta ki és okozott az adatbázis-kezelő rendszer biztonságában rendelkezésre állás megsértést. A kártékony kód olyan rendszereket tudott megfertőzni, melyek a már bejelentett sérülékenységet javító biztonsági frissítést nem alkalmazták [45].

1.4 KÖVETKEZTETÉSEK

A fejezetben megvizsgáltam az adatbázis-biztonság fogalmát, helyét és szerepét jártam körül. Munk Sándor biztonság alapmodellje szerint az adatbázis-biztonság fogalmának elemzésekor meghatároztam a biztonság alanyát, ennek védendő tulajdonságait. Kutatásomban az adatbázis-biztonság alanyának mind az adatbázisban tárolt adatokat, mind az azokat kezelő adatbázis-kezelő rendszereket tekintem. A védendő tulajdonságok közé elsődlegesen a bizalmasságot, sértetlenséget és rendelkezésre állást sorolom, de az auditálhatóság és hitelesség biztonsági tulajdonságokat is létjogosultnak tekintem az adatbázis-biztonság védendő tulajdonságai között.

A fejezetben elvégzett vizsgálatok alapján megállapítottam, hogy az adatbázis-biztonság az informatikai biztonság egyik fontos részterülete, ugyanakkor azt csak az informatikai rendszer többi elemével egységben, komplex módon lehet megvalósítani.

Napjainkban az egyre erősebb védelmi módszerek átjátszása egyre kifinomultabb és felkészültebb technikákat igényel, ugyanakkor az informatikai rendszerek - többek között adatbázisok – támadására kifejlesztett programkódok (exploitok) felkerülnek az internetre, ezek rosszindulatú használatához már nem kell olyan tudás, mint a támadó programok kifejlesztéséhez, a biztonsági rések megtalálásához. Ez is hozzájárul a sikeres támadások számának folyamatos emelkedéséhez. Az adatbázis fenyegetéseket a különböző publikációk, biztonsági dokumentumok jellemzően felsorolásszerűen tárgyalják, rendszerezési szempontokat nem érintenek. A fejezetben elvégeztem az információs jellegű adatbázis fenyegetések rendszerezését, ehhez többféle szempontrendszert is megadtam. Az informatikai rendszerek védelme és az adatbázis-biztonság megvalósítása szempontjából legfontosabbnak a támadási pont szerinti rendszerezést tartom

Az adatbázis fenyegetéseket a támadási pont (azaz a támadás által kihasznált sérülékenység architektúrában elfoglalt helye) szerint rendszerezve megkülönböztettem az adatbázis-kezelő rendszernek, az adatbázisokban tárolt adatoknak, az adatbázis-kezelő rendszer platformjának, a hálózatnak és az alkalmazásoknak a sérülékenységeire épülő támadásokat, és ezek alapján gyűjtöttem össze adatbázis fenyegetéseket.

A különböző támadási pontokat, az ezekhez tartozó fenyegetés típusokat és példákat a következő táblázatban rendszereztem[1]:

[1] ABKR: adatbázis-kezelő rendszer, AB: adatbázis

Támadási pont		Fenyegetés és sérülékenység típusok	Példák
Adatbázis rendszer	ABKR	ABKR program hibája	DoS támadás, Puffer túlcsordulás, SQL injekció
		Rossz konfigurációs paraméterek használata	
		Hitelesítés sérülékenysége	Szótár támadás, Brute force, Social engineering
		Rossz Működtetés	Patchek telepítésének hiánya, Túlzott privilégium kiosztás, Gyenge hitelesítés, Mentések rossz kezelése, Gyenge AB audit, Éles és teszt környezetek szétválasztásának hiánya
		AB kommunikációs protokolljának hibája	Puffer túlcsordulás, Beékelődéses támadás
	Tárolt adatok	Tárolt eljárások hibája	SQL injekció, Puffer túlcsordulás
		Objektum hozzáférések rossz beállítása	
Platform (operációs rendszer és egyéb szolgáltatások)		Program hiba	DoS támadás
		Jogosulatlan hozzáférés elérése	
		Állományok hiányos védelme	
Alkalmazások		Input ellenőrzés hiánya	SQL injekció, Puffer túlcsordulás, Cross site scripting
		Helytelen adatbázis csatlakozás	
Hálózat		Üzenetek lehallgatása, módosítása	Beékelődéses támadás
		Szolgáltatás ellehetetlenítése	DoS támadás

1. táblázat: Az adatbázis fenyegetések rendszerezése [készítette a szerző]

2 AZ ADATBÁZIS-BIZTONSÁG ÉS SZEREPE A KRITIKUS INFRASTRUKTÚRA VÉDELEMBEN

BEVEZETÉS

A kritikus infrastruktúrák működése napjainkban az informatika eszközeinek, rendszereinek, alkalmazásainak támogatását erőteljesen igénybe veszi. Ez az informatikai támogatás részben önálló információs infrastruktúrák révén, részben önmagukban kritikus infrastruktúrát nem alkotó támogató összetevők révén jelenik meg. A támogató informatikai rendszerek jelentős részének működésében lényeges, esetenként kiemelt szerepet játszanak az adatbázisok is.

A banki szolgáltatásokra, egyes hálózatokra épülő szolgáltatásokra (energia-ellátás, közlekedés), vagy egyes közhiteles nyilvántartásokra gondolva megfogalmazható, hogy az adatbázisok számos kritikus infrastruktúrában (ha nem valamennyiben) megtalálhatóak és sok esetben biztonságuk megsértése (működésképtelenné tételük, meghamisításuk, adataik jogtalan megismerése) az adott kritikus infrastruktúra biztonságát fenyegeti.

A kritikus infrastruktúrák és a mögöttük álló adatbázisok védelmének feladatrendszerében meghatározó a kritikus infrastruktúrák és adatbázisok azonosítása és priorálása. A fejezet célja az adatbázisok előfordulásának, helyének, szerepének és azonosítási lehetőségeinek elemzése, rendszerezése és értékelése a különböző kritikus infrastruktúra szektorokban. A felvázolt kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Összegeztem az infrastruktúrák, kritikus infrastruktúrák és kritikus információs infrastruktúrák fogalmi kérdéseit; feltártam az infrastruktúrák támadási módszereit és védelmi lehetőségeit; majd elemeztem a kritikus infrastruktúrák azonosításának kérdéseit.
- Feltártam, rendszereztem és általánosságban értékeltem az adatbázisok előfordulását, helyét és szerepét a különböző kritikus infrastruktúra szektorokban.
- Elemeztem a kritikus adatbázisok azonosításának lehetőségeit; bevezettem a kritikus adatbázis fogalmát.

2.1 A KRITIKUS INFRASTRUKTÚRÁK BIZTONSÁGÁNAK ALAPJAI

A XX. század végén, a nemzeti infrastruktúra sebezhetőségének értelmezésében új dimenziók jelentek meg. A kritikus infrastruktúrák és a kritikus információs infrastruktúrák védelmének kérdése a világ számos országában, így Magyarországon is a figyelem

központjába került, kiváltképp a 2001. szeptember 11-én az USA elleni támadás, valamint a 2004-es madridi és 2005-ös londoni metrórobbantások után.

2005 novemberében az Európai Bizottság kiadta az úgynevezett Zöld Könyvet [46] a kritikus infrastruktúrák védelmére vonatkozó európai programról (angolul European Programme for Critical Infrastructure Protection, EPCIP*)*, melynek célja többek közt az Unió kritikus infrastruktúráinak folyamatos működtetésének biztosítása és ebben, az iparágak és tagállamok kormányainak támogatása.

2008-ban az Európai Unió Tanácsa kiadta, az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló a 2008/114/EK irányelvet [47]. Az irányelv eljárási rendet állapít meg az európai kritikus infrastruktúrák (ECI) azonosítására és kijelölésére. Az irányelv két szektorban - energia és közlekedés -, illetve ezek alszektoraiban írja elő a tagországok számára az azonosításra vonatkozó feladatokat. Az irányelvben meghatározott 2011. január 12-i nemzeti jelentéstételi kötelezettségi határidő tekintetében is a fenti két szektor vizsgálata szükséges. Az irányelv tartalmazza, hogy a hatálybalépéstől számított 3 év múlva felül kell vizsgálni más ágazatok bevonásának szükségességét, amiben az IKT (infokommunikációs technológia) szektornak prioritást kell élveznie.

Az Európai Bizottság 2009-ben kiadott a kritikus információs infrastruktúrák védelmével kapcsolatos közleményt (COM(2009) 149) [48], melynek címe „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”. A dokumentum tartalmaz egy cselekvési tervet, mely a következő 5 pillérből áll: felkészülés és megelőzés, észlelés és válasz, kárenyhítés és helyreállítás, nemzetközi együttműködés, valamint a kritériumok az Európai Kritikus Infrastruktúráknak az ICT (Information and Communications Technology - Információs és Telekommunikációs Technológia) területén. A pillérek kidolgozandó feladatokat jelölnek ki a tagállamok számára.

A COM(2009) 149 akcióterv által elért eredményeket a Bizottság 2011. márciusában kiadott, a Kritikus Információs Infrastruktúra Védelemről szóló COM(2011) 163 [49] közleménye tartalmazza. A dokumentum kifejti a tagországok számára az elkövetkező években váró feladatokat. A kihívások nemzetközi kiterjedtségére helyezi a hangsúlyt, valamint felhívja a figyelmet a tagállamok és a privát szektor együttműködésének fontosságára.

Magyarországon 2008-ban jelent meg a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló kormányhatározat és Zöld könyv [50]. A dokumentum tartalmazza a kritikus infrastruktúrákkal kapcsolatos fogalmak meghatározását és a szektorok kijelölését.

Hazánkban 2010-ben a 2008/114/EK tanácsi irányelvnek való megfelelés érdekében született meg a 1249/2010. számú Kormányhatározat [51], mely felelősöket és határidőket rendel az irányelv által megszabott feladatokhoz. Például a belügyminiszter hatáskörébe utalja a nemzeti kapcsolattartó pont feladatait, az európai kritikus infrastruktúrák védelmével kapcsolatos kérdések koordinálását; az azonosítás és kijelölés folyamataihoz szükséges két- vagy többoldalú egyeztetések lebonyolítását; valamint további érintett miniszterek bevonásával egy kritikus infrastruktúra védelmi tárcaközi szakmai munkacsoport felállítását. A nemzeti fejlesztési miniszter feladataként nevesíti a Magyarországon található európai kritikus infrastruktúrák kijelölését és egy konzultációs fórum létrehozását. A tárcaközi szakmai munkacsoport feladata az európai és nemzeti kritikus infrastruktúrák azonosításához szükséges kritériumrendszer kidolgozása.

2011. évi katasztrófavédelemről szóló törvény [52] kimondja, hogy a katasztrófák elleni védekezésért felelős miniszter felelős a kritikus infrastruktúrák védelméért a katasztrófák elleni védekezés területén. A törvény értelmében felhatalmazást kap a kormány, hogy rendeletben állapítsa meg a közlekedés és energia szektorok tekintetében az európai és nemzeti kritikus infrastruktúrák kritériumrendszerét és kijelölésének folyamatát.

A jogszabályi háttér felvázolása után következőkben áttekintem az infrastruktúrák, kritikus infrastruktúrák és kritikus információs infrastruktúrák fogalmi kérdéseit, majd elemzem az infrastruktúrák támadási módszereit, védelmi lehetőségeit és azonosításuknak kérdéseit.

2.1.1 INFRASTRUKTÚRÁK

Fogalom meghatározás

Az infrastruktúra fogalma viszonylag egységesen értelmezett, egy meghatározás szerint az infrastruktúra "*egy adott rendszer (termelő-, elosztó- vagy szolgáltatórendszer, tudományos, állami, magán-, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézmények, felszerelések és berendezések, továbbá a működtetést ellátó személyzet szabályszerűen működő összessége*" [53].

Infrastruktúrák osztályozása

Az infrastruktúrákat az információs társadalom szempontjából vizsgálva rendeltetésük szerint a következő megkülönböztetéseket tehetjük meg [54], [55]:

1. Általános feladatú infrastruktúra
2. Információs rendeltetésű infrastruktúra
    a. Funkcionális (alap) infrastruktúra
    b. Támogató információs infrastruktúra

Az általános feladatú infrastruktúra fogalma alatt olyan állandóhelyű vagy mobil építmények, eszközök, rendszerek, hálózatok, az általuk nyújtott szolgáltatások, és működési feltételek összességét kell érteni, amelyek valamilyen társadalmi, gazdasági vagy akár katonai funkciók és rendszerek feladatorientált, zavartalan és hatékony működését teszik lehetővé.

Az információs rendeltetésű infrastruktúrák vagy más névvel információs infrastruktúrák olyan állandóhelyű vagy mobil létesítményeket, eszközöket, rendszereket, hálózatokat, illetve az általuk nyújtott szolgáltatásokat jelentik, melyek az információs társadalom működéséhez szükséges információk megszerzését, előállítását, tárolását, szállítását és felhasználását teszik lehetővé. Az információs infrastruktúrákat feladatkörük alapján csoportosíthatjuk a következőképpen:

A funkcionális információs infrastruktúrák feladatorientált szolgáltatást végeznek. A társadalom valamilyen információs funkciójának zavartalan működését biztosítják, vagyis információs alapszolgáltatásokat végezzenek. Az információs társadalom információs infrastruktúráin belül ezek az elsődlegesek. Biztosítják az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását. A funkcionális információs infrastruktúrák rendszerint nagykiterjedésű, bonyolult szervezésű hálózatok vagy rendszerek formájában működnek.

A támogató információs infrastruktúrák rendeltetése, hogy létrehozzák, és folyamatosan biztosítsák az alapvető információs szolgáltatásokat végző funkcionális információs infrastruktúrák zavartalan működését.

2.1.2 KRITIKUS INFRASTRUKTÚRÁK

Fogalom meghatározás

A kritikus infrastruktúra fogalmát különböző szerzők hasonló definíció meghatározásával tárgyalják. Muha Lajos doktori értekezésében [56] a következőképpen definiálta a fogalmat:

„A kritikus infrastruktúra alkotói azon létesítmények, szolgáltatások és információs rendszerek, melyek olyan fontosak a nemzet biztonsága szempontjából, hogy megzavarásuk, vagy megsemmisítésük országos és/vagy nemzetközi jelentőségű káros hatással jár a biztonságra, a gazdaságra, a közegészségügyre és közrendre, valamint a közigazgatás minden szintjének hatékony és akadálymentes működésére, és a társadalom egészére”.

A 2080/2008-as magyar kormányhatározatban a következő meghatározás szerepel: *„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.”*

Kritikus infrastruktúrák feltérképezése

Alapvető fontosságú, hogy feltárjuk, és pontosan behatároljuk a kritikus infrastruktúrákat, mivel ezek különféle - többek között az információs térből érkező - támadásoknak potenciális célpontjai lehetnek. A kritikus infrastruktúrák elemei minden országban mások lehetnek adottságaik folytán. A kritikus infrastruktúrák mögött legtöbbször komplex informatikai rendszerek állnak. Több szervezet is meghatározta a kritikus infrastruktúrák ágazatonkénti osztályozását. Ezek a csoportosításuk jellegüket tekintve hasonlóak, de tartalmaznak különbségeket az osztályok számát és elnevezését illetően is. A 2080/2008-as magyar kormányhatározat 10 ágazatot (szektort) és ebben a 43 alágazatot állapít meg a következők szerint:

Ágazat	Alágazat
I. Energia	1. kőolaj kitermelés, finomítás, tárolás és elosztás
	2. földgáztermelés, tárolás, szállítás és rendszerirányítás, elosztás
	3. villamosenergia-termelés, átvitel és rendszerirányítás, elosztás
II. Infokommunikációs technológiák	4. információs rendszerek és hálózatok
	5. eszköz-, automatikai és ellenőrzési rendszerek
	6. internet, infrastruktúra és hozzáférés
	7. vezetékes és mobil távközlési szolgáltatások
	8. rádiós távközlés és navigáció
	9. műholdas távközlés és navigáció
	10. műsorszórás
	11. postai szolgáltatások
	12. kormányzati informatikai, elektronikus hálózatok
II. Közlekedés	13. közúti közlekedés
	14. vasúti közlekedés
	15. légi közlekedés
	16. vízi közlekedés
	17. logisztikai központok
IV. Víz	18. ivóvíz szolgáltatás
	19. felszíni és felszín alatti vizek minőségének ellenőrzése
	20. szennyvízelvezetés és -tisztítás
	21. vízbázisok védelme
	22. árvízi védművek, gátak
V. Élelmiszer	23. élelmiszer előállítás
	24. élelmiszer-biztonság
VI. Egészségügy	25. kórházi ellátás
	26. mentésirányítás
	27. egészségügyi tartalékok és vérkészletek
	28. magas biztonsági szintű biológiai laboratóriumok
	29. egészségbiztosítás
VII. Pénzügy	30. fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek
	31. bank és hitelintézeti biztonság
VIII. Ipar	32. vegyi anyagok előállítása, tárolása és feldolgozása
	33. veszélyes anyagok szállítása,
	34. veszélyes hulladékok kezelése és tárolása,
	35. nukleáris anyagok előállítása, tárolása, feldolgozása
	36. nukleáris kutatóberendezések
	37. hadiipari termelés
	38. oltóanyag és gyógyszergyártás
IX. Jogrend - Kormányzat	39. kormányzati létesítmények, eszközök
	40. közigazgatási szolgáltatások
	41. igazságszolgáltatás,
X. Közbiztonság - Védelem	42. honvédelmi létesítmények, eszközök, hálózatok
	43. rendvédelmi szervek infrastruktúrái

Kritikusság mérése

Mivel az infrastruktúrák kritikusságának ismertetői igen sokrétűek és ágazatonként változóak lehetnek, feltérképezésük és azonosításuk meglehetősen bonyolult feladat. Egy konkrét rendszer kritikussá minősítését több szempont együttes vizsgálata után lehet eldönteni, a következő kritériumok [56] figyelembe vételével:

- Hatókör: földrajzi kiterjedésben mutatja a kritikus infrastruktúra megsemmisülésének vagy működésképtelenné válásának hatását. Ez lehet nemzetközi, nemzeti, regionális, territoriális vagy helyi.
- Nagyságrend: a veszteség vagy a megzavarás mértéke (kategóriák: nincs hatás, minimális, mérsékelt és jelentős). A nagyságrend megállapításához a következő szempontokat érdemes átgondolni:
    - Mekkora a népességre gyakorolt hatás (az érintett lakosság száma, áldozatok, betegségek, súlyos sérülések, kitelepítések)
    - Mekkora a gazdasági hatás (GDP-re gyakorolt hatása, jelentős gazdasági veszteség, és/vagy termelés, szolgáltatás fokozatos romlása)
    - Mekkora a környezetvédelmi hatás (a lakosságra és lakókörnyezetére gyakorolt hatás)
    - Mekkora az interdependencia hatása (azaz más kritikus infrastruktúrák működését hogyan befolyásolja a vizsgált megzavarás)
    - Mekkora a politikai hatás (az államba vetett bizalom)
- Időbeli hatás: amely megmutatja, hogy az adott infrastruktúra vagy egyes elemének vesztesége milyen gyorsan, illetve mennyi ideig fejti ki komoly hatását (azonnal, 24—48 óra, egy hét, hosszabb időtartam).

2.1.3 KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK

Napjainkban a különböző infrastruktúrák, eszközök és szolgáltatások túlnyomó többsége az informatikai és kommunikációs rendszereken alapszik. A kritikus infrastruktúrák védelmén belül ezért megjelent egy más megközelítést igénylő feladat, a kritikus információs infrastruktúrák védelme. A 2080/2008-as magyar kormányhatározatban nem szerepel a kritikus információs infrastruktúra fogalma. Az Európai Bizottság kritikus infrastruktúra védelem európai programjáról szóló Zöld könyve [46] szerint a kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is

kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.). A kritikus információs infrastruktúra fogalma, a kritikus infrastruktúrához hasonlóan értelmezhető nemzeti, védelmi, illetve regionális és szervezeti keretek között is.

Korábban egy ország kritikus infrastruktúrái fizikailag és logikailag is önállóak voltak, egymástól csekély mértékben függtek. Az információtechnológia fejlődése következtében napjainkra e rendszerek már egyre inkább automatizáltak és egymással szoros kapcsolatban állnak. Mivel szinte minden fajta kritikus infrastruktúrát különböző szintű és rendeltetésű infokommunikációs rendszerek vezérelnek, irányítanak és ellenőriznek, ezek állnak a kritikus infrastruktúrák közötti függőség idegen szóval élve interdependencia oka mögött. Azaz egy kritikus infrastruktúra valamilyen behatás (pl. támadás) miatti sérülése magával vonzhatja más kritikus rendszerek sérülését is. Ez az összekapcsolódás lehet fizikai, de lehet logikai is, hiszen sok esetben az infokommunikációs rendszerek által összegyűjtött, feldolgozott, majd a megfelelő helyre eljutatott adat vagy információ jelenti az infrastruktúrák közötti elengedhetetlen kapcsolatot.

A kritikus infrastruktúra védelem feladatrendszerének egyik első, általánosan elfogadott feladata a kritikus infrastruktúrák azonosítása. Ennek legmagasabb szintjét a gyakorlatban a kritikus infrastruktúrák ágazatonkénti, szektoronkénti felsorolása képezi. Munk Sándor publikációjában [57] felhívja a figyelmet arra, hogy a kritikus infrastruktúrák szektorok szerinti meghatározása csak a kezdő lépés lehet. Tehát önmagában nem elegendő annak kimondása, hogy például a villamosenergia-ellátó rendszer (vagy a bankszektor) a nemzeti kritikus infrastruktúra összetevője. Ezen belül – például a nemzeti biztonsági stratégiában és a kapcsolódó ágazati stratégiákban – meg kell határozni a villamosenergia-ellátó rendszerrel (bankszektorral stb.) szemben támasztott általános követelményeket. A stratégiai szintű követelményeket ezt követően le kell bontani részletesebb, konkrét külső szolgáltatás-szint jellegű követelményekre. Ennek alapján lehet majd dinamikusan meghatározni, hogy az adott szektor, vagy infrastruktúra mely összetevői minősülnek kritikusnak és hogy ezekkel szemben milyen belső szolgáltatási-szint követelményeknek kell eleget tenniük.

Korábbi tanulmányok egymástól általában csak kis mértékben eltérve meghatározták, hogy hazánkban mik minősülhetnek kritikus információs infrastruktúrának, a következő felosztás [54] hét szektort jelöl ki:

1. energiaellátó rendszerek rendszerirányító számítógép-hálózatai;
2. kommunikációs hálózatok (vezetékes, mobil, műholdas);

3. közlekedés szervezés és irányítás számítógép-hálózatai;
4. pénzügyi-gazdasági rendszer számítógép-hálózatai;
5. védelmi szféra riasztási, távközlési, számítógép-hálózatai;
6. egészségügyi rendszer számítógép-hálózatai;
7. kormányzati és önkormányzati információs rendszerek.

Az információs infrastruktúrákat, így a kritikus információs infrastruktúrákat rendeltetésük szerint csoportosíthatjuk az alapján, hogy funkcionális vagy támogató szerepet töltenek be egy adott infrastruktúra életében. A funkcionális információs infrastruktúrák infrastrukturális alapon végeznek információs alapszolgáltatásokat, fizikailag lehetővé teszik s társadalom információs funkciójának zavartalan működését (például a légi forgalmat biztosító rendszerek). A támogató információs infrastruktúrák a kutató, fejlesztő és ellátó információs infrastruktúrák gyűjtő elnevezése. Rendeltetésük, hogy létrehozzák és folyamatosan biztosítják az előző csoportba tartozó infrastruktúrák zavartalan működését, fejlődését és hátterét (például villamos energetikai ellátó rendszerek informatikai alrendszerei) [54].

2.1.4 KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK TÁMADÁSAI

A kritikus infrastruktúrák esetében a fenyegetéseket és a veszélyeket jórészt a hagyományos támadások (robbantások, fizikai károkozások, stb.) jelentik, a kritikus információs infrastruktúrák esetében a helyzet ettől eltérő. Esetükben a hagyományos veszélyek mellett az információs térből érkező támadások és kihívások fenyegetésével is jelentősen számolni kell [56], [57], [58], [59].

Az utóbbi években több, főleg interneten keresztül végrehajtott információs támadás következett be, amik legtöbbször a világháló működésképtelenségét célozzák meg. Közülük sok nem is kerül nyilvánosságra, ami pedig igen, annak a bizonyíthatósága nehéz, sokszor megoldhatatlan feladat. A következőkben megnézzük az információs fenyegetés kategóriáit több szempontrendszer alapján.

A kritikus információs infrastruktúrákat fenyegető támadások három területen fejthetik ki hatásukat, ezek szerint megkülönböztetünk: anyagi (fizikai), információs és szellemi dimenziókat. Az első csoportba a következők tartoznak: fizikai behatás; elektromágneses, vagy radioaktív besugárzás; illetve anyagi (fizikai) jellemzők megfigyelése, érzékelése, lehallgatása. A második csoportba azokat a fenyegetéseket soroljuk, melyek az adott rendszerbe általa értelmezhető információt juttatnak be, vagy a rendszer által kezelt információkon módosítást, törlést valósítanak meg, vagy információkat szereznek meg az

adott rendszer folyamatai, résztevékenységei útján. Végül a harmadik csoportot az emberi tudatban érvényesülő szellemi kölcsönhatások (pld. megtévesztő propaganda, pánik-, vagy félelemkeltés, stb.) alkotják [58], [59].

A kritikus információs infrastruktúrákat érintő veszélyek csoportosíthatóak forrásaik, kiváltóik szerint is. Megkülönböztethetünk tudatos szereplőkhöz köthető fenyegetéseket, valamint gondatlanságból származó és természeti, vagy ipari eredetű veszélyeztetéseket.

Fenyegetések vizsgálatakor meg kell határoznunk a fenyegetés szintjét, mértékét, esetleg komplexitását. Különbséget kell tennünk a tekintetben, hogy e fenyegetések a társadalom egészének működését vagy csak a társadalom egyes szereplőit (egyéneket, vállalatokat, intézményeket) érintik. Egy vállalkozást érintő esetleges támadás nagy hatással lehet az adott gazdálkodó szervezet működésére, piaci helyzetére, ugyanakkor ezt nem lehet egy szinten kezelni azokkal a veszélyekkel, amelyek össztársadalmi szintűek, vagyis mindenki számára érezhető hatással bírnak. Ezek a veszélyek sokkal nagyobb horderejűek annál, minthogy pl. egy vállalat egy információs támadás következtében jelentős gazdasági haszontól esik el, vagy elveszíti piaci pozícióját [58].

A veszélyforrásokat osztályozhatjuk eredetük szerint, illetve a támadók tevékenységeinek szervezettségének szintje alapján. Eredetüket tekintve beszélhetünk külső és belső forrásból származó veszélyekről, strukturáltságukat tekintve, pedig magas szinten szervezett és alacsonyan szervezett fenyegetésekről.

A belső veszélyeket elsősorban a szervezet saját alkalmazottai okozzák, akik a biztonsági rendszabályok be nem tartásával, képzetlenségükkel, hanyagságukkal, illetve vélt vagy valós sérelmeik megtorlásával veszélyeztetik az adott szervezet vagy vállalat. infokommunikációs rendszereit. Ezek a veszélyek, amennyiben felfedésükre és elhárításukra nem helyeznek hangsúlyt, komoly biztonsági problémák forrásai lehetnek.

A külső veszélyek közé mindazon fenyegetések tartoznak, amelyek valamilyen külső forrásból származnak, és a támadás célja anyagi- politikai-, gazdasági- vagy katonai előnyszerzés. E támadásokat általában az információs technológiához kiválóan értők hajtják végre. E támadók köre az infokommunikációs rendszerek elterjedésével és fejlődésével egyenes arányban napról-napra növekszik és bővül. Napjainkban ezek közé sorolhatjuk: a hackereket, crackereket, számítógépes bűnözőket, hacktivistákat, ipari kémeket, terroristákat, valamint a hírszerző szolgálatok-, illetve katonai és félkatonai szervezetek alkalmazottait [58].

Magasan szervezett fenyegetéseket az előzőekben felsoroltak közül olyan szervezett csoportok, terror szervezetek, hírszerző szolgálatok, katonai és félkatonai szervezetek hajtják végre, akik képesek megszervezni akár egyszerre több fontos létesítmény elleni többirányú összehangolt támadást is. E támadások célja szinte minden esetben több mint anyagi haszonszerzés. Elsősorban gazdasági, politikai illetve katonai célok elérését szolgálják.

Ezzel szemben az alacsony szervezettségű támadásokat azon jogosulatlan felhasználók (hackerek, crackerek) hajtják végre, akiket elsősorban anyagi haszonszerzés vagy a saját képességeik megmutatása motivál. Ebből látható, hogy a magasan szervezett fenyegetések nagyságrendekkel komolyabb biztonsági problémát jelentenek, mint az alacsonyan szervezettek. Ezek közül is külön kiemelendő a terrorszervezetek ilyen irányú képességei és lehetőségei, amelyeket napjainkban egyre komolyabban kell vennünk. Az un. információs terrorizmus sokkal veszélyesebb, mint az egyszerű hacker vagy cracker támadás, mivel minden esetben politikai tartalommal rendelkezik.

A magas szinten szervezett fenyegetésekkel összefüggésben kialakult két fontos fogalom, a cyberterrorizmus és az információs terrorizmus. A cyberterrorizmus fogalmát Keith Lourdeau, az FBI cyber részlegének volt vezetője elsőként a következőképpen definiálta: „*A cyberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében.*” [60]

Az információs terrorizmus definícióját a következőképpen adhatjuk meg: „*a cyber-támadásokat és a hagyományos terrortámadásokat egyszerre alkalmazó olyan terrortevékenység, amely az információs infrastruktúrákat felhasználva, a kritikus információs infrastruktúra elleni támadásokkal próbálja meg célját elérni*.” [61]

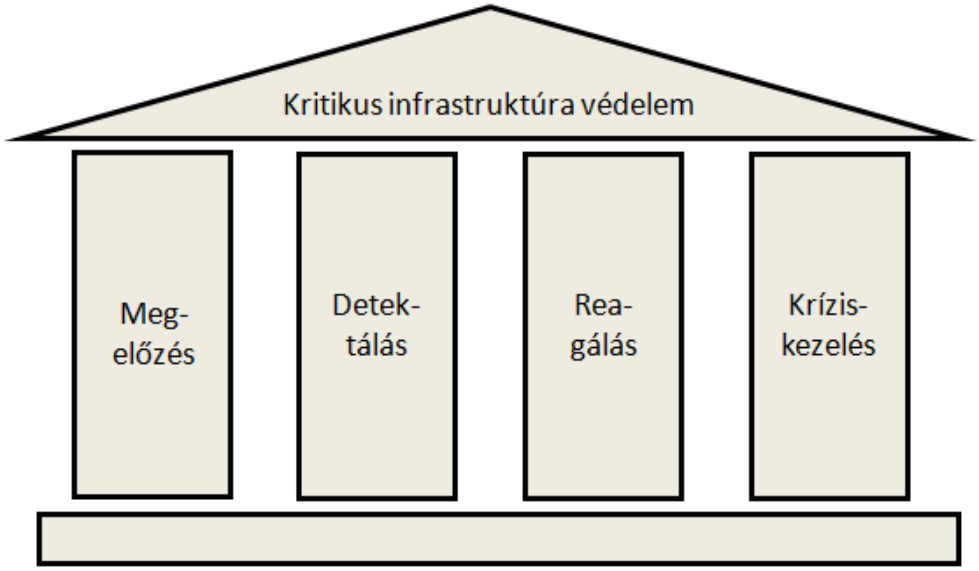
Az [56], [62] publikációkban infrastruktúrák elleni informatikai támadásokról olvashatunk részletesebben, jelen írás az Észtország ellen végrehajtott akciót ismerteti a következőkben. 2007 tavaszán DDoS támadások érték Észtország számítógépes hálózatait. A fejlett információs infrastruktúrával rendelkező, és az e-kormányzat területén komoly sikereket elért Észtország, a több mint kéthetes támadás során komoly anyagi károkat szenvedett, mert számos kormányzati, minisztériumi és több bank internetes oldala elérhetetlenné vált a támadások következtében. A támadások a tallinni orosz emlékmű elmozdítása után kezdődtek, és nagy részük többé-kevésbé beazonosíthatóan Oroszországban működtetett

szerverekről indult. Az észt miniszterelnök az orosz kormányt tette felelőssé a támadások miatt. Oroszországot korábban Ukrajna és az Egyesült Államok is megvádolta hasonló támadások végrehajtásával, de Moszkva minden alkalommal határozottan tagadta részvételét az akciókban. Az online támadások alatt összesen 128 túlterheléses támadás történt, a legkomolyabbak öt-tíz órán át, több száz megabit/s adatátviteli sebességgel bombázták folyamatos adatlekérésekkel a megtámadott szervereket, addig amíg azok össze nem omlottak. Az észt hálózaton az adatforgalom esetenként órákon át a normális ezerszerese volt. Ehhez egyes források szerint valószínűleg az internetes alvilágtól kellett erőforrásokat bérelnie a támadóknak. Érdemes megjegyezni, hogy közel fél évvel a támadások után csak egyetlen támadót sikerült bizonyíthatóan azonosítani. Meglepő módon azonban ez a támadó egy észt fiatalember volt, akit a bizonyítékok alapján pénzbüntetésre ítéltek.

2.1.5 KRITIKUS INFRASTRUKTÚRÁK VÉDELMI FELADATAI

A kritikus információs infrastruktúra védelme többszereplős feladatrendszer. Mivel napjainkban a kritikus információs infrastruktúrák jelentős része – piacgazdaságra épülő államokban mintegy 80-90%-uk – az adott államtól teljesesen vagy részben független magánvállalkozások kezelésében van, védelmükben egyaránt érintettek a kormányzati szervek és intézmények, az egyes infrastruktúrák tulajdonosai és üzemeltetői, sőt az informatikai ipar szereplői, bizonyos vonatkozásokban pedig még az információs szolgáltatásokat igénybevevő felhasználók is. A védelem célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat [57], [59].

A kritikus információs infrastruktúra védelmében a megelőzés és korai figyelmeztetés, az észlelés, a reagálás és a válságkezelés alkotja a négy fő pillért, ezt szemlélteti az alábbi ábra.



9. ábra: A kritikus infrastruktúra védelem négy pillére [63]

Az első pillér szerepe, hogy a védekezésben érintettek felkészültek legyenek a bekövetkező incidensekre, illetve megkapják az időbeni figyelmeztetést a várható fenyegetésekről. A második pillér lényege az új fenyegetések minél gyorsabb felfedezése. A reagálás, mely a harmadik pillért jelenti, magában foglalja a működés, szolgáltatás megszakadása okainak azonosítását és megszüntetését. Az incidensre adott válasz nem csak technikai jellegű, létfontosságú része lehet a támadók megbüntetése is. Ennek a pillérnek a része az incidens elemzése és a tapasztalatok közreadása is. Végül a válságkezelés pillérébe az incidens bekövetkezését követő döntéshozatali, irányítási és koordinációs feladatok tartoznak. A kritikus információs infrastruktúra védelem főbb feladatcsoportjai közé a következőket sorolhatjuk: elemzés és értékelés (fenyegetések és sebezhetőségek); kiküszöbölés (sebezhetőségek); felkészülés és felkészítés; figyelés, észlelés és tájékoztatás; mérséklés; reagálás; és helyreállítás [59].

A különböző országokban a kritikus információs infrastruktúra védelem feladatai megvalósításának szervezetrendszere rendkívül heterogén, számos szervezetet, intézményt, hatóságot foglal magában. A kormányzati szereplők között vannak minisztériumok, ágazatközi szervezetek, minisztériumokon belüli szervezeti egységek (hivatalok, bizottságok) és minisztériumok alárendeltségébe tartozó szervezetek. Az érintett szereplők között szinte minden országban találkozunk a köz- és magánszféra partnerségére épülő szervezetekkel is. Az érintett szereplők körét, helyét és feladatrendszerét különböző tényezők befolyásolják: hagyományok, történelmi tapasztalatok, az erőforrások elosztása, valamint az aktuális fenyegetésekkel kapcsolatos politikai elképzelések [59].

A kritikus információs infrastruktúra védelemmel kapcsolatos alapvető megközelítések négy csoportba sorolhatóak. Az első szerint ez egy technikai szintű, információ-, illetve informatikai biztonsági kérdés kiemelt tekintettel az Internet-biztonságra. A második megközelítés lényege az e-gazdasághoz kapcsolódó működésfolytonossági (üzletmenet-folytonossági) szemlélet. A harmadik a rendvédelmi megközelítés, amely az informatikai bűnözés elleni tevékenységre összpontosít. Végül a negyedik a kritikus információs infrastruktúra védelmet nemzetbiztonsági megközelítésben, annak lényeges összetevőjeként szemléli.

Az első két elképzelést valló országok esetében az információs infrastruktúra alapvetően az információs társadalom, az elektronikus gazdaság, az információs szolgáltatások bázisa, így a kritikus információs infrastruktúra védelem alapvető felelősei az e-kormányzatért, az informatikáért és a távközlésért felelős szervezetek, illetve a katasztrófavédelmi szervezetek. Többségében ezen országok esetében is megemlítésre kerül a rendőrség, mint az informatikai bűnözés elleni harc megvalósítója, azonban ez erőteljesebben a harmadik megközelítés esetében jelenik meg [59].

A védelmi szféra szervezeteinek jelentősebb szerep azon országokban jut, amelyek megfogalmazzák az információs infrastruktúrák nemzetbiztonsági jelentőségét és ehhez kapcsolódóan reális veszélynek tartják a terrorfenyegetettséget, sőt egyes esetekben már az államilag támogatott/megvalósított információs támadásokat. Ezen országokban így kiemelt szerepet kapnak katonai szervezetek és a nemzetbiztonsági szolgálatok is.

2.1.6 KRITIKUS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK KÉRDÉSEI

A következőkben a kritikus infrastruktúrák azonosításának kérdéseivel foglalkozom [FR6] publikációm alapján. A kritikus infrastruktúra védelem egyik lényeges feladata a védendő objektumok meghatározása, ezen a területen hazánkban is folynak kutatások. A hazai kritikus infrastruktúra elemek meghatározására egy kiindulási pontot találunk Muha Lajos doktori disszertációjában [56]. A [64] tanulmány a kritikus infrastruktúrák priorálására ír le egy módszert, mely az adott infrastruktúra hatókörét, népességre gyakorolt hatását, gazdasági hatását, interdependenciáját, politikai hatását és időbeni hatását vizsgálja, majd ezen jellemzők összegzésével előállítja az infrastruktúra kritikusságának mértékét.

A következőkben a kritikus infrastruktúra azonosítását vizsgálom meg részletesebben. Az azonosítás végterméke, célja egy (vagy több) kritikus infrastruktúra lista felállítása, mely a

védelem tárgyait tartalmazza. A kritikus infrastruktúra lista nem egy statikus meghatározás, azt bizonyos időszakonként (pl. évente) aktualizálni, megújítani, jóváhagyni szükséges. A első ránézésre nagyon konkrétnak tűnő feladat mögött számos megfontolandó kérdés húzódik meg. Mivel hazánkban a kritikus infrastruktúra védelem még nem tart azon a szinten, hogy kritikus infrastruktúra lista megalkotására sor került volna, érdemes megvizsgálni azt, hogy ezen a téren nálunk előrébb járó országokban milyen módszereket követnek. A következőkben az Amerikai Egyesült Államok gyakorlatának néhány sajátosságát ismertetjük [65], [66], [67] alapján

Az USA-ban a Belbiztonsági Minisztérium (Department of Homeland Security) a kritikus infrastruktúra védelem központi felelős szerve, továbbá minden kritikus infrastruktúra szektorhoz – összesen 18 – hozzárendelték a felelős minisztériumot, mely az adott szektor kritikus infrastruktúra védelméért felel (a privát szférával való együttműködést is beleértve). A nemzet legkritikusabb objektumait kettő darab listába szervezve tartják számon, melyek létrehozásáért és jóváhagyásáért a Belbiztonsági Minisztérium felel. Az 1. szintű lista azokat az objektumokat tartalmazza, melyek sérülése katasztrofális következményekkel járna a nemzet számára. A 2. szintű lista bővebb tartalmú, magában foglalja az előző lista elemeit is, kritériuma pedig nemzeti jelentőségű következmény kialakulása valamely elemének megsérülése esetén. A nemzeti listák mellett minden szektor gondoz egy saját listát, mely az adott szektor kritikus elemeit tartalmazza, illetve minden államnak van egy listája a saját kritikus infrastruktúra objektumairól. Ezt a két listát a Belbiztonsági Minisztérium (azaz a kritikus infrastruktúra központi szerve) hagyja jóvá és a két nemzeti listát ezek segítségével állítja össze.

Érdemes megvizsgálni az USA kritikus infrastruktúra listáinak elemeit. Itt igazából arra keressük a választ, hogy a kritikus infrastruktúrákat mivel lehet megadni, ugyanis az infrastruktúra, mint fogalom önmagában nehezen megfogható dolog. A hivatkozott dokumentumok rendszerek (systems) és vagyontárgyak (assets) összességeként határozzák meg a listák tartalmát. Továbbá kiemelik, hogy a kritikus infrastruktúra szektorok vagy vagyon-alapúak - angolul „asset-based” -, vagy rendszer-alapúak – „system-based” -; az elsőre példák a Vegyipari, Kereskedelmi, Vízügyi, Védelmi ipari bázis, Nukleáris szektorok, míg a másodikra a Mezőgazdaság és élelmiszeripari, Bank és pénzügyi, Kommunikáció és Információ technológiai szektorok. Figyelemre méltó tény, hogy a rendszer-alapú kritikus infrastruktúra szektorok listáinak elkészítése, illetve ezen listák esetében a kritikussági

kritériumok alkalmazása a gyakorlat szerint sokkal bonyolultabban és nehezebben kivitelezhető, mint a vagyon-alapú szektorok esetében.

A kritikus infrastruktúra listák különböző szervezetek, az ipar és közszféra szereplőinek segítségével, ajánlásaival születnek meg. Ehhez a munkához, azaz a kritikusság eldöntéséhez a kritikus infrastruktúra védelem központi szerve különböző útmutatókat, ajánlásokat dolgoz ki. A 2009-es évben az USA-ban teljes mértékben átálltak a következmény-alapú kritikusság meghatározására. A következmény-alapúság azt jelenti, hogy olyan kritériumokat és mérőszámokat dolgoznak ki a lista összeállításának segítségére, melyek az egyes kritikus infrastruktúra objektum támadásának, megsérülésének következményeit vizsgálják, nem pedig olyan paramétereket, mint például az adott objektum mérete vagy kapacitása. Minden szektor számára szektor-specifikus útmutatókat, kritérium rendszereket is készít a Belbiztonsági Minisztérium. Ezek alapján készítik el a szektorok kijelölt partnerei a listába felveendő objektumok halmazát, melyet legvégül a Belbiztonsági Minisztérium hagy jóvá és véglegesít.

Az 1. és 2. szintű listákat a következő lehetséges következmények megvizsgálása alapján állítják elő: 1) halálesetek száma, 2) az első évben elszenvedett gazdasági kiesés, 3) evakuáltak száma, 4) bizonyos biztonsági funkciók (hírszerzés és védelem) sérülése. A szektorok listáinak elkészítéséhez a Belbiztonsági Minisztérium szektor specifikus azonosítási útmutatót, segédletet is megad [66].

A Zürichi Biztonsági Tanulmányok Központja (Center for Security Studies, ETH Zurich) kétévente kiad egy kézikönyvet a nemzetközi kritikus információs infrastruktúra védelemről (International CIIP Handbook), mely átfogó képet ad a kritikus információs infrastruktúra védelem nemzetközi gyakorlatáról, tapasztalatáról, kutatásáról és a nemzeti tapasztalatok felhasználásával általános következtetéseket von le. A következőkben ismertetem a kritikus infrastruktúra azonosításával kapcsolatos gondolatokat az említett kézikönyvekre támaszkodva [68], [69].

A kritikusság megállapításához, azonosításához 4 lépést javasol a kézikönyv: 1) kritikus szektorok meghatározása, 2) szervezeti megfontolások alapján kritikus alszektorok meghatározása, 3) a kritikus alszektorok alapfunkcióinak meghatározása, 4) azon erőforrások meghatározása, melyek az előző pont funkcióinak elvégzéséhez szükségesek [69].

A kézikönyv szerint a kritikus infrastruktúra lista termékek (products) és szolgáltatások (services) összességéből áll fel. Mivel az infrastruktúra rendszerek legtöbbször meglehetősen

komplexek, esetleg több szektor alá is besorolhatók, ezért gyakran szükséges lehet az infrastruktúrákat az általuk nyújtott szolgáltatások felől megközelíteni. Egy adott infrastruktúra kritikussága fennállhat abból kifolyólag, hogy az adott infrastruktúra 1) önmagában kritikus funkciót, szerepet, szolgáltatást tölt be a társadalom életében, vagy 2) egy kritikus funkcióhoz nyújt alapvető szolgáltatást [69]. A kézikönyv hangsúlyozza, hogy az utóbbi csoportba eső kritikus infrastruktúra komponensek meghatározása bonyolultabb, nehezebb.

Az előbbiekben tanulmányozott két szemlélet tükröz bizonyos különbözőségeket, például a vagyontárgyak-rendszerek (USA), illetve termékek-szolgáltatások szerinti modellek (Zürichi Biztonsági Tanulmányok Központja) felépítése tekintetében. A különbségek további elemzése az értekezés kereteibe nem fér bele, esetleg egy másik tanulmánynak a témája lehet. A következőkben inkább az előző megfontolások figyelembe vételével a hazai feladatokra koncentrálunk. Magyarországon is szükséges lépés lesz a jövőben a kritikus infrastruktúrák azonosítása és a kritikus infrastruktúra lista (listák) elkészítése. A feladat előkészítésének tükrében a következő gondolatok megfontolását javaslom.

A kritikus infrastruktúra védelem szervezeti kereteit át kell gondolni, le kell fektetni és a szükséges felelősségi köröket ki kell jelölni. Mindenképpen szükséges egy kormányzati hatáskörű központi szerv kijelölése, mely a kritikus infrastruktúra védelem koordinációjáért felel. A szektorok meghatározása a Kormányhatározatban [50] megtörtént, 10 ágazatba és azon belül 43 alágazatba osztották a kritikus infrastruktúrákat, az ágazatokhoz felelősöket rendeltek. A kritikus infrastruktúra lista létrehozását a központi szervnek kell irányítania, koordinálnia, a létrehozás folyamatát kijelölnie, partner szervezetekkel (magán szféra, ipar képviselői) konzultálnia és a végleges listát felállítania. A kritikus infrastruktúra lista felállítása nem egy statikus meghatározás, bizonyos időszakonként (pl. évente) aktualizálásra szorul.

Egy másik fontos tény, hogy a kritikusságnak különböző fokozatai léteznek. A kritikusság rendkívül erős foka az, amikor a sérülés következményét országos szintű katasztrófában határozzuk meg. Definiálhatjuk a kritikusságot országos jelentőségű negatív hatással is. Az USA-ban például a már említett négy kritérium (halálesetek száma, az első évben elszenvedett gazdasági kiesés, evakuáltak száma, bizonyos biztonsági funkciók sérülése) különböző értékekkel való ellátásával határoznak meg két szintet. Tehát a kritikus infrastruktúra lista létrehozását meg kell, hogy előzze a kritikusság mértékét leíró kritériumoknak és a hozzájuk tartozó mérőszámoknak a megadása. A kritikussági kritériumoknak és a hozzá tartozó

útmutatónak a felállítása mindenképp a központi szervnek feladata közé tartozik. Dönteni kell arról is, hogy egy listába rendezve tartjuk számon a kritikus infrastruktúrákat, és listán belül kezeljük a kritikusság különböző szintjeit, vagy több listát készítünk.

A kritikus infrastruktúra lista elemeinek típusát, tartalmi szerkezetét is meg kell határozni. Mit értünk védendő objektumok alatt, azaz miket is tartalmazzon a lista? Ha a kritikus infrastruktúra fogalmát megvizsgáljuk, akkor az létesítmények, szolgáltatások, rendszerek és folyamatok összességeként definiálja a kritikus infrastruktúrát, ami a lista megalkotásának kezdeti fázisában túl tág halmaz. Ha az USA gyakorlatát, illetve a kritikus információs infrastruktúra védelem kézikönyvének ajánlását megnézzük, akkor látjuk, hogy azok kritikus 1) termékeket vagy vagyontárgyakat (product, asset) és 2) rendszereket vagy szolgáltatásokat (system, service) rögzítenek első körben. Ezeket persze a következő lépésként további részelemekre kell bontani, azaz a szükséges és kritikus szerepet játszó létesítmények, szolgáltatások, személyzet, folyamatok, rendszerek és eszközök szintjéig lefúrni.

Véleményem szerint az infrastruktúrákat, így a kritikus infrastruktúrákat is az általuk nyújtott szolgáltatások felől érdemes megközelíteni. A szolgáltatásokban való gondolkodás nem kerülhető el, napjaink folyamataiban, az egyének és a közösségek életében, illetve a gazdasági életben is a szolgáltatások egyre nagyobb részt töltenek be. Az állam szerepének típusa, feladatköre is a szolgáltató állam felé tolódik (tolódott) el.

A szerző javasolja átgondolásra a következőket. A kritikus infrastruktúra lista készítésének első fázisában kizárólag a kritikus szolgáltatásokat határozzuk meg és szolgáltatásokként azt a minimális szintet, amivel a szolgáltatásnak még vészhelyzetben is működnie kell. Minden szolgáltatáshoz minőségi jellemzőket kell rendelni és ezek segítségével meghatározni a szükséges minimális szintet, ami az előírt kritikussági szintnek megfelel. A következő fázis feladata az adott szolgáltatáshoz és minimális működési jellemzőhöz felsorolni azokat a létesítményeket, szolgáltatásokat, személyzetet, folyamatokat, rendszereket és eszközöket, amik a meghatározott működéshez szükségesek.

A kritikus infrastruktúrák szolgáltatások felőli azonosítása esetén át kell gondolni, hogy nem hagyunk-e ki lényeges infrastruktúra elemet. Azaz létezik-e olyan kritikus infrastruktúra elem, mely mögött nem áll kritikus szolgáltatás, de az adott elem sérülése súlyos hatást gyakorolna például a közegészségre vagy közbiztonságra. Ez a kérdés összefüggésben áll az infrastruktúra kifejezés definíciójával is, a fogalmat lehet szűken, illetve tágan is értelmezni. Mi a szűkebb értelmezést választjuk, tehát feltételezzük, hogy az infrastruktúra

szolgáltatáshoz kötődik. Ha ennek feldolgozása megtörténik, az a tágabb értelmezés elrendezését is segíti.

2.2 ADATBÁZISOK SZEREPE A KRITIKUS INFRASTRUKTÚRÁKBAN

A következőkben az adatbázisok biztonsága és a kritikus infrastruktúrák biztonsága összefüggéseit, illetve az adatbázis-biztonság kritikus infrastruktúra védelmen belüli helyét és szerepét vizsgálom a [FR7], [FR8] publikációim alapján. Ennek érdekében elemzem, rendszerezem és általánosságban értékelem az adatbázisok előfordulását, helyét és szerepét a különböző kritikus infrastruktúra szektorokban.

2.2.1 ADATBÁZISOK HELYE, SZEREPE KRITIKUS INFRASTRUKTÚRÁKBAN

A kritikus infrastruktúra szektorok (ágazatok) közé a kritikus infrastruktúravédelem nemzeti programjáról szóló kormányhatározatban [50] foglaltaknak megfelelően a következőket soroljuk: energiaellátás; közlekedés; vízellátás; élelmiszerellátás; egészségügy; pénzügy; ipar; jogrend-kormányzat; közbiztonság-védelem; és végül az infokommunikációs szolgáltatások. A továbbiakban szektoronként röviden, általánosságban értékelem az adatbázisok helyét, szerepét

Az **adatbázisok általános helye és szerepe** áttekintésének alapját elsőként az adott szektor főbb informatikai rendszereinek, informatika-alkalmazási szintjének, informatika-függőségének megítélése képezi (ennek során figyelmen kívül hagyásra kerülnek a nem szakterület-specifikus – pld. vezetési, gazdálkodási, stb. – informatikai rendszerek). Ezt követően kerül sor a főbb szakterületi adatbázisok áttekintésére és az alaprendeltetés szempontjából vett kritikusságuk előzetes értékelésére.

Az **energiaellátás** területén az informatika alkalmazása a kőolaj, földgáz és villamos energia termelés, tárolás, elosztás és rendszerirányítás támogatására irányul. Ezen belül informatikai rendszerek, alkalmazások támogatják az egyes termelő egységek, erőművek tevékenységét, valamint a kőolaj-, földgáz és villamos-energia hálózat működtetését, az energia-elosztás rendszerirányítását. A szakterület jellemző, informatikai eszközökkel támogatott rendszerei az ún. felügyeleti és adatgyűjtő (SCADA[2]) rendszerek közé tartoznak.

Mind az üzemi, erőműi informatikai rendszerek, mind a szállító, elosztó hálózatok rendszerirányító rendszereinek rendeltetése az irányított rendszerben zajló folyamatok,

[2] Supervisory Control and Data Acquisition.

események valós idejű figyelemmel kísérése, illetve befolyásolása. E rendszerek – pld. MAVIR SPECTRUM [70], [71], MOL OTR IIM [72] – működése valósidejű helyzetismeret adatbázisokra épül, amelyek jellemzően két összetevőt, részadatbázist tartalmaznak. Az egyik az irányított rendszer, hálózat topológiáját (ritkábban változó jellemzőit) tárolja, a másik pedig az egyes összetevők, objektumok dinamikusan változó aktuális állapotát. E két adatbázis az eltérő követelmények miatt általában különböző adatbázis-kezelési megoldásokkal kerül megvalósításra.

Az energiaellátó rendszerek, hálózatok más kritikus infrastruktúra szektorokhoz hasonlóan lényegében működésképtelenek a támogató – mindenekelőtt a rendszerirányításban alkalmazott – informatikai rendszerek, alkalmazások nélkül. Országos szintű hatással elsősorban az országos hálózati rendszerirányító (SCADA) rendszerek adatbázisainak veszélyeztetései, illetve egyes, jelentős szerepet játszó energia-előállító szervezetek (pld. Paksi Atomerőmű) rendszerirányító adatbázisait érintő támadások járhatnak.

A **közlekedés** területén az informatika-alkalmazás (közlekedési informatika) szakterületi szempontból a következő részterületekre osztható: személyszállítási, áruszállítási és forgalomirányítási informatika. Ezen belül az egyes közlekedési alágazatok – közúti, vasúti, vízi, légi, városi – természetesen sajátosságokkal is rendelkezhetnek. A következőkben foglaltakat nagyrészt Szászi Gábor jegyzetére [73] alapozva tárgyaljuk.

A személyszállítás esetében informatikai rendszerek támogatják a tervezést, előkészítést (kapacitás és menetrend tervezés), az utazás előkészítését (menetrendi információszolgáltatás, helyfoglalás, menetjegy kiadás), valamint az utazást magát (utas tájékoztatás, fedélzeti tájékoztatás). A fenti szolgáltatások számos különböző adatbázis alkalmazására épülnek. Ilyenek mindenekelőtt a következők: menetrendi, járat, tarifa, helyfoglalási és menetjegy adatbázisok.

Az áruszállítás informatikával támogatandó folyamatai közé a rakodás-kirakodás, az útvonali közlekedés-irányítás és az árurendezés tartozik. Az adatbázisok ezen a területen is jelentős szerepet játszanak, köztük például: szállítóeszköz, szállítási feladat, valamint közlekedési hálózat adatbázisok.

A forgalomirányítás informatikai támogatása a két előző területtel szemben nem közlekedési szervezetekhez, hanem több szereplő által használt közlekedési hálózatokhoz, hálózatrészekhez kapcsolódik (pld. városok, autópályák, stb.). E területen elsősorban a felügyelt körzet közlekedési hálózatát leíró adatbázis játszik jelentősebb szerepet.

Napjainkban a kritikus infrastrukturális közlekedési szolgáltatások a támogató informatikai rendszerek és adatbázisaik nélkül gyakorlatilag működésképtelenek, egyes részfolyamataik ugyan korlátozott mértékben, hagyományos támogatással is működtethetőek, azonban a rendszer egésze nem. Egyes adatbázisok megrongálása, vagy meghamisítása teljes közlekedési káoszhoz és tovagyűrűző hatásokhoz vezet, sőt emberi életeket, jelentős anyagi javakat veszélyeztet. Ezek közül országos szintű hatást elsősorban a MÁV és a Ferihegyi repülőteret üzemeltető szervezet egyes adatbázisainak támadása válthat ki, emellett regionális hatású lehet az egyes VOLÁN vállalatok adatbázisainak támadása.

A **vízellátás** területén az informatika-alkalmazás – a kritikus infrastruktúra védelem szempontjából – a megfelelő minőségű ivóvíz szolgáltatás és szennyvízelvezetés/tisztítás biztosításához, valamint az árvízvédelemhez kapcsolódik. A vízügyi informatikai rendszerek, más területekhez hasonlóan országos és területi/szervezeti rendszerekre csoportosíthatóak.

Az országos szintű vízügyi rendszerek közül a legjelentősebbek közé a Vízgazdálkodási, a Vízkárelhárítási Védekezési és a Vízminőségi Kárelhárítási Információs Rendszerek tartoznak. Ezek működését számos, országos szintű adatbázis – köztük az Objektum és Törzsadat-kezelő Rendszer és a Magyar Hidrológiai Adatbázis – támogatja, amelyek nagyobbrészt vízügyi objektumokra vonatkozó leíró adatokat, valamint hidrológiai mérési, megfigyelési eredményeket tartalmaznak [74].

A területi/szervezeti szintű vízügyi informatikai rendszerek közül a vízellátás és szennyvízelvezetés szempontjából a vízművek, az árvízvédekezés szempontjából pedig a regionális vízügyi igazgatóságok rendszerei érdemelnek figyelmet. A vízművek üzemirányító rendszerei a felügyeleti és adatgyűjtő rendszerek csoportjába tartoznak, helyzetismeret adatbázisaik más alkalmazási területekhez hasonlóan térinformatikai alapú, ritkán változó leíró adatokat és dinamikusan változó mérési adatokat tartalmaznak. Az értékesítést támogató rendszerek adatbázisai a végrehajtott szolgáltatások adatait tárolják [75]. A vízügyi igazgatóságokon speciális informatikai rendszerek, adatbázisok gyakorlatilag nincsenek, a meglévő rendszerek, adatbázisok a már említett országos rendszerek részét képezik.

A vízügyi adatbázisok megrongálása, meghamisítása egyes esetekben jelentős – de alapvetően csak regionális, vagy helyi – problémákat okozhat a vízellátásban, esetleg az árvízvédekezésben. Országos szintű hatást kiváltó fenyegetés megvalósítására azonban jelenleg nem látszik lehetőség.

Az **élelmiszerellátás** kritikus infrastruktúra jellege az élelmiszer-ellátási lánc egészére – a termelésre, feldolgozásra és forgalmazásra – kiterjed. Ezen belül speciális részterület az egészséget veszélyeztető hatások kiküszöbölésére irányuló élelmiszer-biztonság. Az informatikai támogatás az általános alkalmazási területek mellett elsősorban az élelmiszerek nyomon követésére, szennyeződésének figyelésére, illetve az élelmiszer eredetű megbetegedések jelzésére szolgáló adatgyűjtő és értékelő rendszerek esetében játszik kiemelt szerepet [76].

Az élelmiszer-biztonságot szolgáló nemzeti hálózat és adatbázisok szoros együttműködésben állnak európai és más nemzetközi rendszerekkel. A szakterület témánk szempontjából fontos, létező és tervezett adatbázisai közé a viszonylag állandó jellegű, leíró adatokat tartalmazó adatbázisok, valamint az előírt bejelentésekből, ellenőrzésekből, laboratóriumi vizsgálatokból származó adatokat tartalmazó adatbázisok tartoznak. Az előzőekre alapozva egy Európai Uniós projekt keretében jelenleg tervezett egy egységes nemzeti élelmiszer-biztonsági adatbázis kialakítása [77].

Az élelmiszer-biztonsági adatbázisok veszélyeztetettsége önmagában csak különleges esetekben járhat országos szintű hatással, azonban más biztonsági fenyegetésekhez hozzáadódva növelheti, erősítheti azok káros következményeit.

Az **egészségügy** területén az informatika-alkalmazás (egészségügyi informatika) több más mellett a következő részterületekre osztható: kórházi, ápolási, orvosi képalkotó, közegészségügyi, fogorvosi, gyógyszerészeti, illetve egészségbiztosítási informatika. Az egészségügyben alkalmazott informatikai rendszerek alkalmazásuk hatókörét tekintve feloszthatóak intézményi (kórházi, háziorvosi, gyógyszertári, stb.), intézményközi és országos szintű rendszerekre. Az egészségügy informatikai támogatása folyamatosan fejlődik. Ez megnyilvánul mind az egészségügyi igazgatás, mind az egészségügyi ellátás, szolgáltatások területén.

Az egészségügyi intézményi informatikai rendszerek szakmai adatbázisai alapvetően az ellátásban részesülők intézményi kezelésével kapcsolatos információkat tartalmaznak. Ezek közé mindenekelőtt a diagnosztikai és terápiás információkat tároló, köztük a képalkotó diagnosztikai adatbázisok tartoznak.

A Magyarországon még csak tervezett intézményközi rendszerek az ellátottakra vonatkozó összes egészségügyi információ központi, vagy regionális tárolására épülnek. Ezek a személyi

egészségügyi életút adatbázisok várhatóan jelentős mértékben javítják majd az egészségügyi ellátórendszer globális teljesítményét [78].

Az országos szintű rendszerek adatbázisai közé elsősorban az olyan közhiteles nyilvántartások tartoznak, mint a különböző személyi, szervezeti nyilvántartások; gyógyszer, orvostechnikai eszköz és gyógyászati segédeszköz nyilvántartások; TAJ adatbázis; szakmai kódrendszerek (betegségek, orvosi eljárások, stb.), illetve finanszírozási, besorolási kategóriák [79], [80], [81].

Az egészségügyi szolgáltatások ma már gyakorlatilag szintén működésképtelenek az informatikai támogatás nélkül. Az előzőekben említett adatbázisok elleni támadások elsősorban egészségügyi ellátási képességeket, kapacitásokat rombolnak, befolyásolnak és ezzel közvetve, vagy közvetlenül – az ellátás elmaradásával, vagy hibás kezeléssel – emberi életeket veszélyeztetnek. Ezek közül országos szintű hatással elsősorban egyes közhiteles nyilvántartások támadása járhat, regionális hatású pedig a súlyponti kórházak veszélyeztetése lehet.

A **pénzügyi** területen az informatika-alkalmazás két nagy területre csoportosítható: a pénzintézetek tevékenységének támogatására és a pénzintézetek közötti fizetési forgalom, elszámolások támogatására. Mind a pénzintézeti, mind az elszámolási tevékenység élenjáró területe az informatikai rendszerek, szolgáltatások alkalmazásának.

A pénzintézeti (ezen belül pld. a banki) tevékenység szinte egésze ma már informatikai folyamatokon keresztül valósul meg, amelynek alapját az alapvető pénzintézeti – pld. ügyfél-, számla-, valamint tranzakciós – adatbázisok képezik. Napjainkra már az ügyfelek oldalán is egyre jobban terjed az informatikai eszközök segítségével, az elektronikus banki szolgáltatások igénybevételével történő ügyintézés [82].

A pénzintézetek közötti fizetési, elszámolási tevékenység hatékonyan és gyorsan csak informatikai rendszerek segítségével lehetséges. Ilyen rendszerek a világ számos országában működnek, Magyarországon ide sorolhatóak a GIRO, VIBER és KELER[3] rendszerek. Ma már ezen rendszerek is belső adatbázisokra épülnek, amelyek biztonságának megsértése a bankközi forgalom felborulását is eredményezheti. Egyes vizsgálatok ezt már akár egyetlen résztvevő rendszerének kiesése esetén is valószínűsítik [83].

[3] GIRO = bankközi fizetési forgalmat lebonyolító elszámolási rendszer; VIBER = Valós Idejű Bruttó Elszámolási Rendszer a nagy értékű átutalások teljesítésére; KELER = értékpapír elszámoló rendszer.

A fejlett államokban a pénzügyi rendszerek ma már működésképtelenek az informatikai támogatás és ezen belül az alapvető pénzügyi adatokat tartalmazó adatbázisok rendelkezésre állása, sértetlensége és hitelessége nélkül. Ezen adatbázisok megrongálása, vagy meghamisítása a pénzügyi folyamatok leállását, vagy hibás megvalósulását vonja maga után és ezzel általában országos szintű káros hatás kiváltására is alkalmas.

Az **ipar** területén a kritikus infrastruktúrák közé a vegyi anyagok előállítása, tárolása és feldolgozása; a veszélyes anyagok, hulladékok kezelése, tárolása, szállítása; a nukleáris anyagok előállítása, tárolása, feldolgozása; valamint az oltóanyag és gyógyszergyártás során felhasznált infrastruktúrákat sorolják, mivel ezek sérülése, hibás működése a lakosságot veszélyeztető ipari balesetekhez vezethet. A veszélyes anyagok kezeléséhez kapcsolódó jelentősebb informatikai rendszerek, alkalmazások két nagy csoportba sorolhatóak: az elsőt a más területeken korábban már említett folyamatirányítási, rendszer-felügyeleti rendszerek képezik, míg a másodikba a veszélyes anyagokkal kapcsolatos nyilvántartási és tájékoztató rendszerek tartoznak.

A nyilvántartási és tájékoztató rendszerek fenntartását az Európai Unió a SEVESO II. irányelvben határozta meg. Az ebben foglalt követelményeknek megfelelően került kialakításra a Seveso Üzemek Nyilvántartási Rendszere (SPIRS) [84], Súlyos Balesetek Jelentési Rendszere (MARS) [85], valamint a Veszélyes Anyagok Adatkezelő Rendszere (DSDMS).[4] A két előbbi rendszer alapját egy-egy elosztott – egy központi és a tagállamok illetékes szervezeteinél működő helyi összetevőkből felépülő – adatbázis képezi, amelyek a veszélyes anyagokat kezelő főbb európai ipari létesítmények veszélyhelyzet-kezeléséhez szükséges, valamint a súlyos balesetekre vonatkozó alapvető információkat tartalmazzák. Ehhez kapcsolódóan az egyes országok, köztük Magyarország is működtet saját nemzeti nyilvántartásokat és az ezeket támogató informatikai rendszereket.[5]

A folyamatirányítási és rendszer-felügyeleti rendszerek adatbázisainak veszélyeztetése egyes vegyi és nukleáris létesítményekben, üzemekben (pld. Paksi Atomerőmű) közvetlenül országos hatású súlyos ipari balesetekhez vezethet. A nyilvántartási és tájékoztató rendszerek adatbázisainak sérülése ezzel szemben közvetett módon, az esetlegesen bekövetkező ipari balesetek elleni védekezés eredményességének, hatékonyságának csökkentésén keresztül

[4] Seveso Plants Information Retrieval System, Major Accident Reporting System, Dangerous Substances Data Management System.
[5] Ipari Katasztrófaelhárítási Információs Rendszer (IKIR).

jelent fenyegetést az állampolgárok életére, egészségére, valamint a szervezetek és állampolgárok vagyoni javaira.

A **jogrend és kormányzat** területén a kritikus infrastruktúra védelem szempontjából a kormányzati/közigazgatási létesítmények és eszközök működőképessége, valamint a közigazgatási szolgáltatások rendelkezésre állása játszik jelentős szerepet. A közigazgatási szolgáltatások informatikai rendszerekkel, eszközökkel támogatott megvalósítása, az úgynevezett e-kormányzat, vagy e-közigazgatás napjaink egyik legfontosabb célja, megvalósulóban lévő eredménye.

A közigazgatási szolgáltatások informatikai támogatása két jól elkülöníthető, de egyformán fontos területre bontható: a közszolgálati intézmények belső működésének támogatása (back office) és a lakosság, valamint a gazdálkodó szervezetek kapcsolattartása ezen intézményekkel (front office). Az elektronikus – vagyis informatikai rendszerekkel, eszközökkel támogatott – ügyintézés és az elektronikus ügykezelés alapvető rendeltetése a szolgáltatási igények kielégítése, illetve a közigazgatási folyamatok hatékonyságának növelése [86].

Az informatikai támogatással működő közigazgatás alapvető feltétele a tevékenység során felhasznált, naprakészen tartott nyilvántartások, adatbázisok megléte, elérhetősége. Ezek között vannak alap-, vagy köznyilvántartások amelyek az adott területen (vagy az ország területén) élő személyek, szervezetek, események adatait közhiteles módon tárolják és vannak ágazati, vagy szakági rendszerek, amelyek az adott szakterület (tárca) funkcióihoz igazodnak, a szakterületi informatikai rendszerek szerves részét képezik. A közhiteles nyilvántartások, adatbázisok közé tartoznak többek között a népesség-, anyakönyvi, közműtulajdon-nyilvántartások, míg az ágazati csoportba a rendőrségi, bírósági, oktatási, adóügyi, vámügyi, társadalombiztosítási, földhivatali, stb. nyilvántartások tartoznak.

A fentiekben is említett adatbázisok napjainkban már kulcsfontosságú szerepet töltenek be a közigazgatásban. Sérülésük, meghamisításuk alapvető közigazgatási szolgáltatásokat hiúsít meg, vagy tesz megbízhatatlanná. Számos szolgáltatás hiánya a mindennapi és a gazdasági élet lényeges folyamatainak megvalósulását országos szinten akadályozza.

A **közbiztonság és védelem** területéhez a honvédelmi és rendvédelmi rendszerek, hálózatok, infrastruktúrák sorolhatóak. A védelmi szféra harmadik jelentős részterülete, a katasztrófavédelem kérdései alapvetően már tárgyalásra kerültek az iparhoz és a vízellátáshoz kapcsolódó szektorokban. Ezen a területen nemzeti szempontból azon infrastruktúrák

kritikusak, amelyek kiesése, működéscsökkenése közvetlenül van hatással a társadalom életére.

A honvédelem, a haderő esetében kritikus infrastruktúrákat megítélésünk szerint alapvetően a műveleti rendszerek képeznek, a mindennapi működéshez kapcsolódó igazgatási rendszerek károsodásai kevéssé jelentenek közvetlen veszélyt a társadalmi, gazdasági és mindennapi élet folyamataira. A műveleti rendszerek veszélyeztetése ezzel szemben a katonai erőt, katonai képességeket és ezzel az ország védelmi képességét fenyegeti. A műveleti rendszerek alapvető adatbázisai közé mindenekelőtt a helyzetismeret adatbázisok tartoznak, amelyeknek részét képezik a térbeli helyzetinformációk időben lassan változó részét tartalmazó térképészeti adatbázisok, a mobil objektumok helyzetét tartalmazó 'nyomvonal' adatbázisok, valamint a leíró helyzetinformációkat tartalmazó hagyományos adatbázisok [87]. A katonai informatikai rendszerek adatbázisainak támadásai elsősorban akkor tekinthetők kritikus infrastruktúra fenyegetésnek, amikor az adott erők az ország védelmében vesznek részt.

A rendvédelmi területen számos olyan adatbázis található, amelynek működőképessége és hitelessége a különböző – bűnügyi, közrendvédelmi, határrendészeti, közlekedésrendészeti – szakterületek tevékenységének alapvető feltétele. Ezen adatbázisok közé sorolhatóak például a különböző bűnügyi nyilvántartások (bűntettesek, büntetőeljárás alatt állók, körözöttek, fogvatartottak, ujj és tenyérnyomatok, fényképek, stb.), a közlekedésrendészeti nyilvántartások (vezetői engedélyek, járművek tulajdonosai, stb.), valamint a határforgalom ellenőrzési és idegenrendészeti nyilvántartások.

Az **infokommunikációs szolgáltatások** a kritikus infrastruktúrák egyik legfontosabb területét képezik. Ide tartoznak a vezetékes és mobil távközlési hálózatok, a műholdas és a rádiós távközlés és navigáció, az Internet hálózat, a műsorszóró hálózatok, a postai szolgáltatások. A korábban már említett szektorokhoz is kapcsolódnak a kormányzati (és védelmi) zártcélú hálózatok, valamint az automatikai és ellenőrző rendszerek.

A távközlési hálózatok esetében témánk szempontjából elsősorban a működés során felhasznált adatbázisok érdekesek. A mobil hálózatok működése alapvetően az előfizetői adatbázisokra épül, amelyek sérülése lehetetlenné teszi a szolgáltatást. Napjainkban már a vezetékes telefonközpontok is számos működéstámogató adatbázist használnak. A helymeghatározó, illetve műsorszóró hálózatokban, valamint a postai szolgáltatások esetében viszont az adatbázisok nem játszanak jelentős szerepet.

Az Internet hálózatokban működési szempontból elsősorban az útvonalválasztó adatbázisok (routing táblák) és a tartománynév (DNS) adatbázisok játszanak kritikus szerepet. Amennyiben tágabban értelmezzük, akkor számos internetes szolgáltatás (elektronikus levelezés, valósidejű társalgás, online játékok, stb.) elsősorban a felhasználókra vonatkozó információkat tartalmazó adatbázisait is ide sorolhatjuk.

Egyes infokommunikációs szolgáltatások esetében tehát az alapvető, többnyire sajátos technológiájú működési adatbázisok jelentős szerepet játszanak, sérülésük, meghamisításuk a szolgáltatások jellegéből következően országos méretű hatással jár.

Az előzőekben foglaltak alapján megállapítható, hogy a kritikus infrastruktúrákban előforduló adatbázisok a következő nagyobb csoportokba sorolhatóak: a közhiteles nyilvántartások; a folyamatirányítási, rendszerirányítási, illetve a felügyeleti és adatgyűjtő (SCADA) rendszerek jellemzően helyzetismeret-adatbázisai; valamint egyes hagyományos relációs, esetleg objektum-orientált (pld. egészségügyi, pénzügyi/banki) adatbázisok.

2.3 KRITIKUS ADATBÁZISOK ÉS AZONOSÍTÁSUK

A szakterületenkénti áttekintések, értékelések alapján megállapíthatjuk, hogy a kritikus infrastruktúrákban vannak olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisok megnevezésére – legalábbis a kritikus infrastruktúra védelem vonatkozásában – javaslom bevezetni a **kritikus adatbázisok** kifejezést. Az ebbe a csoportba tartozó adatbázisok meghatározásához először az érintett infrastruktúra kritikus jellegét, majd ezen belül az adott adatbázis működéskritikus (mission critical) jellegét kell meghatározni.

A kritikus infrastruktúrák azonosításának kérdéseiről már az előzőekben esett szó. A következőkben a kritikus infrastruktúra egy szeletének, a kritikus adatbázisoknak az azonosítási lehetőségeit tekintem át két különböző nézőpontból két különböző módszer meghatározásával a [FR6] publikációm alapján.

A kritikus infrastruktúrákban létezhetnek olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisokat a kritikus infrastruktúra védelem vonatkozásában kritikus adatbázisoknak nevezzük. A kritikus adatbázisok azonosításának első módszere a kritikus szolgáltatások középpontba állítására épül, ahol a kritikus adatbázisok meghatározásának javasolt módszere a következő lépéseket tartalmazza:

1. lépés: Az előzőekben leírtak alapján össze kell állítani a kritikus szolgáltatásokat tartalmazó kritikus infrastruktúra listát. A szolgáltatásokhoz minőségi jellemzőket kell rendelni és ezek segítségével kijelölni azt a szintet, melyet a kritikus infrastruktúra védelem meghatározása által biztosítani szükséges.

2. lépés: A kritikus infrastruktúra lista minden szolgáltatásához meg kell határozni a kritikus elemeket, melyek az adott szolgáltatáshoz szükségesek, azaz a működtető személyzetet, folyamatokat, rendszereket, létesítményeket és eszközöket. Ebben a lépésben kell feltárni azt is, hogy a kritikus infrastruktúra mögött áll-e kritikus információs infrastruktúra.

3. lépés: Az adott szektor kritikus szolgáltatásai mögött álló adatbázisok azonosítását el kell végezni. Az adatbázisokat kritikusság szerint priorálni kell. Azaz meg kell vizsgálni, hogy az adatbázis kiesése milyen mértékű sérülést okoz a szolgáltatás működésében. Itt figyelembe kell venni a szolgáltatás esetében meghatározott szükséges minimális szintet. Ehhez viszonyítva kell nézni, hogy teljes, részleges vagy nem számottevő akadályoztatást okoz az adatbázis kiesése, ezt egy 3-4 fokozatú skálán érdemes nyilvántartani. Az adatbázis sérülés persze jelenthet részleges vagy teljes kiesést az adatbázis-biztonsága szempontjából, de javasoljuk a teljes kieséssel való számolást. Az adatbázis-biztonságának sérülése bekövetkezhet az integritás, bizalmasság vagy rendelkezésre állás megsértése által [68].

Kritikus adatbázisok azonosítása után fel kell tárni a reális fenyegetéseket és sérülékenységeket, majd kockázat elemzéssel egybekötve meg kell határozni az adatbázis-biztonságát garantáló védelmi módszereket.

A második módszer egy másik nézőpontból vizsgálja a kérdést. Nem a szolgáltatásból, illetve annak kritikusságának megközelítése felől indul el, hanem magából az adatbázisból, illetve az abban nyilvántartott adatokból. Ebben az esetben feltételezhetünk egy olyan helyzetet, amikor is a nyilvántartást fenntartó szervezetnek kell döntést hoznia az adatbázis kritikussága felől. A következő fontos jellemzőket célszerű megvizsgálni:

1. Az adott adatbázis hány különböző szolgáltatás számára szolgáltat adatokat.

Ennek a kérdésnek a megválaszolásakor szükséges tisztában lenni azzal, hogy mit tekintünk különböző szolgáltatásnak. Meg lehet vizsgálni azt is, hogy hány különböző kritikus infrastruktúra szektor szolgáltatásához biztosít adatokat az adott adatbázis. Ezeknek a kérdéseknek a megválaszolása sok esetben túlmutathat az adatbázis adminisztrátorának a feladatkörén, tudásán.

2. Az adatbázisban tárolt adatokat használó szolgáltatások mennyire kritikusak.

Ennek a kérdésnek a megválaszolása visszavezet az előzőkben kifejtett problémára, azaz a kérdés viszonylag gyorsan eldönthető, ha rendelkezünk kritikus szolgáltatások listájával. Amennyiben nem létezik ilyen lista, akkor az adatbázis kritikusságát meghatározó szervezetnek kell dönteni az adatokat használó szolgáltatás kritikusságáról. E lépés nélkül az adatbázis kritikusságát meghatározni nem célszerű.

3. Az adatbázisban tárolt adatok sérülése, elérhetetlensége a kapcsolódó szolgáltatásban milyen mértékű kárt okoz.

Ennek a kérdésnek a vizsgálatánál a közvetlen károk mellett a közvetett károk felmérésére is figyelni kell. A szolgáltatások egymással kölcsönhatásban állnak, köztük kölcsönös függés – idegen szóval interdependencia – állhat fenn. A károkozás minősítését egy 3-4 fokozatú skálán érdemes nyilvántartani.

4. Az adatbázis kiesése a teljes kezelt adatok mekkora részét érinti.

Ennek a kérdésnek a megválaszolása talán a legegyszerűbb a négy kérdés közül. Például osztott adatbázis rendszerek esetén egy adatbázis sérülésekor vizsgálni lehet, hogy a sérült adatbázisban tárolt adatok száma hogyan viszonyul a teljes rendszerben megtalálható adatokéhoz.

Az adatbázis kritikusságának felmérését tehát nem vezethetjük le csupán mennyiségi adatokból (tárolt adatok száma, adatbázis mérete, adatok változásának gyakorisága), hanem itt is a sérülés következményét kell áttekinteni, figyelembe venni. Ugyanakkor valószínűsíthető, hogy a tárolt adatok számának nagysága, az adatok változásának sűrűsége gyakran összefügg a védelem nehézségével, a veszélyeztetés könnyebb lehetőségével, ezáltal az adatbázis kritikusságával is.

Az irodalomban nem találtam példát az eredeti kérdés, azaz az adatbázis kritikusságának megválaszolását illetően. A fenti négy kérdés valószínűleg nem teljes, ugyanakkor észrevehető, hogy segítségükkel – a megfelelő analógiát használva – tetszőleges informatikai rendszer kritikusságának vizsgálata is megfogalmazható. Az adatbázisok felöli kritikusság meghatározás a gyakorlat szempontjából fontos (főleg a jelenlegi helyzetben, mikor még nem létezik kritikus infrastruktúra lista), ám észrevehető, hogy sok tekintetben visszavezet az 1. módszer folyamatára.

2.4 KÖVETKEZTETÉSEK

A fejezetben először a kritikus infrastruktúrák fogalmi kérdéseit tekintettem át, majd a kritikus infrastruktúrák azonosításának módszereivel foglalkoztam. A kritikus infrastruktúra azonosítás végterméke egy vagy több kritikus infrastruktúra lista, mely a védelem tárgyait tartalmazza. Hazánkban még nem került sor kritikus infrastruktúra lista megalkotására, ezért külföldi példákat vizsgáltam meg az azonosítás rendjére vonatkozóan.

Megállapítottam, hogy Magyarországon szükség van egy kormányzati hatáskörű központi szervre, mely a kritikus infrastruktúra védelem koordinációjáért felel. A kritikus infrastruktúra lista létrehozását a központi szervnek kell irányítania, koordinálnia, és a végleges listát felállítania. A kritikusságnak különböző fokozatai léteznek, ezért a kritikus infrastruktúra lista létrehozását meg kell, hogy előzze a kritikusság mértékét leíró kritériumoknak a megadása.

A kritikus infrastruktúra lista elemeinek típusát, tartalmi szerkezetét is meg kell határozni. Ennek kapcsán értekezésemben a következő javaslatot fogalmaztam meg. A kritikus infrastruktúra lista készítésének első fázisában a kritikus szolgáltatásokat határozzuk meg és szolgáltatásokként azt a minimális szintet, amivel a szolgáltatásnak még vészhelyzetben is működnie kell. A következő fázis feladata az adott szolgáltatáshoz és minimális működési jellemzőhöz felsorolni azokat a létesítményeket, szolgáltatásokat, személyzetet, folyamatokat, rendszereket és eszközöket, amik a meghatározott működéshez szükségesek.

Az értekezésben feltártam az adatbázisok általános helyét és szerepét a különböző kritikus infrastruktúra szektorokban. A kritikus infrastruktúrákban előforduló adatbázisokat a következő nagyobb csoportokba soroltam be: közhiteles nyilvántartások; folyamatirányítási, rendszerirányítási, illetve a felügyeleti és adatgyűjtő (SCADA) rendszerek jellemzően helyzetismeret-adatbázisai; valamint egyes hagyományos relációs, esetleg objektum-orientált (pld. egészségügyi, pénzügyi/banki) adatbázisok.

Megállapítottam, hogy számos infokommunikációs szolgáltatás esetében az alapvető adatbázisok jelentős szerepet játszanak, sérülésük, meghamisításuk országos méretű hatással jár. A kritikus infrastruktúrákban vannak olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisok megnevezésére javasoltam bevezetni a kritikus adatbázisok kifejezést.

A kritikus adatbázisok azonosítása kapcsán két módszert különböztettem meg. Az első módszer a kritikus szolgáltatások középpontba állítására épül. Eszerint azonosítani kell az adott kritikus szolgáltatás mögött álló adatbázisokat, majd el kell végezni ezek kritikusság

szerinti priorálását. A második módszer nem a szolgáltatásokból, illetve azok kritikusságának megközelítésből indul ki, hanem magából az adatbázisból, illetve az abban nyilvántartott adatokból és ezek tulajdonságaiból.

3 AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁS KERETEI A MAGYAR KÖZIGAZGATÁSBAN

BEVEZETÉS

Napjainkban a kormányzati tevékenység törekvése az elektronikus működés kiterjesztése, e-kormányzati megoldások, szolgáltatások bevezetése és széleskörűvé tétele. A hagyományos kormányzati működési folyamatokban jelentős szereppel bírnak központi, ágazati, illetve intézményi nyilvántartások, illetve az elektronikus kormányzatban a nyilvántartások elektronikus változatai, az adatbázisok.

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 kritikus infrastruktúrákban az adatbázisok biztonságának védelme fontos feladat, ezért érdemes az adatbázis-biztonság szabályozási lehetőségeit vizsgálni. Kutatásomban áttekintettem az adatbázis-biztonság állami szabályozásának kereteit, lehetőségeit. Az informatikai biztonság - és ennek részterülete az adatbázis-biztonság - állami szabályozása a közigazgatás szereplőire és a kritikus infrastruktúrákra vonatkozóan lehet kényszerítő eszköz. Mivel a közigazgatás egyike a kritikus infrastruktúra szektoroknak, a részét képező elektronikus kormányzat pedig kritikus információs infrastruktúrának minősül, értekezésemben az adatbázis-biztonság magyar közigazgatáson belüli szabályozásának lehetőségeit elemeztem. Az elvégzett vizsgálatok a későbbiekben, a kritikus infrastruktúra biztonságának szabályozásában is felhasználhatóak.

A fejezet célja az adatbázis-biztonság szabályozás jelenlegi helyzetének, kereteinek feltárása a magyar közigazgatásban. A felvázolt kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Elemeztem a magyar elektronikus kormányzat felépítését és ebben az adatbázisok helyét,

szerepét; feltártam az országos alapnyilvántartásokat vezető központi szerv szerepét.

– Megvizsgáltam az informatikai biztonság szabályozás jelenlegi helyzetét a magyar közigazgatásban, feltártam a szervezeten belüli informatikai-, és adatbázis-biztonsági dokumentumok, szabályozók és szerepkörök kapcsolatrendszerét, majd elemeztem - mint egy lehetséges modellt-, az USA haderejében kifejlesztett adatbázis-biztonsági szabályozást.

3.1 ADATBÁZISOK A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁSBAN

Az elektronikus kormányzatnak fontos részét képzik a központi elektronikus nyilvántartások, adatbázisok, ezek között találunk lényeges számú kritikus adatbázist is. Az adatbázis- biztonság központi szabályozásának a közigazgatásban jelen kell lennie és a központi adatbázis-biztonság szabályozás különböző alkotóelemeit meg kell határozni.

A következőkben elemzem a magyar elektronikus kormányzat felépítését és ebben az adatbázisok helyét és típusait; feltárom az országos alapnyilvántartásokat és az ezeket vezető központi szerv szerepét és értékelem az adatbázis sérülések és következményeinek hatását a [FR6], [FR8] publikációim alapján.

3.1.1 A MAGYAR ELEKTRONIKUS KORMÁNYZAT FELÉPÍTÉSE

A közigazgatás azon szerveztek összessége, amelyek közhatalmat gyakorolva, az állam vagy az önkormányzat nevében közfeladatokat látnak el és jogszabályokat hajtanak végre. A helyi közügyekben az önkormányzati igazgatás, az országos jelentőségű ügyekben a központi közigazgatás jár el. A központi közigazgatást államigazgatásnak nevezzük [88]. A közigazgatás az állam feladatainak megvalósításában vesz részt, folyamatait igazgatási, rendvédelmi, honvédelmi, környezetvédelmi, oktatási, szociális, kulturális, egészségügyi és gazdasági funkciókra oszthatjuk fel [89], [90].

Az elektronikus kormányzattal (vagy e-kormányzattal) kapcsolatosan különböző fogalmak, kifejezések terjedtek el. A magyar nyelvben az elektronikus közigazgatás és az elektronikus kormányzat fogalmai összemosódtak, egymás szinonimájaként használatosak. Az elektronikus közigazgatás két területet foglal magába, az elektronikus önkormányzást és az elektronikus államigazgatást, vagy más szóval elektronikus központi kormányzást. A témához kapcsolódó, fontos fogalom még az elektronikus közszolgáltatás, mely az állam által nyújtott, az állampolgárok és vállalkozások számára elektronikus úton elérhető szolgáltatásokat foglalja magába [91]. Kutatásomban a központi kormányzat vizsgálatát helyeztem előtérbe

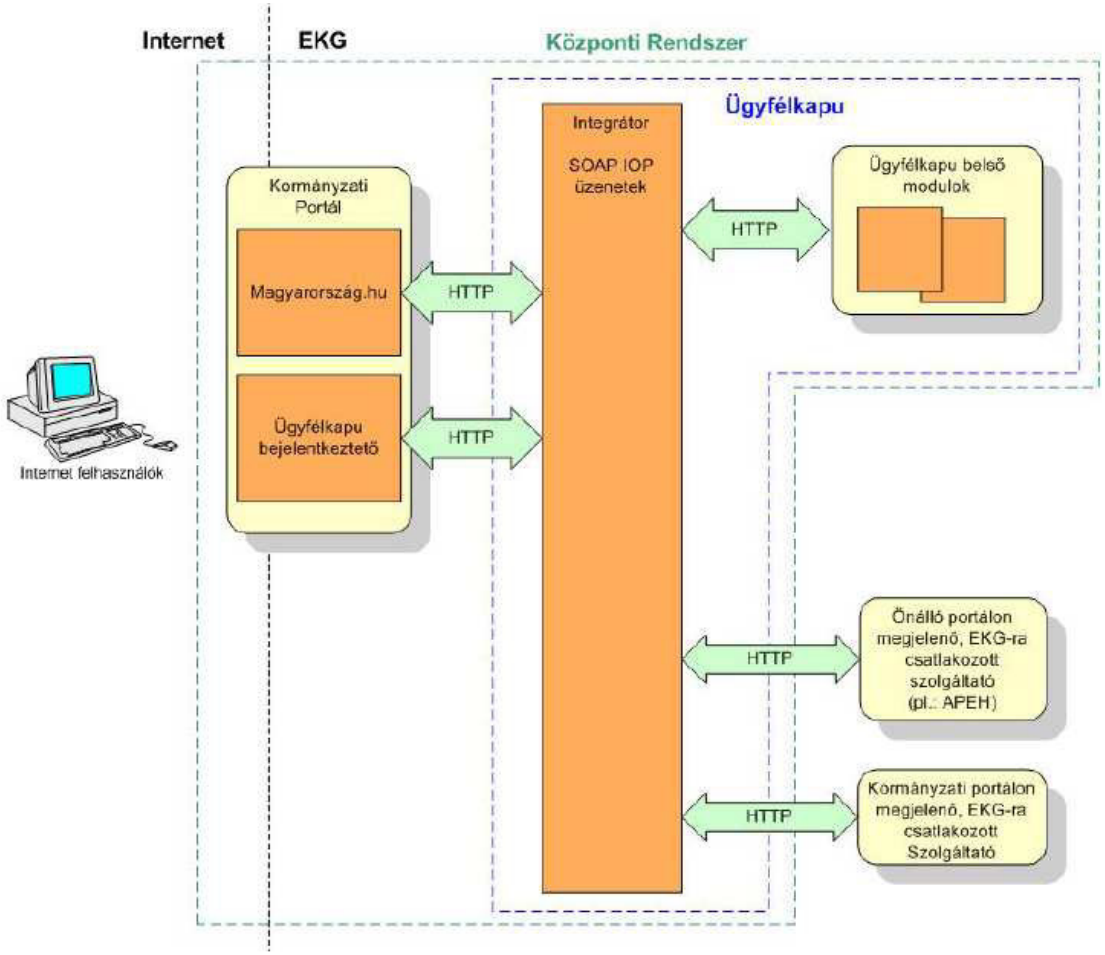
(ide tartoznak a minisztériumok, költségvetési szervek, közfeladatot ellátó gazdálkodó szervek), ezért értekezésemben az elektronikus kormányzat fogalmát szűk értelemben használom.

A korszerű elektronikus közigazgatás kettős feladatrendszerrel rendelkezik. Egyrészt biztosítja a lakosság és a vállalkozások számára az elektronikus ügyintézés lehetőségét, másrészt a közigazgatás számára hatékony, informatikailag támogatott hivatali működést tesz lehetővé. Ennek megfelelően az elektronikus kormányzat alapvetően két összetevőből áll: egyrészt az állampolgárokkal kapcsolatos ügyintézést, kapcsolattartást támogató rendszerekből (front office), másrészt a közigazgatási intézmények háttérfolyamatait, belső működését támogató informatikai rendszerekből és munkafolyamatokból (back office). A kritikus adatbázisok elektronikus kormányzás folyamatában betöltött helyének és szerepének elemzéséhez a következőkben felvázolom az e-közigazgatás informatikai alapjait.

Az elektronikus kormányzat egyik legfontosabb eleme a központi elektronikus szolgáltató rendszer (KR), mely a front office jellegű szolgáltatások alapját, keretrendszerét adja. Ez a következő részekből épül fel [91]:

- Elektronikus kormányzati gerinchálózat (EKG): az alapinfrastruktúrát biztosítja a felek kommunikációjához és együttműködéséhez;
- Kormányzati portál (magyarorszag.hu): alapvető feladata a tájékoztatás és az elektronikus közszolgáltatások nyújtásának központi kiinduló felületének nyújtása,
- Kormányzati ügyfél-tájékoztató központ (KÜK): teljes körű és szakszerű tájékoztatásra törekszik, és segít a közigazgatási ügyekben való eligazodásban a magyar állampolgároknak, szervezeteknek és külföldieknek egyaránt,
- Elektronikus ügyfélkapu: az ügyfél azonosítását végzi a KR-ben,
- Hivatali kapu: a csatlakozott közigazgatási szervek közötti, illetve a szervek és a hitelesen azonosított ügyfelek közötti elektronikus üzenetcserének lebonyolítását segíti (off-line ügyintézés).

A következő ábra az ügyfélkapu elhelyezkedését mutatja meg a központi rendszeren belül:



10. ábra: Az ügyfélkapu elhelyezkedése a KR-ben [92]

A KR-hez csatlakozó közigazgatási szerv informatikai rendszere és a KR között mindig kiépül egy biztonságos hálózati kapcsolat, amelynek a célja a rendszerek közötti titkosított és azonosított kommunikáció biztosítása. A kapcsolat vagy az EKG hálózatán, vagy az internet felől titkosított VPN/SSL interfészen keresztül épülhet fel.

Az ügyfél az egyes elektronikus szolgáltatást internetes böngészőn keresztül érheti el. A csatlakozott szervezet szolgáltatását az ügyfél indíthatja a csatlakozott szervezet honlapjáról vagy a kormányzati portálról is attól függően, hogy csak az egyik vagy mindkettő helyen megtalálható-e a szolgáltatás linkje. Mindkét esetben az ügyfél böngészője átirányításra kerül az ügyfélkapu bejelentkezési oldalára, majd sikeres bejelentkezés után elirányításra kerül a szolgáltatás oldalára, ahol az ügyfél a kívánt ügyintézést lebonyolíthatja.

Az elektronikus ügyintézés történhet online vagy offline módon. Az online elektronikus ügyintézés során folyamatos kapcsolat áll fenn az ügyfél és a csatlakozott szervezet informatikai rendszere között. Az offline elektronikus ügyintézés elektronikus dokumentum alapú kommunikációval valósul meg, azaz a kommunikáció és a feldolgozás időben elkülönül egymástól. Az ügyfél elektronikus dokumentum alapú kommunikációt folytat a szolgáltatást

nyújtó (csatlakozott) szervezettel a KR-en keresztül. Az ügyfél által küldött dokumentumok az ügyfélkapun keresztül kerülnek betöltésre a KR-be. A csatlakozott szervezet az elektronikus dokumentumok fogadását és a válaszdokumentumok küldését a hivatali kapun keresztül valósítja meg.

A közigazgatási szerv tehát nyújthat elektronikus szolgáltatást vagy a kormányzati portálon keresztül vagy saját portálon keresztül (esetleg mindkettőn). Az elsőre példa a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, a másodikra pedig az APEH elektronikus bevallás szolgáltatása; vagy az OEP TAJ szám ellenőrzése, illetve betegéletút lekérdezése. A szolgáltatásnyújtók jelentős része saját portálon keresztül csatlakozik az ügyfélkapuhoz [92].

A back office az intézmények háttérfolyamatait támogató rendszerekből áll, ezek az ügyfél szempontjából a „háttérben" futnak és a front office feltételét, hátterét adják. Mondhatjuk azt is, hogy a front office közvetíti a back-office által feldolgozott, kezelt adatokat. A közigazgatási szerv informatikai rendszerének (back office) feladatai közé tartozik (1) az egyéneknek, vállalkozásoknak, civil szervezeteknek történő elektronikus szolgáltatások nyújtása, (2) a közigazgatási intézmények közötti adatcserének, kommunikációnak a lehetőségét biztosítása, (3) saját munkafolyamatainak támogatása [91].

Az elektronikus közszolgáltatásoknak, illetve a közigazgatási szerv informatikával támogatott folyamatainak szükséges és alapvető feltétele az adatoknak, nyilvántartásoknak elektronikus tárolása, mely leggyakrabban adatbázisok segítségével valósul meg. Az áttekinthetően és hatékonyan működő központi adatbázisok megléte az elektronikus közigazgatás alapvető eleme. A közigazgatás adatbázisai lényeges részét alkotják a teljes elektronikus kormányzati rendszernek, ebből dolgozik mind a háttér rendszer (back office), mind az ügyfeleket kiszolgáló részrendszer (front office) is.

A jogszabályok által meghatározott kereteken belül a nyilvántartásoknak összekapcsolhatónak, átjárhatónak, egymással együttműködően kell működniük ahhoz, hogy magasabb szintű közigazgatási szolgáltatások jöhessenek létre. Magyarországon a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) értelmében az ügyfélnek nem kell a hivatalok között ingáznia különböző adatokért. Ha az adatok már szerepelnek valamely állami, illetve önkormányzati adatbázisban, akkor az állampolgár ismételten nem kötelezhető a beszerzésükre. Ezt a követelményt „egy adatot csak egyszer megadni" elvnek is nevezik. A kormányzati adatbázisok közötti átjárhatóság, összeköttetés szükséges feltétele az ügyfelek részére nyújtott eredményes

szolgáltatásoknak, a közigazgatási szervek egymás közötti hatékony kommunikációjának, és egészében véve a jó kormányzásnak [91].

A közigazgatás adatbázisainak egyik csoportját az alapnyilvántartások alkotják, amelyek az adott területen (vagy az ország területén) élő személyek, szervezetek, események adatait tárolják el. A másik csoportba az ágazati, vagy szakági rendszerek tartoznak, amelyek az adott szakterület (tárca) funkcióihoz igazodnak, a szakterületi informatikai rendszerek szerves részét képezik. Az adatbázisok amellett, hogy nyilvántartják a tárolt entitások adatait, döntéstámogatási eszközként is szolgálnak, illetve lehetővé teszik az adatok elemzését, statisztikai célú felhasználását is. A nyilvántartás tárgya szerint beszélhetünk személyi (pl. polgárok személyi adatai), dologi (pl. ingatlan, gépjármű, közmű), szellemi javak (pl. szabadalmak), illetve jogszabályok nyilvántartásairól.

A közigazgatásban jelenlévő nyilvántartások egyik fontos típusa a közhiteles nyilvántartás. Közhiteles nyilvántartás vezetését mindig jogszabály írja elő, azt hatóság vezeti és tartalmát, a benne szereplő adatok valódiságát az ellenkező bizonyításig mindenki köteles elfogadni. A helyesség bizonyítása elsődlegesen nem a hatóság feladata. A bizonyítást annak kell kezdeményezni, aki kétségbe vonja, ill. támadja a nyilvántartás tartalmának helyességét. Közhiteles nyilvántartásra példa a cégnyilvántartás, a polgárok személyi és lakcím adatait tartalmazó nyilvántartás vagy az ingatlan nyilvántartás.

Kritikus szolgáltatások és kritikus adatbázisok azonosítása a közigazgatásban

A kritikus infrastruktúrákban, így a kormányzati szektorban is léteznek olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisokat a közigazgatás kritikus adatbázisainak nevezzük. A védelem szempontjából alapvető feladat a kritikusnak minősíthető szolgáltatások és a mögöttük álló létfontosságú adatbázisok meghatározásának folyamata. A következőkben a kormányzati kritikus infrastruktúra szektorban a kritikus szolgáltatások és kritikus adatbázisok azonosításának lehetőségeit vizsgáljuk.

A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló Kormányhatározatban [50] a kritikus infrastruktúra szektor neve Jogrend – Kormányzat, mely három alszektort foglal magában, melyek a 1) kormányzati létesítmények, eszközök, 2) közigazgatási szolgáltatások, 3) igazságszolgáltatás. Fontos és egyben bonyolult feladat a kormányzati szektor feladatkörének behatárolása, mivel az összes többi szektorhoz tartoznak kormányzati funkciók, ugyanakkor szerencsés lenne egymást nem átfedő hatókörrel rendelkező szektorok

felállítása. Egy kis túlzással „maradék” szektornak is lehet a kormányzatit tekinteni, mivel azokat a kritikus infrastruktúra elemeket tartalmazza, melyek a többi szektorba nem férnek bele.

A Zürichi Biztonsági Tanulmányok Központja által kiadott, a nemzetközi kritikus információs infrastruktúra védelemről szóló kézikönyv [69] javasolja, hogy a szektorok és az azokon belüli alszektorok felállítása után meg kell határozni az alszektorok alapfunkcióit, csak ezután lehetséges a kritikus erőforrások azonosítását elvégezni, ugyanis azok az alapfunkcióktól függnek. Ez az elv a kormányzati szektorban is egy fontos feladatot határoz meg. A kormányzat alapfunkciói összefüggnek a társadalom alapértékeinek meghatározásával, mivel a kritikus infrastruktúra védelem feladata ezen értékek fenntartása egy szükséges minimális szinten. Az alapértékek közé tartoznak 1) az állampolgárok és a terület védelme, 2) a politikai függetlenség és autonómia védelme és 3) a nemzeti gazdasági biztonság megvédése [68].

Napjainkban az állam szerepének, feladatkörének hangsúlyváltozása megy végbe, új célként a szolgáltató állam kialakulása jelenik meg, melyet a szolgáltatás orientáltság, a polgárok igényeinek kiszolgálása jellemez. Az eKormányzat stratégia középpontjában is a szolgáltató állam megvalósítása áll. Ezek a folyamatok is alátámasztják, hogy a kormányzati kritikus infrastruktúra lista első lépéseként a kritikus szolgáltatások (illetve az ezekért felelős intézmények) meghatározását javasoljuk. Egy kormányzati szolgáltatás kritikusnak minősíthető, ha hozzájárul az alapértékek fenntartásához, vagyis szükséges a 1) nemzeti és nemzetközi jog és rend, 2) közbiztonság, 3) gazdasági termelés, 4) közegészség, 5) ökológiai környezet védelmének fenntartásában vagy 6) elvesztése vagy sérülése a polgárokat vagy a kormányzati folyamatot nemzeti szinten érintheti [68].

A kritikus kormányzati szolgáltatások meghatározása történhet a következő folyamat alapján. Először a kormányzati szektor szolgáltatásainak listáját készítjük el, melyben minden szolgáltatáshoz egyedileg minőségi jellemzőket és ezek segítségével szolgáltatási szinteket jelölünk ki. Javasolunk 3-4 szintet meghatározni, melyben a két szélső az adott szolgáltatás minimális működési szintje, illetve a tökéletes működési szintje. A minimális működési szint a szolgáltatás kritikusságát határozza meg azáltal, hogy a szolgáltatás teljes megszűnését írja le, ha a szolgáltatás nem kritikus, kritikus esetben pedig működéstől elvárt, szükséges minimális szintet.

A kormányzati szektor kritikus adatbázisainak azonosítása az értekezés előző fejezetében tárgyalt két módszer szerint történhet, azaz vagy a kormányzati kritikus szolgáltatásokból

levezetve, vagy pedig az adatbázisban tárolt adatok jellegéből kiindulva. Az utóbbi esetben is mindenképp szükséges az adatokat felhasználó szolgáltatások vizsgálata.

3.1.2 KRITIKUS ADATBÁZISOK A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁSBAN

Az előzőekben lefolytatott elméleti alapozás után megvizsgálom, hogy hazánkban a kritikus adatbázisok meghatározása kapcsán milyen intézkedések születtek. A minősített információkat feldolgozó informatikai rendszerek, adatbázisok biztonsági kérdései (elvárásai, követelményei, engedélyezése) a Nemzeti Biztonsági Felügyelet hatókörébe tartoznak, ennek a témának a tárgyalását nem tekintem értekezésem tárgyának.

A nemzeti adatvagyon

A nemzeti adatvagyon körébe tartozó nyilvántartások fokozott biztonságának és a közigazgatás folyamatos és zavartalan működésének biztosítása érdekében született a 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről [93]. A törvény értelmében nemzeti adatvagyonnak minősülnek a közfeladatot ellátó szervek által kezelt közérdekű adatok, a személyes adatok és a közérdekből nyilvános adatok. A közigazgatás kritikus adatbázisai és a nemzeti adatvagyon között szoros kapcsolat feltételezhető, a nemzeti adatvagyon nyilvántartásai kritikus adatbázisoknak tekinthetők.

A törvény kimondja, hogy a nemzeti adatvagyon részét képező nyilvántartásokra vonatkozóan korlátozni lehet az adatfeldolgozást végző szervek vagy szervezetek körét, és meghatározott nyilvántartások esetében az adatfeldolgozást csak államigazgatási szerv vagy kizárólagos állami tulajdonú gazdálkodó szervezet láthatja el. Ilyen esetben az adatkezelő kizárólag az adott nyilvántartás tekintetében meghatározott szervet vagy szervezetet bízhat meg adatfeldolgozással. Ezen nyilvántartások, illetve az adatfeldolgozást végző szerv vagy szervezet meghatározása a 38/2011. (III. 22.) kormányrendeletben történik [94].

Az adatfeldolgozás típusa szerint a rendelet megkülönböztetheti az elektronikus, illetve nem elektronikus adatfeldolgozást. Elektronikus adatfeldolgozásnak minősül az elektronikus úton vezetett nyilvántartás létrehozásának, működtetésének, üzemeltetésének és fejlesztésének folyamata. Elektronikus úton vezetett nyilvántartások esetén az adatok tárolása leggyakrabban adatbázisok segítségével valósul meg, tehát a nemzeti adatvagyon védelme és az adatbázis-biztonság megvalósítása között szoros kapcsolat áll fenn. A nyilvántartások listája alapján látható, hogy a közigazgatás biztonsága számos helyen veszélyeztethető adatbázisok támadásán keresztül.

A törvény kimondja, hogy elektronikus adatfeldolgozás esetén a minősített adatnak nem minősülő adatok feldolgozásánál az informatikai rendszert a „Korlátozott terjesztésű!" minősítési szintű adatot kezelő rendszernek kell tekinteni és ennek megfelelően kell a személyi, fizikai, adminisztratív és elektronikus biztonsági követelményeket alkalmazni. Továbbá az elektronikus adatfeldolgozást végző adatfeldolgozó az elektronikus adatfeldolgozás során bekövetkezett biztonsági eseményekről köteles az érintett adatkezelőt tájékoztatni. A törvény szerint, aki a nemzeti adatvagyon nyilvántartásainak adataihoz történő hozzáférést vagy az adatkezelés más műveletét akadályozza, az bűntettet követ el és szabadságvesztéssel büntetendő.

A törvényhez szorosan kapcsolódó 38/2011. (III. 22.) számú kormányrendelet a nemzeti adatvagyon részét képező állami nyilvántartásokat, azok adatfeldolgozóinak körét, illetve az adatfeldolgozó igénybevételének kötelező vagy az adatkezelő döntésétől függő jellegét határozza meg. A rendelet a következő 23 nyilvántartást sorolja a nemzeti adatvagyon körébe:

1. A polgárok személyi adatainak és lakcímének nyilvántartása
2. Központi útiokmány-nyilvántartás
3. Központi szabálysértési nyilvántartás
4. Közúti közlekedési nyilvántartás
5. A Magyar igazolvány és a Magyar hozzátartozói igazolvány tulajdonosainak nyilvántartása
6. Cégnyilvántartás
7. Központi idegenrendészeti nyilvántartás
8. N.SIS
9. Kötvénynyilvántartás
10. Az egyéni vállalkozók nyilvántartása
11. Bűnügyi nyilvántartási rendszer
12. Foglalkoztatási és Szociális Adatbázis
13. Egységes szociális nyilvántartás
14. Az Áht. 124. § (2) bekezdés l) pontjában foglalt felhatalmazás alapján kiadott kormányrendeletben meghatározott nyilvántartások, ide nem értve a Magyar Államkincstár által működtetett kincstári monitoring rendszert (a költségvetésből és az európai uniós forrásból nyújtott támogatásokkal, valamint az államháztartás alrendszereinek felajánlott külföldi segélyek és adományok felhasználásának információs és monitoring rendszereivel kapcsolatos nyilvántartások)

15. Földhasználati nyilvántartás
16. Az állami földmérési alaptérképek, nagyméretarányú állami topográfiai térképek, alapponthálózatok, az államhatár földmérési munkarészei, valamint a magyarországi hivatalos földrajzi nevek nyilvántartása
17. Közepes és kisméretarányú állami topográfiai térképek
18. Nyugdíj-biztosítási nyilvántartás
19. Egészségbiztosítási nyilvántartás
20. Kulturális örökségvédelmi nyilvántartás
21. A Nemzeti Adó- és Vámhivatal által kezelt adóhatósági és vámhatósági adatok nyilvántartása
22. A Nemzeti Adó- és Vámhivatal által kezelt, a 15. pont alá nem tartozó adatok nyilvántartása
23. A mezőgazdasági és vidékfejlesztési támogatási szerv által kezelt nyilvántartási rendszerek

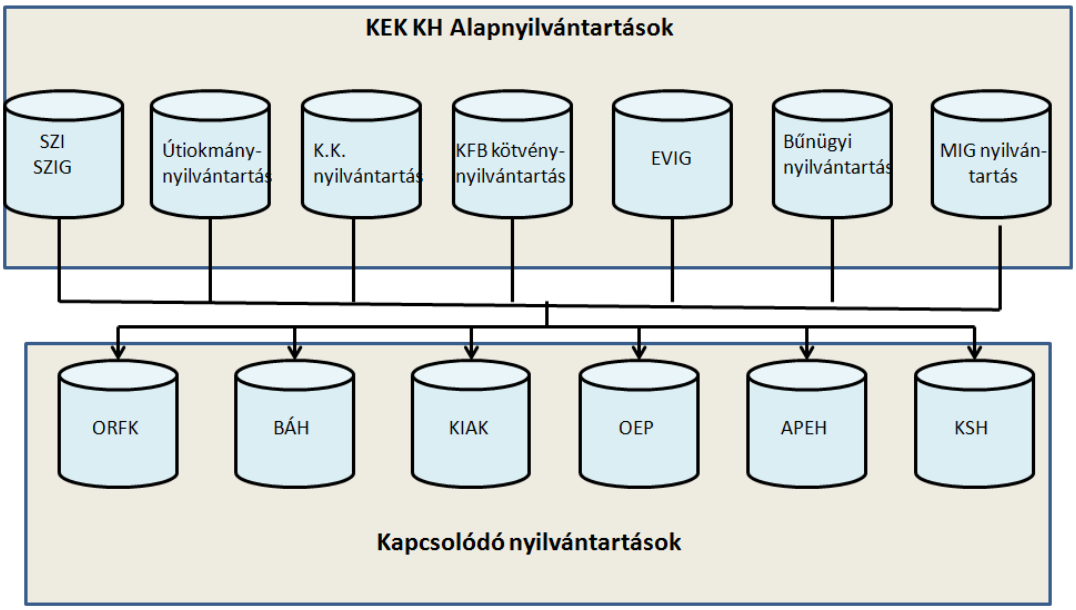
A fenti lista első 11 nyilvántartása esetén a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (a továbbiakban KEK KH) végzi kötelező jelleggel az adatfeldolgozást. Kijelenthetjük, hogy a nemzeti adatvagyon felügyelete tekintetében a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalának kiemelt jelentősége van, illetve az általa kezelt nyilvántartások adják az országos alapnyilvántartások jelentős részét.

Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatal

A Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala 2007. január 1-én jött létre, országos hatáskörű szervezet, székhelye Budapest. A nemzeti adatvagyon részét képező közhiteles nyilvántartások adatkezelőjeként Magyarország közigazgatási intézményrendszerének meghatározó szervezete. Jellemző feladatai közé tartozik a nemzeti adatvagyon kezelése, a nyilvántartások vezetése, a nyilvántartásokból történő adatszolgáltatás szervezetek és magánszemélyek számára, a központi elektronikus nyilvántartásokhoz kapcsolódó közigazgatási és elektronikus szolgáltatások nyújtása, az okmányirodai rendszerek üzemeltetése, választások és népszavazások lebonyolításának informatikai támogatása és a Schengeni Információs Rendszer nemzeti hivatala feladatainak ellátása.

A KEK KH a következő szervek felé bír adatszolgáltatási tevékenységgel (a teljesség igénye nélkül): Országos Rendőr Főkapitányság (ORFK), Bevándorlási és Állampolgársági Hivatal (BÁH), Katonai Igazgatási és Adatfeldolgozó Központ (KIAK), Országos

Egészségügyi Pénztár (OEP), Adó- és Pénzügyi Ellenőrzési Hivatal (APEH) és a Központi Statisztikai Hivatal (KSH). Természetesen jogszabályok rögzítik, hogy az előbb említett szervek mely központi adatbázishoz és annak mely adataihoz férnek hozzá [95]. Az alábbi ábra a KEK KH nyilvántartásainak kapcsolódási pontjait, adatszolgáltatási irányait mutatja be más, közigazgatási szervek által vezetett nyilvántartásokhoz.



11. ábra: KEK KH nyilvántartásaiból történő adatszolgáltatás [96]

Az ábrán látható rövidítések jelentése a következő:

- SZL, SZIG: A polgárok személyi adatainak és lakcímének nyilvántartása
- K.K. nyilvántartás: Közúti közlekedési nyilvántartás
- KFB kötvénynyilvántartás: Kötelező gépjármű felelősségbiztosítási kötvény-nyilvántartás
- EV IG: Egyéni vállalkozói igazolvánnyal rendelkező vállalkozók nyilvántartása
- MIG nyilvántartás: Magyar igazolvány és magyar hozzátartozói igazolvány nyilvántartása

Fenyegetettségek, biztonsági sérülések, kockázat elemzés

A közigazgatás adatbázisaira is érvényes a belső támadás, belső károkozás lehetősége. A külső támadás felületét a rendszerek külső elérései biztosítják, a közigazgatás esetében számos adatbázist az állampolgárok az ügyfélkapun keresztül tudnak lekérdezni, illetve módosítani. Az ügyfélkapu biztonságos működésének egyik korlátja az egylépcsős bejelentkezés (azonosító és jelszó megadásával) [97], mely viszonylag könnyen támadható. 2009 februárjában súlyos incidens történt az ügyfélkapu használatában. Az üzemzavar

következtében az oldalra belépő ügyfelek más személyek és cégek fiókjaiba lettek irányítva, ezáltal mások adatait, APEH-től érkező leveleit látták a sajátjuk helyett [98]. Ez egy igen súlyos biztonsági incidensnek számít, mivel nemcsak a tárolt adatok bizalmasságának kritériuma sérült, hanem mód volt mások adatainak, tehát adatbázisok tartalmának módosítására is, mely az adatok sértetlenségének kritériumát szegte meg. Kijelenthetjük, hogy ebben az esetben kritikus infrastruktúrát ért veszélyeztetés lépett fel.

A közigazgatás adatbázisait kívülről nemcsak az ügyfélkapun keresztül lehet elérni, a nyilvántartások egyéni vizsgálatával más módokat is találunk. Példaként említhető az OEP által vezetett TAJ-nyilvántartás és jogviszonyadatok nyilvántartása. Ezeket az ügyfélkapun kívül az egészségügyi szolgáltatók és gyógyszertárak a VIREP és OJOTE online elérést biztosító rendszerekkel tudják lekérdezni, melyek szintén rejthetnek sebezhetőségeket magukban. 2009 januárjában (hivatalos közlemény szerint szoftver hiba miatt) az OEP jogviszony-nyilvántartási adatbázisa megsérült és jelentős számú lekérdezés esetében hibás jelzést küldött a biztosított jogállásáról. A rendezett jogviszonyú biztosítottak is helytelen igazolást kaphattak, amikor háziorvosuknál, patikákban vagy más egészségügyi ellátónál jelentkeztek. Az adatbázis helyreállításáig a jogosultság ellenőrzést szüneteltették. A hiba miatt sérült a jogviszony-nyilvántartási adatbázis tartalma, de pár napos munkával (feltehetőleg előző mentések visszaállításával) a hibát korrigálni tudták [99]. Ebben az esetben is kijelenthető, hogy kritikus adatbázist ért veszélyeztetés. Az előző példák is mutatják, hogy a kritikus információs infrastruktúrák, ezen belül pedig a kritikus adatbázisok védelme a mai világban egy kiemelt jelentőségű feladat.

Az elektronikus nyilvántartások esetében is a biztonsági sérüléseket feloszthatjuk a bizalmasság, a sértetlenség és a rendelkezésre állás biztonsági tulajdonságok sérüléseire. Ha a közigazgatás elektronikus nyilvántartásainak biztonságát a kritikus infrastruktúra védelem szempontjából vizsgáljuk, akkor a szerző véleménye szerint a három biztonsági tulajdonság közül a bizalmasság sérülése jelenti a legkisebb, bár egyáltalán nem elhanyagolható veszélyt. A kritikus állami (ezen belül közigazgatási) funkciók megvalósítása a bizalmasság sérülése esetén tovább tud működni.

A biztonság szempontjából fő szerepe a rendelkezésre állás és sértetlenség biztonsági kritériumok biztosításának van. A hosszútávú biztonsági célt a rendelkezésre állás biztosítása jelenti, azonban a nyilvántartások adattartalmának sérülése igen veszélyes lehet. Ha az adatok sértetlenségére irányuló támadás kiszámíthatatlan ideig észrevétlen marad, nagyon nehéz a helyes állapotba való visszaállás, még akkor is, ha rendszeres biztonsági mentések készülnek

az adatokról. A támadás észlelése után két kritikus kérdés vár válaszra: (1) mi az utolsó hiteles verzió időpontja, (2) az azóta történt jogszerű módosításokat hogyan lehet újra életbe léptetni.

A rendelkezésre állás megsértése abban az esetben nem jelent kritikus veszélyt, ha bizonyos idő elteltével a nyilvántartások működése újra biztosított, méghozzá sérülésmentes módon. Az időszakos kiesés kellemetlenséget okoz, de a kritikusság sérülésére nincs közvetlen hatással.

Az informatikai védelem módszertana (azaz az informatikai rendszer elemeinek meghatározása, a rendszer sebezhetőségeinek, sérülékenységeinek feltárása, kockázat elemzés, a kockázat elemzés alapján a védelmi intézkedések kiválasztása, védelmi intézkedések megvalósítása) az elektronikus nyilvántartások védelme tekintetében is végigvihető. A kockázat elemzés során egy adott fenyegetés bekövetkezésének valószínűségét és az okozott kár mértékét vizsgálják. Az okozott kár mértékét általában az informatikai rendszer tulajdonosa, az üzemeltető szervezet tudja felmérni, meghatározni.

A közigazgatás, a nemzeti adatvagyon és ezen belül például a KEK KH elektronikus nyilvántartásainak biztonsága szempontjából végrehajtandó kockázat elemzés szempontjából a helyzet lényeges különbséggel bír. Az adatfeldolgozást végző szerv – például a KEK KH - nem tudja a kár nagyságát megállapítani, hisz az a nyilvántartások által szolgált közigazgatási folyamatokban okozott kártól függ. Ezek a folyamatok pedig nem a KEK KH alá tartoznak, hanem a teljes közigazgatás részét, annak szerves vázát alkotják. Tehát igazából a károk nem a KEK KH-ban, hanem a közigazgatás egészében jelentkeznek. A lehetséges károk súlyosságának felmérése így egy sokkal bonyolultabb folyamat része, mintha csupán egyetlen szervezet biztonságának veszélyeztetése állna fenn. Itt párhuzamot lehet vonni a kritikus infrastruktúra védelem egyik nehézségével, a sérülésekből következő károk mérésének nehézségével.

Megállapítható tehát, hogy a nemzeti adatvagyont alkotó elektronikus nyilvántartások kockázat elemzési feladatait nem az adatfeldolgozó szervnek, hanem magának az államnak kell elvégeznie. Szakterületenként kell felmérni a nyilvántartások biztonsági sérüléseinek következményeit, ami igazából nem informatikai, hanem az adott szakterület alá tartozó feladat. Ha a jövőben megalakulna a közigazgatási informatikai rendszerek - esetleg a kritikus infrastruktúra - védelméért felelős központ, akkor a kockázatok felmérését, elemzését célszerű lenne ennek a központnak végrehajtania. Az elektronikus nyilvántartások sérülékenységeinek

felmérése, illetve a védelmi módszerek, eljárások kiválasztása és megvalósítása már az informatikai védelem szakterülete alá tartozik.

A fentiek alapján kijelenthetjük, hogy a közigazgatásban megtalálható számos, kulcsfontosságú szerepet betöltő adatbázis, melyek sérülése, meghamisítása alapvető közigazgatási szolgáltatásokat hiúsít meg, vagy tesz megbízhatatlanná. Számos szolgáltatás hiánya a mindennapi és a gazdasági élet lényeges folyamatainak megvalósulását országos szinten akadályozza. A közigazgatás kritikus adatbázisainak meghatározásához először az érintett infrastruktúra által nyújtott szolgáltatás kritikus jellegét, majd ezen belül az adott adatbázis működéskritikus jellegét kell meghatározni. A kritikusnak ítélt adatbázisok védelmére sajátos biztonsági szabályozást célszerű alkalmazni.

3.2 AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁSÁNAK HELYZETE A MAGYAR KÖZIGAZGATÁSBAN

Az informatikai-, illetve adatbázis-biztonság állami szabályozása a közigazgatás szereplőire és a kritikus infrastruktúrákra vonatkozóan lehet kényszerítő eszköz, a magán szféra szereplői pedig saját döntés alapján felhasználhatják ezt szervezetük informatikai biztonságának biztosítására.

A következőkben megvizsgálom a közigazgatás informatikai rendszerein belül az adatbázis-biztonság szabályozásának jelenlegi helyzetét. Ennek kapcsán elemzem az adatbázis-biztonságot érintő informatikai biztonsággal kapcsolatos szabályozó dokumentumok típusait, rendeltetését, tartalmát, célközönségét; rendszerezem az adatbázis-biztonság és az informatikai biztonság szabályozási rendszerének jelenlegi szereplőit; végül megvizsgálom - mint egy lehetséges modellt-, az Egyesült Államok Védelmi Minisztériuma által kidolgozott szabályozókat. A témát részletesebben lásd a [FR9], [FR10], [FR11] publikációimban.

3.2.1 ADATBÁZIS ÚTMUTATÓK HELYE AZ INFORMATIKAI BIZTONSÁG DOKUMENTUMAINAK KÖRÉBEN

Magyarországon konkrétan adatbázis-biztonságra vonatkozó szabályozó nem létezik, ezért egy tágabb terület, az informatikai rendszerek biztonságára kiterjedő állami szabályozást tanulmányoztam és feltártam ezek adatbázis-biztonságot érintő vonatkozásait. A következőkben az informatikai biztonságot és a kritikus infrastruktúrákat érintő magyar jogszabályokat és a közigazgatásra vonatkozó ajánlásokat elemzem, majd kiemelem ezek adatbázis-biztonságot érintő aspektusait.

Jogszabályok

Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény [100] 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* [12] 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, illetve az elektronikus közszolgáltatáshoz kapcsolódó informatikai rendszert informatikai biztonsági szempontból értékeltetni kell.
- 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 [1], [101], [102], [103]. Ezek az adatbázis-biztonság témáját csak nagyon távolról érintik, részletesebb vizsgálat az értekezés 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* [50], 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 [104], [105]. 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)** [106] 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) [107], amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK) [10], 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) [108], amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

A **Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)** [109] 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)** [110] 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* [105] 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.

Dokumentumok értékelése, összegzése

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

1. Jelen pillanatban Magyarországon 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 szükség arra – például a kritikus infrastruktúrák védelmének szabályozása kapcsán -, hogy jogszabályi vagy ajánlási szinten is megjelenjen az adatbázis-biztonság szabályozása.
2. A 223/2009. számú kormányrendelet kimondja, hogy az üzemeltető köteles az elektronikus közszolgáltatáshoz kapcsolódó informatikai rendszert és háttérrendszert informatikai biztonsági szempontból értékeltetni. Ugyanakkor ma Magyarországon nincs olyan szervezet, amelyik például egy ORACLE bonyolultságú adatbázis-kezelő rendszert biztonsági szempontból értékelni tudna. Magyarország 2003-ban csatlakozott a CCRA (A Közös szempontok szerint kibocsátott tanúsítványok kölcsönös elismeréséről szóló nemzetközi megállapodás) nemzetközi megállapodáshoz, mely kimondja, hogy az aláíróknak kötelező érvénnyel el kell fogadniuk a CC (Common Criteria) tanúsítványokat, illetve a tagállamoknak elő kell segíteniük a tanúsított termékek és védelmi profilok használatát. Emellett az Európa Tanács 2002/C 43/02 sz. határozata (megjelent: *Official Journal of the European Communities 16.2.2002*) felkéri a tagállamokat, hogy támogassák a Common Criteria szabványnak a használatát és a vonatkozó tanúsítványok kölcsönös elfogadását. Mindezek alapján megállapítom, hogy a kritikus adatbázisokat tartalmazó informatikai rendszerek esetén a releváns kormányrendeletnek szükséges lenne előírnia, hogy kizárólag értékelt, tanúsított (például a Common Criteria módszertana szerint) adatbázis-kezelő rendszer használata a megengedett.
3. 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 Szabályzatnak nagyobb szervezeteknél kétszintűnek kell lennie. 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.

4. 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.

5. 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 sajnálatos módon nem egyezik a nemzetközi szabványok és bevált gyakorlatok alapján kidolgozott KIB ajánlásokban található osztályozási rendszerrel. A rendelet három helyett öt kategória használatát írja elő, melyek a következők:

I. Különlegesen védendő (minősített) adatok, amelyekhez a belső és külső hozzáférés csak erősen korlátozva, szigorúan ellenőrizve és dokumentálva engedélyezhető,
II. Érzékeny adatok, amelyekhez a belső és külső hozzáférést korlátozni, a hozzáférést naplózni kell,
III. Belső adatok, amelyekhez a külső hozzáférés nem lehetséges, belső hozzáférés korlátozása nem kritikus,
IV. Nyilvános, közhiteles adatok, ahol a rendelkezésre állás és a megváltoztathatatlanság biztosítása kritikus,
V. Általános kezelésű adatok.

6. A 223/2009. (X. 14.) Kormányrendelet az elektronikus közszolgáltatások biztonságát elősegítő fontos dokumentum, mely jó néhány helyen pontosításra, újragondolásra szorul. Például a Kormányrendeletben szerepel, hogy „az adattovábbítás során kriptográfiai megoldásokat kell használni az adatok titkosítására”. Az adatok titkosítása csak akkor szükséges és helyénvaló, ha a bizalmasság biztonsági kritérium megvalósulása szükséges az adott rendszerben. Ez sok közszolgáltatásnál nem elvárás, sőt, a kezelt adatok nyilvánossága az elvárt. Továbbá az elektronikus közigazgatásban célszerű lenne az adatok biztonsági osztályozásánál használt kategóriák számában és minősítésében megegyezni és a különböző jogszabályokban és ajánlásokban ezeket egységesen kezelni.

Összességében megállapítom, hogy 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.

3.2.2 ADATBÁZIS-BIZTONSÁGI ÉS AZ INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSI RENDSZERÉNEK SZEREPLŐI

Mint azt korábban már bemutattam, 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 vizsgálom 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[6] 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.

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

A jogszabályok előkészítése a szakmailag illetékes miniszter feladata. A miniszterek feladat- és hatáskörét legmagasabb szinten a miniszterek feladat- és hatáskörét szabályozó kormányrendelet [111], valamint az egyes törvények képezik. Az állami vezetők feladat- és hatásköre az informatikai biztonságot átfogó módon nem tartalmazza. 2010 óta az e-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 [111, 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. [112, 61. §], [113, 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. [114, 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. [12, 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 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 [115].

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 [116], 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 [116, 5.c]. A Közigazgatási Informatikai Bizottság és jogelődjei eddig hat informatikai biztonsági témájú ajánlást (ajánláscsomagot) fogadtak el.[7]

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.

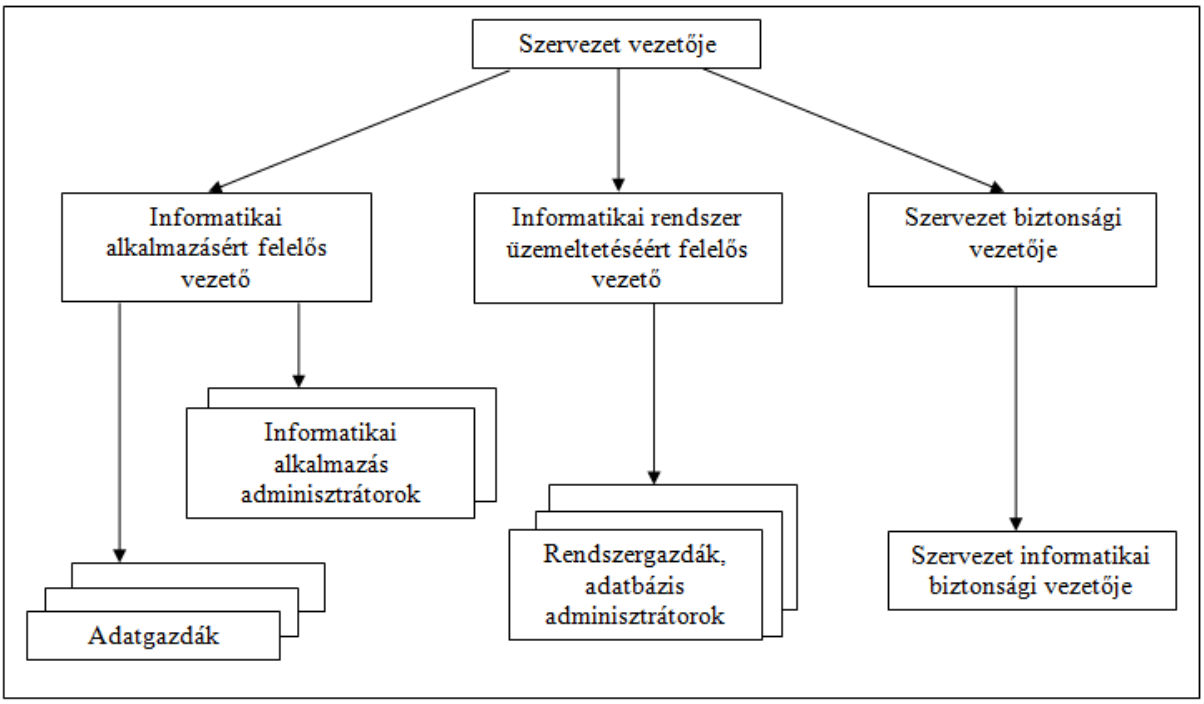
A kormány 2008-ban a KKB javaslatára fogadta el Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló Zöld Könyvet [50] és elrendelte a hazai infrastruktúra létfontosságú elemeinek védelméről szóló szabályozási koncepció összeállítását. 2010 őszére volt tervezve egy kritikus infrastruktúra védelmi törvény elfogadása, erre azonban nem került sor.

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 végzem 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).

[7] 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).



12. ábra: Szervezeti szerepkörök az informatikai biztonság területén [készítette a szerző]

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 [117].

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 [10].

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 [10].

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 [118].

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.

3.2.3 EGY LEHETSÉGE MODELL: ADATBÁZIS-BIZTONSÁG AZ USA HADEREJÉBEN

Az adatbázis-biztonság állami szintű szabályozásával kapcsolatban egyetlen forrást találtam, az Egyesült Államok Védelmi Minisztériuma (Department of Defense, DoD) által kidolgozott és alkalmazott rendszert, mely az USA haderejében lévő informatikai rendszerek adatbázisainak védelmére született. A dokumentumok precízen felépítettek, nyilvánosak és bármely szervezet számára hasznosíthatóak, így a civil szféra is profitál belőle. (Például az Ohio Állami Egyetem adatbázis szerver biztonsági szabályzata, illetve Alabama állam Információ Biztonsági Központjának adatbázis-biztonsági útmutatója is ezen dokumentumok alapján született [119]. A következőkben a DoD által kidolgozott rendszert elemzem, majd áttekintem a hazai adaptáció lehetőségeit.

A DoD adatbázis-biztonsággal foglalkozó szabályozása egy nagyobb szabályozási egységnek, az Egyesült Államok haderején belüli teljes informatikai rendszerre vonatkozó, az

informatikai védelem megvalósításával és ellenőrzésével foglalkozó *Informatikai Védelmi Direktívának* [120] és az erre épülő *Informatikai Védelmi Megvalósítási Utasításnak* [121] a része. 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 Védelmi Direktívában szerepel, amely előírja, hogy minden informatikai rendszert be kell sorolni ezen kategóriák egyikébe. 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, ezek részletes leírását lásd [120]. 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, ezek részletes leírását lásd [121].

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 [FR9].

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 [121]:

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* [9] 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* [122] 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.

Az amerikai modell vizsgálata kapcsán annak két fontos tulajdonságát mindenképp célszerű szem előtt tartani:

- Az adatbázis-biztonsági szabályozás a teljes informatikai biztonsági szabályozás keretein belül helyezkedik el, annak struktúrájához és terminológiájához illeszkedik,
- Az adatbázis-biztonsági szabályozás két nagyobb egységből áll. Egyrészt egy általános adatbázis-biztonsági útmutatóból, másrészt a konkrét adatbázis-kezelő rendszerekhez kidolgozott ellenőrzési listákból.

Megállapíthatjuk, hogy 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. Fel kell tárni, mik a hazai adaptációra alkalmas részei, illetve mi az, ami a magyar viszonyok között nem alkalmazható.

3.3 KÖVETKEZTETÉSEK

A fejezetben először a magyar elektronikus kormányzat felépítését és ebben az adatbázisok helyét, szerepét elemeztem, majd feltártam az informatikai biztonság szabályozás jelenlegi helyzetét a magyar közigazgatásban. Vizsgálataim alapján a következő gondolatokat emelem ki. 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 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 megítélésem 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.

A közigazgatás informatikai rendszerei igen jelentős mértékben adatbázis rendszerek, ennek ellenére az adatbázisok biztonságára vonatkozó specifikus előírást a hazai jogszabályok és ajánlások nem tartalmaznak. 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 előzőekben bemutatott amerikai modell esetén. Például egy jövőbeli 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.

4 AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁS FEJLESZTÉSÉNEK IRÁNYAI A MAGYAR KÖZIGAZGATÁSBAN

BEVEZETÉS

Az adatbázis-biztonság szabályozó rendszerének fejlesztési lehetőségeinek áttekintésekor abból indultam ki, hogy egyrészt a hazai informatikai biztonság szabályozásában már sok fontos lépés történt, 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 érzékelek. Célom a nemzetközi szabványokhoz és a hazai jogszabályokhoz illeszkedő adatbázis-biztonság megteremtéséhez és fenntartásához szükséges lépések megfogalmazása.

A fejezet célja meghatározni az adatbázis-biztonság szabályozás fejlesztési irányait és dokumentumait a hazai elektronikus közigazgatás keretein belül. A felvázolt kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Elemeztem az informatikai biztonsági és adatbázis-biztonsági útmutatók fogalmával, rendeltetésével és típusaival kapcsolatos kérdéseket.
- Körvonalaztam az adatbázis-biztonság szabályozásának javasolt rendjét, szabályozási koncepcióját. Az eredményeket a [FR12], [FR13] publikációim alapján állítottam össze.

4.1 ADATBÁZIS-BIZTONSÁGI ÚTMUTATÓK ALAPJAI

Az információk, az informatikai rendszerek és az ezek részét képező adatbázis rendszerek biztonságát sebezhetőségeiken keresztül számos fenyegetés veszélyezteti. Az egyes fenyegetések bekövetkezésük valószínűsége és várható következményeik alapján eltérő kockázatokat jelentenek a védendő objektumok biztonságára. A kockázatok azonosítása, elemzése és értékelése alapján lehet kiválasztani a megfelelő védelmi rendszabályokat, intézkedéseket, biztonsági kontrollokat.

Az informatikai és ezen belül az adatbázis-biztonság megkívánt állapota megfelelő biztonsági kontrollok (folyamatok, eljárások, szervezeti megoldások, szoftver és hardver funkciók) segítségével érhető el és tartható fent. Ezeket a kontrollokat meg kell határozni, meg kell valósítani, folyamatosan figyelemmel kísérni és szükség esetén továbbfejleszteni, hogy a kitűzött biztonsági és ennek következtében szervezeti célkitűzések megvalósuljanak. Egy adott szervezet számára az alkalmazandó biztonsági kontrollok meghatározását, kiválasztását elméleti vizsgálatok és bevált gyakorlati tapasztalatok alapján nemzetközi és

nemzeti szakmai szervezetek, informatikai gyártók által összeállított kontroll-gyűjtemények, biztonsági útmutatók segítik.

Az informatikai biztonsági útmutatók és a kapcsolódó dokumentumok kiemelt szerepet játszanak az informatikai biztonság megvalósításában, ennek keretében az informatikai biztonság irányításában, valamint szabályozásában. A következőkben az adatbázis-biztonsági - illetve tágabb csoportjuk az informatika biztonsági - útmutatók és ellenőrző listák szerepének, helyének és felépítésének elemzését végzem el, majd a javasolt felépítés szerint ismertetek egy általam megírt, a közigazgatásban hasznosítható adatbázis-biztonsági útmutatót.

4.1.1 INFORMATIKAI BIZTONSÁGI ÚTMUTATÓK, KONTROLLOK

A **biztonsági útmutatók** (security guideline) az útmutatók egyik csoportját alkotják, amelyek rendeltetése biztonsági célkitűzések megvalósítását szolgáló megoldások, eljárások, tevékenységek meghatározása. Szűkebb vizsgálati témánk szempontjából a továbbiakban a biztonsági útmutatók alapterületének az átfogó informatikai biztonságot, illetve ennek egy részterületét az adatbázis-biztonságot tekintjük.

Az informatikai biztonsági útmutatók és a kapcsolódó dokumentumok (ellenőrző listák) az informatikai biztonság kialakítását és fenntartását szolgáló védelmi megoldások, rendszabályok és tevékenységek kialakításának, illetve ellenőrzésének alapvető eszközei. Az útmutatók fő összetevőit a védelmi megoldások, intézkedések, biztonsági kontrollok képzik. A biztonság kialakításához és fenntartásához meg kell határozni a biztonsági célkitűzéseket, azonosítani és értékelni kell a biztonságot veszélyeztető kockázatokat, majd ezek alapján meg kell határozni és valósítani a védelmi intézkedéseket.

Szervezetek biztonsági szabályozórendszer három szintre osztható: Felső szinten a biztonsági politika és stratégia, középső szinten átfogó és részterületi szabályzatok, míg alsó szinten a konkrét feladat- és szerepkörökre vonatkozó részletes biztonsági eljárások találhatóak. A biztonsági útmutatók a szervezetekben a középszintű szabályozóknak és az alsó szintű biztonsági feladatoknak az átfogó biztonsági politika és biztonsági célkitűzések alapján történő kialakítását támogatják, segítik. A biztonsági útmutatók általában több szervezet számára felhasználható módon, azokon kívül kerülnek kidolgozásra.

A biztonsági ellenőrző listák (security checklist) a biztonsági útmutatókban foglalt konkrét megoldások, tevékenységek megvalósulásának – más megközelítésben az útmutatóban foglaltaknak történő megfelelés – ellenőrzésére szolgáló dokumentumok. Az informatikai

biztonsági területen jelentős szerepet játszanak a biztonsági konfigurációs ellenőrző listák (security configuration checklist), amelyek adott informatikai termékek javasolt, biztonságos beállításait, valamint az alkalmazott adminisztrációs megoldásokat, eljárásokat ellenőrzik.

A biztonsági útmutatók, ellenőrző listák felhasználásának lehetőségei három nagy területbe sorolhatóak. (1) A *biztonsági intézkedések kiválasztása, kialakítása során* történő felhasználás jelenti az alapvető felhasználási módot, ahol a biztonsági útmutatók elméletileg megalapozott és a bevált gyakorlatra épülő általános célkitűzés- és megoldás-gyűjteményként szolgálnak. (2) A *szabályozás során* történő felhasználás külső előírásokhoz kapcsolódik. Ennek során a szabályozás hatálya alá tartozó szervezetek számára előírják, hogy mely védelmi megoldásokat, intézkedéseket kell kötelező érvénnyel, vagy bizonyos feltételek fennállásának függvényében megvalósítaniuk. (3) Az *ellenőrzés céljára* történő felhasználás a biztonság állapotának ellenőrzéséhez, felülvizsgálatához, illetve a meghatározott követelményeknek történő megfelelés értékeléséhez kapcsolódik. A biztonsági útmutatókban foglaltak az ellenőrzés, értékelés során etalonként használhatóak fel annak megítéléséhez, hogy a meghatározott biztonsági célkitűzésekhez és kockázatokhoz megfelelőek-e a megvalósított védelmi intézkedések és megfelelő módon kerültek-e megvalósításra.

A **biztonsági útmutatók, ellenőrző listák osztályozása** különböző szempontok szerint lehetséges, például az alkalmazási terület vagy a kidolgozók szerinti osztályozás. Az *alkalmazási terület szerint* az osztályozás többféleképpen kijelölhető, például a következőek alapján:

- az informatikai rendszerek főbb összetevői szerint: alkalmazás-, operációs rendszer, adatbázis-, hálózat- és hardverbiztonsági útmutatók;
- a biztonság összetevői szerint: fizikai, személyi és dokumentum biztonsági útmutatók;
- a védelmi megoldások szerint: fejlesztés-, hozzáférés-, jelszó-, vagy kriptográfiai biztonsági útmutatók;
- valamint az informatikai biztonság adott alkalmazási területre kidolgozott – az átfogó biztonsági útmutatókat specializáló, kiegészítő – útmutatók[8] is.

A biztonsági útmutatók, ellenőrző *listák kidolgozók szerint* több csoportra oszthatóak. Az első csoportot a nemzetközi szabványosítási és szakmai szervezetek által kidolgozott dokumentumok képezik. Ezek a legátfogóbb módon összegzik a biztonság kialakításához és fenntartásához szükséges, jónak tartott megoldásokat, napjainkban ezek képezik minden

[8] Az ISO 27000 szabványcsaládban például külön csoportot képeznek az úgynevezett alkalmazási terület-specifikus útmutatók (jelenleg az egészségügyi ISO 27799 és a távközlési ISO 27011). [1, 12. o.]

biztonsági útmutató alapját. A második csoportba a nemzeti szintű dokumentumok tartoznak, amelyek egy adott ország biztonsági célkitűzései, szabályozásai megvalósítását támogatják. A harmadik csoportba az informatikai ipar szervezetei, a gyártók által kibocsátott dokumentumok sorolhatóak, amelyek egy-egy termék (esetleg termékcsoport) biztonságos alkalmazásához kapcsolódóan nyújtanak útmutatást. Végül a negyedik csoportot a szervezeti szintű dokumentumok alkotják, amelyek általában összetettebb szervezetrendszerekben, az összetevő szervezetek által történő felhasználásra kerülnek kidolgozásra.

A legfontosabb informatikai biztonsági útmutatók közé az ISO/IEC 27000 szabványsorozat egyik eleme - az ISO/IEC 27002:2005 Az informatikai biztonság irányítási gyakorlatának kézikönyve[9]-, az Informatikai Biztonsági Fórum biztonsági ajánlásgyűjteménye és az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete 800-as kiadványsorozatának egyes összetevői tartoznak.

Az informatikai biztonsági útmutatók alapvető összetevőit a védelmi megoldások, intézkedések, biztonsági kontrollok (security control) képezik. Informatikai biztonsági kontroll alatt az informatikai biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedést (óvintézkedést, ellenintézkedést) értünk. Az informatikai biztonsági kockázat (information/IT security risk) erőforrások, erőforráscsoportok sérülékenységét kihasználó, a szervezetnek kárt okozó potenciális fenyegetés [123], ahol erőforrás minden, aminek értéke van a szervezet számára (információ, szoftver, hardver, szolgáltatások, emberek).

Az **informatikai biztonsági kontrollok osztályozásá**hoz felhasználható egy tágabb fogalom, a biztonsági kontrollok osztályozásának vizsgálata, melyre az irodalomban számos különböző szempont található (részletesebben lásd [FR13]).

A COSO[10] Integrált Belső Kontroll Keretrendszer [124] *jelleg szerint* két átfogó típust különböztet meg: előírások ("mit kell tenni") és eljárások (az előírások megvalósítása). Az ISO 27000 osztályozásában adminisztratív, technikai, vezetési és jogi kontrollok szerepelnek [123]. A NIST dokumentumok három típust különböztetnek meg: vezetési, működési és technikai kontrollok. A vezetési (menedzsment) kontrollok a biztonság és a kockázatok kezelésére irányulnak, míg a működési kontrollok az elsődlegesen emberek által, a technikai kontrollok pedig a technikai eszközök által megvalósított eljárások [125].

[9] Code of practice for Information Security Management.
[10] Committee of Sponsoring Organizations of the Treadway Commission = A Treadway Bizottság Támogató Szervezeteinek Bizottsága (könyvvizsgáló szervezetek önkéntes együttműködése).

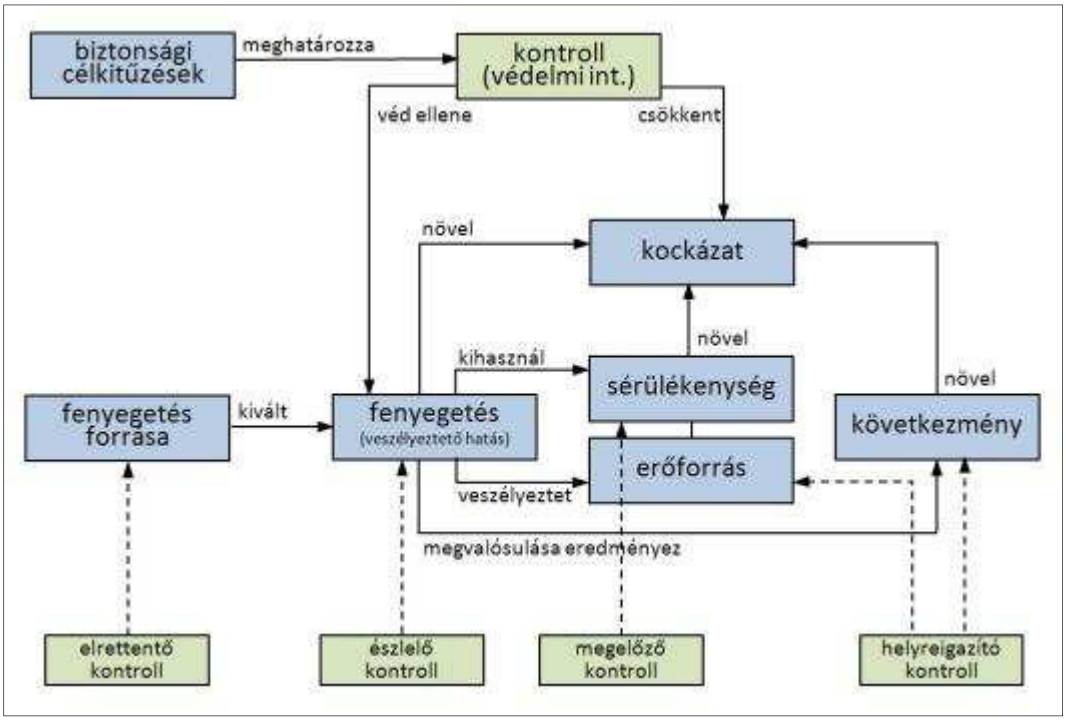
Egy másik megközelítés szerint a biztonsági kontrollok három típusát az adminisztratív, a fizikai és a technikai (más néven logikai) kontrollok alkotják. Az adminisztratív kontrollok a szervezeti erőforrások megóvására irányuló szervezeti előírások, eljárások és más tevékenységek. A fizikai kontrollok közé a fizikai hozzáférést, beavatkozást megakadályozó technikai eszközök, megoldások tartoznak. Végül a technikai kontrollok a technikai eszközökben megvalósított logikai, eljárási jellegű megoldások [126].

A biztonsági kontrollok *rendeltetés szerint* is csoportosíthatóak. A megelőző (preventive) kontrollok rendeltetése a nem kívánatos események, eredmények megakadályozása, elkerülése azok bekövetkezése előtt. Az észlelő, feltáró (detective) kontrollok rendeltetése a már bekövetkezett nem szándékolt események, eredmények feltárása, azonosítása, jelzése a bekövetkezés alatt vagy után. A helyreigazító, helyesbítő (corrective) intézkedések rendeltetése a bekövetkezett nem kívánatos események káros hatásainak csökkentése. Az elrettentő (deterrent) kontrollok rendeltetése a nem kívánatos – elsősorban szándékos – események bekövetkezési valószínűségének csökkentése, valamint a helyreállító (recovery) kontrollok fogalmával, amelyek rendeltetése a biztonságsértés előtti állapot visszaállítása. E két utóbbi típus a megelőző és a helyreigazító kontrollok altípusának is tekinthető.

A korábban bemutatott jelleg és rendeltetés mellett az informatikai biztonsági kontrollok osztályozása az *általánosság-részletesség skálán* is lehetséges. Az általános kontrollok a jól bevált gyakorlatra épülő biztonsági útmutatókhoz kapcsolódnak, az egyes konkrét megoldások általánosításait tartalmazzák. Ezek az általános kontrollok (meghatározások) a különböző szervezetekben, illetve különböző biztonsági célkitűzések esetén történő felhasználhatóság érdekében célszerűen technológia- és megvalósítás-függetlenek. Mindez viszont szükségessé teszi, hogy konkrét megvalósításuk esetén az útmutatóban szereplő kontrollok részletezésre, kiegészítésre kerüljenek.

Az általános kontrollok testre szabását segíti, ha azok eleve tartalmaznak a szervezetek által meghatározható, vagy választható paramétereket (pld. jelszavak minimális hossza, jelszóváltás előírt gyakorisága, stb.). A részletezés azonban enélkül is megvalósítható (pld. legyen minimális jelszó-hossz előírás ~ a jelszó minimális hossza legalább 8 karakter legyen). Az általános biztonsági kontrollok kiegészítése további biztonsági funkciók megvalósítását, vagy a kontroll "erősségének" növelését szolgálja. [125, B-12. o.] Egy biztonsági útmutató az egyes kontrollokhoz több kiegészítést is tartalmazhat, amelyek közül a konkrét biztonsági követelmények függvényében lehet egyet, vagy többet választani. Emellett kiegészítéseket az adott szervezetek is megfogalmazhatnak.

Az informatikai biztonsági kontrollok szerepe az informatikai biztonság megvalósításában eszközjellegű. A kontrollok a biztonsági célkitűzések és a kockázatok elemzése, értékelése alapján kerülnek meghatározásra, majd megvalósításra. Rendeltetésük a kockázatok és ezzel a káros következmények bekövetkezésének, illetve mértékének csökkentése. A kontrollok kapcsolatrendszerét az informatikai biztonság (illetve általában a biztonság) más összetevőivel a következő ábra szemlélteti.



13. ábra: Informatikai biztonsági kontrollok helye, szerepe[11] [127]

A biztonsági útmutatók, kontrollok az informatikai biztonság megvalósításában, ennek keretében az informatikai biztonság irányításában, valamint szabályozásában kiemelt szereppel bírnak. Az informatikai biztonsági útmutatók, kontrollok szerepet játszanak a biztonsági kockázatok feltárásában, értékelésében. Az útmutatók közvetve járulnak hozzá a kockázatok feltárásához azzal, hogy tartalmaznak különböző szintű kontroll-célkitűzéseket, amelyek felhasználása segíthet a kockázatok felismerésében. Az informatikai biztonsági útmutatók, kontrollok a kockázatok kezelésében alapvető szerepet játszanak. Ennek során a kontrollok az egyik legfontosabb megoldást képezik. A védelmi intézkedések, kontrollok kiválasztásának alapvető támogatását a biztonsági útmutatók nyújtják, amelyek a bevált gyakorlat alapján általánosan megfogalmazott biztonsági célkitűzéseket megvalósító kontrollokat biztosítanak alapként a konkrét célkitűzéseket megvalósító kontrollok

[11] Készült az ISO 15408 Védelmi fogalmak és kapcsolatrendszerük ábrájának felhasználásával és kiegészítésével [127].

meghatározásához. Az informatikai biztonsági útmutatók, kontrollok a biztonság helyzetének értékelésében is felhasználhatóak. A szervezeti szintű útmutatók, a bennük foglalt előírások megvalósulásának értékelése referencia-alapot képez a biztonsági helyzet értékeléséhez.

4.1.2 ADATBÁZIS-BIZTONSÁGI ÚTMUTATÓK, KONTROLLOK

Az adatbázis-biztonsági útmutatók az adatbázis rendszerek telepítésére, konfigurálására, üzemeltetésére, illetve az adatbázis-kezelő rendszer működésére kiható, az informatikai rendszer egyéb összetevőire (operációs rendszer, hálózat, adatbázist elérő alkalmazások) vonatkozó biztonsági követelményeket és biztonsági kontrollokat tartalmazzák.

Adatbázis-biztonsági útmutatók készítői között megtaláljuk az adatbázis-kezelő rendszerek gyártóit, fejlesztőit, különböző informatikai biztonsághoz kötődő szervezeteket illetve állami szerveket. Példaként említhetjük az Egyesült Államok Védelmi Minisztériumát, az Adatbázis-biztonsági Konzorciumot, az Internet Biztonság Központját, a SANS intézetet[12], illetve az adatbázis-kezelő rendszerek fejlesztőit, például az Oracle-t.

A dokumentumokat két fő csoportra oszthatjuk a bennük található biztonsági kontrollok általános-részletes jellege alapján. Az egyik csoportot az *általános adatbázis-biztonsági útmutatók* alkotják (például [128], [129]), melyek az adatbázis-kezelő rendszer típusától függetlenül fogalmaznak meg biztonsági követelményeket. A másik csoportot az adatbázis-kezelő rendszer típusához (esetleg még verziójához is) készült útmutatók alkotják, melyek általában *adatbázis ellenőrző lista* (database checklist) elnevezést viselik (például [122], [130], [131]). Természetesen minél szorosabban kötődik az útmutató egy konkrét termékhez (azaz a gyártó és a verziószám is adott), annál precízebb és konkrétabb ellenőrzési és megvalósítási módszereket, biztonsági kontrollokat tartalmaz. Az általánosabban megfogalmazott útmutatók előnye, hogy szélesebb kör számára hasznosíthatók, azonban alkalmazás esetén a felhasználótól nagyobb szakmai tudást várnak el a követelmények konkrét megvalósításának meghatározása folyamán.

Az adatbázis ellenőrző listák fejezetekre osztva, táblázatos formában tartalmazzák a biztonsági kontrollok listáját. A táblázat egy sora egy biztonsági kontrollt tartalmaz, ami egy konkrét biztonsági követelményt, illetve annak megvalósítási és ellenőrzési módját írja le. A követelmény mellett gyakran találunk annak biztonsági szintjét leíró osztályozást is, ami azt mutatja meg, hogy a követelmény be nem tartása milyen mértékű biztonsági sérülést rejt

[12] Database Security Consortium, Center for Internet Security; SysAdmin, Audit, Networking, and Security Institute.

magában. Bizonyos szervezetek (pl. DoD, CIS) az ellenőrzési lista mellé automatikus eszközöket, szkripteket is kifejlesztettek az ellenőrzések gyorsabb elvégezhetősége érdekében. A listákban találhatunk utalást az ellenőrzési pontoknál arra vonatkozólag, hogy az adott követelmény ellenőrzését az automatikus eszköz elvégi-e.

Adatbázis-biztonsági kontrollok alatt az adatok adatbázis rendszerekben történő tárolásával kapcsolatos biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedéseket értjük.

Az adatbázis-biztonsági útmutatók felhasználása az adatbázis rendszerek biztonsági kockázatainak feltárásában és kezelésében, az adatbázis-biztonsági kontrollok kiválasztásának és alkalmazásának folyamatában és a biztonsági ellenőrzés, biztonsági audit folyamán lehetséges. Az adatbázis-biztonsági útmutatók tartalma kiterjed többek közt az adatbázis-kezelő rendszer és működési környezetének biztonságos beállításaira, az adatbázisok biztonságos beállításaira, illetve a működési folyamatok biztonságos kezelésére (például a felhasználók menedzsmentjére, a hitelesítés, mentés, helyreállítás, telepítés és log elemzés folyamataira).

Az adatbázis-biztonsági kontrollok esetében is végigkövethetők az informatikai biztonsági kontrolloknál bemutatott csoportosítási lehetőségek. A technológia- és megvalósítás-független általános kontrollokat az általános adatbázis-biztonsági útmutatók tartalmazzák. A biztonság gyakorlati megvalósítása során szükséges az útmutatóban szereplő kontrollok részletezése, kiegészítése, testre szabása. Ennek a folyamatnak a végterméke lehet egy olyan biztonsági útmutató (vagy más néven ellenőrző lista), mely konkrét, specifikált biztonsági kontrollok gyűjteményéből áll. Természetesen ebben az esetben a kontrollok függnek az adatbázis-kezelő rendszer típusától, verziójától és a működési környezet tulajdonságaitól. Egy konkrét típusú és verziójú adatbázis-kezelő rendszerhez adnak ki (gyártók, illetve különböző biztonsági szervezetek) ellenőrző listákat, melyek a helyes telepítés, konfigurálás és működtetés technikai és működési elemeit fogalmazzák meg. A COSO keretrendszer által meghatározott előírások kategória az általános adatbázis-biztonsági útmutatók kontrolljaira jellemző, míg a specifikus adatbázis-biztonsági ellenőrző listák kontrolljai az eljárások kategória alá esnek.

Az 13. ábra osztályozását tekintve megállapíthatjuk (például [129] alapján), hogy az adatbázis-biztonsági kontrollok többsége a megelőző típusba tartozik. Ide sorolhatjuk – a teljesség igénye nélkül – az adatbázis-kezelő rendszer konfigurációs kontrolljait, a hitelesítéssel kapcsolatos kontrollokat, a hozzáférési jogosultságokat szabályozó kontrollokat

vagy a titkosítás szabályozását biztosító kontrollokat. Észlelő kontroll kategóriájába tartozik a log menedzsment és elemzés, illetve az illetéktelen hozzáférések megfigyelésének kezelése. Helyreigazító kontrollok körébe az adatbázismentést és helyreállítást szabályozó kontrollok tartoznak. Az elrettentő kontrollok az adatbázis-biztonsági útmutatókra nem jellemzőek, az elrettentés feladatát adminisztrációs módszerekkel, intézkedésekkel lehetséges kezelni.

Az adatbázis-biztonsági kontrollok rendeltetés szerint besorolhatók a következő három kategóriába: technikai kontrollnak az adatbázis-kezelő rendszerben megvalósított biztonsági beállításokat, működési kontrolloknak az adatbázis-kezelő rendszer működtetésével, üzemeltetésével kapcsolatos, emberek által megvalósított eljárásokat, adminisztratív kontrollnak pedig a szervezeti erőforrásokkal kapcsolatos szervezeti előírásokat, eljárásokat értjük.

Az adatbázis-biztonsági útmutatók felépítésére a gyakorlatban különböző példákat láthatunk. Az általam logikusnak vélt rendszerezés a biztonsági kontrollok rendeltetés szerinti csoportosításra épül. Ezek alapján megkülönböztetem a technikai, a működési és az adminisztratív kontrollokat. Technikai kontrollnak az adatbázis-kezelő rendszerben megvalósított biztonsági konfigurációs beállításokat, működési kontrolloknak az adatbázis-kezelő rendszer működtetésével, üzemeltetésével kapcsolatos eljárásokat, adminisztratív kontrollnak pedig a szervezeti erőforrásokkal kapcsolatos előírásokat, eljárásokat értjük.

A technikai kontrollok tovább osztályozhatóak aszerint, hogy azok a védendő objektum mely részelemének védelméért felelősek. Itt elsőként kell említeni az adatbázisban tárolt adatok védelmét, illetve az adatbázis-kezelő rendszer védelmét, illetve az informatikai rendszer más részelemeit, melyek biztonsága szorosan kihat az adatbázis-biztonságra. Ide tartozik az adatbázis-kezelő rendszer számítógépének operációs rendszere, a hálózat és az adatbázist elérő alkalmazások, de ezeknél az informatikai rendszer elemeknél csak az adatbázis-biztonságra kiható biztonsági követelmények meghatározására szorítkozunk. A következő táblázatban összefoglalom az adatbázis-biztonsági útmutató egy lehetséges felépítését:

Adatbázis-biztonsági útmutató felépítése	
Technikai kontrollok	
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 • Adatok védelme titkosítással - Hálózaton - Adatbázisban
Működési kontrollok	• Ügyrendi, biztonsági és egyéb eljárások szabályzatok • Adatbázis-kezelő rendszer telepítése és biztonsági frissítése - 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 - 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

Adminisztratív kontrollok	• Adatbázis felhasználók megkülönböztetése - Adatbázis alkalmazás felhasználó - Adatbázis adminisztrátor - Alkalmazás tulajdonos - Alkalmazás felhasználó adminisztrátor - Automatikus feldolgozás számára létrehozott felhasználó • Adatbázis szerepkörök kialakítása - Adatbázis adminisztrátori szerepkör - Alkalmazás fejlesztői szerepkör - Adatbázis alkalmazás felhasználói szerepkör - Adatbázis alkalmazás adminisztrátori szerepkör

2. táblázat: Adatbázis-biztonsági útmutató szerkezeti felépítése [készítette a szerző]

A fejezet végén ismertetek egy, a fenti felépítés szerint általam megírt, a közigazgatásban hasznosítható adatbázis-biztonsági útmutatót.

4.2 ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁSÁNAK ALAPJAI

Az **informatikai biztonság szabályozása** általános értelemben az informatikai biztonsághoz kapcsolódó szabályok – feladatok, felelősségi és hatáskörök, előírások és korlátozások – meghatározása. Mint minden szabályozás, elsősorban a rendszeresen ismétlődő tevékenységek végrehajtásának eljárási, szakmai, vagy technikai szabályait rögzíti. A szabályozás szintjét tekintve lehet nemzetközi, nemzeti, ágazati (szakterületi), vagy szervezeti, emellett megkülönböztethetünk jogi és önszabályozást is. Az informatikai biztonság szabályozásában fontos szerepet játszanak az informatikai biztonsági útmutatók és kontrollok.

A szabályozás során a biztonsági útmutatók közvetlen alkalmazása nemzeti, ágazati, vagy szervezeti szinten azt jelenti, hogy az adott szabályozó a hatálya alá tartozó szervezetek, számára előírja kiválasztott útmutatókban foglalt kontrollok, vagy azok egy meghatározott részének alkalmazását, megvalósítását. Ezek az útmutatók nemzeti szinten – a saját felügyelet érdekében – általában nemzeti szabványok, ajánlások. Erre példa az Egyesült Államok Szövetségi Információbiztonsági Törvénye [132], amely a szövetségi informatikai rendszerekre előírja a vonatkozó NIST dokumentumokban foglaltak alkalmazását. Ágazati (szakterületi) szinten szintén találkozhatunk közvetlen hivatkozással, például az ISO 27000 szabványcsalád egészségügyi informatikai tagja [133] az ISO 27002 útmutatóra épít. Szervezeti szabályozások előírhatják az alkalmazott rendszerekre, eszközökre vonatkozó gyártói útmutatók alkalmazását is.

A szabályozás során a biztonsági útmutatók közvetett alkalmazása esetén az adott szabályozó közvetlenül nem hivatkozik útmutatóra, ehelyett – mintegy szakmai

háttéranyagként – az abban foglaltak kerülnek felhasználásra. Ennek során elsősorban az útmutatóban található informatikai biztonsági célkitűzések, kontrollok kerülnek felhasználásra, mérlegelve az érintett terület biztonsági kockázatait és magas szintű biztonsági célkitűzéseit. Ez a felhasználás egyaránt előfordulhat nemzeti, ágazati és szervezeti szintű szabályozások esetében.

A biztonsági útmutatók szabályozási alkalmazásának jellegzetes területei közé nemzeti szinten mindenekelőtt az e-közigazgatás, a védelmi szféra és a kritikus infrastruktúra védelem tartozik. Jelentős szabályozási terület a minősített adatok, illetve a személyes adatok védelme is. Az ágazati, szakterületi – ezen belül mindenekelőtt az infokommunikációs területi – szabályozás alapvető jellemzője az önszabályozás, általában az ISO 27000 szabványcsaládnak történő megfelelés. A pénzügyi szolgáltatásokkal kapcsolatos magyar szabályozórendszer pedig jelentős mértékben épít a COBIT módszertanra [118].

Magyarországon az adatbázis-biztonság szabályozását megítélésem szerint az informatikai biztonság szabályozó rendszerének integráns részeként, a jelenleginél mélyebb tartalommal és önálló dokumentumokkal szükséges megvalósítani, az átfogó informatikai biztonságért felelős miniszter feladat- és hatáskörében. Véleményem szerint az adatbázis-biztonság szabályozásnak törvényi szinten nem szükséges megjelennie, önálló kormányrendeletet sem igényel. Ugyanakkor az elektronikus közigazgatás biztonságával kapcsolatos kormányrendeletben egy fejezetet célszerű lenne az adatbázisok biztonságának szabályozására szentelni.

Az adatbázis-biztonság szabályozásának kapcsán javaslom a közigazgatási informatikai rendszerek és a kritikus információs infrastruktúrák teljes körű informatikai védelmének koordinációs és egyes konkrét feladataival egy központi szervezetet megbízni. (A továbbiakban, az egyértelműség kedvéért erre a szervezetre nemzeti informatikai biztonsági központ megnevezést használom.) A nemzeti informatikai biztonsági központ az illetékes miniszter irányítása alatt állhatna, egyben – ágazati résztvevőként – együttműködne a kritikus infrastruktúra védelem feladatait megvalósító szervezettel. Az adatbázis-biztonság felügyelete és megvalósításával kapcsolatos konkrét feladatok is e központi szervezet feladatát kell, hogy képezze.

Javaslatom 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 – például a Közigazgatási Informatikai Bizottság - adná ki. (Erre a

dokumentumra az értekezés következő pontjában bemutatok egy általam összeállított, a közigazgatásban hasznosítható példát.) 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, használatát az elektronikus közigazgatás biztonságával kapcsolatos kormányrendelet rendelné el a kormányrendeletben meghatározott szervezetek számára.

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 kontrollok gyűjteményévé, 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 magyar közigazgatásban – ellentétben a bemutatott Egyesült Államokbeli példával - 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. Ebből kifolyólag a rendszer specifikus adatbázis-biztonsági ellenőrző listákat a szervezeteknek maguknak kellene elkészíteni saját környezetükre vonatkoztatva.)

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 feladata 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. A központi szerv adatbázis-biztonság felügyeletével kapcsolatos feladatkörét, illetve az érintett szervezetek adatbázis-biztonsággal kapcsolatos kötelezettségeit az elektronikus közigazgatás biztonságával kapcsolatos kormányrendeletnek kellene előírnia.

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

a) Nagyobb szervezetek esetén a rendszerszintű Informatikai Biztonsági Szabályzatok közé
b) Egyszintű Informatikai Biztonsági Szabályzat esetén annak egy fejezetének
c) Eljárásrendek közé

A rendszer specifikus adatbázis-biztonsági ellenőrző listák a szervezeti biztonsági dokumentumok rendszerében az Eljárásrendek kategóriájába sorolható be.

A következő alfejezetben ismertetek egy általam megírt, a közigazgatásban hasznosítható adatbázis-biztonsági útmutatót.

4.3 ÁLTALÁNOS ADATBÁZIS-BIZTONSÁGI ÚTMUTATÓ

A. Technikai kontrollok

A.1 Adatbázis-kezelő rendszer konfigurációs követelményei

Az adatbázis rendszer (az adatbázis-kezelő rendszer és a tárolt adatok) az államilag előírt, illetve a szabványok által meghatározott általános biztonsági követelményeknek, a jelen Útmutatónak és termék-specifikus adatbázis-biztonsági ellenőrző listának megfelelően konfigurált és biztosított. Felhasználható, illetve adaptálás céljából igénybe vehető adatbázis-biztonsági ellenőrző listákat fejlesztettek ki többek közt az USA Védelmi Minisztériuma (Department of Defense, DoD), a CIS, a NIST, a SANS szervezetek, továbbá az adatbázis-kezelő rendszerek gyártói.

Az adatbázis-kezelő rendszer működését meghatározó konfigurációs fájlok és az ezekben szereplő paraméterek az adott típusú és verziójú adatbázis-kezelő rendszer biztonsági útmutatója alapján legyenek beállítva.

Az adatbázis-kezelő rendszert úgy kell konfigurálni, hogy indulás, leállítás, abortálás és egyéb nem tervezett megszakítás esetén az adatbázis-kezelő rendszer csak megbízható fájlokat, eljárásokat és egyéb komponenseket használjon.

Az adatbázis-kezelő rendszer hoszt gépének operációs rendszere, a hálózat és más adatbázissal kapcsolatos alkalmazás és informatikai komponens biztonságosan konfigurált és üzemeltetett.

Az adatbázis-kezelő rendszer típusát és verzióját működés közben tilos a felhasználók számára megjeleníteni.

A.2 Operációs rendszer biztonsága

A.2.1 Adatbázis-kezelő rendszer program könyvtárának és fájljainak védelme

Az adatbázis rendszer program fájljait, konfigurációs fájljait operációs rendszer szinten is védeni kell a jogosulatlan hozzáférésekkel szemben. Ezekre az állományokra a hozzáférési beállításokat a legkisebb jogosultság elve szerint kell beállítani, az aktuális adatbázis-kezelő rendszer biztonsági útmutatója alapján.

Az adatbázis-kezelő rendszer szoftver könyvtárai – beleértve az adatbázis rendszer konfigurációs fájljait is -- kijelölt könyvtárakban vagy lemez partíciókon legyenek, melyek

különböznek az operációs rendszer és más alkalmazások állományait tartalmazó könyvtáraktól és partícióktól.

Az adatbázis-kezelő rendszer és egyéb adatbázis alkalmazás szoftver programjait meghatározott időközönként (például hetenként) felül kell vizsgálni annak érdekében, hogy az azokon végrehajtott jogosulatlan módosítások kiderüljenek.

Az adatbázis-kezelő rendszerről és szükséges adatbázis objektumokról baseline-t (hash értéket) kell készíteni annak érdekében, hogy a szoftver kódokban és adatbázis objektumokban véghezvitt jogosulatlan módosításokat észlelni lehessen. Frissítés és jogosult módosítás esetén a baseline-t is frissíteni kell. Baseline-nak nevezzük egy jóváhagyott dokumentum, fájl vagy programkód hash értékét, melyhez az azt követő változtatásokat viszonyítani lehet.

Az adatbázis-kezelő rendszer és az adatbázist elérő alkalmazások szoftver programjainak tulajdonosai erre kijelölt és felhatalmazott felhasználók legyenek.

Az adatbázis-kezelő rendszer szoftveréhez való hozzáférés csak arra felhatalmazott operációs rendszerbeli felhasználók számára legyen lehetséges.

Az adatbázis rendszerleíró kulcsaihoz (registry key) való írási jogot csak adatbázis- és más rendszer adminisztrátorok számára szabad megadni.

A.2.2 Adatbázis rendszerrel kapcsolatos operációs rendszer szintű felhasználók beállításai

Adatbázis-kezelői privilégiumokkal rendelkező operációs rendszerbeli szerepköröket csak arra felhatalmazott felhasználók kaphassanak.

Biztosítani kell, hogy az adatbázis adminisztrátorhoz tartozó operációs rendszerbeli felhasználó az adatbázis-kezelő rendszer működtetéséhez és rendszergazdai tevékenységéhez szükséges minimális szintű operációs rendszer jogosultságokkal rendelkezzen.

Az adatbázis adminisztrátorok számára az adatbázis-kezelő rendszer hoszt gépén való jogosultságokat operációs rendszer szintű csoportokhoz történő hozzárendeléssel célszerű megvalósítani. A csoporttagság hozzáférési jogosultságokat állít be az adatbázis-kezelő rendszer gépén lévő könyvtárakhoz és fájlokhoz, ezen kívül még adatbázis-kezelő rendszeren belüli jogosultságok beállítását is jelentheti. Csak az illetékes adatbázis adminisztrátorokat szabad privilégiumokkal bíró operációs rendszer szintű csoporthoz hozzárendelni.

Célszerű az adatbázis-kezelő rendszer telepítését egy speciálisan erre a célra létrehozott felhasználó nevében végezni. Az adatbázis-kezelő rendszer telepítését végző felhasználó nevében csak felhatalmazott személyek léphessenek be az operációs rendszerbe. Ha ez egy megosztott felhasználói hozzáférést jelent – azaz több személy is használhatja egyidejűleg--, akkor megfelelő audit és logolás mellett kell biztosítani, hogy csak arra felhatalmazott személy használhassa azt.

Az adatbázis-kezelő rendszer telepítését végző felhasználó az adatbázis-kezelő rendszer számítógépébe csak az adatbázis telepítésekor, frissítésekor és karbantartásakor legyen jogosult belépni. Az adatbázis-kezelő rendszer telepítését végző felhasználó nem végezhet hagyományos adatbázis adminisztrátori tevékenységet, csak olyat, ami kapcsolódik az adatbázis-kezelő rendszer fájljainak hozzáférési beállításainak karbantartáshoz.

Minden adatbázis szolgáltatás és folyamat (processz) egy erre a célra kijelölt és beállított operációs rendszerbeli felhasználó nevében fusson, aki csak a szükséges (azaz minimális) operációs rendszerbeli jogosultságokkal rendelkezik. Az operációs rendszer felhasználóra specifikus konfigurációs követelmények vonatkoznak, amik a használatban lévő adatbázis-kezelő rendszertől függnek

Az operációs rendszerbeli felhasználók, akik nevében az adatbázisból kezdeményezett külső eljárások futnak, csak a szükséges (azaz minimális) operációs rendszerbeli jogosultságokkal rendelkezzenek.

A.3 Hálózati biztonság

A.3.1 Listener védelme

Az adatbázis-kezelő rendszer hálózati kapcsolatát biztosító listener folyamatának konfigurációja az adott termék biztonsági specifikációja alapján megvalósított.

Az adatbázis listener konfigurációjában a hálózati megszorításokat úgy kell beállítani, hogy csak jogosult hálózati címekről és protokollokról fogadhasson adatbázis kapcsolatot.

A.3.2 Port védelem

Az adatbázis-kezelő rendszer hálózati kommunikációját úgy kell beállítani, hogy az csak kontrolált és előre definiált portokat, protokollokat és szolgáltatásokat használjon. Az adatbázishoz történő hálózati kapcsolat konfigurációjában a véletlenszerű port hozzárendelést (random port assignment) nem szabad engedélyezni.

Az adatbázis-kezelő rendszer hálózati kommunikációjában használt alapértelmezett port számot - ha az architektúra megengedi - változtassuk meg.

A.3.3 Az adatbázis-kezelő rendszer külső interfészeinek és ezeken áramló információknak a védelme

Az adatbázis-kezelő rendszerből kifelé, illetve abba befelé irányuló távoli és helyi kapcsolatokat nevezzük külső interfésznek. Ez lehet az adatbázis-kezelő rendszer hoszt gépén futó, az adatbázis-kezelő rendszer részét nem képező helyi folyamat, vagy az adatbázis-kezelő rendszerből távoli adatbázis klienshez vagy alkalmazáshoz történő kapcsolódás. A kapcsolatot kezdeményezheti kliensként az adatbázis-kezelő rendszer, illetve fordított irányban egy távoli kliens az adatbázis rendszer felé. A külső kapcsolatokat megfelelően védeni kell, hisz ezeken keresztül az adatbázis rendszerbe irányuló jogosulatlan hozzáférések valósulhatnak meg. A külső interfészeken áthaladó adatok – melyek lehetnek hitelesítési információk is - szintén támadási felületet jelentenek.

Publikusan elérhető adatbázis azonosítók, adatbázis rendszerek hálózati címei és hoszt nevei adatbázisok jogosulatlan elérésére irányuló támadások kiinduló pontjai lehetnek. Ezeket az információkat lehetőség szerint védeni kell és csak a feljogosult felhasználók számára érdemes ismertté tenni.

Az adatbázis rendszerhez kapcsolódó kliensek jogosultságának meghatározásakor a kliens hálózati helyének figyelembe vétele segíti az adatbázis rendszer védelmét biztosítani illetéktelen felhasználókkal szemben. Az adatbázis rendszert védeni kell a direkt kliens kapcsolatoktól, melyek nyilvános, illetve jogosulatlan hálózati helyekről érkeznek.

Adatbázis kliens program csak olyan adatbázisokhoz tartalmazzon azonosító paramétereket, melyekhez jogosult hozzáférése van.

Az adatbázist elérő alkalmazások ne azzal az opcióval működjenek, mely parancssorban megjeleníti az adatbázis csatlakozási jelszavakat.

A.3.4 Külső objektumok elérése és külső eljáráshívás

Az adatbázison kívül tárolt, de az adatbázisban definiált és onnan meghívható külső folyamatok, eljárások sokszor más operációs rendszerbeli biztonsági környezetben futnak, mint maga az adatbázis-kezelő rendszer. A külső eljárások biztonsági rést jelenthetnek a hoszt rendszer számára.

Biztonsági szempontból az adatbázis rendszer általi külső eljáráshívás engedélyezését kerülni kell, kivéve, ha a helyes működés a használatát megköveteli. Ebben az esetben külső eljáráshívás engedélyezését és használati módját dokumentálni kell és a külső eljáráshívás folyamatának konfigurációját a használatban lévő adatbázis-kezelő rendszer biztonsági specifikációja alapján kell megvalósítani.

Az operációs rendszerbeli felhasználók, akik nevében az adatbázisból kezdeményezett külső eljárások futnak, csak a szükséges (azaz minimális) operációs rendszerbeli jogosultságokkal rendelkezzenek.

Az adatbázis rendszeren kívül, az adatbázis helyi hoszt gépén tárolt objektumokat az adatbázis-kezelő rendszerből ne lehessen elérni, kivéve, ha a helyes működés ezt megköveteli. Ebben az esetben ezt dokumentálni kell.

Az adatbázis alkalmazás felhasználói szerepköre ne adjon illetéktelen hozzáférési lehetőséget külső adatbázis objektumok elérésére.

A.3.5 Tükrözés, elosztott rendszerek, database link

Távoli adatbázisokhoz, távoli vagy külső alkalmazásokhoz és folyamatokhoz történő adatbázis kapcsolat csak szükséges esetben engedélyezett megfelelő szabályzati dokumentáció mellett. A távoli adatbázishoz történő kapcsolódáskor (database link) használt hitelesítés alapulhat (1) a kezdeményező adatbázis munkafolyamat (session) hitelesítési információira vagy pedig (2) statikusan beállított felhasználó névre és jelszóra.

Az adatbázis kapcsolat (database link) definiálásakor a biztonsági konfigurációs szempontokat be kell tartani. A publikus database link használata biztonsági okok miatt kerülendő. Helyette privát database link használata célszerű.

Az adatbázis rendszerből távoli adatbázisok és alkalmazások eléréséhez szükséges hitelesítési információk csak arra felhatalmazott adatbázis felhasználók számára legyenek elérhetőek és csak a működés szempontjából szükséges célokra legyenek használva megfelelő dokumentáció mellett. A hitelesítési információk titkosított formában legyenek tárolva és teljes minősített nevet tartalmazzanak (azaz legyenek globálisan egyediek) a kapcsolat specifikációjában.

Az adatbázis tükrözés folyamatának védelme érdekében önálló adatbázis felhasználót kell létrehozni a tükrözés adminisztrációja, illetve magának a tükrözési folyamatnak a végrehajtása számára. A tükrözési folyamat hitelesítési információit a hálózati forgalomban

védeni kell. A tükrözés folyamatához és konfigurációjához csak felhatalmazott felhasználók férhessenek hozzá. A tükrözési adatok speciális operációs rendszer könyvtárban lehetnek ideiglenesen eltárolva. Ezeket az adatokat megfelelően védeni kell jogosulatlan hozzáféréssel szemben.

A.3.6 Távoli hozzáférés adminisztrációs feladatok elvégzésekor

Az adatbázis-kezelő rendszer távoli adminisztrációja sokszor megkönnyíti a kívánt feladatok elvégzését, ugyanakkor biztonsági rést okozhat a rendszerben, ezért használatát célszerű kerülni. Ha a működés megköveteli az adatbázis távoli adminisztrációját, az csak fokozott körültekintés és védelem mellett használható visszaélések elkerülése érdekében.

Távoli adminisztrációt csak meghatározott hálózati helyekről (cím és port szám) szabad engedélyezni titkosítás használata mellett.

A.4 Adatbázist elérő alkalmazások biztonsági beállításai

Az adatbázist elérő alkalmazásoknak a lehető legszűkebb szerepkörrel szabad az adatbázisokhoz hozzáférést biztosítani. Ha egy alkalmazást privilegizált szereppel (pl. adatbázis adminisztrátorként) engedünk egy adatbázishoz hozzáférni, annak szükségességét minden esetben külön dokumentálni kell.

Az alkalmazás számára megadott felhasználói adatok helyességét ellenőrizni kell.

Az érzékeny adatokhoz történő hozzáférést mind az alkalmazás, mind az adatbázis szintjén naplózni kell.

A helyi és a hálózaton elérhető adatbázis szolgáltatásokat egyértelműen meg kell határozni és azonosítani.

A.5 Adatbázis adatfájljainak védelme

Az adatbázis adatfájljait operációs rendszer szintjén is védeni kell a jogosulatlan hozzáférésekkel szemben. Ezekre az állományokra a hozzáférési beállításokat a legkisebb jogosultság elve szerint kell beállítani, az aktuális adatbázis-kezelő rendszer biztonsági útmutatója alapján.

Az adatbázis adatfájljai – beleértve a tranzakciós logokat és audit fájlokat is -- kijelölt könyvtárakban vagy lemez partíciókon legyenek, melyek különböznek más szoftver és alkalmazás fájlokat tartalmazó könyvtáraktól és partícióktól.

Az adatbázis-kezelő rendszer működését támogató rendszertáblák és rendszerobjektumok elkülönítve, számukra kijelölt könyvtárban vagy partíción legyenek az adatbázis alkalmazások által használt adatbázis objektumoktól.

A különböző alkalmazásokhoz tartozó adatfájlok alkalmazásonként legyenek meghatározva és elkülönítve.

Az adatbázis-kezelő rendszer állományainak kontrolljakor el kell különíteni az éles rendszer adatait az egyéb járulékos adatoktól.

A.6 Adatbázis objektumok védelme hozzáférés szabályozással

A.6.1 Általános elvek

Az adatok jogosulatlan megváltoztatása, törlése, elérhetetlenné tétele és közzététele elkerülésének érdekében a hozzáférés szabályozásban a legkevesebb privilégium elvét és a feladatkörök szétválasztását kell alkalmazni.

Az adatbázisban vagy külső fájlokban található érzékeny adminisztrációs adatbázis adatokhoz csak az adatbázis adminisztrátor és más erre felhatalmazott adatbázis vagy operációs rendszerbeli felhasználó férhessen hozzá.

Az adatbázisban vagy külső fájlokban található érzékeny alkalmazás adatokhoz csak a megfelelő felhasználói szerepkörrel bíró adatbázis vagy operációs rendszerbeli felhasználó férhessen hozzá.

Az adatbázisból távoli adatbázisba vagy alkalmazásba exportálandó érzékeny alkalmazás adatokhoz fel nem hatalmazott felhasználók vagy alkalmazások ne férhessenek hozzá.

Az adatbázis objektumokból kinyerhető érzékeny alkalmazás adatokhoz való hozzáférés adatbázis szerepkörökhöz kötött és nem individuális felhasználókhoz.

Éles környezetben használt adatbázis adatokat teszt környezetbe importálni tilos, kivéve, ha ezt felsőbb biztonsági vezetők jóváhagyják.

Az adatbázis felhasználók csak annyi adatbázis jogosultsággal rendelkezzenek, amennyit a saját feladatkörük megkíván.

A.6.2 Objektum privilégiumok

Az adatbázis rendszerben élő jogosultságok – más szóval privilégiumok – két csoportra oszthatók, a rendszer és az objektum típusúakra. Az objektum jogosultságok azt

szabályozzák, hogy már létező adatbázis objektum esetén egy felhasználó olvashatja-e, módosíthatja-e, törölheti-e, illetve – ha aktuális – lefuttathatja-e az adott objektumot.

Adatbázis objektum privilégiumok – vagyis adatbázis objektumokhoz való hozzáférés - hozzárendelése az adatbázis alkalmazás felhasználókhoz ne közvetlenül, hanem szerepkörökön keresztül történjék. A szerepkörök meghatározását a felhasználók feladatköre alapján kell elvégezni.

Objektum privilégiumokat nem szabad nyilvánossá (PUBLIC) minősíteni, azaz az adatbázis összes felhasználója számára alapbeállításként megadni. Az adatbázis-kezelő rendszer telepítésekor automatikusan nyilvánosnak beállított objektum jogosultságtól a PUBLIC opciót vissza kell vonni, ahol ez kivitelezhető.

Adatbázis adminisztrátori nézetekhez és rendszer táblákhoz – például adatszótár objektumokhoz - való hozzáférést korlátozni kell az adatbázis rendszer, adatbázis adminisztrátorok és más adminisztrátori vagy biztonsági funkciót betöltő, illetve batch folyamatok feldolgozását ellátó felhasználók részére.

Az adatbázis objektum tulajdonosa teljes jogosultsággal rendelkezik az adott adatbázis objektum felett. Minden adatbázis objektumnak az adatbázis adminisztrátor, az adatbázis rendszer vagy egy speciális felhasználó – akit direkt az adott alkalmazás adatbázis objektumainak birtoklására hoztak létre – legyen a tulajdonosa. Installáláskor automatikusan létrejövő egyéb adatbázis felhasználók ne lehessenek adatbázis objektum tulajdonosok.

Ajánlatos minden alkalmazás esetében létrehozni egy speciális adatbázis felhasználót –az úgynevezett alkalmazás tulajdonos felhasználót -, aki az adott alkalmazáshoz tartozó összes adatbázis objektumnak a tulajdonosa lesz. Alkalmazás felhasználók ne legyenek alkalmazás objektum tulajdonosok.

Alkalmazás tulajdonos felhasználónak legyen egyedül joga a tulajdonában lévő adatbázis objektumokat érintő objektum jogosultságokat alkalmazás szerepkörökhöz hozzárendelni. Alkalmazás tulajdonos felhasználóként az adatbázisba belépni csakis az alkalmazás adatbázis objektumainak módosítása és karbantartása céljából szabad. Ezen időszakon kívül a biztonság érdekében célszerű az alkalmazás tulajdonos felhasználót zárolni.

A.6.3 Rendszer privilégiumok

Rendszer privilégiumok adatbázis rendszer szintű módosítások, adminisztratív feladatok elvégzését teszik lehetővé. Rendszer privilégiumokat szerepkörökön keresztül kell kiosztani.

Rendszer privilégiumokat nem szabad nyilvánossá (PUBLIC) minősíteni, azaz az adatbázis összes felhasználója számára alapbeállításként megadni.

Rendszer privilégiumokat adatbázis adminisztrátorok számára szabad beállítani. Bizonyos esetekben szükséges lehet privilégiumokkal ellátott felhasználók – például alkalmazás adminisztrátorok, automatikus feldolgozásra létrehozott felhasználók - számára is rendszer privilégiumokat hozzárendelni. Alkalmazás felhasználók számára ne engedélyezzünk rendszer privilégiumot.

A.7 Adatok védelme titkosítással

Az adatbázis rendszerben titkosításhoz, digitális aláíráshoz, kulcs cseréhez és hash algoritmushoz csak megfelelő erősségű és szabványos kriptográfiai módszereket lehessen alkalmazni.

A jelszavak és más érzékeny adatok titkosítására használt szimmetrikus kulcsokat a megfelelő kulcskezelésre vonatkozó szabványok és eljárások szerint kell védeni és menedzselni.

Az érzékeny adatok titkosítására használt aszimmetrikus kulcsokhoz megfelelően szabványos tanúsítványokat kell használni és a titkos kulcsokat szabványos kulcs menedzsment technikák szerint kell védeni és tárolni.

A.7.1 Hálózaton

Az adatbázis távoli adminisztrációja esetén a kapcsolatot titkosítani kell.

Az adatbázis érzékeny adatainak nem megbízható hálózaton történő továbbítását titkosítani kell.

A.7.2 Adatbázisban

Ahol az előírás megkívánja, ott az adatbázisban tárolt érzékeny adatokat titkosított formában kell tárolni. Ahol az adatok titkosítását adatbázison belül nem lehet megoldani, ott az adatbázis adatfájljait kell titkosítani.

Az adatbázis rendszer titkosítással kapcsolatos biztonsági követelményeit dokumentálni kell és ez alapján kell azokat megvalósítani.

Az adatbázisban tárolt és feldolgozott érzékeny adatokat azonosítani és dokumentálni kell.

Az adatbázison belüli forráskódok a támadók számára értékes információkkal szolgálhatnak. Az adatbázisban tárolt, nem nyilvános forráskód objektumokat (például triggereket,

eljárásokat) célszerű titkosítással védeni, ha erre az adatbázis-kezelő rendszer lehetőséget biztosít.

B. Adminisztratív kontrollok

B.1 Adatbázis felhasználók megkülönböztetése

Az adatbázis rendszer felhasználóit a feladatkörük alapján különböző kategóriákba sorolhatjuk be. Jelen Útmutatóban a következő főbb kategóriákat különböztetjük meg:

B.1.1 Adatbázis alkalmazás felhasználó

Az adatbázis alkalmazás felhasználónak az adott alkalmazás adatbázis objektumaihoz van hozzáférési lehetősége. A felhasználó jogosultsága az adatbázis objektum olvasására (select), beszúrására (insert), módosítására (update), törlésére (delete) és futtatására (execute) korlátozódik.

B.1.2 Adatbázis adminisztrátor

Az adatbázis adminisztrátor felelős az adatbázis rendszer konfigurálásáért, működtetéséért és a felhasználók menedzseléséért. Legtöbbször teljes körű jogosultsága van az összes adatbázis objektum és erőforrás felett.

B.1.3 Alkalmazás tulajdonos

Az alkalmazás tulajdonos felhasználó az adott alkalmazáshoz tartozó összes adatbázis objektumnak a tulajdonosa. Az alkalmazás tulajdonos felhasználó definiálhat alkalmazáshoz tartozó szerepköröket, illetve meghatározhatja ezen szerepkörökhöz tartozó és a tulajdonában lévő adatbázis objektumokat érintő objektum jogosultságokat. Az alkalmazás tulajdonos jogosultsága az alkalmazás adatbázis objektumainak létrehozására, módosítása vagy törlésére korlátozódik.

B.1.4 Alkalmazás felhasználó adminisztrátor

Az alkalmazás felhasználó adminisztrátor létrehozza, szerepkörökkel felruházza és menedzseli az alkalmazás felhasználókat.

B.1.5 Automatikus feldolgozás számára létrehozott felhasználók

Automatikus feldolgozás céljából létrehozott felhasználók speciális feladatkörrel bírnak (például napló adatok tárolása távoli eszközökön vagy emberi beavatkozást nem igénylő karbantartást végző batch jobok futtatása). Ezeket a feladatokat nem személyhez kötött (azaz

humán) adatbázis felhasználóknak kell ellátniuk és használatukat speciális körültekintés kell, hogy kísérje. Az automatikus feldolgozást végző felhasználókhoz kötődő elsődleges sérülékenységet a felhasználó nevének és jelszavának gyakori tárolási igénye jelenti alkalmazás kódokban és külső fájlokban, továbbá ezen információk felfedése a felhasználók bejelentkezési folyamatai során.

Az azonosítási információk megfelelő védelmét és titkosságát biztosítani kell, ennek módja függ a használatban lévő operációs és adatbázis rendszertől. A felhasználók aktivitását bizonyos időszakokra (például a nap bizonyos óráira) célszerű korlátozni, ezáltal is a biztonságos használatot segítjük elő. Az automatikus feldolgozásra létrehozott felhasználók jelszavainak élettartamát a feladatkörükhöz specifikusan kell beállítani (maximum egy év a javasolt). Az automatikus feldolgozásra létrehozott felhasználókat és feladatkörüket dokumentálni szükséges.

B.2 Adatbázis szerepkörök

A felhasználók jogosultságait a legkevesebb privilégium elve alapján kell beállítani, nem egyéni hozzárendelés útján, hanem szerepkörök segítségével. Adatbázis szerepkörök segítségével jogosultságok körülhatárolt rendszerét lehet egyidejűleg felhasználókhoz hozzárendelni, illetve tőlük azokat visszavonni. Tipikus adatbázis felhasználói szerepkörök a következők: adatbázis adminisztrátori szerepkör, alkalmazás adminisztrátori szerepkör, meghatározott alkalmazáshoz tartozó felhasználói szerepkör (pl. pénzügyi rendszer felhasználói szerepkör).

Az adatbázis adminisztrátornak biztosítania kell, hogy az adatbázis jogosultságokat szerepkörök segítségével rendelik a felhasználókhoz és nem egyéni beállítások útján. Ha az adatbázis-kezelő rendszer nem támogatja a szerepkörök szerinti jogosultság beállítást, akkor azok egyéni beállítását kell alkalmazni.

Az adatbázis szerepkörök és a hozzájuk tartozó jogosultságok ellenőrzöttek és megfelelően dokumentáltak

Csak azok a felhasználók rendelkezzenek speciális adatbázis jogosultságokkal, akiknek a feladatköre ezt ténylegesen igényli is.

Az adatbázis szerepköröket nem szabad nyilvánosnak (PUBLIC) minősíteni, ugyanis ezáltal a szerepkörhöz tartozó összes adatbázis jogosultságot minden adatbázis felhasználóhoz hozzárendelnénk.

Tükrözéshez és elosztott rendszerben történő tranzakciókhoz használt adatbázis felhasználók ne rendelkezzenek adatbázis adminisztrátori privilégiumokkal.

B.2.1 Adatbázis adminisztrátori szerepkör

Biztosítani kell, hogy adatbázis adminisztrációs szerepkörök számára a minimálisan szükséges jogosultságok tartoznak. Adatbázis adminisztrátori szerepkör csak adminisztrációs feladatok ellátására legyen jogosult, ne legyen használható alkalmazásfejlesztésre, tesztelésre és alkalmazás felhasználásra. Ezen követelmény teljesülését rendszeresen (például havonta) felül kell vizsgálni.

Az adatbázis-kezelő rendszeren belüli és azon kívüli adatbázis adminisztrációs jogosultságok csak adatbázis és operációs rendszerbeli szerepkörökön keresztül kerüljenek kiosztásra.

Telepítéskor automatikusan létrejövő adminisztrátori szerepköröket, felhasználókat és jelszavakat törölni kell, majd egyénileg létre kell hozni a szükséges beállításokkal.

Operációs rendszerbeli csoporthoz történő hozzárendeléssel adatbázis adminisztrációs jogosultságok megadása esetén a felhasználókat egyénileg kell az operációs rendszerbeli csoporthoz hozzárendelni.

Adatbázis adminisztrátori szerepkört csak arra felhatalmazott adatbázis adminisztrátorok számára szabad beállítani az éles adatbázis környezetben. Fejlesztői adatbázis környezetben adatbázis adminisztrátori szerepkört csak adatbázis adminisztrátorok és arra felhatalmazott alkalmazás fejlesztők számára szabad beállítani.

Adatbázis adminisztrátori szerepkör minden kiosztásakor felül kell vizsgálni az addigi kiosztást.

Az adatbázisok helyreállításának jogosultságával csak az adatbázis adminisztrátor, és/vagy az adatbázis tulajdonosa rendelkezzen.

B.2.2 Alkalmazás fejlesztői szerepkör

Alkalmazás fejlesztői szerepkör számára a fejlesztői környezetben szükséges adatbázis jogosultságokat rendeljük hozzá.

Optimális esetben alkalmazás fejlesztői szerepkörrel rendelkezők ne férhessenek hozzá az éles adatbázis rendszerhez. Kivételes körülmények között, például hibaelhárítás során szükséges lehet alkalmazás fejlesztők számára hozzáférést engedélyezni az éles rendszerhez. Ilyenkor csak korlátozott időre, felsőbb vezetők írásos engedélye alapján szabad számukra

hozzáférést engedélyezni. Az adatbázis fejlesztők ne rendelkezzenek rendszer szintű jogosultságokkal az éles adatbázis rendszerben.

B.2.3 Adatbázis alkalmazás felhasználói szerepkör

Alkalmazás felhasználókhoz jogosultságokat ne egyénileg, hanem szerepkörökön keresztül rendeljük hozzá. Kivételt képezhet, ha egyetlen ilyen alkalmazás felhasználó létezik az adatbázis rendszerben, illetve azok az automatikusan létrejövő adatbázis felhasználók, akik az adatbázis rendszer telepítésekor és karbantartásakor jönnek létre.

Minden alkalmazás számára létre kell hozni szerepköröket, melyek az adott alkalmazás felhasználói számára szükséges jogosultságokkal bírnak. Alkalmazás felhasználói szerepkörökhöz kizárólag azokat a jogosultságokat szabad hozzárendelni, melyek a felhasználóhoz tartozó feladatkör elvégzéséhez feltétlen szükségesek.

Alkalmazásonként létezhet alkalmazás adminisztrátori szerepkör is. Alkalmazás adminisztrátori szerepkör az adatbázis alkalmazás felhasználóinak karbantartására szolgál.

Minden adatbázis alkalmazás felhasználó számára be kell állítani a szükséges alkalmazás felhasználói szerepkört (akár többet is).

Az adatbázis alkalmazás felhasználói szerepköre a SELECT, INSERT, UPDATE, DELETE és EXECUTE privilégiumokra korlátozódhat.

Az adatbázis alkalmazás felhasználói szerepköre ne adjon illetéktelen hozzáférési lehetőséget külső adatbázis objektumok elérésére.

B.2.4 Adatbázis alkalmazás adminisztrátori szerepkör

Bizonyos esetekben szükségese lehet olyan szerepkörre, ami alkalmazás felhasználók karbantartására, kezelésére szolgál. Alkalmazás felhasználók létrehozása, ezekhez szerepkörök hozzárendelése és profilok beállítása tartozik a feladatkörébe.

Adatbázis alkalmazás adminisztrátori szerepkör kizárólag adminisztrációs feladatok ellátására szolgál és nem alkalmazható alkalmazás felhasználói feladatok ellátására.

C. Működési kontrollok

C.1 Ügyrendi, biztonsági és egyéb eljárások szabályzatok

Meg kell határozni a szervezet adatbázis rendszerének működését és biztonságát érintő dokumentumok és szabályozók típusait, céljait, illetve ki kell ezeket dolgozni. Meg kell

határozni az adatbázis rendszer működését és biztonságát érintő, a szervezet informatikai rendszerével kapcsolatos működési és biztonsági dokumentumokat és szabályozókat.

A szervezet adatbázis-biztonsági szabályzatát és eljárásrendjét legalább évente egyszer felül kell vizsgálni, továbbá ezeknek konzisztensnek kell lenniük az egyéb (állami, iparági, szervezeti, gyártó-specifikus) informatikai biztonsági követelményekkel.

A szervezet informatikai rendszerével és ennek részét képező adatbázis rendszerével kapcsolatos vezetői, biztonsági és adminisztratív szerepköröket és a hozzájuk tartozó feladatokat meg kell határozni, és írásba kell foglalni. A szervezeten belül az említett szerepköröket betöltő személyeket meg kell határozni és dokumentálni kell.

Az adatbázis-kezelő rendszert időközönként sérülékenység vizsgálati tesztelés alá kell vonni, illetve vizsgálni kell, hogy megfelel-e a biztonságos konfigurációs követelményeknek.

Biztosítani kell, hogy az adatbázis-kezelő rendszer konfiguráció menedzsmentjét megvalósító eljárások a szervezeten belül kialakítottak, dokumentáltak és alkalmazottak. (Jelen dokumentumban konfiguráció menedzsment alatt az adatbázis-kezelő rendszer konfigurációját, szoftver könyvtárait és más, az adatbázis rendszerhez kötődő alkalmazás szoftver könyvtárait érintő változások kezelését és nyilvántartását értjük.)

C.2 Adatbázis-kezelő rendszer telepítése és biztonsági frissítése

C.2.1 Adatbázis-kezelő rendszer telepítésének és frissítésének tesztelése

Az adatbázis-kezelő rendszer telepítését, frissítését és foltozását az éles környezetbe való beállítás előtt előre definiált, dokumentált tesztelési eljárásrend kell, hogy megelőzze.

C.2.2 Az adatbázis-kezelő rendszer frissítése

Az aktuális rendszert érintő, a gyártó által kifejlesztett biztonsági foltozást telepíteni kell.

Az adatbázis-kezelő rendszer szoftverét a gyártó időközönként frissíti újabb verziók és foltozások kiadásával. Az elavult verziókhoz egy bizonyos idő után a gyártó nem gondoskodik támogatásról, ezáltal ezek sérülékenysége megnövekszik. Emiatt nagyon fontos a szoftverek folyamatos frissítése és foltozása.

A gyártó által már nem támogatott szoftver komponenseket a támogatás felfüggesztése előtt el kell távolítani és az adatbázis-kezelő rendszer szoftverének frissítését végre kell hajtani.

Az adatbázis-kezelő rendszer eltávolítására és új verziójának frissítésére vonatkozó átállási tervet el kell készíteni legalább 6 hónappal azelőtt, hogy a gyártó az aktuális rendszer támogatását felfüggesztené.

C.2.3 Az adatbázis-kezelő rendszer elkülönítése, a nem használt komponensek eltávolítása

Az adatbázis szerver számára elkülönített számítógép álljon rendelkezésre, amin ne fusson web-, alkalmazás-, fájl-, nyomtató- vagy más szolgáltatás, kivétel, ha a működés úgy kívánja meg. Ebben az esetben a többszörös használatot dokumentálni szükséges.

Az adatbázis-kezelő rendszer hoszt gépén nem futhat címtárszolgáltatás (directory service) és egyéb biztonsági szolgáltatás, kivéve, ha az adatbázis-kezelő rendszer a biztonsági szolgáltatás egyik részelemét képezi. Windows tartományvezérlőre (Windows Domain Controller) ne telepítsük az adatbázis-kezelő rendszert.

Az adatbázis rendszer telepítésekor automatikusan létrejövő felhasználó neveket és jelszavakat törölni, megváltoztatni vagy érvényteleníteni kell.

Tesztelés és egyéb nem üzemeltetési célból telepített adatbázis komponensek, alkalmazások, felhasználói fiókok és objektumok az éles használat előtt eltávolítandók az adatbázis rendszerből és az adatbázis-kezelő rendszert futtató hoszt gépről.

A működés során nem használt adatbázis komponenseket, programokat, alkalmazásokat és objektumokat el kell távolítani az adatbázis rendszerből és az adatbázis-kezelő rendszer hoszt gépéről. Ha valamely ilyen komponens nem eltávolítható, akkor azt le kell tiltani.

C.3 Felhasználók azonosítása, hitelesítése, bejelentkezése

C.3.1 Csoportos azonosítás és hitelesítés

Csoportos hitelesítéskor egy azonosítóval több felhasználó is csatlakozhat az adatbázis rendszerhez. Csoportos hitelesítés használata gyakori alkalmazások adatbázis elérésének megvalósításakor. Ekkor az adatbázis szintjén történő egyénekre bontott auditálási lehetőség elveszhet, azt az alkalmazás réteg szintjén kell megvalósítani. 3 vagy több rétegű architektúrák esetén gyakori, hogy az alkalmazás szerver a mögötte álló adatbázis réteghez csoportos hitelesítés útján csatlakozik.

A biztonság és elszámoltathatóság érdekében csoportos azonosítás és hitelesítés esetén másodlagos módszerek segítségével célszerű a felhasználók egyértelmű azonosítását megvalósítani, ezáltal egy felhasználó egyértelműen hozzárendelhető lesz egy konkrét

cselekményhez. A csoportos hitelesítést megvalósító felhasználó bejelentkezését hálózati konfiguráció és a kérvényező alkalmazás alapján korlátozni kell.

Csoportos azonosítás használatát engedélyeztetni és dokumentálni kell.

C.3.2 Egyéni azonosítás és hitelesítés

Az adatbázis-kezelő rendszerhez való csatlakozás megvalósításánál az egyéni felhasználói hitelesítést kell előnyben részesíteni és lehetőség szerint alkalmazni. Azaz egy adott adatbázis csatlakozás egyértelműen hozzárendelhető legyen egy felhasználóhoz.

C.3.3 Inaktív felhasználók

A jogosulatlan adatbázis felhasználókat a rendszerből törölni vagy kizárni szükséges.

Az adatbázis felhasználók inaktivitását és érvényességük lejárását monitorozni kell. Egy meghatározott időtartamon felüli inaktív vagy lejárt érvényességű felhasználót törölni kell a rendszerből.

C.3.4 Jelszavak tárolása és tulajdonságai

Az adatbázis felhasználók jelszavai titkosított formában tárolandók, függetlenül attól, hogy az adatbázison belül, külső fájlokban, környezeti változókban vagy más helyen találhatók meg. Az adatbázisban tárolt felhasználó nevek és jelszavak az adatbázis-kezelő rendszer hoszt gépének és kliens gépeknek operációs rendszerei számára ne legyenek láthatóak.

Az adatbázis felhasználók jelszavai a hálózati kommunikációban is titkosított formában jelenhetnek csak meg.

Az adatbázis felhasználói jelszavak nem jelenhetnek meg batch fájlokban és alkalmazás forráskódokban.

Az adatbázis felhasználót létrehozásakor ideiglenes jelszóval kell ellátni.

A jelszavakra vonatkozó biztonsági megszorításokat (pl. jelszó hossza, komplexitása, megváltoztatásának körülményei, élettartama) le kell fektetni és be kell tartatni.

C.3.5 Tokenekre és tanúsítványokra vonatkozó szabványok

Olyan környezetekben, ahol a felhasználó név és jelszó szerinti azonosítás és hitelesítés nem nyújt kielégítő biztonsági szintet, megfelelően szabványos tanúsítványokat, hardver alapú biztonsági tokeneket és termékeket kell használni az azonosítás és hitelesítés céljaira.

C.3.6 Adatbázis rendszerekbe történő belépések

Az adatbázishoz történő kapcsolódási kísérletek számát egy meghatározott időkereten belül korlátozni kell.

A sikertelen belépési kísérletek miatti felhasználói zárolás időtartamát korlátlanra kell állítani, így az adatbázis adminisztrátor feladata lesz a zárolás feloldása.

Ha az adatbázis-kezelő rendszer lehetővé teszi, az adatbázis adminisztrátornak be kell állítani egy korlátot az adatbázis felhasználók egyidejű kapcsolódásainak maximális számát illetően. Ez a korlát az adott rendszer tesztelése és log elemzése alapján állítható jól be. A korlát csak kivételes működési feltételek miatt legyen végtelenre állítva, és a rendszer biztonsági dokumentációjában legyen feltüntetve.

Felhasználók adatbázis kapcsolataira maximális üres járatidőt (maximum idle time) kell beállítani, ezáltal DoS és munkafolyamat eltérítéses (session hijacking) támadások kockázatát lehet csökkenteni.

C.4 Adatbázis audit, log elemzés

C.4.1 Általános követelmények

Az adatbázis-kezelő rendszerben az audit funkciót konfigurálni és használni kell. Az adatbázis műveleteket, úgy mint az adatbázis objektumok megváltoztatását, adatbázis paraméterek és állományok módosítását, adatbázis-kezelő rendszer és annak hoszt gépének eseményeit (például leállítás, indítás) auditálni kell.

Az audit adatokat a biztonsági előírásnak megfelelő ideig meg kell őrizni és védeni kell a jogosulatlan hozzáférésekkel szemben. Az audit adatok törlését és módosítását felül kell vizsgálni.

Dokumentálni kell, hogy a rendszerben kinek van jogosultsága az audit adatokhoz való hozzáféréshez.

C.4.2 Az audit tartalma

Az auditálandó eseményeket meg kell határozni és dokumentálni kell.

Az adatbázis-kezelő rendszer konfigurációs fájljaihoz, audit adataihoz, hitelesítési információihoz és más adatbázis-biztonsági adatokhoz való hozzáférést auditálni kell.

Az adatbázis rendszerbe való belépéseket, felhasználói kizárásokat, csatlakozási lehetőségek ellehetetlenítését, hozzáférések megakadályozását és a hozzáférés kontrol kijátszását auditálni

kell. Ahol az audit adatok erőforrása korlátozott, a felhasználói belépések rögzítését korlátozni lehet a sikertelen esetekre.

Privilégiumokhoz kötött (például adatbázis adminisztrátori) adatbázis rendszer tevékenységeket auditálni kell. A távoli adminisztráció teljes folyamatát auditálni kell és az audit nyomot naponta felül kell vizsgálni.

Az audit adatok tartalmazzák az auditált eseményhez kötődő felhasználó azonosítóját, az esemény időpontját és az esemény típusát.

Az audit adatok tartalmazzák a felhasználói kizárások és csatlakozási pontok megszüntetésének okát.

Léteznek adatbázis-kezelő rendszerek, melyek a tárolt adatokat biztonsági szempontból osztályozzák és jelölik. Ilyen esetekben a bizalmas/érzékeny adatok biztonsági osztályainak módosulását auditálni kell. Az érzékeny adatokban végbement változást a biztonsági szabályzat alapján kell auditálni.

Az adatbázis-kezelő rendszer telepítését végző operációs rendszer felhasználó tevékenységét logolni és/vagy auditálni kell annak érdekében, hogy ennek segítségével belépett személyeket követni lehessen.

C.4.3 Audit nyomvonal, monitorozás, elemzés és jelentés

Audit vonalnak (audit trail) nevezzük az audit rekordok kronologikus sorozatát. Ahol lehetséges, az audit nyomvonalnak tartalmaznia kell az auditált eseményt kiváltó adatbázishoz kapcsolódó alkalmazás nevét.

Rendszeresen ellenőrizni kell az audit adatokat. A gyanús és jogosulatlan eseményeket azonnal jelenteni kell.

Célszerű automatikus eszközöket, szoftvereket alkalmazni az adatbázis audit adatainak felügyelete és monitorozása céljából.

Az adatbázis rendszer audit nyom adatait legalább 1 évig őrizni kell.

Az audit adatok mellett rendszeresen monitorozni kell az adatbázis rendszerhez történő alkalmazás kapcsolatokat a jogosulatlan elérés észrevétele céljából.

Rendszeresen monitorozni kell a lejárt érvényességű és az inaktív felhasználókat.

Rendszeresen monitorozni kell az adatbázis rendszerhez kötődő batch és job sorokat annak érdekében, hogy jogosulatlan folyamatok ne érhessék el az adatbázist és a jogosulatlan használat észlelésre kerüljön.

C.5 Éles és teszt környezetek szétválasztása

Alkalmazás fejlesztők adatbázis hozzáférése csak a minimálisan szükséges jogosultságokkal rendelkezzen, annak érdekében, hogy az éles rendszer adatbázis objektumai védettek maradjanak.

Minimum háromhavonta felül kell vizsgálni a fejlesztők számára beállított jogosultságokat a nem elkülönített, egyszerre fejlesztői és éles adatbázis rendszerekben, különös tekintettel azokra a jogosultságokra, melyek alkalmazásokhoz tartozó adatbázis kódok és objektumok megváltoztatását teszik lehetővé.

A nem elkülönített, egyszerre fejlesztői és éles adatbázis rendszerek hoszt gépén a fejlesztők számára beállított jogosultságok ne tartalmazzanak operációs rendszerbeli jogosultságokat az éles rendszert érintő rendszer fájlokhoz, könyvtárakhoz és adatbázis komponensekhez.

DDL utasításnak nevezzük az adatbázis objektumokra vonatkozó CREATE, DROP és ALTER parancsokat. Az éles adatbázis környezetben DDL utasítások kiadása kerülendő, mivel e parancsok használata a fejlesztés fázisába tartozik. Kivételt képez a dinamikus adatbázis objektum struktúrák használata (például objektum orientált adatbázisok esetén), ekkor ugyanis új objektumok keletkezése a korrekt működés következményének tekinthető.

Az éles adatbázis rendszerben a szoftverfejlesztés különálló egységet képez elkülönített és egyértelműen azonosított adat és alkalmazás fájl partícióval, folyamatokkal és szolgáltatásokkal.

C.6 Adatbázismentés és helyreállítás

Az adatbázis mentési és helyreállítási stratégiáját legalább évente felül kell vizsgálni, tesztelni és dokumentálni kell. Az adatbázis rendszer és támogató részrendszereinek helyreállítási prioritását meg kell határozni és írásba kell foglalni.

Az adatbázisban tárolt adatokat, konfigurációs és egyéb működéskritikus fájlokat az adatbázis kritikusságától függő időközönként menteni kell. Az adatbázis mentési folyamatának ki kell terjedni az általa létrehozott audit állományokra is.

A kritikus adatbázis szoftver könyvtárakat meghatározott időközönként menteni kell.

Az adatbázis rendszer helyreállításához szükséges fájlokat védeni kell az adatbázis és operációs rendszer magas rendelkezésre állás technikái segítségével - például a RAID technológiával megvalósított tárolással.

Az adatbázis mentési és helyreállítási fájljaihoz való hozzáférés kizárólag az adatbázis és operációs rendszer mentési és helyreállítási folyamatai, az adatbázis adminisztrátorok és az adatbázis rendszer mentési és helyreállítási operátorai számára biztosított.

Olyan adatbázis rendszerek esetén, ahol az adatok bizalmassága elvárt biztonsági kritérium, szabályozni kell a mentési adatokat kezelését. Vagy a mentések titkosítását kell előírni, vagy egyéb adminisztratív eszközökkel kell biztosítani az adatok illetéktelen megszerzését.

Az adatbázis-kezelő rendszert úgy kell konfigurálni, hogy a helyreállítási folyamat során kizárólag megbízható szoftver, adat és egyéb fájlokat használjon fel.

4.4 KÖVETKEZTETÉSEK

A fejezetben felvázolt elemzések alapján az adatbázis-biztonság szabályozásával kapcsolatban összegzésképpen a következőket fogalmazom meg. A kellően kritikus adatbázisokat üzemeltető közigazgatási szervek számára az adatbázis-biztonság szabályozását az elektronikus közigazgatás biztonságával kapcsolatos kormányrendeletnek kellene előírnia. A kormányrendelet meghatározná a szabályozó alá eső szervezetek körét. A kormányrendelet hivatkozna egy már létező, – például a Közigazgatási Informatikai Bizottság által kiadott – adatbázis-biztonsági útmutatóra, melynek adaptációját és használatát kötelezően előírná a megnevezett szervezetek számára. A kormányrendelet előírná továbbá, hogy az érintett szervezeteknek bizonyos időközönként belső ellenőrzést kell lefolytatniuk az adatbázis-biztonsági útmutató kontrolljai alapján. A szabályozó dokumentum tartalmazná a felügyeletet ellátó központi szerv nevét is. A kormányrendelet által hivatkozott adatbázis-biztonsági útmutató mintaként szolgálna a szervezetek számára a saját adatbázis-biztonsági útmutató elkészítéséhez, mely már szervezet és tevékenység specifikusan tartalmazná a követelményeket, előírásokat. A szabályozó által hivatkozott adatbázis-biztonsági útmutató az adatbázis üzemeltetők feladatául jelölné ki termékfüggő adatbázis ellenőrzési listák elkészítését is.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Értekezésemben áttekintettem az adatbázis-biztonság alapjait, ennek keretében elemeztem az adatbázis-biztonság fogalmát, helyét és szerepét. Az adatbázis-biztonság fogalmának elemzésekor meghatároztam a biztonság alanyát, ennek védendő tulajdonságait. Az adatbázis-biztonság alanyának mind az adatbázisban tárolt adatokat, mind az azokat kezelő adatbázis-kezelő rendszereket tekintem, védendő tulajdonságok közé elsődlegesen a bizalmasságot, sértetlenséget és rendelkezésre állást sorolom. Megállapítottam, hogy az adatbázis-biztonság az informatikai biztonság egyik fontos részterülete, ugyanakkor azt csak az informatikai rendszer többi elemével egységben, komplex módon lehet megvalósítani.

Értekezésemben elvégeztem az információs jellegű adatbázis fenyegetések rendszerezését, ehhez többféle szempontrendszert is megadtam. Az informatikai rendszerek védelme és az adatbázis-biztonság megvalósítása szempontjából legfontosabbnak a támadási pont szerinti rendszerezést tartom. Az adatbázis fenyegetéseket a támadási pont (azaz a támadás által kihasznált sérülékenység architektúrában elfoglalt helye) szerint rendszerezve megkülönböztettem az adatbázis-kezelő rendszernek, az adatbázisokban tárolt adatoknak, az adatbázis-kezelő rendszer platformjának, a hálózatnak és az alkalmazásoknak a sérülékenységeire épülő támadásokat, és ezek alapján gyűjtöttem össze adatbázis fenyegetéseket.

Dolgozatomban áttekintettem a kritikus infrastruktúrák fogalmi kérdéseit és elemeztem a kritikus infrastruktúrák azonosításának módszereit. A kritikus infrastruktúra azonosítás végterméke egy vagy több kritikus infrastruktúra lista, mely a védelem tárgyait tartalmazza. Mivel hazánkban kritikus infrastruktúra lista megalkotására még nem került sor, ezért külföldi példák vizsgálatán keresztül fogalmaztam meg javaslatokat a lista létrehozásának folyamatához, mely a kritikus szolgáltatások és azok minimális működési szintjének meghatározására épül.

Az értekezésben elemeztem és összegeztem az adatbázisok általános helyét és szerepét a különböző kritikus infrastruktúra szektorokban. Megállapítottam, hogy számos infokommunikációs szolgáltatás esetében az alapvető adatbázisok jelentős szerepet játszanak, sérülésük, meghamisításuk országos méretű hatással jár. A kritikus infrastruktúrákban vannak olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisok megnevezésére javasoltam bevezetni a kritikus adatbázisok kifejezést.

A kritikus adatbázisok azonosítása kapcsán két módszert különböztettem meg. Az első módszer a kritikus szolgáltatások középpontba állítására épül. Eszerint azonosítani kell az adott kritikus szolgáltatás mögött álló adatbázisokat, majd el kell végezni ezek kritikusság szerinti priorálását. A második módszer nem a szolgáltatásokból, illetve azok kritikusságának megközelítésből indul ki, hanem magából az adatbázisból, illetve az abban nyilvántartott adatokból.

Értekezésemben az adatbázis-biztonság- állami szabályozásának lehetőségeit vizsgáltam. Mivel az informatikai biztonság - és ennek részterülete az adatbázis-biztonság- állami szabályozása a közigazgatás szereplőire és a kritikus infrastruktúrákra vonatkozóan lehet kényszerítő eszköz, továbbá a közigazgatási szolgáltatások a Jogrend - Kormányzat kritikus infrastruktúra szektor alágazata, értekezésemben az adatbázis-biztonság szabályozási lehetőségeinek vizsgálatát a magyar közigazgatásra behatárolva végeztem el.

Megállapítottam, hogy 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 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. Az adatbázis-biztonság szabályozásának kapcsán javaslom a közigazgatási informatikai rendszerek teljes körű informatikai védelmének feladataival egy központi szervezetet megbízni, amelynek feladatkörébe tartozna többek közt az adatbázis-biztonság felügyelete és megvalósítása is.

Javaslatom szerint az adatbázis-biztonsági szabályozásnak egy többszintű rendszert kellene alkotnia. A szabályozás egyik részét a szervezet és tevékenység független általános adatbázis-biztonsági útmutató alkotná, mely rendszabályok rendezett listájából állna és egy kormányzati központi szerv adna ki. A szabályozás másik részét szervezet specifikus dokumentumok alkotnák. A szabályozás hatálya alá eső szervezetnek az előző általános útmutató adaptálásával ki kellene dolgoznia a saját általános adatbázis-biztonsági útmutatóját. Továbbá az általános követelményeket át kellene fogalmazni konkrét biztonsági kontrollok gyűjteményévé (saját adatbázis-kezelő rendszer és az aktuális működési környezet alapján), ez lenne a szervezet adatbázis-biztonsági ellenőrző listája. Ebből a két dokumentumból épülne fel a szervezet adatbázis-biztonsági szabályzata. Értekezésem végén ajánlást tettem egy közigazgatáson belül használható általános adatbázis-biztonsági útmutatóra.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1. Kialakítottam az adatbázis fenyegetések támadási pontok szerinti rendszerezését.
2. Rendszereztem és értékeltem az adatbázisok helyét és szerepét a különböző kritikus infrastruktúra szektorokban.
3. Bevezettem a kritikus adatbázis fogalmát és meghatároztam azonosításuk lehetőségeit.
4. Meghatároztam az adatbázis-biztonság szabályozásának javasolt rendjét és fejlesztési irányait a magyar közigazgatásban.
5. Elkészítettem egy közigazgatásban hasznosítható általános adatbázis-biztonsági útmutatót.

AJÁNLÁSOK

Értekezésem a téma további kutatásához szakirodalomként felhasználható.

Javaslom az értekezésemet felhasználni a kritikus információs infrastruktúrák, az adatbázis-biztonság és az elektronikus közigazgatás biztonságával kapcsolatos szakterületeken folyó felsőoktatási alap, mester és doktori képzésekben tananyagként.

Javaslom az értekezésemben megfogalmazottakat felhasználni az adatbázis-biztonság szabályozás fejlesztésének folyamatában a közigazgatás és a kritikus infrastruktúra védelem területein. A doktori dolgozatom mellékletében található adatbázis-biztonsági útmutató felhasználható bármely szervezet számára az adatbázis-biztonság megvalósítása és szabályozása folyamatában.

Budapest, 2011. november 8.

ÉRTEKEZÉSSEL KAPCSOLATOS PUBLIKÁCIÓIM

[FR1] Fleiner Rita: Az adatbázis-biztonság alapjai. – Hadmérnök, 2010 (V.)/2. (277-292.o.) ISSN 1788-1919

[FR2] Fleiner Rita: Kritikus adatbázisokra épülő informatikai rendszerek architektúrái és biztonsági szempontjai. – Hadmérnök, 2009 (IV.)/3. (218-230.o.) ISSN 1788-1919

[FR3] Fleiner Rita: SQL injekcióra épülő támadások és védekezési lehetőségek. – Hadmérnök, 2008 (III.)/4. (117-128.o.) ISSN 1788-1919

[FR4] Fleiner Rita: Adatbázis-kezelő rendszerek kommunikációs protokolljai és sérülékenységei. – Kommunikáció 2009 Tudományos konferencia kiadványa. 2009.10.14. ISBN 978 963 7060 70 0 (193-198.o.)

[FR5] Fleiner Rita: Adatbázisok fenyegetettségeinek rendszerezése. – Hadmérnök, 2009 (IV.)/4. (132-141. o.) (Robothadviselés 9 konferencia, 2009.11.24., Budapest. Zrínyi Miklós Nemzetvédelmi Egyetem) ISSN 1788-1919

[FR6] Fleiner Rita: Kritikus adatbázisok meghatározásának lehetőségei, módszerei a kormányzati szektorban. – Bolyai Szemle, 2010 (XIX.)/1. (299-317.o.) ISSN 1416-1443

[FR7] Munk Sándor, Fleiner Rita: Adatbázisok kritikus infrastruktúrákban. – Hadmérnök, 2009 (IV.)/1. (225-234.o.) ISSN 1788-1919

[FR8] Fleiner Rita: Adatbázisok szerepe kritikus infrastruktúrák biztonságában. – Hadmérnök, 2009 (IV.)/2. (284-295.o.) ISSN 1788-1919

[FR9] Munk Sándor, Fleiner Rita: Az adatbázis-biztonság szabályozása és megvalósítása az Egyesült Államok haderejében.– Bolyai Szemle, 2009 (XVIII.)/4. (81-102.o.) ISSN 1416-1443

[FR10] Muha Lajos, Fleiner Rita: Adatbázisok biztonságának kezelése a közigazgatásban.– Hadmérnök, 2010 (V.)/4. (235-247.o.) (Robothadviselés 10 konferencia, 2010.11.24., Budapest, ZMNE) ISSN 1788-1919

[FR11] Fleiner Rita, Munk Sándor: Az adatbázis-biztonság szabályozásának alapjai a Magyar Köztársaságban.– Hadmérnök, 2011 (VI)./2. (148-163. o.) ISSN 1788-1919

[FR12] Rita Fleiner: Significance and structure of database security guides and checklists. – New Challenges in the Field of Military Sciences 2010,7th International Conference, 2010.09.28-30., Budapest, ZMNE BJKMK ISBN 978-963-87706-6-0

[FR13] Fleiner Rita, Munk Sándor: Informatikai biztonsági útmutatók, kontrollok és szerepük az adatbázis-biztonság megvalósításában– Hadmérnök, 2011 (VI)./3. (100-116. o.) ISSN 1788-1919

FELHASZNÁLT IRODALOM

[1] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

[2] Az adatvédelmi biztos honlapja, http://abiweb.obh.hu/adatved/magyar/b049.htm (2011.11.04.)

[3] C. J. Date: An Introduction to Database Systems, 8th Edition, Addison Wesley 2004 ISBN 0-201-38590-8

[4] Ramez Elmasri, Shamkant B. Navathe: Fundamentals of Database Systems, 5th Edition, Addison Wesley 2007 ISBN 0-321-36957-4

[5] Mario Guimaraes, Meg Murray: Using animation courseware in the teaching of database security. Proceedings of the 8th ACM SIGITE conference on Information technology education 2007 ISBN 1-59593-920-3

[6] Mario Guimaraes, New challenges in teaching database security, Proceedings of the 3rd annual conference on Information security curriculum development, September 22-23, 2006, Kennesaw, Georgia ISBN 1-59593-437-5

[7] Mario Guimaraes, Herb Mattord, Richard Austin: Incorporating Security Components into Database Courses. Proceedings of the 1st annual conference on Information security curriculum development, October 8, 2004, Kennesaw, Georgia

[8] Dimple Arora: Introduction to Database Security and Auditing, http://cert-in.org.in/training/14Oct09/database_security.pdf (2010.03.19.)

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

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

[11] Útmutató az IT biztonsági szintek meghatározásához http://www.ekk.gov.hu/hu/emo/ekozigkeretrendszer/ek3-itbiztonsag/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.doc (2010.03.19.)

[12] 223/2009. (X. 14.) Korm. Rendelet az elektronikus közszolgáltatás biztonságáról

[13] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[14] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. Bolyai Szemle, 2008 (XVII.)/4. ISSN 1416-1443

[15] Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49

[16] AAP-31(A), NATO Glossary of Communication and Information Systems Terms and Definitions. - NATO C3 Agency, 1998.

[17] Munk Sándor: Katonai informatika II. Egyetemi jegyzet. Budapest 2006, ZMNE

[18] Bodlaki Ákos-Csernay Andor-Mátyás Péter-Muha Lajos-Papp György-Vadász Dezső: Informatikai Rendszerek Biztonsági Követelményei, Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása. Budapest, 1996. http://www.itb.hu/ajanlasok/a12/html/a12_1.htm (2010.03.19.)

[19] Vicente Aceituno Canal: On Information Security Paradigms. – ISSA Journal 2005/9 ISSN 1750-9386 http://www.issa.org/Library/Journals/2005/September/Aceituno Canal - On Information Security Paradigms.pdf (2010.03.19.)

[20] Network Working Group Request for Comments: 2828 Internet Security Glossary http://www.ietf.org/rfc/rfc2828.txt (2010.03.19.)

[21] National Institute of Standards and Technology (NIST): Risk Management Guide for Information Technology Systems, Special Publication 800-30 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (2010.03.19.)

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

[23] Munk Sándor: Információbiztonság vs. informatikai biztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám ISSN 1788-1919

[24] Munk Sándor: Az informatikai biztonság rendszertanához Bolyai Szemle 2009. XVIII/4 ISSN 1416-1443

[25] Budai Péter: Hogyan csökkentsük az IT-kockázatokat? http://www.microsoft.com/hun/technet/dl.aspx?id=2c4172ce-c0f2-4dc5-9a11-583345d58663 (2010.03.19.)

[26] Control Systems Cyber Security: Defense in Depth Strategies http://csrp.inl.gov/Documents/Defense in Depth Strategies.pdf (2010.03.19.)

[27] Ifj. Zettner Tamás: Meghackelték a NASA-t http://itcafe.hu/hir/nasa_hacker_tamadas.html (2010.03.19.)

[28] Miniszterelnöki Hivatal, Informatikai biztonsági felügyelő: Részletes jelentés a Központi Elektronikus Szolgáltató Rendszer egyes szolgáltatásainak üzemzavarairól. Budapest, 2009. február 24.

[29] Zakor Szilárd: Adatbázis-alapú alkalmazás-fejlesztés Borland Delphiben. Készletnyilvántartó program. Szakdolgozat, 2008 Debrecen http://ganymedes.lib.unideb.hu:8080/dea/bitstream/2437/4156/1/Szakdolgozat.pdf (2009.06.01.)

[30] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla, Anandha Murukan: Improving Web Application Security. Threats and Countermeasures. Microsoft Corporation http://msdn.microsoft.com/en-us/library/aa302420(printer).aspx (2009.06.01.)

[31] J. D. Ullman, J. Widom: Adatbázisrendszerek – Alapvetés, Második, átdolgozott kiadás. Panem kiadó, Budapest, 2009. ISBN 963-5454-81-5

[32] Göndör Gábor, Verseczki Roland: Több számítógép összekapcsolásának főbb módjai. A Clusterek http://architekturak.elte.hu/html/anyagok/06072/tobb_szgep_gondor_verseczki.pdf (2009.06.01.)

[33] Oracle® Real Application Clusters Administration and Deployment Guide 11g Release 1 (11.1) http://download.oracle.com/docs/cd/B28359_01/rac.111/b28254/admcon.htm (2009.09.09.)

[34] Oracle® Data Guard Concepts and Administration, 10g Release 2 (10.2), Part Number B14239-05 http://download.oracle.com/docs/cd/B19306_01/server.102/b14239/toc.htm

[35] Kovács Zoltán: Új funkciók, kevesebb hiba http://download.microsoft.com/download/8/f/7/8f75bdd7-a0f9-4f53-a0ad-9d9aae86e21e/44-46.pdf (2009.06.01.)

[36] Gopal Ashok, Paul S. Randal: SQL Server Replication. Providing High Availability using Database Mirroring. Microsoft Corporation. http://download.microsoft.com/download/d/9/4/d948f981-926e-40fa-a026-5bfcf076d9b9/ReplicationAndDBM.docx (2009.06.01.)

[37] ISO/IEC 15408-1:2009, Information Technology - Security Techniques -Evaluation criteria for IT security - Part 1: Introduction and general model. Third Edition. - ISO, 2009.12

[38] ISO/IEC 15408-2:2008, Information Technology - Security Techniques -Evaluation criteria for IT security - Part 2: Security functional components. Third Edition. - ISO, 2008.08

[39] ISO/IEC 15408-3:2008, Information Technology - Security Techniques -Evaluation criteria for IT security - Part 3: Security assurance components. Third Edition. - ISO, 2008.08

[40] US Government Protection Profile Database Management Systems, Version 1.3, 2010. December 24.

[41] Amichai Shulman: Danger From Below: The Untold Tale of Database Communication Protocol Vulnerabilities http://www.imperva.com/resources/adc/db_comm_protocol.html (2009. 12.10.)

[42] Bucsay Balázs: MySQL and SQL Column Truncation Vulnerabilities http://rycon.hu/papers/02mysqlcolumntruncation.pdf (2009.12.10.)

[43] Simon Whatley: What is a SQL Injection Attack http://www.simonwhatley.co.uk/what-is-a-sql-injection-attack (2009.12.10.)

[44] CERT® Advisory CA-2003-20 W32/Blaster worm http://www.cert.org/advisories/CA-2003-20.html

[45] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver: Inside the Slammer Worm IEEE Security and Privacy. July 2003. ISSN 1540-7993

[46] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2004) 702 final

[47] A TANÁCS 2008/114/EK IRÁNYELVE (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

[48] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai gazdasági és Szociális bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről - „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”, COM (2009) 149

[49] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai gazdasági és Szociális bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről „Eredmények és következő lépések: a globális kiberbiztonság felé” COM(2011) 163

[50] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[51] A Kormány 1249/2010. (XI. 19.) Korm. határozata az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról

[52] 2011. évi CXXVIII törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[53] Haig Zsolt,Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9

[54] Kovács László: Kritikus információs infrastruktúrák Magyarországon, Hadmérnök Robothadviselés 7. Tudományos Szakmai Konferencia különszáma – 2007. november 27. ISSN 1788-1919

[55] Varga Péter: A kritikus információs infrastruktúrák értelmezése, Hadmérnök, 2008 (III.)/2. (149-156.o.) ISSN 1788-1919

[56] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori értekezés. ZMNE, Budapest, 2007.

[57] Munk Sándor: A kritikus infrastruktúrák védelme információs támadások ellen, Hadtudomány, 2008 (XVIII.)/1-2. (95-106.o.) ISSN 1215-4121

[58] Haig Zsolt: Az információs társadalmat fenyegető információalapú veszélyforrások, Hadtudomány, 2007 (XVII)/3. (37-56.o.) ISSN 1215-4121

[59] Munk Sándor: Kritikus információs infrastruktúrákhoz kapcsolódó, sajátos katonai (védelmi szférabeli) képességeket igénylő feladatok, Hadmérnök, 2008 (III.)/3. (130-146.o) ISSN 1788-1919

[60] Andrew M. Colarik: Cyber terrorism. Political and economic implications, Idea Group Inc (IGI), 2006

[61] Kovács László: Kritikus információs infrastruktúrák. Egyetemi jegyzet. ZMNE, 2007.

[62] Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai, Hadmérnök, 2008 (III.)/2. (138-148.o.) ISSN 1788-1919

[63] Manuel Suter: A Generic National Framework For. Critical Information Infrastructure. Protection (CIIP). Center for Security Studies, ETH Zurich. August 2007.

[64] Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. ENO Avisory Kft., 2009.

[65] HITRAC: Informing the decisions that protect the nation. http://www.nctcog.org/ep/Workshop_Presentations/CIKR/HITRACRISK_TEXAS.swf (2010.01.07.)

[66] National Critical Infrastructure Prioritization Program (NCIPP), FY09 Tier 1 and Tier 2 Data Call Guidance, Department of Homeland Security http://cryptome.org/dhs-datacall.pdf (2010.01.07.)

[67] Department of Homeland Security, Office of Inspector General: Efforts to Identify Critical Infrastructure Assets and Systems. OIG-09-86, 2009 June. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-86_Jun09.pdf (2010.01.07.)

[68] Myriam Dunn and Victor Mauer (eds.): International CIIP Handbook 2006, Vol. II. Analyzing Issues, Challenges, and Prospects. Center for Security Studies, ETH Zurich ISBN 3-905696-08-8

[69] Elgin M. Brunner, Manuel Suter: International CIIP Handbook 2008/2009. Center for Security Studies, ETH Zurich ISBN 3-905696-22-6

[70] Kaszás Árpád: A MAVIR Rt. informatikai stratégiája. – A Magyar Villamos Művek Közleményei, 2001 (XXXVIII.)/3. (21-27.o.) ISSN 1786-674X

[71] Kaszás Árpád: Az MVM-MAVIR-ban az ÜRIK keretében létesített számítógéprendszer kialakítása. A SPECTRUM funkciók összefoglalása. – Elektrotechnika, 2002 (95.)/különszám (6-16.o.) ISSN 0367-0708

[72] MOL Rt., KFÜ: OTR-IIM projektek (ismertetés). – X-Prompt Automatizálási Szakértői Kft., Budapest, 2006. http://www.x-prompt.hu/Portal.php?Page=PROJ/OTR2M (2008.12.12.)

[73] Szászi Gábor: Közlekedési informatika. – Bolyai János Katonai Műszaki Főiskola, Budapest, 1999.

[74] A vízügyi informatika fejlődése, szerepe és kapcsolódásai a többi környezeti informatikai rendszerhez. – EKOSPEKTRUM Kft., Budapest, 2004.

[75] Tolnai Béla (szerk.): A térinformatikai szerepe a vízi közműszolgáltatásban (Fogalmak, feladatok, eszközök, elvárások, szabványok). – Víz- és Csatornaművek Országos Szakmai Szövetsége, Budapest, 2003. http://www.tova-partner.hu/letoltesek/a_terinformatika_szerepe.pdf (2008.12.12.)

[76] Nagy Rudolf-Vincze Árpád: Az élelmiszer-biztonság a környezetbiztonság szemszögéből. – Hadmérnök, 2007 (II.)/4. (38-45.o.) ISSN 1788-1919

[77] Ambrus Árpád-Vanyur Rozália: Az élelmiszer-biztonsági intézményrendszer megerősítése az EU támogatásával. – Élelmiszer-biztonság, 2008 (VI.)/2. (22-27.o.) ISSN 1589-780X

[78] Jávor András-Surján György-Tóth Annamária: Személyi Elektronikus Egészségügyi Életút Archívum. – Informatika és Menedzsment az Egészségügyben, 2003 (II.)/3. (30-36.o.) ISSN 1588-6387

[79] Sinkó Eszter: Közhiteles nyilvántartások az egészségügyben. I. rész. – Informatika és Menedzsment az Egészségügyben, 2005 (IV.)/3. (43-45.o.) ISSN 1588-6387

[80] Sinkó Eszter: Közhiteles nyilvántartások az egészségügyben. II. rész. – Informatika és Menedzsment az Egészségügyben, 2005 (IV.)/4. (44-48.o.) ISSN 1588-6387

[81] Sinkó Eszter: Közhiteles nyilvántartások az egészségügyben. III. rész. – Informatika és Menedzsment az Egészségügyben, 2005 (IV.)/5. (38-43.o.) ISSN 1588-6387

[82] Burián Gábor: Az Internet banking kockázatai. – Hitelintézeti Szemle, 2005 (IV.)/2. (36-56.o.) ISSN 1588-6883

[83] Lublóy Ágnes-Tanai Eszter: A működési kockázat és a hazai nagy összegű fizetési rendszer (VIBER). – Hitelintézeti Szemle, 2007 (VI.)/4. (324-357.o.) ISSN 1588-6883

[84] SPIRS 2.0, Seveso Plants Information Retrieval System (SPIRS), an Electronic Documentation and Analysis System for Industrial Establishments Data. User's Manual. – European Comission, 2001.

[85] MARS 4.0, Major Accident Reporting System (MARS), an Electronic Documentation and Analysis System for Industrial Accidents Data. User's Manual. – European Comission, 2001.

[86] eKormányzat 2005, e-Kormányzat stratégia és programterv. – Miniszterelnöki Hivatal, Elektronikus Kormányzat Központ, 2004.

[87] Munk Sándor: Helyzetismeret-bázisok a katonai vezetésben, helyzetinformációk gyűjtése és feldolgozása. – In. Horváth István-Kiss Jenő (szerk.): Válogatás a Honvédelmi Minisztérium 2001. évi kutatási eredményeit összegző tanulmányokból, pályázatokból. HM Oktatási és Tudományszervező Főosztály, Budapest, 2001. (143-156.o.) ISBN 963-7037-44-6

[88] Görög Katalin: Közigazgatási egyszerűsítési technikák az Európai Unióban, PhD értekezés, Miskolci Egyetem 2009.

[89] Lőrincz Lajos: A modern állam feladatai– kiemelten a közigazgatásban. In: A modern állam feladatai. Szerkesztette: Halm Tamás és Vadász János. Magyar Közgazdasági Társaság és a Gazdasági és Szociális Tanács konferenciájának előadásai. Budapest, 2009.

[90] Közigazgatási alapvizsga tankönyv. Budapest 2007. Kormányzati személyügyi szolgáltató és közigazgatási képzési központ

[91] Bevezetés az elektronikus közigazgatás ismereteibe. Tankönyv a köztisztviselők továbbképzéséhez. Szerk.: Köteles Bernadett. Budapest, 2007.

[92] Közigazgatási Informatikai Bizottság 21. számú AJÁNLÁSA. Az ügyfélkapu és hivatali kapu kapcsolódás műszaki specifikációja 2.0 verzió. 2008. augusztus

[93] 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről

[94] A Kormány 38/2011. (III. 22.) Korm. rendelete a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról

[95] Urbán György: Az okmányirodák rendszere és a közigazgatási informatika kapcsolata http://www.otk.hu/cd00/plenaris/urbangyorgy.htm (2010.05.18.)

[96] Vadászi Tiborné: Az okmányirodák szerepe az e-közigazgatásban, a Helyi Ügyintézési Pontok www.etk-rt.hu/doku_rendezveny/r_172_2008_11_11_9.ppt (2010.05.18.)

[97] Krasznay Csaba, Szigeti Szabolcs: A magyar elektronikus közigazgatási rendszer biztonsági analízise, Networkshop 2006 Konferencia, Miskolc, http://www.krasznay.hu/presentation/nws2006_krasznay.doc (2009.02.09.)

[98] Dajkó Pál: Súlyos üzemzavar az Ügyfélkapu rendszerében http://itcafe.hu/hir/ugyfelkapu_uzemzavar_meh.html (2009.02.09.)

[99] Dajkó Pál: Helyreállították az OEP informatikai rendszerét http://itcafe.hu/hir/oep_szoftverhiba.html (2009.02.09.)

[100] 2009. évi LX. törvény az elektronikus közszolgáltatásról

[101] 2009. évi CLV. törvény a minősített adat védelméről

[102] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[103] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

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

[105] 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

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

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

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

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

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

[111] 212/2010. (VII. 1.) Korm. rendelet az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről.

[112] 17/2010 (VIII. 31.) KIM utasítás a Közigazgatási és Igazságügyi Minisztérium Szervezeti és Működési Szabályzatáról.

[113] 9/2011. (II. 15.) NFM utasítás a Nemzeti Fejlesztési Minisztérium Szervezeti és Működési Szabályzatáról.

[114] 42/2011 (IV. 20.) KIM utasítás a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala Szervezeti és Működési Szabályzatáról.

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

[116] 1026/2007. (IV. 11.) Korm. határozat a közigazgatási informatikai feladatok kormányzati koordinációjáról.

[117] Póserné Oláh Valéria A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei, Hadmérnök II. Évfolyam 4. szám, 2007. ISSN 1788-1919

[118] A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről – PSZÁF, Budapest, 2007. október.

[119] State of Alabama: Information Technology Guideline, Guideline 660-01G3: Database Security, http:// isd.alabama.gov/Policy/Guideline_660-01G3_Database_Security.pdf (2011.09.06.)

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

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

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

[123] ISO/IEC 27000:2009 (E), Information technology – Security techniques – Information security management systems – Overview and vocabulary. First edition. – ISO/IEC, 2009.05.01.

[124] Internal Control – Integrated Framework. Executive Summary. – Committee of Sponsoring Organizations of the Treadway Commission, 1992.

[125] NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations. Revision 3. – National Institute of Standards and Technology, Gaithersburg, 2009 augusztus.

[126] CERT Resilience Management Model, Version 1.0, Glossary of Terms. – Carnegie Mellon University, Software Engineering Institute, 2010 május.

[127] ISO/IEC 15408-1:2005, Information Technology - Security Techniques -Evaluation criteria for IT security - Part 1: Introduction and general model. Second Edition. - ISO, 2005.10.01.

[128] Database Security Technical Implementation Guide, Version 8, Release 1. – DISA, 2007. szeptember.

[129] Database Security Guideline. – Database Security Consortium, 2009.

[130] Security Configuration Benchmark For Oracle Database Server 11g. - The Center for Internet Security, 2008 szeptember, http://cisecurity.org (2011.08.10.)

[131] Oracle Database Security Checklist. – SANS Institute. http://www.sans.org/score/oraclechecklist.php (2011.08.10.)

[132] Federal Information Security Management Act. (Title III of the E-Government Act) – 2002.

[133] ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002. – ISO, 2008.07.01.

ÁBRAJEGYZÉK

1. ábra: Információvédelem és informatikai védelem kapcsolata [14] 17
2. ábra: Az informatikai biztonság hagyma modellje [25] 21
3. ábra: Adatbázisokat tartalmazó rendszerek architektúrája [30] 26
4. ábra: A 4-rétegű architektúra több-szerveres környezetben [31] 27
5. ábra: Adatbázis szerverek fürtözése [33] 29
6. ábra: Adatbázis szerverek tükrözése [34] 30
7. ábra: Informatikai rendszer és az adatbázis sérülékenységek [készítette a szerző] 35
8. ábra: Az adatbázis kommunikációs protokoll elhelyezkedése [készítette a szerző] 36
9. ábra: A kritikus infrastruktúra védelem négy pillére [63] 54
10. ábra: Az ügyfélkapu elhelyezkedése a KR-ben [92] 76
11. ábra: KEK KH nyilvántartásaiból történő adatszolgáltatás [96] 83
12. ábra: Szervezeti szerepkörök az informatikai biztonság területén [készítette a szerző] 99
13. ábra: Informatikai biztonsági kontrollok helye, szerepe [127] 113

TÁBLÁZATJEGYZÉK

1. táblázat: Az adatbázis fenyegetések rendszerezése [készítette a szerző] 41
2. táblázat: Adatbázis-biztonsági útmutató szerkezeti felépítése [készítette a szerző] 118