HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

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

AZ ADATBÁZIS-BIZTONSÁG ALAPJAI

Absztrakt

A publikáció az adatbázis-biztonság fogalmának, helyének és szerepének vizsgálatával foglalkozik. A szerző bemutatja az adatbázis-biztonság eddigi értelmezéseit és a fogalomban idők során bekövetkezett változásokat, fejlődéseket; feltárja az informatikai biztonság és az adatbázis-biztonság kapcsolatrendszerét; illetve elemzi az adatbázis-biztonság helyét, szerepét és jelentőségét az informatikai biztonságon belül. Végül pedig ismertetésre kerül a szerző által javasolt adatbázis-biztonság fogalom értelmezése.

The publication studies the concept, the place and the role of database security. The author describes the different interpretations of database security up to the present, the changes and the evolution of the concept during the times. Furthermore the relationship between information security and database security is revealed and the place, the role and the importance of database security within information security is analysed. At the end the model of database security is presented by the author.

***Kulcsszavak**: adatbázis-biztonság, informatikai biztonság, adatbiztonság, adatbázis-biztonság tulajdonságai ~ database security, information security, data security, database-security goals*

BEVEZETÉS

Az utóbbi években egyre több olyan eset került nyilvánosságra, melyben bizalmas információk, ügyféladatok szivárogtak ki adatlopás, hacker támadás vagy hűtlen kezelés miatt. Egy-egy ilyen incidens az érintett szervezet számára számtalan káros hatással jár együtt, jelentősen ronthatja annak hírnevét, a kártérítési kötelezettség extra költségeket vonhat maga után, a meghamisított adatok és rendszerek visszaállítása időveszteséggel és többletmunkával párosul, továbbá meg kell említeni, hogy sok esetben még jogi pereskedések, bírósági eljárások is

az esetek következményeiként léphetnek fel. Mára az adatok védelmének kérdése a vállaltok és szervezetek általánosan elfogadott feladata lett.

Napjainkban a felgyülemlett óriási adatmennyiséget - egyre szélesebb körben - adatbázisokba szervezve tárolják. Az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az úgynevezett adatbázis-kezelő rendszerek biztosítják. Az informatikai rendszerek jelentős részének működésében az adatbázis-kezelő rendszerek és az általuk tárolt adatok lényeges, esetenként kiemelt szerepet játszanak. Az adatbázisok biztonságának megsértése (működésképtelenné tétele, meghamisítása, a tárolt adatok jogtalan megismerése) az adott informatikai rendszer és az általa nyújtott szolgáltatás biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázis-biztonság megvalósítása, szabályozása és támogatása.

Jelen publikáció alapvető célja az adatbázis-biztonság fogalmának, helyének és szerepének vizsgálata. Ezen belül a publikáció:

- bemutatja az adatbázis-biztonság eddigi értelmezéseit és a fogalomban idők során bekövetkezett változásokat, fejlődéseket;
- feltárja az informatikai biztonság és az adatbázis-biztonság kapcsolatrendszerét;
- elemzi az adatbázis-biztonság helyét, szerepét, jelentőségét az informatikai biztonságon belül;
- ismerteti a szerző által alkalmazott adatbázis-biztonság fogalom értelmezését.

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 tá-

rolt 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.

Az adatbázis-biztonság vizsgálata kapcsán hangsúlyozni kell, az általunk vizsgált témakör eltér az adatvédelem fogalmától. 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.

Adatbázis-biztonság értelmezésekor nem szorítkozunk az adatok csak egy bizonyos csoportjára, hanem az informatikai rendszerekben, azon belül adatbázis rendszerekben tárolt adatok egészének védelme, biztonsága képezi a vizsgálatunk tárgyát. A következőkben áttekintjük több forrást megvizsgálva az adatbázis-biztonság fogalmának értelmezéseit.

Először megvizsgálunk néhány több kiadást megélt, felsőoktatásban is használt adatbázis témájú szakkönyvet. C.J.Date: An Introduction to Database Systems című könyvében [2] 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 [3] 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 hoz-

záférés szabályozásának lehetőségei, a hitelesítés, a többszintű biztonság, a közvetett következtetés (inference), az adatbázisban tárolt adatok titkosítása és az adatbázis audit [4]. 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. [5], [6]

Az adatbázis-biztonság fogalmát az indiai CERT szervezet a következőképpen határozza meg [7]: 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 [8] 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 [9] 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 [10] 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.) Kormány rendeletben [11] 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 [12] 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.

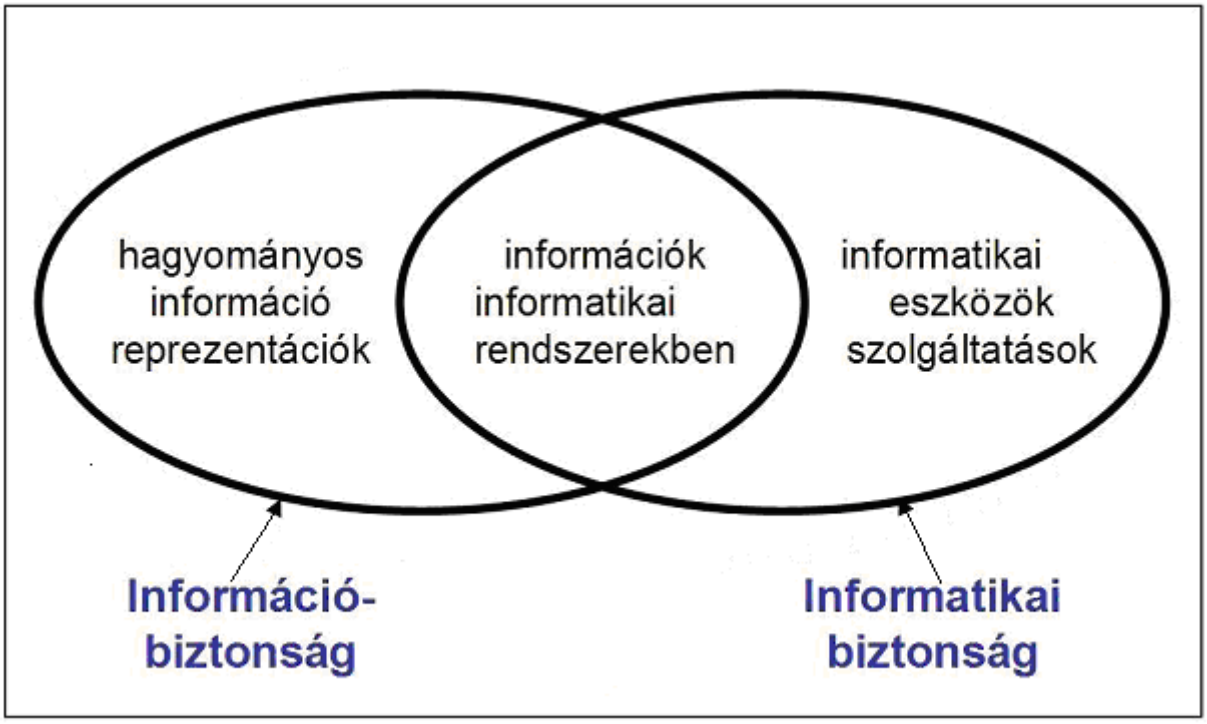
Az adatbázisok védelme szempontjából a bizalmasság, sértetlenség és rendelkezésre állás biztosításának követelménye mindenképp fontos szerepet játszik. A letagadhatatlanság és a hitelesség biztonsági kritériumait adatbázisokkal kapcsolatban ritkán említik, ezeket szokás a sértetlenség biztonsági tulajdonság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

moltathatóságnak is szokták hívni. A hitelesség az adat forrásának, eredetének a valódiságát jelenti.

ADATBÁZIS-BIZTONSÁG ÉS INFORMATIKAI BIZTONSÁG KAPCSOLATRENDSZERE

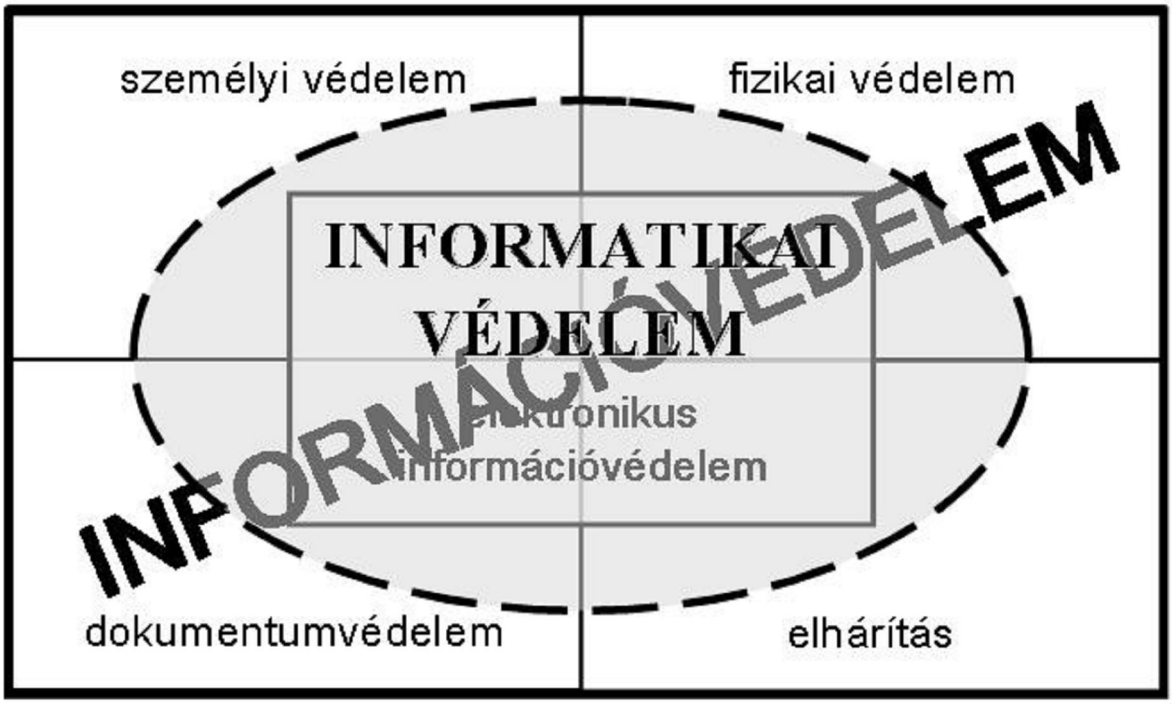
A következőkben az informatikai biztonság és az adatbázis-biztonság kapcsolatát vizsgáljuk meg, amit a témához szorosan kapcsolódó fogalmak értelmezésével kezdünk. Az informatikai biztonság és az információbiztonság kifejezéseket még ma is gyakran összekeverik, felcserélik, egymás szinonimájaként használják. 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 kapcsolatáról több tudományos cikkben is olvashatunk. Munk Sándor [13] a következő értelmezés szerint tárgyalja a fogalmakat. Az informatikai biztonság jelentése az informatikai rendszerek és az általuk kezelt adatok biztonságához kötődik, az információbiztonság pedig a tetszőleges módon hordozott (pl. papíron, fejben, adatbázisban, elektronikus dokumentumban) információ védelmével kapcsolatos, ugyanakkor nem tartalmazza az informatikai rendszereknek a biztonságát. Az információbiztonság és az informatikai biztonság egymáshoz való viszonyát a szerző a következő ábrával szemlélteti:



1. ábra. Információ biztonság és informatikai biztonság [13] alapján

Muha Lajos [14] 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:



2. ábra. Információvédelem és informatikai védelem kapcsolata [14] alapján

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, mely a következő elemekből épül fel [17]:

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.

Informatikai rendszerek közé a következő rendszerek tartoznak [14]:

1. a számítástechnikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
2. a vezetékes, a mobil, a rádiós és műholdas távközlés;
3. a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
4. a rádiós vagy műholdas navigáció;
5. az automatizálási, vezérlési és ellenőrzési rendszerek;
6. az előbbiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

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. [18].

Az említett különböző hangsúlyok megjelennek például a hálózati munkacsoport egyik releváns RFC dokumentumában [19], 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 [12] ’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 [20] az 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. [21]

Munk Sándor által javasolt biztonság alapmodellje [13] 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 [13].

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. [22]

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 [23]. 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 [9]:

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 érvé-

nyesülnek.

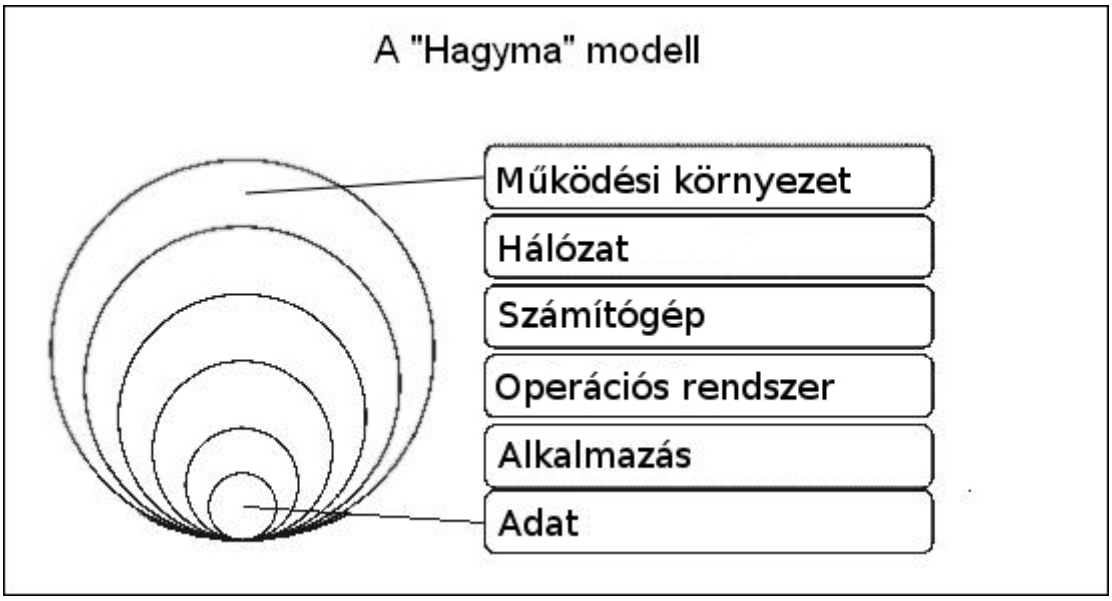
Ha az informatikai biztonság és az adatbázis-biztonság kapcsolatát szeretnénk feltárni, akkor meg kell vizsgálnunk mindkét esetben a biztonság alanyát, illetve annak védendő tulajdonságait. Az informatikai biztonság alanya az informatikai rendszer és az abban kezelt adatok halmaza, az adatbázis-biztonság 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, megbízhatóság, letagadhatatlanság, 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.

ADATBÁZIS-BIZTONSÁG HELYE, SZEREPE

Mivel az adatbázisokban koncentráltan található érzékeny, kritikus információ, az adatbázisok védelme fontos feladattá vált. 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.

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 [21]). 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.



3. ábra. Az informatikai biztonság hagyma modellje [24] alapján

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 [25], 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 kihatható 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-biztonságimegoldások 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 hálózta, 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 a 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 [8] 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 megvizsgáljuk 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 [26]. 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 [27]. 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.

A fentiek alapján megállapítható, hogy az adatbázis-biztonság az informatikai biztonság egyik fontos részterülete. Az adatbázisok védelme kiemelt figyelmet érdemel az informatikai védelmen belül, mivel az adatbázis-kezelő rendszerekben tárolt adatok tönkretétele helyrehozhatatlan problémát okozhat a teljes informatikai rendszer működésében. Az adatbázis-biztonságot az informatikai rendszer többi elemével egységben, csak komplex módon lehet megvalósítani a rendszer-elemek interdependenciája miatt, ugyanakkor célszerű és létjogosult, mint az informatikai biztonság egy különálló területét kezelni.

ÖSSZEGZÉS: AZ ADATBÁZIS-BIZTONSÁG EGY LEHETSÉGES ÉRTELMEZÉSE

Összegzésképpen megállapítható, 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 például az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutatóban [8]. Mivel a témát kutatásaimban a kritikus infrastruktúra védelem, illetve az informatika biztonság megvalósítása oldaláról is tanulmányozom, az adatbázis-biztonság alanyának mind az adatbázisban tárolt adatokat, mind az azokat kezelő adatbázis-kezelő rendszereket tekintem.

Az adatbázis-biztonság védendő tulajdonságai közé tartozik a bizalmasság, sértetlenség és rendelkezésre állás. Bizonyos esetekben szükség lehet a hitelesség és letagadhatatlanság tulajdonságokra is, szemléletmód kérdése, hogy ezeket külön kategóriáknak tekintjük, vagy pedig a sértetlenség tulajdonság részének. Az utóbbi időben, a törvényi szabályozások és megfelelőségi elvárások hatásának köszönhetően kialakult egy újabb védendő tulajdonság is, amit elszámoltathatóságnak vagy más néven auditálhatóságnak nevezünk. Kijelenthetjük, hogy igazából nem a kategóriák száma a fontos, hanem a mögöttük lévő tartalom és védendő értékek, illetve az adatbázis-biztonság védendő tulajdonságai konkrét alkalmazások és környezetek

esetén eltérőek lehetnek.

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, 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 is hívják. A hitelesség az adat forrásának, eredetének a valódiságát jelenti.

FELHASZNÁLT IRODALOM

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

[2] C. J. Date: An Introduction to Database Systems, 8th Edition, Addison Wesley 2004

[3] Ramez Elmasri Shamkant B. Navathe: Fundamentals of Database Systems, 5th Edition, Addison Wesley 2007

[4] 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

[5] 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

[6] 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

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

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

[9] Közigazgatási Informatikai Bizottság 25. számú Ajánlása, MIBA Magyar Informatikai Biztonsági Keretrendszer, 25/1-2. kötet Informatikai Biztonság Irányítási Követelmények (IBIK), 2008. június

[10] 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.)

[11] 223/2009. (X. 14.) Korm. Rendelet az elektronikus közszolgáltatás biztonságáról

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

[13] Munk Sándor: Információbiztonság vs. informatikai biztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám

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

[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] Vicente Aceituno Canal: On Information Security Paradigms http://www.issa.org/Library/Journals/2005/September/Aceituno Canal - On Information Security Paradigms.pdf (2010.03.19.)

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

[20] 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.)

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

[22] 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.)

[23] Munk Sándor: Az informatikai biztonság rendszertanához Bolyai Szemle 2009. XVIII/4

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

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

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

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