HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

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

Munk Sándor
munk.sandor@zmne.hu

INFORMATIKAI BIZTONSÁGI ÚTMUTATÓK, KONTROLLOK ÉS SZEREPÜK AZ ADATBÁZIS-BIZTONSÁG MEGVALÓSÍTÁSÁBAN

Absztrakt

Az információk és az azokat kezelő informatikai rendszerek, eszközök a szervezetek fontos erőforrásai, biztonságuk valamennyi szervezet számára alapvető fontosságú. Ennek megfelelően jelentősen megnőtt az informatikai biztonság megvalósítására irányuló tevékenységek, eszközök szerepe is. Ez utóbbiak közé tartoznak a biztonsági útmutatók és kontrollok, amelyek a biztonság megvalósításának, szabályozásának és értékelésének fontos eszközei. Jelen publikáció bemutatja a biztonsági útmutatók fogalmát, rendeltetését, típusait; bemutatja a biztonsági kontrollok fogalmát, értelmezését, elemzi csoportosításuk lehetőségeit; végül elemzi az informatikai biztonsági útmutatók, kontrollok helyét, szerepét az informatikai biztonság irányításában, szabályozásában.

Information and the supporting IT systems, devices are important organizational assets, their security is fundamental for all organizations. As a consequence the role of security activities and means has significantly increased. Security guidelines and controls are important means of implementation, regulation, and evaluation of security. Recent publication presents the concept, purpose, and types of security guidelines; presents the concept, and interpretation of security controls, analyses their classifications; finally analyses the role of security guidelines, controls in management and regulation of information (IT) security.

***Kulcsszavak**: informatikai biztonság, adatbázis-biztonság, informatikai biztonsági útmutató, informatikai biztonsági kontroll ~ information (IT) security, database security, information security guideline, information security control*

BEVEZETÉS

Az információk és az azokat kezelő folyamatok, rendszerek, eszközök napjainkra megkérdőjelezhetetlenül valamennyi szervezet-típus alapvető szervezeti erőforrásává váltak. Ma már közhely, hogy az információk és a kezelésükben szerepet játszó erőforrások biztonsága szinte egyaránt fontos a gazdálkodó szervezetek, a kormányzati szféra, a védelmi szféra és gyakorlatilag minden szervezet számára. Ennek megfelelően jelentősen megnőtt az informatikai biztonság megteremtésére és fenntartására irányuló tevékenységek és az ezek során felhasznált eszközök, módszerek és eljárások szerepe, jelentősége is.

Az információk és az informatikai rendszerek, eszközök biztonságát sebezhetőségeiken keresztül számos fenyegetés veszélyezteti. A fenyegetések ellen különböző módokon és eszközökkel lehet védekezni, azonban tökéletes védelem elvileg nem létezik és nem minden védelmi megoldás "éri meg" a ráfordítást. 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 tehát 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.

A biztonsági útmutatók – bár sok közülük nemzetközi, nemzeti és szervezeti szintű szabványokban is megjelenik – nevükből következően[1], alapvetően nem kötelező erejű dokumentumok. Ennek ellenére felhasználhatóak az informatikai biztonság, vagy valamely részterülete szabályozására is, meghatározva például, hogy bizonyos szervezetek, tevékenységek, rendszerek, rendszerelemek esetében az adott útmutató mely kontrolljait kell kötelezően megvalósítani. Ez általában nem egyedileg kerül meghatározásra, hanem a biztonság alanyai egyéb szempontok alapján biztonsági kategóriákba (osztályokba) kerülnek besorolásra és a minimálisan megvalósítandó kontrollok ezekhez a kategóriákhoz vannak rendelve. Végül a segítségnyújtás és a szabályozás mellett az útmutatók, illetve az azokban foglalt kontrollok kiterjedten felhasználásra kerülnek a biztonsági megfelelőség-vizsgálatok, igazolások, auditok során is.

A fentiek alapján jelen publikáció alapvető célja, hogy rendszerezze, bemutassa az informatikai biztonsági útmutatók, kontrollok alapvető információit és meghatározza szerepüket az informatikai biztonság megvalósításában. Ennek érdekében:

- - bemutatja a biztonsági útmutatók fogalmát, rendeltetését, típusait, valamint a főbb útmutatókat;
- - bemutatja a biztonsági kontrollok fogalmát, értelmezését, elemzi csoportosításuk lehetőségeit, helyüket és szerepüket az informatikai biztonság megvalósításában;
- - elemzi az informatikai biztonsági útmutatók, kontrollok helyét, szerepét az informatikai biztonság irányításában, szabályozásában, meghatározza a kapcsolódó feladatokat.

[1] Guideline = iránymutatás, irányelv.

BIZTONSÁGI ÚTMUTATÓK ALAPJAI

Az informatikai biztonsági útmutatók és a kapcsolódó dokumentumok (ellenőrző listák) az informatikai biztonság kialakítását és fenntartását (az informatikai biztonsági célkitűzések megvalósulását) szolgáló védelmi megoldások, rendszabályok és tevékenységek kialakításának, illetve ellenőrzésének alapvető eszközei. A következőkben a biztonsági útmutatókkal kapcsolatos alapvető kérdéseket összegezzük és rendszerezzük, ezen belül:

- bemutatjuk a biztonsági útmutatók és ellenőrző listák fogalmát, rendeltetését;
- rendszerezzük az útmutatók, ellenőrző listák felhasználásának lehetőségeit;
- megvizsgáljuk az útmutatók csoportosításának lehetőségeit, főbb típusaikat;
- ismertetjük a jelentősebb informatikai biztonsági útmutatókat;
- végül ismertetjük a jelentősebb adatbázis-biztonsági útmutatókat.

Az első három kérdésben a megállapításokat általános biztonsági megközelítésben fogalmazzuk meg, de példáinkat az informatikai biztonság területéről vesszük.

A *biztonsági útmutatók és ellenőrző listák* kérdéseinek vizsgálatához először meg kell határoznunk fogalmukat, rendeltetésüket. Az *útmutató* (guide, guideline[s]) az általános értelmezés szerint egy nem kötelező érvényű ajánlás arra, hogy meghatározott célkitűzések elérése érdekében mit és hogyan kell megtenni. [1, 2] Más megfogalmazásban az útmutató egy adott cél eléréséhez megkívánt, javasolt, jónak tartott, bevált eljárások, tevékenységek leírása. Az útmutatók általában a törvényekben, szabványokban, szabályozókban előírtak megvalósításának javasolt, célszerű módját tartalmazzák.

Útmutatók az élet sok területén felhasználásra kerülnek: felhasználói útmutatók (kézikönyvek) ismertetik, magyarázzák készülékek használatát; technikai útmutatók segítik rendszerek, eszközök telepítését, üzemeltetését, karbantartását, javítását; orvosi szakmai protokollok írják le egy betegség, vagy állapot kezelésének tevékenységeit.[2] Több szabványügyi szervezet (pld. ISO, IEC, ITU, NIST[3], stb.) bocsát ki dokumentumokat 'útmutató' megnevezéssel. Míg a szabványok megismételhető, mérhető és tesztelhető, normatív technikai referenciaként használható specifikációk, addig az útmutatók általában szabadabb értelmezéseket is lehetővé tévő iránymutatások.

A *biztonsági útmutatók* (security guideline) az útmutatók egyik csoportját alkotják, amelyek rendeltetése biztonsági célkitűzések megvalósítását szolgáló megoldások, eljárások, tevékenységek meghatározása: "hogyan lehet elérni a biztonságot". A biztonság alatt a továbbiakban olyan állapotot értünk, amelyben valaki/valami a lehetséges fenyegető hatások ellen a megkívánt mértékben védett. 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 esetében a biztonsági szabályozórendszer három szintre osztható (az informatikai biztonság esetében pld. lásd a KIB 25/1. ajánlást [3, 46. o.]). Felső szinten a biztonsági politika és stratégia található, amelyek megfogalmazzák az alapvető biztonsági elveket, célkitűzéseket és felelősségi köröket, illetve meghatározzák a biztonság fejlesztésének közép (hosszú) távú tervét. Középső szinten átfogó és részterületi szabályzatok, szabályozók, míg alsó szinten a konkrét feladat- és szerepkörökre vonatkozó részletes biztonsági eljárások, feladatok (eljárásrend) találhatóak.

---

[2] User's guide (manual), technical guide (manual), medical guide (protocol).

[3] International Organization for Standardization, International Electrotechnical Commission, International Telecommunication Union, National Institute of Standards and Technology [USA].

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. Ennek megfelelően a biztonsági útmutatók általában több szervezet számára felhasználható módon, azokon kívül kerülnek kidolgozásra. Emellett összetett szervezetrendszerekben (közigazgatás, haderő, stb.) is szükség lehet biztonsági útmutatók kidolgozására az egyes szervezetek biztonsági eljárásai, feladatai meghatározásának támogatásához.

Az *ellenőrző lista* (checklist) általános értelemben egy összetett feladat elemi tevékenységeinek, lépéseinek teljes körét tartalmazó lista, amelynek rendeltetése emlékeztetés, végigvezetés a végrehajtandó részfeladatokon. Az egyes lépések között lehetnek függőségek, egy lépés választásától, vagy eredményétől függhet, hogy egy másikat (másikakat) végre kell-e hajtani. Egy ellenőrző lista sok esetben ténylegesen egy fennálló állapot értékelésének, ellenőrzésének lépéseit tartalmazza.

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. [4, 2-1. o.] Az ellenőrző listák a megfelelőség-vizsgálat mellett természetesen felhasználhatóak a beállítások végrehajtása során is és a hagyományos dokumentum-formátum mellett megvalósíthatóak automatizált ellenőrzést lehetővé tévő elektronikus (pld. szkript) formában is.

A *biztonsági útmutatók, ellenőrző listák felhasználásának lehetőségei* három nagy területbe sorolhatóak. Ezek közé tartozik felhasználásuk:

- biztonsági intézkedések kiválasztása, kialakítása során;
- biztonsági szabályozások hivatkozási alapjaként;
- és biztonsági követelményeknek történő megfelelés ellenőrzése során.

A *biztonsági intézkedések kiválasztása, kialakítása során történő felhasználás* tekinthető az alapvető felhasználási módnak. Ebből a szempontból a biztonsági útmutatók elméletileg megalapozott és a bevált gyakorlatra épülő általános célkitűzés- és megoldás-gyűjtemények. Az útmutatók alapvető összetevőit a védelmi megoldások, intézkedések (biztonsági kontrollok, amelyekkel részletesebben a következő pontban foglalkozunk) képezik. Az egyes összetevők esetében a meghatározás mellett szerepelhet a megvalósítás javasolt módja is.

Az útmutatókban a rendszerezettség és a könnyebb kezelhetőség érdekében az egyes összetevők (kontrollok) jellemzően különböző szempontok alapján – esetleg több szinten is – csoportokba vannak sorolva. Az egyes csoportok esetében megfogalmazásra kerül a bennük foglalt összetevők általános célja, illetve e biztonsági célkitűzés részletesebb indoklása, elvei.

A *szabályozás során történő felhasználás* az önálló döntés alapján történő felhasználással szemben a külső előírásokhoz kapcsolódik. Ennek során egy szabályozás hatálya alá tartozó szervezetek számára meghatározásra kerül, hogy mely védelmi megoldásokat, intézkedéseket kell kötelező érvénnyel, vagy bizonyos feltételek fennállásának függvényében megvalósítaniuk. A szabályozás történhet nemzeti, vagy szervezeti szinten (utóbbi esetben olyan összetett szervezetrendszerek esetében, ahol az egyes szervezetek önálló biztonsági irányítási rendszert működtetnek), de lehetséges uniós, vagy szövetségi keretek között is. A felhasználásnak ez a módja tulajdonképpen egy többszintű biztonsági irányítási rendszert jelent, amelyben a magasabb szint célkitűzéseket és ezek megvalósítására egy minimum védelmi intézkedési "csomagot" határoz meg, amelyet az alacsonyabb szint saját hatáskörében bővíthet, finomíthat.

Az *ellenőrzés céljára történő felhasználás* a biztonság irányításának másik alapvető részterületéhez, egy szervezeten belül a biztonság állapotának ellenőrzéséhez, felülvizsgálatához, illetve a meghatározott követelményeknek történő megfelelés értékeléséhez kapcsolódik. Az ellenőrzés, értékelés lehet szervezeten belüli és azon kívüli (magasabb szintű irányító, vagy független minősítő szervezet részéről). 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 korábban említett konfigurációs ellenőrző listák alapvető rendeltetése (már nevük alapján is) a biztonság állapotának ellenőrzése.

A *biztonsági útmutatók, ellenőrző listák osztályozása* különböző szempontok szerint lehetséges. Ezek közül a következőkben röviden kettőt mutatunk be:

- az alkalmazási terület szerinti osztályozás;
- és a kidolgozók szerinti osztályozás.

A *biztonsági útmutatók, ellenőrző listák alkalmazási terület szerint* egy terület egészére, vagy egyes részterületeire vonatkozó típusokra osztályozhatóak. Ehhez az osztályozáshoz természetesen meg kell határozni az alapul vett szakterületet, ami lehet például informatikai biztonság, termékbiztonság, munkabiztonság, stb. Szűkebb vizsgálati témánk szempontjából a továbbiakban alapterületnek az átfogó informatikai biztonságot tekintjük.

Az informatikai biztonság részterületei többféleképpen kijelölhetőek és ennek megfelelően többféle részterületi útmutatóval is találkozhatunk. Ilyenek például a következőek:

- 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[4] is.

A *biztonsági útmutatók, ellenőrző listák kidolgozók szerint* több csoportra oszthatóak, ami egyben rendeltetésüket, célközönségüket is meghatározza. 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 és az adott szervezetben kialakított rendnek megfelelően időszakonként újra kiadásra, átdolgozásra kerülnek. Ma már tulajdonképpen ezek képezik minden biztonsági útmutató alapját. A második csoportba a nemzeti szintű dokumentumok (köztük szabványok) tartoznak, amelyek egy adott – nagyobb, fejlettebb – 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 Informatikai Biztonsági Fórum biztonsági ajánlásgyűjteménye és az Egyesült

[4] 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.]

Államok Nemzeti Szabványügyi és Technológiai Intézete 800-as kiadványsorozatának egyes összetevői tartoznak.

Az ISO/IEC 27000 szabványsorozat az informatikai biztonság menedzsmentjének "legjobb gyakorlatait" fogja össze, melyet a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) közösen adott ki. A szabványcsalád egyik eleme az *ISO/IEC 27002:2005 Az informatikai biztonság irányítási gyakorlatának kézikönyve*[5] [2], amely a szervezet teljes körű informatikai biztonságának megteremtéséhez nyújt útmutatást biztonsági intézkedések, kontrollok felsorolásával.

A szabvány fejezetekből (sections) áll, ezek elején megtaláljuk az aktuális megvalósítandó biztonsági célokat (objectives); a célok megvalósításához szükséges biztonsági intézkedéseket, kontrollokat; a biztonsági kontrollok megvalósítási útmutatóját (implementation guidance) és egyéb szükséges információkat. A biztonsági kontrollok megfogalmazása általános szintű, a gyakorlati megvalósítás részleteit a szervezetnek saját magának kell kidolgoznia.

A szabvány felépítése alapján a védelem megvalósításának területei a következők: kockázatelemzés, szabályzati rendszer, biztonsági szervezet, vagyontárgyak kezelése, személyi biztonság, fizikai és környezeti biztonság, kommunikáció és üzemeltetés biztonsága, hozzáférés-ellenőrzés, informatikai rendszerek beszerzése, fejlesztése és karbantartása, incidenskezelés, üzletmenet-folytonosság, jogszabályi megfelelőség.

A szabványt bármely szervezet felhasználhatja a szervezeten belüli informatikai biztonság kialakításához, menedzseléséhez és javításához. A szabvány biztonsági kontrollok gyűjteményének tekinthető. A szervezetnek először kockázatelemzést kell végeznie, azonosítania kell a számára szükséges biztonsági előírásokat, követelményeket, majd ezek alapján fel kell építenie a saját biztonsági programját. Ezt a szabvány segítségével meg tudja tenni, a szabványban felsorolt biztonsági kontrollok kiválasztása és alkalmazása által.

Az Informatikai Biztonsági Fórum[6] (ISF) nevű nonprofit informatikai biztonsági szervezet kétévente frissíti az ingyenesen elérhető informatikai biztonsági ajánlásgyűjteményét, az *Informatikai biztonság legjobb gyakorlatainak szabványát*[7] [21]. Az ISO/IEC 27002-höz hasonlóan ennek a dokumentumnak is a célja a szervezeten belüli informatikai biztonság megvalósítása és támogatása gyakorlati és mérhető biztonsági intézkedések felsorolásán keresztül. A szabványt kutatások, nemzetközi szervezetek tapasztalatai és más jelentős szabványok alapján állítják össze elsősorban nagy nemzeti és nemzetközi szervezetek számára, de deklarálják, hogy a szabvány tetszőleges méretű szervezet számára alkalmas az informatikai biztonság megteremtéséhez és fenntartásához. Az ISF ajánlásgyűjteménye célul tűzi ki, hogy lefedje más hasonló célú szabványok (például ISO/IEC 27002 és COBIT) kontroll gyűjteményét.

A szabvány 6 fő fejezetre (aspects), alfejezetekre (areas) és szekciókra (sections) oszlik fel. Minden szekció egy speciális informatikai biztonsági területet fed le, tartalmazza az adott biztonsági elvet (principle), annak célját (objective) és a cél eléréséhez szükséges biztonsági intézkedéseket, kontrollokat, gyakorlati lépéseket (statements).

A szabvány a biztonsági intézkedéseket a következő hat csoportba sorolja be: számítógép telepítés, hálózatok, kritikus üzleti alkalmazások, felhasználói környezet, rendszerfejlesztés és biztonságkezelés.

Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) IT laboratóriuma által kiadott *informatikai biztonsági 800-as sorozat*[8] [5] különböző területek kérdéseivel foglalkozó dokumentumokból, útmutatókból áll. Az útmutatók felépítése

[5] Code of practice for Information Security Management.
[6] Information Security Forum.
[7] The Standard of Good Practice for Information Security.
[8] NIST Special Publications 800 Series.

ismertető-leíró jellegű, ebben eltérnek az előzőleg ismertetett két szabványtól, amelyek inkább pontokba szedett, biztonsági kontrollok gyűjteményeként jelennek meg.

Az Egyesült Államok hadseregében az informatikai rendszerek különböző összetevőire vonatkozó informatikai biztonsági ellenőrzési célokat, az alkalmazandó védelmi rendszabályokat, eljárásokat biztonsági beállítási (konfigurációs) útmutatók rögzítik, melyeket a Védelmi Informatikai Rendszerek Ügynöksége (DISA), valamint a Nemzetbiztonsági Ügynökség készít el és bocsát ki.

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

A DISA útmutatókhoz, az azokban foglaltak ellenőrzéséhez 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 útmutatók és az ellenőrző listák bárki által ingyenesen letölthetők a szkriptek viszont belső használatra készültek [6, 7].

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[9], 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 [8, 9]), 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 [10, 11, 12]). 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 magában. Bizonyos szervezetek (pl. DoD, CIS) az ellenőrzési lista mellé automatikus eszközöket, szkripteket is kifejlesztettek az ellenőrzések gyorsabb elvégezhetősége

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

érdekében. A listákban találhatunk utalást az ellenőrzési pontoknál arra vonatkozólag, hogy az adott követelmény ellenőrzését az automatikus eszköz elvégi-e.

BIZTONSÁGI KONTROLLOK ALAPJAI

A megfelelő biztonsági kontrollok az informatikai biztonság kialakításának és fenntartásának, a biztonság megkívánt (megkövetelt) szintje értékelésének alapvető eszközei, alapját képezik az informatikai biztonsági irányítás (security management) különböző módszertanainak, keretrendszereinek (pld. COBIT[10], ISO 27000 család). A következőkben a biztonsági kontrollokkal kapcsolatos alapvető kérdéseket összegezzük és rendszerezzük, ezen belül:

- bemutatjuk a biztonsági kontrollok fogalmát, rendeltetését;
- rendszerezzük a kontrollok csoportosításait, főbb típusait;
- elemezzük az informatikai biztonsági kontrollok fogalmát, értelmezését;
- megvizsgáljuk a kontrollok helyét, szerepét az informatikai biztonság megvalósításában;
- végül ismertetjük az adatbázis-biztonsági kontrollok fogalmát, csoportosítási lehetőségeit.

A biztonsági kontrollok fogalmának, rendeltetésének vizsgálatához először a kontroll fogalom tartalmát, értelmezését kell rögzítenünk. A *kontroll* (control) kifejezés angolul egyaránt jelent irányítást, illetve felügyeletet, ellenőrzést, többes számban pedig vezérlő-, irányító-, szabályozó szerkezetet, berendezést. Témánk szempontjából a kontroll kifejezés a (belső) ellenőrzés területéhez kapcsolódóan értelmezendő, amelynek széles körben, más szabályozók, módszertanok által is felhasznált alapdokumentuma a COSO[11] Integrált Belső Kontroll Keretrendszere. [13]

A dokumentumban két alapfogalom szerepel: a belső kontroll és a kontroll-tevékenység. A *belső ellenőrzés / belső kontroll* (internal control): a szervezet vezetői és munkatársai által megvalósított összetett folyamat, amelyet a szervezeti célkitűzésekkel kapcsolatos kockázatok meghatározására és ésszerű biztosítékok kialakítására hoztak létre. [14, 65. o.] A *kontroll tevékenység* (control activity) pedig a kockázatok meghatározása és a szervezet céljainak elérése érdekében kialakított elv (előírás) és eljárás, amelyet egy tevékenység kimenetele bizonytalanságának korlátok között tartására irányul. [14, 59. o.]

A COSO dokumentum értelmezésében tehát a szervezeti célkitűzések elérését fenyegető kockázatok kezelésére és megvalósításuk valószínűségének növelésére speciális rendszabályokat, tevékenységeket kell kialakítani, amelyek – más összetevőkkel együtt – egy összetett folyamatot alkotnak. A továbbiakban a két fogalom közül elsősorban a kontroll tevékenységre építünk. Ez az értelmezés szerepel a kockázatkezelés alapelveit rögzítő ISO 31000 nemzetközi szabványban is, amely szerint a *kontroll* olyan intézkedés, amely módosítja a kockázatot. [15, 6. o.]

A *biztonsági kontroll* (security control) a szervezeti célkitűzések megvalósulását biztosító kontrollok egyik, kiemelt szerepet játszó típusa, biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedés (óvintézkedés, ellenintézkedés).

A biztonsági kontroll és a kontroll fogalmak megkülönböztetése a biztonsági kockázat és a kockázat fogalmak értelmezésétől függ. Amennyiben a kockázatot bizonytalan események hatásához kapcsoljuk (ahol a hatások lehetnek pozitívak és negatívak = lehetőségek és

[10] Control Objectives for Information and Related Technology = információs és kapcsolódó technológiára vonatkozó kontroll célkitűzések.

[11] Committee of Sponsoring Organizations of the Treadway Commission = A Treadway Bizottság Támogató Szervezeteinek Bizottsága (könyvvizsgáló szervezetek önkéntes együttműködése).

fenyegetések), a két kontroll fogalom tartalma között nincs különbség. Ilyen értelmezéssel találkozhatunk az ISO 31000 szabványban. [15, 1. o.] Amennyiben viszont a kockázatot a negatív, káros hatású események körére szűkítve értelmezzük, akkor a két fogalom rész-egész viszonyban áll egymással. Erre az értelmezésre épülnek az informatikai biztonsági dokumentumok. [1, 4. o.; 16, 222. o.] A továbbiakban mi is erre a szűkebb értelmezésre építünk.

A *biztonsági kontrollok osztályozása* számos különböző szempont szerint lehetséges. Ezek közül a következőkben a jelleg és a rendeltetés szerinti osztályozást mutatjuk be.

A *biztonsági kontrollok jelleg szerint* többféleképpen csoportosíthatóak, ahol a csoportosítás alapját a megvalósítás módjai, eszközei képezik. A COSO keretrendszer két átfogó típust különböztet meg: előírások ("mit kell tenni") és eljárások (az előírások megvalósítása). [13, 51. o.] Az ISO 27000 osztályozásában adminisztratív, technikai, vezetési és jogi kontrollok szerepelnek meghatározás nélkül. [1, 2. o.] 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. [17, B-9, B-6, B-8, B-11. o.]

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. [18, 2., 18., 26. o.]

A *biztonsági kontrollok rendeltetés szerint* is csoportosíthatóak, ami egyben a biztonságot veszélyeztető (nem kívánt) esemény bekövetkezéséhez viszonyított megvalósulásuk szerinti csoportosítást is jelent. Két alapvető típus gyakorlatilag minden dokumentumban megjelenik. 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. [13, 120., 121. o.; 14, 60., 68. o.; 16, 220., 223. o.; 19, 20. o.]

Több alapvető dokumentumban szerepelnek a helyreigazító, helyesbítő (corrective) intézkedések is, amelyek rendeltetése a bekövetkezett nem kívánatos események káros hatásainak csökkentése, azonban definíció nélkül és nem kontrollnak minősítve. [16, 19] Más dokumentumokban találkozhatunk az elrettentő (deterrent) kontrollok fogalmával, amelyek 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.

Az *informatikai biztonsági kontroll* (information/IT security control) fogalmának értelmezése szorosan kapcsolódik az információbiztonság és az informatikai biztonság fogalmak viszonyához, értelmezéséhez, ami mindmáig eltérő szakmai megközelítések, nézeteltérések tárgya. A két fogalom és az alkalmazott kifejezések megkülönböztetése a releváns szabványokban, módszertanokban sem egyértelmű[12], általában csak a tartalom jelzi, hogy az adott dokumentumban szereplő értelmezés melyik megközelítéshez áll közelebb.

A továbbiakban jelen publikációban arra a megközelítésre építünk (részletesebben lásd 20), amely szerint az előbbi fogalom az információ és annak minden megnyilvánulási formája (emberek tudatában, hagyományos hordozón, információs tevékenységeket támogató

[12] Bár a vonatkozó ISO szabványok mindegyike (27000, 13335, 15408, 15443, 18045, stb.) az 'Information technology - Security techniques' szabványcsoportban szerepel.

eszközökben) biztonságához, míg az utóbbi az informatikai rendszerekben, eszközökben kezelt információk és maguk a rendszerek, eszközök biztonságához kapcsolódik. A biztonsági területen, a gyakorlatban a kettő egymástól valójában elválaszthatatlan, önmagában egyik sem jelent teljes körű megoldást.

A fentiek alapján 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 [1, 4. o.], ahol erőforrás minden, aminek értéke van a szervezet számára (információ, szoftver, hardver, szolgáltatások, emberek). [1, 2. o.]

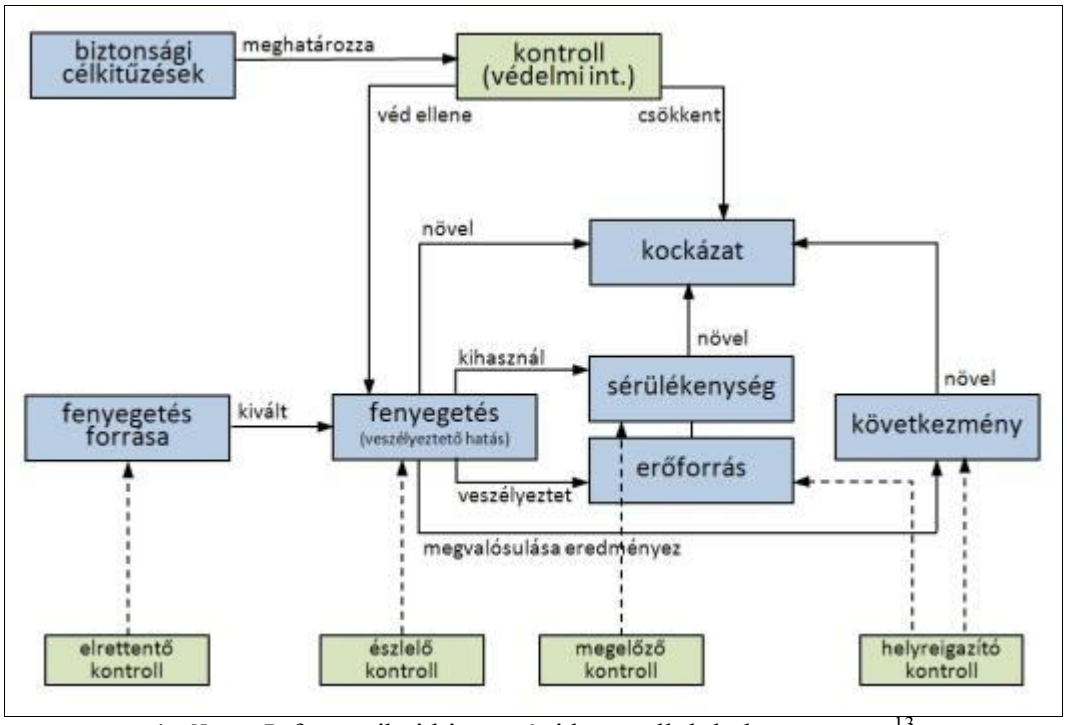
A korábban bemutatott jelleg és rendeltetés mellett az *informatikai biztonsági kontrollok osztályozása az általánosság-részletesség skálán* is lehetséges. Egy védelmi megoldás, intézkedés, eszköz ugyanis többféle szinten meghatározható, például:

- ISO 27002, 11.3.1: A felhasználóknak megfelelő jelszó választási és használati gyakorlatot kell követniük. [2, 64. o.];
- NIST 800-53, IA-5.1.a: Az informatikai rendszer megkövetel bizonyos jelszó-összetettségi előírásokat. [17, F-58. o.];
- CI4.5.3: biztosítani kell, hogy a jelszavak hossza meghaladjon egy minimális értéket, különbözzön a felhasználói azonosítótól, ne tartalmazzon kettőnél több azonos karaktert egymás mellett és ne tartalmazzon kizárólag alfabetikus, vagy kizárólag numerikus karaktereket. [21, CI4.5 o.]

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. Ennek alapjai és rendje részletesebben megtalálható a NIST 800-53 dokumentumban. [17, 7-8., 19-25. o.]

Az általános(abb) 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 kontrollok kiegészítése (control enhancement) további biztonsági funkciók megvalósítását, vagy a kontroll "erősségének" növelését szolgálja. [17, 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.



1. ábra. Informatikai biztonsági kontrollok helye, szerepe[13]

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 kontrollok esetében is végigkövethetők az előzőleg 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 1. ábra osztályozását tekintve megállapíthatjuk (például [9] 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

[13] Készült az ISO 15408 Védelmi fogalmak és kapcsolatrendszerük ábrájának felhasználásával és kiegészítésével [25, 12.o.].

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.

BIZTONSÁGI ÚTMUTATÓK ÉS KONTROLLOK SZEREPE A BIZTONSÁG MEGVALÓSÍTÁSÁBAN

A biztonsági útmutatók, kontrollok – mint korábban már többször megfogalmaztuk – kiemelt szerepet játszanak az informatikai biztonság megvalósításában, ennek keretében az informatikai biztonság irányításában, valamint szabályozásában. A következőkben a biztonsági útmutatók, kontrollok helyével, szerepével, felhasználásával kapcsolatos néhány alapvető kérdést vizsgálunk meg, ezen belül:

- elemezzük a biztonsági útmutatók, kontrollok helyét és szerepét az informatikai biztonság irányításában;
- meghatározzuk a biztonsági útmutatók, kontrollok helyét és szerepét az informatikai biztonság szabályozásában;
- végül körvonalazzuk az adatbázis-biztonsági útmutatók, kontrollok felhasználásának, kialakításának és továbbfejlesztésének rendjét, feladatait.

Az informatikai biztonság eredményes és hatékony megvalósítása – kialakítása és folyamatos fenntartása – *informatikai biztonsági irányítási rendszer* működtetését igényli, amelynek alapvető feladatai közé a következők tartoznak:

- az informatikai biztonsági követelmények meghatározása;
- az informatikai biztonsági kockázatok feltárása, értékelése;
- az informatikai biztonsági kontrollok (védelmi megoldások, intézkedések) kiválasztása és megvalósítása;
- az informatikai biztonság helyzetének figyelemmel kísérése, szükség esetén a követelmények módosítása, a kockázatok újra értékelése és a védelmi intézkedések újbóli meghatározása, továbbfejlesztése és kiegészítése. [1, 10. o.]

Az *informatikai biztonsági útmutatók, kontrollok a kockázatok feltárásában, értékelésében* (risk identification, analysis, evaluation) már szerepet játszanak. Az útmutatók közvetve járulnak hozzá a kockázatok feltárásához azzal, hogy általánosított módon – az útmutató alkalmazási területére vonatkozóan teljes körűen – tartalmaznak különböző szintű kontroll-célkitűzéseket, amelyek felhasználása segíthet kockázatok felismerésében. Emellett a kockázatok alapját a védendő erőforrások sérülékenységei és az ezeket kihasználni képes fenyegetések mellett a már létező védelmi megoldások, intézkedések (kontrollok) is képezik. Ezek ugyanis megszüntethetik, vagy csökkenthetik az erőforrások eredendő sérülékenységét, korlátozhatják a fenyegetések káros hatásait, ezzel befolyásolhatják a kockázatokat.

Az *informatikai biztonsági útmutatók, kontrollok a kockázatok kezelésében* (risk treatment) alapvető szerepet játszanak. Ennek során a kontrollok az egyik legfontosabb megoldást képezik. Amennyiben a döntéshozók nem a kockázatok felvállalását, elkerülését, vagy áthárítását választják, a kockázatok csökkentésére megfelelő védelmi intézkedéseket kell alkalmazniuk. [3, 42. o.] 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 meghatározásához. Természetesen védelmi

intézkedések (kontrollok) útmutatók nélkül is meghatározhatóak, ez azonban a gyakorlat meglévő tapasztalatainak, eredményeinek figyelmen kívül hagyását jelenti.

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. Az általános (több szervezetben is hasznosítható) útmutatók felhasználási lehetősége kétoldalú. Egyrészt a tapasztalatok alapján frissített útmutatók új követelményekre, sebezhetőségekre és megoldásokra hívhatják fel az egyes szervezetek figyelmét, másrészt – mivel a biztonsági helyzet folyamatos figyelemmel kísérése, illetve ennek különböző megoldásai maguk is szerepelnek a kontrollok között – konkrét útmutatást is tartalmaznak. A legismertebb útmutatók (kontroll-gyűjtemények) mindegyikében megtalálhatóak a felülvizsgálatra, értékelésre irányuló kontrollok.[14]

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. A szabályozáshoz kapcsolódóan fontos szerepet játszanak a szabványok is.

A *biztonsági útmutatók közvetlen alkalmazása* nemzeti, ágazati, vagy szervezeti szinten azt jelenti, hogy az adott szabályozó a hatálya alá tartozó szervezetek, szervezeti elemek számára előírja kiválasztott útmutató(k)ban 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 [22], 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 [23] az ISO 27002 útmutatóra épít. Szervezeti szabályozások előírhatják az alkalmazott rendszerekre, eszközökre vonatkozó gyártói útmutatók alkalmazását is.

A *biztonsági útmutatók közvetett alkalmazása* esetében az adott szabályozó közvetlenül nem hivatkozik útmutatóra, ehelyett – mintegy szakmai háttéranyagként – az abban (azokban) foglaltak kerülnek felhasználásra. Ennek során elsősorban az útmutató(k)ban található informatikai biztonsági célkitűzések – kontroll célkitűzések – 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 minőségbiztosítási alkalmazása a szabályozásban* elsősorban belső minőségellenőrzési és külső minőségtanúsítási előírásokra épül. Az informatikai biztonság területén régóta léteznek minőségértékelési, tanúsítási módszertanok, szabványok, útmutatók. Míg ezek korábban függetlenek voltak a biztonsági kontrollok gyűjteményét tartalmazó útmutatóktól, az ISO 27000 szabványcsalád esetében ez a kapcsolat már kiépült, a kidolgozás alatt álló szabványok egyike[15] kimondottan a biztonsági kontrollokhoz kapcsolódik.

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

---

[14] ISO 27002 [2]: 5.1.2, 6.1.8 és 15.2 kontrollok;
ISF SGOP [21]: SM3.5, SM7.1, CB5.4, CI5.5, NW4.5 és SD2.3 kontroll-csoportok (szekciók);
NIST 800-53 [17]: AU és CA kontroll-családok.

[15] ISO 27008, Guidance for auditors on ISMS controls = Útmutató ellenőrök számára a biztonsági kontrollokhoz.

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. [24, 3. o.]

Az *adatbázis-biztonsági útmutatók felhasználása* – a fentiekkel összhangban – 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).

Jelenleg hazánkban nemzeti szintű adatbázis-biztonsági szabályozás nem létezik, a jövőben azonban az e-közigazgatás és a kritikus infrastruktúra védelem területén szükség lehet ennek bevezetésére. A szerzők véleménye szerint a jövőben kialakítandói szabályozást érdemes lenne a következő többszintű modell mentén felépíteni.

A szabályozás egyik részét képezné a szervezet- és tevékenység-független általános adatbázis-biztonsági útmutató, mely rendszabályok rendezett listája lenne. Az általános adatbázis-biztonsági útmutató keretszabályozást jelentene, az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági kontrollokat 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. Az útmutató önmagában nem egy kötelező erejű jogszabály lenne, helyét magyar viszonylatban a Közigazgatási Informatikai Bizottság ajánlásai között tudnánk elképzelni. Használatát viszont meghatározott szervezetek számára egy kormányrendelet elrendelhetné.

A szabályozás másik része szervezet specifikus dokumentumokból állna. A szabályozás hatálya alá eső szervezetnek ki kellene dolgoznia a saját általános adatbázis biztonsági útmutatóját az előző pontban leírt útmutató adaptációjával. Ebben az adatbázis rendszerre vonatkozó követelményeket saját szervezetére vonatkoztatva kellene megfogalmazni. Továbbá a szervezetnek az általános biztonsági követelményeket át kellene fogalmaznia konkrét biztonsági kontrollok, ellenőrzési pontok halmazává, ami a saját adatbázis-kezelő rendszerére és az aktuális működési környezetre érvényes, ez lenne a szervezet adatbázis-biztonsági ellenőrző listája. Ebből a két dokumentumból épülne fel a szervezet adatbázis-biztonsági szabályzata.

Az adatbázis-biztonsági útmutatók felépítésére a gyakorlatban különböző példákat láthatunk. Egy általunk logikusnak vélt rendszerezés a biztonsági kontrollok rendeltetés szerinti csoportosításra épül. Ezek alapján megkülönböztetjük 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.

ÖSSZEGZÉS

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 szervezetek biztonsági szabályozórendszere 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* a biztonsági útmutatókban foglalt konkrét megoldások, tevékenységek megvalósulásának ellenőrzésére szolgáló dokumentumok. Az informatikai biztonsági területen jelentős szerepet játszanak a biztonsági konfigurációs ellenőrző listák, 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.

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. A dokumentumokat két fő csoportra oszthatjuk a bennük található biztonsági kontrollok általános-részletes jellege alapján. Az egyik csoportot az általános adatbázis-biztonsági útmutatók alkotják, melyek az adatbázis-kezelő rendszer típusától függetlenül fogalmaznak meg biztonsági követelményeket. A másik csoportot az adatbázis-kezelő rendszer típusához készült útmutatók alkotják, melyek általában adatbázis ellenőrző lista elnevezést viselik.

Az informatikai biztonsági útmutatók összetevőit képző *biztonsági kontrollok* az informatikai biztonság kialakításának, fenntartásának és értékelésének alapvető eszközei, alapját képezik az informatikai biztonsági irányítás különböző módszertanának. *Informatikai biztonsági kontroll* alatt az informatikai biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedést (óvintézkedést, ellenintézkedést) értünk. Az informatikai biztonsági 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.

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

Az általános adatbázis-biztonsági útmutatók technológia- és megvalósítás-független általános kontrollokat tartalmaznak. 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. Ekkor a kontrollok függnek az adatbázis-kezelő rendszer típusától, verziójától és a működési környezet tulajdonságaitól.

A biztonsági útmutatók, kontrollok szerepe az informatikai biztonság megvalósításában, ennek keretében az informatikai biztonság irányításában, valamint szabályozásában kiemelt jellegű. 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 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.

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).

Jelenleg hazánkban nemzeti szintű adatbázis-biztonsági szabályozás nem létezik, a jövőben azonban az e-közigazgatás és a kritikus infrastruktúra védelem területén szükséges lehet ennek bevezetésére.

Felhasznált irodalom

[1] ISO/IEC 27000:2009 (E), Information technology – Security techniques – Information security management systems – Overview and vocabulary. First edition. – ISO/IEC, 2009.05.01.

[2] ISO/IEC 27002:2005 (E), Information technology – Security techniques – Code of practice for information security management. First edition. – ISO/IEC, 2005.06.15.

[3] Berkes Zoltán, Déri Zoltán, Krasznay Csaba, Muha Lajos: KIB 25. ajánlása, 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK). 25/1-1. kötet, Informatikai Biztonsági Irányítási Rendszer (IBIR). 1.0 verzió. Budapest: Miniszterelnöki Hivatal, 2008.

[4] NIST Special Publication 800-70, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers. Revision 2. – National Institute of Standards and Technology, Gaithersburg, 2011 február.

[5] Special Publication 800 Series. – NIST. [csrc.nist.gov/publications/PubsSPs.html, 2011.08.10.]

[6] Security Technical Implementation Guides. – DISA. [iase.disa.mil/stigs/index.html, 2011.08.10.]

[7] Munk S., Fleiner R.:Az adatbázis-biztonság szabályozása és megvalósítása az Egyesült Államok haderejében– Bolyai Szemle, 2009 (XVIII.)/4. (81-102.o.)

[8] Database Security Technical Implementation Guide, Version 8, Release 1. – DISA, 2007. szeptember.

[9] Database Security Guideline. – Database Security Consortium, 2009.

[10] Security Configuration Benchmark For Oracle Database Server 11g. - The Center for Internet Security, 2008 szeptember
[cisecurity.org, 2011.08.10.]

[11] Oracle Database Security Checklist. – SANS Institute.
[www.sans.org/score/oraclechecklist.php, 2011.08.10.]

[12] Database Security Checklist, Version 7, Release 2.2. – DISA, 2006. október.

[13] Internal Control – Integrated Framework. Executive Summary. – Committee of Sponsoring Organizations of the Treadway Commission, 1992.

[14] INTOSAI GOV 9100, Irányelvek a belső kontroll standardokhoz a közszférában. (magyar fordítás) – INTOSAI Főtitkárság, Bécs, 2004.

[15] ISO 31000:2009(E), Risk Management – Principles and guidelines. First Edition. – ISO, 2009.11.15.

[16] COBIT 4.1 Magyar Változat. – Információrendszer Ellenőrök Egyesülete, 2007.

[17] 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.

[18] CERT Resilience Management Model, Version 1.0, Glossary of Terms. – Carnegie Mellon University, Software Engineering Institute, 2010 május.

[19] NIST Special Publication 800-30, Risk Management Guide for Information Technology System. – National Institute of Standards and Technology, Gaithersburg, 2002 július.

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

[21] The Standard of Good Practice for Information Security. – Information Security Forum, 2007.

[22] Federal Information Security Management Act. (Title III of the E-Government Act) – 2002.

[23] ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002. – ISO, 2008.07.01.

[24] A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről. – PSZÁF, Budapest, 2007 október.

[25] 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.