Répás Sándor – Dalicsek István

AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATELEMZÉS MÓDSZERTANI KÉRDÉSEI A KRITIKUS INFRASTRUKTÚRA ELEMEKET ÜZEMELTETŐ SZERVEZETEK ESETÉBEN

A létfontosságú rendszerek üzemeltetése során is egyre nagyobb szerep hárul a mind komplexebb informatikai rendszerekre. A térhódítással együtt jár a kockázatok számának, a rendszerek sérüléséből eredő károk mértékének ugrásszerű növekedése. Ma már egyetlen szervezet működéséből sem hiányozhat az információbiztonsági tevékenység. Különösen igaz ez a kritikus infrastruktúra rendszereket üzemeltető szervezetek esetében, ahol jogszabályok is rögzítik az információbiztonsági tevékenység kereteit és elvárásait.

Ennek tükrében – gyakorlati tapasztalatainkat is felhasználva – mutatjuk be az információbiztonsági kockázatmenedzsment tevékenység folyamatának egy olyan lehetséges kialakítását, amely egyszerre veszi figyelembe a szabványok elvárásait, valamint a vonatkozó jogszabályi követelményeket. Véleményünk szerint a két követelményrendszer megfelelően harmonizálható, a szervezet adottságait is figyelembe vevő működési keret alakítható ki, mely nagymértékben képes növelni a szervezet biztonsági szintjét.

Kulcsszavak:
biztonsági osztályok, CIP, IBIR, interdependencia, ISO/IEC 27 000, létfontosságú rendszer, vagyonelemek

1. BEVEZETÉS

A létfontosságú rendszerekről és létesítményekről szóló törvény[1] (Lrtv.), valamint hozzá kapcsolódóan, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény[2] (Ibtv.) rengeteg feladatot ró a kritikus infrastruktúrát üzemeltető szervezetekre. Az állami törekvések hatásaként a kritikus infrastruktúrák üzemeltetésében várhatóan

1 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
2 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

egyre nagyobb szerep hárul különböző állami intézményekre, vállalatokra.[3] Ezen túlmenően a létfontosságú ágazatok közé tartozik a jogrend, kormányzat, valamint a közbiztonság, védelem területe is. A létfontosságú rendszereket üzemeltető szervezetek jelentős része működése során alkalmaz valamilyen (akár több) irányítási rendszert, ugyanakkor a közigazgatás területén is kezdenek megjelenni a különböző irányítási rendszerek.[4] Az információbiztonság területén széles körben alkalmazott az ISO/IEC 27001-es szabvány szerinti információbiztonsági irányítási rendszer (IBIR).[5]

A kritikus infrastruktúra rendszerek működése és védelme a társadalom működése szempontjából kiemelt jelentőséggel bír, ugyanakkor a kockázatokkal arányos és költséghatékony védelem kialakításának elengedhetetlen eszköze a kockázatmenedzsment. Munkánkban azt mutatjuk be, hogy tapasztalataink alapján milyen módon lehet a gyakorlatban kialakítani és megvalósítani az ISO/IEC 27000 szabványcsaládnak teljes mértékben megfelelő, a gyakorlatban jól használható módszertant kritikus infrastruktúrákat üzemeltető szervezetek esetében. A következőkben egy az ISO/IEC 27001 szabványnak megfelelő információbiztonsági kockázatmenedzsment-szabályzat kialakítását mutatjuk be, mely figyelembe veszi a kritikus infrastruktúra üzemeltetőkre vonatkozó jogszabályi követelményeket. Megvizsgáljuk a felmerülő kérdéseket, problémákat, és bemutatunk egy lehetséges megoldást is.

2. A KRITIKUS INFRASTRUKTÚRÁK JELLEMZŐI

A modern társadalmak működéséhez elengedhetetlenül szükség van különböző infrastruktúrák szolgáltatásaira, melyek folyamatosan biztosítják az emberek életének és a gazdaság működésének feltételeit. Ilyen infrastruktúra lehet például az energiaellátás, az infokommunikáció, a közlekedés, de a pénzügyi rendszer is. Könnyen belátható, hogy a felsoroltak közül bármelyik elégtelen működése komoly károkat okoz a társadalom számára, így ezen infrastruktúrák kielégítő működése kritikus fontosságú.

2.1. Jogszabályi környezet

A kritikus infrastruktúráknak (létfontosságú rendszerek) számos meghatározása létezik.[6,7] A katasztrófavédelemről szóló kormányrendelet[8] a következő definíciót tartalmazza:

3 Bálint Norbert et al: *A közösségi közműszolgáltatás megszervezésének egyes szabályozási kérdéseiről*, Pro Publico Bono – Magyar Közigazgatás, 3(2015)/1, 4–18.

4 Soós Hajnalka: *Szemelvények a minőségbiztosítási rendszerek megjelenéséről*, Pro Publico Bono – Magyar Közigazgatás, 1(2013)/3, 121–124.

5 Michelberger Pál és Lábodi Csaba: *Vállalati információbiztonság szervezése* = Vállalkozásfejlesztés a XXI. században II., szerk. Nagy Imre Zoltán, Óbudai Egyetem, Budapest, 2012, 241–302.

6 USA PATRIOT Act (H.R. 3162)

7 COM(2006) 787 final 2006/0276 (CNS), Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

8 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról, 25. bekezdés

„Kritikus infrastruktúra: Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."

Az Lrtv. pedig a következő definíciót használja:

„Létfontosságú rendszerelem: az 1–3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."

A mellékletben meghatározott tíz ágazat – valamint az utolsó két ágazat esetében az alágazatok is – a következő:

- Energia
- Közlekedés
- Agrárgazdaság
- Egészségügy
- Pénzügy
- Ipar
- Infokommunikációs technológiák
- Víz
- Jogrend – Kormányzat
  - kormányzati rendszerek, létesítmények, eszközök
  - közigazgatási szolgáltatások
  - igazságszolgáltatás
- Közbiztonság – Védelem
  - rendvédelmi szervek infrastruktúrái
  - honvédelmi rendszerek és létesítmények

Azon szervezeteknek, melyek kritikus infrastruktúrát üzemeltetnek, be kell tartaniuk az Ibtv.-t, valamint a hozzá kiadott végrehajtási rendeletet[9] (vhr.), mely a szervezet informatikai rendszerével kapcsolatos követelményeket tartalmaz.

A felsoroltakon kívül természetesen még rengeteg jogszabályhoz kell alkalmazkodnia a szervezeteknek, azonban az ismertetett jogszabályok az elsődleges források a szabályzat kidolgozása során.

9 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről, majd 2015. július 17-től pedig 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

2.2. Interdependencia

Az egyes infrastruktúrák működtetéséhez szükség van más infrastruktúrák igénybevételére. Az infokommunikációs technológiák (IKT) fejlődésének következtében szerepük kiemelkedő fontosságú, aminek oka, hogy szinte minden infrastruktúra üzemeltetéséhez elengedhetetlenül szükséges a megfelelő működésük. A magyarországi távközlési és energetikai szektor bevonásával[10] végrehajtásra került kritikus infrastruktúra védelmi gyakorlat szintén rámutatott az IKT-ágazat kiemelt fontosságára. Ráadásul az ipari automatizálási rendszerek (Supervisory Control and Data Acquisition, SCADA) elterjedésével olyan informatikai eszközök kerültek alkalmazásra, melyek tevékenységük során fizikai beavatkozó eszközöket irányítanak, mint például a jelzőlámpák, vasúti váltóberendezések, szivattyúk, repülőgépek, atomerőművek, de akár fegyverrendszereket is. Az informatikai rendszerek komplexitásának növekedése pedig egyre nagyobb kockázatok megjelenését idézte elő.[11] A kritikus infrastruktúrák kölcsönös függőségét Rinaldi és társai,[12] valamint Dudenhoeffer és társai[13] vizsgálták részletesen. Az IKT kiemelkedő jelentőségét mutatja az is, hogy bevezetésre került a kritikus információs infrastruktúrák fogalma. A 2005. november 17-én elfogadott, a „Létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló „Zöld könyv"[14] 1-es melléklete a kritikus információs infrastruktúrákat a következőképpen azonosítja: „Kritikus Információs Infrastruktúra (CII): IKT-rendszerek, melyek önmagukban kritikus infrastruktúrák, vagy létfontosságúak kritikus infrastruktúrák működéséhez."[15]

Mindezek alapján különösen fontos az informatikai rendszerek megfelelő kockázatmenedzsment-folyamatának kialakítása.

2.3. Kritikus infrastruktúra üzemeltető szervezetek jellemzői

A kritikus infrastruktúrát működtető szervezetek általában nagyvállalatok vagy jelentős állami intézmények. Működésük jól szabályozott, sokszor folyamatalapú, rendelkeznek a speciális ágazati tudást hordozó szakembergárdával és kialakult vállalati kultúrával. Általában saját informatikai infrastruktúrát építenek ki és biztosítják a hozzá megfelelő belső üzemeltetési erőforrásokat. Sok, ebbe a körbe tartozó szervezet már korábban is megfelelt az ISO/IEC 9001, valamint az ISO/IEC 27001 szabvány elvárásainak. Néhányuk pedig működését rendszeres auditok során tanúsíttatta is. Fontos változás, hogy megjelent az ISO/IEC 27001

10 Angyal Zoltán, Maros Dóra: *A távközlési és energiaszektor infrastruktúráinak interdependenciái, a 2010 KIV gyakorlat tapasztalatai = 17. HTE Infokommunikációs Hálózatok és Alkalmazások Konferencia és Kiállítás (Intelligens infrastruktúrák és alkalmazások),* HTE, Siófok, 2010. 10. 27–2010. 10. 29, 34–45.

11 Rajnai Zoltán, Puskás Béla: *The risks of network complexity,* Bolyai Szemle, 33(2014)/2, 60–66.

12 Steven M. Rinaldi et al.: *Identifying, understanding and analyzing critical infrastructure interdependencies*, IEEE Control Systems Magazine, 21(2001)/6, 11–25.

13 Donald D. Dudenhoeffer et al.: *CIMS: A framework for infrastructure interdependency modeling and analysis = WSC 06. Winter Simulation Conference*, IEEE, Monterey, 2006, 478–485.

14 Green Paper on a european programme for critical infrastructure protection (COM/2005/0576 final) Forrás: eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576 (2015. 12. 30.)

15 Saját fordítás.

szabvány első revíziója, az ISO/IEC 27001:2013, majd magyar szabványként az MSZ ISO/IEC 27001:2014. Az új szabvány beépítette az eddigi tapasztalatokat, valamint átstrukturálásra is került.

Az ISO/IEC 27005:2011 Information security risk management szabvány az ISO 27001 elvárásai alapján történő kockázatmenedzsmenttel kapcsolatban ad iránymutatásokat.

3. INFORMÁCIÓBIZTONSÁGI KOCKÁZATKEZELÉS

A kritikus infrastruktúra elemeket üzemeltető szervezetek valamilyen szinten formalizált Információbiztonsági Irányítási Rendszert (IBIR) működtetnek. A megváltozott körülmények és a megszerzett tapasztalatok szükségessé teszik az IBIR rendszer folyamatos értékelését és fejlesztését, melynek keretében az információbiztonsági kockázatkezelési tevékenység is zajlik. Általánosnak mondható, hogy Információbiztonsági Szabályzattal valamenynyi szervezet rendelkezik, ugyanakkor az információbiztonsági kockázatkezelési szabályzat nem, vagy nem megfelelő minőségben áll rendelkezésre.

3.1. Az információbiztonsági kockázatkezelési szabályzat

Az információbiztonsági kockázatkezelési szabályzat kidolgozását (átdolgozását) egy erre dedikált projekt keretén belül célszerű megvalósítani.

A projekt résztvevői:

- az információbiztonságért felelős szervezet szervezetiegység-vezetője (célszerűen a projektszponzor),
- az információbiztonságért felelős személy (a projekt vezetője),
- az informatikai terület képviselője,
- a szervezet általános (pénzügyi) kockázatkezelési területének képviselője,
- a szervezet szabályozási területének képviselője,
- amennyiben a szervezet nem rendelkezik a megfelelő szakmai kompetenciával (pl. CISA), akkor célszerű külső erőforrás bevonása is – akár tanácsadóként, akár minőségbiztosítóként.

A projekt működésének támogatását adminisztratív eszközökkel is biztosítani kell:

- projektalapító dokumentum kidolgozása,
- projektértekezletek,
- változáskezelés stb. a szervezet projektkultúrájának megfelelően.

A projekt információbiztonsági vonatkozásai miatt különösen fontos a résztvevők közti biztonságos elektronikus kommunikáció megoldása, ezért titkosított megoldások (pl. SMIME, HTTPS) alkalmazása javasolt.

A szabályzat kidolgozása során, a folyamat egyes lépéseinek meghatározásához javasolt az ISO/IEC 2700X szabványcsalád, ezen belül is kiemelten az ISO/IEC 27001:2013 szabvány elvárásait figyelembe venni – még abban az esetben is, ha a szervezet nem tervezi a szabványnak való teljes megfelelést és ennek auditálását. A szakmai részletek kidolgozásánál pedig – mint erre a későbbiekben majd rámutatunk – célszerű a 2013. évi L. törvény és a hozzá tartozó végrehajtási rendelet elvárásait ötvözni, hiszen így biztosítható majd az elvárásoknak való megfe-

lelés. Ezen túlmenően, a folyamatos fejlődés érdekében, a PDCA modell alkalmazásához szükséges az eddigi tapasztalatok, valamint auditok megállapításainak, észrevételeinek beépítése is.

Arra kell törekedni, hogy az információbiztonsági kockázatkezelési szabályzat – és így végső soron maga az információbiztonsági kockázatkezelési tevékenység – megfeleljen az alábbi követelményeknek:

– a kockázatkezelési tevékenység a szervezet által meghatározott kereteken belül, a biztosított erőforrásokkal folyamatszerűen végezhető;
  teljes mértékben lefedi a kockázatfelmérés és -kezelés folyamatát:
  - kockázatfelmérés,
  - kockázatértékelés,
  - kockázatkezelés,
  - kockázatelfogadás,
  - kockázatismertetés (kommunikáció),
  - követés és fejlesztés;
– a szabályzat alapján a kockázatfelmérés egyértelműen elvégezhető és bármikor reprodukálható, illetve aktualizálható,
– a kockázatok kezelésére meghatározott intézkedések hatékonyabb, kockázatarányos információbiztonsági kockázatkezelési tevékenységet tesznek lehetővé.

3.2. Az információbiztonsági kockázatkezelés folyamata

3.2.1. Biztonsági osztályok kialakítása

Az Ibtv. vhr.-je sok esetben meghatározza az új információbiztonsági kockázatkezelési szabályzat tartalmát, hiszen a jogszabályi megfelelés minden esetben elsődleges szempont. A jogszabály 1. Általános irányelvei is említik, hogy a kritikus infrastruktúrák esetében a rendelkezésre állás a legfontosabb szempont. Ugyanakkor azt is fontos megemlíteni, hogy a jogszabály sok kérdés esetében a döntést (vagy a pontosítást, vagy a konkrét megoldást) a szervezetre bízza. A biztonsági osztályok meghatározásánál is így járt el, ahhoz csak irányelveket fogalmaz meg, így lehetővé teszi a szervezet számára fontos szempontok alkalmazását is. Az osztályba sorolás szempontjai elsődlegesen az Ibtv. vhr. és a szervezet kockázatkezelési szabályzata alapján kerülhetnek kialakításra. Mindkét forrásból figyelembevételre kerülhetnek a lényeges szempontok, célszerű összerendelni az egyes kárérték-kategóriákat az egyes biztonsági osztályok összeghatáraival. A káresemények mértékének meghatározása során az adattípusokhoz és adatmennyiségekhez elsődlegesen a jogszabály, míg az összeghatárokhoz elsődlegesen a vállalati kockázatkezelési szabályzat szolgálhat forrásként.

A biztonsági osztályok kialakításánál fontos szempontok a következők:

– a vhr. 5 osztályt határoz meg a rendszerek biztonsági osztályba sorolásához;
– a szervezet létfontosságú rendszerelemeket üzemeltet;
– a szervezet általános kockázatkezelési gyakorlata;
– a szervezet pénzügyi mutatószámai;
– milyen típusú adatokat kezel a szervezet;

– milyen mennyiségben kezeli az adott adatokat;
– milyen forrásokból jut az adatokhoz;
– kiknek továbbítja az adatokat.

3.2.2. Információs vagyonelemek meghatározása

A szervezeti keretek definiálása után következő lépésként azonosítani kell azon adatforrásokat, melyek alkalmazhatók az információs vagyonelemek felmérése során. A szervezetek (tevékenységükből és méretükből adódóan is) számtalan nyilvántartással rendelkeznek, melyek általában sajnos nincsenek összekötve, integrálva, nem egységesek és csak manuálisan hozhatók kapcsolatba egymással. Nagyon fontos szempont, hogy a vagyonelemek felmérését rendszeresen el kell végezni, annak kellően pontosnak, részletesnek kell lennie, hogy elősegítse a kockázatmenedzsment feladatának elvégzését. Mindemellett a legtöbb szervezet nem használ az információbiztonsági kockázatmenedzsment feladatának elvégzésére automatizált eszközöket, így célszerűen olyan módszertan kerülhet kidolgozásra, mely az információs vagyonelemek azonosítását csak olyan részletességgel végzi el, mely feltétlenül szükséges.

Az információs vagyonelemek azonosítása során két lehetséges megközelítés merül fel. Az első módszer esetében alulról építkezve, az összes vagyonelem összegyűjtése a különböző nyilvántartásokból, majd azoknak folyamatokhoz rendelése történik meg bottom-up módon. Ez lényegesen pontosabb, minden részletre kiterjedő azonosítást eredményezhet, azonban nagyon sok energiát igénylő feladat. A második megoldás esetében top-down módon, első lépésként az üzleti folyamatok kerülnek azonosításra, majd ezt követően az egyes folyamatokhoz a folyamatokban részt vevő vagyonelemek azonosítása történik meg. Ez a megoldás alacsonyabb erőforrás-ráfordítással elvégezhető, azonban a nem azonosított információs vagyonelemek aránya magasabb lehet, mint az első módszer esetében.

Külön hangsúlyoznunk kell, hogy a nyilvántartások rendelkezésre állása és tartalmuk minősége nagymértékben meghatározza a teljes kockázatkezelési tevékenység minőségét. Abban az esetben, ha a kockázatkezelési projekt keretében kell elvégezni felméréseket, leltározásokat, az adatok aktualizálását és tisztítását, akkor az eredetileg becsült erőforrás- és időszükséglet valószínűleg többszörösére nő. A megfelelő megközelítés kiválasztása mindig az adott szervezet, valamint a projekt adottságai alapján történik, sőt lehetőség van a két megközelítés kombinációjának az alkalmazására is. A továbbiakban ezt mutatjuk be.

Az elsődleges vagyonelemek (adatok, alkalmazások) meghatározására a folyamatalapú megközelítést javasoljuk, amennyiben ehhez a megfelelő peremfeltételek rendelkezésre állnak. A szervezet folyamatalapú működése azt jelenti, hogy minden tevékenység folyamatszinten formalizált, az egyes folyamatok leírása utasításként jelenik meg, az egyes folyamatokat nyilvántartják, rendszeresen felülvizsgálják, szükség esetén átdolgozzák és frissítik. Minden egyes folyamat rendelkezik felelőssel (folyamatgazdával). A szervezet üzleti folyamatainak kialakítása és nyilvántartása érdekében általában üzletifolyamat-tervező eszközt alkalmaz. Lehetséges források így az utasítások, azok nyilvántartása, és az üzletifolyamat-tervező eszköz. A cél, hogy az elsődleges vagyonelemek minél nagyobb mértékben automatizált módon azonosításra kerüljenek – ezért célszerű a folyamattervező eszköz használata, mint elsődleges adatforrás. Problé-

ma adódik abból, ha nem azonos minőségű (kidolgozottságú) folyamatok szerepelnek a folyamattervezőben, illetve ha nem egységes névterminológiát használnak a folyamatok dokumentálásakor (pl. azonos adatkört más névvel azonosítanak eltérő folyamatokban). Ilyen esetben lehetőség van az adatok utasításokból történő pontosítására, azonban ez jelentős erőforrás- és időszükséglettel járhat. Az eltérések egyik oka lehet például, hogy az egyes folyamatokat nem ugyanazok a személyek tervezik, hanem az adott folyamatok működését jól ismerők, az adott szakterület szakemberei tervezik meg.

Az elsődleges vagyonelemek folyamatalapú azonosítása sok tanulsággal szolgálhat magának a folyamatalapú működésnek, a folyamatok kidolgozásának és naprakészségének minőségét illetően. Úgy gondoljuk, a tapasztalatok összefoglalása és a visszajelzés fontos e tekintetben is. Ugyanakkor véleményünk szerint a folyamatok kidolgozása és dokumentálása kapcsán felmerülő tényleges hibák és hiányosságok javítása nem lehet a kockázatkezelési projekt feladata és hatékonyan nem is végezhető el egy ilyen projekt keretein belül.

3.2.2.1. Bizalmasság (B)/Sértetlenség (S)/Rendelkezésre állás (R) értékek meghatározása

A vhr alapján a B/S/R értékeket ötfokozatú skálán kell meghatározni, valamint „a veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárértékszinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő."

Az elsődleges információs vagyonelemek B/S/R értékeinek meghatározásában kompetenciával elsődlegesen a folyamat üzemeltetője, az adott üzleti terület rendelkezik. Az egyes folyamatok elvárt R értékeit a szervezet üzletmenet-folytonossági terve (ÜFT) rögzíti. Joggal feltételezhető, hogy kritikus infrastruktúra elemeket üzemeltető szervezetek esetében ez rendelkezésre áll. Így a folyamatokban részt vevő információs vagyonelemekre az R érték örökíthető. Fontos azonban, hogy a folyamatot nem minden esetben akasztja meg egy-egy vagyonelem elérhetetlensége. Tehát R értékének örökítésével erőforrás takarítható meg, ugyanakkor hiba és pontatlanság is keletkezhet. Mérlegelni kell, hogy ez a pontatlanság kezelhető, vagy az adatok pontosítására van szükség. A B és S értékek meghatározására többféle interjúzási technika áll rendelkezésre:

– online adatgyűjtés (e-mail, elektronikus felület),
– személyes megkérdezés (interjú, workshop).

Az e-mailes megkeresés alacsonyabb erőforrás-szükséglettel rendelkezik, ugyanakkor nem egységes, pontatlanabb eredményeket produkál, hiszen a meghatározásokat az egyes kitöltők más és más módon értelmezhetik.

Az interjúk alkalmazása lényegesen több erőforrást igényel, hiszen a folyamatgazdákkal interjúidőpontok egyeztetése, esetleges módosítása szükséges. Ugyanakkor a begyűjtött információk minősége miatt jóval egységesebb és pontosabb képet nyújt a valós helyzetről.

Lehetőség van kombinált megoldások alkalmazására: a pontos adatfelvétel érdekében a személyes interjúk készítését választjuk, ugyanakkor az eredményesség fokozása (és nem mellékesen időszükségletének csökkentése) érdekében e-mailben ebben az esetben is (előzetesen) kiküldésre kerülhetnek az előzetesen azonosított folyamatok, és kapcsolódó információs vagyonelemek.

3.2.2.2. B/S/R értékek konszolidációja

Az adatfelvétel során meghatározott B/S/R értékek további feldolgozása szükséges, hiszen van olyan információs vagyonelem, mely több folyamatban is részt vesz, azonban az egyes folyamatokban más B/S/R elvárások érvényesülnek vele szemben. Így minden olyan információs vagyonelem esetében, mely több folyamatban is részt vesz, az egyes folyamatokból képzett értéket kell a vagyonelemre érvényesíteni.

3.2.3. Támogató vagyonelemek meghatározása

Az elsődleges vagyonelemek nem létezhetnek önmagukban, szükség van valamilyen eszközre azok feldolgozásához. Egy adatbázisban szereplő adat sincs meg az adatbázis-kezelő rendszer, szerver, tárolórendszer nélkül. Eléréséhez szükség van munkaállomásra, hálózati infrastruktúrára stb. Az egyes támogató vagyonelemek azonosításához forrásként célszerű a minden szervezetnél létező tárgyieszköz-nyilvántartást választani kiindulásként. Ez egy bottom-up elvű megközelítést ad, mely a feldolgozás során finomítható. A tárgyi eszközök nyilvántartásában minden egyes eszköz megtalálható, és mindegyikhez rögzítve van az is, hogy az adott eszköz kinek a használatában van.

A nyilvántartás adatai, valamint a korábban már összeállított folyamatadatok alapján elkészíthető a támogató információs vagyonelemek listája, valamint a B/S/R értékek meghatározása. A szerverek, tárolórendszerek és egyéb, a gépteremben elhelyezkedő számítástechnikai eszközök (központi infrastruktúra) az összes folyamatot figyelembe véve célszerűen a legmagasabb előforduló besorolást kapják, aminek elsődleges oka, hogy a szervezetek jelentős része ma már szinte kizárólag virtualizált környezetet alkalmaz, így nem rendelhetők egyértelműen az egyes eszközök egy-egy informatikai alkalmazáshoz. Ez a tény az Ibtv. által használt rendszerértelmezés alkalmazása során problémákat vethet fel.

3.2.4. Kockázatok azonosítása

A kockázatok azonosítása a következők szerint történik:
- El kell készíteni vagy frissíteni kell a fenyegetés és veszély katalógust, mely alapját képezi a következő lépéseknek. A katalógust ajánlott az Ibtv. szakmai tartalmának megfelelően összeállítani;
- Fel kell mérni a jelenleg érvényben lévő biztonsági intézkedéseket és azok hatókörét;
- Vagyonelemenként fel kell mérni a következő jellemzőket: a vagyonelem vonatkozásában releváns fenyegetések, veszélyek, a bekövetkezési valószínűségek, valamint a meglévő intézkedések.

3.2.5. Kockázatok számszerűsítése

A B/S/R értékek, valamint a sebezhetőségek, veszélyek, bekövetkezési valószínűségek alapján számszerűsítésre kerülnek az egyes kockázatok. A meghatározott kockázatok mértékét csök-

kentik a már meglévő intézkedések, így ezeket is figyelembe kell venni a számszerűsítés során. A kockázatok „forintosításához" a már meghatározott biztonsági osztályok is irányt mutatnak.

3.2.6. Kockázatok kezelése

A kockázatok mértékének meghatározására több módszer is kidolgozásra került.[16] Mi a kockázatok kezeléséről szóló döntés meghozatalához a széles körben elterjedt CCTA Risk Analysis and Management Method (CRAMM) alkalmazását javasoljuk. Egy CRAMM mátrixa látható az 1. ábrán.

Figyelembe véve a jogszabályi hátteret, az 5 × 5-ös mátrix alkalmazása a célszerű. A zöld mezőbe került kockázatok esetében nem kerülnek kidolgozásra új kockázatjavító intézkedések, azok elfogadásra kerülnek. A sárga tartományba került kockázatok esetében a szervezeti működésnek megfelelő döntés szükséges azok további kezeléséről, míg a piros tartományba került kockázatok kezelésére intézkedési terv kidolgozása szükséges.

1. ábra • *Példa a CRAMM mátrixra (saját szerkesztés)*

		Üzleti hatás				
		I	II	III	IV	V
Gyakoriság	1	Elfogadható	Elfogadható	Elfogadható	Elfogadható	Döntés
	2	Elfogadható	Elfogadható	Elfogadható	Döntés	Kezelendő
	3	Elfogadható	Elfogadható	Döntés	Kezelendő	Kezelendő
	4	Elfogadható	Döntés	Kezelendő	Kezelendő	Kezelendő
	5	Döntés	Kezelendő	Kezelendő	Kezelendő	Kezelendő

3.2.7. Intézkedési terv kidolgozása és végrehajtása

Minden kezelendő és kezelésre kiválasztott kockázat esetében intézkedési terv kidolgozása szükséges. Az intézkedési terv kidolgozásánál elsődleges szempont a költséghatékonyság, valamint hogy a terv végrehajtásához szükséges erőforrások rendelkezésre álljanak. Figyelembe kell venni a környezetet, valamint az adottságokat. Érdemes előnyben részesíteni azon intézkedéseket, melyek több kockázat mértékét is csökkentik. Az intézkedési tervben foglaltak végrehajtásának ellenőrzésére rendszeres felülvizsgálatot kell végezni. Eltérések, nem megfelelő eredmény esetén beavatkozás szükséges, melyet akár a környezet változása is okozhat. A 2. ábrán látható az ismertetett kockázatelemzési folyamat grafikusan ábrázolva.

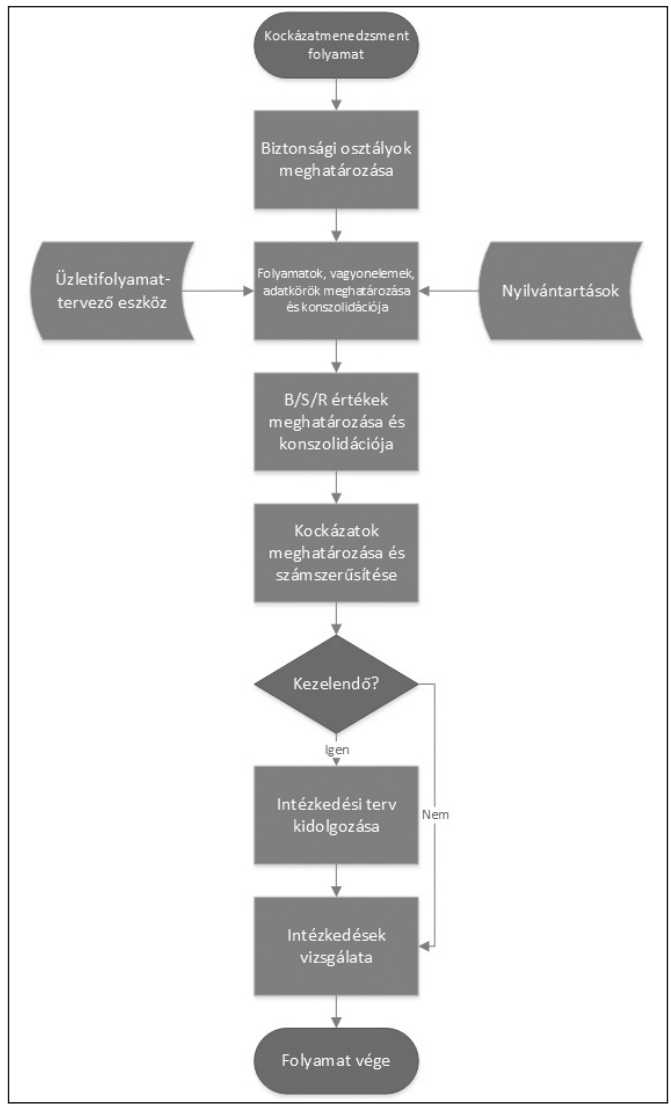
4. KONKLÚZIÓ

Az informatikai rendszerek térhódításával együtt jár a kockázatok számának, a rendszerek sérüléséből eredő károk mértékének ugrásszerű növekedése. Ma már egyetlen szervezet mű-

16 Mógor Tamásné, Rajnai Zoltán: *Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása,* Bolyai Szemle, 33(2014)/2, 43–59.

ködéséből sem hiányozhat az információbiztonsági tevékenység. Különösen igaz ez a kritikus infrastruktúra rendszereket üzemeltető szervezetek esetében, ahol törvényi szabályozás rögzíti az információbiztonsági tevékenység kereteit és elvárásait.

2. ábra • *Kockázatelemzési folyamat grafikusan ábrázolva (saját szerkesztés)*



Ennek tükrében mutattuk be az információbiztonsági kockázatkezelési tevékenység folyamatának egy olyan lehetséges kialakítását, amely egyszerre veszi figyelembe a vonatkozó szabvány (mint legjobb gyakorlat) elvárásait és a jogszabályi követelményeket. A két követelményrendszer harmonizálható, a szervezet adottságait is figyelembe vevő működési keret alakítha-

tó ki. Ebben a keretben a konkrét lépések megfelelő kiválasztásával felépíthető egy hatékony és eredményes kockázatkezelési tevékenység. Erre egyrészt példákat mutattunk, másrészt alternatívák is választhatók. A kialakított folyamatot nem hisszük sem egyedül üdvözítőnek, sem véglegesnek – a gyakorlati tapasztalatok magukkal hozzák a továbblépés lehetőségét.

• • • • • • • • • • •

SUMMARY IN ENGLISH: Operating critical infrastructures requires integrated IT systems; however, their widespread use inevitably involves the increase in the number of risks and potential damages resulting from system vulnerabilities. An effective IT security strategy is fundamental for any organization; especially in case of critical infrastructure systems, whose IT security framework and requirements are laid down by national legislation. In this paper we describe a possible solution for IT security risk management, utilizing our professional experience, which simultaneously meets the demand of different standards and related laws and regulations. According to our results it is possible to conciliate both requirements and develop a highly effective security framework suitable for several organizations increasing their security level.

Répás Sándor (RSandor@ahol.co.hu): gazdálkodás és menedzsment alapképzési szakon diplomázott 2009-ben a Budapesti Corvinus Egyetemen, majd 2011-ben villamosmérnöki alapképzési szakon, az Óbudai Egyetemen. Okleveles villamosmérnöki képzettséget 2013-ban a Széchenyi István Egyetemen szerzett. 2013-ban elnyerte a Nemzeti Kiválóság Program ösztöndíját. 2002 óta foglalkozik az informatika mellett informatikai és információbiztonsági képzésekkel is. 2004-től kezdődően munkájában az informatikai biztonság került előtérbe. 2014-től kezdődően független hálózati és hálózatbiztonsági tanácsadóként dolgozik. Munkái során részt vett hálózatok tervezésében, kivitelezésében, információbiztonsági ellenőrzésekben, auditfelkészítésekben, kapcsolódó szabályzatok kidolgozásában, etikus behatolási tesztek elvégzésében. Jelenleg PhD-hallgató. Kutatási területe az IPv6 bevezetése, valamint a kritikus információs infrastruktúrák biztonsága. Fontosabb gyártói minősítései: CCSI, MCT, CISA, CISM, CRISC, MTCC. Jelentősebb szakmai szervezeti tagságai: IEEE, ACM, HTE, ISACA, MEE, MKT, NJSZT.

Dr. Dalicsek István (dalicsek.istvan@scetix.hu): a Budapesti Műszaki Egyetem villamosmérnöki karán szerzett okleveles villamosmérnöki diplomát 1982-ben, majd ugyanitt egyetemi doktori fokozatot ért el 1987-ben (BME 4697/1987). A Budapesti Közgazdaságtudományi Egyetem Vezetőképző Intézetének London Business School programjában kapott MBA szakoklevelet 1997-ben. Többéves, hazai nagyvállalatoknál és nemzetközi tanácsadó cégeknél szerzett vezetői tapasztalatok birtokában 2005-ben alapította meg saját vezetői tanácsadással foglalkozó vállalkozását, melynek azóta is szakmai és adminisztratív irányítója. A cég egyik kiemelt tevékenységi területe az informatikai és információbiztonsági tanácsadás. Az integrált biztonságirányítási rendszerek működtetése és az információbiztonsági kockázatok kezelése területén több sikeres projektreferenciával rendelkeznek mind a vállalati, mind az államigazgatási szektorban.