HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Muha Lajos – Tóth Georgina Nóra
muha.lajos@zmne.hu - toth.georgina@bgk.uni-obuda.hu

A BANKBIZTONSÁG VIZSGÁLATA KOCKÁZATELEMZÉSSEL

Absztrakt

Minden szervezet esetében a biztonság a stratégiai célokat szolgálja. Különösen igaz ez a piaci körülmények között működő társaságoknál, ahol a biztonság a védendő értékek megőrzésén túlmenően, a működés folyamatosságában is fontos szerepet játszik. A biztonság megteremtése szempontjából elengedhetetlen egy hatékony kockázatelemzés elvégzése. Jelen cikkben pénzintézetek esetén jól alkalmazható biztonsági vizsgálatának előkészítésével és folyamatával foglalkozunk. Ennek során egy hatékony kockázatelemzési módszertant dolgoztunk ki.

For most institutions security is part of their strategy. This is especially true for profit-oriented institutions, where security not only protects their investments but also ensures continuous revenue to continue their operation. For these institutions it is essential to carry out a detailed risk assessment analysis in order to ensure security. In this paper we investigate the preparation and procedure of security evaluation for monetary institutions. For this, we prepared an effective methodology for risk assessment analysis.

Kulcsszavak: *bankbiztonság, biztonsági vizsgálat, kockázatelemzés ~bank security, security audit, risk analysis*

BEVEZETÉS

A pénzintézetek esetében – alapfunkcióikból eredően – az általuk őrzött és kezelt alapértékek, a fizető eszközök, az értékpapírok közvetett és közvetlen biztonságának garantálása alapvető érdekük, mert az ezen értékek elleni sikeres támadások nemcsak közvetlenül számszerűsíthető károkat, hanem komoly presztízsveszteséget is okozhatnak. Ez utóbbi pedig vevői bizalomvesztés előidézésén keresztül további károkat is okozhatnak.

Ezen túlmenően az olyan fenyegetések, amelyek a pénzintézet működésének folyamatosságát, az általuk kezelt érzékeny információk, adatok bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztetik, szintén komoly veszélyt jelentenek a profittermelő képességre.

A fentiekből következik, hogy az *értékmegőrzés*, a *forgalom és működés folyamatosságának biztosítása*, valamint az informatikai biztonság megőrzése azok a kiemelten fontos védelmi célok, amelyek a komplex védelem kialakításánál meghatározóak. A szervezet védelmi céljain túlmenően, a védelmi intézkedéseknek a jogszabályokban, a pénzintézetekre vonatkozó előírásokban és ajánlásokban megfogalmazott biztonsági előírásoknak is meg kell felelni. A pénzintézet belső biztonsági előírásaival együtt ezek egy olyan szabályozási követelményrendszert adnak, amelyek meghatározóan hatnak az adminisztratív védelmi rendszerre és szintén a korábban megfogalmazott védelmi célokat szolgálják.

A biztonság megteremtése és fenntartása szempontjából elengedhetetlen egy hatékony kockázatelemzés elvégzése. Ehhez valamilyen kockázatelemzési módszertant kell felhasználni. Számos kvalitatív és kvantitatív kockázatelemzési módszertan létezik, ezek közül széles körben ismert:

- az informatikai biztonsági kockázatok elemzésére használt CRAMM (Central Computer and Telecommunications Agency: Risk Analysis and Management Method) [1],
- az ipari veszélyek és működési problémák feltárására használt HAZOP (Hazard and Operability Studies) [*2*],
- a deduktív hibaanalízisre használt FTA (Fault Tree Analysis) [3],
- a hibaforrások azonosítására használt FMEA (Failure Modes and Effects Analysis) [4],

Ebben a munkában a brit kormány Központi Számítógép és Távközlési Ügynökség, a CCTA által kidolgozott CRAMM kvalitatív kockázatelemzési és kezelési módszertanát használtuk fel, mivel ez, ha nem is a bankbiztonsági kockázatok, de biztonsági kockázatok elemzésére készült, és arra számos alkalommal felhasználásra került hazánkban is. A választás mellett szólt, hogy az ezen a módszertanon alapuló szoftvereszközt alkalmaz a NATO. Ez a módszertan került feldolgozásra például a Közigazgatási Informatikai Bizottság 25. számú ajánlásának a biztonsági vizsgálatokkal foglalkozó kötetében [5] is.

VÉDELMI CÉLOK

A pénzintézetek esetében a következő védelmi célok meghatározóak a kockázatelemzésben:

- Minden védendő alapértékre (fizető eszközök, értékpapírok) és az azokat körülvevő rendszerelemekre (épület, infrastruktúra, személyzet, stb.) meghatározandók a releváns fenyegetések és a védelmek gyenge pontjai, amelyek ismeretében olyan intézkedési javaslatok alakíthatók ki, amelyekkel javítani lehet a védelem teljes körűségét és zártságát.

- A védelemi képességeknek időben folyamatosan biztosítottaknak kell lenniük. Az egyszer már kellő szinten megvalósított védelmi képességek erodálása (fegyelmezetlenség, hanyagság, a biztonság fontosságának nem kellő tudatosítása miatt, a technika szinten tartásának hiánya és erkölcsi elavulása) is veszélyezteti a folyamatosságot. Ennek fenntartásában fontos szerepet játszik a szabályozottság kielégítő szintje, annak betartása és betartatása. Fontos a folyamatosság biztosításának és biztosítottságának, a szabályozottság, a jogszabályi megfelelősség és ezek ellenőrzésének meghatározott időközönkénti vizsgálata.
- A zárt, teljes körű és folytonos védelem önmagában még nem biztosítja a védelmi képességek a szervezet elfogadható mértékét. Ehhez elengedhetetlen a kockázatok ismerete, de legalábbis közelítő szintű becslése. A kockázatok felmérése, elemzése és minősítése, abból a célból történik, hogy a védelmi rendszerek tervezése, továbbfejlesztése során olyan védelem kerüljön kialakítása, amely a rendszer minden pontján kockázatokkal arányos védelmet nyújt úgy, hogy közben figyelembe veszi a védelem kiépítésének és üzemeltetésének költségeit.

A bankbiztonsági vizsgálat igen sokrétű. Holisztikus megközelítésben ki kell térnie a pénzintézet működésre és szervezetére, ezen belül:

- szervezeti felépítésre,
- a bankbiztonsági szervezetre,
- a biztonsági szervezet tevékenységére, működésére, és annak szabályozottságára,
- a bankbiztonságra vonatkozó jogszabályoknak, külső szabályozóknak (PSZÁF, BASEL II., SOX) való megfelelőségére,
- az élőerős védelemre,
- a személyi védelemre,
- a mechanikai-fizikai védelemre,
- az elektronikai védelemre,
- a tűzvédelemre,
- a pénz- és értéktárolásra, szállításra,
- a pénzmosás elleni védelem belső szabályozottságának végrehajtására,
- a rendkívüli események (katasztrófák, terrorcselekmények) elleni védelemre,
- a humánerőforrás gazdálkodás biztonsági kérdéseire,
- a külső szerződéses partnerek bankon belüli mozgásával kapcsolatos kérdésekre,
- az ügyfél- és vendégforgalommal kapcsolatos kérdésekre.

A fenyegetettségek konkrét ismeretének hiányában az egyik lehetséges módszer a fenyegetések kockázatának megbecsülése, amely a fenyegetés által okozható legnagyobb kárérték és a fenyegetettségek az adott kárértékkel történő bekövetkezésének becsült gyakorisága (valószínűsége) szorzatával azonos. Ha a lehetséges kárértékeket és a bekövetkezési gyakoriságokat tartományokra osztjuk, akkor a kapott kockázati mátrixban meghatározhatók azok a kárérték-gyakoriság értékpárok, amelyek alatt a kockázat "elviselhető", illetve amely felett "nem elviselhető", azaz minden esetben konkrétan mérlegelendő a kockázat értéke és a csökkentését célzó védelmi intézkedések költségeinek egymáshoz való viszonya. Ez alapján lehet tervezés közben az azonos védelmi célú, de különböző védelmi szintű és költségű megoldásokat mérlegelni és kiválasztani. A tervezési feladat alapvető célja az, hogy minimális védelmi költségekkel a maximális kockázatcsökkentést tudjunk elérni.

KOCKÁZATELEMZÉSI MÓDSZERTAN

A vizsgálati módszer egy olyan modell, amelynek a középpontjában a védendő alapértékek (fizetőeszközök, értékpapírok, vagyontárgyak, információk, adatok, személyzet) állnak, amelyeket az értékek környezetét alkotó rendszerelemek vesznek körül. A fenyegetések, támadások a rendszerelemekre közvetlenül hatnak és az ezeken megvalósított védelem által realizált védelmi képességektől függően veszélyeztetett a védendő érték. A kockázat mértékét az egy időtávon belül felmerült fenyegetések gyakorisága és a védendő érték által hordozott kárérték szorzata határozza meg. Adott kockázati szinten a védelem erőssége szabja meg a fenyegetések "sikerességének" valószínűségét és az ezek során okozott kár összegét. Mivel a "sikeres" fenyegetések, támadások valószínűségét gyakorlatilag nem lehet nullára csökkenteni, minden szervezetnek meg kell határoznia azt a minimális kockázati értéket, azaz egy adott időtávra vetített kárösszeget, amelyet még el tud viselni, és ez határozza meg a szükséges védelmi szintet.

A kockázat meghatározása:

$$r = \sum_{t \in T} \left(p_t \times d_t \right),$$

ahol: **r**: a rendszer biztonsági kockázata [pl.: Ft/év],

T: a releváns fenyegetések halmaza,

$\mathbf{p_t}$: egy adott fenyegetés bekövetkezésének valószínűsége [pl.: 1/év],

$\mathbf{d_t}$: egy adott fenyegetés bekövetkezéséből származó kár [pl.: Ft]. [6]

A fenti modellre azért esett a választás más, sztochasztikus vagy determinisztikus kockázati modellekhez viszonyított pontatlansága ellenére a kvalitatív kockázatelemzéseknél[1] a gyakorlatban nagyon jól felhasználható. A vizsgálati módszer lépései azt célozzák meg, hogy végül hozzá lehessen rendelni minden rendszerelemhez a releváns fenyegetéseket, azok gyakoriságát és a védendő értékre jellemző és a vele funkcionális kapcsolatban levő rendszerelemekre vetített kárértéket. Az elviselhető kockázati határ ismeretében minden releváns fenyegetésre és minden felmért rendszerelemre már minősíthetők a kockázatok.

Ezek alapján a teljes vizsgálat elvégzése során a következő lépések [5] szerint érdemes haladni:

1. lépés: Tényhelyzet felmérés:
   - a védendő értékek meghatározása,
   - a védelmi igények és célok megfogalmazása,
   - a kárérték-osztályok meghatározása, kárértékek hozzárendelése a védendő értékekhez.
2. lépés: Fenyegetettség elemzés:
   - a veszélyeztetett rendszerelemek feltérképezése,
   - az alapfenyegetettségek és a rendszerelemek.
3. lépés: A fenyegető tényezők meghatározása:
   - gyenge pontok meghatározása a rendszerelemek területén,
   - a fenyegető tényezők meghatározása rendszerelem csoportonként,
   - rendszerelem-alapfenyegetés-fenyegető tényező összerendelés.

[1] Összetett rendszerek biztonsági kockázatainak vizsgálatához általában a kvalitatív kockázatelemzés kielégítő eredményt ad. Amennyiben kvantitatív kockázatelemzést kell végezni, a kockázat fenti definíciója – pontatlansága miatt – nem alkalmazható!

4. lépés: Kockázatelemzés:
   - kárértékek átvitele a rendszerelemekre,
   - a bekövetkezési gyakoriságok meghatározása,
   - a fenyegető tényezők és a bekövetkezési gyakoriságok összerendelése,
   - kockázati mátrix meghatározás,
   - kockázat minősítés a kockázati mátrix alapján.
5. lépés: Kockázat-kezelés:
   - a "nem elviselhető" minősítésű kockázati sorok összegyűjtése,
   - intézkedési javaslatok,
   - költségbecslés,
   - megvalósítás ütemezés, prioritások.

A fenti lépések szerint haladva egyrészt pontos képet kaphatunk egy pénzintézet biztonsági szempontok szerinti helyzetét illetően, valamint hatékony, széleskörű kockázatelemzést végezhetünk.

TÉNYHELYZETFELMÉRÉS

A vizsgálat során a bankbiztonság teljes körű vizsgálatát végezzük el, ehhez kapcsolódóan át kell tekintenünk a banknál megvalósuló alapfolyamatokat, a működés módját és a szabályozottságot, a szervezeti egységeket és azok tevékenységeit, bizonyos értelemben azokra szűkítve, amelyek a bankbiztonság szempontjából legfontosabb folyamatokat realizálják. Így behatárolhatóvá válnak azok az értékek, amelyek a bank folyamataiban meghatározók és így a bankbiztonság szempontjából érzékenyek.

A védendő alapértékek ez alapján meghatározhatóak és alapvetően három csoportba sorolhatók:

- fizetőeszközök, értékpapírok és vagyontárgyak,
- információk,
- személyek.

A védelmi célok feltérképezése, védelmi igények meghatározásához először is célszerű definiálni magának a biztonságnak a fogalmát. A biztonság értelmét, tartalmát sokan sokféleképpen magyarázzák. Elfogadva, hogy a biztonság egy *kedvező állapot*, amellyel szemben elvárható, hogy a fenyegetések bekövetkezésének lehetősége, valamint az esetlegesen bekövetkező fenyegetés által okozott kár a lehető legkisebb legyen. Ahhoz azonban, hogy teljes legyen ez a biztonság az szükséges, hogy minden valós fenyegetésre valamilyen védelmet nyújtson, ugyanakkor körkörös legyen, vagyis minden támadható ponton biztosítson valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy folyamatosan létezzen. [7]

A fentiek alapján *a biztonság a rendszer olyan – az érintett*[2] *számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.* Ahol a *zárt védelem* az összes releváns fenyegetést figyelembe vevő védelmet, a *teljes körű védelem,* pedig a rendszer valamennyi elemére kiterjedő védelmi intézkedések összességét jelenti. A *folytonos védelem* az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg. A *kockázattal arányos védelem* esetén egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel, azaz a védelemre akkora összeget és oly módon fordítanak, hogy ezzel a kockázat az érintett számára még elviselhető, vagy annál kisebb. [7]

[2] Az *érintett* alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő.

„A védelem akkor kielégítő erősségű (mértékű), ha a védelemre akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a releváns fenyegetésekből eredő kockázat (kárérték × bekövetkezési gyakoriság) a szervezet számára még elviselhető szintű vagy annál kisebb.” [8]

Hangsúlyozzuk, hogy a védelemre fordított költségeknek nemcsak az összege, hanem a ráfordítás módja is lényeges, azaz a védelmet teljes körűen és zártan kell kialakítani. A ráfordítás mértékét az elviselhető kockázat mértéke szabja meg, amelyet a kárérték és a bekövetkezési gyakoriság alapján meghatározott elviselhetőségi határ determinál. Ezt a határt minden szervezetnek egyedileg kell meghatároznia.

Egy szervezet biztonsági auditjának végső célja azon értékek biztonságának értékelése, amelyek egyéb veszélyeztetés tárgyai, illetve birtoklása a potenciális támadók célja és védelmük a tulajdonos alapvető érdeke. Minden esetben – így egy bank esetében is – vizsgálni kell, hogy milyen objektumok, milyen szempontból és milyen szinten képviselnek értéket a tulajdonos számára. A védelmi igények könnyebb meghatározása céljából ezt először általános szinten fogalmaztuk meg.

A hagyományos bankbiztonság szempontjából a védelmi célokat alapvetően két területen, az értékek tulajdonlása és a működőképesség területein fogalmaztuk meg, ezek sérülését vagy elvesztését tekinthetjük alapfenyegetettségeknek. Az értékek tulajdonlása területén az értékek a bank számára való tulajdonlásának, kezelésének, felhasználhatóságának biztosítását, a működőképesség területén az értékek rendelkezésre állásának és funkcionalitásának a biztosítását határozzuk meg alapvető védelmi célként.

A védelmi igények, azaz a szükséges védelmi szintek általános megfogalmazásához a megismert funkcionális folyamatok és működési mód alapján vizsgáltuk a védendő értékek és rendszerelemek természetét, tulajdonságait az alapfenyegetettségek szempontjából.

Ha az előzőekben megjelölt általános védelmi célok nem valósulnak meg, az adott bankot károk érhetik. Az audit során a károk tipizálását a következő területekre csoportosíthatjuk:

- közvetlen anyagi kár,
- közvetett anyagi kár,
- társadalmi, gazdasági-politikai jellegű károk,
- titok és adatvédelmi jogszabályok, előírások megsértése,
- személyi sérüléssel járó károk.

FENYEGETETTSÉG-ELEMZÉS

A védelmi igények feltárásakor egy pénzintézet objektumainak, illetve pénzintézeti tevékenységének és az ezekhez kapcsolódó értékek veszélyeztetettségét elemezzük és értékeljük.

A fenyegetettség elemzés során:

- feltérképezzük a veszélyeztetett rendszerelemeket,
- feltárjuk a védendő értékek és a rendszerelemek közötti függőségeket, amelyek segítségével megítélhetők a fenyegetések hatásmechanizmusai,
- meghatározzuk a rendszerelemek azon gyenge pontjait, amelyeken keresztül a fenyegetettségekből származó potenciális károkozás esélye magasabb szinten valószínűsíthető,
- feltérképezzük a rendszerelemekre ható fenyegető tényezőket.

Így megítélhető a rendszerelemekre és az értékekre ható fenyegetettségi kép, amely a rendszerelemekre – különösen azok gyenge pontjain át– a releváns fenyegetéseket foglalja magába.

A fenyegetett rendszerelemek feltárása során az értékek fenyegetettségének megítéléséhez a banki tevékenység és annak környezete minden olyan elemét figyelembe kell venni, amelyek valamilyen módon az értékekkel kapcsolatban vannak. Ezeket a továbbiakban rendszerelmeknek nevezzük. Ezeken keresztül az értékekre ható fenyegetések feltérképezéséhez kiinduló pont valamennyi olyan rendszerelem feltérképezése, amely valamilyen potenciális veszélynek van kitéve. A pénzintézeti biztonság szempontjából a veszélyeztetett rendszerelemek a következők:

- épület,
- közvetlen/támogató infrastruktúra (villamos és energetikai rendszerek, informatikai és távközlési hálózatok, raktárak, víz, csatorna, stb.),[9]
- banki tulajdonú berendezések, eszközök,
- készpénz és értékpapír tároló, feldolgozó helyiségek,
- vagyonvédelmi rendszerek,
- dokumentumok és dokumentáció,
- személyzet.

A bank biztonságát – az üzleti biztonságon kívül – többféle megközelítésben lehet értelmezni. A bankbiztonságot meghatározza a bank – ide értve minden az értékkezelésben résztvevő egységét – közvetlen környezete, a helyiségcsoportok kialakítása, azok megközelíthetősége, funkcionalitása, a telepített behatolás jelző-, tűzjelző-rendszer, valamint a videó-megfigyelőrendszerek, a dolgozók kiválasztása, a belső szabályozások és azok végrehajtása és nem utolsósorban a mobilizálható értékek (készpénz, értékpapír) tárolása, feldolgozása, szállítása, körülményei.

Érdemes külön megemlíteni, hogy a személyek elemcsoportot három egymástól jól elkülöníthető alcsoportra lehet bontani, ezek:

- a bank ügyfelei,
- a bankkal szerződéses jogviszonyban álló szervezetek, cégek dolgozói,
- a bank állományában dolgozók.

A korábban ismertetett védelmi modell szerint a fenyegetések végső célpontját azok a védendő alapértékek képzik, amelyeket a vizsgált szervezettől és az auditálás tárgyától függően mindig konkrétan meg kell határozni. Egy pénzintézet esetén esetében a következő alap kategóriákat vesszük figyelembe, mint védendő értékeket:

- fizetőeszközök, értékpapírok és vagyontárgyak,
- személyek,
- információk.

A felsorolt csoportokra ható konkrét fenyegetéseket általánosítva az alapfenyegetések két kategóriáját, a tulajdonlás, illetve a működőképesség elvesztését határoztuk meg és minden védendő alapértékhez a két alapfenyegetettség szerint rendelünk kárértéket. Ez a kárérték hozzárendelés meghatározó a kockázatelemzés során, mert a védendő alapértéket "körülvevő" rendszerelemekre - amelyekre a fenyegetések valamilyen gyakorisággal közvetlenül hatnak - ezek a kárértékek kerülnek rávetítésre.

A védendő alapértékek fenti kategóriái közül néhányat további csoportokra bontottunk, mert azok kárértékei egyrészt egymáshoz képest, másrészt az alapfenyegetettségek szempontjából lényegesen is eltérhetnek egymástól.

Az értékpapírok és az értéktárgyak banki, illetve nem banki tulajdonú alcsoportokra történő bontását a biztosítottság mértékében levő lényeges különbség indokolja.

A banki tulajdonú ingatlanok esetében a tulajdonost nagyobb kár sújtja, így a bankra nézve értelemszerűen a banki tulajdonú ingatlanokat ért károk dominánsak.

A berendezések és banki eszközök, mint tulajdon is komoly kárértéket képviselnek, de a bank működőképessége szempontjából is meghatározó szerepük van.

A személyek, mint védendő alapérték kategóriával kapcsolatosan ki kell térnünk egy különleges fenyegetésre, nevezetesen amikor emberi élet kerül közvetlen veszélybe, pl. bankrablás esetén. Ennek a fenyegetésnek a kockázat kezelése, az ezzel kapcsolatos intézkedések kívül esnek annak a védelmi modellnek a hatókörén, amelyet az korábban röviden ismertettünk. Az emberi élet közvetlen veszélyeztetésének elhárítása jóval magasabb prioritású minden más fenyegetés elleni védelemhez képest. Ebben az esetben elsődleges cél az emberi élet megmentése, azaz legmagasabb anyagi és/vagy erkölcsi kárt is el kell szenvednie a banknak, ha ezáltal az arra irányuló közvetlen fenyegetés elhárítható. Erre az esetre - mint ezt a banki szabályzatok is rögzítik - minőségileg más megfontolások és intézkedések lépnek életbe.

Az információknak két csoportját alakíthatjuk ki jogszabályi megfontolások alapján. A banktitkot tartalmazó információk, amelyek az ügyfelekre vonatkoznak és a bank üzleti titkait tartalmazó információk, amelyek a bank saját védendő értéke. A személyes adatok, ha azok az ügyfélre vonatkoznak banktitkot (is) jelentenek, ha saját alkalmazottra, akkor az üzleti titok csoportjába sorolhatjuk (logikailag, csak itt, de nem jogilag).

Egy bank védendő alapértékeinek a felsorolását az alábbi táblázat tartalmazza, amely azt tükrözi, hogy ezen alapértékekhez milyen kárértéket rendelünk a tulajdonlás és a működőképesség elvesztése esetén. A kárértékek nagyságát egy többfokozatú értékskála-rendszerbe soroljuk be. Érdemes páros számot választani, hogy az értékelés során a szakértőket egyértelmű állásfoglalásra késztessük. A kárértékek megállapításakor a biztosítások kárcsökkentő hatását célszerű figyelembe venni.

Sor-szám	Az alapérték megjelölése	a tulajdonlás	a működő-képesség
		értéke	
	készpénz és készpénz-helyettesítő fizetőeszközök		
	a bank tulajdonát képző értékpapírok		
	nem a bank tulajdonát képző értékpapírok		
	a bank tulajdonát képző ingatlanok (fiókok)		
	berendezések, banki eszközök		
	banktitkot képző adatok, információk		
	a bank üzleti titkát képző adatok, információk		

1. táblázat. Kárérték megállapításához alkalmazandó táblázat (készült az [5] alapján)

A FENYEGETŐ TÉNYEZŐK MEGHATÁROZÁSA

A védendő alapértékek alapfenyegetettségeihez kapcsolódó kockázatok megítéléséhez meg kell határozni az egyes rendszerelemekre, illetve elemcsoportra ható fenyegető tényezőket. A fenyegető tényezők legnagyobb valószínűséggel a rendszer gyenge pontjain keresztül tudnak érvényesülni. Az adott rendszerelemhez kapcsolódó kár kockázati tényezője így lesz reálisan megítélhető.

Egy bank biztonsági szempontból értelmezett gyenge pontjai a rendszerelemeket veszélyeztető károk fellépési valószínűségét növelik, illetve a védelmi intézkedések csökkentik.

Globálisan a fenyegetések három szintjét különböztetjük meg:

- gondatlan károkozás,
- szándékos, előre megfontolt, de egyedi károkozás,
- szervezett bűnözés (amely a szándékosan elkövetett bűncselekmények közül a legveszélyesebbnek tekintett).

Jelenleg elmondható, hogy mindhárom fenyegetés típus reális veszélyt jelent, mert – amint tapasztalható – a szervezett bűnözés is megjelent a hazai bankrendszerben. Ez a fenyegetési szint egy későbbi időszakban, a gazdasági és a pénzügyi élet egy magasabb fokán, illetve a szervezett bűnözés "magasabb intelligencia" szintjén fokozódni fog. Ezt a körülményt azért nem szabad lebecsülni, mert a szervezett bűnözés, mint professzionális támadó ellen minőségileg jóval magasabb szintű védelmet kell biztosítani, mint az első két típusú fenyegetés esetében.

KOCKÁZATELEMZÉS

A biztonsági vizsgálat eddigi lépései során a helyi sajátosságok figyelembevételével felmérésre kerülnek a védendő értékek a tulajdonlás, illetve a működőképesség elvesztése szempontjából. Megbecsüljük mind a két alapfenyegetettség szempontjából a hozzájuk kapcsolható kárértékeket. A fenyegetések közvetlenül a védendő értékeket "körülvevő" rendszerelemekre hatnak, ezért az alapértékekre becsült kárértékeket – mindkét alapfenyegetést sorba véve – rávetítjük a rendszerelemekre. Ezen értékek közül a legrelevánsabb alapfenyegetéshez tartozó kárértéket vesszük majd figyelembe az adott rendszerelemre ható fenyegetés által okozott kockázat meghatározásához.

Mint az előzőekben említettük a konkrét fenyegetések a rendszerelemekre hatnak, így a védelmi intézkedésekkel is elsősorban ezeket kell megcéloznunk. Rendszerelemnek nevezünk a rendszer vagy annak környezetét képző minden olyan elemet, amely valamilyen kapcsolatban (fizikai, logikai, funkcionális, szervezeti, stb.) van a védendő alapértékekkel. A védelem teljes körűségét és zártságát az biztosítja, hogy minden ilyen lehetséges rendszerelemet és az ezekre ható fenyegetéseket figyelembe vesszük és értékeljük. A mechanikai védelem eszközeit, az azokat magába foglaló rendszerelemmel együtt értékeljük.

A kárértékek meghatározásánál a meglévő biztosításokat nem vesszük figyelembe, mert bár jelentős kárcsökkentő hatása van a szervezetre nézve, a tulajdonos szempontjából ez nem egyértelmű a biztosítótársaságban való érdekeltsége miatt.

Egy adott fenyegetésnek egy rendszerelemre adódó kockázatát a rendszerelemre átvitt releváns kárérték és a káresemény becsült gyakorisága szorzata adja.

A rendszerelemekhez rendelve egyedileg határozhatóak meg azok a fenyegető tényezők, amelyek a vizsgált környezetben egyáltalán felléphetnek. Mivel valamennyi lehetséges fenyegető tényező ellen nem lehet tökéletes védelmet kialakítani, ezért ki kell választani a legfontosabb, azaz a bank működése szempontjából a legnagyobb kockázatot jelentő fenyegető tényezőket. Ehhez valamennyi feltárt fenyegető tényezőt értékelni kell. Az értékelés függ a fenyegetés valóra válása esetén, a lehetséges kár nagyságától és a kár bekövetkezésének várható valószínűségétől (gyakoriságától) – a kettő együttes értéke a kockázat.

A kárnagyság értékelésekor mérlegeljük, hogy az adott fenyegető tényező hatására milyen anyagi vagy más természetű károk következnek be, amelyek az ún. közvetlen károk és milyen későbbi következményekkel, úgynevezett következményes károkkal kell számolni.

A bekövetkezés várható gyakoriságára statisztikák, különösen a bűnügyi statisztikát, továbbá a műszaki hibák, a személyek akaratlan hibás tevékenysége miatt vagy vis maior esetek által bekövetkező károk gyakoriságának meghatározását a vonatkozó statisztikák alapján kell elvégezni. Nagyon fontos azonban a statisztikák használatakor annak vizsgálata, hogy azt ki, mikor és milyen célból készítette, mert a statisztikákat nem szabad kritika nélkül alkalmazni. Jelentős gondot okoz, hogy a statisztikai adatok mindig tartalmaznak bizonytalanságokat is.

A következő lépésben elvégzendő kockázat minősítéshez szükséges a releváns kárértékek és a gyakoriságok osztályai alapján adódó kockázati mátrixban annak a határvonalnak a meghatározása, amely felett a kárérték-gyakoriság értékpárokhoz tartozó kockázatot NEM ELVISELHETŐ-nek, az alatta levőket pedig ELVISELHETŐ-nek minősítjük. E határ-vonal megállapítását az adott szervezetre jellemző adatkategóriáknak, a hozzájuk tartozó kár-értékeknek és káresemény gyakoriságoknak az interjúk és az átadott dokumentumok elemzése határozza meg. E minősítés lesz az alapja a későbbiekben kiválasztandó védelmi intézkedésekre vonatkozó javaslatoknak.

A NEM ELVISELHETŐ kockázatok határát azon a becsült szinten, ahol a lehetséges kárnagyság, vagy a közvetett erkölcsi, politikai károk a bankok funkcionális működését egészében és alapvetően veszélyeztetik.

Minden korábban ismertetett fenyegető tényezőhöz a már felsorolt gyenge pontok súlyozott figyelembevételével külön-külön meghatároztuk, hogy a legnagyobb kár bekövetkezésével melyik alapfenyegetettség, mely rendszerelemen keresztül fenyeget és ez mekkora kárértéket (releváns kárérték) képvisel. Ezután táblázatos formában célszerű minden fenyegetéshez párosítottuk a rendszerelemet, amelyre az hat, a legjellemzőbb alapfenyegetést, a kockázat szintjét meghatározó releváns kárérték/káresemény gyakoriság számpárt valamint ezek figyelembevételével a kockázati mátrix (2. táblázat) alapján meghatározott kockázati minősítést (3. táblázat).

K	4^+	**E**	**N**	**N**	**N**	**N**	**N**
Á	4	**E**	**N**	**N**	**N**	**N**	**N**
R	3	**E**	**E**	**N**	**N**	**N**	**N**
É	2	**E**	**E**	**E**	**N**	**N**	**N**
R	1	**E**	**E**	**E**	**E**	**E**	**N**
T	0	**E**	**E**	**E**	**E**	**E**	**E**
É	-	**E**	**E**	**E**	**E**	**E**	**E**
K		0^-	0	1	2	3	4
GYAKORISÁGI ÉRTÉK							

2. táblázat. Kockázati mátrix (készült az [5] alapján)

A fenyegető tényező megnevezése	Az alap-fenyegetettség (… elvesztése)	A fenyegetett rendszerelem	Kárérték	Gy. érték	KOCKÁZAT

3. táblázat. Fenyegető tényezők kockázatának meghatározása táblázat (készült az [5] alapján)

KOCKÁZAT-KEZELÉS

A kockázat-kezelés során hozott intézkedések a kárnagyságot vagy a kárgyakoriságot csökkenthetik, és olyan hatásúaknak kell lenniük, hogy a NEM ELVISELHETŐ minősítésű kockázatok ELVISELHETŐ-vé mérséklődjenek. Az intézkedések alapvetően a rendszerelemek biztonsági jellemzőinek javítására irányulnak, de hatásuk a környezeti kapcsolódások miatt szélesebb területre terjed ki, olyan mértékben, hogy a védelem teljes körű és zárt legyen. Az intézkedések kiválasztásánál figyelembe vesszük azok kölcsönös, szinergikus hatásait. Az intézkedések megfogalmazását követően fontos a felelős személyek és tartható határidők megjelölése valamint a vizsgált területeket érintő változás esetén, illetve rendszeres időközönként történő felülvizsgálat elvégzése.

A CSOPORTMUNKA JELENTŐSÉGE A VIZSGÁLAT SORÁN

A biztonsági vizsgálat során célszerű csoportmunkában dolgozni, a hatékonyság érdekében. A csoport tagjainak kiválasztása során célszerű figyelembe venni a vizsgált terület összetettségét és minden érintett téma megfelelő szakértelemmel rendelkező képviselőjét bevonni a munkába. A megfelelő hatékonyság érdekében a csoportmunkában résztvevők száma célszerű, hogy 6-10 fő között legyen.

Mivel a munka során a csoport végzi az értékelést, elkerülhetetlen, hogy az „emberi” tényező nagy szerepet játszik az eredményben. A csoport segítségével azonban a szélsőséges vélemények megjelenésekor is ki lehet alakítani egy ésszerű kompromisszumot.

A csoporttagok a munka során a problémafeltárás és megoldás mellett számszerűsíthető értékeléseket is végeznek. Ebben az esetben számolnunk kell a csoportban működő különböző pszichológiai hatásokkal is (pl.: konformitás).[10] Mégis a munka során meghatározott értékek az amellett, hogy a csoport véleményét képviselik, segítenek a szubjektív álláspontokat közelíteni egymáshoz egy „átlag” meghatározásával. Így a szubjektív véleményekből egy kvázi objektív eredményre juthatunk. Persze a csoportösszetétel meghatározó a vizsgálat eredményét, eredményességét illetően.

ÖSSZEFOGLALÁS

A cikkben ismertettünk egy a pénzintézetek esetében jól alkalmazható kockázatelemzési módszertant, amelynek alkalmazása során vizsgálatra kerül a biztonsági rendszer zártsága, teljes körűsége és kockázattal arányos kiépítettsége, valamint a külső és a belső szabályozásoknak való megfelelés egyaránt.

A vizsgálat egy informatikai biztonsági kockázatelemzési módszertanon alapul, de ez a módszertan, mint a fentiekben is látható – megfelelő átalakításokkal – alkalmazható a pénzintézetek biztonságának vizsgálatára is. Bemutattuk, hogy e módszertan lépéseinek alkalmazása során csak a vizsgálat tárgyát kell megfelelően megváltoztatni ahhoz, hogy más (biztonsági) kockázatok elemzésére is alkalmas legyen.

A módszertannal szinkronban a pénzintézet biztonsági rendszere jelenlegi helyzetének felmérése után nemcsak a releváns fenyegetéseket és a védelmi rendszer gyenge pontjait kell vizsgálni, hanem a bank minden védendő alapértékére és az azt körülvevő rendszerelemekre vonatkozó kockázatokat is elemezni és minősíteni kell. Ez képezheti a szükséges biztonsági intézkedések kidolgozásának alapját.

Felhasznált irodalom

[1] The CCTA Risk Analysis and Management Method (CRAMM) User Guide, UK Government Central Computer and Telecommunications Agency (CCTA), IT Security and Privacy Group, 1993.

[2] BS IEC61882:2002 Hazard and operability studies (HAZOP studies) - Application Guide, British Standards Institution, 2002.

[3] MIL–HDBK–338B - Electronic Reliability Design Handbook : Fault Tree Analysis, Department of Defense (USA), 1998.

[4] MIL-STD-1629A - Procedures for performing a failure mode effect and criticality analysis, Department of Defense (USA), 1980.

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

[6] Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna: A KIB 25. számú ajánlása: 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió, Miniszterelnöki Hivatal, 2008.

[7] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana: Az információbiztonság egy lehetséges taxonómiája, Bolyai Szemle XVII:4 (2008), 137-156.

[8] Bodlaki Ákos, Csernay Andor, Mátyás Péter, Muha Lajos, Papp György, Vadász Dezső: Informatikai rendszerek biztonsági követelményei, Miniszterelnöki Hivatal, 1996.

[9] Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren, HM Kommunikációs Szolgáltató Kht. – Zrínyi Kiadó, 2005.

[10] Tóth László: Pszichológia a tanításban, Pedellus Tankönyvkiadó, 2004.