Az informatikai kockázatok elemzése

Dr. Horváth Károly[*], Dr. Katona Péter[**]

2006. 03. 29.

Összefoglaló

Az információvédelmi irányítási rendszerek „de facto" általános szabványának tekinthető BS/7799 szabvány 2005 októberében ISO 27001 névvel nemzetközi szintre emelkedett. A szabvány hangsúlyosan foglalkozik az informatikai kockázatelemzés elvégzésének szükségességével. Emellett a hazai jogszabályi környezet a pénzügyi szektor számára 2006. január 1-jétől kezdődően már kötelező jelleggel írja elő az informatikai rendszer védelmét, és ezen belül a kockázatelemzés rendszeres elvégzését. Jelen cikkben az **informatikai kockázatelemzés gyakorlatias elvégzéséhez** kívánunk segítséget nyújtani.

Bevezetés

Az ISO 27001 szabvány ill. a pénzügyi szervezetekre vonatkozó törvény alkalmazásánál a legtöbb kérdés az informatikai rendszer kockázatelemzésével kapcsolatban vetődik fel. Mind a szabvány, mind a törvény megengedi a szervezethez illeszkedően a kockázat elemzési módszertan szabad megválasztását, bár a szabványban szerepel erre vonatkozóan némi megszorítás.

Az informatikai rendszerek biztonsága ellen ható veszélyek mára már annyira összetetteké váltak, hogy a kockázat elemzés **formális** módszerének az informatikai kockázatok elemzésére történő **általános** alkalmazása több komoly nehézségbe is ütközik. Az informatikai kockázatok elemzése – a vonatkozó törvényi előírásnak és a szabványnak is eleget téve – azonban elvégezhető a közvetlenül az informatikai védelmi intézkedésekre fókuszáló **direkt** módszerrel is, melynek segítségével, jóval kisebb ráfordítással könnyebben értelmezhető eredményt lehet elérni.

Az informatikai kockázatelemzés célja

Az informatikai kockázat elemzés elvégzése az informatikai rendszerek biztonságának kialakításában nyújt segítséget. Az informatikai kockázat elemzés **nem védelmi intézkedés**, elvégzése **önmagában nem erősíti a védelmet**, de **segítség** lehet ahhoz, hogy létrejöhessen egy biztonságos informatikai rendszer.

Az informatikai kockázatelemzés szerepe kettős. Feladata egyrészt, hogy feltárja azokat az informatikai sebezhetőségeket – gyenge pontokat –, amelyeken keresztül bizonyos esetekben sérülés érheti az informatikai rendszert – sérülhet az adatok bizalmassága, integritása és rendelkezésre állása –, és amely következtében üzleti kár érheti a szervezetet. Feladata továbbá meghatározni a feltárt kockázatok csökkentéséhez szükséges védelmi intézkedéseket. Ez utóbbit pedig **szervezet-specifikusan**, tömören és világosan kell meghatároznia, úgy, hogy a vállalat vezetése megértse azokat, és a védelmi intézkedések bevezetéséhez – azaz az informatikai védelem megteremtéséhez – a leghatékonyabb intézkedési tervet tudja elkészíteni.

A kockázatok elemzésének formális módszere

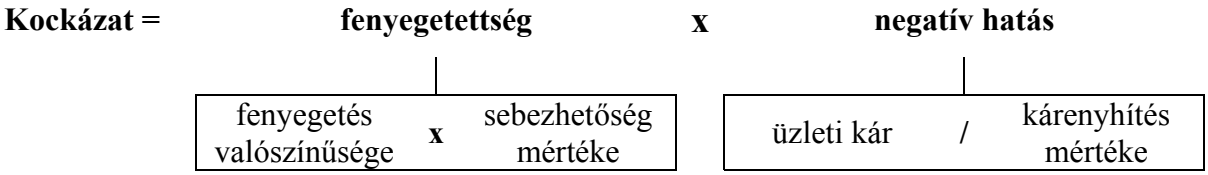
[*] okl. vill. mérnök, CISA, IRCA QMS Lead Auditor, a HOPET Informatika Kft. ügyvezető igazgatója
[**] okl. vill. mérnök, CISA, QMS és ISMS Lead Auditor, HOPET Kft., BVQI Hungary

A szervezet működését biztosító vagyonelemek **fenyegetéseknek** vannak kitéve, amelyek az egyes fenyegetésekre jellemző valószínűséggel különféle **káreseményeket** okozhatnak. A lehetséges káresemények egyfajta **fenyegetettséget** jelentenek a vagyonelemekre nézve, ahol a fenyegetettség mértéke nem csak a fenyegetés bekövetkezési valószínűségétől függ, hanem függ a vagyonelem **sebezhetőségétől**, azaz az adott eseménnyel szembeni védtelenségétől is.

Az adott esemény bekövetkezése **negatív hatást** vált ki, amelynek nagysága függ az **üzleti kár** értékétől, valamint a **kárenyhítés** mértékétől.

A valós **kockázat** mértékét a fenyegetettség és a negatív hatás szorzata adja meg.

Ábrában összefoglalva: egy **adott** fenyegetés által bekövetkezett **adott** esemény kockázata:



A kockázatelemzés formális módszere szerint meg kell határozni az egyes vagyonelemekre ható kockázati értékeket, és döntést kell hozni a még elviselhető kockázatok szintjéről. Az e szint feletti kockázatok esetében védelmi intézkedéseket kell bevezetni a kockázatok csökkentésére. A védelmi intézkedés figyelembevételével újból meg kell határozni a kockázat értékét, ez lesz a védelmi intézkedés bevezetését követően megmaradó ún. maradék kockázat.

A formális kockázatelemzési módszer kritikája
A fenyegetésekből kiinduló formális módszer elve könnyen megérthető, de alkalmazása az informatikai kockázatok elemzésére több szempontból is problematikus.

Az egyik – a kisebbik – probléma, hogy a módszer a kockázati tényezők **mérhetőségén** alapul, ami azonban a gyakorlatban nem áll fenn. Sem az informatikai fenyegetések valószínűségére, sem az informatikai rendszerek által okozott üzleti károk mértékére nem állnak rendelkezésre statisztikai adatok, így azokra csak nagyon megközelítő, **kvalitatív** elemzéseket lehet elvégezni. A sebezhetőség és a kárenyhítés mértéke is szubjektív értékelések eredményei, azokat a kvalitatív eredményekkel összevonva a kapott adatok megbízhatósága már igen csekély, az azokból származtatott kockázati érték megbízhatósága pedig még ezeknél is kisebb lesz.

Az eljárás elvégzése során mégsem ez okozza a legnagyobb nehézséget, mivel magának a kockázati értéknek viszonylag csekély a jelentősége – ez az intézkedési tervek prioritás értékeiben fog megjelenni csupán –, és így a kockázati érték meghatározása a kockázat elemzésnek **csak másodlagos** feladata.
Az **elsődleges** feladat, az elsődleges cél az – ahogy azt korábban már láttuk -, hogy az informatikai rendszer **valamennyi** gyenge pontját feltárjuk, és a hiányzó védelmi intézkedéseket hiánytalanul meghatározzuk.

Az eljárás igazi problematikája a káresetek számosságában rejlik. Az informatikai fenyegetések szinte végtelen számú különböző káreseményt idézhetnek elő, és ezeket szisztematikusan minden vagyonelemre vetítve meg kell vizsgálni. Továbbá, több fenyegetés is okozhatja ugyanazt a káreseményt, valamint ugyanaz a fenyegetés ugyanazt az eseményt

különböző módokon is előidézheti, és ezeket mind külön káreseményként kellene tekintenünk ahhoz, hogy az egyes események negatív hatását értékelni lehessen.

Sajnos az a viszonylag triviális egyszerűsítés sem használható, hogy az egyes vagyonelemeket csak a reájuk jellemző fenyegetések szempontjából vizsgáljuk, mert a vizsgálat ezen pontján ez egy önkényes előszelektálás lenne. Az események összevonása sem lehetséges, mert ekkor a káresemény meghatározása nem lesz egyértelmű, és emiatt sem a kárérték, sem a negatív hatás nem lesz meghatározható.
A formális kockázatelemzést elvégzését áttekinthetőbbé teheti, ha abban követjük az informatikai rendszerek felépítésének hierarchiáját, de a vizsgálandó esetek számát a gyakorlatban ez sem csökkenti jelentősen.

A formális kockázatelemzés elvégzését követően, a kockázatkezelési terv elkészítése során szintén a számosság problematikájába ütközünk. Az informatikai védelmi intézkedések túlnyomó többsége egyidejűleg ugyanis több káresemény kockázatát csökkentheti. Ezen felül a kockázatok csökkentésére általában több, alternatív védelmi intézkedés is létezik (pl. megelőző, kárenyhítő, esetleg áthárító jellegűek), amelyek használhatóságát csak **valamennyi fennálló kockázat értékelését követően** lehet eldönteni, iterációs módszerrel, ugyanis a kockázati események is függenek egymástól. A rendelkezésre állás biztosítására például megfelelő védelmi intézkedés lehet tartalék modulok tartása a helyszínen vagy külső helyszínen, de ha a géptermi tűz bekövetkezésére magas kockázatot állapít meg a vizsgálat, akkor a tartalék modulok helyszínen való tartása már nem lesz megfelelő védelmi intézkedés. Viszont mégis megfelelő lehet, ha üzembe helyezünk egy automata tűzérzékelő és -oltó rendszert, ami elviselhetővé teszi a tűzesetek bekövetkezésének a kockázatát.

Nem megoldott az ún. **általános** informatikai védelmi intézkedések kezelése sem. Ilyen pl. az adatbiztonsági politika megfogalmazása, a munkaköri leírások elkészítése, a dolgozói elkötelezettség biztosítása, az adatbiztonsági oktatások szükségessége stb. A formális módszertan logikája szerint a káresemények döntő többsége mellé ezeket is fel kellene venni védelmi intézkedésként, mivel ezek szükségességét is a fenyegetésekből, illetve a kockázatokból kell a módszertan szerint levezetni.

A formális kockázatelemzési módszertan általános informatikai alkalmazásának korlátai jól látszanak a vizsgálati jelentésben is. A vizsgálat eredményeképp – még egyszerű informatikai rendszer esetén is –, létrejöhet egy többszáz oldalas jelentés, amely szükségképpen megismétli az informatikai biztonsággal foglalkozó tankönyvekben ismertetett általános fenyegetéselemzési fejezeteket. Emellett a jelentés túlnyomó többségében olyan sebezhetőségekkel és kockázatokkal fog foglalkozni, amelyek a már érvényben lévő védelmi intézkedések miatt elhanyagolhatóak, valamint olyanokkal, amelyek még a menedzsment számára is nyilvánvalóan szóba sem jöhetnek az adott szervezetnél – pl. kimutatja, hogy nem szükséges egy hitelintézet esetében a géptermet elektromágneses árnyékolással ellátni –. Mindezek a menedzserek szemében is kérdésessé teszik **a vizsgálat módszerének megfelelőségét** és a kockázatfelmérést irányító tanácsadó **szakértelmét**.

Az informatikai kockázatok elemzésének direkt módszere
A formális módszernél lényegesen hatékonyabban végezhető el az informatikai kockázatok elemzése a **direkt módszer** alkalmazásával.

A direkt módszer a fenyegetések helyett közvetlenül a védelmi intézkedések halmazából indul ki, és a vizsgálat közvetlenül arra irányul, azt tárja fel, hogy ezek közül melyek azok, amelyek

a szervezetnél hiányoznak, de szükségesek lennének. Mivel a védelmi intézkedések száma véges – ráadásul a többségükben egyszerre több káresemény ellen is hatásosak –, ezért ezen az úton jóval kevesebb vizsgálatot kell elvégezni, azaz jóval egyszerűbb a végeredményhez eljutni.

A módszer kétfajta védelmi intézkedést különböztet meg: vannak olyanok, amelyek alkalmazása jogszabályi kötelezettség vagy a kialakult „legjobb gyakorlatok" és a kialakult nemzetközi szakmai vélemény szerint ma már szinte kötelezőek – ilyen pl. egy vírusvédelmi rendszer használata egy Internetre kapcsolódó hálózat esetén –, és vannak olyanok, amelyek alkalmazása a szervezet üzleti követelményei alapján mérlegelhető – ilyen lehet pl. a tartalék üzemeltetési helyszínen való tartalék rendszer létrehozása.

Az eljárás alkalmazása a védelmi intézkedések ellenőrzésén alapul.
A „kötelező" védelmi intézkedések keretében ellenőrzik azok meglétét és megfelelő működését, és amennyiben az intézkedés hiányzik, vagy nem az elvárt szinten működik, szakértői javaslat készül a védelmi intézkedés bevezetésére.
A szervezetre releváns, mérlegelhető védelmi intézkedések között a felkészítő tanácsadó irányításával hoznak szakmai döntést arról, hogy a védelmi intézkedés hiánya jelent-e sebezhetőséget, továbbá döntenek arról is, hogy a sebezhetőség jelent-e üzleti kockázatot a szervezetre nézve? A döntését a „legjobb gyakorlatok" ismeretében hozzák meg.
A feltárt sebezhetőségekre **és csak azokra** célszerű (ill. tanúsítás esetén a szabvány előírások miatt kötelező is) elvégezni a formális kockázatelemzést, melynek eredményei segítséget nyújtanak a kockázatkezelési terv kialakítása során meghozandó döntésekhez.

A védelmi intézkedések fontossága – prioritása – többnyire megegyezik a sebezhetőség kockázati értékével, de amennyiben a sebezhetőséghez kapcsolódóan több védelmi intézkedés bevezetése is javasolt, elegendő, ha csak az egyik védelmi intézkedés fontossága egyezik meg a kockázati értékkel. A többi védelmi intézkedés fontossági értékét a kialakult nemzetközi szakmai megítélés alapján kell meghatározni.

Az informatikai kockázatok elemzését általában olyan auditorok végzik, akik informatikai védelmi intézkedéseket, valamint ezek alkalmazásának a „legjobb gyakorlatát" szakértői szinten ismerik. Amennyiben azonban szükséges, a direkt módszer alkalmazásához felhasználhatók kidolgozott módszertanok. Számos nemzetközi ajánlás tartalmaz védelmi intézkedés-katalógusokat, amelyek szintén felhasználhatóak a vizsgálat elvégzése során. Ilyen pl. a német BSI[1], a magyar MSZ/ISO 17799 ajánlás, de ide érthetők az ISACA[2] Control Objectives és Audit Guidelines kiadványai is. A BSI ajánlás védelmi intézkedések katalógusában pl. az egyes informatikai alaprendszerek technikai kontrolljai is szerepelnek.

A direkt módszer alkalmazása

Az átvilágítás

A védelmi intézkedések oldaláról történő megközelítés legnagyobb érdeme, hogy közvetlenül a hiányzó védelmi intézkedések, a védelmi intézkedések hiánya által jelentett sebezhetőségekre – gyenge pontokra – koncentrál, A gyenge pontok feltárása, az átvilágítás elvégzése a kockázatelemzés első fázisának a feladata.

[1] Bundesamt für Sicherheit in der Informationstechnik: Baseline Protection Manual, 2004.
[2] Information Systems Audit and Control Association, az informatikai auditorok nemzetközi szervezete

Ahhoz, hogy a feltárás teljes körű legyen, minden tevékenységre kiterjedően **alaposan, részleteiben** kell átvilágítani a szervezet üzleti tevékenységét. Legegyszerűbb ezt üzleti folyamatokra bontva elvégezni, az egyes üzleti folyamatokat és a kiszolgáló informatikai rendszereket, valamint adatkapcsolataikat külön-külön vizsgálni. Az átvilágítás akkor lesz megfelelő, a **védendő vagyonelemek – az informatikai rendszerek, a rendszer elemek és a kiegészítő vagyonelemek –** feltárása akkor lesz teljes körű, a vizsgálat akkor fogja valamennyi sérülékenységet kimutatni, ha a munka ebben a szakaszában informatikai, adatbiztonsági valamint a szervezet üzleti folyamatait naprakészen ismerő helyi szaktudás együtt vesz részt a munkában. Így kerülhetnek csak napvilágra olyan nehezen feltárható, de kritikus gyenge pontok, mint pl., ha két informatikai rendszer között az operátor floppy-n visz át üzletileg szigorúan bizalmas osztályba sorolt adatokat, vagy ha pl. egy üzletileg kritikus alkalmazás önálló felhasználói hitelesítést valósít meg, de a jelszavakat nyíltan tárolja. Ha ezeket nem tárja föl a vizsgálat, akkor használata többet árt, mint használ, ugyanis **hamis biztonság tudatát** keltheti a menedzsmentben (a menedzsment azt hiszi, hogy a kockázat elemzés az informatikai rendszer valamennyi gyenge pontját felderítette).

Az átvilágítás során a sebezhetőségek későbbi értékeléséhez szükséges, hogy elvégezzük az üzleti hatáselemzést, melynek során az üzleti folyamatokból kiindulva meghatározzuk az elsődleges vagyonelemek, az informatikai rendszerek – szerver rendszerek, munkaállomások, hálózati rendszerek – védelmi követelményeit a bizalmasság, az integritás és a rendelkezésre állás vonatkozásában. A védelmi követelmények meghatározásához a „legjobb gyakorlatok" szerint elegendő egy 3-as fokozatú kvalitatív skála használata (alapszintű, fokozott, kiemelt).

Az átvilágítás elvégzését követően az üzleti folyamatokat, a környezetet, az informatikai működést és az alkalmazott védelmi intézkedéseket (a kontroll környezetet), valamint az üzleti folyamatok és az elsődleges vagyonelemek védelmi követelményeit dokumentálni kell. A dokumentum alapján ellenőrzi a menedzsment, hogy a szervezetre vonatkozó vizsgálati megállapítások helyesek-e, ez a dokumentum bizonyítja – a felügyeleti szervek előtt is – a vizsgálat alaposságát és teljeskörűségét.

A kockázatelemzési jelentés

A kockázatelemzés második fázisában készül el a kockázatelemzési jelentés. Feladata, hogy a menedzsment számára bemutassa a feltárt gyenge pontokat, és megindokolja a javasolt védelmi intézkedések bevezetésének fontosságát.

A kockázatelemzési jelentés – a jobb áttekinthetőség érdekében – csoportosítva[3] sorolja fel a **feltárt** észrevételeket – a sebezhetőségeket. A sebezhetőségek érzékeltetése a legjellemzőbb lehetséges káresemények bemutatásával, az üzleti kockázatot pedig a lehetséges negatív üzleti hatások – a szervezetet érő legjellemzőbb üzleti károk – bemutatásával érzékeltetik. Az üzleti kockázatokat kockázati érték megadásával hasonlítják össze, melyre elegendő egy 5-ös skálát használni.

A jelentés minden feltárt sebezhetőséghez megadja a bevezetésre javasolt védelmi intézkedést, illetve intézkedéseket. Ez utóbbi akkor fordul elő, ha az adott sebezhetőség kockázatának csökkentésére több védelmi intézkedés bevezetése is szükséges, vagy ha alternatív védelmi intézkedések léteznek (pl. a helyszínen tartalék-modulok vagy

[3] A csoportosítás bármely vonatkozó módszertan, ajánlás szerint elvégezhető.

melegtartalék szerver). A bevezetendő védelmi intézkedés fontosságának jellemzésére a fontossági érték szolgál, egy 5-fokozatú skála szerinti fontossági érték megadása elegendő.

A kockázatkezelési terv

A kockázatelemzés része a védelmi intézkedések megvalósítására készített intézkedési terv. A tervben a **fontossági értékek,** azaz a **prioritások** sorrendjében tüntetik fel a védelmi intézkedéseket. A terv tartalmazza az egyes védelmi intézkedések bevezetésének erőforrás szükségleteit is.
Ha a szervezet valamennyi intézkedés bevezetését azonnal meg tudja valósítani, azaz biztosítani tudja a szükséges erőforrásokat – belső munkatársak rendelkezésre állása, pénz, idő –, akkor a fontossági értéknek nincs jelentősége, nem használják fel. Amennyiben nem biztosítható a szükséges erőforrás, nincs elegendő anyagi fedezet, vagy a szervezet leterheltsége nem engedi meg az azonnali bevezetést, akkor a megvalósítást ütemezni kell. Az ütemezés során az egyes intézkedések bevezetésének a sorrendjét szinte azonos súllyal három tényező fogja meghatározni: a belső erőforrások lehetséges biztosítása, a fontossági érték, valamint az anyagi források rendelkezésre állása.

Teendők a kockázatelemzés időszakos felülvizsgálata során

A pénzügyi szektorban a jogszabályi előírások alapján legalább kétévente (a tanúsított információvédelmi irányítási rendszerrel rendelkező vállalatoknál évente) felül kell vizsgálni a szervezet informatikai kockázatelemzését. Az esedékes felülvizsgálat teendői már maguktól értetődőek: elő kell venni a korábbi kockázatelemzési jelentést, és a szervezet üzleti- és informatikai tevékenységét átvilágítva meg kell vizsgálni, hogy történt-e változás a korábbi vizsgálat óta. A megállapításokat dokumentálni kell. Amennyiben a szervezetnél – bármilyen formában – rendszeres informatikai biztonsági ellenőrzés megvalósul – pl. a belső ellenőrzés részeként vagy önálló belső audit formájában –, elegendő a változásokkal érintett területeket átvizsgálni, a működő védelmi intézkedéseket értékelni, illetve feltárni a hiányzó védelmi intézkedések által jelentett sebezhetőséget a korábban leírtaknak megfelelően.