Paper 16 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

A CRAMM módszer alkalmazásának kiterjesztése

Zs. Horváth[1] és I. Kocsis[2]

[1]Gépészeti és Biztonságtudományi Intézet, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest

[2]Kiemelt Vállalatok és Tudásgazdasági Főosztály, Nemzetgazdasági Minisztérium, Budapest

Kivonat. Az információbiztonsági kockázatok felmérésében elterjedt a CRAMM módszer alkalmazása. Ennek alapját olyan káresemények kockázatai képezik, amelyek a vállalat adataival kapcsolatban lévő vagyonelemek sebezhetőségeit kihasználó fenyegetések következtében lépnek fel, és a vállalat adatvagyona CIA-kritériumának sérülésén keresztüli okozhatnak károkat. Ennek a módszernek az értelmezése, kis általánosítással könnyen kiterjeszthető bármely folyamatalapú működési kockázat felmérésére is. Jelen előadásunkban bemutatjuk ennek a módszertani kiterjesztésnek a módját, és az így kapott módszer alkalmazási lehetőségeit az információbiztonsági és működési kockázatok integrált felmérésének és kezelésének lehetőségeire is. Bemutatjuk továbbá, hogy miképp lehet ezzel a módszerrel egyidejűleg megfelelni különböző szabványok szerinti irányítási rendszerek kockázatokkal kapcsolatos követelményeinek is.

Kulcsszavak: informatika; információbiztonság; kockázat; CRAMM módszer

1. Bevezetés

A vállalatok egyre nagyobb körben vezetnek be működésük támogatására tanúsítható irányítási rendszereket. A legtöbb vállalat a tanúsítható irányítási rendszerek kiépítését az ISO 9001 szerinti minőségirányítási rendszerrel kezdi, majd azt egészíti ki a működéséhez szükséges egyéb irányítási rendszerrel, amelyeket együtt már integrált irányítási rendszerként működtet.

Az információbiztonság jelentőségének a növekedésével észrevehetően nő az ISO/IEC 27001-es szabvány szerinti információbiztonsági irányítási rendszert használó vállalatok száma. Ezen vállalatoknál jellemző ily módon az integrált irányítási rendszer működése, amely egyszerre tartalmazza (legalább) az ISO 9001 szerinti minőségirányítási rendszert, valamint az ISO/IEC 27001 szerinti információbiztonsági irányítási rendszert is. [1]

Paper 16 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

Az információbiztonsági irányítási rendszer egy kockázatalapú irányítási rendszer, ami azt jelenti, hogy az irányítási rendszer a vállalat adatvagyonának információbiztonsági szempontú kockázatain keresztül határozza meg a szükséges védelmi intézkedéseket, majd az irányítási rendszer a vállalat folyamatait ezen intézkedések beépülésével és hatékony működtetésével menedzseli. Ezeknek a kockázatoknak a felmérésére az információbiztonsági szakmában elterjedt a CRAMM módszer elvének a használata. A minőségirányítási rendszer szabványa a legutolsó (2015. szeptemberi) kiadásakor bevezette a minőségirányításba a kockázatalapú megközelítést, és ezzel kockázatalapúvá tette a minőségirányítási rendszert is. [2] Meghatározta a kockázatok felmérésének és kezelésének a célját, valamint előírta – többek közt – a folyamatok menedzselése során a folyamatkockázatok menedzselését is. Ugyanakkor nem adott meg konkrét módszert a kockázatok felmérésére.

A gyakorlatban a vállalatok sokszor tehetetlenek, és nehezen találnak módszereket a minőségirányításhoz kapcsolódó – legtöbbször – működési kockázatainak felmérésére. A bevezetett megoldások jellemzően egyediek, esetlegesek. Az (ISO 9001 és ISO/IEC 27001 szerinti) integrált irányítási rendszert működtető vállalatoknál is megfigyelhető, hogy az információbiztonsági kockázatok felmérésére sokan használják a bevált CRAMM módszert, míg saját működési kockázataikat mindenféle más, attól eltérő elven és skálázással működő módszerekkel mérik fel. Ez számtalan problémát hordoz, de gondoljunk csak az egyik legfontosabbra: a különböző jellegű kockázatok értékelésének összemérhetetlenségére.

A továbbiakban bemutatjuk, hogy a CRAMM módszer alapelvét, és azt, hogy annak értelmezése és használata miként terjeszthető ki a működési kockázatok felmérése is.

2. A CRAMM módszer értelmezésének kiterjesztése

A kockázat és a kockázatfelmérés fogalmai

A kockázat fogalmának a használata sajnos különböző szakmákban nem egységes. Induljunk ki az általános kockázatok menedzselésére vonatkozó ISO szabványok alapdefiníciójából:

Kockázat: „A bizonytalanság hatása a célokra.” [3]

Ebben a definícióban minden szónak jelentősége van. A „**bizonytalanság**” kifejezi, hogy kockázatról mindig csak akkor lehet szó, amikor egy jövőbeli cselekvés vagy esemény kimenetele többféle is lehet, és nem tudhatjuk előre, hogy az mi lesz. Ez a lehetségesen különböző kimenetel pedig „**hatással**” lehet az általunk elérni kívánt

Paper 16 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

„**célokra**”. Ebből az is következik, hogyha a bizonytalan kimenetelű cselekvésnek vagy eseménynek nincs hatása a céljainkra, akkor az számunkra nem is jelent kockázatot.

A kockázat okát, azaz a kockázati eseményt kiváltó okot **kockázati forrás**nak vagy **kockázati tényező**nek hívjuk. A kockázati forrás vagy kockázati tényező tehát valamilyen esemény, cselekvés vagy annak elmulasztása lehet, amelynek bekövetkezése hatást gyakorol meghatározott céljainkra. Noha ez a hatás lehet pozitív vagy negatív is, a gyakorlatban legtöbbet a negatív kockázatokkal és az azok elleni védekezéssel foglalkoznak. A különböző jellegű biztonsági kockázatok tipikusan mind negatív kockázatok ellen védenek, és így azoknál a kockázatok kezelésének a célja valamely biztonság megsértéséből következő károk elkerülése vagy enyhítése. A továbbiakban mi is a negatív kockázatokkal, és ezen keresztül a kockázatok csökkentésének lehetőségeivel és módszereivel foglalkozunk.

A kockázatok menedzselésének életciklusa 3 fő lépésből áll, a kockázatok felméréséből, kezeléséből és felügyeletéből:

- A **kockázatok felmérése**: a kockázatok azonosításából, elemzéséből és értékeléséből áll, azaz jelenti azt a teljes folyamatot, amíg a lehetséges kockázati források és kockázati események meghatározásától kezdve elemezzük azok mibenlétét, jellemezzük azokat, alkalmas módszerrel számszerűsítjük azok bekövetkezési valószínűségét, majd meghatározzuk a kockázat lehetséges mértékét (a kockázati hatás nagyságát), és azt a kockázati kritériumokhoz (elfogadási kritériumokhoz) hasonlítva döntünk a kockázatok kezelésének szükségességéről.
- A **kockázatok kezelése**: a nem elfogadható mértékű kockázatok esetén intézkedések bevezetését jelenti általában a kockázat mértékének csökkentésére. Ezek az intézkedések nagyon sokrétűek lehetnek.
- A **kockázatok felügyelete**: maguknak a kockázatoknak és a kockázatok csökkentésére tett intézkedések hatékonyságának a folyamatos figyelemmel kísérését, és szükség esetén a kockázatok felmérésének és kezelésének megismétlését jelenti.

A kockázatok felmérésére egymástól nagyon eltérő jellegű és hatásmechanizmusú, különböző módszerek léteznek. Ezek egyike – az információbiztonság területén – a CRAMM módszer.

Paper 16 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

A CRAMM módszer vagy más néven a CRAMM[1] támadási modell [4]

A CRAMM támadási modell lényege, hogy a kockázatokat fenyegetések okozzák, amelyek kihasználják a sebezhetőségeket, aminek következtében biztonsági események következnek be, amelyek kárt okoznak vagyontárgyakban, és ennek hatása lesz a tulajdonosra nézve. Ez a megközelítés azt jelenti, hogy a biztonsági esemény bekövetkeztéhez három dolog szükséges:

- **cél**, amiben/amivel kárt lehet okozni,
- **sebezhetőség**, amin keresztül a fenyegetés kifejti a hatását (vagy amin keresztül a támadás megindítható), ez lehet magában a védelemben is, és
- maga a **fenyegetés**.

Hogyha ezt az információbiztonsági kockázatok vonatkozásában értelmezzük, akkor

- a **cél**, ami kárt jelent a vállalatnak, az az általa kezelt, feldolgozott illetve használt adatok biztonságának (azaz bizalmasságának, sértetlenségének illetve rendelkezésre állásának) sérülése vagy elvesztése által okozott kár;
- a **sebezhetőség** azoknak a vagyontárgyaknak (azaz eszközöknek, berendezéseknek, infrastruktúráknak, személyeknek illetve folyamatoknak) a sebezhetősége (működési hibája, hiányossága vagy gyenge védelme), amelyek az adatokat tárolják, kezelik, feldolgozzák, továbbítják, illetve védik;
- a **fenyegetések** azok az események vagy cselekvések (vagy azok elmaradása), amelyek a nevezett vagyontárgyakban – azok sebezhetőségeit kihasználva – kárt tudnak okozni, és amin keresztül az adatok illetve információk biztonságát veszélyeztetik.

Ezeknek az elveknek az értelmezésévek az információbiztonsági kockázatfelmérés lépései feltölthetők konkrét tartalommal. Az információbiztonsági kockázatok felmérésekor a lehetséges kockázatok meghatározása során célszerű a kockázatokat valamilyen logikai rendező elv (sorrend) szerint feltárni. Többféle rendező elv lehetséges. Az egyik, a gyakorlatban egyre inkább elterjedő módszer a vállalat folyamatainak vizsgálata, és a folyamatok mentén az ahhoz köthető lépések, adatok, eszközök, erőforrások – mint a vizsgálat alapját képező vagyontárgyak – vizsgálata, és azok mentén a sebezhetőségek, fenyegetések és lehetséges kockázatok összegyűjtése.

[1] A CRAMM támadási modell a Central Computer and Telecommunation Agency (Egyesült Királyság) által kidolgozott kockázatelemzési és kezelési módszertan. A mozaikszó a „CCTA Risk Analysis and Management Method” kezdőbetűiből adódik.

Paper 16 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

Az értelmezés kiterjesztése működési kockázatokra

Amikor a vállalatok működési kockázatait vizsgáljuk, akkor is a kockázatokat célszerű valamilyen logikai rendező elv szerint feltárni. A vállalatok jellemzően folyamatalapú működése mellet, és megfelelve az ISO 9001:2015 szabvány elvárásainak szinte adja magát a lehetőség, hogy itt is a kockázatok feltárását folyamatalapon végezzük el. Ha folyamatonként számba vesszük a lehetséges kockázati forrásokat és azok lehetséges kockázati eseményeit és hatásait, amelyek előfordulhatnak a folyamat lépéseihez, adataihoz, eszközeihez vagy egyéb erőforrásaihoz kötötten, akkor hirtelen analógiát fedezhetünk fel a CRAMM módszer alkalmazott lépéseiben. Ezek után gondoljunk abba bele, hogy

- a **kockázati forrás** nem más, mint valamely lehetséges esemény, cselekmény (vagy annak elmulasztása) – azaz mint lehetséges **fenyegetés** – bekövetkezése, ami
- azért tud bekövetkezni, mert valamely folyamatlépés, eszköz, erőforrás, stb. nem megfelelően működik vagy nem kellő a védelme az adott fenyegetéssel szemben, tehát **sebezhető,** mert az adott fenyegetés ki tudja használni, és emiatt
- a bekövetkező kockázati eseménynek hatása lesz valamely **cél**unkra (kárt okoz nekünk).

Ebből is látszik, hogy a CRAMM módszer alapelemei a folyamatalapú kockázatfelmérés során a kockázatfelmérés fogalmainak teljesen megfeleltethetőek. Az általános működési kockázatfelmérés során a CRAMM módszer tehát ugyanúgy használható. Az egyetlen lényegi különbséget talán az okozza, hogy míg a működési kockázatok meghatározásakor a kockázat hatását az eseti, tetszőlegesen meghatározott célhoz viszonyítva vizsgáljuk, addig az információbiztonsági kockázatok esetén ezt a hatást mindig valamilyen adat biztonságának sérülése következtében vizsgáljuk.

3. A CRAMM módszer kiterjesztésének használata

A CRAMM módszer értelmezése kiterjesztésének gyakorlati jelentőségét az adja, hogy ily módon egyazon kockázat-felmérési eljárásban együtt, egyszerre tudjuk felmérni az információbiztonsági és a működési kockázatokat. Ennek több előnye is van:

- Először is az együttes felméréssel időt és energiát, munkát spórolhatunk meg.
- A közös felmérés biztosítja, hogy ugyanazoknak a kockázati forrásoknak az elemzését egyszer végezzük csak, még ha különböző jellegű kárhatást – és így különböző jellegű kockázatokat – is okoznak, és így a különböző hatások azonos kockázati forráshoz köthető elemzései biztos azonosak és egységesek lesznek.

Paper 16 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

- A közös felmérésből adódik, hogy abban egyszer csináljuk meg a különböző kárjellegekhez tartozó kárhatások értékbecslését, és azt a teljes felmérés során – amibe mind az információbiztonsági, mind a működési kockázatok beletartoznak – egységesen használjuk. Ilyen formán automatikusan biztosított, hogy a különböző kockázatokhoz tartozó kockázati értékek meghatározása egységes alapelveken nyugszik, és a meghatározott kockázatok egymással összemérhetők lesznek.
- Az információbiztonsági kockázatok CRAMM módszer alapján történő felméréséhez léteznek informatikai támogató célprogramok, tool-ok. Ezek közül néhány már felkészített arra, hogy ne csak információbiztonsági kockázatokat, hanem egyidejűleg ugyanazzal a felméréssel működési kockázatokat is meghatározzon. Ilyen módon az integrált minőségirányítási és információbiztonsági irányítási rendszert is használó vállalatok a működési kockázatok kezeléséhez is használni tudják az információbiztonsági kockázatok kezelésére bevált és alkalmazott módszereket, eszközöket.

4. Összefoglalás

A CRAMM módszer elvének kiterjesztésével bemutattuk, hogy az az általános, folyamatalapú működési kockázatok felmérésére is használható. Ezzel a kiterjesztéssel azok a vállalatok, akik az információbiztonsági kockázatok felmérésében már használták a CRAMM módszert, most a minőségirányítási rendszerek kockázatainak immáron kötelezővé vált felmérése során is használhatják azt. Ily módon új kockázatokkal foglalkozó rendszer bevezetése nélkül, egyszerűen tudnak az integrált kockázatfelmérés és kezelés irányába továbblépni.

Hivatkozások

[1] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

[2] ISO 9001:2015 Quality management systems— Requirements

[3] ISO/IEC Guide 73:2002 Risk management — Vocabulary — Guidelines for use in standards

[4] Horváth, Zs.: *A kockázatmenedzsment információbiztonsági kérdései*, Minőség és Megbízhatóság, 2016/03. szám, p.148-155