DR. HORVÁTH ZSOLT LÁSZLÓ, egyetemi adjunktus, Óbudai Egyetem,
Kandó Kálmán Villamosmérnöki Kar

A kockázatmenedzsment információbiztonsági kérdései

Napjainkban a vállalatok életében egyre jelentősebb szerepet játszik az információbiztonság. Van ahol ezt külső követelmények (jogszabályok, szabványok, ügyfelek stb.) kényszerítik ki, de nagyon sok esetben ez belső kényszer, illetve szükségszerűség is. Az információbiztonság célirányos és hatékony kialakítása elképzelhetetlen az információbiztonsági kockázatok felmérése, és az új védelmi intézkedések bevezetésekor a kockázatarányosság figyelembe vétele nélkül. Így gyorsan felértékelődnek az információbiztonsági kockázatok felmérését és kezelését megvalósító, illetve támogató módszerek, eljárások. Jelen publikáció célja az információbiztonsági kockázatok felmérése és kezelése gyakorlati és alkalmazási alapelveinek bemutatása az ezzel foglalkozni kívánó szakemberek számára.

Az információbiztonság szükségessége

Mit is jelent tulajdonképpen az információ biztonsága? Sokak számára egyszerűen az adatok védelmét illetéktelenek általi megismeréstől, azaz a bizalmasságuk megőrzését. Az információbiztonsági szakmában ez azonban ennél sokkal többet jelent.

Az információk biztonsága fogalom alatt az információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítását értjük. Ez azt jelenti, hogy az információkhoz csak az férhet hozzá, aki arra jogosult, viszont annak mindig és sértetlenül, továbbá módosítatlanul álljon rendelkezésre a szükséges információ.

Miért fontos ezt így hangsúlyozni? Azért, mert a vállalatok működése jellemzően folyamatalapon szervezett, és a vállalati folyamatok egyik legfontosabb erőforrása az információ. A folyamatok a működésükhöz bemenő információkat használnak fel, kezelnek, és alakítanak át kimenő információkká. Hogyha a működésükhöz a bemenő információ nem áll rendelkezésre, vagy nem pontosan (vagyis hibásan) áll rendelkezésre, akkor a folyamatok nem tudnak működni vagy hibásan működnek. Ha a folyamatok működéséhez szükséges információszolgáltatás nem megfelelően működik, akkor az a folyamatok működésében problémát, a vállalat számára pedig kárt jelent. A másik oldalról nézve pedig az információk illetéktelenek általi hozzáférése, megismerése számos visszaélésre és károkozásra adhat lehetőséget. Összegezve tehát, minden vállalatnak a működése szempontjából alapvető üzleti érdeke a működéséhez szükséges információszolgáltatás folyamatosságának és megbízhatóságának a fenntartása valamint az információszivárgás megakadályozása, azaz az információi biztonságának a megőrzése.

Ezt felismerve az információbiztonság követelménye már bújtatva megjelenik a tanúsítható irányítási rendszerek Nemzetközi Szabványosítási Szervezet (ISO) által kiadott új rendszerszabványaiban is. Ezek az újonnan kiadott irányítási rendszerszabványok 2012 óta egységes struktúrával rendelkeznek, amelyet HLS-nek (High Level Structure) neveztek el. Ez a HLS biztosítja, hogy a különböző irányítási rendszerszabványok azonos témájú menedzsmentkövetelményei azonos módon és a szabványban azonos helyen jelenjenek meg, majd (esetlegesen) integrált irányítási rendszer kiépítésekor egységes kezelhetők legyenek. Ebben a struktúrában a 7.5.3 fejezetben a „dokumentált információk" felügyeletére követelményként jelenik meg annak biztosítása, *hogy a dokumentált információk elérhetők és alkalmasak legyenek a használathoz, ahol és amikor szükséges, valamint megfelelően védve legyenek (pl. bizalmasság elvesztésétől, helytelen használattól vagy sértetlenség elvesztésétől)*. Ez tulajdonképpen a vállalati működés során az összes szabályozó és igazoló, elektronikus és papíralapú dokumentumra kimondja a bizalmasság, sértetlenség és rendelkezésre állás követelményét!

Az információbiztonság fenntartásának követelményét nemcsak azoknak a vállalatoknak kell teljesíteniük, amelyek magukat az ISO/IEC 27001:2013 (MSZ ISO/IEC 27001:2014) szabvány szerinti információbiztonsági irányítási rendszert működtetnek, hanem minden olyan vállalatnak is, amelyek bármely más irányítási rendszert. Például a most nemrég életbe lépett ISO 9001:2015 (MSZ EN ISO 9001:2015) szabvány használatára átálló cégek most szembesülnek vagy hamarosan szembesülni fognak mind ezzel az új követelménnyel.

A kockázatmenedzsment információbiztonságának szükségessége

Az információbiztonság kialakítása költséges. Minél magasabb szintű biztonságot szeretnénk kiépíteni, az annál többe fog kerülni. Cserébe viszont az információbiztonság sérülése esetén kisebb kárt szenvedünk el. Célszerű tehát egy optimális munkapontot, biztonsági szintet megtalálni, ahol a bekerülési költségek és a lehetséges károk is még elfogadhatóak. Ennek az optimális információbiztonsági szintnek a meghatározásában, és ott a szükséges intézkedések kiválasztásában segít az információbiztonsági kockázatmenedzsment, mint módszertan és eljárás.

Az információbiztonsági kockázatok felmérése, kezelése majd folyamatos figyelemmel kísérése és aktualizálása – azaz az információbiztonsági kockázatok menedzselése – biztosítja azt, hogy a fenntartott információbiztonsági rendszer az információk biztonságának sérülése következtében fellépő károk ellen kellő védelmet nyújt, a lehetséges kockázatok mértéke egy elfogadható szint alatti.

Ehhez természetesen szükséges az információbiztonsági kockázatok menedzselésének folyamatát bevezetni és folyamatosan fenntartani. Az információbiztonsági kockázatok felmérését, kezelését és azok folyamatos figyelemmel kísérését sokféle módon is meg lehet valósítani. Bármely vállalat maga választhatja meg a saját viszonyaira a legjobb, legalkalmasabb, neki legjobban tetsző módszert. Azonban a módszertan kiválasztása és alkalmazása előtt célszerű megismerni az információbiztonsági kockázatok menedzselése életciklusára vonatkozó alapelveket és elvárásokat, amelyek sokat segíthetnek a konkrét alkalmazandó módszer kiválasztásában és testre szabásában. Ezeket a módszereket az ISO/IEC 27005 szabvány mutatja be, szemléletesen és magyarázatokkal kiegészítve. Jelen publikáció is ennek a szabványnak a szellemében mutatja be a kockázatmenedzsment alapelveit.

Kockázatmenedzsmenttel kapcsolatos fogalmak, alapelvek

Mielőtt azonban rátérnénk az információbiztonsági kockázatmenedzsment alapelveire, szükséges néhány általános kockázatmenedzsment-alapelvet tisztázni.

Egy vállalat életében egyszerre számos, különböző fajta kockázat van jelen, és ezek közül a gyakorlatban sok kockázattal kénytelen a vállalat egyidejűleg foglalkozni. Nagyon komoly problémákhoz vezethet, amikor egyazon vállalaton belül a különböző fajta kockázatok kezelésekor már magának a kockázat fogalmának és menedzselésének az értelmezése sem azonos. Ilyenkor az egyes kockázati területek egymással olyan mértékben nincsenek összhangban, hogy az nemcsak a vállalat összes kockázatai csökkentésére tett intézkedéseinek hatékonyságát kérdőjelezi meg, hanem az egyes kockázati területek önálló működési hatékonyságát, eredményességét is. Szükséges tehát egy egységes kockázati értelmezés, amihez mindegyik kockázati terület alapvetően tud illeszkedni.

Ilyen egységes kockázatmenedzsment alapelveket határozott meg az ISO 31000-es szabványcsoport, amelynek magyar nyelvű címei a következők:

- MSZ 13073:2014 Kockázatfelmérés és -kezelés. Szakszótár
- MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek
- MSZ EN 31010:2010 Kockázatkezelés. Kockázat-felmérési eljárások

A kockázatokról való egységes értelmezés érdekében bemutatjuk néhány alapfogalom meghatározását és értelmezését, amely megfelel az MSZ 13073:2014 szabványban adott meghatározásnak:

- **Kockázat** (Risk): „A bizonytalanság hatása a célokra.”
- **Kockázatfelmérés és -kezelés** (Risk Management): „Egy szervezet kockázatokkal kapcsolatos összehangolt irányítási és felügyeleti tevékenységei.”

– **Kockázatfelmérési és -kezelési keretrendszer** (Risk Management Framework): „Azon összetevők együttese, amelyek a szervezetben a kockázatfelmérés és -kezelés tervezéséhez, bevezetéséhez, monitoringjához és átvizsgálásához, valamint folyamatos fejlesztéséhez alapelveket és szervezeti kereteket adnak."
– **Kockázatfelmérés** (Risk Assessment): „A kockázatfelmérés folyamata magában foglalja a kockázatazonosítást, a kockázatelemzést és a kockázatértékelést."
– **Kockázatazonosítás** (Risk Identification): „Folyamat a kockázat elemeinek feltárására, felismerésére és leírására."
– **Kockázatelemzés** (Risk Analysis) „Folyamat, amely egyrészt a kockázat sajátosságának megértését, másrészt a kockázati szint meghatározását foglalja magában."
– **Kockázatértékelés** (Risk Evaluation) „Folyamat, amelyben a kockázatelemzés eredményének összevetése a kockázati kritériumokkal annak megállapítására, hogy az adott kockázat és/vagy annak nagysága elfogadható-e vagy elviselhető-e."
– **Kockázatkezelés** (Risk Treatment): „A kockázat hatásának módosítására irányuló folyamat."

Ebből a kockázat-terminológiából több dolog következik: Egyrészt az, hogy kockázatról mindig a jövő időben beszélünk, amikor egy esemény vagy cselekvés bekövetkezése nem ismert, és ezért annak lehetséges hatása is különböző lehet. Ha ugyanis egy ismert hiányosságnak vagy hibának következtében annak káros hatása előre tudhatóan bizonyosan bekövetkezik, akkor ott nem kockázatról, hanem ismert problémáról beszélünk. A kockázatnak a jövőbeli hatása lehet viszont jó is, nemcsak rossz. Általános értelmezésben tehát a kockázat bekövetkezése lehet pozitív hatással is, amit utána a vállalat kihasználni igyekszik és nem elkerülni.

A biztonsági rendszerek célja azonban mindig az adott témájú biztonsági események nyomán bekövetkező károk csökkenése, ezért ezekben az esetekben mindig a negatív kockázatok csökkentéséről beszélünk. Az információbiztonság esetén is a továbbiakban a kockázatok fogalma alatt negatív kockázatokat értünk.

Mind a hétköznapi szóhasználatban, mind számos kockázatokkal foglalkozó publikációkban is találkozhatunk a „kockázatkezelés" kifejezés **különböző értelmezésével.** Számos helyen egyidejűleg értik a kockázatkezelés fogalma alatt a kockázatokkal való összes tevékenység teljes életciklusát, azaz a kockázatmenedzsmentet is, valamint annak – a már feltárt kockázatok javítására tett intézkedések bevezetésére és használatára vonatkozó – egyetlen lépését is. Terminológiailag kimondottan veszélyes és rengeteg hibára és félreértésre ad alkalmat az, amikor ugyanazt a kifejezést használjuk egy egész folyamatciklusnak, valamint annak egy kiválasztott eleme azonítására is. Ezért javasoljuk egy egységes terminológia következetes használatát, amire a fenti nemzetközi szabvány egy általánosan elfogadott terminológiát nyújt.

A kockázatok menedzselésének általános folyamata

A legtöbb kockázatok felmérésével és kezelésével foglalkozó módszertanban fellelhető az életciklus (lásd 1. ábra):

1. ábra: A kockázatok felmérésének és kezelésének általános életciklusa

A kockázatok felmérésének és kezelésének általános életciklusa a következő lépéseket tartalmazza:

– **A kockázatok azonosítása**: annak verbális meghatározása, hogy milyen kockázati események következhetnek be, ami hatással van az általunk meghatározott célokra. A kockázati események meghatározásakor jellemezzük annak bekövetkezési mechanizmusát, valamint a lehetséges kárhatásokat is.
– **A kockázatok elemzése**: annak számszerűsítése vagy legalábbis becslése, hogy az egyes kockázati események mekkora koc-

kázati potenciált jelentenek a vállalat számára. A cél az, hogy az egyes kockázati események a vállalat szempontjából mért jelentőségük alapján egymással összehasonlíthatóak legyenek. Jellemzően a kockázati potenciált, mint kockázati értéket a bekövetkezési valószínűség mértékének és a hatás mértékének a kombinációjával mérik.

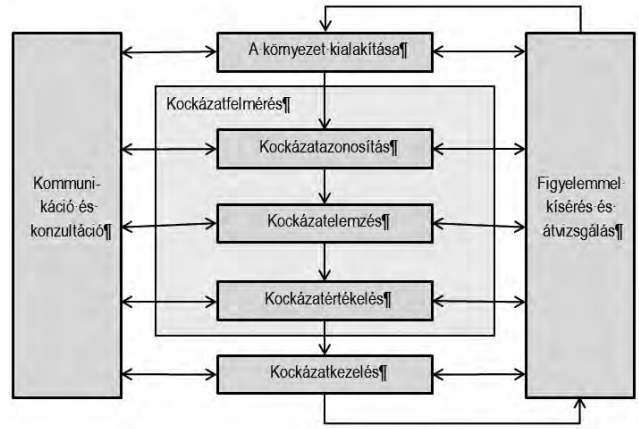
– **A kockázatok értékelése**: a már kockázati potenciálokkal meghatározott kockázati események elfogadását vagy intézkedési szükségesség meghatározását jelentik.
– **A kockázatok kezelése**: intézkedések bevezetése a nem elfogadható mértékű kockázatok esetén a kockázat csökkentése céljából. Ezek az intézkedések nagyon sokfélék lehetnek. Szükséges arra is felhívni a figyelmet, hogy egy új kockázatcsökkentő intézkedés sokszor a vállalati működésben okoz(hat) változásokat, ami maga is újabb kockázatok forrása lehet. Ilyen esetekben az új intézkedések bevezetésekor annak kockázati hatásait is ismételten fel kell mérni és szükség esetén kezelni.
– **A kockázatok felügyelete**: a feltárt kockázatok és a nem megengedhető mértékű kockázatok csökkentésére tett intézkedések működésének folyamatos megfigyelése, és szükség esetén a kockázatok felmérésének és kezelésének (teljes vagy részleges) megismétlése. Cél az, hogy a feltárt és kezelt kockázatok mindig az aktuális állapotnak feleljenek meg.

Az ***MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek*** c. szabvány általános keretet ad a vállalati kockázatfelmérési és -kezelési keretrendszer kialakításához, valamint az egyes kockázat-felmérési és kezelési folyamatok általános életciklusának kialakításához is.

A szabvány alapján a kockázatfelmérési és -kezelési folyamat alapelve megfelel az előbb bemutatott általános gondolatmenetnek (lásd a 2. ábrát), azonban néhány pontban kirészletezve egy sor további hasznos szakmai szempontot ad annak alkalmazásához.

A kockázatfelmérés és -kezelés egyes lépéseinek főbb szempontjai:

– **A környezet kialakítása**: jelenti a kockázatok felmérése és kezelése életciklus során az elérni kívánt célok meghatározását, valamint a következő kockázatfelmérési és -kezelési folyamatnak, az alkalmazott módszertannak, feltételrendszernek a részletes meghatározását.



2. ábra: A kockázatfelmérés és -kezelés általános folyamata (MSZ ISO 31000:2015)

A meghatározott módszertannak mindig illeszkednie kell a vállalati általános kockázatfelmérési és -kezelési keretrendszerhez. Itt kerülnek meghatározásra alapvetően a kockázatkezelési és -felmérési folyamattal kapcsolatosan a következők:

- célok,
- felelősségek és szerepek,
- erőforrás- és időkeretek,
- kapcsolatrendszer,
- módszerek,
- kockázatkritériumok,
- mérőszámok.

– **Kockázatazonosítás**: jelenti a kockázati események verbális meghatározását, amely tartalmazza a kiváltó (lehetséges) okok, mint kockázati források, valamint a lehetséges következmények minél szélesebb körű leírását. A kockázatazonosítás is annál részletesebb és pontosabb, minél nagyobb ismereti tapasztalatra tud támaszkodni.
– **Kockázatelemzés**: jelenti a kockázatok természetének megértésén keresztül a kockázati szint meghatározását.
Ez sokszor tapasztalatokon alapuló becsléssel történik. A kockázati szintet általában a bekövetkezési valószínűség és a következmény (általában kárérték) becsült mértékeinek szorzatával határozzák meg. (Természetesen vannak ettől eltérő módszerek is, de a legtöbb esetre általánosan ez a jellemző.)
– **Kockázatértékelés**: jelenti a kockázatelemzés eredménye alapján a kockázatkezelésről szóló döntéshozatal támogatását.

A kockázatelemzés során a kockázati eseményekhez becsült (vagy kiszámított) kockázati értékekhez, az előre meghatározott kockázati kritériumok alapján itt kell meghatározni, hogy az adott kockázati esemény elfogadható-e vagy sem, és annak alapján kell dönteni a kockázatkezelés szükségességéről illetve módjáról. A döntésben természetesen szerepet játszanak különböző szempontok, mint például a vállalat kockázatvállalási hajlandósága, a bevezetendő intézkedéssel várható előnyök, kapcsolódó jogszabályi elvárások, illetve lehetséges következmények stb.

– **Kockázatkezelés**: jelenti – a nem elfogadható mértékű kockázatok esetén – a kockázatok csökkentése[1] érdekében tett intézkedések bevezetését.

  Ez a lépés önmagában is tartalmaz egy intézkedés-bevezetési életciklust a következők szerint: a kockázatkezelési igény becslése, a maradványkockázat elfogadhatóságának meghatározása, kockázatkezelés megtervezése, kialakítása, végrehajtása és a hatékonyság visszacsatolása.

  Ismételten fel kell hívni a figyelmet, hogy a kockázatkezelési lehetőségek közül az alkalmazandó intézkedés kiválasztásakor figyelembe kell venni az adott intézkedéshez kapcsolódó új kockázatok lehetőségét, amelyet az adott intézkedés bevezetéséhez tartozó maradványkockázat meghatározásánál alapul kell venni.

  A kockázatkezelési intézkedések jellegüket tekintve többfélék lehetnek, amelyek a következő kategóriákba sorolhatóak:
  - kockázat elkerülése,
  - kockázat vállalása vagy növelése,
  - kockázati forrás eltávolítása,
  - bekövetkezési valószínűség megváltoztatása,
  - következmények változtatása,
  - kockázat megosztása, áthárítása,
  - kockázat megtartása.

– **A kockázat figyelemmel kísérése és átvizsgálása** jelenti a kockázatmenedzsment során a rendszeres ellenőrzési és felügyeleti tevékenységek elvégzését.

  A kockázatok figyelemmel kísérési és átvizsgálási tevékenységeinek a célja a kockázat-kézbentartások hatékonyságának és hatásosságának biztosítása. Ennek érdekében a teljes kockázat-felmérési és kezelési életciklus alatt a következő tevékenységek ajánlottak:
  - folyamatos monitoring,
  - időszakos és ad-hoc felülvizsgálatok,
  - tapasztalatok levonása (normál működés, változások, események, incidensek stb.),
  - rendszeres jelentések.

– **Kommunikáció és konzultáció** jelenti a külső és belső érintettekkel folytatott konzultációt a kockázat-felmérési és –kezelési teljes életciklus alatt.

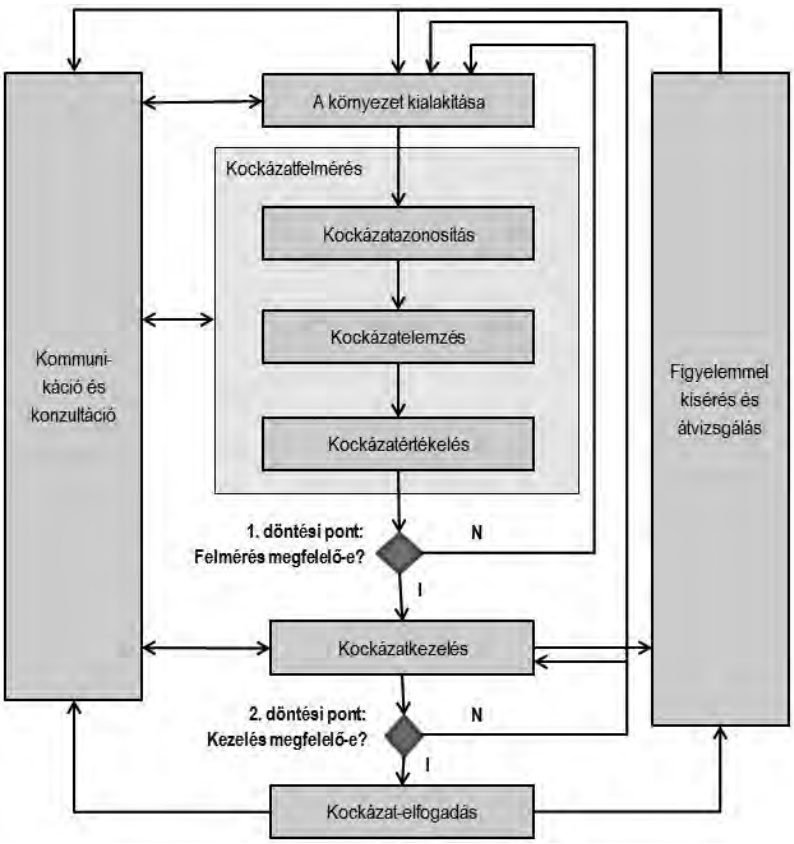
  Ennek célja a teljes kockázatfelmérési és -kezelési folyamat eredményességének, hatékonyságának javítása minden érdekelt fél bevonásával és megnyerésével.

A kockázatok menedzselési folyamatának leképezése az információbiztonsági kockázatokra

Az információbiztonsági kockázatok menedzselésének (felmérésének és kezelésnek) életciklusára vonatkozó követelményeket és gyakorlati tanácsokat mutat be az ***ISO/IEC 27005:2011 Information technology – Security techniques – Information risk management*** c. szabvány. Jellemzően ez a szabvány is a kockázatmenedzsmentnek az eddig bemutatott általános terminológiájára és módszertani megközelítésére épít, és azt képezi le speciálisan az információbiztonsági követelmények figyelembevételével.

Ennek megfelelően az információbiztonsági kockázatok felmérését és kezelését a következő életciklusnak megfelelően mutatja be (3. ábra). A 3. ábrán látható, hogy az információbiztonsági kockázatfelmérés és -kezelés folyamatában megvan minden egyes lépés ugyanúgy, mint az általános kockázatfelmérés és -kezelés esetén, néhány elemmel kiegészülve.

[1] Általánosan a kockázatok hatása lehet pozitív és negatív is, ezért a kockázatkezelési intézkedések célozhatják a kockázatok növelését, vagy a kívánt hatás bekövetkezésének elősegítését is. Jelen esetben az információbiztonsági kockázatokra fókuszálunk, ezért csak a negatív hatású kockázatokkal foglalkozunk.



3. ábra: Az információbiztonsági kockázatfelmérés és -kezelés folyamata az ISO/IEC 27005:2012 szerint

– Az általános modellben (2. ábra) lévő kockázatkezelés lépései szét vannak bontva két részre oly módon, hogy kiemelésre került belőle a **Kockázat-elfogadás lépése.** Ez a kockázatkezelési intézkedés bevezetését követő maradvány-kockázat elfogadását jelenti. Az információbiztonsági irányítási rendszerben ezt kötelező tudatosan átgondolni, és a felelős felső vezető által dokumentáltan elfogadtatni.
– Az információbiztonsági kockázatfelmérési és -kezelési életciklus kiegészült két döntési ponttal: a kockázatfelmérést követően a felmérés megfelelőségének, valamint a kockázatkezelést követően a kezelés megfelelőségének az eldöntésével.
  E két döntési pont bevezetésének a célja a kockázatfelmérési és -kezelési életciklus hatékonyságának a javítása, azaz a felmérésre, valamint az intézkedések meghatározására és bevezetésére fordított időigény csökkentése.
  A kockázatfelmérés során, amennyiben a felmért és értékelt kockázati listák elég információt tartalmaznak megfelelő kockázatkezelési intézkedések meghatározására, folytatható a folyamat a kockázatkezelési lépéssel. Amennyiben azonban nem elégséges az az információ, akkor egy újabb kockázatfelmérési ciklussal javasolt egy újabb iterációt megvalósítani, aminek kezdetén a környezeti feltételek (pl. kockázat-elfogadási kritériumok) meghatározása is újragondolható, pontosítható.
  A kockázatok kezelése lépést követően többféle eredmény születhet, különös tekintettel a maradvány kockázatokra. Amennyiben a kockázatkezelési intézkedéseket követően nem sikerült a kockázati szintet a kívánt elfogadható értékre csökkenteni, akkor vagy új kockázatkezelési intézkedéseket kell meghatározni és bevezetni (vissza a kockázatkezeléshez), vagy a kockázat-felmérési- és kezelési ciklust újra elkezdve elölről iterálni a folyamatot, pl. a kockázatok elfogadási kritériumainak módosításával (vissza a környezet kialakításához).

Az ISO/IEC 27001:2011 szabvány részletesen bemutatja az információbiztonsági kockázat-menedzsment lépéseit, azok végrehajtásának követelményeit, módszereit, továbbá példákat (ajánlásokat) mutat be a következőkre:

– a (védendő) vagyontárgyak kategóriái;
– a vagyontárgyak veszteség-kategóriái;
– a jellemző fenyegetési típusok;
– lehetséges sebezhetőségek (az azokat kihasználó fenyegetésekkel párban);
– m**ódszerek a sebezhetőségek meghatározására**;
– m**ódszerek az információbiztonsági kockázati értékek elemzésére**.

Az információbiztonsági kockázatok felmérési és kezelési életciklusa során az általános irányelvek nagyon kézzelfoghatóan konkretizálhatók, az információbiztonsági kockázatok természetét ismerve. Az információbiztonsági kockázatok hatásmechanizmusát legjobban a CRAMM támadási modell szemlélteti, és a legtöbb információbiztonsági kockázatfelmérési módszertan is erre a gondolatmenetre épít.

A CRAMM[2] támadási modell

A CRAMM támadási modell lényege, hogy a kockázatokat **fenyegetések** okozzák, amelyek **kihasználják a sebezhetőségeket**, aminek következtében **biztonsági események következnek be, amelyek kárt okoznak** vagyontárgyakban, aminek 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 **értelmezzük az információbiztonsági kockázatok vonatkozásában, akkor**

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

Ezeknek az elveknek az értelmezésévek az információbiztonsági kockázatfelmérés lépései feltölthetők konkrét tartalommal.

Az információbiztonsági kockázatok felmérésének alapelvei

Ehhez először néhány fogalmat kell tisztázni:

- Az **ADATVAGYON** tartalmazza a vállalat **védendő adatait, információit.**
- Az (információbiztonsági szempontból értelmezett) **VAGYONTÁRGYAK** nem csak magukat a védendő adatokat foglalják magukba, hanem az azokat tartalmazó adathordozókat, az adat átalakító, továbbító és feldolgozó eszközöket, folyamatokat, személyeket, rendszereket (és azok dokumentációit), amelyeken keresztül az adatok elérhetők, illetve biztonságuk sérülhet. Tágabb értelemben a vagyontárgyak fogalomba beleértendők azok a kommunikációs és védelmi rendszerek is, amelyek az adatvagyon biztonságát hivatottak (közvetve vagy közvetlenül) védeni.

A vagyontárgyak értelmezésébe ilyenformán sokféle kategória is beleeshet. Egy informatikai rendszerben lévő adat biztonságának sérülése sok rétegen (vagyontárgy típuson) keresztül megvalósulhat, ezt mutatja be szemléletesen a 4. ábra.

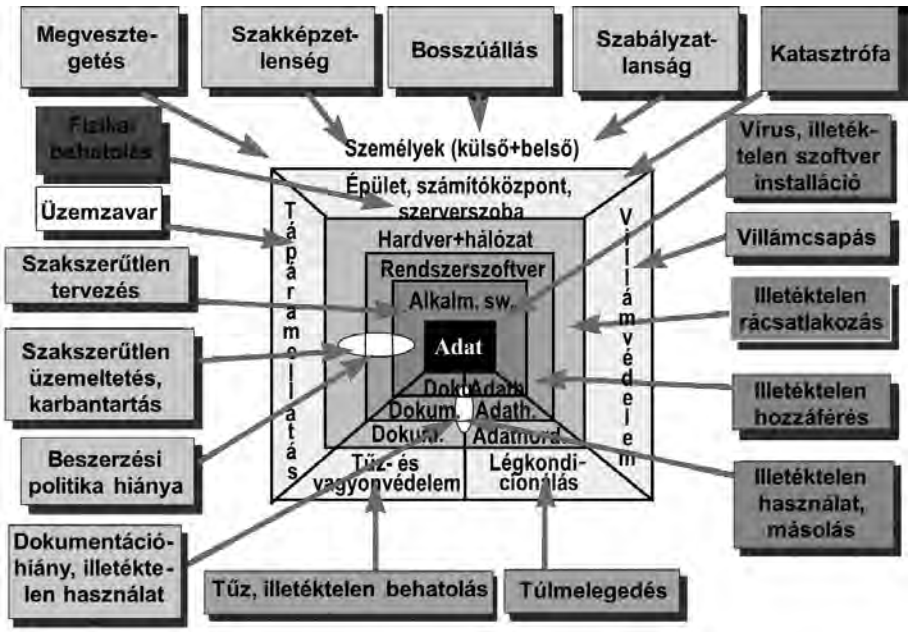
Információbiztonsági szempontból a fontos vagyontárgyakat, amelyeket a különböző fenyegetésektől védeni kell, a következőképpen lehet csoportosítani az ISO/IEC 27005:2011 szerint.

- Elsődleges vagyontárgyak:
  - Üzleti folyamatok és tevékenységek;
  - Információk.
- Támogató vagyontárgyak:
  - Hardver (*adatfeldolgozó, tároló, szállító eszközök, perifériák, médiák stb.*);
  - Szoftver (*különböző funkciójú számítógépes programok*);
  - Hálózat (*hálózatok, hálózati aktív és passzív elemek*);
  - Személyzet (*minden szinten, aki kapcsolatba kerül, külső és belső*);
  - Telephely (*külső környezet, épületek és létesítmények, helyiségek, azokhoz kapcsolódó közművek, felszerelések, kommunikációs eszközök stb.)***;**
  - Szervezeti struktúra (*szervezeti egységek és funkciók stb.)*.

Ezeknek a vagyontárgyaknak a sérülése következtében az azokon tárolt vagy azok által elérhető adatok biztonságának a sérülése a következő veszteségeket, mint jellemző káresemény kategóriákat jelenthetnek:

- jogszabályok, szabályozások megsértése;
- üzleti teljesítmény csökkenése;
- jó hírnév elvesztése;
- személyes adatokkal való visszaélés;
- személyes biztonság veszélyeztetettsége;
- bűnüldözés akadályoztatása;
- bizalmasság megsértése;
- közrend megzavarása;

[2] 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.



4. ábra: Az információbiztonság szempontjából releváns vagyontárgyak és lehetséges fenyegetések példája a MEH ITB 12. sz. ajánlás szerint

– pénzügyi veszteségek;
– üzleti tevékenységek zavarása;
– környezetvédelem veszélyeztetése.

Ezeknek a vagyontárgyaknak a sérülése jellemzően a következő fenyegetési típusok következtében lehetséges:

– fizikai károk *(tűzkár, vízkár, por, korrózió, baleset stb.)*;
– természeti jelenségek (*klímaváltozás, szeizmikus jelenségek, extrém időjárási viszonyok, árvíz stb.*;
– alapvető szolgáltatások hiánya (*klímarendszer, vízellátás, elektronos áramellátás hiánya stb.)*;
– sugárzási zavarok (*hősugárzás, elektromágneses sugárzások* stb.);
– információszivárgás (*HW / SW manipulálása, dokumentumok/ médiák ellopása, lehallgatás, távoli kémkedés stb.*;
– műszaki hiba *(HW / SW hibás működése, IT rendszer túlterheltsége* stb.;
– jogosulatlan tevékenységek (jogosulatlan eszközhasználat, illegális adatfeldolgozás, hamisított/másolt szoftverhasználat stb.);
– működés(i funkciók) megzavarása **(**hibaokozás, jogosultságokkal való visszaélés, személyes hozzáférés akadályozása stb.).

A fenyegetési típusok között külön kategóriát képviselnek a humán tényezőre visszavezethető fenyegetési típusok, amelyek jellemzően a következők lehetnek:

– hacker, kracker (*rendszer feltörése, social engineering, jogosulatlan rendszerhasználat* stb.);
– számítógépes bűnözés (*számítógépes csalás, visszaélés, megszemélyesítés, megvesztegetés, IT rendszerben károkozás* stb.);
– terrorizmus (*információs hadviselés, rendszer feltörések, bombák* stb.);
– ipari kémkedés (*védelmi/ politikai/gazdasági előnyök szerzése, social engineering, információlopás, jogosulatlan hozzáférések* stb.);
– belső munkatársak által (*rendszer hibája, kártékony kódok, szabotázs, csalás, lopás, hibás/ hamisított adatok bevitele, jogosulatlan rendszer-hozzáférés* stb.).

Ezen alapelvekből kiindulva bármely vállalatnál elkezdhetők az információbiztonsági kockázatok felmérésének a lépései:

– A **kockázatkezelési környezet kialakításakor** a feladat a kockázatfelmérési módszertan részletes eljárásának meghatározása, beleértve a számítási és becslési eljárások értékskáláinak meghatározását, a kockázati kritériumok rögzítését stb.
– A **kockázatok azonosítása** során a feladat tulajdonképpen az adatvagyon és az információbiztonsági szempontból releváns vagyontárgyak strukturált számbavétele, majd azokon a lehetséges fenyegetések és az azokat lehetővé tevő sebezhetőségek összegyűjtése. Ezek alapján verbálisan megfogalmazhatók a lehetséges biztonsági események, amelyekhez adottak a vagyontárgyak sebezhetőségei és az azokat kihasználó fenyegetések, majd az azokon keresztüli adatvagyon sérülések által okozott vállalati veszteségek, mint kárhatások.
– A **kockázatok elemzése** a kockázatok azonosítása során feltárt lehetséges biztonsági események bekövetkezési valószínűségét és a lehetséges kárhatás mértékét becsüli egy előre, a környezeti feltételek megfogalmazásakor rögzített értékskálán, majd ezek alapján számítja az egyes biztonsági

események kockázati értékét, kockázati szintjét.

– A **kockázatok értékelése** a lehetséges biztonsági események becsült kockázati értékeit (szintjeit) veti össze az előre meghatározott kockázati kritériumokkal, majd hoz döntést a kockázatkezelés szükségességéről és módjáról.

Ezen elvek felhasználásával bármely vállalatnál meghatározhatóak az ott szükséges és testre szabott kockázat-felmérési és –kezelési lépések.

Felhasznált források

MSZ 13073:2014 Kockázatfelmérés és –kezelés. Szakszótár

MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek

MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények

ISO/IEC 27005:2011 Information technology – Security techniques – Information risk management

MEH Informatikai Tárcaközi Bizottság 12. sz. ajánlása: Informatikai rendszerek biztonsági követelményei, 1.0 verzió (Budapest, 1996)

Gyártás 2030-ban: Nézzünk a jövőbe!

Az üzleti folyamatok és tevékenységek növekvő digitalizálódása arra kényszeríti a termelő vállalatokat, hogy alkalmazott gyártásmenedzsment módszereiket és jelenlegi termékeiket alaposan elemezzék. A „Smart Operation" elnevezésű Fehérkönyvben, amely a www.fir.rwth-aachen.de honlapról letölthető, a Forschungsinstitut für Rationalisierung (FIR) tudományos kutatói összefoglalják, hogy véleményük szerint hogyan néz ki a gyártás a következő években.

A változásokat más okok mellett a globalizáció, az urbanizáció, a demográfiai alakulás és a legfontosabb erőforrások beszűkülése határozza majd meg. A fejlett ipari államokban várható növekvő jólét az individualizált termékek és szolgáltatások iránti kereslet erősödését fogják eredményezni. Ezen kívül fontosabb lesz a teljesítésekhez való hozzáférés, mint a javak birtoklása, amely trend már jelenleg is megfigyelhető.

A FIR szakértői összesen 6 tézisben foglalták össze a gyártásmenedzsment 2030-ban várható követelményeit és azok környezetét:

– Minden termék és szolgáltatás a vevők számára ad hoc hozzáférhető lesz.
– A tér és idő határai el fognak tűnni.
– Az információ össze fog olvadni a természeti valósággal.
– Az értékteremtés a tudáson keresztül fog megvalósulni.
– A teljesítéshez és használathoz való hozzáférés helyettesíti majd a terméket.
– A pazarlást a gyártási folyamatokban és a használat során teljesen ki fogják küszöbölni.

A magas bérszínvonallal működő Németországban 2 gazdasági trend lesz megfigyelhető. Az internet által támogatva az egyik oldalról a reális valóság egyre inkább össze fog olvadni a virtuális valósággal a „dolgok internetévé". A másik oldalról a termékek egyre inkább össze fognak kapcsolódni az elvárt fontos szolgáltatásokkal az úgynevezett „hibrid termékekké".

A várható drasztikus változások ellenére a szakértők azon a véleményen vannak, hogy a gyártás Németországban alapvetően nincs veszélyeztetve. A gyártásmenedzsmentet ugyanakkor jelentősen fejleszteni kell, hogy az a vevői követelményeknek egyre jobban megfeleljen és a digitalizálás lehetőségeit minél jobban hasznosítsa. A gyártást 2030-ban az a képesség fogja jellemezni, hogy sokkal jobban összegyűjti és hasznosítja a sokszínű adatokat és az egyes információkat. A jövő gyártásirányítását sok önálló és autonóm egység fogja jellemezni, melyek ugyanakkor egymással szoros és összehangolt csereviszonyban fognak állni.

MP