Magyar Rendészet 2024/2. 105–120. DOI: 10.32577/mr.2024.2.6

Folyamatmenedzsment a fizikai biztonság területén

TAKÁCS Soma[1] – TÓTH Attila[2]

A publikáció célja a magánbiztonsági piac szereplőinek körében alkalmazandó folyamatmenedzsment-tevékenység eredményességfokozó hatásainak és a szervezeti szintű folyamatmenedzsment-rendszerbe történő integrációjának ismertetése. A kutatásban bemutatjuk a feltárt szakmai logikai összefüggéseket, illetve azok megjelenését a tevékenységben. A szervezetek stratégiai szintű döntéshozatala során könnyen a feledés homályába kerülhet a szervezeti stratégiába ágyazott fizikai biztonság létrehozása, üzemeltetése és fejlesztése. A vállalatok számára elengedhetetlen kritérium, hogy felismerjék a fizikai biztonság stratégiai szintű jelentőségét, és ennek megfelelően helyezzék előtérbe annak integrálását a szervezeti struktúrába. A stratégia magában foglalja a fizikai biztonsági célok és irányelvek meghatározását, valamint ezen irányelvek és szakmai logikák szerint a felelős személyek kinevezését az eljárás végrehajtására és felügyeletére. A folyamatmenedzsment-rendszer alkalmazása jobb átláthatóságot, rendezettséget, ezáltal hatékonyabb működést eredményez a szakmai területek és a szervezet számára. Emellett a folyamatok integrációja lehetőséget biztosít a folyamatos ellenőrzés és az ellenőrzés során feltárt eltérések vizsgálatát követő fejlesztések kivitelezésére, amellyel biztosítja a szervezet rugalmasságát a piaci viszonyokhoz való alkalmazkodáshoz.
Ezek teljesüléséhez elengedhetetlen a fizikai biztonsági folyamatok integrálása a szervezeti szintű folyamatmenedzsmentbe, amely egyszerre elérhetővé teszi a tevékenység hatékony felügyeletének és irányításának lehetőségét is. Az integrált megközelítés hozzájárul a szervezet hosszú távú eredményes működtetéséhez és piaci versenyképességének fenntartásához.

Kulcsszavak: *folyamatmenedzsment, fizikai biztonság, kockázatkezelés, stratégia, mesterséges intelligencia*

A fizikai biztonság és a folyamatmenedzsment kapcsolata

A fizikai biztonság szakmai területének irányítására kiválasztott vezető meghatározza a fizikai biztonság stratégiai szintűvé tételének esélyét, ezért a szakmai szempontok értékelése mellett kimondottan fontos a stratégiai megközelítés kritériumkövetelményeinek elemzése. Ahhoz, hogy a fizikai biztonság feladatainak

[1] Hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék, e-mail: takacssoma13@gmail.com
[2] Tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék, e-mail: toth.attila@uni-nke.hu

tervezése a szervezet stratégiai szintjén történhessen, elengedhetetlen a folyamatmenedzsment-rendszer integrálása a fizikai biztonság tevékenységi rendszerébe. Az integrálásához szükség van a terület szakmai irányításának felismerésére és elhatározására, egy jól működő folyamatszemléletű rendszer kialakítására, valamint a technológiai fejlődés fontosságának felismerésére, ügymenetekbe integrálására és napi szintű alkalmazására.

A folyamatmenedzsment logikája szerint az alapelemek megléte nélkülözhetetlen a folyamatmenedzsment-rendszer kiépítése során:

- dokumentálás;
- mérhetővé tétel/mérhetőség (kvalitatív és kvantitatív módszerek);
- szabályozás;
- menedzselés;
- fejlesztés.[3]

Az integráció megvalósítása érdekében kiemelt szerepet kap a szakmai terület vezetése, ugyanis a folyamatszemléletű munkatevékenységek kidolgozásához magas szintű menedzsment, illetve az ehhez kapcsolódó gazdasági, pénzügyi, valamint döntéshozói szemléletmódra van szükség. A tapasztalat, az említett szemléletmód és az ahhoz tartozó ismeretanyag megléte a szakmai terület vezetői felelősségi körébe tartozó kérdéskör, amelyek hiányában a hatékony integráció és ennek következményeképp a fizikai biztonság stratégiai szintre emelése sem valósulhat meg.

A fizikai biztonság a szervezetek életében nem az azonnali és közvetlen értékteremtésben, hanem a fő folyamatok támogatásában rejlik. Jogosan merülhet fel a kérdés, hogy a fizikai biztonság hogyan tudja támogatni a szervezetek fő- és kulcsfolyamatait úgy, hogy eközben közvetlen módon értéket nem teremt?

A fizikai biztonság két alapvető célja a személyi, valamint a vagyonbiztonság garantálása, amely alatt a természetes személyek élet- és balesetvédelmét, illetve a materiális (például készpénz, előállított termék) és immateriális (például adatvagyon, know-how és a termelési folyamatok működésfolytonossága) javak garanciáját kell érteni.[4]

A humán faktort érintő kockázatok elleni védekezés alkotóelemei például az alapvető szabályozási rendszerek (rezsimintézkedések), valamint az azt kielégítő műszaki megoldások, amelyekkel a védelem olyan mértékű kockázatcsökkenést eredményez, amely tovább már nem, vagy csak aránytalan erőforrás-befektetéssel csökkenthető, és az a szervezet számára elfogadható mértékű kockázati besorolási osztályba kerül.

A tárgyi eszközök és az infrastrukturális javak védelme a fizikai biztonság kiemelt jelentőségű területe, amelyet a magyar jogrendszer „vagyonvédelem”[5] név

[3] Lásd Kvalikon, www.kvalikon.hu/folyamatmenedzsment/rendszer-kialakitas.php

[4] Szabó 2017.

[5] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint magánnyomozói tevékenység szabályairól törvényben alkalmazott kifejezés.

alatt aposztrofál. Egy szervezet eszközeinek és infrastrukturális javainak védelme elengedhetetlen folyamat a szervezet működésfolytonossága szempontjából. A fizikai biztonság ugyan nem közvetlenül, de stratégiailag is értékelhető módon hozzájárul a szervezet értékképzéséhez az intézkedések és az egyéb biztonsági rendszerek által megelőzött veszteségek és a működési folyamatok hatékony végrehajtása révén.

A digitalizáció korában az információs rendszerekkel kapcsolatos incidensek a legjelentősebb reputációs kockázati források közé tartoznak a szervezetekre nézve, ugyanis a kiszivárgott adatok jelentős piaci versenyhátrányt okozhatnak az információbiztonságra nem kellő hangsúlyt fektető vállalat számára. Napjainkban a védendő materiális értékek egyre inkább kiegészülnek kevésbé kézzelfogható, igen nagy értéket képviselő információval, adattal is.[6] Az „információs rendszerek”[7] és a tárolt adatok védelmének biztosítása szintén a fizikai biztonsági folyamatok kivitelezésével és üzemeltetésével érhető el. A jelenlegi piaci álláspont alapján a megrendelők körében is széles körben elterjedt az információbiztonsági tanúsítványok igénye. A megszerzett tanúsítványok adnak biztosítékot a megrendelő számára, hogy a szabványok által támasztott követelményrendszernek, jó gyakorlatoknak a szerződni kívánt partner megfelel. A szakmai területen kialakított folyamatszemlélet azért is kimondottan fontos, mert a szabványok, valamint a szabvány előírásainak ellenőrzése és a tanúsítás megszerzése érdekében szükséges auditok is a folyamatszemlélet elvét követik, annak számos előnyével. A 20. század végén és a 21. század elején végbemenő „technológiai ipari forradalom” következtében az információbiztonság hamar kiemelt szempont lett a komplex fizikai biztonsági rendszerek kialakítása során is, hiszen az információkhoz, adatokhoz történő fizikai hozzáférések kockázatait szervezeti szinten szükséges kezelni. Továbbá a fizikai biztonsági folyamatok körébe tartozó biztonságtechnikai eszközök (például videómegfigyelő, behatolásjelző, beléptetőrendszerek) műszaki kivitelezésüknél fogva szintén érintettek az információbiztonsági kockázatok által. A gyártás, fejlesztés közben, valamint a fizikai telepítés során figyelembe kell venni a vonatkozó követelményrendszereket, szabványokat (ISO 27001,[8] NIST 800-53,[9] ISO/IEC 27005,[10] ISO 9001,[11] EN 14450,[12] MSZ EN 1143[13]). Az adatbiztonság feltételeinek biztosítása pontosan az információs rendszerek ugrásszerű növekedése és a szervezetet nagymértékben befolyásoló hatása miatt az értékteremtő képességhez közvetlen módon kapcsolódik.

---

6 Tóth 2018.
7 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
8 MSZ ISO/IEC 27001 Információbiztonsági irányítási rendszerek című szabvány.
9 NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations című szabvány.
10 ISO/IEC 27005 Information Technology – Security Techniques – Information Security Risk Management című szabvány.
11 MSZ EN ISO 9001 Minőségirányítási rendszerek című szabvány.
12 EN 14450 Secure Storage Units című szabvány.
13 MSZ EN 1143 Biztonságos értéktárolók című szabvány.

Összefoglalva: a szervezet fizikai biztonsággal kapcsolatos tevékenysége közvetlen módon ugyan nem teremt értéket, azonban a kritikus erőforrások védelmével, a veszteségek minimalizálásával, valamint a fő folyamatok közvetett támogatásával nagymértékben hozzájárul a szervezet valódi értékteremtő tevékenységéhez, amely szempontot figyelembe véve kijelenthető, hogy a fizikai biztonság tervezését, szervezését stratégiai szinten szükséges kezelni a szervezet eredményességének hosszú távú fenntartása érdekében.

Stratégiai döntéshozatal

A stratégiai döntések kihatásai, következményei jelentősen befolyásolják az adott szervezet eredményességét és célkitűzéseinek teljesülését. Az adott szervezeti stratégiák kialakítását, végrehajtását számtalan, a visszacsatolást és a szervezeti tanulást biztosító megoldás támogatja vagy támogathatja, a döntés pillanata azonban minden esetben humán tényezőhöz kötött. A stratégia kidolgozása és végrehajtása során az emberi tényező (például kreativitás, tapasztalatok) egyelőre nélkülözhetetlen elemeknek tekinthetők. A folyamat során a technológiai fejlődésnek köszönhetően bizonyos megoldások (például döntéstámogató szoftverek) nagy mennyiségű adatbázisból épített és folyamatosan tanuló algoritmusai jelentős segítséget nyújthatnak döntéshozatalkor, ugyanakkor a végső döntés továbbra is vezetői beavatkozást igényel, már csak a felelősségi viszonyok miatt is, hiszen a jogrendszer jelenleg nincsen felkészülve az automatizált döntéshozatal felelősségi kérdésköreinek megállapítására.

1. ábra: Stratégiai döntéshozatal

Forrás: a szerzők szerkesztése

A stratégiai menedzsment során a döntéshozatal személyi tényezőjének említése kapcsán szükséges megvizsgálni a stratégiai döntések jellemzőit, amelyek egyértelműen definiálják, hogy miért van szükség a döntés meghozatalakor a szoftverek adatelemzési képességeire és a kreativitás ötvözésére.

A stratégiai döntések jellemzői:

- jövőre vonatkozó – információigénnyel rendelkező szituációk (többféle lehetséges kimenet);
- minden esetben bizonytalan adatokra és információkra kell alapozni őket (magas kockázati szint);
- a stratégiai döntések során több célt figyelembe vevő döntést kell hozni (gazdasági és gazdaságon kívüli egyéb célokat is mérlegelni kell);
- bizonyos esetekben a piaci környezethez való gyors alkalmazkodás érdekében a stratégiai szintű döntéseket is hasonló gyorsasággal kell meghozni, a piac változását követve (például Covid-járvány, amely során azonos időben több stratégiai döntést kellett meghoznia a vállalatok menedzsmentjének).

A stratégiai döntés jellemzőinek felsorolását követően egyértelműsíthető, hogy maga a döntéshozatali folyamat információhiányos állapotban, több célt figyelembe vevő és szolgáló döntés meghozatalára irányul. A szervezet nézőpontjából a stratégiai jelentőségű döntések magas kockázati besorolással rendelkeznek, hiszen közvetlenül befolyásolják a szervezet által kitűzött teljesítési célokat, valamint a gazdaságossági mutatókat.

A stratégiai döntés folyamata során alkalmazható, a körülményeket széles spektrumban figyelembe vevő elemzési technika a PEST(EL)-elemzés, SWOT-elemzés, Pareto-elemzés vagy a dominanciamódszer.

Folyamatmenedzsment alkalmazása a stratégiai szint esetében

A folyamatmenedzsment átható stratégiai alkalmazása lehetőséget ad a vállalatok számára, hogy hatékony módon tervezzék, hajtsák végre és értékeljék az előzetes célkitűzéseik eléréséhez szükséges intézkedéseket. A folyamatmenedzsment alkalmazása segít a vállalatoknak egyértelműsíteni stratégiai célkitűzéseiket, valamint a folyamatok állandósult elemzése és fejlesztése segít e célok elérésében. A célok eléréséhez nagymértékben hozzájárul az elemzés során a felesleges erőforrásokat felemésztő folyamatok kiszűrése és azok átdolgozása vagy megszüntetése, hogy az erőforrások allokációja hatékony módon történhessen. Az elemző tevékenység következtében a folyamatok kritikus pontjai könnyen azonosíthatóvá válnak, amelyek a kockázatmenedzsment során felhasználhatók a folyamatok értékelési keretrendszerében, segítségükkel lehetséges a stratégiai tervezés hatékonyságának javítása. A folyamatmenedzsment támogatja a stratégiai döntések végrehajtását, hogy pontosan meghatározza, hogyan kell azokat az értékteremtő üzleti folyama-

tokba integrálni. A folyamatirányítási eszközök segítenek a stratégiai teljesítmények mérésében és azok egyedi értékelésében. A teljesítménymérés során a folyamatok kontrollpontjaiba integrált KPI-k[14] számszerűen is képesek jól kifejezni a teljesítményszintet, ezzel támogatva a stratégiai célkitűzések elérését. A folyamatszemlélet lehetőséget biztosít az állandósult preventív szervezeti tanulásra és fejlődésre, hiszen a vállalatok a saját értékelési rendszerük szerint a folyamatokon keresztül értékelhetik és javíthatják teljesítményüket. Szponzorálja a vállalatokat a stratégiai célok meghatározásában, a közvetlen értékteremtő és az értékteremtést támogató folyamatok optimalizálásában, és a folyamatos fejlesztéssel kiegészítve hozzájárul a vállalat hosszú távú sikeréhez. A folyamatmenedzsment stratégiai folyamatokba való integrálásával hatékonyabb vállalati működés mellett a szervezetek felkészülhetnek és gyorsabban adaptálódhatnak a változó piaci körülményekhez.

Folyamatmenedzsment

A folyamat értelmezésének nehézsége, hogy ahány szakmai terület létezik, annyi fogalmi meghatározás van. A magánbiztonsági piacot tekintve elmondható, hogy a folyamat szó használata esetén a gazdasági, pénzügyi definícióra kell gondolni. A folyamat fogalmi értelmezéséhez az alkotóelemeit, tulajdonságait, funkcióit kell következetesen megvizsgálni: „a folyamat egy vagy több tevékenység, amely értéket növel úgy, hogy egy bemenetkészletet átalakít kimenetek készletévé (javakká vagy szolgáltatásokká) egy más személy (a vevő, felhasználó) számára, emberek, módszerek és eszközök kombinációjával."[15]

A folyamat lényegi eleme, hogy értéket teremt, amiről akkor lehet beszélni, ha a kimenet értéke nagyobb, mint a bemenet értéke. Egyértelműen megállapítható, hogy a magasabb értéket, amelyet az output (kimenet) képvisel, a folyamat részeként kezelt eszközök, eljárások megfelelő alkalmazásával, az input (bemenet) átalakításával érte el. A folyamat célja nem más, mint az értékteremtés az adott személy/folyamat számára az output oldalon.

Folyamatokat felépítő egységek:

- input és output (be- és kimenet);
- tevékenység;
- információ;
- végrehajtásért/végrehajtatásért felelős megjelölése (személy/szervezeti egység);
- folyamatot szabályozó logikailag összeállított szabályozás/leírás.

[14] KPI: Key Performance Indicator, kulcsteljesítmény-mutató.
[15] Tenner – De Toro 1998.

A folyamatok kialakításának módszere

A folyamat kialakításához pontosan meg kell ismerni a környezeti sajátosságokat, amelyek alapján megalkotható és szervezeti struktúrába illeszthető a folyamat. A folyamatok kialakításának legegyszerűbb formája a szakmai szervezeti egység adatszolgáltatásával történik, amely információk tudatában a folyamat kialakítása, leírása megvalósítható, majd ezt követően összehangolják a szervezet belső szabályozásával és beépítik a cégstruktúrába, hogy az adott output-ot a megfelelő helyen és időben szolgáltassa a cél elérése érdekében. A fizikai biztonsági szakterület egyik fő célja a szervezeten belüli, illetve azokat érintő felelősségek tisztázása (felelősség meghatározása, felelősség megállapítása), felelősségi körök kezelése és alkalmazása (élőerős őrzés; biztonságtechnikai rendszer alkalmazásának módszertanai). A magánbiztonság- és a folyamatmenedzsment-szemléletmód között vont párhuzam tanulmányozásának következtében világossá válhat, hogy a folyamatszemléletnek szintén kritériumkövetelménye a tevékenységet végző személyek felelősségi köreinek tisztázottsága (egymástól egyértelműen elkülönülő felelősségi körök).

A felelősségszemléletű folyamatmenedzsment kialakításához megfelelő módszert biztosíthat a kriminalisztika hét alapkérdésének logikája, ahol a válaszok tudatában – amelyek alapján mindig felelősségeket, tényeket állapítunk meg – egyértelműen kialakíthatók és szervezeti struktúrába integrálhatók a folyamatok.[16]

KI/MI? – felelősségi, hatás- és jogkörök egyértelmű azonosítása és definiálása.

KIT/MIT? – azonosított és egyértelműen meghatározott keretek közötti be- és kimenetek.

KIVEL/MIVEL? – szükséges erőforrások azonosítása.

MIKOR? – időgazdálkodás, időmenedzsment, szükséges idő azonosítása.

HOL? – a folyamat területi hatálya, kiterjedésének leírása.

HOGYAN? – az eljárások definiálása, fő-, illetve részfolyamatok pontosítása.

MIÉRT? – elérendő cél megjelölése, minőségpolitika.

A válaszok alapján összeállítható egy jól strukturált folyamatleírás, amely nélkülözhetetlen a szervezet hatékony szabályozási rendszerének kiegészítéséhez. A folyamatleírásokat alapvetően szervezeti egység szinten kell kialakítani, környezettől függően különböző mértékben kell összehangolni a szervezet célkitűzéseinek elérése érdekében. A folyamatleírások esetében említhető a rendkívül népszerű, William Edwards Deming amerikai nemzetiségű közgazdász által megalkotott PDCA-ciklus, amely a folyamatok esetében is rendkívül hangsúlyos elem. (P = Plan, folyamattervezés; D = Do, folyamat bevezetése és alkalmazása; C = Check, folyamatos ellenőrzés előre meghatározott kontrollpontok alapján; A = Act, az ellenőrzés során feltárt eltérések kezelése, kijavítása, egyben az ellenőrzés során feltárt információk értékelése).

[16] Fenyvesi 2013: 343.

A folyamatleírásban meghatározott kontrollpontok alapján az egyik fő cél a munkahatékonyság növelése mellett a folyamat kvantitatív és kvalitatív mérhetősége, amit figyelembe véve konkrét adatokkal támogatható a döntéshozatal a szervezet esetében. A folyamatleírás akkor tekintendő definiáltnak, ha meghatároztuk a kezdő- és végpontját, a folytatott tevékenységeket, a döntési pontokat és a döntéshozók személyét, a tevékenység felelősét, résztvevőit, szükséges be- és kimeneteket, valamint az információszolgáltatási kötelezettségeket.

Folyamatok csoportosítása

A folyamatok csoportosítását leggyakrabban a szervezetben elfoglalt hely és funkció, továbbá a szervezet tevékenysége determinálja.

Elsődleges folyamatok vagy fő folyamatok

Azon tevékenységek, amelyek stratégiailag kiemelt szerepet töltenek be a szervezet esetében, az értékteremtési lánc szerves részét képezik és/vagy közvetlen kapcsolatban állnak a kimenetek megteremtésében (például termelési folyamatok).

Irányítási folyamatok

Azon folyamatok, amelyek a szervezet és a szervezetben lévő folyamatok összehangolásához, irányításához, szervezéséhez szükségesek (például irányítási rendszerhez kapcsolódó vállalatirányítási folyamatok).

Támogató/mellékfolyamatok

Azon folyamatok, amelyek az elsődleges folyamatok zavartalan működését és az ahhoz nélkülözhetetlen feltételeket biztosítják (például fizikai biztonsági folyamatok).

A folyamatszemlélet és folyamatalapú szabályozás esetén a folyamatleírások és a folyamatábrák *(flow-chart)* alapján a szervezeti egységek munkavállalói átláthatják a munkafolyamatok részleteit, és a folyamatleírások közötti összefüggések értelmezését követően megérthetik a szervezet működését, és a szervezeten belüli munkájuk által előállított outputot, amely közvetlen vagy közvetett módon hozzájárul a szervezet üzleti eredményét biztosító tevékenységhez.[17]

[17] Ambrus–Lengyel 2011.

„Ahhoz, hogy e folyamatokat valóban irányítani, sőt fejleszteni lehessen, valamilyen módon strukturálnunk és értelmeznünk, vagyis megragadhatóvá, kommunikálhatóvá, nyomon követhetővé kell tennünk őket. Arra van szükség, hogy a szervezet folyamatait előzetesen rendszerezni tudjuk: a gyakorlatban ez a működési folyamatok hierarchiájának meghatározását jelenti."[18]

A „folyamathierarchia" kialakítását és a különböző hierarchikus szintek szükségességét teljes mértékben a környezet, azaz a szervezet berendezkedése, tevékenysége, mérete határozza meg.[19]

A folyamathierarchia általánosnak tekinthető kategorizálási rendszere a következő: mozdulat – munkafázis – tevékenység – részfolyamat – folyamat – folyamatköteg.[20]

A folyamathierarchia alapján a kulcsfolyamat az, amely közvetlenül az értékteremtéshez, a szervezet fő folyamataihoz kapcsolódó tevékenységet tartalmaz, vagy amely stratégiailag indokolt és annak minősítenek (például egy biztonságtechnikai eszközöket fejlesztő, gyártó cég nyomtatott áramköröket tartalmazó eszközének minőségellenőrzése az összeszerelést követően).

Kockázatmenedzsment

A fizikai biztonsági tevékenységekben a kockázat fogalma központi szerepet kap, és a vállalat tevékenységi körétől függően közvetlen vagy közvetett veszélyt jelentő fogalmi elemként határozható meg.

A számos kockázatot definiáló fogalom közül a magánbiztonsági szektor rendvédelmi eredetét figyelembe véve a kockázat az alábbiak szerint írható le: „A kockázat fogalma alatt egyszerűsített formában a bizonytalan események negatív hatásait érthetjük."[21] Az egyszerűsített fogalom azonban nem képes lefedni a kockázat teljes értékű jelentését, ezért a tények pontos ismeretéhez szükséges a kockázat fogalmának bővebb feltárása.

A szervezet szemszögéből nézve kockázatoknak tekintjük „azon potenciálisan bekövetkező külső és belső eseményeket, zavarokat, amelyek következtében veszélybe kerül a vevői- és/ vagy ügyféligények kielégítése, vagy bármely érintett biztonsága".[22] Eszerint a kockázat a vállalat tevékenységét tekintve közvetlen vagy közvetett módon veszélyeztető jellegű, hiszen a fogalomból kiderül, hogy a vállalat által nyújtott szolgáltatás/tevékenység bekövetkezésének zavarára utal, és részben vagy akár teljesen meghiúsulhat az adott szolgáltatásra/tevékenységre vállalt szerződéses formájú kötelezettség. Értelemszerűen a szerződéses megállapodás megszegése egy szervezet éle-

[18] Varga-Polyák 2014.
[19] Kiss 1987.
[20] Bernáth 2021.
[21] Michelberger 2024.
[22] Michelberger–Horváth 2017.

tében elkerülendő, ugyanis az közvetlen módon veszteséget termelő tényező. A veszteség egy szinttel enyhébb megnyilvánulási formája lehet a kötbér-kötelezettség, de az adott zavar és nem a szerződéses SLA-ban (Service Level Agreement – szolgáltatásiszint-megállapodás) megjelölt minőségi követelményrendszernek megfelelő teljesítés a szerződéses viszony felbontását is eredményezheti.

A kockázat fogalmáról az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), 1. § 28. pontja [23] is rendelkezik, és alapvetően az információs rendszerek vonatkozásában tekinthető mérvadónak. Ugyanakkor a kockázatot mint fogalmat az azt felépítő részegységeken keresztül magyarázza, miszerint a kockázat „a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye".

Ezek alapján kijelenthető, hogy a kockázatot leíró fogalmak alapvetően negatív jelentéstartalommal rendelkeznek, azonban a kockázat közgazdaságtani megközelítésű fogalomrendszere – amely mind a verseny-, mind pedig a közszférában elfogadott – külön említést tesz a pozitív hatású kockázatokról is.[24] A könnyebb megértés érdekében pozitív kockázat lehet például: belépés egy új piaci környezetbe, hiszen a vállalat számára az új piac számos előre nem látható akadályt képezhet, ugyanakkor az akadályokra való előzetes felkészülés, valamint az adott piaci helyzethez való alkalmazkodás következtében a vállalat számára profitnövekedés képében, pozitív eredményt idézhet elő, ami koherens a szervezet előzetes célkitűzésével. A COSO (Committee of Sponsoring Organizations of the Treadway Commission – A Treadway Bizottság Szponzoráló Szervezeteinek Bizottsága) modell ugyanúgy megkülönböztet negatív és pozitív behatásokat, azonban a pozitívat lehetőségnek *(opportunity),* a negatívat pedig kockázatnak *(risk)* nevezi. Azonban míg a COSO célja leginkább a belső ellenőrzés és a vállalati kormányzat minőségi fejlesztése, addig az ISO 31000 kockázatkezelési keretrendszer egy általános nemzetközi szabvány a kockázatkezelésre és bármilyen típusú szervezet esetében alkalmazható, a földrajzi elhelyezkedéstől és az iparágtól függetlenül. Az ISO 31000 szabvány kockázatkezelési modellje jóval szélesebb körben alkalmazható, köszönhetően annak, hogy a kockázatkezelésre vonatkozó általános irányelveket határoz meg az alkalmazó szervezet számára a COSO-modell öt fix komponensével szemben, amelyek megkerülhetetlen részegységként nagyban függenek a szervezet tulajdonságaitól és körülményeitől (például a szervezet célkitűzései, követelményei, iparág, lefedett piac stb.).[25]

Összefoglalva: a kockázat nem csak és kizárólag negatív hatással rendelkező „tiszta kockázatként" definiálható, ettől elkülönülve megállapítható az üzleti célokat egyaránt eredményező kockázat, amelyet együttes néven pozitív hatású kockázatnak nevezünk.[26]

---

[23] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[24] Pénzügyminisztérium 2021.
[25] Lásd: www.coso.org/
[26] Horváth–Szlávik 2011.

A menedzsment fogalmához igazodva a kockázatmenedzsment (azonosítás, értékelés, kezelés, ellenőrzés) több tevékenység összehangolásával, szervezésével és azok irányításával, a vállalat érdekével megegyező irányba mutató tevékenység optimalizálásával foglalkozik. Eszerint a „kockázatmenedzsment a vezetési elvek, tapasztalatok és eljárások rendszeres alkalmazása a kockázatok azonosítására, megfigyelésére, elemzésére, felmérésére és csökkentésére."[27] A kockázatmenedzsment a feltételezett kockázatok szisztematikus és tervezhető menedzselésére épül, eredményének kiértékelését követően a vállalat a folyamatait kockázatarányos módon hozhatja létre, fejlesztheti, esetlegesen további rész- vagy alfolyamatokra bonthatja, vagy éppen megszüntetheti a meghatározott kockázati szintet meghaladó besorolással rendelkező folyamatot.

Kockázatkezelés

A kockázatkezelés az aktív kockázatok elleni támogató tevékenységet jelenti, amelylyel a kockázatok szintje mérsékelhető, csökkenthető vagy teljes mértékben megszüntethető.

Kockázatkezelési módszerek

Kockázat elfogadása

Az adott kockázati elem elfogadása akkor történik, ha annak kockázata nem, vagy csak a szervezet számára aránytalan költség felhasználása esetén csökkenthető.

Kockázatminimalizálás

A leggyakoribb kockázatkezelési módszer, amely során a szervezetek kockázatkezelési stratégiájuk szerint konkrét intézkedéseket teljesítenek, amelyekkel a kockázati hatás csökkenthető, vagy akár teljes mértékben megszüntethető.

Kockázatátruházás/-áthárítás/-megosztás

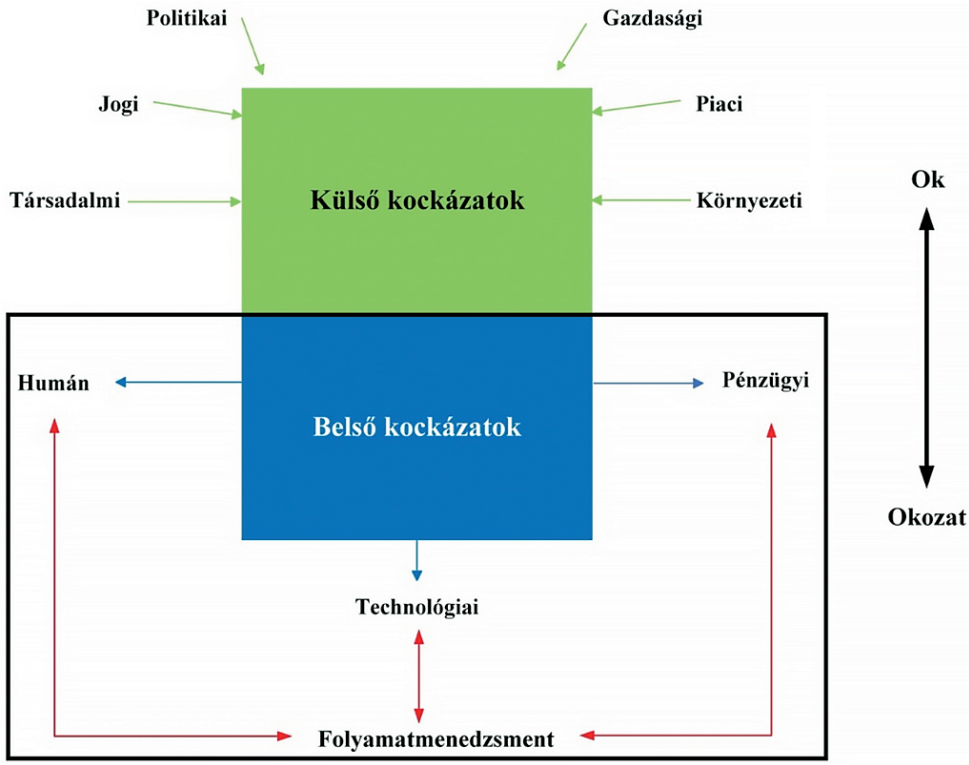
A szervezet az azonosított kockázatot átruházza egy másik félre (például biztosítási szerződés megkötése esetén a biztosító társaságra).

[27] László 2014.

Kockázatok csoportosítása

Kockázat eredete szerint: külső, belső.

Kockázat fajtája szerint: pénzügyi, humán, technológiai, stratégiai, környezeti, jogi, politikai, piaci, társadalmi.



2. ábra: Kockázatok csoportosítása

Forrás: a szerzők szerkesztése

Javaslatok

Az első és egyben az egyik legfontosabb a folyamatmenedzsment-szemléletben megalkotott fizikai biztonsági szakterületet komplex módon átfogó szabályozási rendszer kialakítása, ami lehetővé teszi a rugalmas és gyors alkalmazkodást a változó követelményrendszerekhez. A hatékonyság nagy mértékű növeléséhez a biztonsági szakterületnek is rugalmasan kell alkalmazkodnia oly módon, hogy a vállalati normáknak megfelelő védelmi szint ne csökkenjen a rugalmasság megteremtése érdekében. A rugalmasság irányába való elmozdulásnak is van maximumértéke, amely

összefügg a kockázatelemzési, kockázatmenedzsment-tevékenységgel, hiszen a kockázati érték növekedése nélkül kell elérni ezt az állapotot. A szabályozási rendszert tekintve a folyamatmenedzsmentet leginkább támogató szabályozási rendszer a szakmai szempontrendszert állító fizikai biztonsági szabályozás, amely a vállalat zavarmentes állapotának megteremtéséhez szükséges, és a biztonsági szakterület által folyatatott fő tevékenységeket szabályozza, azonban a konkrét követelményrendszereket, sztenderdeket a szabályozástól független módon, eljárásrendek formájában adják ki. Az eljárásrendekkel szabályozva elérhetjük, hogy a biztonsági szabályozás is folyamatszinten „gondolkodjon", és a tevékenységekre speciális rendszabályokat határozzon meg, ugyanakkor ezt a szabályozási rendszert gyorsan lehet adaptálni a magasabb szintű szabályozáshoz vagy éppen a piaci trendekhez.

A biztonságtechnikai rendszerek alkalmazása során keletkezett adatok rendszerszintű kezelése és integrációja a kapcsolódó folyamatokba. Példaként egy ipari létesítmény (például termelőüzem) áruszállítási folyamataival történő információmegosztás folyamata áll. Az áru be- és kiáramlása során a beléptetőrendszeren hasznos információk keletkezhetnek a rakodást végző szakterület számára, hiszen amíg a teherforgalmi beléptetés zajlik, addig a beléptetőrendszer automatizált módon megküldött adatok alapján előkészítheti az adott árut a berakodásra és az elszállításra. Az egymással logikai összefüggésben lévő folyamatok összekapcsolásával a telephelyen lévő teherforgalom feltorlódása csökkenthető, és a telephely kihasználtsága jól optimalizálható. A be- és kilépés között eltelt idő pedig KPI-ként szolgálhat a folyamatban részt vevők számára.

A folyamatokkal kapcsolatos tevékenység során az egyik legegyszerűbb, négylépéses, folyamatosan ismétlődő menedzsmentmódszer a PDCA-ciklus alkalmazása. A folyamatok körültekintő tervezési szakasza rendkívül fontos, hogy a tevékenység a lehető leghatékonyabban érje el a kitűzött célt a minőségi szint csökkenése, azaz a kockázati szint növekedése nélkül (például kevesebb erőforrás felhasználásával hajtják végre az adott tevékenységet – automatizálás, digitalizáció a folyamat végrehajtásában). Az ellenőrzés szakaszában a tervezés és a megvalósítás közötti eltérések felderítésén van a hangsúly, hogy az eltérések száma csökkenjen, valamint e szakasznak köszönhetően lehetséges a folyamat fejlesztése, ugyanis az ellenőrzés során feltárt hibákra új megoldásokat kell kidolgozni és bevezetni az adott folyamat hatékonyságának maximalizálására. A beavatkozás szakasza már az ellenőrzést követő aktív tevékenység a folyamat megváltoztatására, illetve az abban lévő eltérések minőségi javítására.

A folyamatmenedzsment alkalmazásával kapcsolatos szakterületi oktatási rendszer kidolgozása, valamint annak felülvizsgálata. A piaci versenyelőny megtartása érdekében kiemelt szempont az oktatás folyamatossága és időszakos ismétlése, valamint továbbfejlesztése. Az oktatási rendszer kialakítása során fontos tényező a szervezet hierarchikus szétválasztása és a tananyag szervezeti hierarchiában elfoglalt hely szerinti oktatása (stratégiai, taktikai és operatív szintek). A célorientált szakmai oktatási rendszer kidolgozásához célszerű a képzést követő vizsgakötele-

zettség előírása, továbbá az időszakos vizsgák egyéni értékelési rendszerbe integrálása a vizsga eredményével arányos módon.

Folyamatirányítási, vállalatirányítási rendszerek bevezetése és implementálása az adott vállalati környezetbe. A vállalatirányítási rendszerek nagymértékben hozzájárulnak a szakmai területek, illetve a menedzsmenttevékenység támogatásához, hiszen átfogóan elemzik a szervezet tevékenységeit, és az előre meghatározott ellenőrzési folyamatok mentén állandó, valós idejű monitorozással olyan információt, kulcsfontosságú teljesítménymutatókat képesek szolgáltatni, amelyek alapján a döntéshozatal időtakarékosabbá válhat. A vállalatirányítási rendszerek integrációjához és az abba történő hatékony információbecsatoláshoz szükséges a folyamatalapú gondolkodásmód, hiszen a megfelelő mérőszámokat és adatokat a rendszer csak úgy tudja feldolgozni, ha azok értelmezhető tevékenységek eredményeképp születtek és számszerűsítve kerültek az adatbázisba. A betáplálás alatt természetesen a legtöbb esetben automatizált folyamatot kell érteni, amelyet a rendszer szintén automatizált módon kezel, és teszi azt értelmezhető eredménytermékké a menedzsment számára.

Az automatizált munkafolyamatokat támogató szemléletmódban informatikai irányú fejlesztések és az elektronikus nyilvántartások bevezetésének és üzemeltetésének, valamint további fejlesztésének elősegítése. A folyamatmenedzsment-elveket figyelembe véve az informatikai fejlesztések tekintetében az időtényező játszik kulcsszerepet, ugyanis amennyiben a közvetlen értéket nem teremtő melléktevékenységekre (például mentett fájlok felkutatása, manuális rendszerezés) fordított idő csökkenthető, úgy a szervezet szemszögéből a legértékesebb erőforrás szabadítható fel és csoportosítható át más területekre, mint például a kutatás-fejlesztés, optimalizálás vagy az ellenőrzés. Az erőforrás-allokációt tekintve az időmenedzsment, valamint az időhatékonyság az egyik legjelentősebb erővel bíró tényező, amelynek hasznosítása a magánbiztonsági szektor szolgáltatásalapú piacán rendkívüli előnyt jelenthet a piaci versenyben. Az egyes tevékenységekre fordított részidő csökkentése mellett az informatikai irányú fejlesztések a menedzsmentfunkciók egyik részhalmazát, az ellenőrzést képesek nagymértékben támogatni. Az egyes rendszerek működéséhez az egyértelműen deklarált kontrollpontok szerinti információval szolgáló bemenetek felhasználhatók lesznek a kitűzött cél eléréséhez.

Mesterséges intelligencia folyamatokba történő integrálása, hiszen a jelenleg úttörőnek számító technológiai trend adta lehetőségek felfedezése és alkalmazása rendkívül fontos a piaci versenyelőny elérése és megtartása céljából. A mesterséges intelligencia alapjaiban fogja reformálni a piaci körülményeket, technológiai versenyre sarkallva ezzel a szervezeteket. A jelenlegi folyamatok átdolgozása borítékolható, ha a mesterséges intelligencia széleskörűen elterjed a magánbiztonsági szektorban, hiszen az jelentős felelősség- és szerepkörbéli átrendeződést tartogat. A lehetőségek kapcsán fontos, hogy a piacon érdekelt szereplők mihamarabb reagáljanak és előkészítsék a folyamataikat a technológia adta lehetőségek befogadására és mindennapi alkalmazására. A technológia lehetőséget ad a magánbiztonsági szektornak arra, hogy ne csupán felzárkóztassa magát a szervezeti hierarchiában

magasabban szereplő egyéb szervezeti egységekhez, hanem a helyzet kihasználásával az újonnan kialakuló elvárásoknak más szervezeti egységekkel együtt, közös egységként feleljenek meg.

Fontos, hogy az eddigi lemaradás és technológia pótlására ne használjunk túl sok erőforrást, hiszen az eltereli a fókuszt az igazán jelentős fejlődési lehetőségekről (mesterséges intelligencia), aminek következtében a fejlődés elmaradhat az adottságok alapján lehetséges mértéktől.

Felhasznált irodalom

Ambrus Tibor – Lengyel László (2011): *Humán controlling eszközök a gyakorlatban*. Budapest: Wolters Kluwer.

Bernáth Lajos (2021): Folyamatmenedzsment. *Tudományos és Műszaki Tájékoztatás,* 68(1), 1–11. Online: https://journals.bme.hu/tmt/article/view/36312

Fenyvesi Csaba (2013): A kriminalisztika alapkérdései. In *Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról.* Pécsi Határőr Tudományos Közlemények XIV. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, 341–349. Online: https://pecshor.hu/periodika/XIV/fenyvesics.pdf

Horváth Zsolt – Szlávik Péter (2011): Vállalati integrált kockázatkezelés II. *Minőség és Megbízhatóság,* 45(4), 219–226.

Kiss Imre (1987): *Az informatika alapjai.* Budapest: Tankönyvkiadó.

Kvalikon Vezetési Tanácsadó és Rendszerfejlesztő Kft. Online: www.kvalikon.hu/folyamatmenedzsment/rendszer-kialakitas.php

László Gábor (2014): *Kockázatértékelés, kockázatmenedzsment.* Budapest: NKE. Online: https://oszkdk.oszk.hu/DRJ/13248

Michelberger Pál (2024): *Fejezetek a vállalati biztonságmenedzsmentből: Információ-, folyamat- és vállalatbiztonság.* Budapest: Akadémiai. Online: https://doi.org/10.1556/9789634549376

Michelberger Pál – Horváth Zsolt (2017): Biztonságorientált folyamatmenedzsment. *International Journal of Engineering and Management Sciences,* 2(4), 344–364. Online: https://doi.org/10.21791/IJEMS.2017.4.28.

Pénzügyminisztérium (2021): *Kézikönyv a köztulajdonban álló gazdasági társaságok részére a belső kontrollrendszer kialakításához és működtetéséhez.* Budapest: Pénzügyminisztérium. Online: https://allamhaztartas.kormany.hu/download/8/f9/b2000/Gtbkr_kézikönyv_2021.pdf

Szabó Gergely (2017): Mit értünk know-how alatt? *Kocsis és Szabó Ügyvédi Iroda*. Online: https://kocsisszabougyved.hu/mit-ertunk-know-alatt/

Tenner, Arthur R. – De Toro, Irving J. (1998): *BPR. Vállalati folyamatok újraformálása.* Budapest: Műszaki Könyvkiadó.

Tóth Gábor (2016): *Tudásanyag: A folyamatok kialakítása és újjászervezése.* Online: https://multibridge.hu/multibridge/cikk/a_folyamatok_kialakitasa_es_ujjaszervezese/

Tóth Levente (2018): A komplex objektumvédelem kihívásai napjainkban. *Bolyai Szemle,* 27(1), 35–44. Online: https://szakmaikamara.hu/files/images/Orszagos/Szakmai_Kollegium/publikaciok/Bolyai_Szemle_2018_01_toth-levente.pdf

Varga-Polyák Csilla (2014): *Közigazgatási szervek működési folyamatai.* Budapest: NKE. Online: http://hdl.handle.net/20.500.12944/10538

ABSTRACT

Process Management in the Field of Physical Security

Soma TAKÁCS – Attila TÓTH

The aim of the publication is to present the effectiveness of process management activities among private security market players and their integration into the organisational level process management system. The research will present the professional logics identified and their manifestation in the activity. It is easy for the creation, operation and development of physical security embedded in organisational strategy to be forgotten in strategic decision-making in organisations. It is essential for companies to recognise the importance of physical security at strategic level and to prioritise its integration into the organisational structure accordingly. The strategy includes the definition of physical security objectives and policies, and the appointment of responsible persons to implement and supervise the process in accordance with these policies and professional logics. The application of a process management system will lead to better transparency, orderliness and thus more efficient operations for the professional areas and the organisation. In addition, the integration of processes allows for continuous monitoring and improvements following the examination of discrepancies detected during the audit, thus ensuring the flexibility of the organisation to adapt to market conditions.

To meet these requirements, it is essential to integrate physical security processes into organisational-level process management, which also enables effective monitoring and management of the activity. An integrated approach contributes significantly to the long-term effective operation of the organisation and to maintaining its competitiveness in the market.

Keywords: *process management, physical security, risk management, strategy, artificial intelligence*