DOI: 10.38146/BSZ.2023.2.8

Humán kockázatok hálózatkutatási szempontból

Human risks in network research context

Kemendi Ágnes
doktorandusz
Óbudai Egyetem,
Biztonság- és Biztonságtudományi Doktori Iskola
kemendi.agnes@uni-obuda.hu

Absztrakt

Cél: A hálózatok értelmezhetők a vállalati folyamatok kontextusában, melyek a vállalati „gépi" és a humán erőforrásokon keresztül valósulnak meg. A humán tőke nemzetgazdasági szinten alapvető szerepet játszik. Az emberi tényező a szervezeti működés valamennyi szintjén megjelenik. A folyamatlépések és a kontrolltevékenységek végrehajtásához is kapcsolódik emberi tényező. Meghatározó kérdés, hogy a biztonságos szervezeti működés az emberi tényező oldaláról hogyan biztosítható a folyamatosan változó üzleti környezetben, illetve nem várt események (lásd pandémia) esetén. A kutatás célja bemutatni, hogy a vállalati folyamatok hálózatkutatási aspektusból értelmezhetők; feltárni a hálózatok szerepét a vállalati folyamatokban, ismertetni az emberi tényezőhöz kapcsolódó kockázatokat a vállalati folyamatokban, és értelmezni a vállalati folyamatokban rejlő kockázatok és azok működésének biztonságát segítő kontrollok közötti összefüggéseket.

Módszertan: A publikáció a vállalati belső kontrollrendszer kontextusában hálózatkutatási eszközökkel vizsgálja az emberi tényező vállalati biztonságban betöltött szerepét. A publikáció a bevételi folyamat kontrollhálózatát esettanulmány jelleggel elemzi és tárja fel a folyamathoz rendelt kontrollokat, a kapcsolódó emberi tényezőt, valamint emberi kockázatokat.

Megállapítások: A vállalati folyamatokba épített kontrollok hálózatán keresztül a vállalat a kockázati tűréshatárának megfelelő biztonsági szintet tud megvalósítani, mely biztonság értéket jelent, és az a hosszú távú sikeres működéshez nélkülözhetetlen. A rendszerek biztonsági hálója az emberi tényező kockázatainak egyidejű kezelésével lesz kellőképp erős. Szükséges, hogy a vállalati biztonsági kultúra, a vezetői szinteken munkavállalók felé közvetített értékrend

és a kontrolltudatos szemlélet képes legyen a kontrollkörnyezet és vállalati integritás erősítésére.
Érték: A mai agilis üzleti környezethez való adaptációhoz szorosan kapcsolódik a hálózatos szervezeti felépítés felé történő elmozdulás és a vállalati folyamatok folyamatcentrikus átrendezése. A vállalati folyamatok folyamatcentrikus szemlélete és kezelése révén folyamatláncok jelennek meg, amelyek alkotó folyamatok hálózataként értelmezhetők. A folyamatokhoz kontroll és ellenőrzési tevékenységeket kell rendelni, melyek sikeres megvalósulása a kívánt biztonsági szint elérését segítik. A biztonságos szervezeti működés értéket jelent. A folyamatokban részt vevő emberi tényező változó arányban mindig jelen lesz, ezért szükséges az emberi tényezőhöz kapcsolódó kockázatok azonosítása és kezelése.

Kulcsszavak: humán kockázatok, kontrollok hálózata, vállalati biztonsági háló, biztonsági kultúra

Abstract
Aim: Networks can be interpreted in the context of corporate processes, which are implemented through "machines" and human resources. Human capital plays a fundamental role in the economy. The human factor appears at all levels of an organization. Human resources form part of process steps and control activities. It is a significant question how to ensure the safe organizational operation from human resources' perspective in the constantly changing business environment, resp. in case of unforeseen events (e.g., pandemic). The aim of the research is to demonstrate that corporate processes can be interpreted from a network research aspect, to explore the role of networks in corporate processes, to describe the risks associated with the human factor in corporate processes, and to understand the relationships between corporate risks and controls.
Methodology: The publication examines the role of the human factor in safety using network research tools in the context of the company's internal control system. The publication analyses the control network of the revenue process in case study form and explores the controls assigned to the process, the associated human factor, and human risks.
Findings: Through the network of controls built into corporate processes, the company can achieve a level of security that meets its risk tolerance, which security is a value that is essential for long-term success. The safety net of systems will be strong enough if it addresses simultaneously the risks of the human factor. It is necessary that the corporate security culture, the values represented by top management to employees and the control-conscious approach can strengthen the control environment and corporate integrity.

Value: Adapting to today's agile business environment calls to move towards a network organizational structure, and to rearrange corporate processes in a process-centric manner. Through the process-centric approach and -management of enterprise processes, process chains are created that can be interpreted as network of processes. Control activities shall be assigned to the processes, their successful implementation will help to achieve the desired level of security. Secure organizational operations mean value. The human factor involved in the processes will always be present in varying proportions; therefore, it is necessary to identify and manage the risks associated with the human factor.

Keywords: human risks; network of controls; corporate safety-net; security culture

Bevezetés

Az ipar 4.0 és 5.0 által hozott technológiai innovációk mellett a „hálózatosodás" jelensége is dominánssá válik. A hálózatok mindennapjaink részévé váltak. A „hálózatosodás" megjelenik a vállalati folyamatokban, beleértve a biztonsági szempontokat is. Mindez stratégiai szinten kezelendő kiemelt biztonsági és védelmi témát jelent a hosszú távú vállalati sikeresség érdekében. Az emberi tőke, az emberi erőforrás, valamint az emberi tényező gazdasági szempontból kiemelt jelentőségű, és a vállalati célok megvalósulását segíti. Az emberi kapcsolatok hálózata és a folyamatokban részt vevő emberi tényező a vállalati folyamatok hálózatába ékelődve kulcsterületeket jelentenek a vállalati védelmi hálóban.

A humán kockázatok jelen vannak a vállalati folyamatokban és rendszerekben, ennek megfelelően a kockázatkezelés szerepe döntő jelentőségű. A megváltozott üzleti környezetben szükséges, hogy a vállalat felkészült legyen az információs és kommunikációs technológiához (továbbiakban: IKT) köthető kockázatok kezelésére, beleértve az IKT kockázatok emberi oldalát, a szervezeti működés szempontjából az emberi tényező potenciális hibaforrásként történő kezelését, továbbá az előre nem látható természeti események vagy pandémia hatásainak kezelését a biztonságos szervezeti működés érdekében. A kívánt biztonsági szint elérését kontrolltevékenységek (röviden kontrollok) működtetése segíti elő, amelyek biztosítják, hogy a folyamat hibamentesen, illetve adott elfogadható tűréshatáron belüli hibaszázalékkal következik be. A publikáció hálózatkutatási szemléletet alkalmazva áttekintést ad a szervezetben jelen lévő humán kockázatokról, kiemelt szereppel kezeli a bizalom fogalma köré épülő

úgynevezett „hitelességi kockázatokat", javaslatot tesz a kockázatok integrált kezelésére, ismertetve azt, hogy a kontrollok értéket jelentenek a vállalatnak.

A kutatás ismertetése

Kutatási célok

A vállalati működést meghatározó korlátok (idő, pénz, erőforrás) közül az emberi erőforrással (továbbiakban: HR) kapcsolatos „korlátok" megjelennek a biztonságos működés kontextusában is. Kérdés, hogy mely tényezők, a folyamatok és a kontrollok milyen hálózata segíti a biztonságos szervezeti működést HR oldalról a folyamatosan változó üzleti környezetben, illetve nem várt események (lásd pandémia) esetén, hogy a szervezetek folyamatos, nagy kiesés nélküli működése biztosított legyen. *„Hálózatok mindenhol vannak"* (Barabási, 2006). A hálózatelemzés a vállalati belső és külső struktúrákra is alkalmazható. A hálózatok több vonatkozásban is adaptálhatók a vállalati folyamatokra az üzleti életben. Hálózatot alkotnak a vállalatok és vevők, banki utalások, szállítási rendszerek, a vállalati folyamatok, a folyamatot képező folyamatlépések, de egy projekt is.

A kutatás célja bemutatni, hogy a vállalati folyamatok hálózatkutatási aspektusból értelmezhetők, feltárni a hálózatok szerepét a vállalati folyamatokban, ismertetni az emberi tényezőhöz kapcsolódó kockázatokat a vállalati folyamatokban, és értelmezni a vállalati folyamatokban rejlő kockázatok és azok működésének biztonságát segítő kontrollok közötti összefüggéseket.

Kutatási probléma

A vállalati folyamatok, a rendszerek és az emberi tényező együttese tulajdonképpen egy komplex hálózatként is értelmezhető. A vállalati folyamatok működése egymásra épülő és egymáshoz kapcsolódó folyamatlépések sorozatán keresztül valósul meg, és létrejön a folyamat produktuma, legyen az egy termék vagy szolgáltatás a belső vagy külső „vevők" felé. Egy adott vállalati folyamat gépesítettségétől, illetve automatizáltságától függően a folyamatban részt vevő „gépi", illetve humán erőforrás aránya változó. A mesterséges intelligencia és gépi tanulás térnyerése már laikusok számára is egyre nyilvánvalóbb, azonban a humán tényező részvétele a folyamatokban mindig jelen lesz. A humán tényező részvétele különböző mértékben valamennyi folyamathoz kapcsolódik. A folyamatok biztonságos működése szempontjából mind a „gépi", mind az

emberi tényezőben rejlő kockázatokat kezelni és kontrollálni szükséges. A belső kontrollrendszer a kontrollokra vonatkozóan mutatja, hogy milyen a „biztonsági kultúra” a szervezetben.

Kutatási módszertan

A publikáció az emberi tényező vállalati biztonságban betöltött szerepét vizsgálja hálózatkutatási eszközökkel, a vállalati belső kontrollrendszer kontextusában. A hálózatok absztrakt dolgokat is leírhatnak, mint például egy személy és egy feladat kapcsolata (Temesi-Varró, 2017). A folyamattevékenységek megvalósítása optimális esetben hibamentesen, illetve adott tűréshatáron belüli hibaszázalékkal hozza létre a kívánt végterméket, azaz terméket vagy szolgáltatást. Ahhoz, hogy mindez megvalósuljon, szükséges a kockázatok kezelése, mely a kockázatkezelési folyamaton keresztül történik. A kockázatok ismeretében a szükséges kontrolltevékenységeket kell meghatározni. A kontrollok lehetnek automatikus, manuális vagy félautomatikus megoldások is. A kontrollok elősegítik, hogy a tevékenységek elfogadható kockázattal működhessenek.

A hálózattudomány matematikai módszere

A hálózattudomány eszköze a gráfelmélet, melyet a hálózattudomány matematikai módszerként felhasznál. A gráfelmélet gyökerei az Euler-féle königsbergi hidak problémájához nyúlnak vissza, mely a következő volt: hét híd ívelt át a városon átmenő folyón, a folyó két szigetét is érintve. A kérdés az volt, hogy végig lehet-e menni az összes hídon úgy, hogy minden hídon csak egyszer mennek át, és visszatérnek a kiindulópontba. A gráf csúcsai a szárazföldi részeken találhatók, míg a hidak az élek. Euler bizonyította, hogy ez lehetetlen, mert a gráfban egy pontnak öt, és három pontnak három a fokszáma. Akkor és csak akkor létezne megoldás, ha minden csomópont fokszáma páros lenne (Euler, 1741).

Egy gráfot szimbólumok két halmaza definiál, ezek elemeit csúcsoknak, illetve éleknek hívjuk. Az él egy csúcspontokból álló rendezett pár, amely megadja a két csúcspont közötti mozgás vagy áramlás lehetséges irányát (Winston, 2003).

A hálózati modellezés

Véletlen hálózatok modelljeit Erdős és Rényi (1959); (1960), illetve velük egyidejűleg és függetlenül Edgar Gilbert (1959) állították fel. Az Erdős–Rényi

modellként is ismert (1959) modell a hálózatok véletlenszerűségén alapul, minden él p valószínűséggel következik be, nagyságrendileg ugyanannyi él tartozik a csúcsokhoz, azaz kb. ugyanannyi a fokszáma. A véletlen hálózatok fokszámeloszlása egy haranggörbét követ.

A véletlen hálózatok modellje a való életben jellemző hálózatokra reálisan nem adaptálható. A valódi hálózatok más jellegűek, két pont nem ugyanakkora valószínűséggel kerül egymással kapcsolatba, hanem gyakran egy-egy csomópont köré igazodnak a hálózatok, és a fokszámok eloszlása nem egyenletes.

Az emberi kapcsolatok esetében tapasztalható, hogy egy-egy ember nagy ismeretségi körrel rendelkezik, míg mások szűk ismeretségi körrel rendelkeznek, tehát az Erdős–Rényi modell szerinti Poisson-eloszlással nem írhatók le.

A skálafüggetlen hálózat hatványfüggvény szerinti fokszámeloszlása azt jelzi előre, hogy a legtöbb pontnak csak kevés kapcsolata van, amelyet néhány, nagy összekötöttséggel rendelkező középpont tart össze (Barabási & Albert, 1999). A hálózatokat hagyományosan statikusnak szemlélték, a modellező helyezi el állandó számú csomópont között úgy a kapcsolatokat, hogy az eredményként létrejövő hálózat hasonlóan nézzen ki, mint a hálózat, amelyet modellezni kívánunk. A skálafüggetlen modell a hálózatot dinamikus rendszernek tekinti. A dinamikus hálózat önállóan áll össze, és csomópontok, valamint kapcsolatok hozzáadása és eltávolítása által alakul ki az időben (Barabási, 2006).

Belső kontrollok hálózata

Az IKT rendszerek képet adnak a vállalati folyamatokról, behálózzák a szervezet működését. Analóg módon az emberi tényező is a szervezeti működés valamennyi szintjén megjelenik, a felsővezetés és az operatív munkafolyamatokat végző munkavállalók, illetve a munkaerő szintjén is. A vezetőség „hangja” és a képviselt értékrend beépül a szervezet mindennapi működésébe, meghatározzák a szervezeti kultúrát és a kontrollfolyamatok sikerességét is.

A rendszerek biztonsági hálója az emberi tényező kockázatainak egyidejű kezelésével lesz kellőképp erős. A vállalati biztonsági kultúra célként is értelmezhető, mely a biztonsági kockázatokat „lefedő”, azokat kezelő kontrollokon keresztül valósul meg. Ez a biztonsági kultúra a vállalati reputációban és a brandben is megjelenik. A vállalatközi kommunikáció és a tranzakciók során a vállalat az üzleti partnerekhez, vevőhöz, beszállítókhoz, illetve szabályozó testületekhez is kapcsolódik. Mindez a vállalat kapcsolati hálózatát írja le.

Hálózatkutatási kontextusban lehetnek a csomópontok az emberek, az élek a folyamattevékenységek, egy-egy folyamat egy-egy eleme, mellyel az emberi

kapcsolati háló írható le; értelmezhető a tevékenységek és a tevékenységek közötti logikai kapcsolat által leírt hálózat is. Ez utóbbi esetben a folyamattevékenységek kapcsolati hálózata írható le: az egyes folyamattevékenységek a csomópontok, ahol az emberek és gépek az erőforrások, és a tevékenységek közötti logikai kapcsolatok az élek.

A vállalati folyamatok egymáshoz kapcsolódó lépések láncolatai, nélkülözhetetlen a különféle folyamatok összekapcsolódása. A hatásos és biztonságos szinten történő működéshez szükséges többek között a munkafolyamatok összhangja, a vállalati funkciókat képviselő emberek közötti együttműködés és transzparencia. Szükséges látni a folyamatok közötti összefüggéseket, mely segíthet kiküszöbölni bizonyos hibák, illetve biztonsági események előfordulásának valószínűségét. A vállalati folyamatok között összefüggés, „átadás" és visszacsatolás van. A jól tervezett, működtetett és dokumentált folyamatok esetében szinergia érhető el, mert csökken a felesleges és ezáltal kiküszöbölhető átadás-átvételek, azaz kapcsolatok száma, mely csökkenti a felmerülő idő-, pénz- és energiaráfordításokat.

A kívánt biztonsági szint elérése érdekében szükséges a folyamatok hálózatában gondolkodni, és az összefüggéseket holisztikusan szemlélni. A folyamatok biztonságos működéséhez kockázatkezelés szükséges. A kontrollfunkció működése akkor valósul meg legcélravezetőbben, ha az a munkafolyamatok elválaszthatatlan részeként valósul meg.

A munkafolyamatba épített kontrollok a vállalati folyamatok hálózatának szerves részét képezik. A rendszeres ellenőrzés és monitoring a folyamatok tervezett, illetve operatív működéséről adnak visszaigazolást, mely alapján a szükséges preventív, detektív, illetve korrektív tevékenységek meghatározhatók. A kontrolling funkció pedig pénzügyi szinten járul hozzá a működési folyamatok tervezéséhez, megvalósulásához, és financiális oldalról validálja a vállalati folyamatokat. Pénzügyi aspektusa valamennyi vállalati folyamatnak van. A kontrolling funkció része a szervezeti folyamatoknak.

A vállalati védelmi vonalak – üzleti folyamatokba ágyazott kontrollok, kontroll- és megfelelési funkciók és külső/belső auditok (IIA, 2020) – a vállalati működés valamennyi szintjén megjelennek. A belső kontrollrendszer egyes elemei – a kontrollkörnyezet, kockázatértékelés, kontrollok, információs és kommunikációs folyamat és monitoring (COSO, 2004) – a szervezetet átfogó, hálózatszerű struktúrában jelennek meg. A COSO kocka megjeleníti a stratégiai, megfelelési, riporting és operatív kockázatokat, a vállalati belső kontrollrendszer elemeit, illetve az egyes szervezeti egységeket. A COSO kocka rámutat az egyes elemei közötti kapcsolatokra, a belső kontrollrendszer komplexitására. A COSO kocka szerkezete és logikai összefüggései megerősítik, hogy a belső

kontrollrendszerről érdemes hálózatkutatási szemszögből gondolkodni, és hálózati kapcsolatokat értelmezni.

Esettanulmány – a bevételszerzési folyamat kontrollhálózata

A vállalati folyamatok közül (Pi) a bevételszerzési folyamat (P1) sikeressége a vállalat sikerességének kulcsa. A következőkben a bevételszerzési folyamat főbb lépéseit és a kapcsolódó kontrollokat (CA) ismertetem egy fiktív vállalat példáján. Az esettanulmány kontrolltevékenységeinek összeállításához Rao (2014) munkáját használtam fel.

A folyamat gépi és emberi közreműködéssel valósul meg, és változó arányban tartalmaz automatikus, manuális és félig automatikus tevékenységeket.

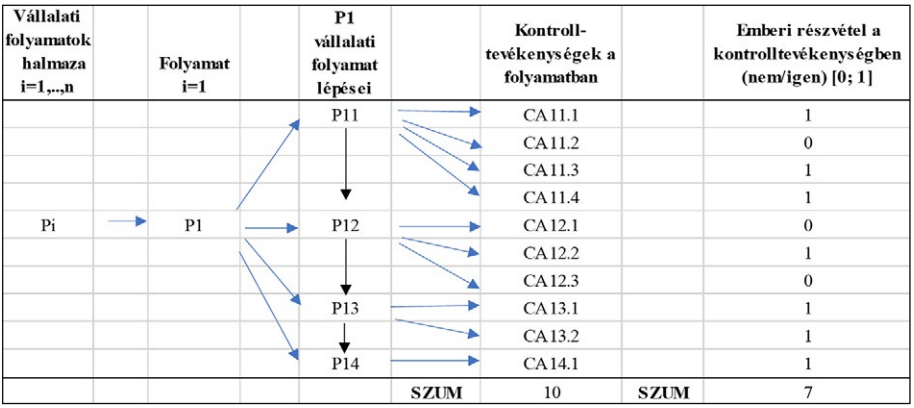
P11: A bevételszerzési folyamat (P1) a rendelésfelvétellel indul. A rendelésfelvételhez kontrolltevékenységek kapcsolódnak: a rendelési adatok ellenőrzésre kerülnek, nem teljes vagy nem pontos rendelési adatok esetén azokat pótolni szükséges (CA11.1). Rendszer általi ellenőrzés történik a duplikált rendelésfelvétel megakadályozása érdekében (CA11.2). A rendelések feldolgozása jóváhagyott hitelkereten belül történik (CA11.3). Magasabb diszkontráták esetén külön független ellenőrzés történik (CA11.4).

P12: Sikeres rendelésfelvételt követően kerül sor a számlázásra. A számlázáshoz kontrolltevékenységek kapcsolódnak: a szállítmány jóváhagyott kiadása alapján a raktárból, a rendszer automatikusan generálja a számlát azonos dátummal (CA12.1). A szállítási dátum nem módosítható megfelelő szintű vezetői jóváhagyás nélkül (CA12.2). Rendszerbeállítás alapján a számlaadatok ellenőrzése a törzsadatok és a megrendelésadatok alapján. Nem valid adatok elutasításra kerülnek vagy egy függő tételeket tartalmazó file-ba, mely később korrigálható (CA12.3).

P13: A számlázást követően kerül sor a pénzbeszedési folyamatlépésre. A pénzbeszedéshez kontrolltevékenységek kapcsolódnak: a vezető ellenőrzi a koros követeléseket és összehasonlítja a beérkezett kintlévőségeket a periódus elején nyitott követelésekkel (CA13.1). A beérkező pénz ügyfélszámlához rendelése az ügyfélnév, az ügyfélszám és a számlaszám alapján történik, és csak nyitott számlákkal szemben (CA13.2).

P14: Az értékesítést követően visszaküldésre is sor kerülhet. A visszaküldött áru fizikai ellenőrzése, felülvizsgálata és a visszáru engedély (RMA – return merchandise authorization) jóváhagyása szükséges (CA14.1).

1. számú ábra: *Kontrollok a bevételszerzési folyamatban*



Vállalati folyamatok halmaza i=1,..,n	Folyamat i=1	P1 vállalati folyamat lépései	Kontroll-tevékenységek a folyamatban	Emberi részvétel a kontrolltevékenységben (nem/igen) [0; 1]
		P11	CA11.1	1
			CA11.2	0
			CA11.3	1
			CA11.4	1
Pi	P1	P12	CA12.1	0
			CA12.2	1
			CA12.3	0
		P13	CA13.1	1
			CA13.2	1
		P14	CA14.1	1
		SZUM	10	SZUM 7

Forrás: Az ábrát a szerző készítette.

Az 1. számú ábraa vállalati folyamatok halmazából (Pi) a vállalati bevételszerzési folyamathoz (P1) rendelten jeleníti meg a folyamathoz rendelt kontrollokat, melyek a kockázatok értékelése során beazonosított kockázatok kezelését biztosítják.

A P1 folyamat alfolyamatai (P11, P12, P13 és P14) részben „gépi", részben manuális, emberi munkaerő segítségével valósulnak meg. Egyes folyamatlépések és hozzájuk kapcsolódó kontrolltevékenységek automatikus, manuális és félig automatikus, félig manuális folyamatlépésekből épülnek fel. A kontrolltevékenységek jellemzően rendszer által támogatott, tipikus kontrolltevékenységek, azonban domináns az emberi tényező részvétele is a kontrolltevékenységekben. A vizsgált esetben 70%-ban volt jelen emberi részvétel a folyamathoz rendelt kontrolltevékenységekben. A „gépi" részvétel, a rendszerek által végrehajtott megoldások jellemzők és preferáltak, azonban a humán faktor részvétele a folyamatokban ennek ellenére mégis meghatározó. Mind a „gépi", mind az emberi tényező részvétele a folyamatokban kockázatokat hordoz, melyek sikeres kezelése a folyamatok biztonságos működéséhez szükséges.

A kockázatkezelés szükséges a biztonságos, kellőképp kontrollált vállalat megteremtése érdekében. Szorosan kapcsolódva a kockázatkezelési feladatokhoz a lehetséges kontrollok közül meg kell határozni, hogy a vállalat mely kontrollokat alkalmazza.

A folyamatokhoz rendelt kontrollok hálózata tulajdonképpen a belső kontrollrendszer megvalósulása a vállalati folyamatokban.

A vállalat működéséhez kapcsolódóan az összes vállalati folyamatot át kell tekinteni, meghatározni a kockázatokat és kontrolltevékenységeket a vállalat

kockázattűrő képességével összhangban. Egyes kontrollok több folyamatlépéshez kapcsolódóan is bizonyosságot nyújtanak.

A magas fokú kontrolltudatosság esetén a kontrollok számossága magas, mely magas szintű biztonsági kultúrát jelez, ahol a reziduális kockázat – a kockázat, mely a kontrollok működése mellett marad – alacsony. Analóg a kockázat, amely a kontrollok jelenléte nélkül tapasztalható magas marad, megfelelő kontrollok hiányában. Leegyszerűsítve, a kontrollok számossága korrelál a biztonsági szinttel. A kontrollfolyamatokat időről időre át kell értékelni, hogy megfelelő védelmet nyújtanak-e, illetve amennyiben változás tapasztalható a kontrollkörnyezetben, például pandémia.

A vállalati folyamatokba épített kontrollokon keresztül a vállalat értéket realizál, mely hozzájárul az átlátható, eredményes és hatékony folyamatokhoz, a minőségcélok megvalósításához, valamint segíti a vállalat alkalmazkodóképességét is.

Humán kockázatok átfogó áttekintése a szervezetben

A humán kockázatok a szervezetben több szinten vannak jelen, melyek megfelelő működés esetén hatásos kockázatkezeléssel párosulva csak marginális kockázatot hordoznak. Mindazonáltal a vállalati kultúra, és ennek részeként a szervezeti biztonsági kultúra átfogóan jelen vannak a vállalati folyamatokban. Mindez az operatív folyamatok szintjén jellemzően áttételesen jelenik meg, de a szervezet egészét tekintve meghatározó. Amikor folyamatokat vizsgálunk azért, hogy azonosítsuk, hogy az a folyamat miért nem működik rendesen, illetve valamely hiba miért következett be, a gyökérok elemzés során az azonosított kiváltó okok és összefüggések tudnak rávilágítani ezekre az áttételes kapcsolatokra és összefüggésekre is. A humán kockázatokat ezért átfogóan ismertetem, mert azok jellegükből adódóan hatással lehetnek a vállalati működésre, annak folyamataira stratégiai és operatív szinten is.

A humán erőforráshoz kapcsolódó kockázatokat a következő szempontok szerint ismertetem (lásd 2. számú ábra):

- Kompetencia.
- Üzletmenet-folytonosság.
- Biztonsági incidensek, véletlen hibák.
- „Hitelességi kockázat”, svájci sajt modell.
- Információbiztonsági kockázat.
- Megváltozott körülményekkel kapcsolatos kockázatok, pandémia, előre nem látható természeti jelenség.
- Vállalati biztonsági kultúra.

Kompetenciakockázat

A vállalati stratégia emberi erőforrás oldalát vizsgálva elsődleges, hogy a működéshez szükséges szakértelem és tudás a kellő időben és helyen rendelkezésre álljon. A kompetencia kérdésköre kiemelt kockázati területet fed le. Lényeges kockázat, hogy a munkatársak nem képesek az irányítási követelmények szerint ellátni feladataikat, melynek fő kockázati tényezői között szerepel a szakértelem hiánya; a munkatársak nem ismerik az eljárásokat és a végrehajtási követelményeket, illetve a változó szakmai készségkövetelmények (Iványos, 2020). Az emberi erőforrás folyamatokkal – azaz a HR-, az emberek irányítási (people management) és teljesítményértékelési (performance management) folyamatokkal – szemben ugyanakkor alapkövetelmény, hogy azok képesek legyenek a kompetenciakockázat kezelésére, ellenkező esetben a felelős személyek nem rendelkeznek megfelelő kompetenciával. A csoportvezetői munkásséghoz szaktudás („hard", azaz kemény képességek), illetve irányítási képességek („soft", azaz puha tényezők) szükségesek. A HR stratégia meghatározó jelentőségű, annak vállalati szintű stratégia részeként történő integrált kezelése elősegíti, hogy az emberi erőforrás a szükséges helyen, időben, „mennyiségben" és minőségben rendelkezésre álljon.

A kompetencia kérdésköre több szinten jelenik meg a vállalati működés során. A feladat végrehajtásához szükséges idő függ az operatív feladatot végrehajtó egyén feladatvégzésben megszerzett rutinjától. Azonos szakmai kompetenciával rendelkező egyének kompetencia szintje eltérő lehet, ami azt eredményezi, hogy egy adott feladat végrehajtásának ideje eltérő lehet attól függően ki végzi a feladatot (Szilágyi, 2015). Ezzel párhuzamosan az elvégzett feladat minősége sem minden esetben sztenderd. Egységes, sztenderd produktumot előállító gyártási folyamat végterméke közelítőleg állandó, míg tanácsadási területen szakértő függvényében más lehet a kimenetel, az output. A minőség és a ráfordított idő fordított arányt mutat, attól függően milyen szinten áll a feladatot végző szakmai tapasztalata, gyakorlata, „rutinja" az adott tevékenység vonatkozásában.

Üzletmenet-folytonosság

Az üzletmenet-folytonosság biztosítása szükséges a humán erőforrás távozása, illetve szabadsága esetén is (Kemendi, 2021a). A vállalati folyamatok szabályozása és a dokumentumkezelési folyamatok átláthatósága a vállalat rezilienciájának megteremtését segíti. A vállalati folyamatok egy adott egyéntől függetlenül is végbe kell, hogy menjenek. Az üzletmenet-folytonosság biztosításának elve egyetemlegesen jelenik meg a vállalati működés során.

Biztonsági incidensek, véletlen hibák

A vállalati működés során bekövetkező biztonsági incidensek jelentős része az emberi tényezőköz köthető (Enisa, 2006). A humán faktorok hatásai biztonsági kockázatot jelentenek, melyek mérsékelhetők, többek között az emberi erőforrás, a munkaerő kellő szakmai felkészültsége és naprakészsége, a szervezeti tudás aktív operatív alkalmazása, a humánerőforrás-menedzsment folyamat integritása, és a szervezeti szinten megfogalmazott és alkalmazott etikai elvek intézményesülése által. Mindezek olyan tényezők, melyek a biztonsági kockázatokat mérsékelni képesek (Kemendi, 2021a).

Biztonsági incidensek, véletlen hibák kategóriáján belül a kumulált kockázat, fatális hiba esete külön figyelmet érdemel, mely több, látszólag független biztonsági hiba együttes bekövetkezése folytán fokozott problémát tud okozni, ahogy azt a Reason (1999) által ismertetett svájci sajt modell példája is illusztrálja. Reason az emberi hibák két fontos jellemzőjére mutat rá, hogy hogyan tud a kontrollok ellenére egy incidens bekövetkezni. Az egyik, hogy a legnagyobb hibát gyakran a legjobb emberek követik el. Másodszor pedig: a szerencsétlenségek messze nem véletlenszerűek, hanem visszatérő mintákba esnek. Adott körülmények hasonló hibákat idézhetnek elő, függetlenül az érintett személyektől (Reason, 2000).

Hitelességi kockázat

A hitelességi kockázatok, azaz az olyan kockázatok, melyek a felek megbízhatóságával, integritásával, hitelességével kapcsolatosak (Kemendi, 2021b), a bizalom fogalma köré épülnek. A vállalati bizalmi kultúra elősegíti a folyamatok működését, a folyamatok sebessége nő, a költségek csökkennek (Takácsné & Benedek, 2016), melyet a „bízz, de ellenőrizz" szemlélet jegyében kontrollálni kell. A hitelességi kockázatok szorosan összefonódnak az emberi tényezővel, melyek a működési folyamatokban napi szinten megjelennek. A hitelességi kockázat minimalizálása a szervezeti biztonsági kultúra fejlesztéséhez és erős, etikus szervezeti kultúra kialakításához járul hozzá.

A biztonság szintje olyan erős, mint a leggyengébb láncszem a folyamatban (ENISA, 2006; Schneier, 2003), így a „hitelességi kockázat" kezelése nagyban elősegíti a biztonsági célok megvalósulását. A támadók is a leggyengébb pontot támadják, vegyük például a pszichológiai manipuláció (social engineering) esetét. A pszichológiai manipuláció az emberi faktor gyengeségein alapulva képes „rést ütni a pajzson", azaz a szervezet védelmi rendszerén. A pszichológiai manipuláció az emberi interakciókra támaszkodik, és kihasználja az emberi

természet sajátosságait, hogy az emberek alapvetően segítőkészek és konfliktuskerülők (Hadnagy, 2011; Mitnick, 2002).

A hitelességi kockázaton belül az emberi tényezőre vonatkozóan kiemelt kockázati területet jelent a csalás kockázata, amikor a munkavállalók egyéni érdekei állnak a csalások (fraud) mögött. A csalás esetek kezelése szintén a vállalat biztonsági rendszerének feladata. Az árulkodó jeleket – személyes figyelemfelhívó jegyek, például anyagi szükséglet, tartozások, életstílus, jövedelem különbözőség, munkafolyamatok izolált végrehajtása stb. – a biztonsági rendszernek kell felismernie és kezelnie.

Információbiztonsági kockázat

Az információbiztonsági kockázatok súlyos, illetve kritikus következménnyel is járhatnak, például adatbiztonsági kockázatok, adatvesztés, adatszivárgás, GDPR nem megfelelés, IKT kitettségek. Információbiztonsági alapelvek – titoktartás, sértetlenség, hozzáférhetőség (confidentiality, integrity, availability, azaz CIA) – követése szükséges (Michelberger & Kemendi, 2020).

Megváltozott körülményekkel kapcsolatos kockázatok, pandémia, előre nem látható természeti jelenség

A vállalatoknak a megváltozott körülményekkel kapcsolatos, illetve az előre nem látható kockázatok kezelésére is fel kell készülniük. A COVID–19 pandémia a kockázati környezetre szignifikáns hatást gyakorolt, és még hangsúlyosabbá tette a biztonság kérdését. A változások mintegy láncreakció jelleggel további változásokat indukáltak. Az információbiztonság, illetve kiberbiztonság kérdése még hangsúlyosabbá vált. Az e-kereskedelem térnyerése és vele párhuzamosan az online kereskedelem új kockázatokat hozott. Nőtt a csalással kapcsolatos esetek száma. A munkavállalók mindennapi munkarutinja is érintetté vált (Kemendi, 2021b).

A pandémia esetében nyilvánvaló volt, hogy a biztonság értéket jelent. Változó környezetben a reziliencia, az alkalmazkodóképesség az üzletmenet-folytonosság képességének biztosítását is jelentheti, melynek fontosságát a folyamatos versenyhelyzeteken túl a pandémia is megmutatta.

Az otthoni munkavégzés és a távmunka helyett kapott olyan munkáltatóknál is, ahol korábban az ilyen gyakorlatra nem volt példa (például biztonsági megfontolásokból), illetve jóval kiterjedtebben jelent meg ez a gyakorlat olyan vállalatoknál, ahol a gyakorlat már működött. Az otthoni munkavégzés gyakorlata kiszakította a munkavállalókat a megszokott életükből, ezáltal a munkahelyi

mentálhigiéné területe még fontosabbá vált. Az otthoni munkavégzés eredményeképp a mentális szorongással vagy motivációvesztéssel küzdő munkavállalók száma jelentősen megnőtt. A dolgozók lelki egészségével foglalkozni kell.

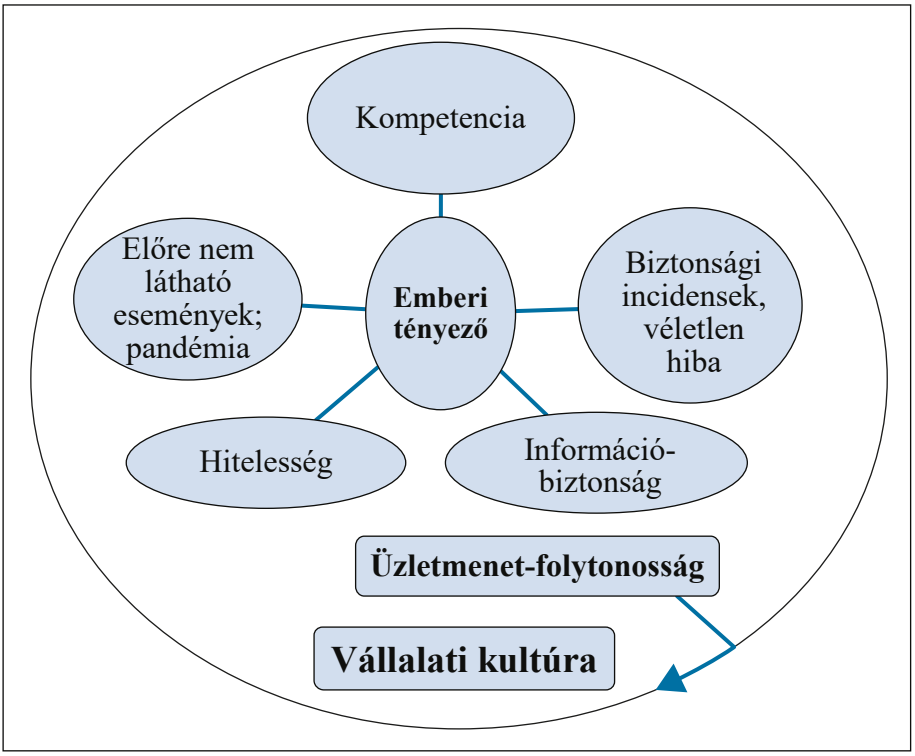
Az új, ismeretlen helyzetek átgondolt változások esetén is kockázatosabbak. A biztonságtudatosság szerepe még inkább meghatározó jelentőségűvé vált. A kockázatkezelés és a kockázattudatos szervezeti kultúra jelentősége még inkább nőtt, melyet a vállalati stratégia részeként lehet hatásosan és eredményesen kezelni.

Vállalati biztonsági kultúra

Szorosan kapcsolódik az egyes kockázati tényezőkhöz, azonban jelentősége miatt külön nevesítem. A vállalati biztonsági kultúra szempontjából a szervezet vezetője (tone of the top) elsődleges szerepet tölt be. A vezető felelőssége az adekvát biztonsági kultúra kialakítása, az értékek megfogalmazása, közvetítése, valamint képviselete az alkalmazottak felé. Az információbiztonsági kultúra is része mindennek, és a felsővezetésnek bizonyítania kell vezetői képességét és elkötelezettségét az információbiztonsági irányítási rendszer (IBIR) vonatkozásában. A vezetői akarat és elkötelezettség a szabályozáson keresztül valósul meg (Magyar Nemzeti Kibervédelmi Intézet, 2019). Fejlett biztonsági kultúra esetén a szervezet dolgozói a biztonságot veszélyeztető tényezőkkel kapcsolatban a szükséges ismereteket elsajátítják és felelősen alkalmazzák (Rajnai, 2017). A vállalatok komplex biztonsági kihívásokkal és kockázatokkal szembesülnek – ideértve az IKT rendszerekhez és az emberi tényezőhöz köthető kockázatokat, továbbá tágabb értelemben a vállalati működéshez kapcsolódó kockázatokat, mint pénzmosás és terrorizmusfinanszírozás kockázata –, amelyek kezeléséhez sikeres, fejlett biztonsági kultúra szükséges.

A 2. számú ábra az üzletmenet során – a folytonos üzletmenet érdekében – az emberi tényezőhöz kapcsolódó kockázatokat – illusztratív jelleggel, szimbolikusan emberként ábrázolva – szemlélteti, és áttekintő jelleggel mutatja be a vállalati biztonsági kultúrát befolyásoló emberi kockázati tényezőket, kiemelve a kompetencia kockázatokat (fej), a hitelesség és információbiztonsági kockázatokat, melyek stabil, folyamatos kezelése alapvető fontosságú a sikeres biztonsági kultúra szempontjából (lábak), illetőleg a váratlan események kockázatait (biztonsági incidensek, véletlen hibák, illetve megváltozott körülményekkel kapcsolatos kockázatok, például pandémia) (kezek), melyeket felmerülésük esetén a vállalati kockázatkezelési szabályzatnak megfelelően adekvát válasszal, cselekvési tervvel szükséges kezelni.

2. számú ábra: *A vállalati biztonsági kultúrát befolyásoló humán kockázatok*



Forrás: Az ábrát a szerző készítette.

Következtetések

A hálózatok által leírható kapcsolatok és összefüggések megjelennek a szervezeti működésben, a vállalati folyamatok rendszerében és kontrollkörnyezetében. A vállalati folyamatok hálózatába épített kontrollok a belső kontrollrendszer megvalósulását jelentik a vállalati gyakorlatban. A kontrolltudatos szervezet magasabb biztonsági szintet ér el. A kockázatkezelés a vállalati folyamatok, illetve a vállalati biztonság megteremtését segíti. A vállalati folyamatokba épített kontrollokon keresztül a vállalat értéket realizál.

A vállalati stratégia, a kockázatkezelés és a vállalati folyamatok integrált kezelése szükséges a hosszú távú sikeres vállalati működés érdekében.

A folyamatok biztonságos működése szempontjából a „gépi" és az emberi tényezőben rejlő kockázatokat kezelni és kontrollálni szükséges. A belső

kontrollrendszer alkalmas a szervezeti „biztonsági kultúra" jellemzésére. A vállalati folyamatok kockázatokat hordoznak, melyeket adott folyamatlépéshez rendelten kontrollokkal kell kezelni.

A folyamatlépések és a kontrolltevékenységek végrehajtásához is kapcsolódik emberi tényező. Szükséges az emberi tényezőben rejlő kockázatok azonosítása és kezelése. A humán kockázatok közé tartoznak többek között a biztonsági incidensek, véletlen hibák, „hitelességi kockázat", információbiztonsági kockázat. A hitelességi kockázat kezelése az erős, stabil vállalati kultúra alapja. A vállalat kockázatkezelési rendszerének képesnek kell lennie a megváltozott körülményekkel kapcsolatos kockázatok kezelésére – lásd pandémia –, mely azonnali alkalmazkodóképességet követel meg. Szükséges, hogy a vállalati kultúra és vele együtt a vállalati biztonsági kultúra olyan értékrendet közvetítsen, mely képes a vállalati integritás és kontrollkörnyezet erősítésére.

Összegzés

A vállalatok komplex biztonsági kihívásokkal szembesülnek az ipar 4.0 technológia intenzív világában. A pandémia, illetve a megváltozott körülményekkel kapcsolatos, előre nem látható kockázatok próbatétel elé állítják a vállalatok védelmi képességét. A biztonság értéket jelent. Kockázatkezelés szükséges a biztonságos, kellőképp kontrollált vállalat megteremtése érdekében. A tudatosan kiépített vállalati biztonsági kultúra, valamint kontrollkörnyezet alkalmasak a vállalat integritásának erősítésére, mely könnyen tud alkalmazkodni a nem várt események esetén is.

A szervezeti működésben és kontrollkörnyezetben a hálózatok által leírható kapcsolatok és összefüggések meghatározók. A folyamatokban részt vevő ember megjelenik a „gépi" tényezők, rendszerek mellett a vállalati működés valamennyi szintjén.

Az emberi tényező kiemelt kockázati tényező a vállalatok biztonsági rendszerében. A vállalati kultúra és a vállalati biztonsági kultúra döntő jelentőségűek a humán erőforráshoz kapcsolódó kockázatok vonatkozásában. Az emberi tényezőt stratégiai és kockázatkezelési szinten adekvát módon és integrált szemlélettel javasolt kezelni. A rendszerek biztonsági hálója az emberi tényező kockázatainak egyidejű kezelésével lesz kellőképp erős.

A vállalati biztonsági kultúra, a vezetői szinteken munkavállalók felé közvetített értékrend és a kontrolltudatos szemlélet a kontrollkörnyezetet erősítik.

A folyamatokhoz rendelt kontrollok hálózata tulajdonképpen a belső kontrollrendszer megvalósulása a vállalati folyamatokban. A kontrollok hálózata

a vállalati kockázati tűréshatárral összhangban segíti a kockázatok kezelését és a kívánt biztonsági szint elérését. A szemléletmód a hosszú távú sikeres vállalati működés szempontjából meghatározó jelentőséggel bír, annak alkalmazását felsővezetői szinten javasolt kiemelt prioritásként kezelni, és stratégiai szintről eredeztetve a mindennapi működésbe tudatosan beépíteni a biztonságtudatosság, a biztonsági kultúra és a vállalati biztonság érdekében.

Felhasznált irodalom

Barabási, A-L. & Albert, R. (1999). Emergence of scaling in random networks. *Science, 286*(5439), 509–512. https://doi.org/10.1126/science.286.5439.509

Barabási A-L. (2006). A hálózatok tudománya: a társadalomtól a webig. *Magyar Tudomány, 167*(11), 1298–1308, http://www.matud.iif.hu/06nov/03.html

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management - Integrated Framework Executive Summary*. https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Erdős, P. & Rényi, A. (1959). On random graphs, I. Publicationes Mathematicae Debrecen, *6*, 290–297. https://snap.stanford.edu/class/cs224w-readings/erdos59random.pdf

Erdős, P. & Rényi, A. (1960). On the evolution of random graphs. Publ. Math. Inst. Hung. Acad., *5*, 17–61. http://snap.stanford.edu/class/cs224w-readings/erdos60random.pdf

Euler, L. (1741). Solutio problematis ad geometriam situs pertinentis Commentarii academiae scientiarum. *Petropolitanae 8*, 128–140. http://eulerarchive.maa.org/docs/originals/E053.pdf

Gilbert, E. N. (1959). „Random Graphs". *Annals of Mathematical Statistics. 30*(4), 1141–1144.

Hadnagy, C. (2011). *Social engineering: The art of human hacking.* Wiley Publishing.

Institute of Internal Auditors (IIA). (2020). *The IIA's three lines model.* https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf

Iványos J. (2020). *Útmutató az integrált kockázatkezelés megvalósításához*. Trusted Business Advisor.

Kemendi, A. (2021a). HR process safety & security in the industry 4.0. era. *Bánki Közlemények 4*(1), 55–60. http://bk.bgk.uni-obuda.hu/index.php/BK/article/view/143

Kemendi. A. (2021b). E-Commerce Safety and Security in the Industry 4.0 era. *National Secretary Review*, (1), 195–217, https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_1_NSR.pdf

Magyar Nemzeti Kibervédelmi Intézet (2019). *Az információbiztonság lélektana* (Psychology of Information Security).

Michelberger, P. & Kemendi, A. (2020). Data, Information and It Security - Software Support for Security Activities. *Problems of Management in the 21st Century, 15*(2), 108–124., https://www.scientiasocialis.lt/pmc/files/pdf/108-124.Michelberger_Vol.15-2_pmc.pdf

Mitnick, K. D. & Simon, W. L. (2002). *Art of depiction: Controlling the human element of security*. Wiley Publishing.

Rajnai Z. (2017). Információbiztonság tudatosság. *Műszaki Tudományos Közlemények,* 37–42. https://www.eme.ro/publication-hu/mtk/mtk7/MTK7_02_Rajnai-plen.pdf

Rao, S. R. (2014). Perspective SOX *Controls - Driving Transformation of the Order-to-Cash Value Chain*. Infosys Limited External Document. https://www.infosysbpm.com/offerings/functions/sales-fulfillment/white-papers/Documents/SOX-controls.pdf

Reason, J. (1999). *The 'Swiss Cheese' model*.

Reason, J. (2000). Human error: models and management. *BMJ, 320*(7237), 768–770. https://doi.org/10.1136/bmj.320.7237.768

Schneier, B. (2003). *Beyond fear – Thinking sensibly about security in an uncertain world*. Springer-Verlag Copernicus Books. https://doi.org/10.1007/b97547

Szilágyi, Gy. A. (2015). Determining delay risks of processes deriving from personal professional competences. 2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY), (pp. 205–208). https://doi.org/10.1109/SISY.2015.7325380

Takácsné Gy. K. & Benedek A. (2016). Bizalmon alapuló együttműködés vizsgálata a kis- és középvállalatok körében. In Csiszárik-Kocsir A. (Szerk.), *Keleti Faculty of Business and Management* (pp. 379–390). Óbuda University.

Temesi, J. & Varró, Z. J. (2017). *Operációkutatás*. Akadémiai Kiadó.

Trusted Business Partners Technical Department of ENISA Section Risk Management ENISA. (2006). *Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools*.

Wayne L. W. (2003). *Operációkutatás I-II*. Aula Kiadó.

A cikk APA szabály szerinti hivatkozása

Kemendi Á. (2023). Humán kockázatok hálózatkutatási szempontból. *Belügyi Szemle*, *71*(2), 317–334. https://doi.org/10.38146/BSZ.2023.2.8