Vállalkozásfejlesztés a XXI. században 2025/3. kötet
Generációs attitűdök, szervezeti kihívások és technológiai
megújulás a vállalkozásfejlesztésben

Közvetlen és közvetett biztonság a szervezetekben

Molnár Balázs

PhD-hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola
molnar.balazs@bgk.uni-obuda.hu

Absztrakt: A tanulmány célja egy integrált fogalmi keret bevezetése a szervezeti biztonság értelmezésére, amely két, egymást kiegészítő dimenzióra épül: a közvetlen (azonnali) és a közvetett (hosszú távon ható) biztonságra. A publikáció megközelítésének alapja, hogy a kettős biztonsági szintet a stabilitást és bizalmat fenntartó feltételrendszerként fogalmazza meg. A tanulmányban elméleti téziseket fogalmazok meg a két dimenzió kölcsönhatásaira, elkülönítve a rendszerszintű zavarokat. Bemutatja, a látszatbiztonság kialakulását, amikor a formálisan létező biztonsági elemek nem képesek tényleges védelmet nyújtani.

Kulcsszavak: biztonság, közvetlen biztonság, közvetett biztonság, bizalom, kontroll

1 Közvetlen és közvetett biztonság

A biztonság fogalmát a 21. században egyre inkább tágabb, multidiszciplináris megközelítésben értelmezzük, amely nemcsak az emberhez kapcsolódó fizikai védelmet, hanem a pszichológiai, szervezeti és információs dimenziókat is magában foglalja (Cooper, 2000; Reason, 2016). Ugyanakkor fontos kihangsúlyozni, hogy a biztonság nem értelmezhető emberek nélkül. A „Human security" című műben is megjelenik, hogy az egyén biztonsága az elsődleges: „Az emberi biztonságra irányuló megközelítés hangsúlyozza az egyének azonnali és kézzelfogható védelmét az életüket és jólétüket fenyegető veszélyekkel szemben." (Tadjbakhsh, 2005).

Ebben a tanulmányban a biztonságot két, egymást kiegészítő szinten vizsgálom: közvetlen biztonságként, amely azonnali, az egyénre és az operatív folyamatokra ható védelmi intézkedéseket foglalja magában, valamint közvetett biztonságként, amely szervezeti és rendszerszintű, hosszabb távon ható mechanizmusokra épül. A két dimenzió kapcsolata nem hierarchikus, hanem komplementer: egymást kiegészítve jelentik a biztonságot a szervezetekben.

A tanulmány a közvetlen és közvetett biztonság fogalmát a „direct vs. indirect entity-level controls (ELC)" logikájára támaszkodva használja. A PCAOB és SEC kimutatásai alapján bizonyos ELC-ék hatása ugyan fontos, ellenben közvetett, nem azonnali hatású (AS 2201). A SEC közleménye szerint „a kontrollok közvetlenül vagy közvetve kapcsolódhatnak egy pénzügyi beszámolási elemhez", illetve "minél inkább közvetett a kapcsolat, annál kevésbé alkalmas a kontroll a kockázatok közvetlen kezelésére". (SEC, 2007).

Az említett logika alapja pénzügyi vonatkozású, de ez alapján hivatkozok közvetlen biztonságként azokra a mechanizmusokra, amelyek azonnal hatnak egy kockázat esetében, így ez fogja jelenteni az egyik biztonsági szintet. Közvetett biztonságon pedig azokat a hatásokat jelenti, amelyek a szervezetekben később fejtik ki a hatásukat egy fenyegetés vagy veszély esetén.

2 Közvetlen és közvetett kontrollok

Szervezeti szinten a közvetlen biztonság Menon megfogalmazása szerint olyan tényezők, amelyek közvetlenül védik az embert vagy a szervezet működését a lehetséges veszélyektől. (Menon, 2007). A szervezetek működésében ezek alatt érthetjük a munkavédelemmel, fizikai védelemmel kapcsolatos előírásokat, adatvédelmi intézkedéseket, továbbá a pszichológiai biztonságot is, ahol a beavatkozások hatása azonnal érzékelhető és mérhető (ISO, 2018; Edmondson, 1999).

A közvetett biztonság mechanizmusai azonban nem azonnal jelentkeznek, így a hatásuk hosszabb távon mérhető. A közvetett biztonság a stratégiai stabilitás, az integritás és a bizalom hosszú távú fenntartásának feltételeit teremti meg. Ez a szemléletmód illeszkedik ahhoz a tágabb értelmezéshez, miszerint a biztonság nem redukálható a fenyegetések hiányára, hanem olyan feltételek meglétéként kell értelmezni, amelyek lehetővé teszik a stabilitást és a bizalmat (Villalón-Fonseca, 2022). Állítása lényegében az integrált biztonság szemlélete. Schnabel megfogalmazásában „Az emberi biztonságra irányuló megközelítésnek nemcsak a közvetlen erőszakot kell magában foglalnia, hanem a strukturális vagy közvetett erőszakot" (Schnabel, 2008), vagyis a biztonság hiánya gyakran nem közvetlen fenyegetésből, hanem a szervezeti és társadalmi struktúrák hibáiból ered.

Következésképpen, a közvetett biztonság olyan eszközökön alapul, mint a belső kontrollrendszerek (COSO, 2013), az etikai megfelelés és integritásmechanizmusok (Trevino & Nelson, 2016), a kiberbiztonsági keretrendszerek (NIST, 2024), valamint a bejelentővédelmi struktúrák (EU, 2019/1937). Ezek a mechanizmusok nem közvetlenül csökkentik a kockázatokat, hanem olyan szervezeti feltételeket teremtenek, amelyekben a biztonság fenntartható és önmegerősítő módon működik.

A szervezetek működésében ez a kettős kölcsönhatás különösen jelentős tényező, mivel a vállalatok sikeressége nem kizárólag a technológiai vagy pénzügyi biztonságon múlik, hanem azon is, hogy képesek-e olyan bizalmi és integritásalapú rendszert kialakítani, amelyben az emberek nemcsak biztonságban érzik magukat, hanem aktív szereplői is a biztonság fenntartásának és formálásának. A közvetlen és közvetett biztonság tehát nem egymás alternatívái, hanem dinamikus rétegek egy integrált szervezeti biztonsági modellben. Egy biztonságos környezet növeli az együttműködési hajlandóságot, a lojalitást és az innovációs készséget (Edmondson, 1999), ami a szervezet iránti bizalmat is növeli.

3 Látszatbiztonság és strukturális gyengeségek

„A vállalkozások hosszú távú működésének biztosítása érdekében szükséges egy biztonságot nyújtó rendszer alkalmazása a hamis biztonságérzetet keltő eszközök és eszközök helyett" (Michelberger & Lábodi, 2012). A közvetett és közvetlen biztonság alapvető feltétele a szervezetek fenntartható működésének. Bármelyikük hiánya nem csupán részleges vagy akár teljes biztonsági problémát okozhat, hanem rendszerszintű zavarokhoz, működési instabilitáshoz, ezzel együtt bizalom elvesztéséhez is vezethet. A biztonsági mechanizmusok kettős védelmi architektúrája tehát nem elméleti konstrukció, hanem az emberi és szervezeti működés egyik alappillére.

Ha a közvetlen biztonság instabil, vagyis nem állnak rendelkezésre az azonnali, fizikai és pszichológiai védelmi megoldások, akkor az egyének közvetlenül sérülékennyé válnak a környezeti, technológiai és szervezeti kockázatokkal szemben. Kutatások igazolták, hogy a veszélyekkel terhelt munkakörnyezet és a gyenge biztonsági környezet balesetekkel, sérülésekkel, kiégéssel és teljesítményromlással jár (Christian et al.,2009). A nem megfelelő munkavédelmi és biztonsági intézkedések növelik a balesetek, a stressz és a pszichés megterhelés kockázatát. A közvetlen biztonság hiánya nem csupán fizikai következményekkel jár: az védőeszközök és védelmi protokollok hiánya érzelmi és egészségügyi problémákhoz vezet (Simms et al., 2020). Ez összhangban áll Edmondson megállapításával, miszerint a pszichológiai biztonság hiánya olyan környezetet teremt, ahol a munkavállalók félnek hibázni, elhallgatják a problémákat, és ezáltal csökken a tanulási és innovációs képességük (Edmondson, 1999).

Ha a közvetett biztonság a hiányzik vagy nem elegendő, akkor a védelmi mechanizmusok ugyan formálisan létezhetnek, de funkciójukat nem látják el. A biztonság látszólagos lesz, mivel a szervezet struktúrája nem támogatja a felelősségvállalást, a hibák okainak feltárását és a nyílt kommunikációt. Ez szintén a bizalom csökkenéséhez vezet. A RUSI tanulmánya szerint a szervezeti biztonsági kudarcok gyökere a kockázatkerülő, szervezeti kultúra, amely

rendszerszinten redukálja a biztonságos döntéseket (RUSI, 2007), ami jól jellemzi, hogy a közvetett biztonság hiánya strukturális eredetű sebezhetőséget idéz elő.

A modern kiberbiztonsági és adatvédelmi szakirodalom is kiemeli, hogy a rendszerszintű (közvetett) biztonsági elemek hiánya komoly gazdasági és reputációs következményekkel jár. Az ENISA Threat Landscape részletezi a fő fenyegetéseket és esettípusokat, alátámasztva, hogy a folyamatok és az együttműködési hiányok megnövelik a kitettséget (ENISA, 2024/2025). Ezek a következmények nem csupán technikai, hanem bizalmi deficitet is generálnak, ami hosszabb távon rontja a szervezet társadalmi legitimációját és együttműködési potenciálját.

Következtetések

A két dimenzió hiányát összevetve elmondható, hogy a közvetlen biztonság hiánya az azonnali kockázatok és emberi sérülések irányába mutat, míg a közvetett biztonság hiánya az elhúzódó, rendszerszintű gyengülés forrása (Reason, 2016; ISO 45001:2018). Egy szervezet képes lehet működni erős közvetett biztonsági keretekkel, de gyenge közvetlen védelemmel – például, ha kiváló szabályozási környezete van, ugyanakkor elhanyagolja a munkavédelmi előírások betartását, viszont ez csak addig tartható meg egy szinten, amíg nem következik be egy kritikus esemény (Weick & Sutcliffe, 2015; Cooper, 2000). Ugyanakkor az erős közvetlen védelem és a hiányzó közvetett struktúrák is instabil környezetet teremthetnek: a válaszok ilyen esetben reaktívak, a bizalom pedig formális, nem belső meggyőződésen alapul (PCAOB, 2007; ISO 22316:2017).

Az integrált megközelítés lényege éppen az, hogy a közvetett biztonság teremti meg a szervezet immunrendszerét, amely a bizalmat, az etikus működést és a tanulási képességet fenntartja, míg a közvetlen biztonság biztosítja a gyors választ, amely azonnal reagál a fenyegetésekre. A két szint tehát nem helyettesíti, hanem feltételezi egymást: ha bármelyik hiányzik, a szervezet viselkedése fragmentált védekezéshez és kiszámíthatatlan reakciókhoz vezet (Reason, 2016; ISO 45001:2018; Weick & Sutcliffe, 2015).

A további kutatási irány, hogy a biztonsággal kapcsolatos előírások (jogszabályok, szabványok, belső szabályozások, kontrollok) hogyan kapcsolódnak egymáshoz, melyek azok a pontok, ahol erősítik vagy éppen gyengítik egymást, és a közvetett és közvetlen biztonság tényezőinek milyen módokon vezethetnek a kockázatok csökkenéséhez.

Hivatkozások

[1] Christian, M. S., Bradley, J. C., Wallace, J. C., & Burke, M. J. (2009). Workplace safety: A meta-analysis of the roles of person and situation factors. *Journal of Applied Psychology, 94*(5), 1103–1127.

https://pubmed.ncbi.nlm.nih.gov/19702360/ Utolsó megtekintés dátuma 2025.10.29.

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control—Integrated Framework. https://www.sechistorical.org/collection/papers/2010/2013_0501_COSOInternal.pdf?utm_source=chatgpt.com Utolsó megtekintés dátuma 2025.10.29.

[3] Cooper, M. D. (2000). Towards a model of safety culture. Safety Science, 36(2), 111–136. https://doi.org/10.1016/S0925-7535(00)00035-7

[4] Edmondson, A. (1999). Psychological Safety and Learning Behavior in Work Teams. Administrative Science Quarterly, 44(2), 350–383. https://doi.org/10.2307/2666999

[5] European Parliament and Council. (2019). Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law. Official Journal of the European Union. https://eur-lex.europa.eu/TodayOJ/ Utolsó megtekintés dátuma 2025.10.29.

[6] ENISA. (2024–2025). Threat Landscape (Finance sector). https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape Utolsó megtekintés dátuma 2025.10.29.

[7] International Organization for Standardization. (2017). ISO 22316:2017 Security and resilience—Organizational resilience—Principles and attributes.

[8] International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use.

[9] Menon, S. (2007). Human Security: Concept and Practice. International Studies, 44(2), 165–176.

[10] Michelberger, P., Jr., & Lábodi, C. (2012). After Information Security – Before a Paradigm Change (A Complex Enterprise Security Model). Acta Polytechnica Hungarica, 9(4), 101–115. https://acta.uni-obuda.hu/Michelberger_Labodi_36.pdf

[11] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf Utolsó megtekintés dátuma 2025.10.29.

[12] PCAOB. (2007, Jun 12). Auditing Standard No. 5—Adopting Release (No. 2007-005A), p. 8. https://pcaobus.org/Rulemaking/Documents/021/2007-06-12_Release_No_2007-005A.pdf Utolsó megtekintés dátuma 2025.10.29.

[13] Public Company Accounting Oversight Board. (n.d.). AS 2201: An audit of internal control over financial reporting that is integrated with an audit of financial statements (§.23). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201 Utolsó megtekintés dátuma 2025.10.29.

[14] Reason, J. (2016). Managing the Risks of Organizational Accidents (Rev. ed.). Routledge.

[15] Royal United Services Institute. (2007, October 12). Conference report: Delivering resilience. RUSI. https://www.rusi.org/explore-our-research/publications/conference-reports/conference-report?utm_source=chatgpt.com Utolsó megtekintés dátuma 2025.10.29.

[16] Schnabel, A. (2008). The Human Security Approach to Direct and Structural Violence. In SIPRI Yearbook 2008: Armaments, Disarmament and International Security (pp. 87–92). Oxford University Press.

[17] Simms, A., Fear, N. T., & Greenberg, N. (2020). The impact of having inadequate safety equipment on mental health. Occupational Medicine, 70(4), 278–281. https://doi.org/10.1093/occmed/kqaa101

[18] Tadjbakhsh, S. (2005). Human Security: Concepts and Implications. Paris: Sciences Po/CERI.

[19] Trevino, L. K., & Nelson, K. A. (2016). Managing Business Ethics (7th ed.). Wiley.

[20] U.S. Securities and Exchange Commission. (2007, June 20). Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting (Release No. 33-8810), pp. 17–18. https://www.sec.gov/files/rules/interp/2007/33-8810.pdf

[21] Villalón-Fonseca, R. (2022). The Nature of Security: A Conceptual Framework for Integral Security. Computers & Security, 119, 102760. https://www.sciencedirect.com/science/article/pii/S0167404822001997?via%3Dihub

[22] Weick, K. E., & Sutcliffe, K. M. (2015). Managing the Unexpected: Sustained Performance in a Complex World (3rd ed.). John Wiley & Sons.