Kiberbiztonsági és felhasználói kihívások a digitális korban: párhuzamok a BYOD és az önvezető autók között

Szikora Péter, Fehér-Polgár Pál

szikora.peter@kgk.uni-obuda.hu feherpolgar.pal@kgk.uni-obuda.hu

Absztrakt: The rapid spread of digital technologies has brought many new opportunities, but at the same time it has created serious security risks. The aim of this study is to present the common risk patterns of Bring Your Own Device (BYOD) practices and self-driving cars in the form of a literature review. Although the two areas appear to be far apart, they share similar problems: network vulnerabilities, lack of user awareness, and regulatory and management dilemmas. In the case of BYOD, the main threats are data theft, malware, and shadow IT, while in the case of self-driving cars, they are software updates and the manipulability of sensors and communication systems. In both areas, increasing user trust and awareness is key, as technological protection alone is not enough. Regulation and management also play a crucial role: without a proactive, risk-sensitive approach, security cannot be guaranteed. The study concludes that the strategies and attitude studies developed in the world of BYOD can serve as lessons for the social and technical introduction of self-driving cars, while the complex ecosystem of AVs can also provide new perspectives on corporate information security.

Keywords: BYOD (Bring Your Own Device), Autonomous Vehicles, Cybersecurity, User Awareness, Regulatory Challenges)

Kiberbiztonsági kockázatok: a BYOD és az önvezető autók párhuzamai

A digitális technológiák fejlődése az elmúlt évtizedekben rendkívül gyors ütemet vett fel, amely egyszerre teremtett korábban elképzelhetetlen lehetőségeket, és hozott magával újfajta sebezhetőségeket. A digitalizáció térnyerésével párhuzamosan a mindennapi és a szervezeti működés egyre nagyobb mértékben vált hálózatokra, adatáramlásra és összekapcsolt rendszerekre épülővé. Ez a tendencia különösen két területen figyelhető meg élesen: egyrészt a vállalatoknál egyre elterjedtebb Bring Your Own Device (BYOD) gyakorlatban, másrészt az önvezető járművek (Autonomous Vehicles, AV) rohamos fejlődésében és térnyerésében. Első pillantásra úgy tűnhet, hogy a két terület nagyon távol esik egymástól: míg az

egyik a munkahelyi informatikai környezethez, a másik a közlekedés jövőjéhez kötődik. Mégis, ha mélyebben megvizsgáljuk a szakirodalom eredményeit, hamar kiderül, hogy mindkettőben központi kérdésként jelenik meg a kiberbiztonsági kockázatok kezelése, az érzékeny adatok védelme és a rendszerszintű sebezhetőségek mérséklése. Az áttekintések alapján világosan kirajzolódik, hogy legyen szó akár a vállalati adatvagyon biztonságáról, akár a közlekedés biztonságáról, a felhasználói tudatosság, a megelőző intézkedések és a megfelelő szabályozási háttér minden esetben kulcsszerepet játszanak.

A BYOD környezetben a szervezetek megengedik vagy eltűrik, hogy a munkavállalók saját magánhasználatban lévő eszközeiket – tipikusan okostelefonjaikat, táblagépeiket vagy hordozható számítógépeiket – alkalmazzák a munkahelyi feladatok elvégzésére. Ez a gyakorlat számos előnnyel jár: egyrészt csökkenti a vállalat költségeit, hiszen kevesebb munkaeszközt kell biztosítani, másrészt növeli a rugalmasságot, mivel a munkavállalók a megszokott eszközeiken dolgozhatnak. Ugyanakkor a szakirodalom egyértelműen rámutat arra, hogy ezzel a modell kiterjeszti a szervezetek támadási felületét, és újfajta veszélyekkel szembesíti az informatikai biztonsági szakembereket. A kutatások kiemelik, hogy a leggyakoribb kockázatok közé tartozik az érzékeny adatok elvesztése vagy kiszivárgása, a rosszindulatú szoftverek és vírusok megjelenése, az illetéktelen hozzáférés megszerzése, illetve a gyenge vagy hiányos hitelesítési eljárások alkalmazása (Ratchford, 2022; Yeboah-Boateng & Boaten, 2016). Mindezek mellett külön problémát jelent a shadow IT jelensége, amely során a munkavállalók megkerülik a hivatalos informatikai előírásokat, és olyan alkalmazásokat vagy szolgáltatásokat vesznek igénybe, amelyek nincsenek engedélyezve vagy ellenőrizve (Wani et al., 2020). A kutatók hangsúlyozzák, hogy a kockázatok mérséklése érdekében szükség van korszerű technikai megoldások bevezetésére, mint például a mobil eszközmenedzsment alkalmazása, az adatátvitel és -tárolás titkosítása, valamint a szigorú hozzáférés-szabályozás kialakítása (Ratchford, 2022).

Az önvezető autók kapcsán a kockázati tényezők hasonló logikára épülnek, mivel ezek a rendszerek szintén rendkívül komplex informatikai hálózatokra támaszkodnak, amelyek nyitottságukból fakadóan sérülékenyek. Az AV-k működését alapvetően a fejlett szenzorok, a mesterséges intelligencia és a folyamatos hálózati kommunikáció – például a V2X (vehicle-to-everything) adatkapcsolat – teszik lehetővé. Ez a nyitottság azonban magával hozza a kibertámadások kockázatát: valós fenyegetést jelent a jármű irányításának átvétele, az adatok kiszivárgása, a GPS-jelek manipulálása, vagy akár a teljes közlekedési rendszer megzavarása (Nayak, 2024; Yousseef et al., 2024). A támadások célpontja sokféle lehet: a fedélzeti vezérlőegységek (ECU-k), a szoftverfrissítési csatornák, vagy éppen a jármű és a külső infrastruktúra közötti adatcsere (De Vincenzi et al., 2024). A szakértők szerint azonban az AV ökoszisztéma biztonságát nem lehet kizárólag technikai problémaként kezelni. A valódi védelem érdekében szükséges a kockázatok átfogó, rendszerszintű értékelése, a megfelelő prioritások

meghatározása, valamint a jogi és szabályozási megfelelés biztosítása is (Lim et al., 2024).

A két terület közötti párhuzam abban ragadható meg leginkább, hogy mind a vállalati BYOD-gyakorlatban, mind az önvezető járművek világában a hálózati alapú technológiák sérülékenysége és a felhasználói tudatosság hiánya döntő tényezőként határozza meg a biztonsági kockázatok mértékét. Ahogy a BYOD esetében gyakori, hogy a munkavállalók alábecsülik a biztonsági előírások és az adatvédelem fontosságát, úgy az önvezető autóknál is problémát okozhat, ha a felhasználók túlzott bizalmat tanúsítanak a rendszer iránt, vagy éppen tudatosan megkerülik a szabályokat (Ratchford, 2022; Nayak, 2024). Mindez arra mutat rá, hogy mindkét területen elengedhetetlen a proaktív és megelőző szemléletű biztonságpolitika kialakítása. Ez a politika akkor lehet igazán hatékony, ha ötvözi a korszerű technikai védelmi megoldásokat, a felhasználók folyamatos képzését és tudatosítását, valamint a megfelelő intézményi és jogi szabályozási keretek megteremtését.

Felhasználói tudatosság és attitűdök: párhuzamok a BYOD és az önvezető autók területén

A technológiai újítások biztonságos használatának egyik legnagyobb és legösszetettebb kihívása nem csupán a fejlett technikai háttérben rejlik, hanem legalább annyira a felhasználói tudatosságban, a kockázatok észlelésében, valamint az ezekhez kapcsolódó attitűdökben. Hiába állnak rendelkezésre a legmodernebb biztonsági protokollok és védelmi rendszerek, ha a felhasználók nem értik vagy nem tartják fontosnak a szabályok betartását, a technológia továbbra is sebezhető marad. Mind a BYOD gyakorlat, mind pedig az önvezető járművek (AV-k) esetében központi kérdés, hogy az emberek hogyan érzékelik a lehetséges veszélyeket, milyen szintű bizalommal fordulnak az adott technológia felé, és miként alakítják ki a mindennapi használati szokásaikat. Más szóval, a technológia elfogadottsága és biztonságos működése nem pusztán műszaki kérdés, hanem mélyen beágyazódik a felhasználói magatartásba és társadalmi attitűdökbe.

A BYOD környezetre vonatkozó kutatások rendre azt mutatják, hogy a munkavállalók hajlamosak alábecsülni az adatbiztonság kritikus jelentőségét. Sok esetben a kényelem és a gyors hozzáférés fontosabb számukra, mint a szabályok pontos betartása. Ez a hozzáállás gyakran kockázatos viselkedésben nyilvánul meg, például gyenge jelszavak használatában, a többfaktoros hitelesítés mellőzésében, vagy éppen a vállalati szabályzatok tudatos megkerülésében (Ratchford, 2022). A kutatások szerint a biztonsági előírások betartása sokszor másodlagossá válik a rövid távú előnyökkel szemben, amelyek a gyors és akadálytalan munkavégzéshez kapcsolódnak (Yeboah-Boateng & Boaten, 2016). A shadow IT jelensége – amikor

a dolgozók engedély nélküli alkalmazásokat és szolgáltatásokat vesznek igénybe – különösen jól szemlélteti, hogy a felhasználói attitűdök sokszor szembe mennek a szervezeti elvárásokkal. A hatékonyság és a rugalmasság érdekében a munkavállalók gyakran vállalnak többletkockázatot, még akkor is, ha ezzel közvetlenül növelik a szervezet adatbiztonsági fenyegetéseit (Wani et al., 2020).

Az önvezető autók esetében a felhasználói attitűdök szintén meghatározó szerepet játszanak a biztonságos használatban és a társadalmi elfogadottságban. A kutatások azt mutatják, hogy a legtöbb ember számára a legfontosabb tényező az észlelt biztonság: ha az AV-technológiát biztonságosnak tartják, akkor sokkal nagyobb eséllyel hajlandók elfogadni és kipróbálni (Prasetio et al., 2023). Ugyanakkor az ellenkezője is igaz: a biztonsági félelmek és a bizalom hiánya komoly akadályt jelenthet a széles körű elterjedésben, és lassíthatja a társadalmi integrációt (Moody et al., 2020; Naiseh et al., 2024). A felhasználók percepcióit erőteljesen befolyásolja, hogy mennyire ismerik a technológiát, illetve milyen tapasztalatokat szereznek vele kapcsolatban. Minél ismerősebbé válik számukra az önvezetés, annál nagyobb a hajlandóságuk arra, hogy kipróbálják, és egyben nagyobb a tolerancia a kockázatokkal szemben (Khoeini et al., 2022). Ez azt jelenti, hogy a társadalmi tanulás és a fokozatos bevezetés jelentősen hozzájárulhat az AV-k elfogadásához.

Kiemelten fontos tényező mindkét területen a bizalom és a felelősségvállalás kérdése. A BYOD környezetben gyakran megfigyelhető, hogy a munkavállalók a felelősséget nem magukra, hanem a szervezetre hárítják, vagyis úgy vélik, hogy a vállalat feladata biztosítani a megfelelő védelmet. Az önvezető autók esetében a kutatások vegyes képet mutatnak: egyes felhasználók túlzott mértékben bíznak a technológiában, és emiatt hajlamosak figyelmen kívül hagyni a lehetséges veszélyeket, míg mások ennek ellenkezőjét teszik, vagyis túlzottan szkeptikusak, és emiatt inkább elutasítják a rendszert (Mutzenich et al., 2021). Mindkét szélsőség magában hordozza a kockázatot: a túlzott bizalom könnyelmű használathoz, a túlzott félelem pedig a technológia elutasításához vezethet, amely szintén hátráltatja az innováció fejlődését és társadalmi hasznosulását.

Az irodalom összegzése alapján egyértelműen látható, hogy a felhasználói tudatosság, a bizalom és az attitűdök kezelése nem kizárólag műszaki kérdés, hanem interdiszciplináris megközelítést igényel. A BYOD környezetben alkalmazott kutatási módszerek, például a kockázatészlelés és a kockázatvállalás kérdőíves vizsgálata (Ratchford, 2022), jól adaptálhatók az önvezető autók világába is, ahol a társadalmi elfogadottság és a biztonsági percepció vizsgálata ugyancsak központi jelentőségű (Olayode, 2023; Nazari, 2024). Ez arra utal, hogy a különböző technológiai területek tanulságai kölcsönösen hasznosíthatók, és a felhasználói attitűdök tudatos alakítása elengedhetetlen feltétele mind a vállalati, mind pedig a közlekedési innovációk sikeres és biztonságos bevezetésének.

Jogi, szabályozási és menedzsment aspektusok: BYOD és önvezető autók

A technológiai fejlődés napjainkban nemcsak tisztán műszaki értelemben állítja új kihívások elé a társadalmat és a szervezeteket, hanem jogi, szabályozási és menedzsment szinten is komoly feladatokat generál. Az innováció gyors üteme gyakran megelőzi a jogalkotás és a menedzsment gyakorlatának alkalmazkodóképességét, így a szabályozási reakció sokszor lassú és reaktív jellegű. Ez különösen szembetűnő két területen: a vállalatoknál elterjedő Bring Your Own Device (BYOD) gyakorlatban és az önvezető járművek (Autonomous Vehicles, AV) térnyerésében. Bár a két terület működési logikája eltér, közös bennük, hogy új helyzeteket teremtenek, amelyekhez a jogi és intézményi eszköztár sokszor csak utólag tud igazodni.

A BYOD kapcsán a vállalatvezetés egyik legjelentősebb dilemmája abban áll, hogyan találjon megfelelő egyensúlyt a rugalmasság előnyei és a biztonság követelményei között. A saját eszközök bevonása növelheti a munkavégzés hatékonyságát, és hozzájárulhat a munkavállalói elégedettséghez is, ugyanakkor egyértelmű kockázatokat hordoz mind az adatbiztonság, mind a jogi megfelelés területén (Ratchford, 2022). A szervezeteknek ráadásul olyan megfelelési kötelezettségekkel kell szembenézniük, mint például a GDPR adatvédelmi előírásai vagy a NIS2 kiberbiztonsági irányelvei, amelyek komoly terheket rónak a menedzsmentre. A kihívás különösen élesen jelenik meg abban, hogy a munkavállalók magántulajdonban lévő eszközein tárolt vagy feldolgozott vállalati adatok védelméért is a szervezet viseli a felelősséget (Enterprise Defence, 2023). A kutatások hangsúlyozzák, hogy a sikeres BYOD-politika nem merülhet ki a technikai védelemben, hanem figyelembe kell vennie jogi és etikai szempontokat is, például a munkavállalók méltányos kezelését vagy az adatvédelemhez való alapvető jog biztosítását (Lam, 2024).

Az önvezető autók esetében a szabályozási és jogi kihívások még komplexebbnek mutatkoznak. Az egyik központi kérdés a felelősség megállapítása: ki viseli a következményeket egy esetleges balesetért – maga a jármű tulajdonosa, a szoftverfejlesztő cég, a járműgyártó vállalat vagy esetleg a közlekedési hatóság? (Nayak, 2024). A szakirodalom szerint az AV-k biztonsági ökoszisztémája kizárólag akkor működhet megbízhatóan, ha világos és részletes jogi keretek szabályozzák mind az adatgyűjtést, mind az adattovábbítást, valamint a rendszerfrissítések folyamatát (De Vincenzi et al., 2024). A szoftvervezérelt járművek esetében külön figyelmet kell fordítani a szoftverfrissítések ellenőrzésére, az ellátási lánc biztonságára, valamint a harmadik felekhez kapcsolódó kockázatok kezelésére is. Ezek a tényezők ugyanis nemcsak technikai, hanem jogi és menedzsment szempontból is jelentős kockázatot hordoznak (De Vincenzi et al., 2024). A megfelelő szabályozási háttér kialakítása tehát alapfeltétele annak, hogy

az önvezető járművek társadalmi és gazdasági bevezetése biztonságosan történhessen meg.

Összegzés és jövőbeli kutatási irányok

A BYOD és az önvezető járművek kiberbiztonsági, felhasználói és szabályozási aspektusait vizsgáló szakirodalom áttekintése világosan rámutat arra, hogy bár első látásra a két terület különállónak tűnik, valójában számos ponton szorosan kapcsolódik egymáshoz. A közös nevezőt három kulcsfontosságú tényező adja: a kiberbiztonsági kockázatok jelenléte, a felhasználói tudatosság és attitűdök szerepe, valamint a szabályozási és menedzsment kihívások.

A jövőbeli kutatásoknak több irányban érdemes elmozdulniuk. Egyrészt szükséges a felhasználói tudatosságot növelő programok hatékonyságának mélyebb és szisztematikusabb vizsgálata. Másrészt interdiszciplináris megközelítésekre van szükség, amelyek képesek összekapcsolni a műszaki, jogi, menedzsment és társadalomtudományi szempontokat. Harmadrészt hangsúlyt kell fektetni a nemzetközi szabályozási keretek harmonizálására is, mivel a digitális technológiák természetüknél fogva nem állnak meg az országhatároknál (Lam, 2024; Kaufman, 2022; Nayak, 2024).

Összességében elmondható, hogy a két terület összehasonlítása lehetőséget kínál olyan átfogó és integrált biztonsági modellek kidolgozására, amelyek egyszerre kezelik a technikai sebezhetőségeket, a felhasználói tényezőket és a szabályozási környezet kihívásait. Ez a holisztikus szemlélet kulcsfontosságú lesz abban, hogy a digitális technológiák a jövőben valóban biztonságosan, megbízhatóan és széles körben használhatóvá váljanak. A BYOD és az önvezető autók példája jól mutatja, hogy az innováció sikere nagymértékben azon múlik, sikerül-e a technikai megoldásokat jogi, intézményi és társadalmi dimenziókkal kiegészítve egységes rendszerbe integrálni.

References

[1.] De Vincenzi, G., et al. (2024). Software-defined vehicles: State of the art and research challenges. arXiv preprint arXiv:2411.10612. https://doi.org/10.48550/arXiv.2411.10612

[2.] Enterprise Defence. (2023). BYOD security & compliance challenges (GDPR, NIS2). Retrieved from https://enterprisedefence.com/blog/byod-security-risks-gdpr-nis2/

[3.] Kaufman, S. (2022). Autonomous vehicle literature review: Policy impact in cities. U.S. Department of Transportation.

[4.] Khoeini, S., Gao, Y., & Khattak, A. J. (2022). Interaction of familiarity, safety perceptions, and willingness to use autonomous vehicles. TOMNET Year 4 Project Report. https://doi.org/10.7922/G2M61HD8

[5.] Lam, H. (2024). Bring-your-own-device (BYOD): Organizational control and perceptions of justice. Journal of Organizational Change Management, 37(2), 151–166. https://doi.org/10.1108/JOCM-06-2023-0200

[6.] Lim, H., et al. (2024). Autonomous vehicle ecosystem security: Utilizing management priorities. Applied Sciences, 14(18), 8247. https://doi.org/10.3390/app14188247

[7.] Moody, J., Bailey, N., & Zhao, J. (2020). Public perceptions of autonomous vehicle safety. Accident Analysis & Prevention, 142, 105577. https://doi.org/10.1016/j.aap.2020.105577

[8.] Mutzenich, S., Koerner, A., & Wiggins, M. (2021). Updating our understanding of situation awareness and trust in autonomous driving. Cognitive Research: Principles and Implications, 6(1), 1–14. https://doi.org/10.1186/s41235-021-00271-8

[9.] Naiseh, M., Al-Kilidar, H., & AlHogail, A. (2024). Trust, risk perception, and intention to use autonomous vehicles: A bibliometric and structural analysis. Frontiers in Psychology, 15, 11968569. https://doi.org/10.3389/fpsyg.2024.11968569

[10.] Nayak, S. (2024). Cybersecurity challenges and risks in connected autonomous vehicles. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4917100

[11.] Nazari, F. (2024). On the role of perceived safety concerns in the adoption of autonomous vehicles. U.S. Department of Transportation Report. https://doi.org/10.21949/1522961

[12.] Olayode, O. (2023). Systematic literature review on the applications, impacts, and perceptions of autonomous vehicles. Transportation Safety and Environment, 5(1), tdad019. https://doi.org/10.1093/tse/tdad019

[13.] Prasetio, R., et al. (2023). Evaluating perceived safety of autonomous vehicles: Cognitive and emotional components. Transportation Research Part F: Traffic Psychology and Behaviour, 96, 1–14. https://doi.org/10.1016/j.trf.2023.01.007

[14.] Ratchford, M. (2022). Systematic literature review on BYOD security environments (2010–2019). Dakota State University. https://doi.org/10.37008/DSU.2022.00001

[15.] Wani, R. J., et al. (2020). Hospital BYOD security challenges: A systematic review. JMIR mHealth and uHealth, 8(7), e17610. https://doi.org/10.2196/17610

[16.] Yeboah-Boateng, E. O., & Boaten, P. O. (2016). Bring-your-own-device (BYOD): An evaluation of associated risks. arXiv preprint arXiv:1609.01821. https://doi.org/10.48550/arXiv.1609.01821

[17.] Yousseef, M., et al. (2024). Autonomous vehicle security: A deep dive into threat modeling. arXiv preprint arXiv:2412.15348. https://doi.org/10.48550/arXiv.2412.15348