DOI: https://doi.org/10.12700/btsz.2025.7.2.133

THE TRANSFORMATION OF WORKPLACE SAFETY IN THE AGE OF TELEWORKING

A MUNKAHELYI BIZTONSÁG ÁTALAKULÁSA A TÁVMUNKA KORÁBAN

GOMBKÖTŐ Judit[1]

Abstract

The rise of teleworking has fundamentally changed the challenges of occupational safety and privacy, especially in the areas of information security and cyber protection. The aim of this research is to map the risks of teleworking and the protection strategies used by companies with the help of a questionnaire survey. The results show that smaller companies are exposed to higher risks due to lower levels of IT security measures and education, while larger organizations reduce threats with more advanced protection protocols. The most significant security challenges are data leakage, identity theft, and network attacks. The research identifies four key areas of development: IT security education, network security measures, securing company devices and applying advanced authentication solutions. Sustainable security of teleworking requires integrated technological and awareness-raising strategies.

Keywords

teleworking, occupational safety, data security, cyber defense, information security

Absztrakt

A távmunka térnyerése alapjaiban változtatta meg a munkahelyi biztonság és adatvédelem kihívásait, különösen az információbiztonság és a kibervédelem területén. Jelen kutatás célja a távmunka kockázatainak és a vállalatok által alkalmazott védelmi stratégiáknak a feltérképezése egy kérdőíves felmérés segítségével. Az eredmények rámutatnak, hogy a kisebb vállalatok magasabb kockázatoknak vannak kitéve az alacsonyabb szintű IT biztonsági intézkedések és oktatás miatt, míg a nagyobb szervezetek fejlettebb védelmi protokollokkal csökkentik a fenyegetéseket. A legjelentősebb biztonsági kihívások az adatszivárgás, az azonosító adatok ellopása és a hálózati támadások. A kutatás négy kulcsfontosságú fejlesztési területet azonosít: IT biztonsági oktatás, hálózatbiztonsági intézkedések, biztonságos céges eszközök biztosítása és fejlett hitelesítési megoldások alkalmazása. A távmunka fenntartható biztonságának érdekében integrált technológiai és tudatosságnövelő stratégiák bevezetése szükséges.

Kulcsszavak

távmunka, munkahelyi biztonság, adatbiztonság, kibervédelem, információ biztonság

[1] judit.gombkoto@msg-plaut.hu | ORCID: 0009-0002-8438-7216 | Senior SAP Consultant, msg Plaut Hungary Kft., Vezető SAP tanácsadó, msg-Plaut Hungary Kft.

BEVEZETÉS

Az elmúlt években a távmunka széles körű elterjedése alapjaiban alakította át a munkahelyi biztonság és adatvédelem kérdését. Míg korábban a dolgozók többsége irodai környezetben, ellenőrzött informatikai rendszerek és biztonsági protokollok mellett végezte feladatait, addig napjainkban egyre többen végzik teendőiket otthonról vagy kevésbé kontrollált helyszínekről. Ez a változás új kihívásokat teremt mind a szervezetek, mind az alkalmazottak számára, különösen az információvédelem, a kiberbiztonság és a digitális fenyegetések kezelése szempontjából.

Jelen kutatás célja annak feltérképezése, hogyan módosult a munkahelyi biztonság a távmunka térnyerésével, milyen kockázatokkal szembesülnek az érintettek, valamint milyen védelmi stratégiákat alkalmaznak a vállalatok az új munkavégzési formákhoz igazodva. A vizsgálat kérdőíves felmérésen alapul, amely a távmunka gyakoriságát, a használt technológiai megoldásokat, a kibervédelmi intézkedéseket és a személyes biztonsági tapasztalatokat elemzi. Az eredmények rávilágítanak a távmunka adatbiztonsági vonatkozásaira, a legjelentősebb fenyegetésekre, valamint arra, mennyire felkészültek a munkáltatók és munkavállalók egy esetleges kibertámadás vagy biztonsági incidens esetén.

A tanulmány elősegíti a távmunka biztonsági aspektusainak alaposabb megértését, valamint javaslatokat fogalmazzon meg a védelmi protokollok és oktatási stratégiák továbbfejlesztésére.

SZAKIRODALMI ÁTTEKINTÉS

A munkahelyi biztonság kérdése az utóbbi évtizedben jelentős átalakuláson ment keresztül, különösen a távmunka és a hibrid munkavégzés elterjedésének következtében. A szakirodalom számos aspektusból vizsgálja ezt a változást, többek között az információbiztonság [1] [11] [12], a szervezeti bizalom [2] [4], a munkavállalói jóllét [3] [7], valamint a jogi és egészségvédelmi szempontok tükrében [5] [9].

A digitális munkahelyek és a távmunka térhódításával új kihívások jelentek meg az információbiztonság terén. A digitális munkakörnyezetek növelik a kibertámadások és adatszivárgások kockázatát, ezért a szervezeteknek új védelmi stratégiákat kell kidolgozniuk, például VPN-használatot, kétfaktoros hitelesítést és szigorúbb hozzáférés-kezelést [1] [11] [15]. A távmunka tömeges elterjedése miatt a hagyományos IT-biztonsági kockázatelemzések már nem feltétlenül érvényesek, ezért a vállalatoknak új biztonsági protokollokat kell alkalmazniuk [12] [19]. A COVID–19 járvány idején az információbiztonsági előírások és gyakorlatok jelentős átalakuláson mentek keresztül, a biztonságos távoli munkavégzés érdekében [5].

A távmunka egyik kritikus aspektusa a munkavállalók közötti bizalom és a szervezeti kommunikáció fenntartása. A távoli munkavégzés csökkentheti a személyes interakciókat és növelheti a bizalmi problémák kialakulásának esélyét [2]. A távmunka során a formális és informális belső kommunikáció sérülhet, ami a munkavállalók elszigeteltségét és a csapatkohézió csökkenését eredményezheti [4]. A hatékony kommunikáció és együttműködés fenntartása érdekében új digitális eszközök bevezetése szükséges [10].

A távmunka nemcsak az információbiztonságot, hanem a munkavállalók fizikai és mentális jóllétét is befolyásolja. A távmunka segítheti a munka-magánélet egyensúlyának megteremtését, ugyanakkor új kihívásokat is felvet a munkáltatók és a munkavállalók számára [3]. A járvány alatti távmunka hatásai között jelentős eltérések figyelhetők meg a hagyományos

irodai munkavégzéshez képest, különösen a szubjektív jóllét tekintetében [7]. A munkavállalói elégedettség és az adatbiztonsági tudatosság szoros összefüggésben állhat a távmunka körülményeivel [13].

A COVID–19 világjárvány katalizátorként működött a távmunka gyors elterjedésében, ugyanakkor számos új biztonsági és egészségvédelmi kérdést is felvetett. A felsőoktatásban dolgozók munkavégzése jelentős átalakuláson ment keresztül, ami hatással volt a termelékenységre és a munkavállalói jóllétre [6]. A vállalatoknak nemcsak technológiai szempontból kellett gyorsan alkalmazkodniuk, hanem jogi és adatvédelmi szempontból is, például a GDPR-nak megfelelő távmunkavégzési szabályzatok kidolgozásával [9] [14]. A hibrid munkavégzésre való áttérés során számos munkahelyi biztonsági és egészségvédelmi kérdés merült fel, amelyek kezelése elengedhetetlen a fenntartható működéshez [5].

Az információbiztonsági fenyegetések kezelése érdekében a szervezeteknek azonosítaniuk kell kritikus folyamataikat, mérniük kell azok távmunka-függőségét, és megfelelő kockázatkezelési stratégiákat kell kidolgozniuk ezek védelme érdekében [12]. A vállalatoknak megfelelő távmunka-biztonsági követelményeket kell kidolgozniuk, amelyek magukban foglalják a titkosítási protokollokat és a biztonságos hozzáférési rendszereket [15]. Az adatvédelmi kihívások sajátos szabályozási megközelítést igényelnek, különösen a munkavállalók online nyomon követése és a munkáltatók ellenőrzési lehetőségei kapcsán [14].

A jövőbeli kutatásoknak érdemes tovább vizsgálniuk a távmunka hosszú távú hatásait, valamint a szervezeti és jogszabályi keretek fejlesztésének lehetőségeit annak érdekében, hogy a munkavégzés ezen formája mind a munkavállalók, mind a munkáltatók számára biztonságos és fenntartható legyen.

ANYAG ÉS MÓDSZERTAN

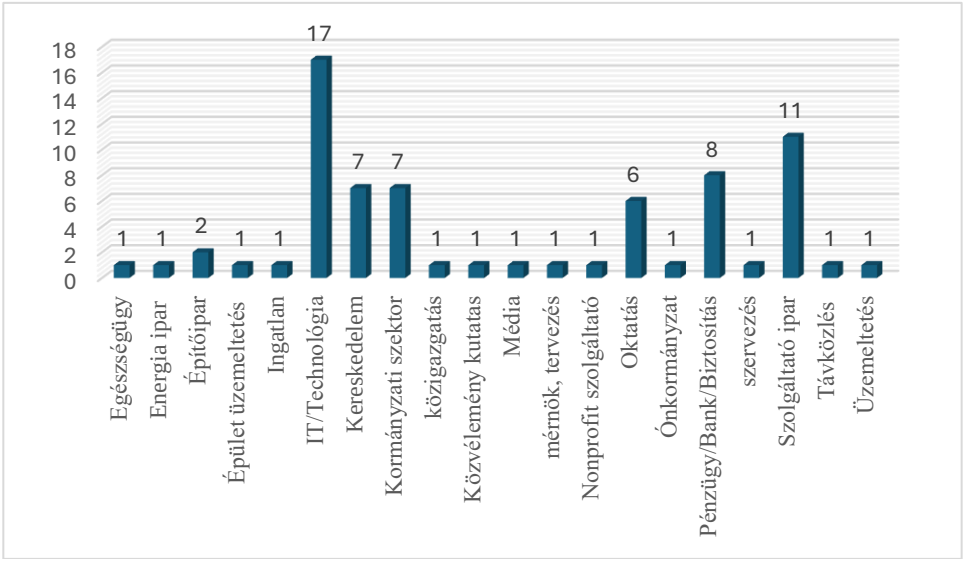
A kutatás célja a távmunka elterjedésével összefüggő munkahelyi biztonsági kihívások és munkavállalói tapasztalatok feltérképezése. Ennek érdekében kérdőíves felmérést végeztem, amely kvantitatív adatokon keresztül vizsgálta a válaszadók távoli munkavégzéssel kapcsolatos tapasztalatait, az alkalmazott biztonsági intézkedéseket és az észlelt kockázatokat.

Az adatgyűjtés egy online kérdőív segítségével történt, amelyet a Google Forms platformon keresztül tettem elérhetővé. A válaszadók különböző iparágakban dolgozó munkavállalók közül kerültek ki lásd, 1-es ábra, ami lehetőséget biztosított a szélesebb körű tapasztalatok elemzésére. Az online adatfelvétel anonim módon zajlott, ami növelte az őszinte válaszok arányát, ezáltal a kapott eredmények megbízhatóságát. A kutatás célja nem a reprezentativitás biztosítása volt, hanem az összefüggések feltárása, így az eredmények kvalitatív értelmezését részesítettem előnyben. Az adatgyűjtés 2025 januárjában zajlott.

A kérdőív 14 kérdésből állt, amelyek több tématerületet érintettek. Az első szakasz a demográfiai jellemzőkre koncentrált, beleértve az iparági hovatartozást, a vállalat méretét és a betöltött pozíciót. A második rész a munkahelyi biztonsági tényezőket vizsgálta, különös tekintettel a távmunka gyakoriságára, a használt eszközökre, a munkavégzés helyszíneire, valamint a munkáltató által biztosított kibervédelmi intézkedésekre. Emellett felmértem, hogy a válaszadók találkoztak-e adatbiztonsági incidensekkel, milyen fenyegetéseket tartanak kockázatosnak, és részt vettek-e informatikai biztonsági képzésen.

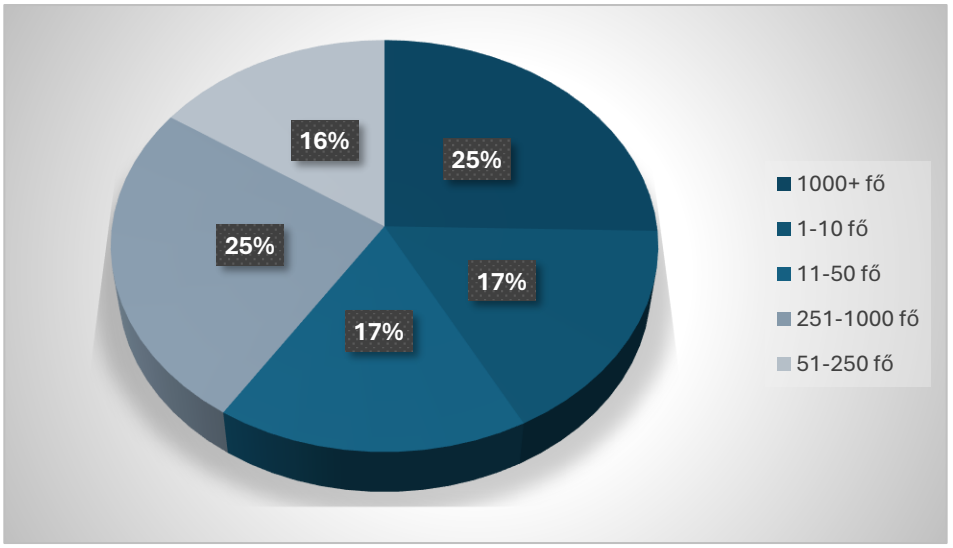
A kérdőív tartalmazott zárt és nyitott kérdéseket is. A skálázott kérdések lehetőséget adtak az objektív mérési eredmények összegzésére, míg a nyitott kérdésben a válaszadók megfogalmazhatták, mely fejlesztési területeket tartják kulcsfontosságúnak a távoli munkavégzés biztonságának javítása érdekében.

A válaszadók iparág szerinti megoszlását az 1. ábra szemlélteti. Az eredmények alapján a kitöltők 40%-a az IT/technológiai és a pénzügyi szektorban dolgozik.



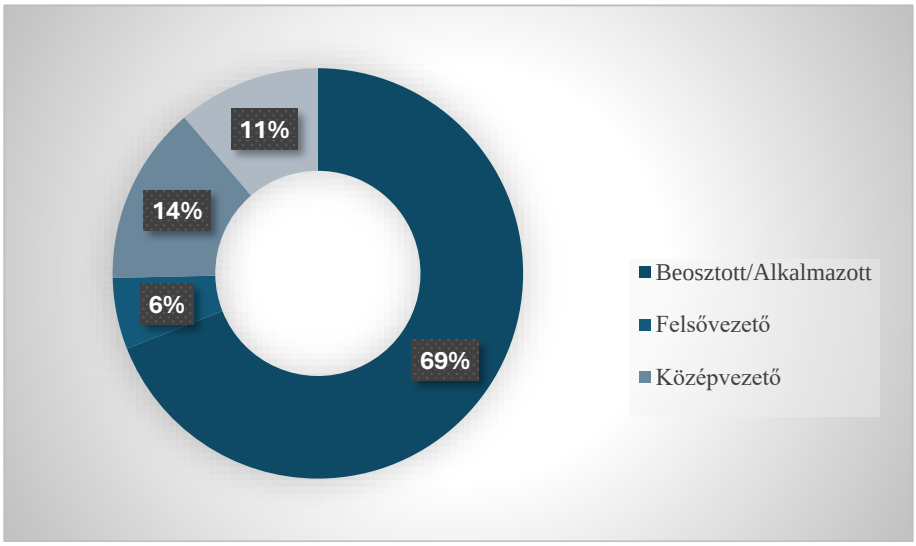
1. Ábra: A válaszadók jelenlegi iparági megoszlása Forrás: Saját kutatás, 2025, N = 71

Az adatgyűjtés során vizsgáltam a kitöltő pozícióját és a vállalat méretét. Egyszeres kitöltési lehetőséget adtam a válaszadóknak, mert ez egyértelműen eldönthető mindenki számára.



2. Ábra: A válaszadók vállalatméret szerinti megoszlása Forrás: Saját kutatás, 2025, N = 71

A válaszadók vállalatméret szerinti eloszlását a 2. ábra mutatja be, amelyből látható, hogy a kitöltők többsége nagyvállalatoknál (1000+ fő) dolgozik, ezt követik a közepes méretű cégek (251–1000 fő), majd a kisebb vállalatok. A legkevesebb válasz a mikro vállalkozások (1–10 fő) kategóriájából érkezett.



3. Ábra: A válaszadók pozició szerinti megoszlása Forrás: Saját kutatás, 2025, N = 71

A munkaköröket vizsgálva (3. ábra) a legtöbben alkalmazotti státuszban dolgoznak, míg a közép- és felsővezetők kisebb arányban szerepelnek a válaszadók között. A vállalkozók és szabadúszók is jelen vannak, de alacsonyabb reprezentációval. Az eredmények azt mutatják, hogy a kutatás résztvevőinek többsége alkalmazottként, jellemzően közép- vagy nagyvállalatoknál dolgozik, amely fontos szempont a távmunka és a biztonság összefüggéseinek értékelésében.

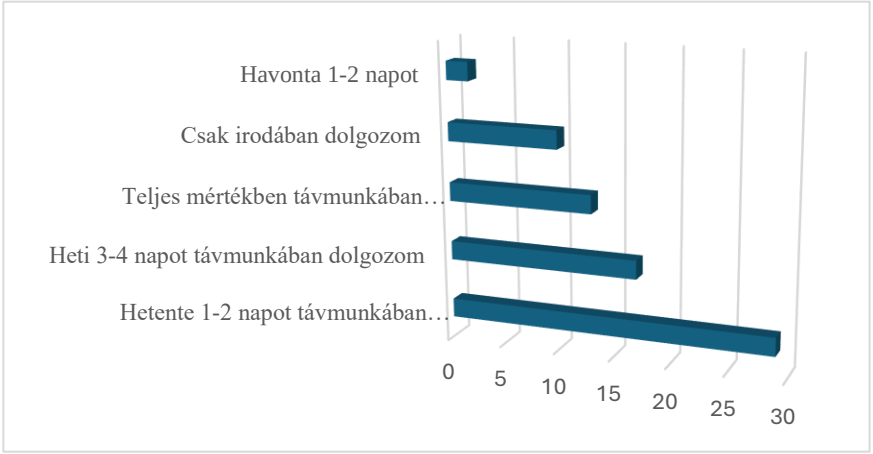
A kutatás hipotézise szerint a távmunka térnyerése új adatbiztonsági és kibervédelmi kihívások elé állítja a munkáltatókat és munkavállalókat egyaránt. Feltételezhető, hogy a kisebb vállalatok nagyobb adatbiztonsági kockázatokkal szembesülnek a korlátozott IT-védelmi intézkedések és alacsonyabb szintű biztonsági oktatás miatt, míg a nagyobb szervezetek fejlettebb technológiai és képzési stratégiákat alkalmaznak a kibertámadások kockázatának csökkentése érdekében. A megfelelő kibervédelmi intézkedések – például a kétfaktoros hitelesítés, VPN-használat és adattitkosítás – valamint a munkavállalók informatikai tudatosságának növelése kulcsfontosságú lehet a távoli munkavégzés biztonságosabbá tételében.

Az összegyűjtött adatokat statisztikai módszerekkel elemeztem, beleértve az eloszlások vizsgálatát, az átlagok és szórások kiszámítását, valamint a különböző változók közötti összefüggések feltárását. Az adatelemzéshez Microsoft Excel szoftvert használtam.

EREDMÉNYEK

A kutatás célja a távmunka munkahelyi biztonságra és adatvédelemre gyakorolt hatásainak feltárása volt. Az alábbiakban a kérdőíves felmérés eredményei kerülnek bemutatásra, amelyek rávilágítanak a távmunka elterjedtségére, a munkavégzés biztonsági kihívásaira és a munkáltatók által biztosított védelmi intézkedésekre.

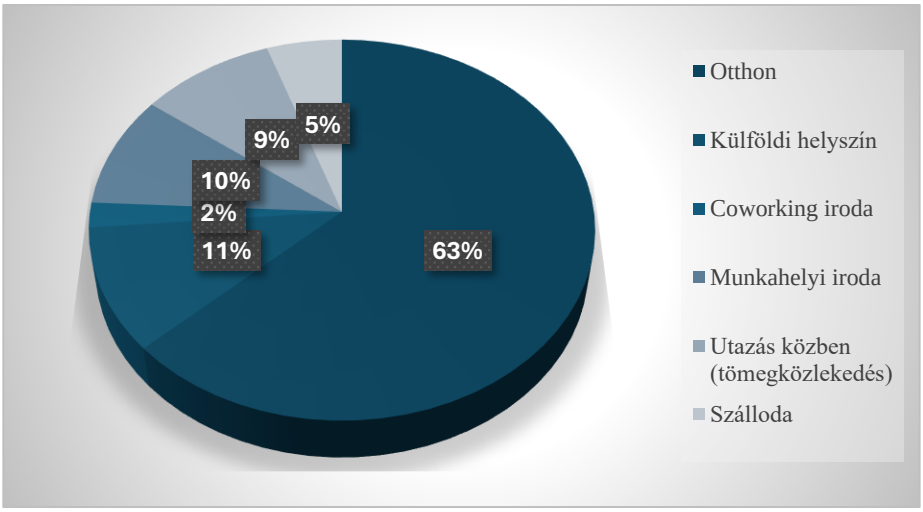
A „Milyen gyakran dolgozik távmunkában?” kérdésre adott válaszok az alábbi ábrán láthatók. A kérdőívben egyetlen válasz megjelölésére volt lehetőség, mivel a kérdésre egyértelmű válasz adható.



4. Ábra: Távmunka gyakorisága Forrás: Saját kutatás, 2025, N = 71

Az eredmények alapján a válaszadók több mint 60%-a rendszeresen dolgozik távmunkában. A leggyakoribb gyakorlat az otthonról végzett munka, amelyet a válaszadók 39,4%-a heti 1–2 napban, 22,5%-a pedig heti 3–4 napban végez.

A távmunkában használt helyszíneket az alábbi ábra szemlélteti. Mivel a válaszadók több lehetőséget is megjelölhettek, az eredmények azt tükrözik, hogy egy személy többféle helyszínen is dolgozhat távmunkában.



5. Ábra: Távmunkára használt helyszínek Forrás: Saját kutatás, 2025, N = 71

Az adatokból kiderül, hogy az otthonon kívüli helyszíneken – például kávézókban, coworking irodákban – végzett munka kevésbé elterjedt, és a legtöbben kizárólag saját lakóhelyükön dolgoznak távmunkában.

A távmunkavégzés elterjedésével az adatbiztonsági kockázatok is növekedtek, így kiemelten fontos annak vizsgálata, hogy a munkavállalók hogyan érzékelik az otthoni munkakörnyezet biztonságát, valamint mennyire érzik magukat felkészültnek egy esetleges kibertámadásra vagy adatbiztonsági incidensre. Kutatásunk célja az volt, hogy feltárjuk a távmunkában dolgozók adatbiztonsággal kapcsolatos percepcióit és a kibertámadásokkal szembeni felkészültségüket.

A vizsgálat során két fő kérdést elemeztünk:

- „Mennyire tartja biztonságosnak az otthoni munkavégzést adatbiztonsági szempontból?"
- „Mennyire érzi magát felkészültnek egy adatbiztonsági incidens esetén?"

A válaszokat egy 1-től 5-ös terjedő Likert-skálán gyűjtöttük, ahol az 1-es érték azt jelentette, hogy a válaszadó egyáltalán nem tartja biztonságosnak vagy felkészültnek magát, míg az 5-ös érték a teljes mértékben biztonságosnak vagy felkészültnek való megítélést jelölte.

Az adatok statisztikai elemzéséhez átlag- és szórásértékeket számítottunk, hogy pontosabb képet kapjunk a válaszok eloszlásáról és az érzékelt biztonsági szintek közötti eltérésekről. Az eredmények segítenek megérteni, hogy a távmunkában dolgozók mennyire érzik magukat biztonságban az otthoni munkavégzés során, illetve milyen mértékben tartják magukat felkészültnek az esetleges kibertámadásokkal szemben.

	Mennyire tartja biztonságosnak az otthoni munkavégzést adatbiztonsági szempontból?	**Mennyire érzi magát felkészültnek egy adatbiztonsági incidens esetén?**
Összesen	71	71
Középérték/átlag	4,32	3,13
Szórás	1,03	1,35
Minimum	1	1
Első kvartilis	4	2
Második kvartilis	5	3
Harmadik kvartilis	5	4
Maximum	5	5

1. Táblázat: Az otthoni munkavégzés biztonságosságának és a kibertámadásra való felkészültség statisztikai mutatói Forrás: Saját kutatás, 2025, N=71

Az eredmények szerint a résztvevők átlagosan 4,32-es értékkel ítélték meg az otthoni munkavégzés biztonságosságát, míg kibertámadás esetén saját felkészültségüket 3,13-as átlagértékre értékelték. A szórás adatokból látható, hogy az egyéni érzékelés jelentős tér el, különösen a kibervédelmi felkészültség esetében.

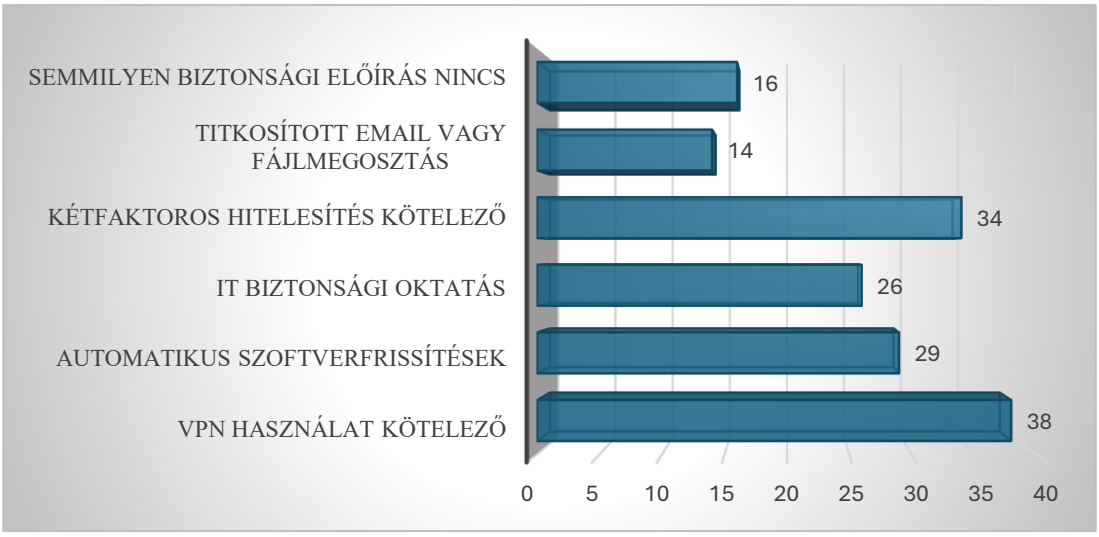
Az alábbi táblázat alapján az adatbiztonsági incidensek előfordulásának aránya és az IT biztonsági oktatásban való részvétel közötti kapcsolat vizsgálható a vállalat méretének függvényében. A cél annak megértése, hogy a nagyobb vállalatok jobban védettek-e az incidensekkel szemben, és hogy az IT biztonsági oktatás befolyásolja-e a kockázatokat.

Vállalatméret	Incidens történt	Összesen vállalt	Incidens aránya	IT biztonsági oktatásban részesült	IT biztonsági oktatásban részesült aránya
1-10 fő	3	12	25%	2	17%
11-50 fő	2	12	17%	6	50%
51-250 fő	1	11	9%	10	91%
251-1000 fő	3	18	17%	14	78%
1000+ fő	1	18	6%	14	78%
Összesen	10	71	14%	46	65%

2. Táblázat: Vállaltméret, adatbiztonsági incidensek és IT biztonsági oktatás összefüggései. Saját kutatás, 2025, N=71

Az eredmények szerint a kisebb vállalatoknál az incidensek előfordulása magasabb (25%), míg a nagyvállalatoknál jelentősen alacsonyabb (6%). Az IT biztonsági oktatásban részesültek aránya szintén méretfüggő: a mikrovállalkozások esetében csupán 17%, míg a nagyobb szervezeteknél 78–91% között mozog. Ez arra utal, hogy a vállalatok méretük növekedésével párhuzamosan egyre nagyobb figyelmet fordítanak a kibervédelemre és a munkavállalók képzésére.

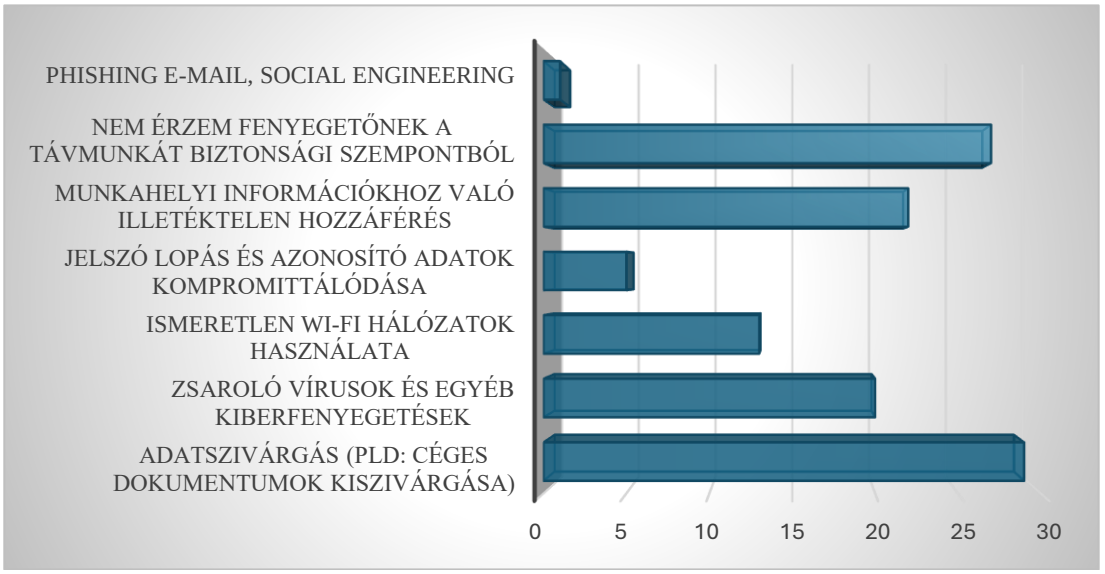
Az alábbi ábra a kibervédelmi intézkedések alkalmazására adott válaszokat szemlélteti. A kérdés többválasztásos volt, így a válaszadók több intézkedést is megjelölhettek, amelyeket távmunkájuk során alkalmaznak. Az ábra az összesített eredményeket mutatja, lehetővé téve a különböző biztonsági megoldások elterjedtségének áttekintését.



6. Ábra: Kibervédelmi intézkedések elérhetősége távmunkában Forrás: Saját kutatás, 2025, N = 71

Az eredmények szerint a munkáltatók általában biztosítanak alapvető védelmi mechanizmusokat, például VPN-t, kétfaktoros hitelesítést, azonban az IT biztonsági oktatás nem minden dolgozó számára érhető el, ami csökkentheti a védelmi intézkedések hatékonyságát.

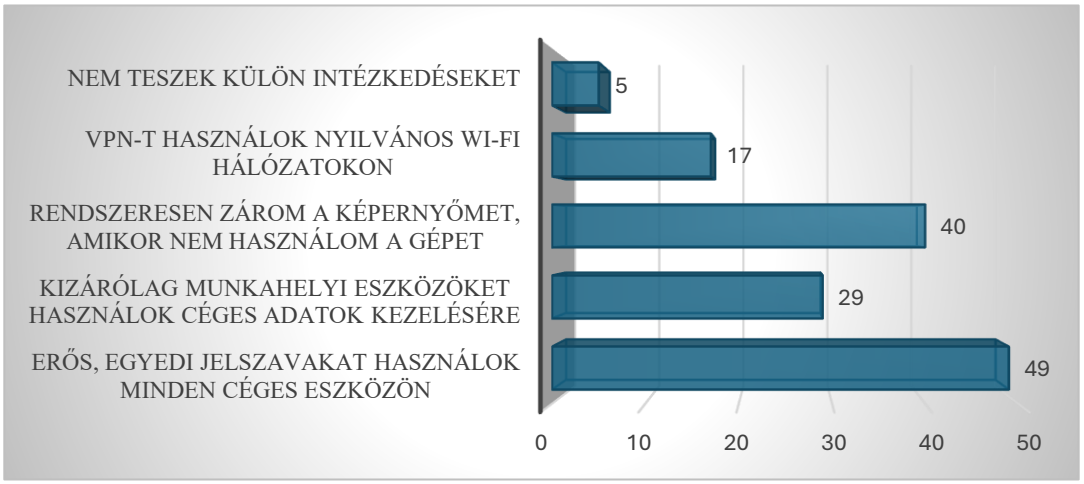
A következő ábra a távmunka során észlelt legnagyobb biztonsági kockázatokat szemlélteti. A kérdés többválasztásos volt, így a válaszadók több kockázati tényezőt is megjelölhettek. Az eredmények összesített formában mutatják, hogy mely biztonsági fenyegetések jelentik a legnagyobb kihívást a távmunkát végzők számára.



7. Ábra: A távmunka során észlelt legnagyobb biztonsági kockázatok Forrás: Saját kutatás, 2025, N = 71

A legnagyobb fenyegetések közé tartozik az adatszivárgás, az azonosító adatok ellopása és a hálózati támadások, amelyek különösen kockázatosak azok számára, akik nem megfelelően védett hálózatokon dolgoznak.

Az alábbi ábra a távmunka során alkalmazott adatbiztonsági intézkedéseket szemlélteti. Mivel a kérdés többválasztásos volt, a válaszadók több intézkedést is megjelölhettek. Az összesített eredmények alapján látható, hogy milyen védelmi gyakorlatokat alkalmaznak a távoli munkavégzés során.



8. Ábra: Intézkedések a saját adatbiztonság érdekében Forrás: Saját kutatás, 2025, N = 71

Az eredmények szerint a legtöbben jelszókezelést és képernyőzárat használnak, míg a VPN és a munkahelyi eszközök kizárólagos használata kevésbé elterjedt. A válaszok alapján szükség lenne további biztonságtudatossági képzésre, különösen azok számára, akik nem alkalmaznak semmilyen védelmi mechanizmust.

A kérdőívben egy nyitott kérdés is szerepelt, amelyben a válaszadók megoszthatták véleményüket arról, hogy mely fejlesztési területeket tartják a legfontosabbnak a távmunka biztonságának javítása érdekében. Az alábbi szófelhő a leggyakrabban említett válaszokat szemlélteti, összegyűjtve a legfontosabb fejlesztési javaslatokat.

9. Ábra: Legfontosabb fejlesztési területek a távmunka biztonságában Forrás: Saját kutatás, 2025, N = 71

A visszajelzések alapján négy fő fejlesztési irány emelhető ki:

- IT biztonsági oktatás és tudatosság növelése
- Otthoni és nyilvános hálózatok biztonságának erősítése
- Biztonságos céges eszközök és szoftverek biztosítása
- Hitelesítési és titkosítási megoldások kiterjesztése

Az adatok azt mutatják, hogy a munkavállalók nagy része a tudatosság növelését és a technikai védelem erősítését tartja a legfontosabbnak. Ennek megfelelően a távmunka biztonságának javítása érdekében olyan komplex stratégia alkalmazása szükséges, amely magában foglalja a technikai intézkedéseket, a szabályozási keretek erősítését és a munkavállalói képzések szélesítését.

A kutatás eredményei alapján komplex stratégiára van szükség, amely ötvözi a technikai védekezési eszközöket és a biztonságtudatossági programokat annak érdekében, hogy a

távmunka biztonságos és fenntartható legyen mind a munkáltatók, mind a munkavállalók számára.

KÖVETKEZTETÉSEK

A kutatás eredményei egyértelműen igazolják, hogy a távmunka elterjedése jelentős kihívásokat teremtett a munkahelyi biztonság és adatvédelem terén. A válaszadók több mint 60%-a rendszeresen végez távmunkát, többségük otthoni környezetben, ahol a munkáltatók által biztosított biztonsági mechanizmusok nem mindig elegendőek a kockázatok hatékony kezelésére. A kutatás eredményei arra utalnak, hogy a kisebb vállalatoknál az adatbiztonsági incidensek előfordulási aránya magasabb (25%), míg a nagyobb vállalatoknál ez lényegesen alacsonyabb (6%), ami összefüggésben állhat az IT biztonsági oktatás eltérő szintjeivel és a védelmi intézkedések különbözőségével.

A távmunka során észlelt legnagyobb kockázatok közé az adatszivárgás, az azonosító adatok kompromittálódása és a hálózati támadások tartoznak, amelyek különösen veszélyesek azok számára, akik nem megfelelően védett hálózatokon keresztül dolgoznak. Bár számos munkáltató biztosít alapvető védelmi mechanizmusokat, például VPN-t és kétfaktoros hitelesítést, az IT biztonsági oktatás még nem ér el minden dolgozót, ami csökkentheti a védelmi intézkedések hatékonyságát. A kutatás eredményei azt mutatják, hogy a kisebb cégeknél a kibervédelmi tudatosság növelése kulcsfontosságú, míg a nagyobb szervezetek esetében a meglévő védelmi stratégiák folyamatos fejlesztésére van szükség.

Az alábbi javaslataim vannak a távmunka biztonságának növelésére:

- IT biztonsági oktatás és tudatosság növelése: Az alkalmazottak folyamatos képzése elengedhetetlen annak érdekében, hogy tisztában legyenek az adatbiztonsági kockázatokkal és a megfelelő védekezési módszerekkel. A rendszeres kibervédelmi tréningek bevezetése segítheti a munkavállalókat a fenyegetések felismerésében és a megfelelő biztonsági gyakorlatok alkalmazásában.
- Kibervédelmi intézkedések fejlesztése: A vállalatoknak érdemes átfogó biztonsági stratégiát kialakítaniuk, amely magában foglalja a VPN-használat kiterjesztését, a kétfaktoros hitelesítés alkalmazását minden távoli belépés esetén, valamint a munkahelyi eszközök és szoftverek titkosítását. Az endpoint security és a folyamatos monitorozás segíthet a potenciális fenyegetések gyors észlelésében és kezelésében.
- Otthoni és nyilvános hálózatok biztonságának erősítése: A kutatás kimutatta, hogy a munkavállalók szoktak kevésbé védett hálózatokon dolgozik, ezért kiemelten fontos az otthoni Wi-Fi hálózatok megfelelő védelme, például erős jelszavak, tűzfalak és biztonságos routerbeállítások alkalmazásával. A vállalatoknak biztosítaniuk kell azokat az eszközöket és útmutatókat, amelyekkel a távmunkát végzők saját otthoni környezetük biztonságát növelhetik.
- Biztonságos céges eszközök és szoftverek biztosítása: A munkahelyi eszközök és a vállalati adatkezelés elkülönítése érdekében célszerű a munkáltatóknak olyan eszközöket biztosítaniuk, amelyeken előre konfigurált biztonsági beállítások és ellenőrzött szoftverek futnak. Az árnyékinformatika (shadow IT) kiküszöbölése érdekében érdemes belső szabályzatokat bevezetni az engedélyezett alkalmazások és hardverek használatára vonatkozóan.

- Hitelesítési és titkosítási megoldások kiterjesztése: Az érzékeny adatok védelme érdekében a vállalatoknak olyan titkosítási technológiákat kell alkalmazniuk, amelyek biztosítják az adatok sértetlenségét és illetéktelen hozzáférés elleni védelmét. A biometrikus azonosítás, hardveres biztonsági kulcsok és fejlett titkosítási protokollok bevezetése hatékony védelmet nyújthat.
- Munkáltatói szabályozás és irányelvek frissítése: A távmunka biztonsági kockázatainak kezelése érdekében a vállalatoknak naprakész belső szabályzatokat kell kidolgozniuk, amelyek egyértelmű iránymutatást adnak a munkavállalóknak a biztonságos munkavégzésre vonatkozóan. Ezeknek az irányelveknek tartalmazniuk kell a távoli munkavégzés során elvárt magatartásformákat, az eszközhasználatra vonatkozó előírásokat, valamint az adatkezelési és incidensjelentési protokollokat.

A kutatás eredményei alapján megállapítható, hogy a távmunka biztonságának növelése egy komplex, többszintű megközelítést igényel, amely ötvözi a technológiai védekezési megoldásokat, a munkavállalók képzését és a szabályozási keretek fejlesztését. A jövőbeli kutatások fókuszálhatnak a kibervédelmi technológiák hatékonyságának elemzésére, valamint a munkavállalók és munkáltatók biztonságtudatosságának hosszú távú alakulására. A megfelelő biztonsági protokollok bevezetésével és folyamatos fejlesztésével biztosítható, hogy a távmunka hosszú távon is fenntartható és biztonságos legyen mind a munkáltatók, mind a munkavállalók számára.

ÖSZEFOGLALÁS

A tanulmány a távmunka elterjedésével kapcsolatos biztonsági kihívásokat vizsgálja, különös tekintettel az adatvédelemre, a kibervédelemre és a munkavállalók biztonságtudatosságára. A kutatás kérdőíves módszert alkalmazott, amely kvantitatív adatokat szolgáltatott a távoli munkavégzés gyakoriságáról, a használt technológiai megoldásokról és a vállalatok által biztosított védelmi intézkedésekről.

Az eredmények rámutatnak arra, hogy a távmunkát végző munkavállalók jelentős része otthonról dolgozik, azonban a biztonsági kockázatok és a védelmi intézkedések alkalmazása szervezeti mérettől függően eltérő. A kisebb vállalatoknál az adatbiztonsági incidensek aránya magasabb, míg a nagyobb cégek hatékonyabb védelmi stratégiákat alkalmaznak, például VPN-t, kétfaktoros hitelesítést és rendszeres IT biztonsági oktatásokat. A legnagyobb biztonsági fenyegetések közé az adatszivárgás, az azonosító adatok kompromittálódása és a hálózati támadások tartoznak, amelyek a távoli munkavégzés során kiemelt figyelmet igényelnek.

A tanulmány kiemeli, hogy a távmunka biztonságának növelése érdekében szükség van az IT biztonsági tudatosság fejlesztésére, az adatvédelmi intézkedések egységesítésére és a munkáltatói szabályozások frissítésére. A kutatás eredményei alapján javasolt lépések közé tartozik az IT biztonsági képzések elérhetővé tétele, az otthoni hálózatok védelmének megerősítése, a munkáltatók által biztosított céges eszközök és szoftverek alkalmazása, valamint a hitelesítési és titkosítási technológiák szélesebb körű bevezetése.

Összességében a kutatás arra hívja fel a figyelmet, hogy a távmunka biztonságos és fenntartható működéséhez átfogó stratégia szükséges, amely ötvözi a technológiai védekezési intézkedéseket, a munkavállalói tudatosság növelését és a szervezeti szabályozás fejlesztését. Az eredmények hozzájárulhatnak a vállalatok adatbiztonsági politikájának kialakításához és a távmunka hosszú távú fenntarthatóságának biztosításához.

FELHASZNÁLT IRODALOM

[1] Cs. Kollár and J. Poór, „Organisations in Digital Age - Information Security Aspects of Digital Workplaces," Management, Enterprise and Benchmarking in the 21st Century, pp. 73-82, 2016.

[2] K. Tardos, Esélyegyenlőség és családbarát vállalati gyakorlatok, mtd Tanácsadói Közösség, Budapest: mtd Tanácsadói Közösség; MTA Társadalomtudományi Kutatóközpont, Szociológiai Intézet, 2014.

[3] T. Venczel-Szakó, G. Balogh and I. Borgulya „Távmunka, home office: hogyan érinti a távolról dolgozás a szervezet intern kommunikációját?," Vezetéstudomány - Budapest Management Review, vol. 52, no. 2, pp. 73-86, 2021.

[4] K. Lazányi and Y. Bilan, „Generation Z on the labour market: do they trust others within their workplace?," Polish Journal of Management Studies, pp. 78-93, vol. 16, no. 1 2017.

[5] Európai Munkahelyi Biztonsági és Egészségvédelmi Ügynökség (EU-OSHA), „Távmunka a COVID-19-világjárvány idején: kockázatok és megelőzési stratégiák," EU-OSHA jelentés, 2021.

[6] Á. Jarjabka, G. Kuráth, N. Sipos, T. Venczel-Szakó, B. Szabó-Bálint, G. balogh and A. Uhrin, „Rugalmasság, produktivitás vagy elszigeteltség? Avagy a COVID-19 hatása a felsőoktatásban oktatók munkavégzésére," Magyar Tudomány, vol. 181, no.12. pp. 1698-1710, 2020.

[7] F. Pataki-Bittó and Á. Kun, „Exploring differences in the subjective will-being of teleworkers prior to and during the pandemic," International Journal of Workplace Health Management, vol. 15, no. 3, pp. 320-338, 2022.

[8] A. Nagy and T. Z. Wentzel Antal, „A távmunka dogmatikai problémái az elméletben és a gyakorlatban - A távmunka fogalmának megreformálására tett kísérlet," Munkajog, vol. 2024, no. 1, pp. 44-54, 2024.

[9] E. Törő and G. Károlyi, „A távmunkavégzés új szabályai, különös tekintettel a munkavédelmi előírásokra," Munkajog, vol. 2022, no. 2, pp. 15-27, 2022.

[10] T. Forgács, A távmunka elmélete és gyakorlati alkalmazásának lehetőségei, Pécsi Tudományegyetem, 2009.

[11] Nemzeti Kibervédelmi Intézet (NKI), Újragondolt IT biztonsági kockázatelemzés a távmunka viszonylatában, Budapest: (NKI), Nemzeti Kibervédelmi Intézet, 2019.

[12] Nemzeti Kibervédelmi Intézet (NKI), Otthoni munkavégzés és utazás – adatbiztonság a munkahelyen kívül, Budapest: (NKI), Nemzeti Kibervédelmi Intézet, 2019.

[13] A. Beláz, "A magyar kibervédelmi szabályozás továbbfejlesztésének lehetőségei – Különös tekintettel a stratégiaalkotásra", Budapest: Nemzeti Közszolgálati Egyetem, 2017.

[14] A. Lukács, „A távmunka során felmerülő sajátos adatvédelmi kérdések," Szegedi Tudományegyetem, Szeged, 2013.

[15] K. László, „A távmunka és távoli hozzáférés IT biztonsági követelményei – az MNB 12/2020 (XI.6.) számú ajánlása," Hétpecsét Információbiztonsági Egyesület, Budapest, 2020.

[16] P. J. Horváth, É. S. Somossy and T. Tóth, „A decentralizált villamosenergia-rendszerek fejlődésének nemzetközi és hazai szempontjai,” Közgazdasági Szemle,vol. 69, no. 6, pp. 697–720, 2022.

[17] I. Székely and Gy. Vasvári, „Adatvédelem és/vagy adatbiztonság?,” Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest, 2004.

[18] V. Honfi and Z. Illési, „COVID-19, Home Office, Cybersecurity,” Journal of Cybersecurity, 2020.

[19] B. R. Barna, Cs. Kollár and E.D. Oroszi, „A social engineering helye az információbiztonsági auditban,” Biztonságtudományi Szemle, p. 25–41, 2023.

[20] Cs. Krasznay and G. Gyebnár, „Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems,” *Proceedings of the 13th International Conference on Cyber Conflict (CyCon)*, p. 171–188, 2021.

[21] A. Faludi and L. Szabó, „Villamosenergia-rendszer üzeme és irányítása,” Budapesti Műszaki és Gazdaságtudományi Egyetem (BME), Budapest, 2002.