

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

A PRIVÁTSZFÉRÁT ERŐSÍTŐ TECHNOLÓGIÁK SZEREPE A KIBERBIZTONSÁGBAN

Jelige: *privacy18*

Pályamunka lezárásának időpontja:
2022. május

2023.

A PRIVÁTSZFÉRÁT ERŐSÍTŐ TECHNOLOGIÁK SZEREPE A KIBERBIZTONSÁGBAN

Kézirat lezárásának a dátuma

2022. április 19.

Tartalomjegyzék

Bevezetés.....	1
A téma aktualitása	1
A tudományos probléma megfogalmazása	2
Kutatási célkitűzések.....	3
Kutatási hipotézisek megfogalmazása	4
Kutatási módszertan	4
1. fejezet – A privátszférát erősítő technológiák.....	5
1.1. A PET-ek és az információbiztonság	6
1.2. A privátszférát erősítő technológiák fogalmi meghatározása.....	8
1.2.1. A PET-ek és a kibertér kapcsolata, a fizikai lehetőségek különválasztása	9
1.3. A PET-ek rendszertana, alapvető kritériumaik és csoportosításuk	10
1.3.1. A PET-ek alapvető kritériumai	10
1.3.2. A PET-ek csoportosítása	11
1.3.3. A PET-ek rendszertana.....	12
1.4. Példák, kategorikus ismertetőik.....	13
1.5. Privacy by design.....	16
Következtetések	17
2. fejezet – Szakértői interjúk.....	18
2.1. Humán tényező az információbiztonságban.....	18
2.2. A privátszféra és kapcsolódó fenyegetések	22
Következtetések	24
3. fejezet – Az empirikus kutatás bemutatása	25
3.1. Az empirikus kutatás összeállítása	25
3.2. A kérdőív kiértékelés	25
3.2.1. Statisztikák	26
3.2.2. Az empirikus kutatás eredményei	28

3.2.3. Tudományos elemzés	32
Következtetések	36
Összegzés	36
További kutatást igénylő területek	37
Irodalomjegyzék.....	39
Függelék, mellékletek	42
Rövidítések jegyzéke.....	42
Ábrajegyzék	43
Táblázatok jegyzéke:	43
Mellékletek.....	43

Bevezetés

Dolgozatom elsődleges célja feltárni a privátszférát erősítő technológiák ismérveit, jelenlegi szerepüket és hasznosíthatóságukat, a fenyegetésekkel szembeni relevanciájukat és alkalmazási lehetőségeiket, melyekkel potenciálisan növelhető az egyének és szervezetek kiberbiztonsági képessége.

A téma aktualitása

XXI. századi társadalmunkra gyakran információs társadalomként szoktunk hivatkozni, mely nem véletlen, ugyanis az egyre növekvő számú és egyre fejlettebb infokommunikációs technológiák (továbbiakban: IKT) mára életünk megannyi szegmensében kulcsfontosságú szerepet játszanak. Ide tartozik a családtagjainkkal, barátainkkal, ismerőseinkkel és munkatársainkkal történő kapcsolattartás, a közösségi média használata, de összességében a mindennapos teendők virtuális térbe történő integrálódása is. Utóbbiak kapcsán a rendelkezésünkre álló szolgáltatások és lehetőségek közül a taxatív felsorolás és teljesség igénye nélkül gondolhatunk például az online ügyintézésre, számlabefizetésre, pénzügyeink kezelésére, vásárlásra, a szolgáltatások széles tárházának igénybevételére, ismereteink nagyarányú bővítésének lehetőségére, ismeretszerzésre, érdeklődésünk kiszélesítésére, mely kapcsán számtalan (szabad)időtöltési lehetőséget találhatunk az online térben.

Mind ezek tekintetében elmondható, hogy a jelenlegi innovációs folyamatok jelentősen hozzájárulhatnak a komfortosabb, egyszerűbb és kényelmesebb, a történelem során eddig még sosem tapasztalt életmódhoz.

Azonban egy ismert közgazdasági alaptörvény szerint „There’s no free lunch”, valakinek mindig állnia kell a költségeket, semmi sincs ingyen. Az első bekezdésben felsorolt lehetőségeink jelentős része ingyenes, viszont még az anyagi vonzattal járó szolgáltatások igénybevétele sem jelent kivételt az alábbiak alól:

A költségvonzat nélkül igénybe vett szolgáltatások tekintetében az adott felület, platform, eszköz, szoftver vagy alkalmazás az annak használata közben gyűjtött adatokat „jobb esetben” például célzott hirdetési tevékenységek kapcsán értékesíti. Rosszabb esetben – és ennek sajnos időről-időre szemtanúi lehetünk – a szolgáltató a rendelkezésére álló személyes adatokat is kifejezetten sajátos üzleti érdekei szerint, bármilyen adatvédelmi szabályzó figyelembevétele

nélkül értékesítheti, melyre egy eklatáns közelmúltban történt példa a Facebook-Cambridge Analytica botrány, mely kapcsán 87 millió személyes adatot használtak fel jogszerűtlenül. Amennyiben pedig kategorizálni kell, úgy a legrosszabb esetek közé a különböző, nem ritkán akár több tíz- vagy százmillió felhasználót érintő adatszivárgások tartoznak. Ezek tekintetében nem pusztán üzleti szempont szerinti értékesítéséről, hanem a személyes adatok kapcsán azok rosszindulatú, potenciálisan kibertámadásokban történő felhasználásáról beszélhetünk.

Az anyagi vonzattal igénybe vett szolgáltatások esetében sincs másként a helyzet, ugyanis azok fejlesztése, szofisztikálása, felhasználóbarátabbá tétele, és az értéknövelés vonatkozásában ugyanúgy nagyarányú, a felhasználókról történő adatgyűjtésre támaszkodhatnak, és különbséget maximum a „jobb eset” kapcsán tapasztalhatunk, ha nem célzott hirdetésekre, hanem a saját szolgáltatás javítására használják fel azokat. Ám a jogszerűtlen, adatokat érintő értékesítés, vagy adatszivárgás vonatkozásában az ingyenes szolgáltatóknál is megfogalmazott problémákat definiálhatjuk.

A tudományos probléma megfogalmazása

Kutatásom tudományos problémájának középpontjában az előzőekben megfogalmazottakból eredően a rólunk – akár beleegyezésünkkel – gyűjtött adatok értékesítése vagy kiszivárgása esetén fennálló potenciális veszélyforrások problémaköre, és azoknak a privátszférát erősítő technológiák (továbbiakban: PET) általi csökkentési lehetőségeinek vizsgálata áll.

A különböző online felületek, szolgáltatások, IoT eszközök (Internet of Things – internetes hozzáféréssel, hálózati kommunikációs képességekkel rendelkező eszközök), szoftverek vagy alkalmazások több ezer szempont szerint gyűjtenek adatokat a felhasználókról, melyek egyaránt felhasználhatók egyéni, vagy lokális, regionális, esetleg globális mintázatokban.

A tudományos probléma szűkítése kapcsán az ezen – kiszivárgott vagy értékesített – adatokból megvalósítható profilozás veszélye emelhető ki. Az Európai Unióban (továbbiakban: EU) 2018. május 25-től kezdődően hatályban lévő, az Európai Parlament (továbbiakban: EP) által elfogadott általános adatvédelmi rendelet (továbbiakban: GDPR) már nem csak azokat a döntéseket szabályozza, melyek az automatizált adatfeldolgozással és profilalkotással vannak összefüggésben, hanem már keretet adnak a profilozással kapcsolatos adatok gyűjtésének is. A profilalkotás alapvető ismérvei kapcsán annak fogalma az alábbiak szerint határozható meg: a

profilozás / profilalkotás a személyes jellemzők értékelése, elemzése és meghatározása céljából a személyes adatokon végzett automatizált adatfeldolgozás.¹

A profilalkotás egy súlyos következménye lehet a sikeres kibertámadások számának növekedése, ugyanis a támadók – akár az említett lehetőségek (vásárlás, adatszivárgás) kapcsán rendelkezésre álló adatokból – a profilozás következtében az eredményeket felhasználhatják az egyénnel vagy meghatározott csoportokkal kapcsolatos előrejelzések készítésére, valamint következtetések levonására.

A profilalkotás tehát egy adott személyre, vagy személyek meghatározott csoportjára jellemző viselkedési mintáknak az elemzését jelenti annak érdekében, hogy azok egy bizonyos kategóriába, keretrendszerbe sorolhatóak legyenek, melyekből előrejelzések és/vagy értékelések készíthetők.

Összességében elmondható, hogy a különböző, a dolgozatban több szempont alapján elemzett és részletezett, valamint a kutatás tárgyát is képző privátszférát erősítő technológiák védelmi szempontból egy adekvát választ nyújtanak az előzőekben részletezett fenyegetésekkel szemben.

Kutatási célkitűzések

Kutatásom elsődleges célja, hogy felmérjem a privátszférát erősítő technológiák befogadásának és akár a mindennapi életbe, otthoni és munkahelyi környezetbe történő integrálásának lehetőségeit és különböző aspektusait. Ehhez kapcsolódóan a kutatás további célja jelen kérdéskörben hazai, az állami- és magánszektor egyaránt felölelő, a mindennapos munkavégzés során elsajátított gyakorlattal rendelkező szakértőkkel, valamint a tudományos élet elismert kutatóival készített szakmai interjúk összevetése.

A fő cél az interjúk és az empirikus felmérés, a kérdőívek kapcsán, hogy a konzekvenciák levonásával jó gyakorlatot határozhassunk meg, mely magában hordozza a védettség prosperálásának lehetőségét egyaránt egyéni és vállalati szinten.

¹ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Kutatási hipotézisek megfogalmazása

A kutatási téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

H1. Az információbiztonság növelhető szervezeti szinten a munkavállalók számára nyújtott, a privátszférát erősítő technológiák alkalmazását elősegítő oktatások, képzések által.

H2. Az egyének a munkahelyi környezetben alkalmazott PET-eket otthoni környezetben is alkalmaznák.

H3. A szervezetet fenyegető támadások tekintetében a munkavállalók nem tekintenek önmagukra kiemelt kockázatként, és nem realizálják a privátszféra nem megfelelő szintű védelméből adódó kockázatokat sem.

H4. A munkavállalók a szervezet védett rendszereihez történő hozzáférés esetén fokozottabban ügyelnek az adatvédelmi megoldásokra egyaránt otthoni és munkahelyi környezetben is.

Kutatási módszertan

Kutatásom empirikus részét egy 154 főből álló mintán készült kérdőíves felmérés adta.

A módszertan alapját a tudás-képesség-viselkedés modell és az információbiztonság humán aspektusa (Human Aspects of Information Security Questionnaire (HAIS-Q)) modell alapján elkészített kérdőíves felmérés jelentette, melyet tudományos statisztikai módszertannal (keresztábra-elemzéssel) értékeltem ki, az IBM SPSS Statistics szoftver segítségével.

A módszertan részét képezte továbbá az empirikus kutatás eredményeinek összevetése a szakmai interjúk konklúzióival.

A felhasznált szakanyagot releváns hazai, és nemzetközi (Scopus, Springer, Taylor & Francis, Science Direct) szakirodalomra alapozva implementáltam a kutatásomba. A nemzetközi szakirodalmak feldolgozásakor, adoptálásánál igyekeztem a Scimago Journal Rank (továbbiakban: SJR) által Q1-esként kategorizált folyóiratokat alapul venni.

Dolgozatomban a hivatkozásokat a Zotero nevű hivatkozáskezelő program segítségével készítettem, Chicago Manual of Style of 17th Edition hivatkozási stílusban.

1. fejezet – A privátszférát erősítő technológiák

Az információs technológiák rohamos fejlődése lehetővé teszi a minden korábbinál jobb és hatékonyabb adatgyűjtést, valamint a különböző adatok felhasználására, összevetésére, elemzésére tervezett – bizonyos esetekben jogszerűtlenül használt – platformok létrehozását. A személyes adatok gyűjtése és feldolgozása gyakran decentralizált módon, különböző kontextusokban, módszerekkel és számtalan indokból történhet. Az elosztott alkalmazások megjelenésével a szolgáltatók általában összevetik saját nyilvántartásaikat, és személyre szabott szolgáltatásokat nyújtanak ügyfeleiknek. Ezen gyakorlatra gyakran teljes üzleti modellek épülhetnek, melyek célja a profitmaximalizáció többek között a célzott hirdetések, vagy akár hírek minél hatékonyabb célbajuttatásával. Az összegyűjtött adatok közé tartoznak a földrajzi és beltéri (geolokációs) pozíciók, ideértve a felhasználók mozgásmintáit, valamint a gyűjtött elemek közé tarthatnak a különböző érzékelők által gyűjtött adatok, amelyekből kiderülhet a felhasználók fizikai állapota, szokásai és érdeklődési köre is. Következésképpen ez olyan nemkívánatos következményekhez vezethet, mint a kéretlen reklámok, de rosszabb esetben ezen adatok jogszerűtlen felhasználása, amely például diszkriminációhoz és zaklatáshoz is vezethet. A bevezetésben már említett profilozás pedig (például egy adatszivárgás következtében) potenciális veszélyforrást jelenthet a sikeres humán-alapú támadások végrehajtásának tekintetében.^{2,3,4,5}

A magánéletünk biztonságát fenyegető veszélyek mérséklésére számos technika jelent meg, amelyeket összefoglaló néven angolul privacy enhancing technologies-ként, magyarul privátszférát erősítő technológiaként, röviden pedig PET-ekként nevezhetünk.

Ebben a fejezetben szeretném bemutatni a privátszférát erősítő technológiák fogalmi hátterét, azok alapvető kritériumait, csoportosíthatósági lehetőségeit és rendszertanát, az információbiztonsággal kapcsolatos viszonyát, valamint a kibertér vonatkozásában a fizikai tér

² James Curzon, Abdulaziz Almeahmadi, és Khalil El-Khatib, „A Survey of Privacy Enhancing Technologies for Smart Cities”, *Pervasive and Mobile Computing* 55 (2019. április): 76–95, <https://doi.org/10.1016/j.pmcj.2019.03.001>.

³ Nesrine Kaaniche, Maryline Laurent, és Sana Belguith, „Privacy Enhancing Technologies for Solving the Privacy-Personalization Paradox: Taxonomy and Survey”, *Journal of Network and Computer Applications* 171 (2020. december): 102807, <https://doi.org/10.1016/j.jnca.2020.102807>.

⁴ David Reinsel, John Gantz, és John Rydning, „The Digitization of the World from Edge to Core”, International Data Corporation White Paper. 2018, 28.

⁵ Daniele Riboni és Claudio Bettini, „Differentially-private release of check-in data for venue recommendation”, in *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)* (2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), Budapest, Hungary: IEEE, 2014), 190–98, <https://doi.org/10.1109/PerCom.2014.6813960>.

különbözöseit, illetve a beépített alapértelmezett adatvédelmi megoldásokat, és a konkrét példákat, kategorikus ismertetőket.

1.1. A PET-ek és az információbiztonság

Miért fontos kiemelni a privátszférát erősítő technológiák kapcsán az információbiztonságot? Ahogy a gyakran ismételt anekdota is tartja, a kiberbiztonság leggyengébb láncszeme az ember. Ebből az alapvetésből kiindulva pedig a személyek egyéni biztonságát és a szervezeti biztonságot is összességében az információs rendszereket akár otthoni, akár munkahelyi környezetben kezelő emberek információbiztonsági (-tudatossági) attitűdjéből és kompetenciáiból kiindulva tudjuk vizsgálni.

Egy szervezet biztonságának szempontjából annak védelmi képességei pontosan annyira hatékonyak, amennyire az információs rendszerhez hozzáférő legalacsonyabb biztonság tudatossággal, vagy legkisebb információbiztonsági (szakmai) attitűdökkel rendelkező munkavállaló képességei, ugyanis a támadók ezeken a személyeken keresztül férhetnek hozzá a legegyszerűbb, leggyorsabb és legköltséghatékonyabb módon a támadni kívánt információs rendszerekhez.

Jelen problémakör pedig az állami szférában dolgozók, illetve szervezeti szempontból a védett rendszerekhez hozzáférő munkavállalók szempontjából egyértelműen kiszélesedik, és egy jelentősebb kiberbiztonsági kockázatot jelent.

Az informatikai biztonság egyik alapelve az úgynevezett CIA triád, mely a bizalmasság (Confidentiality), sértetlenség (Integrity), és rendelkezésre állás (Availability), együttes, megkerülhetetlen és a megfelelő mértékben fenntartott alkalmazását írja elő a fennálló fenyegetettségekkel szembeni hatékony védekezés okán. Ez a magyar jogrendben a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.) szóló jogszabályban került lefektetésre.

A PET-ek általában nagyobb hangsúlyt fektetnek a biztonság bizalmas jellegére, pontosabban az egyének vagy személyes adataik, személyazonosságuk elrejtésére. A PET-ek esetében olyan szempontok is említésre kerülnek, mint az anonimitás, az összeköthetetlenség és a megfigyelhetetlenség.⁶ Az anonimitás azt az esetet írja le, amikor a támadó nem tud azonosítani

⁶ Johannes Heurix és mtsai., „A Taxonomy for Privacy Enhancing Technologies”, *Computers & Security* 53 (2015. szeptember): 1–17, <https://doi.org/10.1016/j.cose.2015.05.002>.

egy adott alanyt a számára rendelkezésre álló halmazon belül. Egy hasonló fogalom és kapcsolódó elem, a pszeudonimitás esetén a valódi nevek helyett álneveket használnak az alanyok azonosítójaként. Ez lehetővé teszi az egyes alanyok egyedi, de a valóstól eltérő alapokon nyugvó azonosítását egy halmazon belül (vagy az álnevek kiválasztásától és újrafelhasználásától függően az alanyok egy csoportján belül), miközben az alany tényleges személyazonossága továbbra is rejtve marad.⁷

Az információbiztonsági tudatosságot és a megfelelő kompetenciákat számtalan módon van lehetőségünk erősíteni és a mindennapi életben gyakorlati szinten alkalmazni. Alapvetően a védelem prosperálására alkalmazhatunk különböző szoftveres- és fizikai biztonsági megoldásokat, kötelező érvényű szabályzókat, szervezhetünk és rendezhetünk tudatosító oktatásokat, kampányokat, valamint bevezethetünk vagy ajánlásként megfogalmazhatunk bizonyos kiberhigiéniai erősítő és a digitális lábnyomokat minimalizáló megoldásokat. Mind ezek egyik szegmense a privátszférát erősítő technológiák alkalmazása.

A „Bevezetés”-ben megfogalmazott és részletezett profilalkotást a sikeres humán-alapú támadások egyik fő indikátoraként azonosíthatjuk. Ennek fő oka, hogy a profilalkotás következtében a támadó rendelkezésére állnak azok az információk (pl. személyes jellemzők, érdeklődési kör, viselkedési minták, stb.) a célponttól, melyek segítségével ki tudja használni azokat a humán-alapú viselkedési mintákat, melyekkel sikeresen végrehajthatja támadását (pl. social engineering).^{8,9}

Ezek közé a profilalkotással meghatározható emberi tényezők közé tartozhatnak például az alábbi kategóriák:

- szimpátia;
- együttérzés, empátia;
- kíváncsiság;
- hiszékenység;
- naivitás;
- segítőkészség.

⁷ Andreas Pfitzmann és mtsai., „Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology”, é. n., 83.

⁸ Ryan Heartfield és George Loukas, „A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks”, *ACM Computing Surveys* 48, sz. 3 (2016. február 8.): 1–39, <https://doi.org/10.1145/2835375>.

⁹ Matthew Edwards és mtsai., „Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces”, *Computers & Security* 69 (2017. augusztus): 18–34, <https://doi.org/10.1016/j.cose.2016.12.013>.

A szintén profilalkotással meghatározott manipulációs alapok közé tartozhatnak például az alábbiak:

- barátság vagy rokonszenv kialakítása;
- egy adott álláspont vagy elköteleződés fennállása;
- társadalmilag helyesnek vélt cselekedetek ismerete.

Mind ezek (emberi tényezők, manipuláció alapja) akár egyikének adott személyre vetített konkretizálódása esetén beszélhetünk egy humán-alapú támadás potenciális sikerességének alapfeltételéről.^{10,11}

Összességében tehát a PET-ek egyaránt otthoni és munkahelyi környezetben történő alkalmazásával minimalizálhatóak a profilalkotásból adódó kockázatok.

1.2. A privátszférát erősítő technológiák fogalmi meghatározása

A privátszférát erősítő technológiák fogalmi meghatározásának tekintetében a téma egyik legmeghatározóbb magyarországi kutatójának, Dr. Székely Ivánnak a definícióival szeretném bemutatni a PET-ek alapvető ismérveit. Összességében két, egymást kiegészítő, adekvát fogalom határozható meg:¹²

„A PET olyan információs és kommunikációs technológiák gyűjtőfogalma, amelyek megerősítik az egyén magánéletének védelmét egy információs rendszerben azáltal, hogy megakadályozzák a személyes adatok szükségtelen vagy jogellenes felhasználását, vagy olyan eszközöket és beavatkozási lehetőségeket kínálnak, amelyek növelik az egyén ellenőrzését személyes adatai felett.”

„A PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az információs privacyt a személyes adatok kezelésének kiiktatásával vagy minimalizálásával védi, és így megakadályozza a személyes adatok szükségtelen vagy nemkívánatos kezelését, anélkül, hogy csökkentené az információs rendszer funkcionalitását.”

¹⁰ Efthymia Metalidou és mtsai., „The Human Factor of Information Security: Unintentional Damage Perspective”, *Procedia - Social and Behavioral Sciences* 147 (2014. augusztus): 424–28, <https://doi.org/10.1016/j.sbspro.2014.07.133>.

¹¹ Moti Zwilling és mtsai., „Cyber Security Awareness, Knowledge and Behavior: A Comparative Study”, *Journal of Computer Information Systems* 62, sz. 1 (2022. január 2.): 82–97, <https://doi.org/10.1080/08874417.2020.1712269>.

¹² Székely Iván, „Privát szférát erősítő technológiák”, *Információs Társadalom* 8, sz. 1 (2008. március 1.): 20, <https://doi.org/10.22503/inftars.VIII.2008.1.3>.

A második fogalmi meghatározás tekintetében fontos kiemelni azt a megállapítást, hogy a PET-ek az információs rendszer funkcionalitásának csökkentése nélkül kell, hogy a tőlük elvárt módon szabjanak gátat a nemkívánatos / szükségtelen / jogellenes adatkezelésnek / adatgyűjtésnek.

1.2.1. A PET-ek és a kibertér kapcsolata, a fizikai lehetőségek különválasztása

A privátszférát erősítő technológiák kapcsán azok „térbeliségének” tekintetében megkülönböztethetjük a kibertérben, és a fizikai térben alkalmazható technológiákat, eszközöket.

Székely Iván előző alfejezetben ismertetett megfogalmazásából adódóan fontos megjegyezni, hogy a privátszférát erősítő technológiák „egy információs rendszerben” értelmezendők. Ezzel összefüggésben Magyarország Nemzeti Kiberbiztonsági Stratégiájának megfogalmazása szerint „a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti”.¹³

Kutatásom során az előzőekben megfogalmazottakból adódóan elsősorban az információs rendszerekben, vagyis a kibertérben alkalmazandó technológiák jelentik a vizsgálat tárgyát.

Mind ezek mellett, amennyiben a teljesség igényével szeretnénk áttekinteni a PET-ek kérdéskörét, úgy elengedhetetlen legalább említés szintjén foglalkozni a fizikai eszközökkel.

Összességében ezek a fizikai megoldások a kibertér technológiáival megegyezően a magánéletünk védelmét szolgálják, segítve a szükségtelen / nemkívánatos / jogellenes adatgyűjtés megakadályozását, viszont mindezt a valós, „offline” (on-site) térben.

Az alábbi felsorolásban összegyűjtöttem a legelterjedtebb, legismertebb és legrelevánsabb fizikai eszközöket:

- Webkamerák, valamint a mobiltelefonok előlapi és hátlapi kamerájának eltakarásául szolgáló, általában csúszkával rendelkező kellékek, melyek lényege, hogy a kamerák csak a felhasználó tudtával és (fizikai) hozzájárulásával legyenek alkalmasak képek vagy videók készítésére, azok távoli hozzáférése esetén ne okozhasson potenciális kompromittációs kockázatot;

¹³ 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

- Mikrofonokhoz – akár közvetlenül, akár adapteren keresztül – csatlakoztatott némítási lehetősége, mely feloldásához vagy aktiválásához közvetlen felhasználói fizikai interakcióra van szükség (az nem oldható fel távoli hozzáféréssel);
- A különböző adathordozók fizikai-biztonsági védelemmel ellátott verziói vagy kiegészítői, melyek alkalmasak például az adathordozó felületén biztosított titkosítási / jelszómegadási lehetőséggel szavatolni az eszköz integritását;
- USB portok biztonságát támogató blokkolók;
- Laptopok, tabletek, monitorok képernyővédő fóliái, melyek biztosítják, hogy mindössze egy bizonyos szögből legyen látható a képernyő tartalma, ezzel gátat szabva többek között az úgynevezett „shouldering”-nek, például bizonyos munkafolyamatokba történő illetéktelen betekintés, vagy hitelesítő adatok jogosulatlan megszerzésének megakadályozása által;¹⁴
- Kártyaadatok – akár távoli – leolvasását blokkoló igazolványtartó, vagy kifejezetten bankkártyákhoz / hitelkártyákhoz tartozó biztonsági külső borítás.

A fizikai eszközökhöz kapcsolódó részletes, átfogó kutatómunka lehetőségeivel és részleteivel a dolgozat végén, a „További kutatást igénylő területek” fejezetben foglalkozom.

1.3. A PET-ek rendszertana, alapvető kritériumaik és csoportosításuk

Ebben az alfejezetben a PET-ek fogalmi meghatározását követően azok leglényegesebb jellemzőit szeretném ismertetni. A különböző fogalmi magyarázatok tekintetében fontos megjegyezni, hogy a három kategória elemei (kritériumok – csoportosítás – rendszertan) együttesen jelentenek egy koherens egészet, a fogalmi meghatározások a releváns kategóriában kerülnek definiálásra.

1.3.1. A PET-ek alapvető kritériumai

A privátszférát erősítő technológiák tekintetében négy alapvető kritériumot határozhatunk meg:

- Anonimitás, mely estében az adatok nem összekapcsolhatók meghatározott személyekkel;

¹⁴ Leon Bošnjak és Boštjan Brumen, „Shoulder Surfing Experiments: A Systematic Literature Review”, *Computers & Security* 99 (2020. december): 102023, <https://doi.org/10.1016/j.cose.2020.102023>.

- Pszedonimitás, ahol ugyan van alany, ám annak kiléte például változatos fedőnevek, álprofilok vagy virtuális személyiségek kapcsán nem ismert;
- Megfigyelhetetlenség, amely a harmadik fél kizárását jelenti a kommunikációból azáltal, hogy nyílt hálózat használatakor észlelhetetlenséget biztosít;
- Összeköthetlenség, mely a jogosulatlan harmadik felet zárja ki a kapcsolatteremtésből, s melynek célja az alany szokásainak profilozásának megakadályozása, például egy adott oldal használatakor a megelőző vagy soron következő használt oldalak megfigyelésének letiltásával.^{15,16}

1.3.2. A PET-ek csoportosítása

A PET-ek csoportosításának egyik lehetősége az úgynevezett átláthatóságot fokozó eszközök (transparency-enhancing tools – TET) kategóriáinak meghatározása, mely a következő:

- Az érintettek magánéletének védelme érdekében a felhasználni kívánt adatokról a TET-ek ezen kategóriába eső technológiai információt nyújtanak az alany számára az adatgyűjtésről és adatfeldolgozásról;
- A TET-ek ezen csoportja az érintett számára áttekintést nyújt az alanyról nyilvánosságra kerülő adatokról és azok adatkezelőiről, valamint a rendelkezésre álló irányelvekről,
- Ebben a kategóriában a TET-ek az érintett vagy meghatalmazottja számára online hozzáférést biztosítanak a személyes adataihoz, valamint tájékoztatást nyújtanak arról, hogy az adatokat miként kezelték és dolgozták fel, és hogy ez összhangban volt-e a magánélet védelmére vonatkozó jogszabályokkal és/vagy további szabályzókkal.
- A TET-ek ezen csoportjába tartozó lehetőségek „ellenprofilozási” képességeket biztosítanak az érintettnek, segítve őt abban, hogy „kitalálja”, hogyan illeszkednek az adatai a releváns megalkotott csoportprofilokhoz, amelyek potenciális jövőbeli kockázatot jelenthetnek.¹⁷

¹⁵ Koorn R. és mtsai., *Privacy-Enhancing Technologies White Paper for Decision-Makers* (Directorate of Public Sector Innovation and Information Policy, 2004).

¹⁶ Vanja Seničar, Borka Jerman-Blažič, és Tomaž Klobučar, „Privacy-Enhancing Technologies—Approaches and Development”, *Computer Standards & Interfaces* 25, sz. 2 (2003. május): 147–58, [https://doi.org/10.1016/S0920-5489\(03\)00003-5](https://doi.org/10.1016/S0920-5489(03)00003-5).

¹⁷ Simone Fischer-Hübner és Stefan Berthold, „Privacy-Enhancing Technologies”, in *Computer and Information Security Handbook* (Elsevier, 2017), 759–78, <https://doi.org/10.1016/B978-0-12-803843-7.00053-3>.

A PET-ek egy másik csoportosítási lehetőségét az alábbiak szerint határozhatjuk meg:

- Szobjektumorientált technológiák: középpontjukban az alany szerepel, a cél ebben az esetben az azonosítás megszüntetése vagy korlátozása, mely egyaránt vonatkozik a különböző tranzakciókra és rögzített adatokra. Ilyen technikák lehet például az egyszerűhasználatos azonosítók, vagy digitális fedőnevek használata.
- Objektumorientált technológiák: középpontjukban az eszköz szerepel, és a céljuk a digitális ujjlenyomatok minimalizációja például a naplózások automatikus törlésével.
- Tranzakcióorientált technológiák: céljuk az alany tevékenységének, visszafejthetőségének védelme és a követhetőségének megakadályozása a hálózati tevékenységek során. A módszer ez esetben lehet bejegyzések törlése, adatláncok feldarabolása, például automatikus kitöltések automatikus törlésével.
- Rendszerorientált technológiák: Az előbbi három csoportot szervezi rendszerbe.^{18,19}

1.3.3. A PET-ek rendszertana

A privátszférát erősítő technológiák rendszertan-szerinti elemzése kapcsán három nagy csoportot különböztethetünk meg: a felhasználói-oldali-, a szerver-oldali- valamint a csatorna-oldali technológiákat.²⁰

Az első csoportba a felhasználói-oldali technikák tartoznak. Ezen csoport alkategóriáiként a nyomkövetés-elleni technológiákat (pl.: ad-blockerek, pop-up tiltók és digitális ujjlenyomat minimalizáló technológiák), valamint az adatvédelmi tanúsítványokat azonosíthatjuk. Két további kategória az úgynevezett zajosítók (vagy adatszavarást előidéző PET-ek) és a magánszféra többfaktoros megőrzését szolgáló számítási kategóriák.^{21,22}

A második csoportot a szerver-oldali technikák alkotják. Az itt szereplő alkategóriák közül az első az úgynevezett önmegsemmisítő adatrendszer (ide tartozik az adatok eltüntetése,

¹⁸ John Borking és mtsai., *Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents*, 2003, <https://doi.org/10.13140/2.1.4888.7688>.

¹⁹ Székely, „Privát szférát erősítő technológiák”.

²⁰ Kaaniche, Laurent, és Belguith, „Privacy Enhancing Technologies for Solving the Privacy-Personalization Paradox”.

²¹ Christof Ferreira Torres, Hugo Jonker, és Sjouke Mauw, „FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting”, in *Computer Security -- ESORICS 2015*, szerk. Günther Pernul, Peter Y A Ryan, és Edgar Weippl, *Lecture Notes in Computer Science* (Cham: Springer International Publishing, 2015), 3–19, https://doi.org/10.1007/978-3-319-24177-7_1.

²² Stefano Traverso és mtsai., „Benchmark and comparison of tracker-blockers: Should you trust them?”, in *2017 Network Traffic Measurement and Analysis Conference (TMA)*, 2017, 1–9, <https://doi.org/10.23919/TMA.2017.8002898>.

semlegesítése és helyettesítése), valamint a statisztikai közzététel ellenőrzése (vagyis anonimizáció vagy megkülönböztetés). További alkategóriákként (mint a felhasználói-oldalon) itt is megjelenik az elhomályosítás, mely szerver-oldalon a privát információ-visszafejtést jelenti, illetve a megőrzést szolgáló számítási kategóriában a homomorf titkosítás.^{23,24,25}

A harmadik csoport a csatorna-oldali technikák. Ezek a felhasználó és a szerver közti kommunikáció során használható PET-ek kategóriája. Ebben a csoportban megkülönböztethetjük a biztonságos kommunikációt elősegítő technikákat (kliens-oldali-, és végponti titkosítás), (VPN), valamint az úgynevezett „megbízható harmadik fél” kategóriát, mely az anonimitást és a pszeudonimitást foglalja magában.^{26,27}

1.4. Példák, kategorikus ismertetőik

A privátszférát erősítő technológiák alapvető ismertetése, bemutatása, lényegi leírása mellett elengedhetetlen lenne konkrét példák és technológiák felsorakoztatása, azonban ez egy adott termék vagy szolgáltatás expressis verbis megnevezése, ajánlása nélkül csak kategorikus ismertetés szintjén valósítható meg.

Dolgozatomban és kutatásomban nem célom, és etikátlannak is találnám akár egyetlen gyártó egyetlen szolgáltatásának név szerinti ismertetését, ajánlását is. Ahogy a legkülönbözőbb informatikai-védelmi megoldások tekintetében, úgy a privátszférát erősítő technológiáknál is van lehetőségünk különböző, konkrét technológiai-kategóriákat meghatározni, melyen belül egyénileg mindenki megtalálhatja a neki legmegfelelőbb PET-et, akár személyes preferencia, anyagi vonzat esetén ár-érték arány, szofisztikáltabb technológia tekintetében ráfordított idő és energia, vagy kompatibilitás kapcsán a használt számítógépes vagy mobiltelefonos operációs rendszer, böngésző tekintetében.

²³ Hyejin Shin és mtsai., „Privacy Enhanced Matrix Factorization for Recommendation with Local Differential Privacy”, *IEEE Transactions on Knowledge and Data Engineering* 30, sz. 9 (2018. szeptember): 1770–82, <https://doi.org/10.1109/TKDE.2018.2805356>.

²⁴ Úlfar Erlingsson, Vasyl Pihur, és Aleksandra Korolova, „RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response”, in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14* (New York, NY, USA: Association for Computing Machinery, 2014), 1054–67, <https://doi.org/10.1145/2660267.2660348>.

²⁵ Bolin Ding, Janardhan Kulkarni, és Sergey Yekhanin, „Collecting Telemetry Data Privately”, in *Advances in Neural Information Processing Systems*, kötet 30 (Curran Associates, Inc., 2017), <https://papers.nips.cc/paper/2017/hash/253614bbac999b38b5b60cae531c4969-Abstract.html>.

²⁶ Sohely Jahan, Md. Saifur Rahman, és Sajeeb Saha, „Application specific tunneling protocol selection for Virtual Private Networks”, in *2017 International Conference on Networking, Systems and Security (NSysS)*, 2017, 39–44, <https://doi.org/10.1109/NSysS.2017.7885799>.

²⁷ Ashwin Rao és mtsai., „Meddle: middleboxes for increased transparency and control of mobile traffic”, in *Proceedings of the 2012 ACM conference on CoNEXT student workshop, CoNEXT Student '12* (New York, NY, USA: Association for Computing Machinery, 2012), 65–66, <https://doi.org/10.1145/2413247.2413286>.

A felsorolás sorrendje nincs kapcsolatban a különböző PET-ek értékével, hasznosságával és használhatóságával.

Kriptográfiai megoldások:

- Homomorf titkosítás: Egy titkosítási módszer, amely lehetővé teszi a titkosított adatokon végzett különböző számítási műveleteket, mellyel maga a PET egy olyan titkosított eredményt hoz létre, amely visszafejtéskor megegyezik a műveletek eredményével, mintha azokat titkosítatlan adatokon (azaz egyszerű szövegen) végezték volna el. Ez lehetővé teszi a titkosított adatok továbbítását, elemzését és visszaküldését az adatok tulajdonosának, aki visszafejtheti az információt, és megtekintheti az eredményeket azok eredeti formájában. Ez például lehetővé teszi, hogy a vállalatok elemzés céljából megoszthassák a rendelkezésükre álló érzékeny adatokat harmadik felekkel. Továbbá ez olyan alkalmazásokban is hasznos, amelyek titkosított adatokat továbbítanak felhőalapú tárolókba.

Gyakori típusai:

- Részleges homomorf titkosítás: a titkosított adatokon csak egyféle számtani művelet végezhető, például csak összeadás, vagy csak szorzás, de mindkettő egyszerre nem.
- Részben homomorf titkosítás: egynél több számtani művelettípust (pl. összeadás, szorzás) képes végrehajtani, de korlátozott számú műveletet tesz lehetővé.
- Teljes homomorf titkosítás: egynél több számtani művelettípus elvégzésére képes, és nincs korlátozás az elvégzett műveletek tekintetében.²⁸
- Biztonságos, több fél részvételével történő számítás (Secure multi-party computation – SMPC): A homomorf titkosítás egyik kapcsolódó technológiája, egy jelentős különbséggel: a felhasználók több titkosított adatforrásból is képesek értékeket kiszámítani, ezért a gépi tanulási modellek titkosított adatokra is alkalmazhatók, mivel az SMPC nagyobb adatmennyiségre is alkalmazható.²⁹

²⁸ Bechir Alaya, Lamri Laouamer, és Nihel Msilini, „Homomorphic Encryption Systems Statement: Trends and Challenges”, *Computer Science Review* 36 (2020. május 1.): 100235, <https://doi.org/10.1016/j.cosrev.2020.100235>.

²⁹ Chuan Zhao és mtsai., „Secure Multi-Party Computation: Theory, Practice and Applications”, *Information Sciences* 476 (2019. február 1.): 357–72, <https://doi.org/10.1016/j.ins.2018.10.024>.

- Differenciált adatvédelem: A PET-ek ezen kategóriába tartozó technológiai védelmet nyújtanak az egyénekre vonatkozó szükségtelen vagy jogszerűtlen információk megosztása kapcsán. Ez a kriptográfiai algoritmus egyfajta "statisztikai zavart" kelt, egy réteget ad a felhasználóról gyűjtött valós adathalmazhoz, amely lehetővé teszi az adathalmazon belüli csoportok mintázatainak leírását, ám mindezt az egyének magánéletének megőrzése mellett. Az ezen kategóriába tartozó PET-ek jelentősen megnehezítik a profilozás hatékonyságát / lehetőségét.³⁰
- Nulla-tudásalapú igazolás-támogatás (Zero knowledge proofs – ZKPs): A ZKP-k olyan kriptográfiai algoritmusokat használnak, amelyek lehetővé teszik az információ hitelesítését anélkül, hogy az azt bizonyító adatokat felfednék, tehát a személyazonosság ellenőrzésére a személyes adatok megadásának helyettesítésével kerül sor.³¹

Adatmaszkírozási technikák:

(Melyeket az adatkészletekben található érzékeny információk védelmére használnak.)³²

- Elhomályosítás: Ez egy általános kifejezés az adatmaszkírozásra, amely több módszert tartalmaz az érzékeny információk helyettesítésére azáltal, hogy zavaró vagy félrevezető adatokat adnak hozzá egy naplóhoz vagy profilhoz.
- Pszeudonimizálás: Az azonosító mezők (vagyis az egyénre jellemző információkat tartalmazó mezők) fiktív adatokkal, például karakterekkel vagy más adatokkal történő helyettesítése. A pszeudonimizálást a szervezetek gyakran használják a GDPR-nak való megfelelés érdekében.
- Adatminimalizálás: A személyes adatok lehető legminimálisabb mennyiségének gyűjtése, amely lehetővé teszi a vállalkozások / szervezetek számára, hogy a szolgáltatását még megfelelő minőségben nyújthassa. Gyakran hálózatok végpontjain található központosított csomópontokból történik az adatmentesítés / kiürítés.
- Kommunikációs anonimizáló eszközök: Az anonimizátorok az online identitást (pl.: IP-címek, e-mail címek) egy eldobható / egyszeri lenyomozhatatlan identitással helyettesítik.

³⁰ Waqas Ali, Mohammad Nauman, és Nouman Azam, „A Privacy Enhancing Model for Internet of Things Using Three-Way Decisions and Differential Privacy”, *Computers and Electrical Engineering* 100 (2022. május 1.): 107894, <https://doi.org/10.1016/j.compeleceng.2022.107894>.

³¹ Feng Li és Bruce McMillin, „Chapter Two - A Survey on Zero-Knowledge Proofs”, in *Advances in Computers*, szerk. Ali Hurson, köt. 94 (Elsevier, 2014), 25–69, <https://doi.org/10.1016/B978-0-12-800161-5.00002-5>.

³² Vishal Anjaiah Gujjary és Ashutosh Saxena, „A Neural Network Approach for Data Masking”, *Neurocomputing* 74, sz. 9 (2011. április): 1497–1501, <https://doi.org/10.1016/j.neucom.2011.01.002>.

Algoritmusok és mesterséges intelligencia segítségével üzemeltetett PET-ek:^{33,34}

- Szintetikus adatok generálása: A szintetikus adatok különböző algoritmusok segítségével mesterségesen létrehozott adatok. Optimális abban az esetben, ha felmerülhet harmadik fél általi hozzáférés.
- Adatkészletek: Mesterséges, globális vagy regionális statisztikai jellemzőkre támaszkodó adatgyűjtési folyamat kapcsán a PET a mesterséges intelligencia segítségével mintákat képez, rendszerez és ismételi, ezzel tulajdonképpen való adatokat közöl, viszont Ellehetetleníti az alanyok valós tevékenységének megfigyelését.
- Összevont (Federált) tanulás: egy olyan gépi tanulási technika, amely egy algoritmust több decentralizált (perem)eszközön vagy helyi adatmintákat tároló szerveren keresztül képez ki (tanít), anélkül, hogy azokat kicserélné. A kiszolgálók decentralizálásával a felhasználók adatminimalizálást is elérhetnek azáltal, hogy csökkentik a központi kiszolgálón vagy felhőalapú tárolóban megőrzendő adatok mennyiségét.

1.5. Privacy by design

Az internet és a kapcsolódó intelligens eszközök (IoT-k) használata az egyének személyes adatainak tömeges feldolgozását eredményezi a gyakorlatban, mely egyenesen arányos következménye a személyek magánéletének védelmének csökkenésével. Az Európai Unióban a jogalkotók 2018-ban, az általános adatvédelmi rendelet (GDPR) hatályba lépésével határozottan próbáltak szembenézni ezzel a kihívással. A GDPR a "beépített és alapértelmezett adatvédelem" elgondolásán keresztül arra törekszik, hogy az infokommunikációs technológia fejlesztését és használatát úgy irányítsa, hogy a személyes adatok feldolgozása – a köz- és magánszféra jogos érdekeit figyelembe véve – a lehető legkevésbé zavarja az egyének magánéletét.³⁵

A privacy by design (továbbiakban: PbD) összességében tehát azt jelenti, hogy a különböző adatvédelmi megoldásokra az adekvát válaszokat már a tervezési fázisban meghatározzák, és

³³ Grzegorz Mazurek és Karolina Małagocka, „Perception of privacy and data protection in the context of the development of artificial intelligence”, *Journal of Management Analytics* 6, sz. 4 (2019. október 2.): 344–64, <https://doi.org/10.1080/23270012.2019.1671243>.

³⁴ Bangzhou Xin és mtsai., „Federated Synthetic Data Generation with Differential Privacy”, *Neurocomputing* 468 (2022. január 11.): 1–10, <https://doi.org/10.1016/j.neucom.2021.10.027>.

³⁵ Matjaž Drev és Boštjan Delak, „Conceptual Model of Privacy by Design”, *Journal of Computer Information Systems* (2021. július 1.): 1–8, <https://doi.org/10.1080/08874417.2021.1939197>.

azok integrálása már a fejlesztés, megtervezés legelső szakaszában megjelenik, ezzel megelőzve a hatékonytalan, utólagos, formai „megoldásokat”.

A PbD megoldások jogszabályi szinten az Európai Unióban 2018 május 25-e óta kötelező érvényűek, ám az alapelgondolás régebbi múltra tekint vissza. Az EU-n belül a GDPR-t megelőzően már az 1995-ben elfogadott „a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról” szóló irányelv³⁶ már magában foglalta a megfelelő technikai és szervezési intézkedések feltételét az adatfeldolgozó rendszer tervezésekor, valamint az adatfeldolgozás során, különösen a biztonság fenntartása érdekében. A PbD – és a későbbiekben a GDPR is – azonban túlmutat a biztonság fenntartásán. A PbD magában foglalja azt az elképzelést, hogy a rendszereket úgy kell megtervezni és felépíteni, hogy elkerülhető vagy minimálisra csökkenthető legyen a feldolgozott személyes adatok mennyisége. Az adatminimalizálás kulcsfontosságú elemei a személyes azonosítók és a tartalmi adatok szétválasztása, az álnevek használata és a személyes adatok anonimizálása vagy törlése a lehető legkorábbi időpontban. Az alapvető elgondolás szerint a szolgáltatóknak lehetővé kell tenniük a felhasználók számára személyes adataik jobb védelmét, például megfelelő adatvédelmi eszközök biztosításával (hozzáférés-ellenőrzés, titkosítás, anonim felhasználásra vonatkozó rendelkezések).³⁷

Következtetések

Az 1. fejezetben tárgyaltak alapján levonhatjuk azt a következtetést, miszerint a privátszférát erősítő technológiák egy adekvát megoldást jelenthetnek egy potenciális kiberbiztonsági kockázatra, mely alapjául a rohamosan fejlődő technológia által rendelkezésre álló profilalkotási folyamatok szolgálnak, és melyet a támadók egyre szofisztikáltabb és egyre sikeresebb humán-alapú támadások tekintetében tudnak felhasználni.

³⁶ Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

³⁷ Peter Schaar, „Privacy by Design”, *Identity in the Information Society* 3, sz. 2 (2010. augusztus 1.): 267–74, <https://doi.org/10.1007/s12394-010-0055-x>.

2. fejezet – Szakértői interjúk

Kutatásom során külön figyelmet szenteltem a hazai és nemzetközi szakirodalmi feldolgozás, valamint az empirikus részek mellett a hazai szakértők véleményének megismerésére és összevetésére. Az interjúalanyok között szerepelnek egyaránt egyetemi oktatók, kutatók, valamint a gyakorlati munkavégzés tekintetében kifejezetten a műszaki szakterülettel-, vagy kifejezetten információbiztonsági szabályzókkal foglalkozó szakemberek, valamint nemzetközi szinten is elismert kiberbiztonsági szakértők.

A kiberbiztonsággal jelenleg is munkahelyi környezetben foglalkozó szakértők összességében képviselik a hazai állami – ideértve a rendvédelmi szerveket is – és a magánszektor egyaránt. A szakértői interjúk feldolgozása az anonimitás – mely egyaránt vonatkozik az interjút adó személyére és szervezetére – teljes figyelembevételével zajlott.

A szakértői interjúk vonalvezetéséül szolgáló kérdéssort az 1. számú melléklet tartalmazza.

2.1. Humán tényező az információbiztonságban

Az információbiztonság és a humán tényezők kapcsolatában a szakértői vélemények bizonyos szempontból megegyeznek, bizonyos szempontból pedig különböznek, vagy legalábbis más-más perspektíva mentén közelítik meg az emberi tényezőt a szervezeti biztonság vonatkozásában.

Az alapvető kérdések kapcsán három fő álláspont határozható meg:

- Az első vonatkozásában a válasz egyértelműen nem, ugyanis a folyamatok tekintetében ezen álláspont képviselői nem látják a lehetőségét az emberi tényező kizárásának, mely által a humán-alapú kockázatok – melyek egy részére az 1. fejezetben kitértem – nem szüntethetők meg.
- A második csoport vonatkozásában azt a megközelítést definiálhatjuk, mely szerint lehetséges a humán tényező figyelembevétele nélkül maximalizálni a biztonságot, ám arra csak úgy van lehetőségünk, ha azt a folyamatok hatékonyságának rovására tesszük, tehát például elvonatkoztatunk a kockázatokkal arányos védelem alapvetésétől.
- A válaszok harmadik csoportját alkotó vélemények szerint a hatékonyság csökkenése nélkül lehet minimalizálni a humán tényező biztonsági kockázatát, melyre két lehetőség adott. Az egyik abban az esetben áll fent, ha például olyan zárt, minősített adatok

kezeléséről beszélünk, melyek a Mavtv.³⁸ hatálya alá esnek, viszont ez nem bővíthető szervezeti szintre, csak egy adott folyamatban / szegmensben értelmezhető. A másik lehetőség pedig mindössze azokra a folyamatokra korlátozódik, melyet a mesterséges intelligencia is el tud végezni...

Összességében elmondható, hogy mivel a biztonság megteremtésére vonatkozó erőfeszítéseknek egy megkerülhetetlen szelete a személyi biztonságra vonatkozó intézkedések megtétele, ezért alapvetően a személyekhez kapcsolódó intézkedések nélkül a biztonság nem értelmezhető.

Mind ezek mellett szervezeti szempontból egy fontos aspektusa volt a szakmai interjúnak, hogy a humán tényező figyelembevétele nélkül a biztonság „maximalizálása” egy elég alacsony szintet fog jelenteni, ahhoz képest, mintha a szervezet komplex módon gondolkodna a védelmének megteremtéséről és minden tényezőt figyelembe venne. Az interjúalanyok között továbbá egyetértés volt abban, hogy a legmodernebb védelmi intézkedések beszerzése sem elegendő akkor, ha a munkavállaló nem rendelkezik a megfelelő kompetenciákkal.

A munkavállalók szakmai kompetenciáival kapcsolatos kérdésre a válasz egyöntetű volt. Ennek lényege, hogy az ilyen jellegű kockázatokat már a nulladik lépéskor, vagyis a felvételi folyamat során meg kell próbálni minimalizálni, vagy új típusú szakmai kompetenciát igénylő feladatok esetén szervezeti szinten kell megvalósítani a szükséges képzést és a munkavégzés megkezdése előtt nem hanyagolható el a megfelelő szintű kompetenciák meglétének ellenőrzés sem. Mindennek ellenére, amennyiben mégis felmerül ez a kockázat, úgy az eredményezheti többek között a hibás hardver, szoftver kezelést, karbantartást, konfigurálást, stb.; a fejlesztés során bekövetkezett hibát; a hibajelenségek figyelmen kívül hagyását; az adatvesztést; a nem megfelelő adatkezelés miatt bekövetkezett bizalmasság sérülését; a nem megfelelő adatkezelés miatt bekövetkezett sértetlenség sérülését; nem megfelelő adatkezelés miatt rendelkezésre állás sérülését; stb..

Továbbá konszenzus övezte az a gondolatot is, mely szerint a nem megfelelő szakmai kompetenciák önmagukban hordozzák a nem megfelelő szintű biztonságtudatossági attitűdöt is. A szakmai kompetencia hiánya természetesen nem csak közvetlenül a rendszerrel kapcsolatban mutatkozhat meg, hanem adott esetben tetten érhető a szervezet, annak egyéb területeinek működésében, folyamataiban, dokumentumaiban is.

³⁸ 2009. évi CLV. törvény a minősített adat védelméről

Kifejezetten az információbiztonságra vonatkozó kérdés kapcsán összességében az állapítható meg, hogy ezen képességek fejlesztése tudatossági képzetekkel, oktatásokkal, tudatosítási kampányokkal, stb. érhető el, de csak nagyon nehezen. A humán tényező kapcsán a biztonság megannyi szegmensében számtalan sebezhetőséget definiálhatunk. Egy egyszerű, mindössze az e-mail-ekhez kapcsolódó példán bemutatva, egy átlagos felhasználóra jellemző a gyanakvás hiánya, a feltétel nélkül megbízás a képernyőn megjelentekben, a sürgetésnek való bedőlés (lejáró akciók, soha vissza nem térő lehetőségek), az értelmetlenül, hibásan, árulkodó helyesírási hibákkal rendelkező mondatok, megszólítás figyelembe vételének hiánya, a személyes adatok felelőtlen megadása a weboldalak bármelyikén, az e-mail-ek „aláírójának” ellenőrzésének elmulasztása, a csatolt linkekre, mellékletekre történő gondolkodás nélküli rákattintás, stb., stb..

A szakértők egy része kiemelte az üzemeltetési, illetve fejlesztési oldal szereplő kiemelt veszélyforrásokat, melyek között az alábbiak azonosíthatók: A rendszerben ismeretlen forrásból származó alkatrészek használata, elektromágneses kisugárzás (lehallgatás) és elektromágneses besugárzás (zavarás) lehetősége, nem megfelelő karbantartás, jogosulatlan hozzáférések, szükségtelen hozzáférési jogok, bejutás ellenőrzésének hiánya, nem megfelelő hozzáférés ellenőrzés, gyenge titkosítás használata, ismeretlen forrásból származó alkalmazások, kiegészítők használata, stb..

Az otthoni és a munkahelyi környezet tekintetében a vélemények alapján elmondható, hogy az otthoni környezet eleve nem tekinthető olyan biztonságos környezetnek, mint egy vállalati környezet, például ahol a gépterem, a hálózati eszközök és az irodai környezet fizikai biztonságát beléptető rendszerrel, videókamerás ellenőrzéssel, tűzjelző rendszerrel, gépteremben oltórendszerrel biztosítják. A hálózat és az eszközök védelmét különböző tűzfalak, tartalomszűrők, antivírus rendszer, IDS, stb. biztosítják. A felhasználók viselkedését különböző jogszabályok, szabványok, munkahelyi szabályok és munkautasítások szabályozzák. (Beleértve – annak engedélyezése esetén – az otthoni munkavégzést is, ahol – teoretikus jelleggel megfogalmazva – a munkahelyi szabályokat kell(ene) betartania a munkatársnak. A vállalati környezetben továbbá a munkaállomások és a hálózati eszközök hozzáférési jogosultságai jól szabályozottak, a tevékenységek naplózottak, a karbantartás ütemezett, a változáskezelés mintaszerű, az események bejelentése biztosított, és szükség esetén akár egy ügyfélszolgálat és egyéb segítség is rendelkezésre áll. Mindezek otthoni környezetben – magától érthető módon – nem találhatók meg. Ezek többségének hiányát a felhasználó tudatos viselkedéssel tudná ellensúlyozni, melyek közé tartozik például az, hogy

tudatosan választja meg a meglátogatott honlapokat, keresőmotorokat, ügyel a honlapok https előtagjára, az oldalak tanúsítványaira, az oldalak felkínált cookiekat ellenőrzést követően és szándéka szerint hagyja jóvá vagy tiltja, nem használ, de ha használ akkor is, tudatosan tárol és oszt meg magáról és a családjáról információkat a közösségi médiában és a felhőplatformokon, nem keveri a magáncélú és a munkahelyi adatokat, nem használ két egyforma jelszót a különböző rendszerekben/internetes szolgáltatásokban, gyakran cseréli az összetett és biztonsági jelszavait és azokat biztonságos módon tárolja, jogtiszt szoftvereket használ, amelyeket folyamatosan frissít, használ antivírus szoftvert és tűzfalat, biztonságos böngészőt vagy olyan böngésző bővítményeket használ, melyek segítik a személyes adatai védelmét (biztonságos kapcsolat alkalmazása, cookie-k, szkriptek egyebek tiltása, törlése, stb.), tudatosan választja email szolgáltatóját vagy saját levelezőszolgáltatást üzemeltet, van biztonsági másolata az adatairól több különböző platformon, titkosított / védett adathordozókat és internetkapcsolatot (VPN, proxy, stb.) használ, az eszközei, okoseszközei alapértelmezett bejelentkezési azonosítóit megváltoztatja, a biztonsági és adatvédelmi beállításait önállóan határozza meg, a frissítéseket rendszeresen ellenőrzi és telepíti, az elavult eszközeit selejtezi, selejtezés előtt visszaállíthatatlanul törli azok adatait, nem dob a szemébe semmilyen személyes adatot tartalmazó iratot / fényképet, nem használja a nyilvános vagy a pl. szállodák, egyetem, tömegközlekedési eszközök által biztosított wifi szolgáltatásokat, nem csatlakoztat idegen eszközöket a saját eszközeihez és a saját eszközeit idegen eszközökhöz, nem használja eszközeit nyilvános helyeken mások által betekinthes módon, nem hagyja felügyelet nélkül az eszközeit még az autójában és az otthonában sem, azok elzárásáról, manuális és automatikus zárolásáról is gondoskodik, otthonában és autójában is riasztórendszert használ, az eszközein a nem használt wifit és bluetooth szolgáltatásokat kikapcsolja, stb.. Mindezekbe bele kell érteni azt is, hogy ezeket a szabályokat a felhasználó nem csak maga, hanem a családja esetében szintén betartja, betartatja.

Ezen a ponton kell jelen fejezet kapcsán is kiemelni privátszférát erősítő technológiák és a kiberbiztonság szoros kapcsolatát. Az előző szakértői interjúk által készített felsorolásban is megannyi, az 1. fejezetben is említett / részletezett megoldást láthatunk, melyek alkalmazása – egyaránt otthoni és munkahelyi környezetben – elengedhetetlen a megfelelő szintű információbiztonság megteremtéséhez.

Szakértői vélemények szerint célzott támadások esetén összetettebb módon kell vizsgálnunk a kérdéskört és a felelősséget. Egy ilyen esetben valószínűleg még a megfelelő biztonságtudatosság sem menti meg a felhasználót. A „kimeríthetetlen” erőforrásokkal rendelkező támadók előbb fognak egy kiskaput (pl.: egy sérülékeny eszközt a biztonságtudatos felhasználó környezetében), mint maga a felhasználó, így kompromittálva az eszközt, ezáltal a felhasználót. Ennek elkerüléséhez már nagy fokú biztonságtudatosság, rosszabb esetben paranoia, vagy a modern technológiákról való lemondás, a külvilágtól való nagy fokú elszigetelődés szükséges, ami nem tartozik az átlagos viselkedéshez, ezért ennek vizsgálatától most tekintsünk el, de a vélemények alapján nem életszerűtlen ez a felvetés sem.

Megjegyzés: Tökéletes, áthatolhatatlan, százszázalékos biztonságot nyújtó védelem nincs, még végtelen mennyiségű erőforrás (pénz, idő) befektetése mellett sem. Otthoni környezetben tanúsított nem megfelelő biztonságtudatosság (akár a felhasználó sajátja, akár a családjaé) csak felgyorsítja a kompromittálódás lehetőségét. Emellett a megfelelő szakmai kompetenciákkal és megfelelő, munkahelyi információbiztonsági attitűddel rendelkező munkavállaló esetében is előfordulhat vétlen, de akár szándékos olyan tevékenység / viselkedés is, amely potenciális veszélyforrást jelent a szervezetre vagy a rendszer működésére. Ezek közé tartozhat a személyes vagy munkahelyi stresszhelyzet, fáradtság, munkamenet hibás szabályozása, előírások figyelmen kívül hagyása (kényelmesség, akadályoztatás, figyelmetlenség következtében), túl komplikált (hibákra érzékeny) kezelés, vagy jogosulatlan adatkezelés, jogosultságokkal való visszaélés, beavatkozás a rendszer működésébe, stb. (pl. harmadik fél kényszerítése vagy belső készítés kapcsán).

2.2. A privátszféra és kapcsolódó fenyegetések

A privátszféra nem megfelelő szintű védelmének kapcsán a szakértők a fő veszélyforrásokat a közösségi média, az okos és IoT eszközök, alkalmazások, egyéb webes felületek – felelőtlen, korlátok nélküli, mindennemű biztonságtudatossági attitűdöt figyelmen kívül hagyó – használatával azonosítják.

Az 1. fejezetben és a Bevezetésben is említésre került, hogy az összegyűjtött információmorzsákat rendezve és megfelelően szűrve (profilalkotás) a múltbéli, a jelenlegi és a jövőbeli döntéseinkre, preferenciáinkra bármire lehet következtetni (ld.: személyes jellemzők meghatározása). Meg lehet állapítani, hogy valójában kikkel állunk milyen kapcsolatban, mit fogunk rendelni, hova fogunk utazni, milyen az egészségügyi állapotunk, mik

a vallási, szexuális vagy pártpreferenciáink, stb. Csupa olyan személyes vagy különleges adat, ami vagy eleve kompromittálásra alkalmas, vagy annak a lehetőségét könnyíti meg a támadók számára, például humán-alapú támadások végrehajtásakor.

Alapvetően ezen adatok kapcsán a legkézenfekvőbb felhasználás a célzott hirdetésekkel a meghatározott termékek, szolgáltatások fogyasztására rávenni a felhasználót. Tisztességes vagy tisztességtelen eszközökkel befolyásolni a felhasználók döntéseit (pl.: választások), de használhatók ezen adatok szervezetek részéről ügyfélszerzésre és ügyfélátcsábításra, ügyfélélmény-növelésre és megtartásra, kampányhatékonyság javítására, termék- és szolgáltatásfejlesztésre, stb..

Megjegyzendő továbbá, hogy a szakértők az ilyen formában gyűjtött adatok kapcsán kiemelt veszélyforrásként tekintenek azok tárolása és felhasználása kapcsán a teljes áttekinthetatlenség problémájára.

Ezen a pontos szintén megerősítést nyert a privátszférát erősítő technológiák használatának fontossága.

A privátszféra védelmének és a szervezeti biztonság összefüggéseinek kapcsán az alábbi következtetések határozhatók meg:

A szervezetek szempontjából egyértelműen kockázat, hogy az adott munkatárs vállalaton kívüli tevékenységéből adódóan potenciális fenyegetéseknek van kitéve.

Ha tudni lehet, hogy az adott munkatársa milyen útvonalon, milyen eszközzel (pl.: gyalog) jár munkába, akkor egy csali, elvesztettnek tűnő, de kártékony kódot tartalmazó pendrive kihelyezése erre az útvonalra, majd azt a felhasználó által a munkaállomásra gyanútlanul csatlakoztatva a felhasználó akár korlátlan hozzáférést biztosíthat a támadónak. Ha a felhasználóról tudni lehet, hogy hol ebédel a munkatársaival, akkor ezen beszélgetéseket a közelből ki lehet hallgatni. Ha tudni lehet, hova jár kávézni, milyen témákban járatos, milyen honlapokat látogat, milyen hobbijai és szokásai vannak, akkor szóba lehet elegyedni vele, a támadó bizalmat tud ébreszteni maga irányában. Ha a támadó előre tudja egyes felvetésekre adott felhasználói reakciókat, akkor szinte nyert ügye van, főleg, ha a felhasználó kevésbé tudatos magatartással bír. Kisebb, nagyobb ajándékok, szívességek elfogadása különösen kockázatos, például a „később kérünk majd valamit cserébe” esete. A felhasználót mindezzel nem csak a valós térben, hanem az online térben is lehet kompromittálni (pl.: célzott kampány).

A munkavállalók, alkalmazottak privát szférájának illetve a szervezet által kezelt (pl: ügyfelek) személyes adatainak védelme Magyarországon és az EU-ban elsősorban jogszabályban rögzített előírásokon alapul.^{39,40,41,42}

Következtetések

A kutatás szempontjából levonható legjelentősebb konklúzió az, hogy a hazai és nemzetközi szakirodalmi leírásokat megerősítve a hazai szakértők egyöntetűen azt az álláspontot képviselik, miszerint az egyének humán-alapú sebezhetőségeik következtében potenciálisan a támadók célpontjaivá válhatnak, amennyiben nem rendelkeznek azokkal a lehetőségekkel, melyekkel növelhető a privátszférájuk biztonsága, és az adataik feletti kontroll, mely kockázatok egy jelentős hányadának minimalizációját a különböző privátszférát erősítő technológiák, megoldások jelenthetik.

A felállított kutatási hipotézisekkel, célkitűzésekkel és az empirikus kutatással közvetlen kapcsolatban álló kérdésekkel a 3. fejezetben foglalkozom a továbbiakban.

³⁹ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

⁴⁰ 2012. évi I. törvény a munka törvénykönyvéről (Mt.)

⁴¹ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Info tv.)

⁴² 2018. évi CXXV. törvény a kormányzati igazgatásról (Kit.)

3. fejezet – Az empirikus kutatás bemutatása

A kutatási célkitűzésekkel és módszertannal összhangban jelen fejezetben szeretném bemutatni az általam végzett empirikus kutatásokat, azok elemzését és összevetését.

Az empirikus kutatás gerincét egy, a privátszférával kapcsolatos kérdőív elkészítése, és annak eredményeinek elemzése adta.

3.1. Az empirikus kutatás összeállítása

A kérdőív egésze áttekinthető a 2. számú mellékletben.

A kérdőív kérdéseit 5 nagy csoportra osztottam:

1. Demográfiai adatok
2. A privátszférát erősítő technológiák (PET-ek) aktuális alkalmazása
3. A privátszférát erősítő technológiák (PET) alkalmazásának lehetőségei
4. Privátszféra és adatvédelem a mindennapokban
5. A privátszféra védelme és a munkahelyi biztonság kapcsolata

A demográfiai adatok megadását követően a 2. szakasz / oldal kitöltése előtt az alábbi ismertetőt olvashatták el a kitöltők, melyre a kérdőív leírásában is felhívtam a figyelmet:

A kitöltés folytatása előtt kérem olvassa el az alábbi rövid ismertetőt:

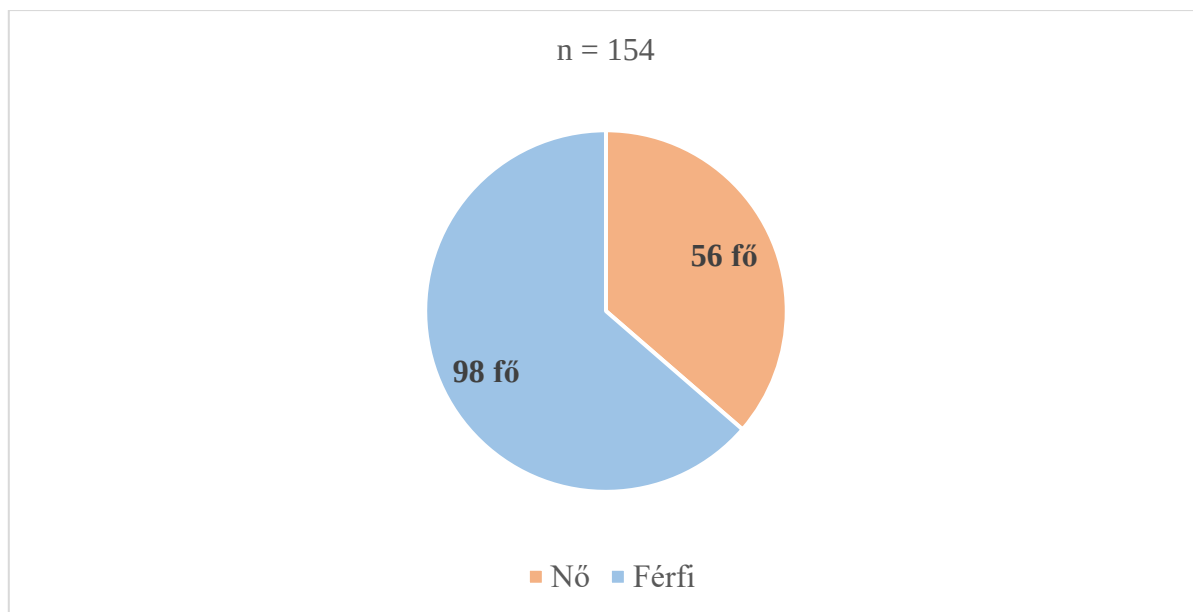
A privátszférát erősítő technológiákat (röviden: PET) összességében úgy határozhatjuk meg, hogy azok megerősítik az egyén magánéletének védelmét azáltal, hogy megakadályozzák a személyes adatok szükségtelen, nem kívánatos vagy jogellenes felhasználását, vagy olyan eszközöket és beavatkozási lehetőségeket kínálnak, amelyek növelik az egyén ellenőrzését személyes adatai felett.

3.2. A kérdőív kiértékelés

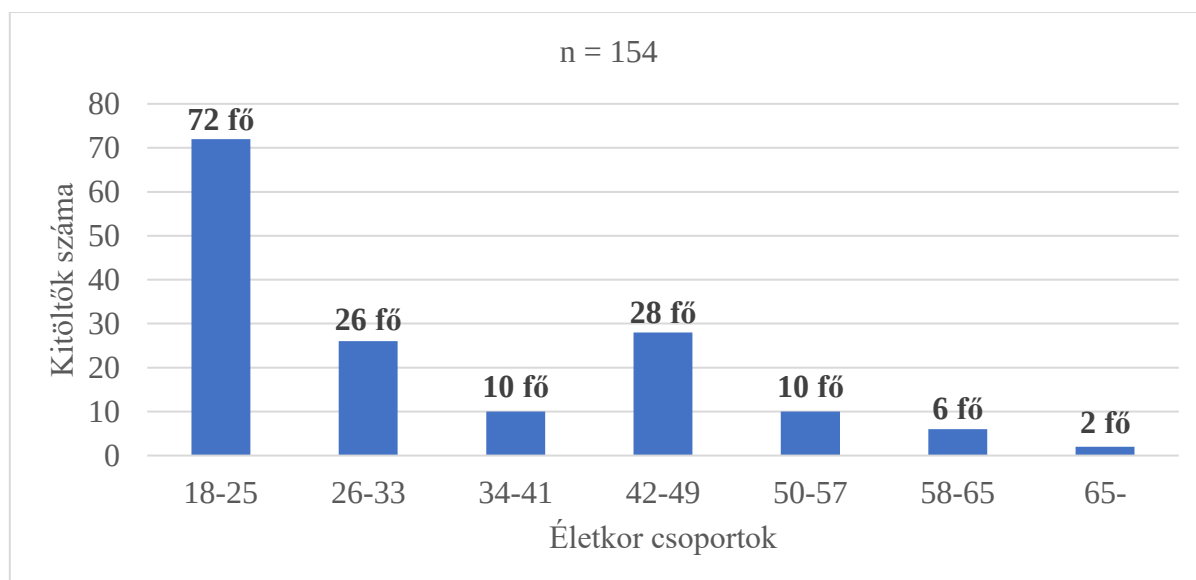
A kérdőívet 154 személy töltötte ki. A kitöltők legnagyobb részét egyetemi alap- és mesterképzésben résztvevő hallgatók, szakkollégisták, egyetemi oktatók, kutatók, az állami- és magánszektor munkavállalói, előbbi tekintetében kiemelten az egészségügyi és rendvédelmi dolgozók, valamint az informatika iránt érdeklődő, illetve információbiztonsággal a gyakorlati munkavégzés során foglalkozó emberek csoportjai adták.

3.2.1. Statisztikák

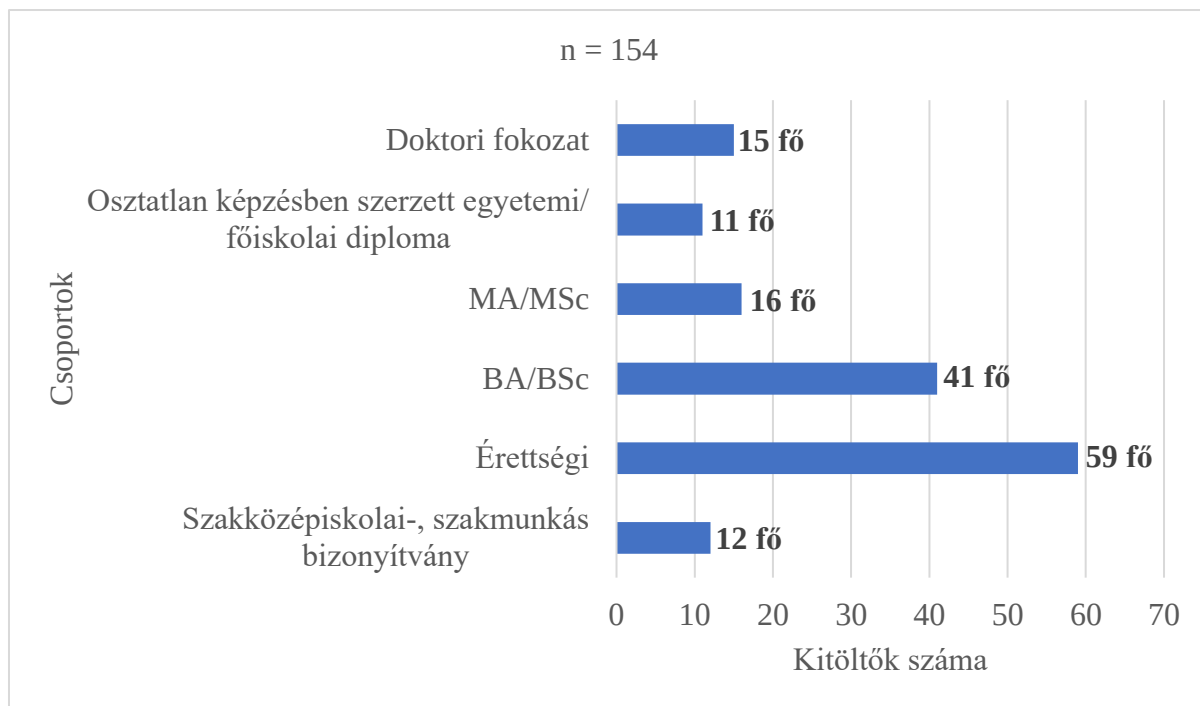
A demográfiai kérdésekre adott válaszok kapcsán a rendelkezésemre álló adatokat a jobb áttekinthetőség végett az alábbiakban diagramok formájában szeretném bemutatni:



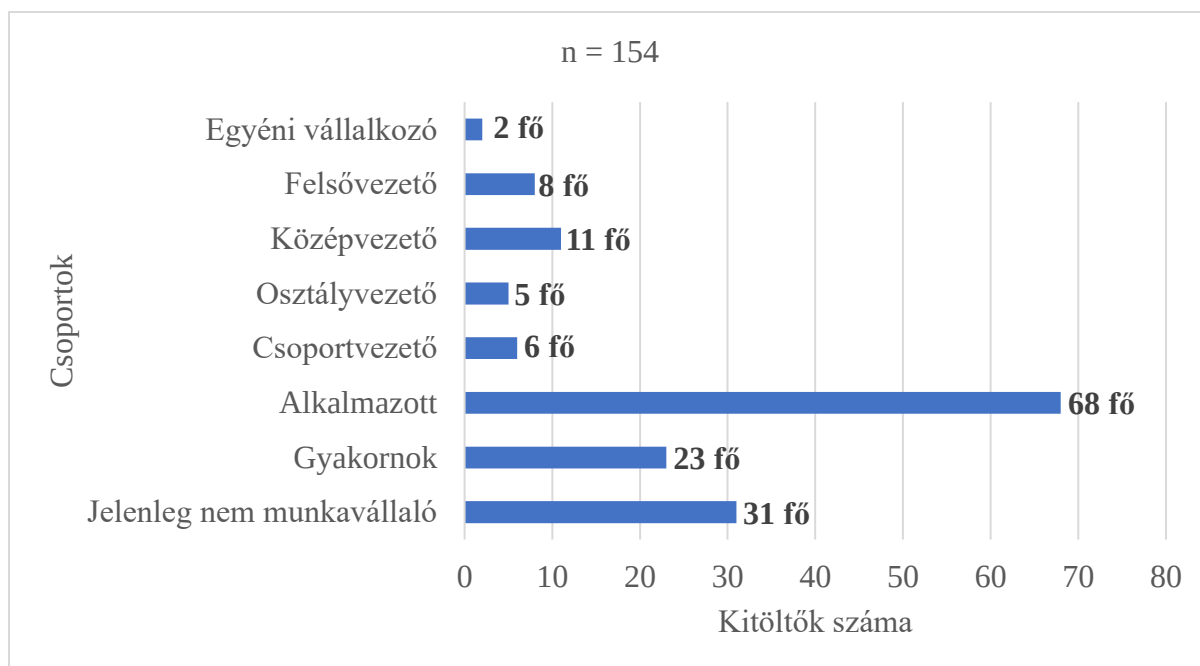
1. ábra - A kitöltők nemi megoszlása
(saját szerkesztés)



2. ábra - A kitöltők életkorának megoszlása
(saját szerkesztés)



3. ábra - A kitöltők iskolai végzettségének megoszlása
(saját szerkesztés)



4. ábra - A kitöltők jelenlegi munkahelyi pozícióinak megoszlása
(saját szerkesztés)

Összességében a kitöltők által rendelkezésemre bocsátott adatok alapján – ideértve a kitöltések „egyéni” vizsgálatát is – megállapítható, hogy az elemzésben egyaránt képviseltetik magukat akár csak az egyetemmel foglalkozó, akár a tanulmányaik mellett például gyakornokként

dolgozó hallgatók, aktív munkavállalók, beosztottak és vezetők, valamint a fiatal, középkorú és idősebb korcsoportba tartozó személyek is, a különböző iskolai végzettségi szintek széles körű megjelenésével megegyezően.

3.2.2. Az empirikus kutatás eredményei

A válaszok elemzése kapcsán szeretném első körben a „*Jelenleg használ egyénileg bármilyen privátszférát erősítő technológiát?*” valamint a „*Tudomása szerint a munkáltatója által munkavégzésre biztosított eszközökön található privátszférát erősítő technológia?*” illetve a „*Szívesebben alkalmazna otthoni környezetben olyan PET-eket, melyeket munkahelyén is használ?*” kérdéseket elemezni.

Ezen kérdések kapcsolatában elmondható, hogy 21 kitöltő nyilatkozott úgy, hogy tudomása szerint a munkáltatója által munkavégzésre biztosított eszköz rendelkezik privátszférát erősítő technológiával, és mind a 21 válaszadó szívesebben alkalmazna otthoni környezetben olyan PET-et, melyet munkahelyén is használ. Közülük ezzel a gyakorlattal 13-an élnek is. Az ezen kategóriába eső kitöltők többsége ugyan azon termékcsaládot, vagy PET-et használja otthoni környezetben, mint munkavégzés során.

A kérdőív egészének vizsgálatával a 154 válaszoló közül továbbá 130 szívesebben használna olyan PET-eket, melyeket munkahelyén is alkalmaz.

1. táblázat - Otthoni és munkahelyi környezetben egyaránt alkalmazott PET-ek (saját szerkesztés)

Szívesebben alkalmazna otthoni környezetben olyan PET-eket, melyeket munkahelyén is használ?	
Igen: 130 fő	Nem: 24 fő
Szervezeti szintű PET használat:	Otthoni környezetben történő PET használat:
21 , mindkét kérdésre azonosan „Igen”-el válaszoló kitöltő	
Megnevezett munkahelyi környezetben használt PET:	Megnevezett otthoni környezetben használt PET:
(21 főből) 13 esetben a munkahelyi környezetben alkalmazott, konkrétan megnevezett PET azonos az otthoni környezetben alkalmazott, konkrétan megnevezett PET-el.	

Ezen a ponton alátámasztottam a H2 hipotézisemet.

Az összes kitöltő tekintetében a leggyakrabban használt PET-ek közé tartoznak a VPN-ek, hirdetésblokkolók, követésblokkolók, egyéb tartalomszűrők, a jelszókezelők, autentikátorok, végpontvédelmi megoldások, hálózatbiztonsági és hálózatfigyelő technológiák, valamint egyéb, a piacvezető cégek által nyújtott különböző lehetőségek.

Az 1.2.1.-es fejezetben részletezett fizikai PET-ek is szerepeltek a felsorolások között, a leggyakrabban a kamerák eltakarói és a titkosított adathordozók.

3.2.2.1. A szakértői interjúk és empirikus eredmények összevetése

A szakértői interjúk és az empirikus kutatás közös tartalmi kérdései, melyek az elemzés alapját képezték a következők:

Szakértői interjúk:

- *Van hatással a munkavállaló privátszférájának nem megfelelő szintű védelme a szervezet biztonságára? Egy támadó szempontjából Ön szerint a szervezet munkavállalói kiemelt, potenciális célpontként jelennek meg?*
- *Egy támadó szempontjából Ön szerint a szervezet munkavállalói kiemelt, potenciális célpontként jelennek meg?*

Felmérés kérdései:

- *Ön szerint a munkavállalók saját privátszférájának nem megfelelő szintű védelme jelenthet kockázatot a szervezet biztonságára?*
- *Ön szerint támadási kísérlet esetén egy szervezet munkavállalói potenciális célpontként jelenhetnek meg a támadók számára?*

A H3. hipotézisemet szakértői válaszok alapján fogalmaztam meg, ugyanis a nem megfelelő szintű privátszféra védelem egyenesen arányos a 2. fejezetben részletezett kockázatok vonatkozásában a szervezeti biztonsággal a humán-alapú támadások és a kompromittációs lehetőségek kapcsán. Ugyanakkor a gyakorlati szempontból adott válaszok, a szakirodalom, valamint a statisztikák alapján a munkavállalók munkahelyi környezetben az adatvédelmi kérdések tekintetében nem realizálnak fokozottabb kockázatot, legalábbis a tapasztalatok alapján.

Ennek ellenére az empirikus kutatások alapján elmondható, hogy a nem megfelelő szintű privátszféra védelméből adódó, szervezeti szintet érintő kockázatot mindössze a 154-ből 12 kitöltő nem realizálta.

Emellett a munkavállalókat 154-ből mindössze 8 kitöltő nem azonosította potenciális célpontként.

Fontos emellett megjegyezni, hogy a két kérdés mindegyikére negligált választ adott kitöltők száma mindössze 4.

2. táblázat - A szervezeti biztonság értékelése munkavállalói részről (saját szerkesztés)

Ön szerint a munkavállalók saját privátszférájának nem megfelelő szintű védelme jelenthet kockázatot a szervezet biztonságára?	
Igen: 142 fő	Nem: 12 fő
Ön szerint támadási kísérlet esetén egy szervezet munkavállalói potenciális célpontként jelenhetnek meg a támadók számára?	
Igen: 146 fő	Nem: 8 fő
Mindkét kérdésre azonosan „Nem”-el válaszoló kitöltők:	
4 fő	

Ezen a ponton részben cáfoltam a H3. hipotézisemet, ugyanis statisztikai a felmérés szerinti szempontból ugyan tisztában vannak a munkavállalók a potenciális fenyegetésekkel, ám a gyakorlati tapasztalatok és a szakirodalom szempontjából ez az eredmény nem állja meg a helyét.

A H4. hipotézisemet szintén a szakirodalomra és szakértői interjúkra alapozva fogalmaztam meg. Ennek kapcsán a következő kérdéseket vettem alapul:

Szakértői interjúk:

- *Ön szerint a különböző védett rendszerekhez való hozzáféréssel rendelkező munkatársak a potenciális fenyegetések (otthoni környezetben – magánszféra nem megfelelő védelméből adódó kockázatok) tudatában nyitottabbak lennének PET-ek otthoni alkalmazására?*

Felmérés kérdései:

- *Amennyiben munkavégzése során hozzáférhetne szervezete védett rendszereihez, úgy fokozottabban ügyelne adatainak védelmére munkahelyi környezetben?*
- *Amennyiben munkavégzése során hozzáférhetne szervezete védett rendszereihez, úgy fokozottabban ügyelne adatainak védelmére otthoni környezetben is?*

A szakértői vélemények alapján elmondható, hogy a védett rendszerekhez történő hozzáférést teljes mértékben elvonatkoztatnák az általános hozzáállástól (ld.: H3. hipotézis esetében), és teljesen más tapasztalatokról számolnak be ennek kapcsán. Ezen szempont esetében az esetek jelentős többségében már olyan szakemberekről, munkatársakról beszélhetünk, akik a hozzáféréseik, jogköreik kapcsolatában már olyan szakmai, információbiztonsági (tudatossági) attitűdökkel rendelkeznek, melyek egyenes arányosan eredményezik a fokozottabb figyelmet az adatvédelmi megoldásokra, és a privátszféra védelmének szerepét, melynek egy fontos aspektusa a privátszférát erősítő technológiák alkalmazása, vagy legalábbis az azok használatára történő hajlandóság egyaránt otthoni és munkahelyi környezetben.

Ezeket az állításokat az empirikus felmérés is alátámasztotta, melyek szerint a 154-ből mindössze 14 fő nem ügyelne fokozottabban az adatvédelmi megoldásokra munkahelyi környezetben a védett rendszerekhez való hozzáférés esetén.

Emellett 154-ből mindössze 12 fő volt, aki a védett rendszerekhez történő hozzáférés esetén otthoni környezetben nem ügyelne fokozottabban az adatvédelmi megoldásokra.

A közös halmazba jelen kérdések esetébe 8 fő tartozik, akik egyik esetben sem tartották fontosnak a megfelelő szintű adatvédelmet.

3. táblázat - A védett rendszerek és az adatvédelem megítélése munkavállalói részről (saját szerkesztés)

Amennyiben munkavégzése során hozzáférhetne szervezete védett rendszereihez, úgy fokozottabban ügyelne adatainak védelmére munkahelyi környezetben?	
Igen: 140 fő	Nem: 14 fő
Amennyiben munkavégzése során hozzáférhetne szervezete védett rendszereihez, úgy fokozottabban ügyelne adatainak védelmére otthoni környezetben is?	
Igen: 142 fő	Nem: 12 fő
Mindkét kérdésre azonosan „Nem”-el válaszoló kitöltők:	
8 fő	

Ezen a ponton alátámasztottam a H4. hipotézisemet.

3.2.3. Tudományos elemzés

A megfogalmazott kutatási célkitűzések és hipotézisek mentén a rendelkezésemre álló kérdőíves adatok alapján az IBM SPSS Statistics szoftverrel szeretném bemutatni a tudományos eredményeimet, melynek módszertanul keresztábra-elemzést választottam, mely segítségével a különböző változók között szignifikáns összefüggéseket kerestem, majd annak megléte esetén azok közötti erősséget határoztam meg, pontosabban a keresztábra elemzés eredményeképpen a Khí-négyzet próba (X^2 vagy X^2) elemzésével szignifikáns összefüggéseket kutattam, majd amennyiben találtam összefüggést, a Cramer's V (C V) asszociációs együtttható vizsgálatának tekintetében az asszociációs mérőszám által meghatároztam az összefüggés mértékét.

Az eredményeket a 3. számú melléklet tartalmazza.

A tudományos módszertan szerinti elemzés alapjául az alábbi, a kérdőív III.-IV. szakaszában szereplő kérdések szolgáltak:

Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok használatát önállóan, autodidakta módon kellene elsajátítania?

Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok használatát a munkáltató munkaidőben, képzés / oktatás keretében mutatná be?

A válaszok alapján a PET-ek autodidakta módon történő elsajátítása 25%-kal nagyobb elutasítottságot mutatott, mint a munkahelyen történő képzés, oktatás keretében történő bemutatás.

Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok esetleges anyagi vonzatát önerőből kellene finanszíroznia?

Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok esetleges anyagi vonzatát a munkáltató finanszírozná?

Az anyagi vonzatok tekintetében pedig a 154 főből mindössze 6 kitöltő nem élne a munkáltató általi finanszírozás lehetőségével, míg önerőből mindössze 66 fő lenne hajlandó fizetni a különböző technológiákért.

Összességében tehát elmondható, hogy a válaszadók az autodidakta elsajátítás helyett inkább vennének részt a munkáltató által szervezett oktatáson, képzésen, és jelentősen többen alkalmaznának privátszférát erősítő technológiákat, amint annak fedezetéről a munkáltató gondoskodik. Mindezekből adódóan a tudományos elemzések alapját így ez a két kérdés fogja adni.

Az összevetés szempontjait pedig a potenciális kockázatok kapcsán határoztam meg, melyek tekintetében az alábbi kérdésekre adott válaszok voltak az irányadók:

Fokozottabban ügyel adatai védelmére, amennyiben különböző adatvédelmi hiátusokat tapasztal?

Fokozottabban ügyel adatai védelmére, amennyiben tudomására jut, hogy azt 3. fél is kezelheti / 3. fél számára is értékesíthető?

Amennyiben anyagi vagy kényelmi szempontból kedvezőbb feltételekkel juthat hozzá bizonyos szolgáltatásokhoz, abban az esetben kevésbé ügyel adatainak teljes körű védelmére?

A szervezeti szinten biztosított oktatás és az anyagi vagy kényelmi kedvezőbb feltételekkel igénybe vehető szolgáltatások kapcsán történő önkéntes adatmegosztás tekintetében az alábbi eredményeket kaptam:

Szignifikáns összefüggést (kétoldalú szignifikanciát) fedeztem fel, fennálló korrelációval.

A Khí-négyzetének (továbbiakban: X^2) megfigyelt értéke 5,066, amelynek kétoldali szignifikanciaszintjének értéke 0,024, tehát megállapítom, hogy a két változó között az összefüggés szignifikáns ($p < 0,05$). A kapcsolat erősségét Cramer's V (továbbiakban C V) segítségével vizsgáltam, ugyanis ez tekinthető az egyik legmegbízhatóbb mutatónak. A C V egy asszociációs együttható, amely két nominális változó közötti szorosságot mutatja meg. A C V értéke 0 és 1 közötti intervallum közötti, a 0-hoz való közelség függetlenséget, az 1-hez való közelség erős kapcsolatot jelent. Vizsgálatomban a Cramer's V mutató megfigyelt értéke 0,024. A 0,024-es érték alacsony korrelációra utal a két változó esetében.

A szervezeti szinten biztosított oktatás és az adatvédelmi hiátusok tapasztalásakor is igénybe vett szolgáltatások kapcsán történő önkéntes adatmegosztás tekintetében az alábbi eredményeket kaptam:

Szignifikáns összefüggést (kétoldalú szignifikanciát) fedeztem fel, fennálló korrelációval.

A X^2 megfigyelt értéke 4,066, amelynek kétoldali szignifikanciaszintjének értéke 0,031, tehát megállapítom, hogy a két változó között az összefüggés szignifikáns ($p < 0,05$). Vizsgálatomban a kapcsolat erőssége, a C V asszociációs mutató megfigyelt értéke 0,173. A 0,173-as érték alacsony korrelációra utal a két változó esetében.

A szervezeti szinten biztosított oktatás és a harmadik fél által történő adatkezelés fennállásának ellenére is igénybe vett szolgáltatások kapcsán történő önkéntes adatmegosztás tekintetében az alábbi eredményeket kaptam:

Szignifikáns összefüggést (kétoldalú szignifikanciát) fedeztem fel, fennálló korrelációval.

A X^2 megfigyelt értéke 5,529, amelynek kétoldali szignifikanciaszintjének értéke 0,019, tehát megállapítom, hogy a két változó között az összefüggés szignifikáns ($p < 0,05$). Vizsgálatomban a kapcsolat erőssége, a C V asszociációs mutató megfigyelt értéke 0,189. A 0,189-es érték alacsony korrelációra utal a két változó esetében.

A szervezeti szinten finanszírozott technológiák alkalmazásának és az anyagi vagy kényelmi kedvezőbb feltételekkel igénybe vehető szolgáltatások kapcsán történő önkéntes adatmegosztás kapcsán az alábbi eredményeket kaptam:

Szignifikáns összefüggést (kétoldalú szignifikanciát) fedeztem fel, fennálló korrelációval.

A X^2 megfigyelt értéke 8,153, amelynek kétoldali szignifikanciaszintjének értéke 0,004, tehát megállapítom, hogy a két változó között az összefüggés szignifikáns ($p < 0,05$).

Vizsgálatomban a kapcsolat erőssége, a C V asszociációs mutató megfigyelt értéke 0,230. A 0,230-as érték alacsony és közepes szint közötti korrelációra utal a két változó esetében.

A szervezeti szinten finanszírozott technológiák alkalmazásának és az adatvédelmi hiátusok tapasztalásakor is igénybe vett szolgáltatások kapcsán történő önkéntes adatmegosztás tekintetében az alábbi eredményeket kaptam:

Szignifikáns összefüggést (kétoldali szignifikanciát) fedeztem fel, fennálló korrelációval.

A χ^2 megfigyelt értéke 8,457, amelynek kétoldali szignifikanciaszintjének értéke 0,004, tehát megállapítom, hogy a két változó között az összefüggés szignifikáns ($p < 0,05$). Vizsgálatomban a kapcsolat erőssége, a C V asszociációs mutató megfigyelt értéke 0,234. A 0,234-es érték alacsony és közepes szint közötti korrelációra utal a két változó esetében.

A szervezeti szinten finanszírozott technológiák alkalmazásának és a harmadik fél által történő adatkezelés fennállásának ellenére is igénybe vett szolgáltatások kapcsán történő önkéntes adatmegosztás tekintetében az alábbi eredményeket kaptam:

Szignifikáns összefüggést (kétoldali szignifikanciát) fedeztem fel, fennálló korrelációval.

A χ^2 megfigyelt értéke 10,089, amelynek kétoldali szignifikanciaszintjének értéke 0,001, tehát megállapítom, hogy a két változó között az összefüggés szignifikáns ($p < 0,05$). Vizsgálatomban a kapcsolat erőssége, a C V asszociációs mutató megfigyelt értéke 0,256. A 0,256-es érték közepes szintű korrelációra utal a két változó esetében.

Ezen a ponton alátámasztottam a H1. hipotézisemet.

A profilalkotás veszélyeivel kapcsolatos tudatosság, és a privátszférát erősítő technológiák szervezeti szintű (oktatás, finanszírozás) elsajátítása kapcsán nem fedeztem fel szignifikáns összefüggést, ám a 3. számú mellékletben is látható eredmények tekintetében mindkét esetben több, mint háromszor annyian élnének valamely bevezetési lehetőséggel azok közül, akik nem tartják kockázatosnak a profilozást, mint akik elutasítóak voltak a kérdés tekintetében.

Ugyan ez az összefüggés állapítható meg az egyénekről történő adatgyűjtés, adatkezelés kockázatosságának és a szervezeti szintű oktatás vagy technológia finanszírozásának tekintetében. Az arányszám ezesetben kétszeres, tehát kétszer annyi kitöltő élne valamely bevezetési lehetőséggel azok közül, akik nem tekintik kockázatosnak az adatgyűjtést, adatkezelést. Az eredményeket a 3. számú melléklet tartalmazza.

Következtetések

Az empirikus kutatás eredményeinek vizsgálatakor a további kutatást igénylő területen belül, a szentiment analízishez felhasználható kérdések kivételével az elemzés tárgyát képezte minden megválaszolt kérdés, melyeket vagy az összekapcsolható esetekben a szakmai interjúk összesített eredményeivel, vagy a tudományos statisztikai módszertannal értékeltem ki.

Összességében megállapítható, hogy az empirikus felmérés és interjúk egy koherens, egész képet nyújtanak a privátszférát erősítő technológiák vizsgált kérdésköreiről és befogadhatóságáról, mely tekintetében az egyének, és általuk a szervezetek kiberbiztonsági képességei is szignifikánsan növelhetők.

Összegzés

Az egyének sikeres kompromittálását a támadók gyakran az úgynevezett humán-eredetű sérülékenységeket kihasználásával érhetik el a legkönnyebb, leggyorsabb és leghatékonyabb módon. A humán-alapú támadások alapanyagául pedig a személyek – akár tudta nélkül, akár beleegyezésével – gyűjtött, a mindennapi online, internetes felületeken töltött idő alatt

Ezzel kapcsolatban a szakértői interjúk és a felmérésre adott válaszok kapcsán egy érdekes következtetésre juthatunk: A szakértők alapvetően nem fogalmaznak meg kifejezetten pozitív álláspontot az egyének információbiztonsági kompetenciáival kapcsolatban, ám a felmérésre adott válaszok alapján – teoretikusan – arra a következtetésre juthatunk, hogy a személyek elméleti síkon tisztában vannak a potenciális kockázatokkal, azonban ez a gyakorlatban nem feltétlenül a „papírforma” szerint elvárt módon mutatkozik meg. Ebből a következtetésből azt a konzekvenciát vonhatjuk le, miszerint nem elegendő az elméleti képzés és oktatás, azt gyakorlati elemekkel, kampányokkal, jó gyakorlat meghatározásával szükséges erősíteni az egyéni és a szervezeti biztonság növelésének érdekében.

A kutatás eredményeként megállapíthatjuk, hogy az egyének védelmi képességeinek növelésével párhuzamosan növelhető a szervezet biztonsági szintje is, többek között a részletezett kockázatokkal kapcsolatban a privátszférát erősítő technológiák alkalmazásával. Az bevezetés kapcsán fontos kiemelni, hogy annak gyakorlati úton történő, a munkáltató által szervezett és az otthoni környezetben is alkalmazható PET-ek jelenthetik a legadekvátabb

megoldást, mely az eredmények kapcsán mind szervezeti, mind egyéni szinten csökkenthetjük a veszélyforrások egy, a profilalkotás és a humán-alapú támadások által relevánsnak mondható hányadát.

A fentiek alapján kutatásomban az alábbi eredményeket fogalmaztam meg:

T1. Bizonyítottam, hogy a privátszférát erősítő technológiák alkalmazásának szervezeti szintű oktatása és képzése általi, vagy az anyagi vonzattal járó technológiák szervezeti szintű finanszírozása növeli az egyének, és ezáltal a szervezet kiberbiztonsági képességeit.

T2. Bizonyítottam, hogy az egyének hajlandók otthoni környezetbe is integrálni olyan PET-eket, melyeket munkahelyi környezetben is használnak. Továbbá a jelenleg egyaránt otthoni és munkahelyi környezetben is PET-eket alkalmazó személyek többsége ugyan azon technológiákat használja egyénileg, mint szervezeti szinten.

T3. Részben cáfoltam, hogy a H3. hipotézisemet, ugyanis szervezeti szempontból a munkavállalók tudatában vannak annak, hogy egy szervezetet ért támadás esetén ők is célpontként jelenhetnek meg, illetve annak is, hogy a privátszférájuk nem megfelelő szintű védelme potenciális veszélyforrásokat rejt magában. Ugyanakkor fontos megjegyezni, hogy a szakértői interjúk, a gyakorlati tapasztalat, a globális statisztikák és a szakirodalom is ennek ellentmondóan kiemeli a humán alapú, az információbiztonsági (tudatossági) attitűdök hiányát, és a nem megfelelő szintű privátszféra védelmét munkavállalói szempontból.

T4. Bizonyítottam, hogy a munkavállalók a védett rendszerekhez történő hozzáférés esetén fokozottabban ügyelnek az adatvédelmi megoldásokra egyaránt otthoni és munkahelyi környezetben.

További kutatást igénylő területek

A további kutatást igénylő területek egyike az 1. fejezetben is tárgyalt, a fizikai térben jelenlévő privátszférát erősítő technológiák kérdéskörének elemzése, mely kapcsán alapvetően vizsgálati szempontból az információs rendszerek tekintetében is alkalmazott módszertannal is élhetünk, ám a hasznosítás, a potenciális kockázatok, az információbiztonságban betöltött szerepe és maga, a szakirodalmi háttér tekintetében egy új kutatást igénylő terület.

Egy másik aspektus, pontosabban kiegészítő kutatási lehetőség egy szentiment analízis, melyet a jelenleg is rendelkezésemre álló kérdőívre adott válaszok és a szakmai interjúk is megalapozhatnak.

Összességében pedig természetesen új hipotézisek, új tudományos elemzések, a résztvevők számának kibővítése és kontrollcsoport bevonása jelentheti ezen kutatás potenciális folytatását.

Irodalomjegyzék

- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
2009. évi CLV. törvény a minősített adat védelméről
2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
2012. évi I. törvény a munka törvénykönyvéről
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
2018. évi CXXV. törvény a kormányzati igazgatásról
- Alaya, Bechir, Lamri Laouamer, és Nihel Msilini. „Homomorphic Encryption Systems Statement: Trends and Challenges”. *Computer Science Review* 36 (2020. május 1.): 100235. <https://doi.org/10.1016/j.cosrev.2020.100235>.
- Ali, Waqas, Mohammad Nauman, és Nouman Azam. „A Privacy Enhancing Model for Internet of Things Using Three-Way Decisions and Differential Privacy”. *Computers and Electrical Engineering* 100 (2022. május 1.): 107894. <https://doi.org/10.1016/j.compeleceng.2022.107894>.
- Anjaiah Gujjary, Vishal, és Ashutosh Saxena. „A Neural Network Approach for Data Masking”. *Neurocomputing* 74, sz. 9 (2011. április): 1497–1501. <https://doi.org/10.1016/j.neucom.2011.01.002>.
- Az Európai Parlament és a Tanács (EU) 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- Borking, John, P. Verhaar, B.M.A. Eck, P. Siepel, G.W. Blarkom, R. Coolen, M. Uyl, és mtsai. *Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents*, 2003. <https://doi.org/10.13140/2.1.4888.7688>.
- Bošnjak, Leon, és Boštjan Brumen. „Shoulder Surfing Experiments: A Systematic Literature Review”. *Computers & Security* 99 (2020. december): 102023. <https://doi.org/10.1016/j.cose.2020.102023>.
- Curzon, James, Abdulaziz Almeahmadi, és Khalil El-Khatib. „A Survey of Privacy Enhancing Technologies for Smart Cities”. *Pervasive and Mobile Computing* 55 (2019. április): 76–95. <https://doi.org/10.1016/j.pmcj.2019.03.001>.
- Ding, Bolin, Janardhan Kulkarni, és Sergey Yekhanin. „Collecting Telemetry Data Privately”. In *Advances in Neural Information Processing Systems*, Köt. 30. Curran Associates, Inc., 2017. <https://papers.nips.cc/paper/2017/hash/253614bbac999b38b5b60cae531c4969-Abstract.html>.
- Drev, Matjaž, és Boštjan Delak. „Conceptual Model of Privacy by Design”. *Journal of Computer Information Systems* 0, sz. 0 (2021. július 1.): 1–8. <https://doi.org/10.1080/08874417.2021.1939197>.
- Edwards, Matthew, Robert Larson, Benjamin Green, Awais Rashid, és Alistair Baron. „Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces”. *Computers & Security* 69 (2017. augusztus): 18–34. <https://doi.org/10.1016/j.cose.2016.12.013>.
- Erlingsson, Úlfar, Vasyi Pihur, és Aleksandra Korolova. „RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response”. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 1054–67. CCS '14. New York, NY, USA: Association for Computing Machinery, 2014. <https://doi.org/10.1145/2660267.2660348>.

- Fischer-Hbner, Simone, és Stefan Berthold. „Privacy-Enhancing Technologies”. In *Computer and Information Security Handbook*, 759–78. Elsevier, 2017. <https://doi.org/10.1016/B978-0-12-803843-7.00053-3>.
- Heartfield, Ryan, és George Loukas. „A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks”. *ACM Computing Surveys* 48, sz. 3 (2016. február 8.): 1–39. <https://doi.org/10.1145/2835375>.
- Heurix, Johannes, Peter Zimmermann, Thomas Neubauer, és Stefan Fenz. „A Taxonomy for Privacy Enhancing Technologies”. *Computers & Security* 53 (2015. szeptember): 1–17. <https://doi.org/10.1016/j.cose.2015.05.002>.
- Jahan, Sohely, Md. Saifur Rahman, és Sajeeb Saha. „Application specific tunneling protocol selection for Virtual Private Networks”. In *2017 International Conference on Networking, Systems and Security (NSysS)*, 39–44, 2017. <https://doi.org/10.1109/NSysS.2017.7885799>.
- Kaaniche, Nesrine, Maryline Laurent, és Sana Belguith. „Privacy Enhancing Technologies for Solving the Privacy-Personalization Paradox: Taxonomy and Survey”. *Journal of Network and Computer Applications* 171 (2020. december): 102807. <https://doi.org/10.1016/j.jnca.2020.102807>.
- Koorn R., Gils H., Hart J., Overbeek P., és Tellegen R. *Privacy-Enhancing Technologies White Paper for Decision-Makers*. Directorate of Public Sector Innovation and Information Policy, 2004.
- Li, Feng, és Bruce McMillin. „Chapter Two - A Survey on Zero-Knowledge Proofs”. In *Advances in Computers*, szerkesztette Ali Hurson, 94:25–69. Elsevier, 2014. <https://doi.org/10.1016/B978-0-12-800161-5.00002-5>.
- Mazurek, Grzegorz, és Karolina Małagocka. „Perception of privacy and data protection in the context of the development of artificial intelligence”. *Journal of Management Analytics* 6, sz. 4 (2019. október 2.): 344–64. <https://doi.org/10.1080/23270012.2019.1671243>.
- Metalidou, Efthymia, Catherine Marinagi, Panagiotis Trivellas, Niclas Eberhagen, Christos Skourlas, és Georgios Giannakopoulos. „The Human Factor of Information Security: Unintentional Damage Perspective”. *Procedia - Social and Behavioral Sciences* 147 (2014. augusztus): 424–28. <https://doi.org/10.1016/j.sbspro.2014.07.133>.
- Pfitzmann, Andreas, TU Dresden, Marit Hansen, és ULD Kiel. „Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology”, é. n., 83.
- Rao, Ashwin, Justine Sherry, Arnaud Legout, Arvind Krishnamurthy, Walid Dabbous, és David Choffnes. „Meddle: middleboxes for increased transparency and control of mobile traffic”. In *Proceedings of the 2012 ACM conference on CoNEXT student workshop*, 65–66. CoNEXT Student '12. New York, NY, USA: Association for Computing Machinery, 2012. <https://doi.org/10.1145/2413247.2413286>.
- Reinsel, David, John Gantz, és John Rydning. „The Digitization of the World from Edge to Core”, 2018, 28.
- Riboni, Daniele, és Claudio Bettini. „Differentially-private release of check-in data for venue recommendation”. In *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 190–98. Budapest, Hungary: IEEE, 2014. <https://doi.org/10.1109/PerCom.2014.6813960>.
- Schaar, Peter. „Privacy by Design”. *Identity in the Information Society* 3, sz. 2 (2010. augusztus 1.): 267–74. <https://doi.org/10.1007/s12394-010-0055-x>.
- Seničar, Vanja, Borka Jerman-Blažič, és Tomaž Klobučar. „Privacy-Enhancing Technologies—Approaches and Development”. *Computer Standards & Interfaces* 25, sz. 2 (2003. május): 147–58. [https://doi.org/10.1016/S0920-5489\(03\)00003-5](https://doi.org/10.1016/S0920-5489(03)00003-5).

- Shin, Hyejin, Sungwook Kim, Junbum Shin, és Xiaokui Xiao. „Privacy Enhanced Matrix Factorization for Recommendation with Local Differential Privacy”. *IEEE Transactions on Knowledge and Data Engineering* 30, sz. 9 (2018. szeptember): 1770–82. <https://doi.org/10.1109/TKDE.2018.2805356>.
- Székely Iván. „Privát szférát erősítő technológiák”. *Információs Társadalom* 8, sz. 1 (2008. március 1.): 20. <https://doi.org/10.22503/inftars.VIII.2008.1.3>.
- Torres, Christof Ferreira, Hugo Jonker, és Sjouke Mauw. „FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting”. In *Computer Security -- ESORICS 2015*, szerkesztette Günther Pernul, Peter Y A Ryan, és Edgar Weippl, 3–19. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-24177-7_1.
- Traverso, Stefano, Martino Trevisan, Leonardo Giannantoni, Marco Mellia, és Hassan Metwalley. „Benchmark and comparison of tracker-blockers: Should you trust them?”. In *2017 Network Traffic Measurement and Analysis Conference (TMA)*, 1–9, 2017. <https://doi.org/10.23919/TMA.2017.8002898>.
- Xin, Bangzhou, Yangyang Geng, Teng Hu, Sheng Chen, Wei Yang, Shaowei Wang, és Liusheng Huang. „Federated Synthetic Data Generation with Differential Privacy”. *Neurocomputing* 468 (2022. január 11.): 1–10. <https://doi.org/10.1016/j.neucom.2021.10.027>.
- Zhao, Chuan, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong-Zhi Gao, Hongwei Li, és Yu-an Tan. „Secure Multi-Party Computation: Theory, Practice and Applications”. *Information Sciences* 476 (2019. február 1.): 357–72. <https://doi.org/10.1016/j.ins.2018.10.024>.
- Zwilling, Moti, Galit Klien, Dušan Lesjak, Łukasz Wiecheteck, Fatih Cetin, és Hamdullah Nejat Basim. „Cyber Security Awareness, Knowledge and Behavior: A Comparative Study”. *Journal of Computer Information Systems* 62, sz. 1 (2022. január 2.): 82–97. <https://doi.org/10.1080/08874417.2020.1712269>.

Függelék, mellékletek

Rövidítések jegyzéke

Rövidítés	Magyar megnevezés	Angol nyelvű megnevezés
C V	-	Cramer's V
CIA	Bizalmasság, sértetlenség, rendelkezésre állás	Confidentiality, Integrity, Availability
EP	Európai Parlament	European Parliament
EU	Európai Unió	European Union
GDPR	Általános adatvédelmi rendelet	General Data Protection Regulation
HAIS-Q	Információbiztonság humán aspektusa kérdőív	Human Aspects of Information Security Questionnaire
Ibtv.	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról	-
IKT	Infokommunikációs technológia	Information and Communications Technology
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról	-
IoT	Hálózati hozzáféréssel (internet kapcsolattal) rendelkező eszközök	Internet of Things
Kit.	2018. évi CXXV. törvény a kormányzati igazgatásról	-
Mavtv.	2009. évi CLV. törvény a minősített adat védelméről	-
Mt.	2012. évi I. törvény a munka törvénykönyvéről	-
PbD	Beépített alapértelmezett adatvédelem	Privacy by design
PET	Privátszférát erősítő technológiák	Privacy-enhancing technologies
SJR	SCImago Folyóirat Rangsor	Scimago Journal Rank
SMPC	Biztonságos, több fél részvételével történő számítás	Secure multi-party computation

TET	Átláthatóságot fokozó eszközök	Transparency-enhancing tools
VPN	Virtuális magánhálózat	Virtual private network
X ²	Khí-négyzet	Chi-Square
ZKP	Nulla-tudásalapú igazolás-támogatás	Zero knowledge proofs

Ábrajegyzék

1. ábra - A kitöltők nemi megoszlása (saját szerkesztés) 26
2. ábra - A kitöltők életkorának megoszlása (saját szerkesztés) 26
3. ábra - A kitöltők iskolai végzettségének megoszlása (saját szerkesztés)..... 27
4. ábra - A kitöltők jelenlegi munkahelyi pozícióinak megoszlása (saját szerkesztés)..... 27

Táblázatok jegyzéke:

1. táblázat - Otthoni és munkahelyi környezetben egyaránt alkalmazott PET-ek (saját szerkesztés)..... 28
2. táblázat - A szervezeti biztonság értékelése munkavállalói részről (saját szerkesztés) 30
3. táblázat - A védett rendszerek és az adatvédelem megítélése munkavállalói részről (saját szerkesztés)..... 32

Mellékletek

1. számú melléklet: Szakértői interjúk vonalvezetésével szolgáló kérdéssor.

1. Értelmezhető-e egy szervezet biztonsága a humán tényező figyelembevétele nélkül?
2. Létezik olyan szoftveres, vagy akár klasszikus értelemben olyan adminisztratív, logikai, fizikai védelmi intézkedés, amely lehetővé teszi a szervezet védelmi képességeinek maximalizálását a humán tényező figyelembevétele nélkül?
3. Milyen potenciális, a szervezetre vonatkozó veszélyforrásokat, a támadók számára kompromittációs lehetőségeket rejt magában (akár konkrétumokkal, példákkal vagy általánosságban):
 - a. a nem megfelelő szakmai kompetenciákkal rendelkező munkavállaló?
 - b. a nem megfelelő szintű (információ)biztonsági tudatossággal rendelkező munkavállaló?
 - c. a megfelelő szakmai kompetenciákkal és megfelelő, munkahelyi információbiztonsági attitűddel rendelkező munkavállaló, aki otthoni környezetben nem alkalmazza a munkahelyi környezetben – akár szabályzók megléte végett – elvárt magatartásokat (közösségi média-jelenlét, jogtisztaszoftverek, böngészőhasználat, alkalmazás és szoftverengedélyek, általános

biztonságtudatossági attitűd (sütik, PET-ek általános alkalmazása), védelmi megoldások (naprakész vírusirtó szoftver), stb.)?

4. A nem megfelelő szintű privátszféra védelem milyen potenciális fenyegetéseket hordozhat magában a személyek vonatkozásában?
5. Van hatással a munkavállaló privátszférájának nem megfelelő szintű védelme a szervezet biztonságára? És ha igen, milyen?
6. Milyen potenciális veszélyeket okozhat a nem megfelelő privátszféra védelme, és ezáltal a munkavállaló kompromittálásának lehetősége a vállalat biztonságára? Összességében tekinthetjük releváns kockázatnak, fenyegetésnek a nem megfelelő szintű privátszféra védelméből adódó, magukat a személyeket érintő kompromittálásokat, melyek közvetlen hatással lehetnek a vállalat biztonságára?
 - a. Mik lehetnek ezek a hatások?
7. Egy támadó szempontjából Ön szerint a szervezet munkavállalói kiemelt, potenciális célpontként jelennek meg?
 - a. Ha igen, úgy Ön szerint a támadás könnyebben és sikerebben végrehajtható, ha a támadó a magánszféra nem megfelelő védelméből eredő hiátusokat használja ki a munkavállaló támadásakor?
8. Hogy tudná megfogalmazni a privátszférát erősítő technológiák fogalmát?
9. Tudna példát mondani potenciálisan, vagy akár jelenleg is alkalmazható vagy alkalmazandó PET-ekről:
 - a. szervezeti környezetben
 - b. otthoni környezetben
10. Van Ön által ismert, bevett, „jó gyakorlat” a PET-ek használatával kapcsolatban?
11. Ön szerint előfordulhat, hogy a munkavállalók kedvezőbb kényelmi, anyagi szempontból kevésbé foglalkoznak adataik védelmével?
12. Ön szerint a fenyegetések potenciális célpontjai tisztában vannak a róluk – akár beleegyezésükkel – tárolt adatok kockázataival?
 - a. Ön szerint melyek a legrelevánsabb kockázatok?
13. Ön szerint munkahelyi környezetükben a szervezet munkatársai fokozottabban ügyelnek azon adataik megadására, melynek kezeléséről harmadik fél gondoskodik; vagy adatvédelmi hiátusokat tapasztalnak?
14. Ön szerint a különböző védett rendszerekhez való hozzáféréssel rendelkező munkatársak a potenciális fenyegetések (otthoni környezetben – magánszféra nem megfelelő védelméből adódó kockázatok) tudatában nyitottabbak lennének PET-ek otthoni alkalmazására?
15. Ön szerint a belső továbbképzések, tudatosítás, oktatások és kampányok (megbízható források) hozzájárulhatnak ahhoz, hogy a szervezet munkatársai gyakrabban és magabiztosabban használják a különböző adatvédelmi és kiber-higiéniát erősítő megoldásokat?
16. Egy szervezet szempontjából a PET-ek használatának, bevezethetőségének kapcsolatában mi jelentheti az optimumot a ráfordított pénz – idő – energia vonatkozásában?

- a. Lehet diverzifikálni a szükségesen a munkavállalók privátszférájának erősítésére allokálható erőforrásokat pl. a beosztás / hozzáférés / jog- és hatáskörök tekintetében?
17. Otthoni környezetben egy szervezet kötelezővé teheti-e PET-ek alkalmazását, vagy ajánlásként megfogalmazhatja-e azt?
18. Munkahelyi eszközökön egy szervezet kötelezővé teheti-e PET-ek alkalmazását, vagy ajánlásként megfogalmazhatja-e azt? Melyek lehetnek az elégséges – optimális megoldások?
19. Ön szerint van különbség a sikeresség, hatásfok, a szükséges támadásra fordítandó erőforrások tekintetében a klasszikus támadások (spam, malware-k, stb.) és kifejezetten a privátszféra nem megfelelő védelmét kihasználó támadások között?

2. számú melléklet: A kérdőív szövege

A privátszférát erősítő technológiák szerepe a kiberbiztonságban

Tisztelt Kitöltő!

NÉV vagyok, a(z) *EGYETEM SZAK* hallgatója.

Jelen kutatásomban a privátszférát erősítő technológiák (PET-ek) befogadásának, alkalmazásának és implementálásának lehetőségeit vizsgálom. Ezen kérdőív kitöltésével (mely nem tart tovább néhány percnél) nagyban hozzájárulhat az említett kérdéskör tudományos értékű elemzéséhez.

Kérem, a második oldal kitöltése előtt olvassa el a lap tetején található leírást.

A kitöltés során keletkezett adatok kezelése bizalmasan zajlik, és azok felhasználása kizárólag a kutatásra korlátozódik.

Az adatvédelmi elveket illetően a Google adatvédelmi szabályzata az irányadó:
<https://policies.google.com/privacy?hl=hu>

Bármilyen felmerülő kérdés, észrevétel, javaslat tekintetében keressen bizalommal az alábbi címen:

E-MAIL CÍM

Köszönettel,

NÉV

I. Demográfiai adatok

1. Neme: (Kötelező)

- Férfi
- Nő

2. Életkora: (Kötelező)

- 18-25
- 26-33
- 34-41
- 42-49
- 50-57
- 58-65
- 65-

3. Legmagasabb iskolai végzettsége: (Kötelező)

- Általános iskola
- Szakközépiskolai-, szakmunkás bizonyítvány
- Érettségi
- BA/BSc
- MA/MSc
- Osztatlan képzésben szerzett egyetemi/főiskolai diploma
- Doktori fokozat
- Egyéb: ...

4. Munkahelyén (akár főállásban, akár hallgatóként részmunkaidőben) milyen pozíciót tölt be?

(Kötelező)

- Gyakornok
- Alkalmazott
- Csoportvezető
- Osztályvezető
- Középvezető
- Felsővezető
- Nincs aktív munkavállalói jogviszonyom
- Egyéb: ...

5. Milyen munkakörben dolgozik? (Opcionális)

II. A privátszférát erősítő technológiák (PET-ek) aktuális alkalmazása

A kitöltés folytatása előtt kérem olvassa el az alábbi rövid ismertetőt:

A privátszférát erősítő technológiákat (röviden: PET) összességében úgy határozhatjuk meg, hogy azok megerősítik az egyén magánéletének védelmét azáltal, hogy megakadályozzák a személyes adatok szükségtelen, nem kívánatos vagy jogellenes felhasználását, vagy olyan eszközöket és beavatkozási lehetőségeket kínálnak, amelyek növelik az egyén ellenőrzését személyes adatai felett.

1. Jelenleg használ egyénileg bármilyen privátszférát erősítő technológiát? (Kötelező)

- Igen
- Nem

2. "Igen" válasz esetén kérem írjon (néhány) példát. (Opcionális)

3. Tudomása szerint a munkáltatója által munkavégzésre biztosított eszközökön található privátszférát erősítő technológia? (Kötelező)

- Igen
- Nem

4. "Igen" válasz esetén kérem írjon (néhány) példát. (Opcionális)

III. A privátszférát erősítő technológiák (PET) alkalmazásának lehetőségei

A következő kérdések különböző alkalmazási, bevezetési scenáriókat, lehetőségeket tartalmaznak.

1. Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok használatát önállóan, autodidakta módon kellene elsajátítania? (Kötelező)

- 1: Egyáltalán nem használnék – 6: Minden bizonnyal használnék

2. Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok használatát a munkáltató munkaidőben, képzés / oktatás keretében mutatná be? (Kötelező)

- 1: Egyáltalán nem használnék – 6: Minden bizonnyal használnék

3. Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok esetleges anyagi vonzatát önerőből kellene finanszíroznia? (Kötelező)

- 1: Egyáltalán nem használnék – 6: Minden bizonnyal használnék

4. Milyen valószínűséggel alkalmazna PET-eket abban az esetben, ha azok esetleges anyagi vonzatát a munkáltató finanszírozná? (Kötelező)

- 1: Egyáltalán nem használnék – 6: Minden bizonnyal használnék

5. Szívesebben alkalmazna otthoni környezetben olyan PET-eket, melyeket munkahelyén is használ? (Kötelező)

- 1: Egyáltalán nem – 6: Minden bizonnyal

IV. Privátszféra és adatvédelem a mindennapokban

1. Érdeklődik / figyelemmel kíséri a különböző adatszivárgásokkal, adatvédelemmel kapcsolatos közéleti, politikai híreket, incidenseket, botrányokat? (Kötelező)

- 1: Egyetlen kapcsolódó hírt sem olvastam még – 6: Minden információt igyekszem megszerezni a témában

2. Kockázatosnak tartja az Önről - akár beleegyezésével - történő adatgyűjtést, adatkezelést? A profilalkotás lényege, hogy a rendelkezésre álló adatok alapján az egyén személyes jellemzői is meghatározhatók. (Kötelező)

- 1: Egyáltalán nem – 6: Minden bizonnyal

3. Kockázatosnak tartja az adatgyűjtést abban az esetben, ha azt profilozásra használják fel? (Kötelező)

- 1: Egyáltalán nem – 6: Minden bizonnyal

4. Fokozottabban ügyel adatai védelmére, amennyiben különböző adatvédelmi hiátusokat tapasztal? (Kötelező)

- 1: Egyáltalán nem – 6: Minden bizonnyal

5. Fokozottabban ügyel adatai védelmére, amennyiben tudomására jut, hogy azt 3. fél is kezelheti / 3. fél számára is értékesíthető? (Kötelező)

- 1: Egyáltalán nem – 6: Minden bizonnyal

6. Amennyiben anyagi vagy kényelmi szempontból kedvezőbb feltételekkel juthat hozzá bizonyos szolgáltatásokhoz, abban az esetben kevésbé ügyel adatainak teljes körű védelmére? Például különböző szolgáltatások kedvezményes, vagy teljesen ingyenes igénybevételekor. (Kötelező)

- 1: Nem veszek igénybe ilyen jellegű szolgáltatásokat – 6: Ilyen esetekben el tudok tekinteni a teljes körű adatvédelemtől

7. A hazai vagy nemzetközi, sajtóban is megjelenő adatszivárgásokat követően fokozottabban ügyel adatai védelmére? (Kötelező)

- 1: Egyáltalán nem – 6: Minden bizonnyal

8. A hazai vagy nemzetközi, sajtóban is megjelenő adatvédelemmel kapcsolatos botrányokat követően fokozottabban ügyel adatai védelmére? Például: Pegasus-botrány. (Kötelező)

- 1: Egyáltalán nem – 6: Minden bizonnyal

V. A privátszféra védelme és a munkahelyi biztonság kapcsolata

1. Ön munkahelyi környezetben fokozottabban ügyel adatainak védelmére? (Kötelező)

- 1: Egyáltalán nem – 6: Teljes mértékben

2. Ön szerint a munkavállalók saját privátszférájának nem megfelelő szintű védelme jelenthet kockázatot a szervezet biztonságára? (Kötelező)

- 1: Egyáltalán nem – 6: Teljes mértékben

3. Ön szerint támadási kísérlet esetén egy szervezet munkavállalói potenciális célpontként jelenhetnek meg a támadók számára? (Kötelező)

- 1: Egyáltalán nem – 6: Teljes mértékben

4. Amennyiben munkavégzése során hozzáférhetne szervezete védett rendszereihez, úgy fokozottabban ügyelne adatainak védelmére munkahelyi környezetben? (Kötelező)

- 1: Egyáltalán nem – 6: Teljes mértékben

5. Amennyiben munkavégzése során hozzáférhetne szervezete védett rendszereihez, úgy fokozottabban ügyelne adatainak védelmére otthoni környezetben is? (Kötelező)

- 1: Egyáltalán nem – 6: Teljes mértékben

3. számú melléklet: Az SPSS Statistics eredményei:

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi oktatás esetén? * Kényelmi szempontból nem ügyel az adatvédelemre	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi oktatás esetén? * Kényelmi szempontból nem ügyel az adatvédelemre

Crosstabulation

			Kényelmi szempontból nem ügyel az adatvédelemre		Total
			Igénybe vesz ilyen jellegű szolgáltatást	Nem vesz igénybe ilyen jellegű szolgáltatást	
Alkalmazna PET-eket munkahelyi oktatás esetén?	Nem alkalmazna	Count	10	30	40
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	25,0%	75,0%	100,0%
	Alkalmazna	Count	12	102	114
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	10,5%	89,5%	100,0%
Total	Count		22	132	154
	% within Alkalmazna PET-eket munkahelyi oktatás esetén?		14,3%	85,7%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5,066 ^a	1	,024		
Continuity Correction ^b	3,953	1	,047		
Likelihood Ratio	4,608	1	,032		
Fisher's Exact Test				,035	,027
Linear-by-Linear Association	5,033	1	,025		
N of Valid Cases	154				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,71.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,181	,024
	Cramer's V	,181	,024
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi oktatás esetén? * Hiátus esetén fokozottabban ügyel	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi oktatás esetén? * Hiátus esetén fokozottabban ügyel Crosstabulation

		Hiátus esetén fokozottabban ügyel		Total
		Nem	Igen	
Alkalmazna PET-eket munkahelyi oktatás esetén?	Nem alkalmazna	Count	14	26
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	35,0%	65,0%
	Alkalmazna	Count	21	93
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	18,4%	81,6%
Total	Count		35	119
	% within Alkalmazna PET-eket munkahelyi oktatás esetén?		22,7%	77,3%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4,634 ^a	1	,031		
Continuity Correction ^b	3,738	1	,053		
Likelihood Ratio	4,360	1	,037		
Fisher's Exact Test				,047	,029
Linear-by-Linear Association	4,604	1	,032		
N of Valid Cases	154				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 9,09.

b. Computed only for a 2x2 table

Symmetric Measures

	Value	Approximate Significance
Nominal by Nominal	Phi	,173
	Cramer's V	,173
N of Valid Cases	154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi oktatás esetén? * Harmadik fél hozzáférése esetén	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi oktatás esetén? * Harmadik fél hozzáférése esetén Crosstabulation

			Harmadik fél hozzáférése esetén		Total
			Nem ügyel	Fokozottan ügyel	
Alkalmazna PET-eket munkahelyi oktatás esetén?	Nem alkalmazna	Count	16	24	40
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	40,0%	60,0%	100,0%
	Alkalmazna	Count	24	90	114
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	21,1%	78,9%	100,0%
Total	Count		40	114	154
	% within Alkalmazna PET-eket munkahelyi oktatás esetén?		26,0%	74,0%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5,529 ^a	1	,019		
Continuity Correction ^b	4,587	1	,032		
Likelihood Ratio	5,236	1	,022		
Fisher's Exact Test				,023	,018
Linear-by-Linear Association	5,493	1	,019		
N of Valid Cases	154				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 10,39.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,189	,019
	Cramer's V	,189	,019
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Harmadik fél hozzájárása esetén	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Harmadik fél hozzájárása esetén Crosstabulation

			Harmadik fél hozzájárása esetén		Total
			Nem ügyel	Fokozottan ügyel	
Alkalmazna PET-eket munkahelyi finanszírozás esetén?	Nem alkalmazna	Count	16	18	34
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	47,1%	52,9%	100,0%
	Alkalmazna	Count	24	96	120
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	20,0%	80,0%	100,0%
Total	Count		40	114	154
	% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?		26,0%	74,0%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	10,089 ^a	1	,001		
Continuity Correction ^b	8,730	1	,003		
Likelihood Ratio	9,305	1	,002		
Fisher's Exact Test				,003	,002
Linear-by-Linear Association	10,023	1	,002		
N of Valid Cases	154				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 8,83.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,256	,001
	Cramer's V	,256	,001
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Hiátus esetén fokozottabban ügyel	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Hiátus esetén fokozottabban ügyel Crosstabulation

			Hiátus esetén fokozottabban ügyel		Total
			Nem	Igen	
Alkalmazna PET-eket munkahelyi finanszírozás esetén?	Nem alkalmazna	Count	14	20	34
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	41,2%	58,8%	100,0%
	Alkalmazna	Count	21	99	120
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	17,5%	82,5%	100,0%
Total	Count		35	119	154
	% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?		22,7%	77,3%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	8,457 ^a	1	,004		
Continuity Correction ^b	7,162	1	,007		
Likelihood Ratio	7,712	1	,005		
Fisher's Exact Test				,006	,005
Linear-by-Linear Association	8,402	1	,004		
N of Valid Cases	154				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 7,73.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,234	,004
	Cramer's V	,234	,004
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Kényelmi szempontból nem ügyel az adatvédelemre	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Kényelmi szempontból nem ügyel az adatvédelemre Crosstabulation

			Kényelmi szempontból nem ügyel az adatvédelemre		
			Igénybe vesz ilyen jellegű szolgáltatást	Nem vesz igénybe ilyen jellegű szolgáltatást	Total
Alkalmazna PET-eket munkahelyi finanszírozás esetén?	Nem alkalmazna	Count	10	24	34
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	29,4%	70,6%	100,0%
	Alkalmazna	Count	12	108	120
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	10,0%	90,0%	100,0%
Total		Count	22	132	154
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	14,3%	85,7%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	8,153 ^a	1	,004		
Continuity Correction ^b	6,645	1	,010		
Likelihood Ratio	7,102	1	,008		
Fisher's Exact Test				,010	,007
Linear-by-Linear Association	8,100	1	,004		
N of Valid Cases	154				

a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 4,86.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,230	,004
	Cramer's V	,230	,004
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Kockázatosnak tarja a profilozást?	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Kockázatosnak tarja a profilozást?

Crosstabulation

			Kockázatosnak tarja a profilozást?		Total
			nem	igen	
Alkalmazna PET-eket munkahelyi finanszírozás esetén?	Nem alkalmazna	Count	5	29	34
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	14,7%	85,3%	100,0%
	Alkalmazna	Count	17	103	120
		% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?	14,2%	85,8%	100,0%
Total	Count		22	132	154
	% within Alkalmazna PET-eket munkahelyi finanszírozás esetén?		14,3%	85,7%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,006 ^a	1	,937		
Continuity Correction ^b	,000	1	1,000		
Likelihood Ratio	,006	1	,937		
Fisher's Exact Test				1,000	,564
Linear-by-Linear Association	,006	1	,937		
N of Valid Cases	154				

a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 4,86.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,006	,937
	Cramer's V	,006	,937
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi oktatás esetén? * Kockázatosnak tarja a profilozást?	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi oktatás esetén? * Kockázatosnak tarja a profilozást? Crosstabulation

			Kockázatosnak tarja a profilozást?		Total
			nem	igen	
Alkalmazna PET-eket munkahelyi oktatás esetén?	Nem alkalmazna	Count	5	35	40
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	12,5%	87,5%	100,0%
	Alkalmazna	Count	17	97	114
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	14,9%	85,1%	100,0%
Total	Count		22	132	154
	% within Alkalmazna PET-eket munkahelyi oktatás esetén?		14,3%	85,7%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,141 ^a	1	,708		

Continuity Correction ^b	,013	1	,910		
Likelihood Ratio	,144	1	,704		
Fisher's Exact Test				,799	,468
Linear-by-Linear Association	,140	1	,708		
N of Valid Cases	154				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,71.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	-,030	,708
	Cramer's V	,030	,708
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi finanszírozás esetén? *	154	100,0%	0	0,0%	154	100,0%
Kockázatosnak tartja az Önről - akár beleegyezésével - történő adatgyűjtést, adatkezelést?						

Alkalmazna PET-eket munkahelyi finanszírozás esetén? * Kockázatosnak tartja az Önről - akár beleegyezésével - történő adatgyűjtést, adatkezelést? Crosstabulation

			Kockázatosnak tartja az Önről - akár beleegyezésével - történő adatgyűjtést, adatkezelést?		Total
			nem	igen	
Alkalmazna PET-eket munkahelyi finanszírozás esetén?	Nem alkalmazna	Count	9	25	34
		% within Alkalmazna PET- eket munkahelyi finanszírozás esetén?	26,5%	73,5%	100,0%
	Alkalmazna	Count	17	103	120
		% within Alkalmazna PET- eket munkahelyi finanszírozás esetén?	14,2%	85,8%	100,0%
Total	Count		26	128	154
	% within Alkalmazna PET- eket munkahelyi finanszírozás esetén?		16,9%	83,1%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	2,858 ^a	1	,091		
Continuity Correction ^b	2,049	1	,152		
Likelihood Ratio	2,627	1	,105		
Fisher's Exact Test				,118	,080
Linear-by-Linear Association	2,840	1	,092		
N of Valid Cases	154				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,74.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,136	,091
	Cramer's V	,136	,091
N of Valid Cases		154	

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Alkalmazna PET-eket munkahelyi oktatás esetén? * Kockázatosnak tartja az Önről - akár beleegyezésével - történő adatgyűjtést, adatkezelést?	154	100,0%	0	0,0%	154	100,0%

Alkalmazna PET-eket munkahelyi oktatás esetén? * Kockázatosnak tartja az Önről - akár beleegyezésével - történő adatgyűjtést, adatkezelést? Crosstabulation

		Kockázatosnak tartja az Önről - akár beleegyezésével - történő adatgyűjtést, adatkezelést?		Total
		nem	igen	
Alkalmazna PET-eket munkahelyi oktatás esetén?	Nem alkalmazna	Count	9	31
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	22,5%	77,5%
	Alkalmazna	Count	17	97
		% within Alkalmazna PET-eket munkahelyi oktatás esetén?	14,9%	85,1%
Total	Count		26	128
	% within Alkalmazna PET-eket munkahelyi oktatás esetén?		16,9%	83,1%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1,215 ^a	1	,270		
Continuity Correction ^b	,734	1	,391		
Likelihood Ratio	1,157	1	,282		
Fisher's Exact Test				,327	,194
Linear-by-Linear Association	1,207	1	,272		

N of Valid Cases	154				
------------------	-----	--	--	--	--

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 6,75.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,089	,270
	Cramer's V	,089	,270
N of Valid Cases		154	