SEMMELWEIS EGYETEM

DOKTORI ISKOLA

Ph.D. értekezések

3170.

PALICZ TAMÁS

Egyének és közösségek erőforrásainak szociológiai és mentálhigiénés megközelítése

című program

Programvezető: Dr. Pethesné Dávid Beáta, egyetemi tanár

Témavezető: Dr. Joó Tamás, egyetemi docens

Egészségügyi adatok biztonsága a kibertérben – zsarolóvírusok és felhasználói biztonságtudatosság

Doktori értekezés

Dr. Palicz Tamás Gyula

Semmelweis Egyetem
Mentális Egészségtudományok Doktori Iskola

Témavezető: Dr. Joó Tamás, Ph.D., egyetemi docens

Hivatalos bírálók: Dr. Bödör Csaba, MTA doktora, egyetemi tanár
Dr. Krasznay Csaba, PhD, egyetemi docens

Komplex vizsga szakmai bizottság:
Elnök: Dr. Szíjártó Attila, MTA doktora, egyetemi tanár
Tagok: Dr. Németh Orsolya, Ph.D., egyetemi docens
Dr. Bányász Péter, Ph.D., egyetemi docens

EDT tag: Dr. Domján Gyula, Ph.D., egyetemi docens

Budapest
2024

Tartalomjegyzék

Rövidítések jegyzéke, rövid magyarázattal 5
Ábrák jegyzéke 8
Táblázatok jegyzéke 9
Bevezetés 10
1. Probléma meghatározása 13
1.1. Fontosabb fogalmak az egészségügyi kiberbiztonság területén 13
1.2. Az egészségügy, mint kritikus infrastruktúra 16
1.3. Az egészségügyi rendszer digitális átalakulása 18
1.4. A digitális ökoszisztéma 22
1.5. Az egészségügyben keletkező adatokról 23
1.6. A biztonság jelentése a kibertérben 26
1.7. Biztonságtudatosság – az emberi tényező 27
1.8. Veszélyek és fenyegetések az egészségügy számára 30
1.9. A COVID hatása a kiberbiztonságra – középpontban az egészségügy 33
1.10. Új technológiák miatti kihívások 36
1.11. Összefoglalás 39
2. Célkitűzések, kutatási kérdések és hipotézisek 42
3. Módszertan 44
3.1. Dokumentumelemzés (M1) 45
3.2. Esetfeldolgozás struktúrált interjúval (M2) 47
3.3. Kérdőíves felmérés (M3) 48
3.4. Adatok másodlagos elemzése (M4) 56
4. Eredmények 58
4.1. A digitális egészségügyi ökoszisztéma 58
4.2. Biztonságos innovatív adathasználat 66
4.3. Zsarolóvírusok az egészségügyben 70
4.4. Lakossági biztonságtudatosság 76
5. Megbeszélés 87
5.1. Digitális egészségügyi ökoszisztéma 87
5.2. Biztonságos innovatív adathasznosítás 91
5.3 Zsarolóvírusok az egészségügyben 94
5.4. Lakossági biztonságtudatosság 98
6. Következtetések 101
6.1. A kutatás jelentősége és egyedisége 101

6.2. A kutatás limitációi 102
6.3. A kutatás gyakorlati hasznosíthatósága 104
7. Összefoglalás 107
8. Irodalomjegyzék 109
9. Saját publikációk jegyzéke 122
10. Köszönetnyilvánítás 128

Rövidítések jegyzéke, rövid magyarázattal

Rövidítés	Magyarázat
AD	Active Directory. Egy olyan Microsoft szolgáltatás, amely központi adatbázisból teszi lehetővé a felhasználói hitelesítést (autentikációt) és hozzáférés/jogosultságkezelést (autorizációt)
AMA	American Medical Association – Amerikai Orvosszövetség
BCM	Business Continuity Management - üzletmenet folytonosság menedzsment
BCP	Business Continuity Plan – üzletmenet folytonossági terv
BPR	Business Process Reengineering – üzleti folyamat újraszervezés
BSI	Bundesamt für Sicherheit in der Informationstechnik, Biztonsági és Információtechnikai Szövetségi Hivatal, Németország
BSR	bizalmasság, sértetlenség, rendelkezésre állás – az információbiztonság három olyan jellemzője, amelynek teljesülnie kell. (angol fordításból CIA: confidentiality, integrity, availability)
CDR	Call Detail Records – mobilkommunikációs hálózatokban a cellát azonosító adat
CIA	a BSR angol megfelelője (lásd fent), illetve az USA Hírszerzési Hivatala (Central Intelligence Agency)
CISA	Cybersecurity & Infrastructure Security Agency - Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség, Amerikai Egyesül Államok
DoH, HHS	Department of Health and Human Services – Egészségügyi és Humánszolgáltatási Minisztérium, Amerikai Egyesült Államok
DRP	Disaster Recovery Plan – katasztrófa helyreállítási terv
EESZT	Elektronikus Egészségügyi Szolgáltatási Tér, Magyarország

ENISA	European Union Agency for Cybersecurity – Európai Kiberbiztonsági Ügynökség
GDPR	General Data Protection Regulation - Általános Adatvédelmi Rendelet, Európai Unió
HIS	Health/Hospital Information System – egészségügyi/kórházi informatikai rendszer
ICT	Information and Communications Technology – információs és kommunikációs technológia
IHME	Institute for Health Metrics and Evaluation – Egészségügyi Mérési és Értékelési Intézet, Washington, USA
NBSZ	Nemzetbiztonsági Szakszolgálat, Magyarország
NHS	National Health Service – Nemzeti Egészségügyi Szolgálat, Egyesült Királyság
NKI	Nemzeti Kibervédelmi Intézet, a Nemzetbiztonsági Szakszolgálaton belül működik, Magyarország
OCR	Office for Civil Rights – Civil Jogok Irodája, az USA Egészségügyi Minisztériumának egysége, amely a betegadatokkal kapcsolatos visszaéléseket gyűjti (nem összekeverendő a jelenlegi kontextusban az Optical Character Recognition – optikai karakterfelismeréssel)
PCR	Polymerase Chain Reaction – polimeráz láncreakció
RaaS	Ransomware-as-a-Service: a zsarolóvírus támadást, és az azzal járó pénzügyi következményeket szolgáltatásként is igénybe lehet venni
RDP	Remote Desktop Protocol – távoli hozzáférési protokoll. Ez egy olyan Microsoft szolgáltatás, amely lehetővé teszi, hogy a felhasználó távolról bejelentkezzen egy számítógépre.
USA	United States of America – Amerikai Egyesült Államok

VPN	Virtual Private Network: virtuális magánhálózat. Olyan technológia, amely révén az interneten történő böngészés biztonságos lesz, illetve ez biztosítja, hogy hálózatokhoz is biztonságos kapcsolódjunk
WHO	World Health Organization – Egészségügyi Világszervezet
WoS	Web of Science, Clarivate kiadó kereshető publikácós adatbázisa
YLD	Years Lived with Disability – rokkantsággal élt évek

Ábrák jegyzéke

1. ábra: A kritikus infrastruktúra jellemzői (Bognár & Bonnyai, 2019) 17

2. ábra: A 2010-2019 között az USA-ban információbiztonsági incidenssel érintett egészségügyi szolgáltatók számának változása (saját szerkesztés) 31

3. ábra: Az Amerikai Kormány Egészségügyi és Humán Szolgáltatási Minisztériumában (HHS) működő Office for Civil Rights (OCR) adatai az egészségügyi intézményeket ért támadások számáról 2019. április – 2021. március között, a COVID-19 járvány indulását megelőzően és azt követően (saját szerkesztés) (Palicz, Bencsik, & Szócska, 2021).... 34

4. ábra: A Nemzeti Kibervédelmi Intézet (NKI) által észlelt események számának alakulása esemény- és intézménytípusonként 2020. január 1- 2020. december 31. között (Nemzeti Kibervédelmi Intézet adatai, saját szerkesztés) (Palicz, Bencsik, & Szócska, 2021) 34

5. ábra: Egészséges mellkas CT felvétel manipulálása mesterséges intelligenciával (Mirsky et al., 2019) 37

6. ábra: Kóros mellkas CT felvétel manipulálása mesterséges intelligenciával (Mirsky et al., 2019) 37

7. ábra: A digitális egészégügyi ökoszisztéma elemei (saját szerkesztés) (Szabo et al., 2021) 60

8. ábra: A “mozgási” (kék), illetve az “otthonmaradási” (zöld) indexek grafikus ábrázolása 2020. január – 2020. április között (COVID-19 járvány magyarországi első hullámának időszaka) (saját szerkesztés) 69

9. ábra: A kórházi és a patológiai rendszer logikai kapcsolatának vázlatos rajza (saját szerkesztés) (Palicz et al., 2021) 72

10. ábra: A Saunders-féle és a kutatás során megalkotott digitális ökoszisztéma modell megfeleltetése (saját szerkesztés) 88

Táblázatok jegyzéke

1. táblázat: Módszertani mátrix a doktori értekezésben használt módszertanok (M) és célkitűzések (C) összefüggéséről (saját szerkesztés) 44

2. táblázat: A dokumentumelemzés kapcsán használt főbb paraméterek összefoglaló táblázata (saját szerkesztés) 46

3. táblázat: A 2021-ben alkalmazott lakossági kérdőív és a válaszlehetőségek (saját szerkesztés) 51

4. táblázat: Digitális generációk születési idejének táblázata (saját szerkesztés) 54

5. táblázat: A 2021-es lakossági biztonságtudatossági országos felmérés szociodemográfiai és eszközhasználati válaszok száma és aránya (saját szerkesztés)... 78

6. táblázat: A 2021--es lakossági biztonságtudatossági országos felmérés szakmai kérdésekre adott válaszok száma és aránya (saját szerkesztés) 81

7. táblázat: „Nyers" kereszttábla, amely a 2021-as adatokkal a nem és az IT hírek olvasási gyakoriságának megoszlását mutatja be esetszámmal és gyakorisággal (saját szerkesztés) 83

8. táblázat: Khi négyzet próba eredményei a független változók (A-B-C) és a biztonságtudatossági szempontok (D) tekintetében – 2021-es adatok alapján (saját szerkesztés) 86

9. táblázat: A CDR alapú és GPS alapú mozgás aktivitási módszertanok összehasonlítása (saját szerkesztés (Szócska et al., 2021) alapján) 93

Bevezetés

A bevezetésben röviden szeretném leírni a témával és kutatással kapcsolatos személyes indíttatásomat.

Az orvosegyetem elvégzését követően klinikusként kezdtem dolgozni, azonban a kutatás, azon belül is a molekuláris biológiai és genetikai problémák foglalkoztattak. Fiatal klinikusként volt lehetőségem megtapasztalni, hogy mit is jelent olyan adatokkal dolgozni, amelyek az emberi létezés legalapvetőbb információit hordozzák, és mit is jelent az, ha az adatok jók, és abból helyes következtetést vonunk le, és ezzel járulunk hozzá egy betegség okának kiderítéséhez és a beteg gyógyításához. Az első tudományos közleményeim ezen a területen születtek, az akkor még gyerekcipőben járó polimeráz-láncreakció (PCR – Polymerase Chain Reaction) módszertan használatával genetikai polimorfizmus vizsgálatokat végeztünk különböző betegcsoportokban (Császár et al., 1997; Szalai et al., 1999; Szombathy et al., 1998). Ennek az időszaknak különlegessége volt, hogy még sem a GDPR, sem a kiberbiztonság még fogalom szintjén sem volt ismert. Viszont már a legérzékenyebb adatokkal, a betegek genetikai adatával lehetett dolgozni abban az időben is.

Azt is volt lehetőségem megtapasztalni, hogy mit jelent ennek az ellenkezője: vagyis, ha rosszak az adatok, és az milyen tévútra vezethet.

A klinikusi munkát követően az egészségügyi szervezetek és rendszerek szervezésével, fejlesztésével találkoztam. Vezetői munkám során az egyik legnagyobb kihívással 2010-et követően szembesültem, amikor az Európai Unió által társfinanszírozott projektek fejlesztését kellett előkészíteni, erről dönteni kellett, illetve a projekteket kellett nyomon követni és a sikeres végrehajtásukat támogatni. Ebben kiemelt helye volt az egészségügyi digitalizációs projekteknek, amely alapján akkor még csak sejteni lehetett, hogy ez lesz az a terület, amely adat és információvédelmi szempontból talán a legizgalmasabb lesz. Ennek oka részben az, hogy ezek az adatok közvetlenül az ember gyógyításával, az emberi élettel vannak összefüggésben, másrészt pedig az a tény, hogy az elmúlt több mint tíz évben mind Magyarországon, mind világszerte robbanásszerű fejlődés zajlott le. A fejlesztési területen, különösen a digitális egészségügy területén kapott impulzusok alapvetően befolyásolták a gyakorlatközpontú tudományos érdeklődésemet.

A fentiek mellett szintén meghatározó volt az, hogy az Egészségügyi Menedzserképző Központ nemzetközi együttműködéseinek is köszönhetően 2020 óta külső szakértője vagyok az Institute for Health Metrics and Evaluation (IHME) által vezetett együttműködésnek, amelyben szintén láttam és látom, hogy milyen jelentősége van az adatok minőségének. Ennek pedig az egyik alapvető feltétele az adatbiztonság. Több olyan publikációba is bekapcsolódhattam, amelyek a korábbi klinikusi érdeklődésemre épülnek, azonban inkább rendszerszintű elemzéseket tesznek lehetővé: elsősorban azért, mert jelentős nemzetközi együttműködés révén nagy mennyiségű adat elemzésére van lehetőség. Ezek az elemzések értelemszerűen az egészségügyi rendszerek szervezéséhez adnak megfelelő hátteret, alapot. Ezen munkák közül a legutóbbi publikációt emelem ki, amely kapcsolódik a korábbi klinikusi munkámhoz is és az egyik leggyakoribb vérképzőrendszeri eltéréssel, a vérszegénységgel foglalkozik (GBD 2021 Anaemia Collaborators, 2023).

A kutatás a vérszegénység (anaemia) globális terheit vizsgálta, bemutatva a prevalenciát, a betegséggel eltöltött évek számát (YLDs – Years Lived with Disability), és a vérszegénység mögött álló okok trendjeit 204 országban és területen 1990 és 2021 között. 2021-ben a vérszegénység globális prevalenciája minden korosztályban 24,3% volt, ami 1,92 milliárd esetet jelent, szemben a 1990-es 28,2%-os prevalenciával és 1,50 milliárd esettel. Nagy változások történtek a vérszegénység terheiben az életkor, nem és földrajzi helyzet alapján, különösen az 5 év alatti gyermekeket, a nőket, és a szubszaharai Afrikában és Dél-Ázsiában található országokat érintve. A fentiek miatt kimondható: a vérszegénység továbbra is jelentős globális egészségügyi kihívást jelent, állandó egyenlőtlenségekkel az életkor, nem és földrajzi hely szerint. Ezek és a mögöttes okok alapján célzott, helyi egészségügyi beavatkozásokra van lehetőség.

A fent vázolt, az egészségügyi adatokra és a digitális egészségügyre épülő érdeklődést befolyásolta az a környezeti tényező, hogy a világháló elterjedésével, a gyógyítást segítő eszközök hálózatba kapcsolódásával hirtelen minden sokkal kitettebb lett a külső környezeti, elsősorban a világháló veszélyeinek, függetlenül attól, hogy egy kódírással próbálkozó fiatalról, esetleg egy szervezett, vállalatszerűen működő bűnözői csoportról, vagy éppen a jelentős erőforrással rendelkező, államilag támogatott hackercsoportokról van-e szó.

Értelemszerűen adódott az a felismerés, hogy a XXI. században a gyógyítás szabadságának és lehetőségeinek, valamint a betegek biztonságának megőrzése érdekében foglalkozni kell a digitálisan keletkező adatok védelmével, ezzel segítve a beteget, az orvost és szakdolgozót illetve az egészségügyi intézményeket és rendszereket.

Mint volt klinikus, így köteleződtem el az egészségügyben keletkező, illetve az egészséggel kapcsolatba hozható adat és információvédelem területén, és lett az egészségügyi kiberbiztonság a kiemelt kutatási területem.

1. Probléma meghatározása

1.1. Fontosabb fogalmak az egészségügyi kiberbiztonság területén

A dolgozat érdemi tárgyalása előtt néhány, a területhez kapcsolódó fogalmat érdemes tisztázni, illetve szeretném leírni, hogy milyen kontextusban használtam ezeket.

Az egészségügyi rendszer fogalmát általában az egészségügyi szolgáltatásokat nyújtó intézmények, szervezetek és szakemberek összességének nevezik, beleértve a köz- és magántulajdonú egészségügyi szolgáltatókat, a kormányzati és nem kormányzati szervezeteket, valamint az egészségügyi oktatási intézményeket. Ezt a WHO (World Health Organization) 2000-ben adott meghatározása alapján használom (World Health Organization, 2000).

Egészségügyi digitalizáció és digitális transzformáció fogalmát egyaránt használom a dolgozatomban. Digitális transzformáció alatt az egészségügyi rendszer digitális átalakulását értjük, amelynek során a technológiai lehetőségeket és képességeket használjuk fel az egészségügyi rendszer javítása érdekében (pl. hozzáférés, eredményesség, hatékonyság), és amelynek végső célja a társadalmi változások támogatása, illetve a társadalmi hasznok növelése (Bloomberg, 2018). Az egészségügy digitális transzformációja kapcsán az adatok jelentőségre utal az az elnevezés, amelyben az adatvezérelt egészség („data driven health") fogalmat használják egyre kiterjedtebben. Ez alatt az adatok másodlagos (nem gyógyítás érdekében történő) felhasználását és ezekre épülő döntéseket értünk.

A kibertér, mint fogalom a múlt század 80-as éveinek „science fiction" irodalmában jelent meg. A kibertér szó a kibernetika és a tér szavak összeolvadásából alakult ki. Nem is hinnénk, hogy egy szépirodalmi mű az alapja a napjainkban olyan széles körben használt fogalomnak: William Gibson „Burning Chrome" (1982) című novellájában használta ezt a szót. A kezdeti szépirodalmi leírás egyre elterjedtebb lett, és később elsősorban a számítástechnikában és a hadtudományokban használták kiterjedten a fogalmat (Gémes, 2018). Ebből a szóból („cyberspace") számos más szó, illetve fogalom is ered. Pl. a kiberbiztonság értelemszerűen a kibertér biztonságát jelenti.

A „hacker" szót olyan személyre használjuk, aki számítógépes rendszerekben jogosulatlanul fér hozzá adatokhoz (a rendszer működését jellemző „machine data"- hoz vagy akár az alaptevékenységhez kapcsolódóan keletkező „business data"-hoz),

elektronikus információkhoz, vagy általában a rendszerekhez, ezáltal kontrollt, felügyeletet gyakorol a rendszer működése felett. Ezt a rendszerek „feltörésével" éri el, így a szónak szinonimája, kicsit kevésbé hétköznapi szóhasználatban a „cracker" is. A „hackerek" az informatikai ismeretek mellett gyakran használnak olyan, a személyt befolyásoló eszközöket, amelyek révén a felhasználóktól csalnak ki személyes, vagy hozzáférési, esetleg műszaki adatokat, ezáltal megkönnyítve a rendszerekbe történő bejutást. Ezt a jelenséget pszichológiai befolyásolásnak („social engineering", pszichológiai manipuláció) nevezi az információbiztonsági szakirodalom (Krasznay & Hámornik, 2018).

Fontos tisztázni azt is, hogy mi a különbség az adatvédelem, információbiztonság és a kiberbiztonság között, annak ellenére, hogy a köznapi beszédben, de gyakran még tudományos köznyelvben is egyenértékűen használjuk ezeket.

Az adatvédelem fogalma alatt – az elnevezésnek megfelelően - az adatok védelmét értjük, a véletlen vagy szándékos hozzáférés, változtatás, nyilvánosságra hozatal és törlés ellen. Napjainkban ennek biztosítására legfontosabb az a jogi eszköztár, amelyet a GDPR biztosít. Az információbiztonság fogalmával pedig az információs rendszerek biztonságát értjük, amelyek az adatokat tárolják és feldolgozzák. Ebbe beletartoznak a hagyományos, analóg (pl. papíron tárolt adatok és információk) és az elektronikus, digitális rendszerek (pl. digitális alkalmazásokban, adatbázisokban tárolt) is.

A kiberbiztonság fogalma alatt az interneten és más hálózatokon keresztül jelentkező biztonsági kihívásokat értjük, beleértve a kibertámadásokat, a vírusokat, a rosszindulatú kódokat és szoftvereket, az adathalászatot („phishing") és a zsarolóvírus támadásokat („ransomware"). A kiberbiztonság megjelenésének legfontosabb katalizátora a hálózatok, elsősorban az internet megjelenése volt (Antunes et al., 2021).

A doktori értekezésemben Magyarország Nemzeti Kiberbiztonsági Stratégiája (2013) című dokumentumban található értelmezést használom, leginkább mert ez a legszélesebb értelmű és polgári felhasználási céllal is jól értelmezhető definíciója mind a kibertérre, mind annak biztonságára vonatozóan: „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. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon

találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett." (Magyarország Kormánya, 2013).

Mint látjuk a kibertér alapvetően egy globális fogalom, amely sem szektoriális, sem országhatárokkal nem rendelkezik. Ezért önmagában az egészségügyi kibertér is nehezen lehatárolható, azonban ha az egészségüggyel kapcsolatban használjuk a kibertér fogalmát, akkor ezalatt kell értenünk az egészségügyi ellátórendszer teljes spektrumának elektronikus infokommunikációs támogatásához szükséges fizikai és virtuális környezetet, az abban keletkező, tárolt, feldolgozott és megsemmisített elsődleges (nyers) és feldolgozott adatokat és információkat, valamint minden ezekhez kapcsolódó tevékenységet, folyamatot és szereplőt.

Röviden összefoglalva: az adatvédelem foglalkozik az adatok védelmével, az információbiztonság foglalkozik az információk és információs rendszerek biztonságával, és a kiberbiztonság foglalkozik az interneten és más hálózatokon jelentkező biztonsági kihívásokkal.

A kritikus vagy létfontosságú infrastruktúra, mint fogalom az utóbbi időben került a középpontba. Ebben jelentős szerepet játszott az, hogy a COVID-19 pandémia, vagy éppen az orosz-ukrán háború alatt a mindennapjainkat is érintően tapasztaltuk meg, hogy vannak olyan infrastruktúrák vagy szolgáltatások, amelyek a XXI. századi modern társadalmak létezéséhez szükségesek, és ezek működésének károsodása vagy kiesése komoly társadalmi, politikai kockázatot jelent biztonsági vagy éppen politikai stabilitási szempontból. Az egészségügyi rendszerek, intézmények, szolgáltatások ilyen körbe tartoznak (Bognár & Bonnyai, 2019). Ezt a fogalmat a dolgozat jelentősége miatt, külön fejezetben (1.2) tárgyalom.

Végül néhány olyan fogalom, kifejezés, amely a dolgozatban gyakrabban előfordul, és közvetlenül a kiberbiztonság szűkebb tématerületéhez tartozik.

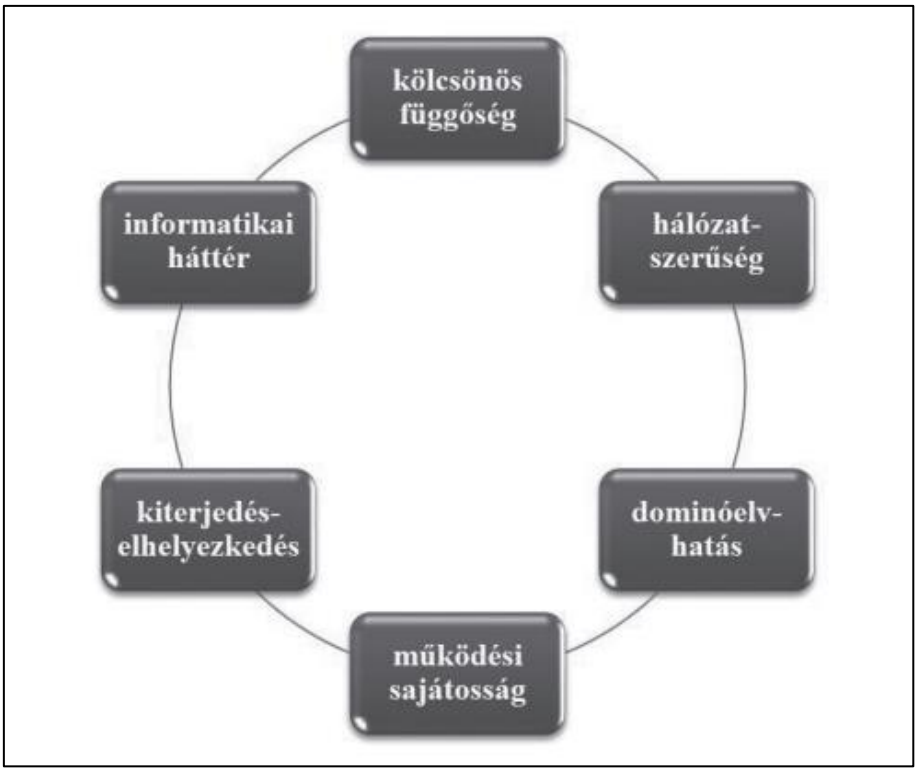
Zsarolóvírusnak nevezzük („ransomware") azokat a rosszindulatú kódokat (digitális vírusok), amelyek akadályozzák az adatokhoz történő hozzáférést, és csak akkor teszik elérhetővé azokat, ha a támadók kérésének eleget tesznek. Általában digitális pénzt, kriptovalutát kell fizetni a feloldó kulcsért. Az adathalászat („phishing") egy olyan csalási forma, amelynek során az kiszemelt áldozattól megszerzik a személyes adataikat,

jelszavakat, hozzáféréseket, és ezek segítségével járnak el az áldozat nevében. Végül érdemes még megemlíteni a kifejezetten egészségügy specifikus kifejezést, amely elsősorban a közeljövő legnagyobb kihívását jelenti az egészségügyi kiberbiztonság területén. Ez az Internet of Medical Things (orvosi dolgok internete), amely a dolgok internetéből (Internet of Things) jött létre, és azokat a hálózatba kapcsolható eszközök összességét jelenti, amelyek valamilyen módon az egészségünkhöz, jól-létünkhöz kapcsolódóan automatikus adattovábbításra és feldolgozásra képesek, ezzel segítve egy-egy orvosi vagy életmóddal kapcsolatos döntést. Leegyszerűsítve ez a hálózatba kötött orvosi eszközöket („medical device") jelenti.

1.2. Az egészségügy, mint kritikus infrastruktúra

A szakirodalom és a hazai jogszabályi környezet alapján az egészségügyi intézmények az ún. kritikus infrastruktúrák közé tartoznak (a kritikus vagy létfontosságú infrastruktúra fogalmát az 1.1 alfejezetben említettem). Definíció szerint: „kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére" (Bognár & Bonnyai, 2019).

A fentiek szerint azokat a létesítményeket, szolgáltatásokat, információs rendszereket és azok alkotóelemeit foglalja magában, amelyek nélkülözhetetlenek az alapvető szolgáltatások folyamatos fenntartásához és a társadalmi feladatok ellátásához. Ezen infrastruktúrák elemei sok esetben hálózatokba szerveződnek és ebben a hálózatban működnek. Tipikus példa erre a közlekedési vagy éppen a villamos hálózatok rendszere (Szócska et al., 2019). Ezek meghibásodása, működésük zavara vagy korlátozása, illetve teljes megszűnése jelentős károkat okozhat az adott terület működésében és a lakosság ellátásában, különösen akkor, ha a probléma nagyobb területi vagy időbeli kiterjedésű. A kritikus infrastruktúra jellemzőit a 1. ábra mutatja be.



1. ábra: A kritikus infrastruktúra jellemzői (Bognár & Bonnyai, 2019)

Az, hogy egy egészségügyi ellátást végző intézmény, a lakosság egészségi állapota szempontjából kulcs vagy kritikus fontosságú, könnyen belátható. Képzeljünk el egy olyan helyzetet, amikor egy beteget beutalnak egy nagyobb, például megyei kórház sürgősségi osztályára, és az érkezésekor kiderül, hogy az alapvető diagnosztikai vizsgálatok, mint például a laborvizsgálatok vagy a képalkotó eljárások, nem végezhetők el. Emiatt a beteg ellátása ellehetetlenül. Az egység működése egy korábbi informatikai rendszerhiba következtében áll le, mivel egy behatolás vagy kibertámadás során az adatokhoz való hozzáférést zárolták vagy titkosították. A létfontosságú fájlok és információk hiánya megbénítja a diagnosztikai és terápiás döntéseket, ellehetetlenítve a sürgősségi ellátást, illetve ezen keresztül az egész kórház, vagy akár egy egész megye betegellátását.

Hasonló esetek a valóságban is előfordultak. Egy példa erre a 2019 szeptemberében az Egyesült Államok középső részén található Campbell County Health egészségügyi központban történt incidens, amely 20 kórházat érintett. A támadás következtében a kórházak kénytelenek voltak a betegeket egy körülbelül 100 kilométerre lévő másik egészségügyi intézménybe irányítani, mivel számos diagnosztikai eljárás, különösen a

laboratóriumi szolgáltatások, nem működtek. Az adatvisszaállítás és a kórházak működésének teljes helyreállítása 17 napot vett igénybe. Az eset hátterében egy zsarolóvírus-támadás állt, amely súlyosan megzavarta az intézmények működését (Janofsky, 2019).

Említésre méltó még az a 2020 őszén Németországban történt egyetemi klinikai sürgősségi központban bekövetkezett zsarolóvírus támadás, amely miatt a betegeket nem tudták fogadni, a működés leállt, és a sürgős ellátást igénylő beteget egy kb. 40 km-re levő város hasonló ellátást nyújtó intézményébe kellett irányítani. A beteg szállítás közben meghalt, ami miatt a német hatóságok ismeretlen tettes ellen feljelentést tettek. Ez volt az első ilyen nyilvánosságra került eset, ahol a zsarolóvírus támadás, a működési probléma és a tartós egészségkárosodás között ok-okozati összefüggést vélelmeztek (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020).

A kritikus infrastruktúrák védelmét a legmagasabb szintű technológiai képességekkel ma már tudják védeni (pl. mesterséges intelligencia eszközök), azonban az emberi tényező és befolyásolhatóság („social engineering") még mindig meghatározó és fontos (Fausto et al., 2021). A fentiek miatt ezen infrastruktúrák esetében, különösen az információbiztonság területén speciális képzések szükségesek (Palicz & Joó, 2020)

1.3. Az egészségügyi rendszer digitális átalakulása

Az egészségügy az egyik olyan ágazat, amelynek digitalizációja és digitális transzformációja az elmúlt évtizedekben, de különösen az elmúlt években jelentősen előre tört. Manapság szinte minden, az egészségügyben használt eszköz digitálisan működik, és ennek következtében jelentős mennyiségű, könnyen tárolható és feldolgozható adat keletkezik (Frisinger & Papachristou, 2024).

Ma már olyan hagyományos orvosi tevékenység, mint pl. a hallgatózás („auscultatio") kiváltására is fejlesztések történnek. A fonendoszkóp és az emberi fül szerepét egyre inkább átveszi az orvos zsebében levő okostelefon, illetve az abba beépített mikrofon és kamera, valamint a háttérben futó mesterséges intelligencia alkalmazások (Diaz, 2022). Ezek a változások gyökeresen átalakítják nemcsak a hagyományos orvosi/egészségügyi dolgozói feladatokat, hanem az egészségügyi ellátó rendszerre is diszruptívan hatnak.

A digitális transzformáció az orvoslás szinte valamennyi területét érinti. Érdemes kiemelni azt, hogy ez megjelenik a diagnosztikus folyamatok képalkotó eljárásaitól a laboratóriumi medicinán keresztül a terápiás területekig, vagy éppen a klinikai gyógyszerfejlesztési és vizsgálati folyamatokat is nagymértékben tudja támogatni (Inan et al., 2020; Mitchell & Kan, 2019). Az egészségügy átalakulása olyan konvencionális területeket is érint, mint az emberi magatartással foglalkozó tudományterületek, vagyis a mentális egészségügy vagy éppen a pszichiátria (Bucci et al., 2019; Roth et al., 2021).
A digitalizáció során keletkező adatok mennyisége (erről a következő fejezetekben is lesz bővebben szó) teremti meg – más tényezők mellett – az alapját a mesterséges intelligencia széles körű elterjedésének az egészségügyben. Az ember-gép együttműködése rendszerszinten is hozzájárulhat az egészségügyben a hozzáférhetőség, a minőség, betegbiztonság, hatékonyság és eredményesség javításához (Chen & Decary, 2020). Külön ki kell emelni, hogy a mesterséges intelligencia biztonságos használatának talán az egyik legfontosabb feltétele, hogy olyan hiteles adatokból felépülő adatbázisok keletkezzenek, amelyek képesek biztosítani az adatok bizalmasságát, sértetlenségét és rendelkezésre állását (magyar szavak kezdőbetűiből BSR, az angol mozaikszó, amelyet az információbiztonság területén is használnak CIA az alábbi elnevezésekből adódik: confidentiality, integrity és accessibility) (Ellahham et al., 2020). Ezek jelentőségéről a későbbiekben részeletesen fogok szólni.

Az egészségügy digitális átalakulásának sikere szempontjából kritikus fontosságú a szereplők megfelelő kommunikációja és együttműködése. Az üzleti életben számos területen definiálták a digitális üzleti ökoszisztéma fogalmát, amely alatt azt a kollaboratív környezetet értik, amelyben a szereplők kölcsönös függőségen alapuló, de mégis együttműködő tevékenysége teremt értéket, és ebben a digitális környezet (szemben az egyszerű üzleti ökoszisztémával) kiemelt szerepet játszik (Senyo et al., 2019).
Ennek az átalakulásnak fontos eredménye lesz, hogy az ellátórendszerrel kapcsolatos eddigi elképzeléseink átalakulnak, a hagyományos ellátórendszeri struktúra felbomlik és egyre inkább új digitális ellátási modellek mentén fog szerveződni az egészségügy. Erre már több területen is vannak kezdeményezések, részint betegség alapon (pl. diabetes

mellitus) (Ellahham, 2020; Nomura et al., 2021) vagy éppen egy-egy orvosi szakterület kapcsán (pl.: szemészeti ellátások) (Tham et al., 2022).

Ennek fontos feltétele, hogy az ökoszisztéma minél pontosabban leírásra kerüljön, az elemek, a folyamatok és a betegek, illetve társadalom számára értéket teremtő képességek meghatározása mellett történjen meg a szereplők érdekeinek azonosítása, vagy éppen az az együttműködések alapja is kerüljön meghatározásra.

Ugyanilyen kulcsfontosságú, hogy az ember-gép kapcsolat mind a betegek, mind a benne dolgozók viszonylatában meghatározásra kerüljön, illetve ezeket finoman hangoljuk, hogy az ellátószemélyzet-betegek/ügyfelek és a technológia megfelelő kapcsolata épüljön ki. Ebben kulcsfontosságú, hogy megfelelő ismeretekkel és képességekkel rendelkezzenek a rendszer szereplői, amelyek a digitális környezet miatt újfajta tudást és készségek fejlesztését jelenti. Ennek egyik fontos komponense a kiberbiztonsági ismeretek és képességek fejlesztése, amelyhez a szereplők alapvető ismereteinek és attitűdjeinek megismerése szükséges (Vuorikari et al., 2016).

A digitalizációs átalakulással foglalkozó irodalmak és koncepciók kiemelik, hogy az emberi tényező milyen fontos a digitalizáció adta lehetőségek kihasználása kapcsán (Nadkarni & Prügl, 2021). Ez az emberi tényező azonban nemcsak lehetőségeket hordoz magában, hanem sajnos olyan veszélyekkel és kockázatokkal is jár, amely csökkenti a biztonságot és bizonyos helyzetekben akár veszélyt is jelent a digitalizáció által hordozott biztonsági kockázatok fel nem ismerése. A fejlett technológiai képességek ellenére az emberi tényező még mindig 39%-ban szerepel a biztonsági kockázatok között, és a sikeres kibertámadások 95%-ban valamilyen emberi hiba ismerhető fel, leginkább biztonságtudatossági problémák (Alsharif et al., 2021).

A digitalizációs folyamatok kapcsán figyelembe kell venni azt a tényt, hogy az elmúlt években zajló COVID-19 pandémia, és annak járványhullámaihoz kapcsolódó távolságtartási kényszerintézkedések sok esetben felgyorsították – más szektorokhoz hasonlóan - az egészségügyön belüli digitalizációs lépéseket is. Így volt ez Magyarországon is, ahol a 2020-as első és második hullámban számos olyan, elsősorban a telemedicina lehetőségeit kihasználó intézkedés történt, amelyek szó szerint kikényszerítették a rendszer, a benne dolgozók és a betegek részéről is a rendelkezésre álló technológiai lehetőségek használatát és mindennapi gyakorlattá tételét (Győrffy et al., 2020).

Az elmúlt időszak változásai következtében az egészségügyi ellátórendszerek fenntarthatósága veszélybe került, számos új kihívás is megjelent, és a komplex problémákra (Szócska et al., 2005) a digitalizáció segíthet megoldást találni.

Az egészségügyi és kapcsolódó szociális ellátórendszerek radikális újraszervezésére van szükség, amelyben a digitális technológiák az eredményesebb, hatékonyabb, és jobb egészség-kimenetek biztosításával tudnak hozzájárulni a kihívások leküzdéséhez. Ilyen jellegű lokális, radikális folyamat–újraszervezésre (BPR, Business Process Reengineering) saját munkám során is voltak kezdeményezések (Palicz et al., 2003), ugyanakkor az egészségügy sok évvel le van maradva más szektorokhoz viszonyítva az információs technológiák bevezetése és kiterjedt használata tekintetében.

Az Európai Unión belül az egészségpolitikai és ehhez kapcsolódóan az egészségügyi fejlesztések tagállami hatáskörbe tartoznak, amely miatt a tagállamok önállóan, és aktívan építették ki a nemzeti alapú e-egészségügyet. Azt ki kell emelni, hogy a digitális egészégügyi fejlesztések túlmutatnak az eszközök és technológiák beszerzésén vagy fejlesztésén. Az e-egészségügy kialakítása kapcsán olyan átfogó fejlesztésekre van szükség, amelyek során át kell alakítani a szervezeti folyamatokat, struktúrákat és szerepeket, figyelembe véve a változó jogszabályi környezetet. Emellett kiemelt jelentősége van az emberi tényezőnek, vagyis a betegek és az egészségügyi dolgozók igényeinek és képességeinek, amelyekhez megfelelő továbbképzésekkel és humán erőforrás fejlesztéssel kell igazodni.

Fontos kiemelni, hogy a WHO a digitalizációt olyan lehetőségnek tekinti, amely segít az általános egészségbiztosítás kiterjesztésének és fenntarthatóságának biztosításához (World Health Organization, 2019)

A WHO 2020-ban elfogadott és közzétett digitális egészségügyi stratégiája mérföldkőnek számít, hiszen hosszú távú célokat és részletes cselekvési tervet határoz meg ezen a területen (World Health Organization, 2020). A digitalizáció kapcsán a WHO is felismerte, hogy a kiberbiztonság milyen jelentőséggel bír. Ezt mutatja a WHO felsővezetésének 2022 október végi szakértői anyaga: az ágazaton belüli digitalizáció előretörésével a biztonság érdekében erőfeszítéseket kell tenni, és ennek érdekében koordinált cselekvésre van szükség (CEB United Nation System, 2022).

Az Európai Bizottság 2004-ben jelentette meg az első e-egészségügyi cselekvési tervet, amelyet 2012-ben újított meg (Európai Bizottság, 2012). Ebben meghatározták azokat a

kereteket is, amelyek biztosítják a Bizottság és a tagállamok számára a koordinált szakpolitikai fellépést. A magyar elnökség idején, 2011-ben tartotta első ülését az e-egészségügyi munkacsoport („EU Task Force on eHealth”), amelynek feladatai közé tartozott, hogy megvizsgálja és ajánlásokat fogalmazzon meg annak érdekében, hogy Európa 2020-ra minél nagyobb mértékben kihasználja az e-egészségügy lehetőségeit (European Comission, 2012). Az Európai Bizottság rámutatott, hogy az egészségügyi rendszerek reformjának egyik kulcsfontosságú eleme a digitális technológiák széles körű bevezetése és alkalmazása (Európai Bizottság, 2014).

1.4. A digitális ökoszisztéma

Úgy tűnik, hogy a "digitális ökoszisztéma" kifejezés eredetének vagy a kifejezés részletes történeti hátterének megtalálása a rendelkezésre álló tudományos irodalomban meglehetősen kihívást jelent, és nincsenek közvetlen hivatkozások, amelyek kifejezetten tárgyalnák a kifejezés kezdetét vagy evolúcióját.

Azonban valószínű, hogy a "digitális ökoszisztéma" kifejezés a "vállalati ökoszisztéma" szélesebb koncepciójából fejlődött ki, amelyet James F. Moore alkotott meg 1993-ban és publikált a Harvard Business Review-ban. Moore alapvetően a verseny szempontjából értelmezte és elemezte az ökoszisztémát, azonban a biológiai rendszerekhez hasonlóan itt a kapcsolódás és egymásra utaltság is nagy jelentőségű. Az ökoszisztéma jelenti a digitális környezettel és egymással összekapcsolt különböző entitásokat, mint például vállalkozások, fogyasztók és technológiák, amelyek nemcsak kapcsolódnak, hanem interakcióba is lépnek egymással (James F. Moore, 1993).

A "digitális ökoszisztéma" kifejezés egy integrált és összekapcsolt hálózatot jelöl, amely vállalatokat, embereket, folyamatokat és technológiákat foglal magában, és együttműködnek egymással egy közös cél vagy érték létrehozása érdekében. A digitális ökoszisztéma szemlélete lehetővé teszi a résztvevők számára, hogy rugalmasan és hatékonyan alkalmazkodjanak a piaci változásokhoz, elősegítsék az innovációt, és értéket nyújtsanak a felhasználóknak vagy ügyfeleknek. Ebben az ökoszisztémában az adatok és információk szabadon áramlanak a rendszeren belül, lehetővé téve a résztvevők számára, hogy informált döntéseket hozzanak, és jobban alkalmazkodjanak az új kihívásokhoz és lehetőségekhez.

A digitális technológiákat a szervezetek külső tényezőjeként tartják számon, amelyek erősítik a különböző ökoszisztéma-szereplők közötti kapcsolatokat, és megváltoztatják azok interakciójának természetét. Egy tanulmány (Zhang et al., 2023) 2001 és 2018 közötti adatokat dolgozott fel 101 országból a digitális technológia vállalkozásra gyakorolt hatásának elemzésére. Az eredmények pozitív összefüggést mutattak a digitális technológia szintje és a nemzeti vállalkozói ökoszisztémák kimenetele között, különösen a támogató kultúrájú, magas minőségű intézményekkel és jól fejlett szolgáltatási iparágakkal rendelkező országokban.

Az egészségügy esetén nem egyértelmű, hogy pontosan mit is értünk digitális egészségügyi ökoszisztéma alatt. Egy 2021-ben megjelent tanulmány (Benis et al., 2021) két koncepcionális keretet javasol a digitális egészségügyi ökoszisztémák megértéséhez: az Egy Egészség (One Health) és a digitális egészség. Három perspektívát vesznek figyelembe: az egyéni egészséget és jólétet, a népességet és a társadalmat, valamint az ökoszisztémát. Az öt dimenzió a következőket foglalja magában: polgárok elkötelezettsége, oktatás, környezet, emberi és állatorvosi egészségügy, valamint az Egészségügyi Ipar 4.0.

A „One Digital Health" célja, hogy digitálisan átalakítsa a jövő egészségügyi ökoszisztémáit, egy olyan rendszerszintű egészségügyi és élettudományi megközelítés alkalmazásával, amely széles körű digitális technológiai nézőpontokat vesz figyelembe az emberi egészség, az állategészség és a környezet kezelése tekintetében. Ez a megközelítés lehetővé teszi, hogy megvizsgáljuk, hogyan tudják a jövő egészségügyi informatikusai kezelni az új egészségügyi és ellátási forgatókönyvek belső összetettségét a digitálisan átalakított egészségügyi ökoszisztémákban. A tanulmány szerint a digitális egészségügyi műveltség, a digitális képességek a megelőzési és egészségmegőrzési tevékenységek megértésére és azokban való részvételre, az öngondoskodás, és az együttműködés a megelőzésben, ellenőrzésben és a lehetséges problémák enyhítésében szükségesek a rendszerszintű, ökoszisztéma-vezérelt közegészségügyi és adattudományi kutatásban.

1.5. Az egészségügyben keletkező adatokról

Az egészségügy digitális transzformációja kapcsán fontos kiemelni, hogy az egyébként is adatgazdag egészségügyben milyen mértékben növekedett meg az adatok mennyisége.

Elég csak arra gondolni, hogy pl. egy egyén teljes életútja kapcsán milyen sokféle szakterületen és modalitásban keletkezik adat az egészségügyi rendszerben.

Az egészségügyi adatok definiálását az 1997-es egészségügyi törvény tette meg. Ez pontosan meghatározta, hogy hogyan keletkeznek az egészségügyi adatok, ki tárolhatja, dolgozhatja fel azokat, és milyen céllal (Magyar Országgyűlés, 1997). Ennek 2013-2015 közötti aktualizálása már az Elektronikus Egészségügyi Szolgáltatási Tér fogalmát is bevezette, illetve ezzel kapcsolatosan meghatározta a digitálisan keletkező egészségi adatok útját és központi kezelését is. Az egészségügyi adatok nemzeti felhő infrastruktúrában történő tárolását az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) 2017. november 1-i elindítása biztosította (Németh, 2019). Ugyanezen jogszabály 2020-as és 2021-es kiegészítése – reagálva a COVID-19 járvány teremtette helyzetre – biztosította azt, hogy az EESZT-n kívüli adatkommunikáció is megvalósuljon, illetve járványügyi célból speciális regiszter készüljön meghatározott adattartalommal. A jogszabály ilyen rugalmas kezelése biztosíthatja azt, hogy a későbbiekben a különböző forrásból származó adatok is felhasználhatók legyenek a közjó érdekében (Magyar Országgyűlés, 1997).

Az egészségügyi adatokhoz kapcsolódóan jelen doktori értekezés tekintetében fontos a 2013-as információbiztonsági törvény is, amely az „adat" kapcsán az alábbi meghatározást adta: „Az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas, számos megjelenési formát vehet fel (például: alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása" (Magyar Országgyűlés, 2013).

Az egészségügyi informatikai rendszerekben (HIS – Health/Hospital Information System) tárolt adatok rendkívül érzékenyek, hiszen ezekben a páciensek teljes egészségügyi anamnézise, diagnózisa és kezelése megtalálható. Ezért az adatvédelemnek kiemelt szerepe van az egészségügyi intézményekben (Ködmön & Csajbók, 2015). Az Európai Unió által bevezetett Általános Adatvédelmi Rendelet (General Data Protection Regulation, GDPR) 2018. május 25-től Magyarországon is szabályozza a magánszemélyek adatainak védelmét. Személyes adatnak tekinthető minden olyan információ, amely egy személyt azonosíthatóvá tesz (közvetlenül vagy közvetve), például személynév, lakcím vagy elektronikus levelezési cím. Ebbe a kategóriába tartoznak azok

a vélemények és értékelések is, amelyek alapján egy adott személy felismerhető. A különleges személyes adatok közé sorolják az egészségügyi információkat, mint a kórelőzmények, zárójelentések, gyógyszerhasználati és kezelési adatok, illetve a káros szenvedélyekkel kapcsolatos információk, valamint a biometrikus adatokat, például a faji vagy etnikai hovatartozásra és a szexuális irányultságra vonatkozó adatokat. Ezeket az adatokat jellemzően az egészségügyi szolgáltatók nagy számban és általában helyben kezelik, ami kiemelt figyelmet érdemel adat- és információbiztonsági szempontból (Kim, 2020). Az ilyen módon tárolt adatok annyira egyediek az adott személyre nézve, hogy azok alapján pontosan azonosíthatóvá válik (különösen biometrikus vagy genetikai adatok esetében) (Mason et al., 2020), illetve az adatok elemzésével a várható megbetegedések is jósolhatók (prognosztikus, prediktív értékek és tulajdonságok) (Frey, 2018). Ezért különösen fontos, hogy a genetikai adatok esetében (pl. egy terhességi genetikai teszt kapcsán is) kiemelt figyelem legyen az adat- és információbiztonságon (Tobias et al., 2022)

Magyarország egészségügyi adatállománya hatalmas, melynek jelentős része még mindig papíralapú. Azonban az utóbbi években jelentős előre lépések történtek az adatok elektronikus tárolása és feldolgozása terén. Itt érdemes újra kiemelni az EESZT fejlesztését, amely 2011-ben indult, majd 2017 őszén került bevezetésre az országos rendszer. Ez már jelenleg is lehetőséget biztosít az online, valós idejű betegadat-továbbításra, tárolásra, valamint az adatok hozzáférésének jogosultságok szerinti biztosítására, és ezek alapján a másodlagos adathasznosításra (Németh, 2019).

Az egészségügyi dolgozók kulcsszerepet játszanak az egészségügyi adatok keletkezésének, tárolásának és feldolgozásának folyamatában, és jelentős felelősséggel bírnak ezen adatok biztonságáért. Az információbiztonság szempontjából azonban az egyes munkakörök és munkaköri csoportok feladatai és felelősségi körei eltérőek.

A technológiai fejlődés gyorsasága elképesztő mértékű, szinte naponta jelennek meg új megoldások, amelyeket nem tudnak követni az emberek. Ezért rendszer, csoportos és egyéni szinten kell olyan kockázatazonosító és kezelő mechanizmusokat kidolgozni, amellyel azok a csoportok azonosíthatók, ahol csoportos vagy egyéni beavatkozás révén lehetőség van ezek menedzselésére.

1.6. A biztonság jelentése a kibertérben

A biztonság az egyének, közösségek és a társadalom egésze szempontjából egy alapvető szükségletként van jelen. Elegendő, ha Maslow piramisára gondolunk: a biztonság olyan, a fiziológiai szükségletek szintje feletti közvetlen alapvető tényező, amely szükséges ahhoz, hogy a magasabb szintű szükségletek (társas, megbecsülés, önmegvalósítás) is megvalósuljanak (Bakacsi, 2015).

A biztonság olyan állapotként határozható meg, amely az érintettek számára megfelelő védelmet nyújt, biztosítva a zárt, átfogó, folyamatos és a kockázatokkal arányos intézkedések érvényesülését. A biztonságérzet együtt jár a fenyegetés és a fenyegetettség érzésének azonosításával, ezek kockázatának meghatározásával, valamint a megelőzési, védekezési és helyreállítási képességekkel (Beaman et al., 2021). A biztonság több szempontból értelmezhető (pl. politikai, társadalmi, gazdasági, szociális vagy éppen egészségbiztonság), és ez az utóbbi időben egyre komplexebbé vált. Gondoljunk csak arra, hogy az elmúlt század során hogyan változott a közlekedésbiztonság vagy éppen egészségbiztonság fogalma, vagy éppen az értekezés tárgyát képező információbiztonság területe.

Hétköznapi értelemben gyakran egyenértékűen használjuk, azonban mégis fontos elkülöníteni az informatikai és az információbiztonságot. Míg az előbbi esetben elsősorban a számítógépek biztonságát értjük (esetleg hálózati biztonságot is), addig az információs rendszerek esetében „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság szintén ide tartozhatnak” (Szádeczky & Szőke, 2018). Értelemszerűen idetartoznak akár a papíralapú, vagy éppen hangalapú adat és információhordozók is. Az elektronikus információbiztonság egy olyan speciális terület, amely az elektronikus információs rendszerekben tárolt és kezelt adatok bizalmasságának, sértetlenségének és hozzáférhetőségének védelmét foglalja magában, biztosítva a zárt, átfogó, folyamatos és a kockázatokkal arányos védelmi intézkedéseket.

A kiberbiztonság komplex értelmezését az Amerikai Egyesül Államok Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökségének (CISA) definíciója adja meg: „azt a komplex védelmi tevékenységet értjük alatta, amely során biztosítjuk a hálózatok, eszközök és adatok védelmét a jogosulatlan hozzáféréssel vagy bűnözéssel szemben, valamint az

információk titkosságát, integritását és elérhetőségét is" (Cybersecurity and Infrastructure Security Agency (CISA), 2021).

1.7. Biztonságtudatosság – az emberi tényező

A biztonságtudatosság a kibertérben egy olyan állapot, amelyben az egyének és szervezetek tisztában vannak a kiberbiztonsági fenyegetésekkel, kockázatokkal és azokkal a legjobb gyakorlatokkal és stratégiákkal, amelyek segítségével megvédhetik magukat és az információkat az online térben. A biztonságtudatosság magában foglalja az alapvető kiberbiztonsági ismereteket, például a jelszókezelést, a kéretlen e-mailek felismerését, a biztonságos webböngészési szokásokat, az adatvédelmi elvek ismeretét, vagy néhány alapvető, az aktuális trendeknek megfelelő fogalom (jelenleg pl. zsarolóvírus) ismeretét (Daengsi et al., 2022). Emellett a biztonságtudatosság azt is jelenti, hogy az egyének és szervezetek képesek felismerni és reagálni a kiberbiztonsági incidensekre, valamint ismerik és követik a szervezet kiberbiztonsági irányelveit és eljárásait (Husák et al., 2020). A biztonságtudatosság nem csak technikai ismereteket és készségeket jelent, hanem egy proaktív hozzáállást is a kiberbiztonsági kockázatok kezelésére, az állandó tanulást és alkalmazkodást az új fenyegetésekhez és kihívásokhoz. A biztonságtudatosság több elemet is magában foglal:

- Kiberbiztonsági fenyegetettség érzés: ahhoz, hogy megfelelő érzékenységgel álljon az egyén a kiberbizonsági veszélyekhez, a biztonságérzet fenyegetettségét kell éreznie (lásd az 1.6 alfejezetben kifejtetteket)
- Kiberbiztonsági tájékozottság és ismeretek: A személynek tájékozottnak kell lennie, és rendelkeznie kell alapvető kiberbiztonsági ismeretekkel, például a különböző kiberbiztonsági fenyegetésekről, a biztonsági kockázatok csökkentésének módjairól és a biztonsági incidensek kezeléséről.
- Kiberbiztonsági viselkedés: A személynek biztonságos viselkedést kell tanúsítania a kibertérben, például erős jelszavakat kell használnia, rendszeresen frissítenie kell a szoftvereket és figyelmesen kell kezelnie az online személyes adatokat. Ezt összefoglalóan biztonságtudatos viselkedésnek hívjuk.

A biztonságtudatosságra számos tényező hatással lehet, de ezek közül - főleg nemzetközi felmérések alapján - ki kell emelni a legfontosabb szociodemográfiai tényezőket: a nem, életkor, lakhely, iskolázottság függvényében vizsgálták a biztonságtudatosságot. Két

dolgot érdemes kiemelni ezen vizsgálatok kapcsán: 1. amennyiben komplexen vizsgálták a biztonságtudatosságot, akkor jellemzően nem nagy mintán, hanem gyakran csak néhány száz főn történt a vizsgálat, ritka az ezer feletti, vagy a több ezres minta (Hadlington, 2017) (Nunes et al., 2021) (Gioulekas et al., 2022). 2. nagyobb minta esetében egy-egy kockázatot elemeztek (phishing), és ebben az esetben volt lehetőség nagymintás vizsgálat végzésére (Gordon et al., 2019) (Rizzoni et al., 2022). Emellett ezeket a vizsgálatokat az is jellemzi, hogy egy „pillanatképet" rögzítettek, vagyis egyszeri felmérésekről volt szó, és nem volt jellemző a minta vagy a sokaság időbeli követése.

A szakirodalmi adatok alapján megállapítható, hogy a kiberbiztonsággal kapcsolatos hiányos ismeretek és helytelen attitűdök jelentős szerepet játszhatnak a szervezetek és a magánélet biztonsági szintjének csökkenésében (Nyikes, 2019; Sasse & Flechais, 2005)

A biztonságtudatosság fejlesztése, például ismeretterjesztés, képzések és készségfejlesztés által, jelentősen hozzájárul az információs rendszerek biztonságának növeléséhez, nemcsak a munkahelyi környezetben, hanem az otthoni használat során is (Alahmari et al., 2023). Az ilyen kampányok, tevékenységek és módszerek tervezésekor elengedhetetlen figyelembe venni, hogy a célzott egyének vagy csoportok milyen szintű ismeretekkel és milyen hozzáállással rendelkeznek az adott problémakör kapcsán (Oroszi, 2020), és a fejlesztési tervekben a fenti igényeket figyelembe vevő tartalmi és módszertani elemekkel kell a tudatosítási programot megvalósítani.

Magyarországon a Kormány 2018. év végén a 1838/2018. (XII. 28.) Korm. határozattal elfogadta a hálózati és információs rendszerek biztonságára vonatkozó stratégiát, amelyben már foglalkoznak a biztonságtudatosság mérésével, és a mérésekre épülő fejlesztésével. A dokumentumban megfogalmazásra került egy „irányítási keretrendszer", amelynek egyik eleme a lakosság biztonságtudatosságának rendszeres felmérése.

A korábbi magyar publikációk már foglalkoztak a biztonságtudatossággal, azonban széleskörben, lakossági felmérés még nem történt.

A publikációk közül kiemelendő egy hazai tanulmány, amely talán legátfogóbban próbálta megközelíteni a különböző demográfiai tényezők és a biztonságtudatosság kapcsolatának vizsgálatát. Nyikes 2019-es doktori értekezésében az emberi tényezők és kiberbiztonság összefüggéseit vizsgálta (Nyikes, 2019). A kutatásban több, mint 1100 résztvevő adatait és válaszait vették figyelembe. A doktori munka keretében végzett

kutatás eredményeiként megállapításra került, a felmérésben a válaszadók többsége rendszeresen használja az internetet, és a digitális kompetencia szintje változó a lakóhely és az életkor függvényében. A fiatalabb korosztályok (34 éves kor alatt) magasabb digitális kompetenciával rendelkeznek, míg az idősebb korosztályok (35 évesek és idősebbek) magasabb biztonságtudatossági szinttel bírnak. A felmérés alapján elmondható, hogy a lakóhely befolyásolhatja a digitális biztonságtudatosságot, míg a nem és az iskolázottság szerepével kapcsolatban nem talált egyértelmű összefüggést a szerző. A jelen dolgozat szempontjából nem releváns, de fontos általános megállapítás volt digitális térben való biztonságos létezésünkhöz, hogy az internetes zaklatás („cyberbullying") főként azokat érinti, akik kevésbé biztonságtudatosak, és az alacsonyabb digitális kompetenciával rendelkező felhasználók hajlamosabbak a problémákat maguk megoldani vagy figyelmen kívül hagyni a zaklatást.

A magatartás és a biztonságtudatosság kapcsolatát az Európai Unió Kiberbiztonsági Ügynöksége (ENISA – European Union Agency for Cybersecurity) is vizsgálta, és ajánlásaiban megfogalmazta, hogy milyen magatartás befolyásolási modellek mentén javasolja az egyének és csoportok biztonságtudatos magatartásának javítását. Michie COM-B modellje és Fogg B=MAT modellje egyaránt alkalmas arra, hogy ez alapján magatartás befolyásolás központú beavatkozás történjen. (European Union Agency for Cybersecurity (ENISA), 2018). A COM-B modell a viselkedés megváltoztatására összpontosít három fő tényezőre építve: Képesség (Capability), Lehetőség (Opportunity) és Motiváció (Motivation), amelyek együttesen meghatározzák a viselkedést (Behavior). A képesség magában foglalja a tudást és készségeket, a lehetőség külső tényezőkre, mint a környezet és erőforrások vonatkozik, míg a motiváció magában foglalja a belső vágyakat és szándékokat. Ezek a tényezők kölcsönhatásban vannak egymással, és a viselkedés megváltoztatása érdekében mindhárom elemre hatni kell.

A Fogg B=MAT modell szerint a viselkedés (Behavior) akkor következik be, amikor három elem együttesen jelen van: Motiváció (Motivation), Képesség (Ability), és Kiváltó tényező (Trigger). A modell azt sugallja, hogy a viselkedés megváltoztatásához elegendő motivációra és megfelelő képességre van szükség, míg a kiváltó tényező az az inger, amely aktiválja a viselkedést.

Mindkét modell egyszerű, és megfelelő keretet adnak a viselkedés kialakításának és megváltoztatásának megértéséhez.

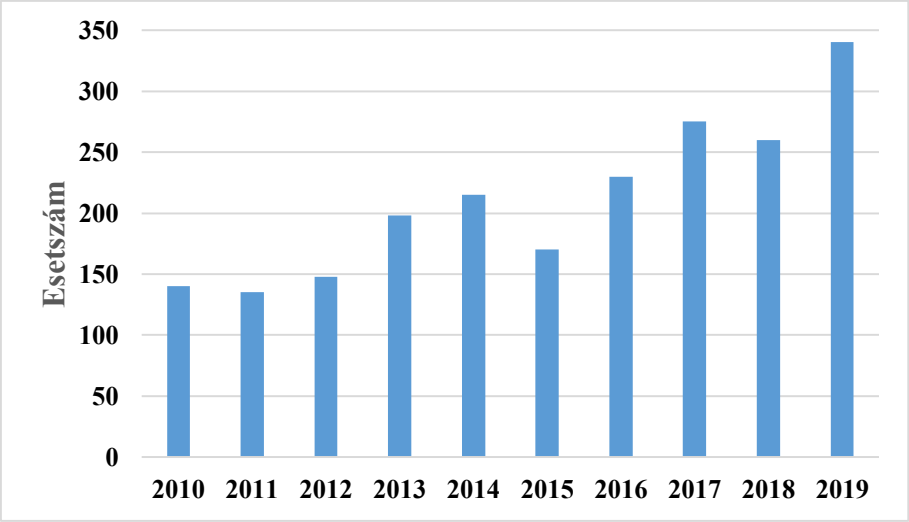
Az elmúlt időszak történései, különösen a COVID-19 pándémia kapcsán fenyegetések alapján egyértelmű (Szabó, 2021), hogy a felhasználói magatartás, különösen a biztonságtudatosság, alapvető szerepet játszik a kibertér biztonságos és felelősségteljes használatában.

Fontos megemlíteni, hogy az általános biztonságtudatossági vizsgálatok mellett az egészségügyi ágazatban dolgozók általános, digitalizációhoz kapcsolód attitűdjét is vizsgálni kell (Tóth et al., 2020), illetve azon belül kifejezetten szükséges a biztonságtudatosság vizsgálata is.

1.8. Veszélyek és fenyegetések az egészségügy számára

A kibertérből érkező fenyegetések nem korlátozódnak egy adott típusú vagy méretű egészségügyi szolgáltatóra, hanem valamennyi intézmény veszélyeztetettnek tekinthető. Az utóbbi években jelentősen megnőtt az egészségügyi szolgáltatók és rendszerek elleni külső támadások száma. Az Egyesült Államokban 2009. óta rendszeresen dokumentálják az egészségügyi rendszerekhez kapcsolódó adatbiztonsági incidenseket, amelyek alapján az érintett intézmények és betegek száma folyamatos emelkedést mutat. Az Amerikai Egyesült Államok Egészségügyi és Humán Szolgáltatási Minisztériumának Civil Jogok Irodája (US Department of Health and Human Services, Office for Civil Rights) 2010 óta gyűjtött adatai jól láthatóan alátámasztják ezt a tendenciát. Az általuk közzétett jelentésekben csak olyan események szerepelnek, amelyek legalább 500 beteg vagy ügyfél adatait érintették.

Amerikai adatok alapján megállapítható (lásd 2. ábra), hogy az egészségügyi intézmények ellen elkövetett információbiztonsági incidensek száma az elmúlt években folyamatosan nőtt: 10 év alatt a kezdeti 147/év esetről 2019-re 342 eset/évre változott, egyenletesen növekvő tendenciát mutatva (Palicz et al., 2020).



2. ábra: A 2010-2019 között az USA-ban információbiztonsági incidenssel érintett egészségügyi szolgáltatók számának változása (saját szerkesztés) (Palicz et al., 2020)

Az egészségügyi ellátás során számos alkalommal áll elő olyan helyzet, amelyben gyors helyzetfelismerésre, a diagnózis felállítására, és beavatkozásra van szükség. Az ellátásban résztvevő személyek erre lettek kiképezve, ez a hivatásuk része. Több olyan helyzet is adódhat, amikor az élet megmentése magasabb prioritású válik, mint pl. a higiénés szabályok betartása, illetve a szakmai szabály és a hivatás az élet megmentését tekinti elsődleges célnak. Ez az attitűd a napi munkavégzésben is megjelenik, és mind a hagyományos, mind a digitális adat- és információkezelésben tetten érhető (pl. néhány évvel ezelőtt a telefonos tájékoztatás szinte elvárt volt az egészségügyi intézmények esetében, ma már ennek is szigorú szabályai vannak, és azonosítás nélkül nem is adható ki semmilyen adat és információ még vészhelyzetben sem). Különösen igaz ez, amikor nemcsak az adatokra gondolunk, hanem az információs rendszerekre is. Példaként említhetjük, hogy általában jellemző a biztonságtudatosság alacsony szintje (pl. nem megfelelően elzárt betegdokumentumok, nővérpulton, orvosi szobákban hagyott leletek, vagy éppen az elektronikus információs rendszerek esetében a belépések és hozzáférések lehetőségei, monitorra ragasztott, közösségi szinten megosztott hozzáférések, stb.).

Az ágazaton és intézményeken belüli fejlesztések priorizálása minden esetben nehéz, ha folyamatosan forrásszűke van egy adott ágazatban. A magyar egészségügyben az elmúlt években a működési források folyamatos szűkössége volt megfigyelhető, amely szinte minden év végére konszolidációs igényben mutatkozott meg. Emellett az informatikai és információbiztonsági fejlesztések területén inkább a központi fejlesztések kerültek

meghatározásra, és intézményi szinten kevés forrás és szabad lehetőség volt az információbiztonság fejlesztésére. Ez a szűkös források miatt általában nem is vezetői preferencia.

Az egészségügy intézményekben előfordult incidensek előfordulása alapvetően befolyásolja a szolgáltató napi működését. Ezzel kapcsolatosan végeztek amerikai kutatást, amiben a Medicare biztosító adatait és a HHS adatait vetették össze a sürgősségi ellátás két fontos mutatója tekintetében: szívizom infarktust szenvedett betegek esetében vizsgálták az első EKG elvégzéséig eltelt időt, illetve az infarktust követő korai halálozást (Choi et al., 2019). A kutatók azt találták, hogy azokban az intézményekben, ahol valamilyen incidens történt a kórházban, ott az incidenst követően szignifikáns megnőtt mindkét érték azon kórházakhoz viszonyítva, ahol nem volt incidens. Ez a tény arra utalhat, hogy a biztonságos működés érdekében olyan folyamatváltozásokat kellett hozni, illetve vélelmezhető, hogy a dolgozói attitűdök is úgy változtak, amelyben nagyobb hangsúlyt helyeztek az információbiztonsági folyamatokra, és így ezek kényszerűen az ellátási időket megnövelték. Ezek oki kutatása, és az összefüggések feltárása nagyon fontos lenne, illetve a magyar környezetbe is szükséges lenne ezeket átültetni.

Az adat- és információbiztonság kapcsán külön figyelmet érdemel az a jelenség, amikor az egészségügyi dolgozók – a belső rendszerek nem megfelelő szolgáltatásai, gyengeségei miatt – előnyben részesítik a külső, piaci alapú szolgáltatásokat. Ezek a kereskedelmi célú levelező- és fájlmegosztó rendszerek, mint például a Gmail vagy a Google Drive, gyakran vonzó alternatívát jelentenek a stabilitásuk, kiforrott működésük és felhasználóbarát jellemzőik miatt. Az ilyen rendszerek használata azonban jelentősen növeli a biztonsági kockázatokat, mivel a szervezet információi kevésbé kontrollált környezetbe kerülnek. További problémát jelenthet az, ha a szolgáltatókat felügyelő hatóságok vagy intézmények is ezeket a csatornákat választják a kommunikáció során a könnyű kezelhetőség és rugalmasság miatt, ami tovább fokozza a potenciális adatvédelmi problémák kockázatát (Greevy, 2022).

Az egészségügyi ellátásban dolgozó orvosoknak, egészségügyi szakembereknek és a támogató folyamatok résztvevőinek minden munkakörben aktívan kell törekedniük a biztonság megerősítésére, valamint a biztonsági incidensekből származó tanulságok megosztására. A kórházi adatvédelem nem szűkülhet le kizárólag a HIS rendszerek (kórházi információs rendszerek) védelmére, hanem ki kell terjednie az összes

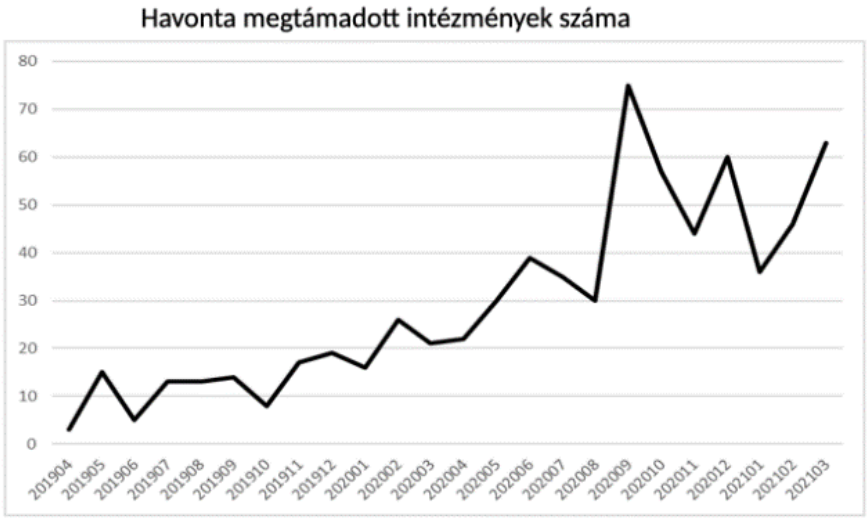
kapcsolódó támogató folyamatra, mint például a kommunikáció és a gazdálkodás. Minden felhasználói csoport számára olyan átfogó és magas szintű biztonsági megoldásokat kell kialakítani, amelyek a folyamatok és az infrastruktúra teljes spektrumát lefedik (Russell Ritenour, 2020). Ez rendkívül komplex folyamat.

Egy 2019-ben három európai országban (Görögország, Portugália és Románia) végzett, majd 2022-ban publikált tanulmány az egészségügyi intézményekben végzett felmérést az információs és kommunikációs technológiai (ICT) szakemberek és az egészségügyi szakemberek között (Gioulekas et al., 2022). A tanulmányban összesen 10,418 egészségügyi szakembert és 69 ICT-szakembert hívtak meg a felmérésben való részvételre, azonban a válaszadók száma összesen 736 volt, ebből 37-en ICT-szakemberek, míg 699-en egészségügyi szakemberek voltak. Az eredmények azt mutatták, hogy a kibervédelmi incidensek a személyzet alacsony kibervédelmi tudatossági szintjével állnak összefüggésben, és hogy a kibervédelmi kultúra fejlesztése és a személyzet folyamatos képzése elengedhetetlen az egészségügyi intézmények kibervédelmének javításához.

1.9. A COVID hatása a kiberbiztonságra – középpontban az egészségügy

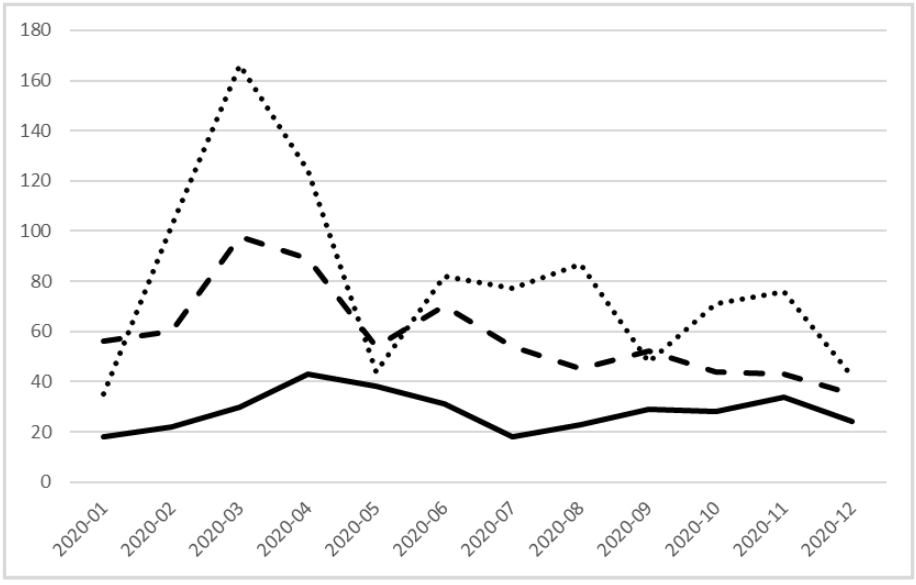
A COVID-19 járvány alatt egyéni és társadalmi szinten számos kihívással kellett szembesülni, amelyek alapvetően megváltoztatták a korábban megszokott életünket, illetve az egészségügyi ellátórendszer kapacitásait extrém módon terhelték ezek a kihívások. Ez a pándémia különböző szakaszaiban eltérő volt. A magyar járványlefolyás – különösen az első hullám esetén – követte az Ausztriában zajló eseményeket, így a magyar kormánynak, az Operatív Törzsnek, és a különböző szervezeteknek volt lehetőségük felkészülni a történésekre, különös tekintettel az egészségügyi ellátórendszert érő terhelésre (Szerencsés et al., 2021).

A járvány nemcsak az egészségügyi rendszerek kapacitását terhelte meg, hanem a kiberbiztonsági infrastruktúrára, azon belül az egészségügyet szolgáló informatikai infrastruktúrára is komoly hatással volt. Tekintettel a kibertér nemzetköziségére, ezt az időszakot jól jellemzik az amerikai egészségügyi ellátórendszerből származó adatok, amelyekből jól látható, hogy 2020. februárját megelőzően, illetve azt követően jelentős számbeli eltérés volt az intézményeket ért támadásoknál (3. ábra).



3. ábra: Az Amerikai Kormány Egészségügyi és Humán Szolgáltatási Minisztériumában (HHS) működő Office for Civil Rights (OCR) adatai az egészségügyi intézményeket ért támadások számáról 2019. április – 2021. március között, a COVID-19 járvány indulását megelőzően és azt követően (saját szerkesztés) (Palicz, Bencsik, & Szócska, 2021)

A magyarországi adatokat, amelyek nem egészségügy specifikusak voltak, a Nemzeti Kibervédelmi Intézettel dolgoztuk fel. Ezekből látható, hogy a magyar tendenciák hasonlóak voltak az amerikaihoz, illetve más nemzetközi tendenciához (4. ábra) (Palicz, Bencsik, & Szócska, 2021; Szabó, 2021).



4. ábra: A Nemzeti Kibervédelmi Intézet (NKI) által észlelt események számának alakulása esemény- és intézménytípusonként 2020. január 1- 2020. december 31. között (Nemzeti Kibervédelmi Intézet adatai, saját szerkesztés) (Palicz, Bencsik, & Szócska, 2021) (észlelés: folytonos vonal, jelzés: szaggatott vonal, bejelentés: pontozott vonal)

A pándémia alatt nőtt az egészségügyi szolgáltatók elleni támadások száma. A támadók gyakran kihasználták az intézmények által a válság miatt bevezetett gyors változásokat, és olyan módszerekkel próbálkoztak, mint a ransomware vagy a phishing támadások. Ezen támadások nemcsak az egészségügyi adatok integritását veszélyeztették, hanem az ellátás minőségét is, mivel az egészségügyi dolgozók gyakran nem tudták elérni a kritikus információkat (He et al., 2021).

Az egyik legfontosabb változás a távmunka és a távdiagnosztika elterjedése volt. Bár ezek a technológiák lehetővé tették az egészségügyi ellátás folytonosságát, új biztonsági réseket is nyitottak. A távmunkára átálló egészségügyi dolgozók gyakran használtak nem megfelelően biztosított eszközöket és hálózatokat, ami növelte a kiberbiztonsági incidensek kockázatát (Wasserman & Wasserman, 2022). Ezekre a kihívásokra Magyarországon is készültek iránymutatások, amelyek kiberbiztonsági iránymutatást is tartalmaztak (Mikesy et al., 2020).

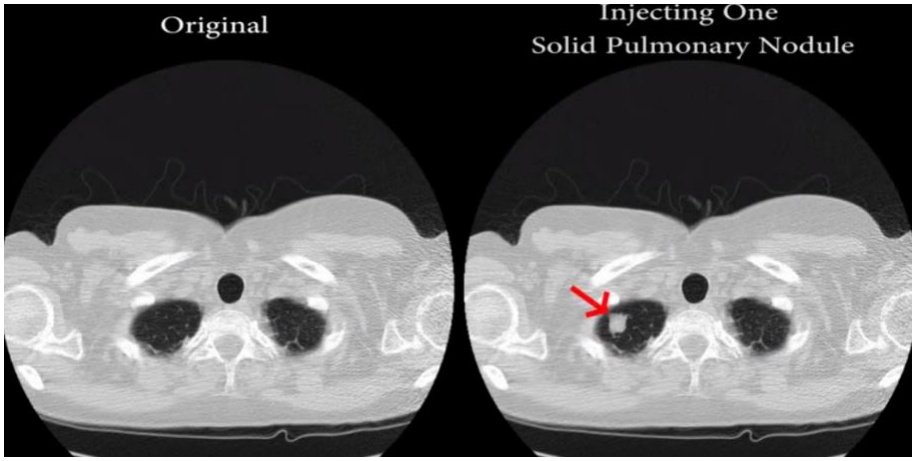
A COVID-19 járvány teremtette helyzetben több országban, lehetővé tették, hogy a különböző adatok összekapcsolásra kerüljenek. Ebben azoknak az országoknak versenyelőnyük volt, ahol nemzeti adatbázisok voltak, és állami tulajdonban vannak az adatok. Így történt ez Magyarországon is, ahol a különleges jogrendben az Operatív Törzs kapott felhatalmazást arra, hogy irányítsa és lehetővé tegye a járványügyi védekezés érdekében szükséges adatok elemzését, adattavak és adattárházak kialakítását akár a különböző forrásból és szektorból származó adatok és adatbázisok összekapcsolásával (Eütv. 232/B. § (7) és (8) bekezdése) (Magyar Országgyűlés, 1997). Egy ilyen helyzetben (járvány) az ágazaton belüli adatok bányászatán kívül a más ágazatokban keletkező, anonimizált adatok is értékesek. Ehhez a jogi környezet fejlesztése mellett elsősorban az interoperabilitási problémákat kell megoldani (Kataria & Ravindran, 2020).

A pándémia felszámolása, illetve további járványok megelőzése, ezáltal a kritikus infrastruktúrák terhelésének csökkentése a kiberbiztonság szintjét is áttételesen is növelik, így hozzájárulnak az általános biztonsági szint javulásához. A biztonság növelése áttételes, elsősorban az emberi tényezőn keresztül hat, hiszen kimutatták: egy járvány, vagy jelentős munkaterhelés kapcsán a kiégés és kimerülés jelentősen csökkenti a munkavállalói figyelmet, ezáltal növeli a kockázatos magatartást az információs rendszerek esetében (Hong et al., 2023). Nem specifikus, általános preventív jellegű

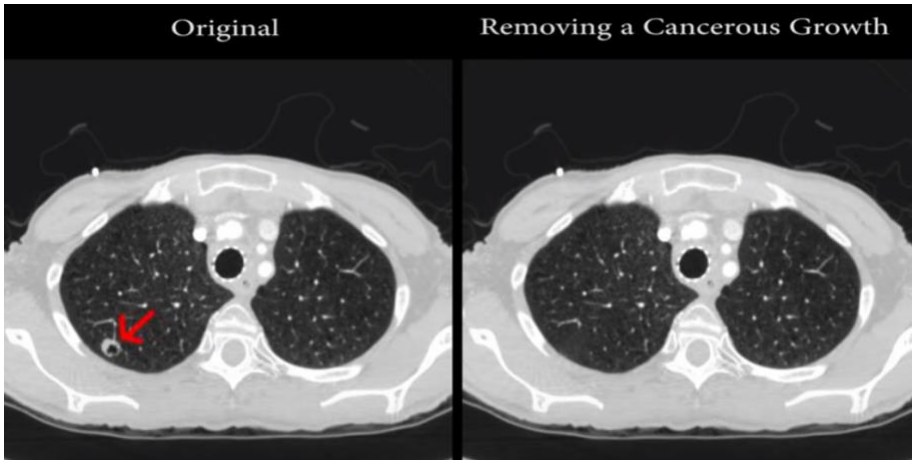
program lehet az élethosszig tartó (life-long) oltási programok bevezetése, amelyek megelőző intézkedésként járulnak hozzá a biztonság javításához (Ugrin et al., 2022).
Összességében a COVID-19 járvány Janus arcú volt: egyrészt általában felhívta a figyelmet a kibertér felől érkező fenyegetésekre, jelentős számú hír, publikáció keletkezett ebben az időben, másrészt a bekövetkezett események révén rávilágított az egészségügyi rendszer sérülékenységére és az ebből fakadó ellátási nehézségekre.
A pandémia az egészségügyben „digitalizációs driver”-ként működött, felgyorsította az egészségügyi technológiai infrastruktúra változásait, de ezzel együtt a digitális transzformáció mértékének növekedésével új kiberbiztonsági kockázatokat is magával hozott.

1.10. Új technológiák miatti kihívások

Mint azt fentebb is említettük, a jelen és közeljövő egészségügyének talán egyik legfontosabb kihívása a mesterséges intelligencia információbiztonsági vonatkozása: elsősorban a napi gyakorlatban alkalmazott orvosi döntéstámogatás miatt, illetve számos területen használhatják predikcióban és a prognosztikában is. A mesterséges intelligencia kapcsán a sikeres fejlesztések egyik kulcsfontosságú tényezője, hogy megfelelő adatok álljanak rendelkezésre a felügyelt tanulás érdekében. Amennyiben az adatok sérülnek, az azt eredményezi, hogy az algoritmus rossz tanulóadatbázison tanul, tehát rossz következtetésre jut a adatok alapján. A mesterséges intelligencia alapú rosszindulatú manipuláció eredményeként az adat integritása sérül, és nem a ténylegesen észlelt, diagnosztizált kép kerül tárolásra. 2019-ben izraeli kiberbiztonsági kutatók demonstrálták, hogy olcsó és egyszerű eszközökkel, valamint social engineering alkalmazásával képesek behatolni egy kórház képalkotó diagnosztikai rendszerébe. A behatolás után mesterséges intelligencia-algoritmusokat használtak az elvégzett CT-felvételek módosítására, ezzel érzékeltetve a rendszerek sérülékenységét és az egészségügyi adatok manipulálásának veszélyét (Mirsky et al., 2019). A kísérlet során a teljesen egészséges felvételre daganatos elváltozást helyeztek el (5. ábra) , illetve a beteg, daganatos tüdő képéről azt eltávolították (6. ábra) (Palicz & Joó, 2020).



5. ábra: Egészséges mellkas CT felvétel manipulálása mesterséges intelligenciával (Mirsky et al., 2019)



6. ábra: Kóros mellkas CT felvétel manipulálása mesterséges intelligenciával (Mirsky et al., 2019)

A kutatók ezt követően tapasztalt radiológusoknak mutatták meg a módosított képeket, akik nem tudták megkülönböztetni, hogy a daganat eredetileg is jelen volt-e, vagy a mesterséges intelligencia algoritmusa hozta-e létre. Ez a kísérlet rávilágított arra, hogy milyen sokféle módon manipulálhatók az egészségügyi diagnosztikai eredmények. Az ilyen jellegű beavatkozások nemcsak a betegellátást veszélyeztetik, hanem potenciálisan alkalmasak lehetnek politikai játszmák befolyásolására vagy akár klinikai gyógyszertesztek eredményeinek manipulálására is.

A jövőbeli technológiák közül – leginkább az érdekessége és jelentősége miatt érdemes – a „cyberbiosecurity” fogalmával foglalkozni. Ez alatt azt a legújabb tudományterületet értjük, amely kiberbiztonság („cybersecurity”) és a biológiai biztonság („biosecurity”)

metszéspontjában van. Ez a határterületi megjelenés nemcsak arról szól, hogy a biológiai vagy biztonsági laborok éppen úgy a kibertérben működek, mint ma már minden, és emiatt kitettek a kibertér biztonsági kockázatainak. Ez olyan futurisztikus területeket is magukba foglalnak, mint a DNS alapú adattárolás és annak biztonsági kérdései, vagy éppen az a lehetőség, hogy hogyan lehet rosszindulatú digitális kódok segítségével befolyásolni a nukleinsav szintézist, vagy éppen hogyan lehet a nukleinsav bázisain keresztül olyan rosszindulatú digitális kódot tárolni, amely képes befolyásolni az elektronikus információs rendszereket (Puzis et al., 2020; Shipman et al., 2017).

A fentiek mellett, ha időben előre tekintünk, akkor számos olyan technológiai trend van, amely már az elkövetkező néhány évben is nagymértékben befolyásolja az egészségügyi adatokhoz történő hozzáférést, az adatok mennyiségét, és biztonságát. Elég, ha csak az 5G vagy 6G technológiára gondolunk, amely teljesen át fogja alakítani az orvosi robotika, a távműtétek területét (Abdel Hakeem et al., 2022; Chen et al., 2021).

Hasonló jelentőségű, elsősorban az adatok titkosítása, és megfelelő tárolása szempontjából a „quantum computing", amely révén a most biztonságosan tároltnak hitt adataink sem lesznek biztonságban, illetve olyan dimenziót nyit meg az adatok értelmezése, elemzése szempontjából, amelynek jelentőségét napjaikban még elképzelni sem tudjuk igazán (SaberiKamarposhti et al., 2024). Nem véletlen, hogy az egészségügyi adattal foglalkozók körében is fontos üzenetként jelenik meg az alábbi, a hacker kultúrában meghonosodott mondat (amely az adatokra vonatkozik): „Harvest now, decrypt later", vagyis „Gyűjts most, később feloldod (a titkosítást)!

A téma multidiszciplináris megközelítése egyre fontosabb lett az elmúlt időkben. Ezt jelzi, hogy számos olyan kezdeményezés, formáció jött létre Magyarországon is, elsősorban kutatási, illetve koordinációs céllal, amiben különböző szakemberek dolgoznak együtt. Példaként említhetjük a Nemzeti Laborokat (Egészségbiztonság Nemzeti Labor, Mesterséges Intelligencia Nemzeti Labor, Infokommunikációs és Információtechnológiai Nemzeti Laboratórium), amelyekben különböző szempontok, megközelítések mentén dolgoznak együtt a kiberbiztonság általános javítása, illetve azon belül az egészségügyi kiberbiztonság érdekben.

1.11. Összefoglalás

Az előzőekben ismertetettek alapján **doktori munkám témájául – általánosan megfogalmazva - az egészségügy digitális transzformációjával együtt járó adat és információbiztonsági változásokat, illetve ezen belül is a kiberbiztonságot választottam.**

A kutatásokat megalapozó irodalmi áttekintés alapján az mondható el, hogy az elmúlt évek digitális átalakulása az egészségügyet is jelentős mértékben érintette, és ez igaz a magyar egészségügyi rendszerre is. Ezek a fejlesztések elsősorban technológiai fókuszúak voltak, és csak mérsékelten érintették például a felhasználókat, vagy a fejlesztések végső kedvezményezettjeit, az egészségügyi fejlesztések esetében a betegeket. A fejlesztések kiegyensúlyozatlansága hátterében az egyik lehetséges ok, hogy **nem rendszerszintű megközelítést alkalmaznak**, amelynek oka részben az, hogy a digitális egészségügyi rendszerek ökoszisztéma jellegű megközelítése és leírása hiányzik. **Ennek a rendszerszintű megközelítésnek a hiánya** kapcsán adódott a logikus lehetőség, hogy **a biológiai rendszerekhez hasonlóan itt is használjuk, és meghatározzuk a digitális egészségügyi ökoszisztéma fogalmát**, és vizsgáljuk meg, hogy abban az adat hol helyezkedik el, illetve ezen megközelítéssel hogyan értékelhető a magyarországi helyzet.

Ezen rendszeren belül sejthető, hogy az **adat kulcsszerepet** játszik. Azonban ez az adat nemcsak az egészségügyi digitális rendszerekben keletkezhet, hanem „kívülről” is érkezhet, és ez is hozzájárulhat az egészségügyi rendszer eredményeihez, vagyis van lehetőség arra, hogy **nem közvetlenül az egészségügyben keletkező adatok is felhasználhatók legyenek az egészségügyi rendszer javítására, monitorozására. Ezen megközelítéssel, megfelelő adat és információbiztonsági feltételek biztosítása mellett a gyakorlati alkalmazással az irodalomban nem találkoztunk.** Ezt az igényt különösen felerősítette, hogy a COVID-19 pandémia alatt a különböző adatforrások kreatív, társadalmi hasznosítására szükség volt, és ezt lehetőség szerint nemzeti szinten kellett megoldani.

Az egészségügyi digitális rendszerek működésére, az adatok és információk biztonságára az egyik legnagyobb veszélyt azok a külső tényezők jelentik, amelyek befolyásolják az

információk bizalmasság-sértetlenség-rendelkezésre állás hármasát. Ennek tipikus esetei az egészségügyi intézményeket érintő és rendszerszintű hatással is bíró zsarolóvírus támadások. Ez a jelenség különösen felerősödött a 2020-ban indult SARS COVID-19 világjárvány alatt és után. Magyarországon a kibervédelmi tevékenység erősödésével párhuzamosan az egyes szektorok is aktívabbá váltak, azonban a zsarolóvírus esetek csak korlátozottan váltak ismertté, holott ezen esetekből nagyon sok tapasztalatot meg lehet osztani: jó és rossz példákat lehet megismertetni. **A tudományos kutatásom kezdetekor nem álltak rendelkezésre olyan esetleírások, amelyek hazai egészségügyi intézmények esetében írták volna le a zsarolóvírus támadás lefolyását.** Ezek megismerése, a rendszerbe kerülés, majd az okozott hatás leírása, tudományos megközelítésű elemzése fontos része a rendszer és egy-egy szervezet tanulási folyamatának.

Végül azt kell kiemelni, hogy ezekben a rendszerekben is emberek dolgoznak, akik ismeretei, viselkedése, attitűdje alapvetően befolyásolja a rendszerek (és benne az adatok és információk) biztonságát. Így a biztonságtudatossággal kapcsolatos emberi szempontok, az azokat meghatározó szociodemográfiai és egyéb jellemzők megismerése kiemelten fontos általában a lakosságot tekintve, majd azt követően az egészségügyi digitális rendszerek, de általában a digitális átalakulások következtében létrejövő elektronikus információs rendszerek biztonsági szintjének emelése érdekében. **A kutatás megkezdésekor a magyar lakosságra vonatkozóan nem, vagy korlátozottan álltak rendelkezésre olyan adatok, amelyek a szociodemográfia jellemzőkre vonatkozóan vizsgálták volna, hogy hogyan lehet jellemezni a biztonságtudatos vagy kevésbé biztonságtudatos csoportokat.**

A bevezetőben és a fenti összefoglalóban bemutatott és kiemelt problémakör magyar, egészségügyi szempontú feldolgozása - egyelőre - gyakorlatilag nem létezik.

Az irodalmi áttekintés és a gyakorlati tapasztalatom alapján az elkövetkező években az egészségügy fejlődésének, és ezen belül is a diszruptív technológiák (pl. mesterséges intelligencia, telemedicina) elterjedésének az egyik legfontosabb területe, vagy talán a fejlődés „Achilles-sarka” az információbiztonság lesz. Mind a betegek (ügyfelek), mind a rendszerben dolgozók számára kritikus lesz, hogy milyen tapasztalatokat szerzünk,

milyen ismeretekkel rendelkezünk, milyen kompetenciákat kell használnunk, fejlesztenünk és milyen attitűddel viszonyulunk az ehhez kapcsolódó változásokhoz ebben az adatgazdag, de rendkívül sérülékeny világban.

Talán azt is lehet mondani, hogy általában a digitális átalakulás, és az azzal járó változtatások egyik kritikus sikertényezőjéről beszélünk: bár számos nemzetközi irodalom már található, azonban **az egészségügy sajátosságai miatt kevés referencia található erre a szektorra vonatkozóan, illetve különösen érintetlen még a magyar egészségügy ebből a szempontból.**

Különösen fontosnak tartom, hogy a magyar egészségügyi digitalizáció, amelynek tervezésénél, a kezdeti lépésinél - kiemelt uniós projektek révén - személyesen is ott lehettem, azt a kezdeti versenyelőnyét, amely az EESZT létrejöttével megszerzett, az elkövetkező években is megtartsa.

Erre elsősorban azért van szükség, hogy mindezen fejlesztések a magyar egészségügy javát szolgálják, vagyis a betegek számára több egészséget eredményezzenek.

2. Célkitűzések, kutatási kérdések és hipotézisek

Általános célkitűzésként azt fogalmaztam meg, hogy az információ- és kiberbiztonság területén megfogalmazott kihívásokat az egészségügy szemszögéből tekintsem át, annak specialitásait figyelembe véve, különösen koncentrálva azokra a tényezőkre, amelyek a betegek biztonságát érdemben befolyásolhatják. Ilyen terület lehet például az egészségügyi intézmények folyamatos működésének biztosítása (üzletmenet folytonosság tervezés és menedzsment: „Business Continuity Plan and Management" – BCP és BCM) illetve az emberi erőforrás biztonságtudatossága.

Az alábbi specifikus célkitűzéseket (C), kutatási kérdéseket (K) és hipotéziseket (H) fogalmaztam meg:

C1. célkitűzés: Annak feltárása és bemutatása, hogy a digitalizáció révén létrejövő, megváltozó digitális egészségügyi rendszer egységes szempontok alapján leírható és értékelhető (rövidítve: C1: digitális egészségügyi ökoszisztéma).
K1.1. kutatási kérdés: Leírható-e a digitalizációs átalakulás során megváltozó egészségügy rendszer egy ökoszisztémaként? Ennek milyen elemei vannak és ezeket mi jellemzi Magyarországon?

C2. célkitűzés: Annak bemutatása, és gyakorlati példával igazolása, hogy az egészségügyi adatokhoz biztonságos környezetben más adatok is kapcsolhatók, és ezen innovatív adathasznosítások olyan értéktöbbletet eredményeznek, amely kormányzati döntéselőkészítési és döntéshozatal szinten is megjeleníthető (rövidítve: C2: biztonságos innovatív adathasznosítás).
Az egészségügyi rendszeren kívül is keletkeznek olyan adatok, amelyek feldolgozása, megfelelő bemutatása az egészségügyi rendszert és állapotot érintő döntések alapjául szolgál. Ezek az adatok különös jelentőséggel rendelkeznek veszélyhelyzetben, amikor az innovatív adathasználat révén egyedi kérdésekre lehet választ találni, illetve ezek a döntések alapjául szolgálhatnak. Ezekben a helyzetekben kritikus fontosságú, hogy az adathasznosítás biztonságos környezetben történjen.

K2.1. kutatási kérdés: Hogyan és milyen módszertannal lehet hasznosítani a digitális egészségügyön kívül keletkezett adatokat, egy globális vagy lokális egészségbiztonsági eseményhez kapcsolódva? Hogyan biztosítható, hogy az adatvédelmi szabályoknak és kiberbiztonsági követelményeknek megfeleljen ez a módszertan?

C3. célkitűzés: Annak bemutatása, hogy az egészségügyben keletkező adatok sértetlensége, bizalmassága és rendelkezésre állása kritikusan fontos a működés szempontjából, és ezt a kibertérből a zsarolóvírus támadások kapcsán reális veszély fenyegeti a kórházak esetében is (rövidítve: C3: zsarolóvírusok az egészségügyben).

K3.1. kutatási kérdés: Milyen hatással voltak zsarolóvírus támadások a magyar kórházak működésre, és milyen mértékben érintették a kórházi informatikai és információs rendszereket, beleértve a szállítói lánc részeként működő szakmai területeket?
K3.2. kutatási kérdés: Hogyan, milyen szempontok és kérdések mentén lehet az eseteket megfelelően összegyűjteni és elemezni annak érdekében, hogy megállapítható legyen: mely funkciók milyen mértékben károsodtak az adott egészségügyi intézményben?

C4. célkitűzés: Annak vizsgálata, hogy van-e összefüggés a demográfiai jellemzők valamint informatikai használati szokások és a kiberbiztonsági tudatosság között (rövidítve: C4: lakossági biztonságtudatosság)
H4.1. hipotézis: Feltételezésem szerint a magyar lakosság esetében a biztonságtudatos magatartás nincs összefüggésben kor, nem, iskolázottság és informatikai használati szokásokkal.

3. Módszertan

A kutatási módszereket tekintve szükségszerű a komplex és interdiszciplináris megközelítés, tekintettel a téma jellegére, összetettségére. Az áttekinthetőség kedvéért a hipotézisek és felhasznált módszertanok összefoglaló mátrixának (1. táblázat) bemutatásával kezdem a fejezetet, és azt követően mutatom be részletesen a releváns módszertanokat.

A módszertani mátrixban összefoglalóan áttekintem, hogy az egyes célitűzések és hipotézisek esetén milyen módszertani ezközöket választottam. Ez elsősorban arra alkalmas, hogy az adott kutatási célkitűzésnél a domináns eszközt jelenítse meg, vagyis nem jelent kizárólagosságot. Pl. az irodalmi áttekintést értelemszerűen minden célkitűzés kapcsán használtam, de az 1-es és 3-as célkitűzések kutatásánál, illetve az irodalmi összefoglalók készítésénél volt nagyobb szerepe.

1. táblázat: Módszertani mátrix a doktori értekezésben használt módszertanok (M) és célkitűzések (C) összefüggéséről (saját szerkesztés)

+ - +++: az adott módszertan használata mennyire jellemző a célkitűzések vizsgálatánál

Módszertanok	C1. digitális egészségügyi ökoszisztéma	C2. innovatív adathasznosítás	C3. zsarolóvírusok egészségügyben	C4. lakossági biztonságtudatosság
Dokumentumelemzés (M1)	+++	+	+++	+
Esetfeldolgozás struktúrált interjúval (M2)	-	-	+++	-
Kérdőíves felmérés (M3)	-	-	-	+++
Adatok másodlagos elemzés (M4)	-	+++	+	+

A bemutatás során az általános kutatásmódszertani sorrendet követem, és nem a célkitűzések sorrendjében mutatom be a módszertanokat.

3.1. Dokumentumelemzés (M1)

A dokumentumelemzés önálló módszertanként történő megjelenítését azért tartom relevánsnak kiemelni a dolgozatomban, mert elsősorban a téma újszerűsége, jellege és a magyar egészségpolitikai környezetben történő megjelenítése miatt a releváns dokumentumok áttekintésével is új tudományos érték teremthető. Emellett azért is érdemes külön megemlíteni, mert az új tudományterületek megjelenése kapcsán – és ilyen a kiberbiztonság - nemcsak a hagyományos tudományos irodalom, értekezések szolgálhatnak forrásként, hanem az ún. szürke irodalom is. Az információ gyors változása és a digitalizáció korában a szürke irodalom egyre fontosabbá válik, mivel gyakran tartalmaz olyan információkat és adatokat, amelyek nem érhetők el más forrásokból (Paez, 2017).

A szürke irodalom („gray vagy grey literature" – a vegyes írásmód is jelzi a terület újdonságát) olyan publikációkat foglal magában, amelyek nem jelennek meg hagyományos tudományos folyóiratokban vagy könyvekben: ilyenek lehetnek például nem publikált konferencia előadások, szakértői jelentések vagy munkaközi beszámolók. A téma jellege, sajátosságai miatt a fentiek mellett ide tartozhatnak olyan újságcikkek is, amelyek nem kerülnek tudományos szempontból feldolgozásra (pl. egy zsarolóvírus támadás), azonban az újszerűség miatt fontos a forrás említése, feldolgozása és ez alapján az adott probléma tudományos megközelítése.

Az egészségügyi kiberbiztonság területén ez az időszak hasonló, mint az orvoslás kezdeti időszakában, a tudományos publikációk hajnalán azok a kazuisztikai tanulmányok, amelyek az esetleírására törekedtek, és még nem is jutottak feltétlenül áttörő tudományos következtetésre, de az adott tünetegyüttes, vagy kórkép esetén hozzájárultak a tudományos ismeretterjesztéshez, illetve a tudományos megközelítés révén a következő eseteket már alaposabban, egy folyamatosan alakuló tudományos szempontrendszer szerint lehetett feldolgozni.

A „gray literature" dokumentumelemzés kapcsán nincs kiforrott módszertan, hogy mi szerint kellene, vagy lehetne beválogatni az ebből a forrásból származó dokumentumokat. Ezért olyan eljárást alkalmaztam, amely már megjelent tudományos publikációban: ezek célja az volt, hogy a grey literature-ből származó információkat is becsatornázzák egy-egy összefoglalóba („systematic review") (Paez, 2017) vagy eljárásrendi ajánlásba

(„guideline”) (Godin et al., 2015). Röviden összefoglalva: megfelelő internetes keresőmotort (Google Chrome) alkalmaztam és a keresést szűkítettem: keresősőszavak vagy kifejezések, dokumentum típus pdf, meghatározott időtartományban kerestem angol nyelvű dokumentumokat. A pdf típusú dokumentumokra szűkítésnek az oka az volt, hogy ezek a dokumentumok általában átesnek valamilyen szakmai lektoráláson, illetve azok kerültek beválogatásra, ahol feltüntetésre került az a szervezet, amely a kiadásért felel (pl. nemzetközi szervezethez köthető dokumentum). Ezek a keresések általában több ezer találatot eredményeztek, azonban ezek közül általában első 30-40 találat az, amely releváns az adott témában. A kutatási kérdésekhez kapcsolódó, de különböző keresési szavas találatok esetében kb. 60-70%-os átfedés volt tapasztalható.

2. táblázat: A dokumentumelemzés kapcsán használt főbb paraméterek összefoglaló táblázata (saját szerkesztés)

	C1: digitális egészségügyi ökoszisztéma	**C3: zsarolóvírusok egészségügyben**
Keresőszavak és kifejezések	#1„health digitisation and ecosystem”, #2:„digital healthcare and ecosystem”, #3:„digital health and ecosystem”, #4:„e-health and ecosystem”, #5:„data-driven health and ecosystem” WoS, Scopus: in Fields Title, Abstract, Keywords PudMed: in AllFields	#1:„ransomware”, #2:„ransomware and hospital”, #3:„ransomware and healthcare”, #4:„cybersecurity and hospital” WoS, Scopus: in Fields Title, Abstract, Keywords PudMed: in AllFields
Publikáció típusa	Áttekintő cikk	Áttekintő cikk
Időszak	2011 – 2020	2016 – 2020
Adatbázisok	Web of Science (W), Scopus (S), PubMed (P)	Web of Science (W), Scopus (S), PubMed (P)
Keresőmotor gray literature esetén	Google Chrome böngésző (a fenti kifejezések kiegészültek a „filetype:pdf” after:2011-01-01 before:2020-12-31 kifejezéssel)	Google Chrome böngésző (a fenti kifejezések kiegészültek a „filetype:pdf” after:2016-01-01 before:2020-12-31 kifejezéssel)
Kiválasztás	Relevancia szerint: - tudományos publikáció: absztrakt szakmai tartalma	Relevancia szerint: - tudományos publikáció: absztrakt szakmai tartalma

	alapján - gray literature: internetes böngésző által felajánlott 30 előre rangsorolt link szakmai tartalom áttekintésével	alapján - gray literature: internetes böngésző által felajánlott 30 előre rangsorolt link szakmai tartalom áttekintésével
Beválogatott, feldolgozott dokumentumok száma	Tudományos publikáció: 17 Gray literature: 11	Tudományos publikáció: 13 Gray literature: 15

3.2. Esetfeldolgozás struktúrált interjúval (M2)

A kórházi incidenseket, azon belül zsarolóvírus támadásokat tartalmazó esetek összeválogatása a Nemzeti Kibervédelmi Intézet (NKI), valamint a kórházakban dolgozó informatikusok által ismert esetekre korlátozódott, 2016-2019 közötti időszakot vizsgáltunk. A kritikus infrastruktúrákhoz tartozó intézményekben, így az egészségügyi intézményekben előforduló incidensek bejelentése az NKI (és jogelődei) felé jogszabály által meghatározott módon történik. A bejelentés során minimális adat szükséges, majd a bejelentést követően az esemény megítélése alapján történnek a szükséges lépések. A vizsgálati időszakra jellemző volt, hogy az esetek feldolgozása nem strukturált űrlapokon, hanem egy-egy rövid, folyószöveges formában került dokumentumtálásra. Az esetek kiválogatását 5 fős szakértői kör végezte. A szakértői kör személyenként legalább 10 éves szakmai tapasztalattal rendelkezett a saját területén, emellett több szakértő legalább 3 éves vezetői tapasztalattal is bírt. A főbb szakmai területek, amelyeket a szakértői kör reprezentált: informatika, egészségügyi informatika, elektronikus információs rendszerek menedzsmentje, információbiztonság, egészségügyi menedzsment, egészségügyi közgazdaságtan, általános orvoslás, jog. A kiválogatásnál elsősorban az volt szempont, hogy olyan esetek kerüljenek részletes feldolgozásra, amelyeknél az érintett szervezet informatikai vagy információbiztonsági vezetői ezt jóváhagyták, valamint amelyek valamilyen módon befolyásolták a szervezeti működést, és elsősorban a szervezet alapfolyamataira, elsődlegesen a betegellátásra voltak hatással. Emiatt ezek az esetek nemcsak az informatikai vagy információbiztonsági tapasztalatok összegzésére adtak lehetőséget, hanem a működési folyamatokra gyakorolt hatásuk is vizsgálható volt.

Ez a kiválasztás nem tekinthető reprezentatívnak. Azonban ezen szórványos esetek leírása és feldolgozása révén is sok tanulsággal és haszonnal jár mind az egyedi

felhasználók (informatikusok, információbiztonsági vezetők, egészségügyi intézmény vezetők) számára, mind rendszerszinten (hasonlóan, mint az orvosi kazuisztikai leírások). Az esetek áttekintése az alábbi fő szempontok mentén történt:

- milyen kórházban történt az eset - itt elsősorban annak a bemutatása volt szükséges, hogy az adott intézmény hogyan vesz részt a betegellátásban
- hogyan is történt az eset – mi volt a pontos „kórlefolyás”, hogyan került be a rosszindulatú kód, és milyen infrastruktúrát, alkalmazásokat, adatokat érintett
- mekkora hatással volt a támadás a kórház „üzleti” folyamataira és a betegellátásra (üzleti hatáselemzés - business impact analysis) – ezeket milyen mértékben érintette
- milyen tanulságokat lehet levonni az esetből, amely más kórházak számára is hasznos lehet

A kórházakban, mint kritikus infrastruktúrákban előforduló zsarolóvírus támadások dokumentáltsága erősen változó. Ez részint annak tudható be, hogy a támadás jellege miatt nem tudományos megközelítésű és alaposságú az esetek leírása, hanem sokkal inkább a gyakorlatra, a működőképeség visszaállítására fókuszálnak az esetek megtörténtekor. Ez azt is jelenti, hogy a vizsgálat időpontjában nem volt olyan tudományosan, vagy szakértői körökben ismertetett leírás, amely egy-egy kórházi zsarolóvírus támadás kapcsán a dokumentálás menetét, tartalmát meghatározta volna.

A feldolgozás módszertana szempontjából fontos, hogy tekintettel az esetek alacsony számára, nem használtunk olyan segédprogramot, amely nagyobb tömegű szöveg, hosszabb esetek vagy interjúk strukturált feldolgozást támogatná (pl. „categorial indexing”), hanem az egyéni szakértői kapacitásokkal történt meg a feldolgozás.

3.3. Kérdőíves felmérés (M3)

A lakossági felmérés során alkalmazott módszerek az alábbiakban részletesen bemutatásra kerülnek, beleértve a kérdőív fejlesztésének alapjául szolgáló szempontokat, a célcsoport meghatározásának folyamatát, a felmérés időzítését, a használt kommunikációs csatornákat, valamint a felmérés végrehajtásának módját.

Az országos szintű adatgyűjtés igénye miatt a kutatás kvantitatív módszertant alkalmazott, amelynek keretében egy online kérdőíves felmérést dolgoztunk ki, amely könnyen hozzáférhető volt a célközönség, azaz a digitális eszközöket használók számára.

Ez a megközelítés lehetővé tette, hogy a felmérés széles körben elérje az érintett populációt, ugyanakkor a digitális technológiák használatára korlátozódott.
Két külön kérdőív készült: az egyik a lakosságnak, a másik pedig szervezeteknek, elsősorban közigazgatási szerveknek és gazdasági társaságoknak szólt. Doktori kutatásomban kizárólag a lakossági kérdőív feldolgozásával foglalkoztam, a másik kérdőív kidolgozását és elemzését nem érintem.

A kérdések kialakításánál arra törekedtünk, hogy az általános szociodemográfiai jellemzők (életkor, nem, lakóhely, iskolai végzettség) mellett adatokat gyűjtsünk a válaszadók informatikai eszközhasználati szokásairól is, beleértve, hogy milyen típusú eszközöket használnak, és naponta hány órát töltenek ezekkel, akár magáncélból, akár munkahelyi kötelezettségeik miatt. Az információbiztonsági tudatosság vizsgálatához mind a lakosság, mind a gazdasági társaságok számára 20-20 kérdést állítottunk össze, amelyek alapjául más, hasonló nemzetközi kiberbiztonsági kérdőíves felmérések szolgáltak (Hadlington, 2017; Nunes et al., 2021). Bár a téma mélysége lehetővé tett volna egy hosszabb kérdőív kidolgozását, figyelembe vettük, hogy a túl hosszú kérdőívek csökkenthetik a válaszadók motivációját, ami sztereotipikus vagy kevésbé átgondolt válaszokhoz vezethet. Ezért a kérdőív terjedelmét úgy alakítottuk ki, hogy az egyensúlyt teremtsen az alapos adatgyűjtés és a válaszadók elkötelezettségének fenntartása között (Herzog & Bachman, 1981).

A vizsgálatot a nemzeti stratégiai intézkedési terv által meghatározott három fő kategória – tájékozottság, tudatosság és fenyegetettségi helyzet – alapján végeztük, figyelembe véve az alábbi szempontokat (Palicz et al., 2020)

- Tájékozottság: Ebben a témakörben azt vizsgáltuk, hogy a lakosság mennyire követi az IT-biztonsági híreket, és milyen mértékben tájékozódik az adatbiztonsággal kapcsolatos kérdésekben. Arra is kíváncsiak voltunk, mennyire ismerik azokat az intézményeken belüli lehetőségeket, ahová adatbiztonsági incidens esetén fordulhatnak, valamint mennyire vannak tisztában az online szolgáltatások által végzett adatgyűjtési gyakorlatokkal.
- Tudatosság: Ebben a kategóriában az információbiztonság alapvető gyakorlataira koncentráltunk, mint például a vírusirtó szoftverek használata, a biztonsági

frissítések telepítése, a jelszókezelés, illetve az email csatolmányok kezelésének biztonsága. Az adatvédelmi tudatosságot is vizsgáltuk, különösen az olyan mindennapi tevékenységek kapcsán, mint a weboldalakon használt sütik kezelése, az okoseszközök adatvédelmi beállításainak konfigurálása és az online szolgáltatások kiválasztásának körültekintő módja.

- Fenyegetettség: Itt azt elemeztük, hogy a lakosság mennyire tartja valószínűnek, hogy kibertámadások célpontjává válhatnak, például közösségi média profiljaik lemásolása és személyazonosságuk megszemélyesítése révén. Az ilyen fenyegetésekkel szembeni kitettségre és az ezekkel kapcsolatos percepciókra összpontosítottunk.

A 2020-ban végzett felmérés eredményei alapján módosított, 2021-ben kiküldésre került kérdőívet a 3. táblázat tartalmazza. Fontos módszertani megjegyzés, hogy az adatok feldolgozása szempontjából a válaszok pontosítása - a korábbi évekhez viszonyítva - nem jelentett problémát, mert az adatfeldolgozás során a válaszok értékelésénél a válaszokat tartalmilag értékeltük, elsősorban olyan szempontból, hogy a válasz mennyire mutatja a válaszadó biztonságtudatos viselkedését, vagy sem.

3. táblázat: A 2021-ben alkalmazott lakossági kérdőív és a válaszlehetőségek (saját szerkesztés)

**-al jelölve: a doktori értekezésben feldolgozott kérdések és válaszok

****1. Ön milyen gyakorisággal olvas IT biztonsággal kapcsolatos híreket?**
Egyáltalán nem olvasok ilyen témájú híreket.
Csak akkor, ha szembejön velem egy hírportálon, amit épp olvasgatok.
Csak akkor, ha valamelyik híresség is érintett benne.
Rendszeresen.
2. Regisztráció során Ön el szokta olvasni a weboldalak adatvédelmi szabályzatait?
Nem.
Csak gyorsan átfutom a számomra érdekes részeket.
Igen.
****3. Kérem, nevezze meg, hogy melyik szervezethez fordulhat, amennyiben Ön adatbiztonsági incidensben érintett!**
Nemzeti Incidenskezelési Hatóság
Nemzeti Adatbiztos
Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet
Nemzeti Adatvédelmi és Információszabadság Hatóság
Nem tudom
4. Ön szerint melyik online szolgáltatás tárol Önről adatokat? (Több választ is megjelölhet.)
Közösségi oldalak (Facebook, Instagram, TikTok, stb.)
E-mail szolgáltatók (gmail.com, protonmail.com, mail.com, freemail.hu, citromail.hu, stb.)
Kereső-motorok (Google, Yahoo, Bing, stb.)
5. Ön szerint miért gyűjtenek Önről adatokat internetes tevékenysége során? (Több választ is megjelölhet.)
Azért, mert így próbálják csökkenteni az online bűnözést.
Azért, mert a kormányok ennek segítségével gyűjtenek adatokat az állampolgárokról.
Azért, hogy személyre szabott célzott hirdetésekkel és tartalmakkal a képernyő előtt tartsanak.
Nem gyűjtenek adatot.
Nem tudom.
****6. Ön milyen gyakorisággal végez biztonsági frissítést eszközein?**
Amikor már nem tudom rendesen használni az eszközt.
Amint kijönnek a frissítések, és van rá időm.
Amint kijönnek a frissítések, mert be van állítva az automatikus frissítés.
Soha.
****7. A különböző online felületeken eltérő jelszavakat használ, vagy törekszik a minél kevesebb jelszó megjegyzésére?**
Eltérő jelszavakat használok.
Törekszem minél kevesebb jelszó megjegyzésére.
Nem válaszolok.
Nem tudom.
8. Webes böngészés során Ön hogyan kezeli a felugró süti (cookie) tájékoztatókat?
Elolvasás nélkül, bezárom.
Kizárólag a weboldal működéséhez szükséges süti-engedélyeket adom meg, és bezárom az ablakot.
Megadom az összes süti-engedélyt, és bezárom az ablakot.
9. Ön átlagosan milyen adatvédelmi beállításokat alkalmaz eszközein (pl.: okostelefonján)? (Több választ is megjelölhet.)
A gyári beállításokat, semmit nem módosítok.
Képernyőzárat.
A nem használt funkciókat (például a GPS, Bluetooth, stb.) kikapcsolom.
Felülvizsgálom a hozzáférési jogosultságokat, és letiltom azokat, amik nem szükségesek a működéshez.
Semelyiket.

10. Egy online szolgáltatás igénybevétele során Ön milyen mértékben ellenőrzi biztonsági és megbízhatósági szempontból az adott szolgáltatást?
Alaposan utánajárok, híreket és véleményeket olvasok a szolgáltatásról.
Az igénybevétel előtt elolvasom más felhasználók véleményeit.
Ezek egyáltalán nem szoktak érdekelni, ha funkcióiban jól működik a szolgáltatás.
****11. Használ-e a számítógépén/laptopján vírusirtó szoftvert?**
Igen, fizetős verziót, ami magától frissül.
Igen, ingyenes verziót, amit rendszeresen frissítek.
Igen, ingyenes verziót, de nem foglalkozom a frissítéssel.
Nem.
Nem válaszolok.
Nem tudom.
12. Milyen gyakran módosítja az online felületek eléréséhez szükséges jelszavait?
Rendszeresen.
Amikor a felület/alkalmazás kéri.
Csak ha üzenetet kapok, hogy megpróbáltak bejutni a fiókomba.
Soha.
Nem válaszolok.
Nem tudom.
****13. Kérjük, fejezze be a mondatot! Az e-mail üzenetekkel érkező csatolmányokat Ön…**
a levél tartalmától függően megnyitja (pl.: számlabefizetéssel kapcsolatos értesítők, banktól beérkező levelek, stb.).
kizárólag akkor nyitja meg, ha megbízható forrásból érkezett a levél.
azonnal megnyitja.
soha nem nyitja meg.
****14. Kérjük, fejezze be a mondatot! Zsarolóvírusnak nevezzük azokat a rosszindulatú programokat, amelyek…**
ellopják a felhasználók jelszavait.
titkosítják a számítógépes eszközön tárolt adatokat.
nem tudom.
15. Az alábbi lehetőségek közül Ön melyiket preferálja okoseszközök képernyőzárának feloldásához? (Több választ is megjelölhet.)
Arcfelismerés
Jelszó
Minta rajzolása
PIN kód
Ujjlenyomat
16. Ön milyen jellegű adatokat tárol magán célra használt számítógépes eszközein az alábbiak közül? (Több választ is megjelölhet.)
családi fényképeket és videókat
magáncélú üzeneteket (SMS, e-mail, chat)
saját jelszavakat
munkahelyi dokumentumokat
orvosi leleteket
pénzügyi dokumentumokat
szolgáltatói szerződések eredeti példányát szkennelve
bizonyítványok szkennelt változatát
17. Milyen mértékű bizalomvesztést eredményezne Önnél, ha kiderülne, hogy egyik szolgáltatója felhasználói adatokat szivárogtat ki?
Azonnal szolgáltatót váltanék.
Átnézném a megosztott adataimat, és szigorítanám az adatvédelmi beállításokat.
Attól függ, hogy mennyire érzékeny adatok szivárogtak ki.
Semmilyet, ha továbbra is működnek a funkciók.
Nem válaszolok.
Nem tudom.

18. Nyilvános Wi-Fi használat esetén milyen tevékenységeket szokott végezni az eszközein? (Több választ is megjelölhet.)
Bejelentkezés online szolgáltatásokba (pl.: e-mail fiók ellenőrzése, netbank használata, közösségi média felületek használata, stb.).
Böngészés hírportálokon.
Dokumentumok, fájlok letöltése.
Nem használok nyilvános Wi-Fi hálózatot.
Nincs válasz.
19. Elképzelhetőnek tartja-e, hogy egy közösségi oldalon valaki az Ön nevében profilt hozzon létre (lemásolja a profilját)?
Igen, elvégre elég sok nyilvánosan elérhető adatot, képet és információt osztok meg magamról.
Nem, mégis ki akarna engem megszemélyesíteni?
Nem, mert minimális adatot osztok meg magamról és azok hozzáférését is szigorúan korlátozom.
20. Ön használja az okoseszközei (pl.: tablet, TV, okos háztartási gépek) azon funkcióját, hogy egy hálózatra csatlakoztathatóak és szinkronizálhatóak egymással a kényelmes használat érdekében?
Az okos számítógépes eszközökön és okostelefonon kívül nem használok okoseszközöket.
Igen, hiszen ezek az eszközök azért okosak, hogy kényelmesen használhassuk azokat.
Igen, mert nem értek annyira a technológiához, viszont nagyon kényelmes azok használata.
Nem, hiszen így az egyik eszközöm kompromittálódásával a többi eszköz is sérülhet, vagy hozzáférhetővé válik.
Nem, mert bár vannak okos eszközeim, de nem látom az előnyeit azok összehangolásának.

Az elkészült kérdőíveket az Európai Bizottság által biztosított EUSurvey webes platformon tettük közzé, amelyet adatvédelmi és információbiztonsági szempontból is megfelelőnek találtunk, hiszen mind hazai, mind uniós szabályozásoknak eleget tesz, és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) is ezt használja.

A kérdőíveket három fő kommunikációs csatornán publikáltuk: weboldalakon (elsősorban az NKI és EMK platformjain), közösségi médiafelületeken (intézményi Facebook- és LinkedIn-oldalakon), valamint közvetlen e-mailes megküldéssel, amelyet gazdasági és közigazgatási szereplőknek továbbítottunk.

Az online kérdőíveket első alkalommal 2020. október 28-november 30. között publikáltuk. Az ott kapott eredményeket feldolgoztuk, publikáltuk a felmérés módszertanát és az első év eredményeit (Palicz et al., 2022). Az eredmények alapján minimálisan módosítani kellett a kérdéseket és válaszokat, elsősorban annak érdekében, hogy a kérdések és a válaszok a laikus válaszadók számára is egyértelműek legyenek. A doktori kutatásban feldolgozásra kerülő kérdéseket 2021. október 15 - november 16. között tettük elérhetővé. Abban az évben összesen 1516 kitöltött kérdőív került elektronikusan benyújtásra.

A beérkezett adatokat először tisztítottuk. Az adattisztítási folyamat során áttekintettük az adatokat, majd elsősorban logikailag értékeltük, illetve a nem megfelelő formátumú adatokat külön jelöltük. Ki kell emelni, hogy 2020-ban még a születési évet kértük (később életkort) és így ezt átalakítottuk életkorra (életkor = 2020-születési évszám),

majd ezt követően az életkorokat korcsoportokba és generációkba soroltuk, amelyet a 4. táblázat mutat be (Veteránok, Baby-boom, X, Y, Z, Alfa generációk).

4. táblázat: Digitális generációk születési idejének táblázata (saját szerkesztés)

Generáció megnevezése	**Születési év - alsó**	**Születési év - felső**
Alfa generáció	2011	--
Z generáció	1996	2010
Y generáció	1981	1995
X generáció	1966	1980
Baby boom	1946	1965
Veteránok	--	1945

Korrigálható hibák esetén az értékeket átírtuk (pl. életkor helyett valaki a születési évét írta be), viszont a nem megfelelő rekordokat töröltük (például 0 életév). Ezek a hibák vélelmezhetően a kitöltés során, az adatbevitelkor kerültek az adatbázisba.

A leíró statisztikai adatok esetében vizsgáltuk a nemi, a generációs összetételt, a település szerinti megoszlást, az iskolai végzettséget, valamint a digitális eszközök számát és a digitális eszközzel töltött napi óraszámot is megnéztük, ezek százalékos megoszlását. Emellett a kérdésekre adott válaszok %-os megoszlását is vizsgáltuk.

Az összehasonlító statisztikai elemzések kivitelezésénél több esetben a kapott eredmények dichotomizálására került sor. Ezt alkalmaztuk a szociodemográfiai tényezők esetében (például a település vagy az iskolai végzettég szerinti kategóriák esetében, ez utóbbinál például megvizsgáltuk mindkét dichotomizált csoportot: egyikben az általános iskola-középiskola által adott válaszok alkottak egy nagyobb csoportot az egyetemiekkel szemben, míg a másik esetben az általános iskolai válaszokat vetettük össze a középiskolai-egyetemi csoport által adott válaszokkal). A szakmai kérdéscsoportokra adott válaszok dichotomizálásánál azt a szakmai szempontot vettük figyelembe, hogy a kérdésekre adott, biztonságtudatosság szempontjából kedvező és kedvezőtlen (nem biztonságtudatos viselkedésre utaló) válaszok kerültek a két csoportba. Ezzel kapcsolatban két példát mutatok be:

1. biztonságtudatosság szempontjából kedvező, ha valaki rendszeresen olvas IT biztonsággal kapcsolatos híreket, és nem csak akkor, ha egy hírportálon szembe találkozik egy ilyen hírrel, vagy egyáltalán nem olvas.
2. ehhez hasonlóan a kedvező válaszokat jelentett a 11. kérdés esetén (11. Használ-e a számítógépén/laptopján vírusirtó szoftvert?"), ha a válaszadó az alábbiakat jelölte meg: „Igen, fizetős verziót, ami magától frissül." vagy „Igen, ingyenes verziót, amit rendszeresen frissítek." Itt mindkét válasz a „biztonságtudatos" kategóriába került (dichotomizálás érték 1). A többi válaszlehetőség esetén a „nem biztonságtudatos" dichotomizált értéket kapta a válaszadó (dichotomizálás érték 0).

Arra minden esetben figyeltünk, hogy a magasabb érték, kötődjön a biztonságtudatosabb viselkedési cselekvésekhez.

Az eredeti lakossági kérdőív feldolgozása során nem került sor valamennyi kérdés elemzésére. Ennek két szakmai oka volt:

1. 2020-as értékelést követően azonosítottuk, hogy vannak olyan kérdések, amelyek esetében pontosítani kell a kérdést, vagy a válaszokat kell egyértelműbbé tenni. Ezért a 2021-es év értékelése szempontjából kiestek azok a kérdések, amelyeknél a kérdés megfogalmazása, vagy a válasz jelentősebben változott.
2. ettől fontosabb szempont volt, hogy bár bizonyos kérdések válaszai érdekesek lehettek, szakmai szempontból nem minden esetben voltak relevánsak az eredeti formájukban. Ennek következtében az eredetileg megfogalmazott húsz kérdés közül kilencet választottunk ki, amelyeket összehasonlító statisztikai elemzésnek vetettünk alá (C-D csoport, lásd 8. táblázat).

Az összehasonlító statisztikai elemzések során Khí-négyzet próbát alkalmaztunk annak vizsgálatára, hogy a dichotomizált demográfiai adatok és a számítógép-használattal kapcsolatos információk milyen összefüggést mutatnak a biztonságtudatosságra vonatkozó kérdések dichotomizált válaszaival (biztonságtudatos vagy nem biztonságtudatos magatartás). Végezetül megvizsgáltuk, hogy a különböző biztonságtudatossággal kapcsolatosan feltett szakmai kérdésekre adott válaszok között van-e összefüggés: ha egy csoport az egyik kérdésnél (pl. vírusirtó használat) a biztonságtudatos viselkedést választja, akkor jellemző-e, hogy egy másik, hasonló

kérdésnél (pl. jelszóhasználatnál) szintén a biztonságtudatos viselkedésre utaló választ jelöli meg. Ezt egy mátrixban tüntettük fel, a vizsgálati éveket külön-külön bemutatva.
A statisztikai elemzések során a szignifikancia szintjét $P<0,05$ értékben határoztuk meg. Az adatok feldolgozásához és elemzéséhez az SPSS 27 szoftvert használtuk (IBM Corp., 2020. IBM SPSS Statistics for Windows, Version 27.0, Armonk, NY: IBM Corp.).

3.4. Adatok másodlagos elemzése (M4)

A ***C2. Biztonságos innovatív adathasznosítás célkitűzés*** kapcsán a COVID 19 pandémiához kapcsolódóan a magyar államigazgatásban létrehozott Operatív Törzs döntéselőkészítési tevékenységét támogató elemzésekhez készültek adatfeldolgozási módszertanok, amelynek használatához egy megfelelő információbiztonsági környezetet kellett teremteni. Az önálló tevékenység mellett (amely elsősorban az információbiztonsági környezet megteremtését célozta) ebben a munkacsoportban mint teamtag is részt vettem az innovatív elemzési módszertanok kidolgozásában és alkalmazásában.
Az adatmennyiség és az adatok jellege meghatározta, hogy milyen környezetet kellett biztosítani. Az elemzések kapcsán a piacot közel 100%-ban lefedő három mobilszolgáltató (piaci részesedésük 2019 végén 44,8%, 27,2% és 26,7% volt) biztosított anonimizált adatokat. (Nemzeti Média- és Hírközlési Hatóság (NMHH), 2020). A három távközlési vállalat 2019. december 15 - 2020. május 20. közötti időszakban napi Call Detail Records (CDR) adatokat szolgáltatott, és a kutatócsoporttal együttműködve dolgozta ki a módszertant és adott tanácsot adott a nyers adatok értelmezéséhez. (Szócska et al., 2021). Ez az időszak a COVID-19 világjárvány első magyarországi hullámát fedte le: több, mint egy hónappal az első azonosított esetek előtt, a kijárási tilalom időszaka, illetve a mozgáskorlátozások fokozatos feloldásának időszaka, 2020. április 30. után (Szerencsés et al., 2021).
A Call Detail Records (CDR) tárolja az egyes kommunikációs munkamenetek (pl. hívások, sms küldés, adatforgalom) helyadatait (készülék és cellatorony helye), amely adatok a telefonszolgáltató által aggregálhatók, így teljes mértékben biztosítható az anonimizált adatkezelés. Azonban ezek az aggregáltságú adatok alkalmasak arra, hogy megfelelő mutatók (indexek) képzése révén a vizsgált időszakban jellemezzék egy

nagyobb csoport (pl. település lakosai) készüléke és a cellatorony közötti kommunikáció intenzitását, amelyből a mozgásokra lehet következtetni.
Az adatok feldolgozásához a Microsoft Power BI Pro szoftvert használtuk.

4. Eredmények

A kutatási eredményeket a Célkitűzések, kutatási kérdések és hipotézisek fejezetben használt tagolás alapján mutatom be.

4.1. A digitális egészségügyi ökoszisztéma

C1. célkitűzés: Annak feltárása és bemutatása, hogy a digitalizáció révén létrejövő, megváltozó digitális egészségügyi rendszer egységes szempontok alapján leírható és értékelhető (rövidítve: C1: digitális egészségügyi ökoszisztéma).

K1.1. kutatási kérdés: Leírható-e a digitalizációs átalakulás során megváltozó egészségügy rendszer egy ökoszisztémaként? Ennek milyen elemei vannak és ezeket mi jellemzi Magyarországon?

Az ökoszisztéma fogalmának alkalmazása nem tekinthető újdonságnak, hiszen a szakirodalom régóta használja ezt a kifejezést különböző területek és azok elemeinek definiálására. Az ökoszisztéma alapvető sajátossága, hogy elemei egymással szoros kapcsolatban állnak, és kölcsönös függőség figyelhető meg közöttük (James F. Moore, 1993). Ez azt jelenti, hogy ha valamelyik elem túlsúlyba kerül a többihez képest, az rövid időn belül a rendszer egyensúlyának megbomlásához, sőt akár működésének bizonytalanságához vezethet. Az ökoszisztéma, mint modell mindig magában hordoz némi egyszerűsítést, a lényeg kiemelését, így nem szükséges, hogy teljes mértékben tükrözze a valóságot. Ugyanakkor elengedhetetlen, hogy a modell alapján a rendszer működése megérthető, leírható és modellezhető legyen.

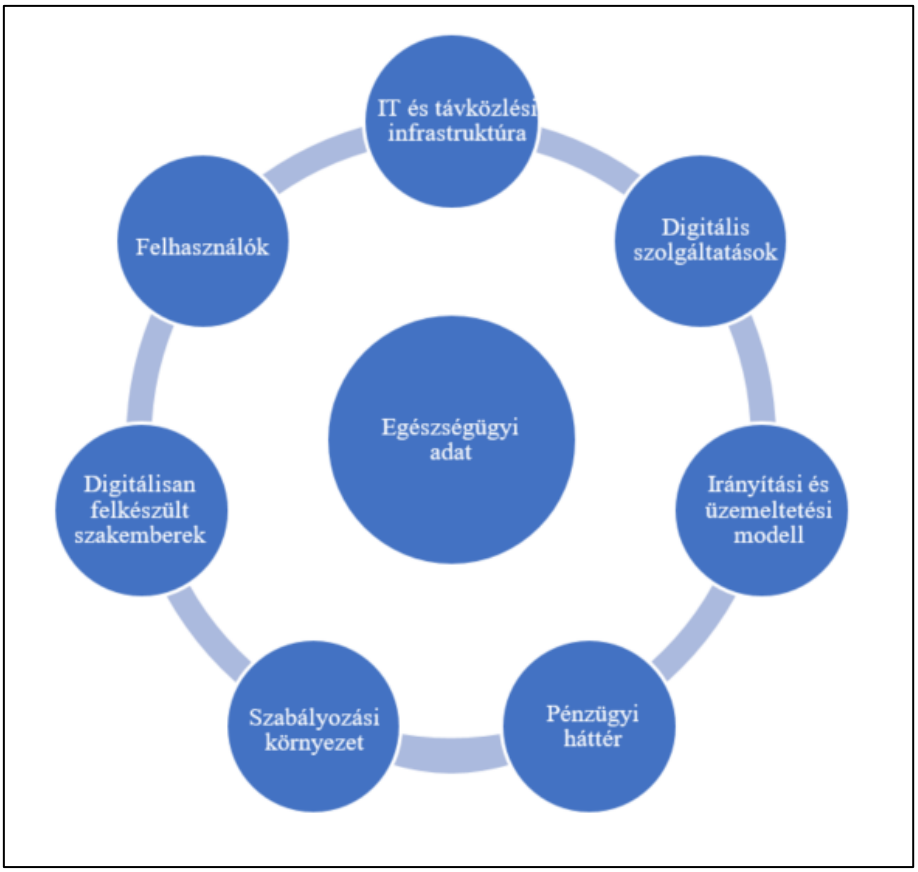
Egy adott szakterület fejlesztése akkor lehet igazán eredményes, ha a stratégiában megfogalmazott célok és az azokhoz kapcsolódó beavatkozások az ökoszisztéma minden elemét érintik, biztosítva az egyensúlyt az egyes komponensek fejlesztési folyamata és az elért fejlettségi szintek között. Ez az egyensúly megőrzése magában foglalhatja a források megfelelő elosztását, de a szabályozó környezet kialakítását is.

Ezen logika mentén beszélhetünk például innovációs ökoszisztémáról, startup ökoszisztémáról vagy digitális ökoszisztémáról. Mivel a digitális technológiák ma már szinte minden gazdasági ágazatban alapvető szerepet töltenek be, indokolt az igény egy

olyan modell meghatározására, amely kifejezetten az egészségügy digitális ökoszisztémáját írja le.

Önmagában a digitális egészségügyi ökoszisztéma fogalma sem ismeretlen, azonban erre vonatkozóan egyértelmű meghatározás nincs, amely talán azzal is magyarázható, hogy az egészségügyi rendszerek és azok fejlődése rendkívül nagy változatosságot mutat.

A digitális fejlesztéseink és az ezzel összhangban levő megalapozó, szintetizáló irodalomkutatások, valamint a digitális egészségügy területén végrehajtott projektek alapján egy modellt alkottunk. A mi modellünk középpontjában az egészségügyi adat áll, mert ez az entitás az, amely a digitális egészségügyi ökoszisztéma legfontosabb, legértékesebb eleme illetve ez az, ami az ökoszisztéma elemei között az egyik legfontosabb összekapcsolódást jelenti. Erre építve lehet az egészségüggyel kapcsolatos egyéni vagy rendszerszintű döntéseket meghozni, a döntések hatásait nyomon követni, értékelni, és az egészségügyi adat az, amely a legfontosabb mozgatórugója, drivere a rendszernek. Adatot generál a felhasználó, a szolgáltató a szolgáltatás révén, de akár az IT infrastruktúra is (és itt akár szélesebb értelemben is használhatjuk: minden olyan, az egészségügyben használt eszköz, ami IT alapú): gondoljunk csak az ún. „machine data”-ra (pl. log file-okra, működést, üzemeltetést támogató adatokra), amely lehetővé teszi, hogy egy infrastrukturális elemre vonatkozóan adatot kapjunk és ez alapján pl. az adott entitás kihasználtságát értékeljük, a karbantartásokat és üzemszüneteket a használattal összhangban megtervezzük, vagy éppen a működési sajátosságokat, munkafolyamatokat is vizsgáljuk (ki honnan, milyen készülékről, milyen időben jelentkezett be, honnan kapott vagy hova továbbított adatot az adott digitális eszköz, mennyi időt vett igénybe egy adott munkafolyamat). Adatot tárolnak az infrastrukturális elemek, de az adat az alapja az egészségügyi innovációnak is. Az adathoz kapcsolódnak és az adatra (business vagy machine data) épülnek a különböző komponensek: irányítási és üzemeltetési modell, IT és távközlési infrastruktúra, digitális szolgáltatások, szabályozási környezet, finanszírozási háttér, digitálisan felkészült szakemberek, felhasználók.



7. ábra: A digitális egészégügyi ökoszisztéma elemei (saját szerkesztés) (Szabo et al., 2021)

A kutatás alapján megalkotott modell (7. ábra) elmeinek a magyar környezetben megjelenő kihívásait az alábbiakban mutatom be (Szabo et al., 2021).

I. Irányítási és üzemeltetési modell

Az egészségügyi digitalizáció kapcsán nem jött létre megfelelően kialakított irányítási és üzemeltetési modell. Több esetben a jelenlegi egészségügyi, és azon beül a digitális egészségügyi irányítást párhuzamba állítják a közigazgatással, amelynek hátterében részben a 2011-es CLIV. törvény hatályba lépését követően megindult egészségügyi szolgáltatások centralizációja áll (Magyar Országgyűlés, 2011). A centralizációval összhangban megindult az ellátórendszer újragondolása is, azonban annak konzekvens végrehajtása 2014-2015-ben megakadt. A tényleges ellátási szükségleteken alapuló szolgáltatások és kapacitások újraszervezése nem történt meg, amely következetesen azzal jár, hogy az ezeket támogató infokommunikációs szolgáltatások sem koherens, és

konzekvens, a külső környezetre reagálni képes, de meghatározott közép- és hosszútávú célok irányába mutató stratégiák és ezzel szinkronban levő szervezeti és irányítási modell mentén alakultak. A centralizációs törekvések valamint a közigazgatással sok párhuzamot felmutató digitális egészségügyet is érintő irányítási modell kialakítása felerősödött a 2022-es kormányváltást követően, amikor is az ágazat, és az azt támogató digitális szolgáltatások kormányzati felelőssége a Belügyminisztériumhoz került.

Napjainkban is jellemző, hogy a korszerű hátteret biztosító digitális infrastruktúrát és szolgáltatásokat, illetve annak szereplőit, valamint az egészségügyi ágazati informatikai területet más-más kormányzati szereplő irányítja, és ez együtt jár a stratégiai és az operatív szintek kompetíciójával, amely jelen esetben inkább káros, mint hasznos.

Habár történtek előre lépések, azonban jelenleg is hiányzik egy átfogó, központi kormányzati szinten kidolgozott, az ágazati stratégiát támogató digitális egészségügyi stratégia, valamint az adatok hasznosítására vonatkozó koncepciók és irányelvek. Operatív szinten az informatikai üzemeltetés továbbra is alapvetően decentralizált módon történik, egységes üzemeltetési sztenderdek nélkül. Az információbiztonsági háttér nem megfelelően biztosított, és az egyes intézmények informatikai üzemeltetését jellemzően saját hatáskörben, sok esetben alvállalkozók bevonásával végzik.

II. Informatikai (IT) és távközlési infrastruktúra

A technológia folyamatos fejlesztése alapvető feltétele az egészségügyi szolgáltatások modernizációjának. Ehhez elengedhetetlenek a konszolidált informatikai és távközlési rendszerek, amelyek biztosítják az adatok átjárhatósága mellett a megfelelő interoperabilitást, valamint az adatok biztonságos tárolását és felhasználását. Az egészségügyi intézmények központi (szervertermek, adatközpontok, hálózati eszközök stb.) és végponti infrastruktúrája jelentős korszerűsítésre szorul. Talán az ágazati informatikai rendszer (EESZT) kivétel ez alól, hiszen az a Kormányzati Adat Központban került elhelyezésre.

Az elavult infrastruktúra nemcsak a napi üzemeltetés során okoz problémákat – mivel a meglévő eszközök és technológiák nem működnek megfelelően –, hanem akadályozza az új technológiai innovációk zavartalan bevezetését és működését is. Gondoljunk például az 5G technológiát igénylő robotikára, a felhőalapú megoldásokra vagy a mesterséges intelligenciára, amely nagy mennyiségű adat feldolgozását igényli. Ezek az innovációk

csak modern és megfelelően karbantartott infrastruktúra mellett válhatnak a mindennapi egészségügyi gyakorlat részévé.

III. Jogi és szabályozási környezet

A folyamatosan változó jogszabályi környezet, a nem egyértelmű alapelvek mentén történő szabályozás, valamint a bizonyos területeken tapasztalható szabályozási hiányosságok – például a nagy adathalmazok, adatkapcsolatok és másodlagos adathasznosítás kérdéseiben – hátrányosan érintik az egészségügyi szektort. Ez különösen problémás, hiszen Magyarország jelentős egészségügyi adatvagyona számos kutatási, fejlesztési és innovációs lehetőséget hordoz, amelyek a megfelelő szabályozási keretek hiányában nem aknázhatók ki.

Példaként említhető, hogy 2018-ban munkacsoportunk javaslatot tett egy digitális egészségügyi módszertani és adatközpont létrehozására. Ez az adatközpont a leírt megközelítések alapján olyan szabályozási és fejlesztési koncepciókat alakított volna ki, amelyek támogatják az egészségügyi adatok felhasználását és az innováció megvalósítását. Azonban a kormányon belüli eltérő prioritások és nézőpontok miatt a javaslat nem valósulhatott meg.

Az elmúlt években az Európai Unióban lezajlott, adatközponú fejlesztési irányok felerősödése egyértelművé tette, hogy a szabályozási környezet területén jelentős előrelépés szükséges Magyarországon: elsősorban az Európai Egészségügyi Adattérre (European Health Data Space – EHDS) gondolok ennek kapcsán.

IV. Digitálisan felkészült szakemberek

A digitális egészségügyben dolgozók digitális készségeinek folyamatos fejlesztése elengedhetetlen, és ma már tudatosan fejlesztett, önálló kompetenciaterületként kell kezelni. Minden területen előrelépés szükséges: a digitális platformokon történő információszerzés és adatfeldolgozás; a digitális eszközök használata a tanulás, tanítás és önfejlesztés során; az online térben való hatékony kommunikáció és együttműködés; a technikai jártasság, amely magában foglalja a digitális problémamegoldást és a technikai akadályok elhárítását; valamint az alkotás, innováció és kutatás digitális technológiák alkalmazásával. Szintén fontos a digitális identitás kezelése és a biztonság megteremtése.

Az egészségügyi szektorban dolgozók digitális felkészültsége terén javítani kell a digitális írástudást, és biztosítani kell, hogy képességeik elérjék legalább az átlagos polgároktól elvárható szintet. Ezen túlmenően egyes területeken támogatást kell nyújtani a magasabb szintű digitális kompetenciák kialakításához, hogy az ágazat szereplői hatékonyan alkalmazkodhassanak a digitális technológiák nyújtotta lehetőségekhez és kihívásokhoz.

V. Felhasználók, ügyfelek

A felnőtt lakosság digitális készségei Magyarországon elmaradnak az EU-átlagtól. Ezt évek óta jelzik az uniós felmérések, amelyek a DESI, majd az azt váltó Digital Decade Index révén – többek között a humántőke területén is – mérik a lakosság digitális felkészültségét. A magyar adatok mindkét mutató esetében jelentős lemaradást mutatnak az uniós átlaghoz képest, és a tagországok között az utolsó harmadban helyezkednek el.
A digitális egészségügyi ökoszisztéma hatékony működéséhez elengedhetetlen, hogy a lakosság megszerezze és folyamatosan fejlessze alapvető infokommunikációs ismereteit és készségeit. Emellett szükséges a specifikus, ágazati vagy intézményi folyamattámogató és ügyfélbarát alkalmazások használatának oktatása is. Ezáltal biztosítható, hogy a digitális egészségügyi szolgáltatások mindenki számára hozzáférhetőek és hatékonyak legyenek.

VI. Szolgáltatások

Az egészségügyi digitalizáció fejlesztése egyszerre érinti az egészségügyi szolgáltatók által biztosított elektronikus lehetőségek (pl. szolgáltatások, alkalmazások) bővítését és elérhetőségének javítását, valamint az intézmények belső működésének kiterjedt elektronizálását. Bár a lakosság számára elérhető online egészségügyi szolgáltatások köre folyamatosan bővül, jelenleg még mindig szűkösnek tekinthető. Néhány esetben már jelen vannak alapszintű elektronikus megoldások, például időpontfoglaló rendszerek, azonban további fejlesztésekre van szükség. Hiányoznak például a megelőzést támogató online platformok, mobilalkalmazások, valamint a kezeléseket és utógondozást segítő, biztonsági és dokumentációs elvárásoknak megfelelő kommunikációs rendszerek, amelyek az egészségügyi dolgozókkal való kapcsolatot is megkönnyítik. Ezen fejlesztések esetében fontos, hogy ne egy-egy egyedi alkalmazás kerüljön kifejlesztésre,

hanem lehetőség szerint országos szinten bevezethető és kiterjeszthető szolgáltatásról legyen szó, hiszen ezzel érhető el a megfelelően biztonságos működés, valamint a méretgazdaságosságból fakadó előnyök. A fentiek mellett rendkívül alacsony a hordozható eszközök elterjedtsége, és a hozzájuk kapcsolódó alkalmazások és szolgáltatások is korlátozottak. Az egészségügyi szolgáltatást nyújtó intézmények honlapjai sok esetben elavultak, átláthatatlanok, és tartalmi, formai, valamint biztonsági megújításuk sürgető feladat.

A szervezeti működés fejlesztése terén a legnagyobb kihívások közé tartozik a korszerű kórházi információs rendszerek (HIS) kiépítése és fejlesztése, továbbá azok az interfészek, amelyek biztosítják az egészségügyi adatok hazai és nemzetközi kommunikációját és cseréjét. Ez magában foglalja az adatkapcsolatot az egyes intézmények, valamint az intézmények és az ágazati irányítás között. Szintén kiemelt jelentőségű a belső folyamatalapú működéstámogató rendszerek fejlesztése. Ezek a speciális egészségügyi szervezési szoftverek alapvető hozzájárulást jelenthetnek a modern digitális egészségügy megvalósításához, mivel hatékonyabbá és átláthatóbbá teszik az intézmények belső működését, jelentősen támogathatják az adminisztratív folyamatokat, ezáltal csökkentve a betegellátásban dolgozók adminisztratív és szervezési terheit.

VII. Pénzügyi háttér, finanszírozás

A fejlesztések és a megfelelő színvonalú üzemeltetés alapfeltétele, hogy elegendő pénzügyi forrás álljon rendelkezésre. Az egészségügyi intézmények többségében tartósan van jelen a forráshiány, amely szükségszerűen együtt jár egyfajta pazarlással is (a forráshiány okozta késedelmes kifizetéseket a szállítók beárazzák és beépítik az áraikba, ad hoc igényekre kell reagálni, a tervezhetőség szempontjai háttérbe szorulnak). Ezért az egészségügyre, különösen az informatikai fejlesztésekre és üzemeltetésre szánt közkiadások felülvizsgálata kiemelten fontos feladat. Már a rövidtávú tervezés és menedzselés során is jelentős támogatást nyújthatnak a digitális technológiák.

Külön figyelmet érdemel, hogy mind ágazati, mind intézményi szinten újra kell gondolni azt a 2004 óta fennálló gyakorlatot, amelynek értelmében a digitális egészségügyi fejlesztések szinte kizárólag az Európai Unió Strukturális Alapjainak támogatásával valósultak meg. Ez a függőség hosszú távon akadályozhatja a fenntartható és önálló

fejlesztések megvalósítását, ezért a források diverzifikálása és a hazai finanszírozás megerősítése kulcsfontosságú.

4.2. Biztonságos innovatív adathasználat

C2. célkitűzés: Annak bemutatása, és gyakorlati példával igazolása, hogy az egészségügyi adatokhoz biztonságos környezetben más adatok is kapcsolhatók, és ezen innovatív adathasznosítások olyan értéktöbbletet eredményeznek, amely kormányzati döntéselőkészítési és döntéshozatal szinten is megjeleníthető (rövidítve: C2: biztonságos innovatív adathasznosítás).

K2.1. kutatási kérdés: Hogyan és milyen módszertannal lehet hasznosítani a digitális egészségügyön kívül keletkezett adatokat, egy globális vagy lokális egészségbiztonsági eseményhez kapcsolódva? Hogyan biztosítható, hogy az adatvédelmi szabályoknak és kiberbiztonsági követelményeknek megfeleljen ez a módszertan?

A mindennapi működés során keletkező, üzleti és gépi adatokat (business and machine data) tartalmazó adatbázisok rekordjaira egyre inkább úgy tekintenek, mint az evidencia alapú, tudományos politika és programalkotás egyik fontos erőforrása. Ezen adatok és adatbázisok összekapcsolása és innovatív módszerekkel történő elemzése kritikus fontosságú (Munné, 2016). Tudjuk azt is, hogy a helyes döntéshozatal szempontjából az egyik legfontosabb szempont, hogy a rendelkezésünkre álló, és/vagy birtokunkban levő adatok esetében a BSR-nek teljeskörűen érvényesülnie kell, egyébként a meglevő adataink nem használhatók döntésre vagy döntéselőkészítésére. A COVID-19 pandémia alatt bevezetett, a lakosság mozgási aktivitását csökkenteni célzó intézkedések hatásának nyomon követésére a mobilkommunikációs cégektől kapott cellaadatok (Call Detail Records, CDR) ideálisnak tűntek, azonban a megfelelő feldolgozáshoz ki kellett alakítani azt a biztonságos környezetet, amivel biztosítottuk a BSR érvényre jutását.

A megkapott adatokat (mennyiségi és minőségi szempontból) az alábbiakkal jellemezzük:

- a megkapott adatmennyiség közel 1,2 TerraByte volt
- a rekordok tárolása 6 ténytáblában, 2 dimenziótáblában 1 log táblában és 26 data management táblában történt
- a ténytáblákban összesen közel 4,3 milliárd rekord tárolása történt meg.

Ki kell emelni, hogy az átadott adatok esetében a CDR-en alapuló mozgásmeghatározás ideális „felbontási” és adatbiztonsági szintet tett lehetővé: egyrészt teljes mértékben

anonimizált adatok kerültek hozzánk adatfeldolgozási szempontból (nem lehetett azonosítani senkit), másrészt a CDR adatokkal be lehetett mutatni a mozgási aktivitást, anélkül, hogy az egyedi, és nagy pontosságú GPS adatokat használtuk volna.

Az ötlet megvalósítása során számos, elsősorban technikai probléma merült fel. Nem volt teljesen világos, hogy hogyan oldható meg a különböző telekommunikációs cégek által eltérő formátumban előállított adatok egységes adatbázisba rendezése (Szócska et al., 2021). További kihívást jelentett annak biztosítása, hogy a személyes adatok védelmét szolgáló jogszabályi előírások, például az Európai Unió általános adatvédelmi rendelete (GDPR – General Data Protection Regulation), maradéktalanul érvényesüljenek. Emellett a nagyadatok biztonságos tárolása és kezelése szintén kiemelt figyelmet igényelt. Munkacsoportunk a három nagy magyar mobilszolgáltatóval együttműködve olyan módszertant dolgozott ki és egy olyan döntéstámogató rendszert hozott létre, amely hatékonyan kezelte ezeket a technikai megvalósíthatósági problémákat. A rendszer létrehozásának legfontosabb lépései, illetve elemei a következők voltak.

1. **kockázatértékelés és előzetes hatásvizsgálat elvégzése**

A kockázatértékelés és előzetes hatásvizsgálat célja az volt, hogy azonosítani lehessen: a kialakításra kerülő rendszer milyen jellegű adatokat tartalmaz, mennyire vannak személyes, vagy érzékeny adatok a rendszerben.

.

2. **információbiztonsági feltételek megteremtése**

Az információbiztonsági feltételek megteremtése előtt szükséges volt kisebb infrastrukturális fejlesztés, amely részint érintette a hálózati kapacitásokat (sávszélesség bővítés optikai kábellel) illetve a kormányzati biztonságos kommunikációt (Nemzeti Távközlési Gerinc - NTG csatlakozás)

Fizikai biztonság megteremtése alapvető lépés minden biztonsági intézkedés kapcsán, bármennyire is triviálisnak tűnik. Ezek a mi esetünkben az alábbiak voltak:

- 0-24 órás portaszolgálat rendszeresítése, portaszolgálat teendőinek meghatározása
- szerverszobába belépés személyre szóló mágneskártyával (veszélyhelyzet esetében kulccsal) lehetséges

- szerverszoba belső tere és a belépés teljeskörűen, folyamatosan nagyfelbontású kamerával megfigyelt

Adminisztratív védelmi intézkedések kialakítása: a szervezet szabályozottsága nem tette szükségessé külön szabályzat létrehozását, azonban a megfelelő munkautasítások kiadása megtörtént, illetve külön dokumentum készült az adatok használatáról, hozzáférésekről, a jogosultságok kiadásáról. A hozzáféréseket és jogosultságokat a biztonságért felelős vezetőként én határoztam meg.

Logikai védelem kialakítása: az adatok elérése többlépcsős azonosításon keresztül valósult meg. A rendszert tűzfal védi,

- első lépésben a VPN (Virtual Private Network) felhasználónévvel, jelszóval és egy tanúsítvánnyal biztosítja a biztonságos kapcsolódást
- az adatbázis elérését biztosító serverre való bejelentkezés érdekében további authentikációra van szükség.
- végezetül az adatbázisba való bejelentkezéshez szükséges újabb authentikációra.
- a VPN-ről készül log állomány, amelyet rendszeresen ellenőriznek

3. **adatkezelői és adatfeldolgozói nyilvántartások létrehozása, adatokkal feltöltése**
4. **kutatócsoport tagok és egyéb szereplők, adatfeldolgozók meghatározása, szerződések megkötése**

Ennél a két lepésnél a legfontosabb a teljeskörűség volt: vagyis mindenki kerüljön nyilvántartásba aki a kialakított rendszerrel és adatokkal bármilyen módon kapcsolatba kerül, legyen egyértelmű, hogy milyen ponton találkozik az adattal, milyen jogosultság szükséges a feladatai elvégzéséhez, és ezek írásban is rögzítésre kerüljenek.

5. **kutatócsoport működési rend kialakítása**

A kutatócsoport működési rendje és információbiztonság szempontjából kritikus pont volt a nyers, deperszonalizált adatok átvétele külső szolgáltatótól, amelyre egyszemélyi felelőst neveztünk ki. Ezt követte a belső, szervezeten belüli fizikai adatátadás, majd az adatok szerverre másolása. A másolás közben az egyes fázisoknál kötelezően ellenőrizni kellet az állományok sértetlenségét igazoló SHA állományt. A nyers adatok rendszerbe kerülését követően indult meg azok adatbázisba töltése, tisztítása, és további előkészítése a kutatómunkához.

Az adatok másolása, és végleges helyre kerülését követően a 3+2+1 szabálynak megfelelően online és offline másolatok (backupok) lettek létrehozva.

A létrehozott biztonságos adatkörnyezetben a döntés előkészítést és döntéseket támogató képességre egy példát mutatok be, amelyet a munkacsoport hozott létre

Példa 1: Az ábrán bemutatjuk a „otthonmaradási" és „mozgási" indexeket, amelyeket a fent ismertetett módszertan alapján alakítottunk ki, valamint ezek magyarországi alakulását a közvetlenül a járvány kitörése előtti időszaktól az első hullám legaktívabb szakaszáig (8. ábra). Ez világosan mutatja a 2020. márciusában bevezetett kormányzati lépések eredményességét, illetve az intézkedések előtti, a felvásárlási láz által előidézett kiugrásokat.

A módszertan lehetőséget nyújtott arra is, hogy települési szintű adatokat elemezzünk, így a helyi szintű eltérések és kiugrások pontosan nyomon követhetők. Ez megalapozhat célzott, lokalizált intézkedések bevezetését, amelyek jelentősen növelhetik a korlátozások eredményességét. Az ilyen célzott beavatkozások csak azokon a területeken lépnek életbe, ahol ténylegesen szükségesek, elkerülve, hogy felesleges többlet terheket rójanak azokra a településekre és lakosokra, akik felelősségteljesen viselkednek.

8. ábra: A "mozgási" (kék), illetve az "otthonmaradási" (zöld) indexek grafikus ábrázolása 2020. január – 2020. április között (COVID-19 járvány magyarországi első hullámának időszaka) (saját szerkesztés)

4.3. Zsarolóvírusok az egészségügyben

C3. célkitűzés: Annak bemutatása, hogy az egészségügyben keletkező adatok sértetlensége, bizalmassága és rendelkezésre állása kritikusan fontos a működés szempontjából, és ezt a kibertérből a zsarolóvírus támadások kapcsán reális veszély fenyegeti a kórházak esetében is (rövidítve: C3: zsarolóvírusok az egészségügyben).

K3.1. kérdés: Milyen hatással voltak a zsarolóvírus támadások a magyar kórházak működésre, és milyen mértékben érintették a kórházi informatikai és információs rendszereket, beleértve a szállítói lánc részeként működő szakmai területeket?

K3.2. kérdés: Hogyan, milyen szempontok és kérdések mentén lehet az eseteket megfelelően összegyűjteni és elemezni annak érdekében, hogy megállapítható legyen: mely funkciók milyen mértékben károsodtak az adott egészségügyi intézményben?

A bemutatott módszertan alapján négy esetet dolgoztunk fel, amelynek forrásait a Módszertani részben mutattam be.

Eset-1 - Megyei Kórház

A 700 ágyas megyei kórház 2016 áprilisának egyik péntekén szokatlan eseménysorozattal szembesült (Palicz et al., 2021). Az egyik osztály telefonos bejelentést tett, hogy az asztali gépeken tárolt Excel fájlok fokozatosan eltűnnek, helyüket pedig ismeretlen fájlok veszik át. A bejelentés után azonnal lekapcsolták az összes szervert, értesítették az osztályvezetőket, és az intézményben minden számítógépet leállítottak. Életbe lépett a vészhelyzeti terv, amelynek keretében az informatikai csapat gyors helyzetértékelést végzett, és jelentésben meghatározta az esemény súlyosságát. Eközben a vezetőség a tájékoztatásért és a sajtóval való kommunikációért felelt, míg az informatikai szakemberek kidolgozták a probléma kezelésének stratégiáját.

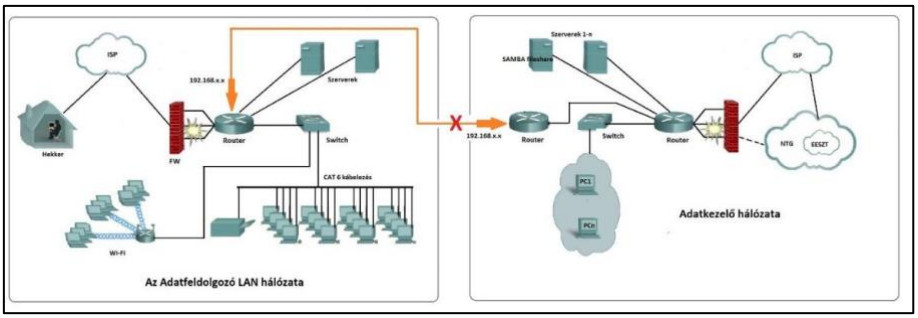
A vizsgálat során kiderült, hogy a támadás egy e-maillel indult, amely Moszkvából, egy egyszerű felhasználótól érkezett. Az e-mailt a kórház titkárságán nyitották meg, de az üzenet forrását már nem lehetett visszakövetni. Utólagos elemzés alapján valószínűsíthető, hogy a moszkvai felhasználó több „ajándék” programot töltött le, amelyek között rosszindulatú szoftverek, úgynevezett trójai programok is voltak. Ezek a

programok a háttérben megnyitották az eszközén azokat a hálózati portokat, amelyek külső szerverekkel való kommunikációt tettek lehetővé anélkül, hogy a felhasználó ezt észlelte volna. A támadó ezután a moszkvai felhasználó számítógépét felhasználva indította el a zsarolóvírust, amely végül a kórház rendszerét is elérte.
Az incidens során a klinikai tevékenység nem sérült, az informatikai rendszerben csak 1-1 végponton volt átmeneti (1-3 óráig) tartó működési zavar.
Ennek az esetnek a legfontosabb tanulságai:

- az informatikai rendszerben és végpontokon jelentkező rendellenes működésről az informatikai rendszer üzemeltetését végzőket és az információbiztonságért felelős személyeket a lehető leghamarabb tájékoztatni kell.
- az informatikai és információbiztonsági szereplőknek azonnali beavatkozást kell tenni a helyzet eszkalálódásának megelőzése érdekében.
- jelentősen segíti a veszélyhelyzetekben a megfelelő működést és cselekvéseket, ha az intézmény rendelkezik ilyen helyzetekre alkalmazható tervekkel, amelyeket gyakorolnak is.

Eset-2 - Megyei Kórház

Egy 800 aktív ágyas, megyei szintű betegellátást végző kórház az egészségügyi ellátás folyamatos biztosítása érdekében több szakmai szolgáltatóval kötött szerződést (Palicz et al., 2021). Ezek a közreműködők különböző szakmai és diagnosztikai szolgáltatásokat nyújtottak, például képalkotó diagnosztikát, laboratóriumi vizsgálatokat és patológiai szolgáltatásokat. A szakmai szolgáltatók saját informatikai rendszereket üzemeltettek, amelyek saját szervereken és kliens gépeken futottak, különálló internetkapcsolattal és internetszolgáltatóval.
A kórház és a szolgáltatók közötti hálózati kapcsolatot általában egy-egy aktív hálózati elosztón (routeren) keresztül biztosították, amely összekötötte a kórházi rendszert a közreműködők informatikai infrastruktúrájával. Ez a megoldás lehetővé tette az együttműködést, ugyanakkor informatikai szempontból kockázatokat is rejtett magában, mivel a hálózatok közötti közvetlen kapcsolat növelte a biztonsági rések kihasználásának lehetőségét (9. ábra).



9. ábra: A kórházi és a patológiai rendszer logikai kapcsolatának vázlatos rajza (saját szerkesztés) (Palicz et al., 2021)

2018 decemberében, egy péntek délelőtt (9:30-kor) jelezték, hogy a titkárság egyik számítógépén tárolt állományok elérhetetlenné váltak, amit az adatfájlok titkosítása okozott. A „fertőzés" gyorsan terjedt: néhány percen belül (9:36-ra) további 11 munkaállomás vált működésképtelenné, majd a kiszolgáló szerver is érintetté vált, amely valójában egy munkaállomás volt, szerverként használva. Ugyanezen reggelen a szakmai szolgáltató is értesítette a kórház informatikai üzemeltetését arról, hogy hálózatuk és eszközeik működése rendkívül lelassult. A probléma megoldására többszöri újraindítást kíséreltek meg, azonban ezek nem hoztak eredményt. A szakmai szolgáltató szerverének vizsgálata során felfedezték a zsarolóvírus képernyőüzenetét, amely megerősítette a fertőzés tényét.

Bár a támadás idején a kórház és a szakmai szolgáltató informatikai rendszerei egy fájlmegosztó szolgáltatás révén össze voltak kötve, a kórházi rendszerek közvetlenül nem váltak érintetté. Ennek ellenére az incidens jelentős fennakadásokat okozott a kórház működésében, és a szolgáltatások helyreállítása több napot vett igénybe. A kórházi rendszerekben klinikai adatvesztés nem történt, azonban a szakmai szolgáltatónál az adatok egy részét nem sikerült teljeskörűen visszaállítani.

Ennek az esetnek a legfontosabb tanulságai:

- a kórházi rendszerbe szállítókon, alvállalkozókon keresztül is kerülhetnek be rosszindulatú programok.
- ezek terjedése nagyon gyorsan történhet.
- bármilyen működési zavar esetén a kórházi informatikai rendszer működtetéséért felelős személyeket értesíteni kell, mert ők tudják leggyorsabban izolálni, szegmentálni a problémát.
- ehhez megfelelő riasztási, értesítési rendszer kidolgozása szükséges.

Eset-3 – Országos Intézet

A nem budapesti székhelyű országos intézet - nevének megfelelően - az ország minden részéről fogadott egy szervrendszerhez tartozóan akut és rehabilitációs ellátásra szoruló betegeket, körülbelül 400 ágyon.

A kórház informatikai rendszerére jellemző volt, hogy régi, elavult infrastruktúra biztosította az informatikai működést: számos rendszer DOS alapú volt, a kliensek jellemzően nem kapcsolódtak az internetre, és a Windows XP rendszerek jelszó nélküli belépéssel működtek. A szerverek (általában Windows szerverek) rendelkeztek publikus IP-címekkel, belső és külső hálózati kártyákkal, azonban hiányzott a megfelelő tűzfal beállítás, és a megosztott könyvtárak a publikus internet felé is nyitva voltak. A helyi informatikusok képzését nem támogatta a kórház, így ők korlátozottan rendelkeztek korszerű hálózati és információbiztonsági ismeretekkel.

2017. áprilisában a katasztrófavédelem jelzése alapján egy vírustámadás jeleit azonosították, amely miatt a helyi informatikai csapat lekapcsolta a szervereket. Ez azonban működési zavart eredményezett: a rendszerek nem működtek, a betegellátás akadozott, problémás volt a képalkotó vizsgálatok „megrendelése”, illetve a leletek megérkezése az osztályokra.

Ebben a helyzetben a menedzsment részéről a legfontosabb döntés az volt, hogy új informatikai osztályvezetőt kérték fel a probléma megoldására, aki gyorsan cselekvési tervet állított össze, beleértve a fertőzött szerver azonosítását, cseréjét, az adatok visszaállítását, és hivatalos tájékoztatást a katasztrófavédelemnek. Ez az új informatikai szakember rendelkezett már incidenskezelési tapasztalattal, illetve az alapvető információbiztonsági és kiberbiztonsági ismeretek birtokában volt.

A beavatkozást követően a rendszer fokozatosan, néhány napon belül helyreállt, de az infrastruktúra biztonságosabbá tétele hosszabb időt vett igénybe. Az azonnali lépéseket követően a biztonsági szint növelésének az egyik legfontosabb feltétele a munkatársak képzése volt, amely bizonyos esetekben együtt járt a munkatársak minőségi cseréjével. A biztonsági szint növelésének fontos komponense volt, hogy az EESZT bevezetésével általában javítani kellett az infrastruktúra helyzetét és a biztonság növelése érdekében is lépéseket kellett tenni, amelyért a menedzsmentnek is felelősséget kellett vállalni.

Az incidens azonnali, és több napon keresztül tartó működési zavart okozott, jelentős erőforrás igénye volt a helyreállításnak, és a fenntartható biztonságos működés további plusz erőforrások (emberi és pénzügyi) bevonását igényelte.
Ennek az esetnek a legfontosabb tanulságai:

- nem megfelelően képzett informatikai csapat információbiztonsági problémát okoz.
- incidens kapcsán a korábbi tapasztalatok nagyon sokat érnek, lehetőség szerint ilyen személy(eke)t igénybe kell venni.
- a probléma megoldásába be kell vonni a szállítókat és a környezetben dolgozó, megbízható informatikai és információbiztonsági szakértőket.
- a vezetésnek közvetlenül és közvetetten is kiemelt felelőssége van a biztonságos környezet kialakításában.

Eset-4 – Megyei kórház

2019-ben egy májusi napon a déli órákat követően a körülbelül 800 ágyas, aktív és krónikus ellátást is biztosító megyei kórház osztályairól az informatikai munkatársaknak jelezték, hogy nem tudják a kórházi rendszerben a klinikai dokumentumokat előállítani. A HIS rendszer fájlszervere elérhető volt, azonban a korábban .rtf kiterjesztésű fájlokat adobe fájlokká alakították át. Emellett találtak egy .txt állományt is, amely tájékoztatott arról, hogy az állományok titkosításra kerültek.
Első lépésként a központi, szerverszobában levő hálózati elosztókat lekapcsolták a hálózatról, miközben az osztályokat is megkeresték, hogy a gépeket kapcsolják le az informatikai hálózatról, és indítsák újra hálózati kapcsolat nélkül. A teljes intézményt végig kellett járni, hogy mindenki értesüljön a történésekről és a legfontosabb teendőkről. Az intézmény valamennyi végpontját ellenőrizték, illetve a központi és megosztott mappák ellenőrzése is megtörtént. A HIS rendszer indítókörnyezetét tartalmazó mappa nem sérült, amely elsősorban a szerencsének volt köszönhető. A különböző sérült állományokról rendelkezett az intézet offline mentésekkel, amely lehetővé tette illetve jelentősen meggyorsította a helyreállítást. A végpontokon levő gépek csak akkor kerültek vissza a hálózatra, amikor meggyőződtek, hogy a gépek nem fertőzöttek, és nem tartalmaznak titkosított állományt illetve rosszindulatú kódot (malware).

Ezt követően a kórház saját szakértelemre és erőforrásra támaszkodva megpróbálta kideríteni, hogy hogyan került be a fertőzés, azonban érdemben nem jutottak előre. Az akut történést követő napokban a munkatársak még jeleztek olyan gépeket, ahol találtak titkosított állományokat: ezek jellemzően ott fordultak elő, ahol a rendszergazda tudomása nélkül hoztak létre publikusan megosztott könyvtárakat. Itt a helyreállítás esetleges volt, mert ezekről a mappákról nem voltak rendszerszintű, offline mentések.
Későbbi vizsgálatok során kiderült, hogy a munkatársak egy része (főként aki távleletezést végez) olyan otthoni környezetből jelentkezik be, amely biztonsági szempontból kockázatos: nincsenek megfelelő frissítések, nincs végpontvédelem, illetve a külső eszközök miatt a tulajdonos általában adminisztrátori jogosultsággal rendelkezik, amely a legkülönbözőbb, nem ellenőrizhető programok telepítését teszi lehetővé.

Ennek az esetnek a legfontosabb tanulságai:

- nem volt olyan központi kapcsolat, amely biztos, hiteles tudást biztosított volna a kórházi rendszerben dolgozók részére, ezért személyes kapcsolatokon keresztül („hallottak már róla") tájékozódtak, illetve határozták meg a teendőket.
- több feladatot párhuzamosan kell végezni és koordinálni, amely a teljes intézmény tekintetében jelentős erőforrást igényel mind szakmai, mind koordinatív szempontból.
- az intézet rendelkezett külső mentésekkel, ami jelentősen könnyítette a helyreállítást.
- a nem rendszergazdák által létrehozott nem megfelelő jogosultsággal rendelkező publikus könyvtárak jelentették az egyik legnagyobb veszélyt a fertőzés szempontjából.
- a kórházak (egészségügyi intézmények) esetében a külső (fizikailag nem kórházban levő) munkavégzés különösen magas kockázatot jelentett, hiszen azokat külső (nem a kórház által tulajdonolt és felügyelt) számítógépeket és hálózati eszközöket nem ellenőrizték, illetve a kórházi informatikai hálózatba történő becsatlakozásuk sem biztonságos csatornán keresztül történt.

4.4. Lakossági biztonságtudatosság

C4. célkitűzés: Annak vizsgálata, hogy van-e összefüggés a demográfiai jellemzők valamint informatikai használati szokások és a kiberbiztonsági tudatosság között (rövidítve: C4: lakossági biztonságtudatosság)

H4.1. hipotézis: Feltételezésem szerint a magyar lakosság esetében a biztonságtudatos magatartás nincs összefüggésben kor, nem, iskolázottság és informatikai használati szokásokkal

A szociodemográfiai és az eszközhasználatra vonatkozó részletes adatokat az 5. táblázat mutatja be.

Szociodemográfiai jellemzők

A 2021-es év válaszainak száma 1516 volt, a válaszadók többsége férfi volt (57,65%). Alacsony százalékban (1,06%) előfordultak olyan válaszadók is, akik nem kívánták megadni nemi hovatartozásukat.

A válaszok esetén életkort kértünk, azonban a feldolgozásnál és elemzésnél már a digitális generációba soroltuk be a válaszadókat. 2021-ben a legtöbb válasz az X generációtól érkezett (33,58%), majd csökkenő sorrendben a Baby boomerek (25,59%), az Y generáció (20,18%) és végül a Z generáció (18,73%) adtak választ a kérdésekre.

A területi megosztás tekintetében Budapesten lakók (34,76%) adták a legtöbb választ, majd a városban (27,77%), a megyei jogú városokban (21,83%), és végül az egyéb településeken (15,63%) lakók válaszoltak.

Az iskolai végzettség esetében a felsőfokú végzettségűek tették ki a válaszadók több, mint felét (58,64%), a középiskolai válaszadók aránya valamivel kevesebb, mint egyharmad volt (30,41%), míg az általános iskolai végzettséggel rendelkezők a válaszadók egytizedét alkották (10,95%).

Ezen adatok alapján is kijelenthető (összhangban az adatgyűjtés módszertanával), hogy a felmérés nem volt reprezentatív az alapvető szociodemográfiaia tényezőket figyelembe véve, a felmérésből származó következtetéseket ezért csak óvatosan szabad általánosítani.

Eszközhasználat

Az eszközök típusát tekintve elmondható, hogy a legmagasabb penetrációval az okostelefon rendelkezik: a válaszadók 93,73%-a rendelkezett mobil telefonkészülékkel. Szintén magas volt a válaszadók között a laptop (83,18%) és a számítógép (60,82%) használók aránya. A tablet használat már kevesebb, mint a válaszadók felér volt jellemző (43,01%), míg az egyéb mobil okoseszköz esetén jóval kisebb (11,74%-27,11% között) penetrancia volt jellemző.

Az elektronikus eszközök használati idejét az jellemezte, hogy a munkahelyen a kitöltők többet használták az eszközöket, mint otthon: 2021-ben a válaszadók közel 30%-a legalább 6, de kevesebb, mint 9 órát használta az informatikai eszközöket. Ezzel szemben az otthoni használatra az volt jellemző, hogy a többség (40,24%) legalább 3, de kevesebb, mint 6 órát használta azokat. Általában elmondható, hogy a válaszadók kb. 21% a munkahelyén nem használt informatikai eszközt (vagy nem árulta el), ezzel szemben ugyanez a szám az otthoni eszközhasználatra vonatkozóan jóval kisebb, mert csak 5% körüli. Vagyis – feletehetőleg munkahelytől és az ellátott feladatoktól függően – az otthoni informatikai eszközhasználat sokkal több válaszadó esetében jellemző.

5. táblázat: A 2021-es lakossági biztonságtudatossági országos felmérés szociodemográfiai és eszközhasználati válaszok száma és aránya (saját szerkesztés)

	2021	
Nem	**N**	**%**
Férfi	874	57,65
Nő	626	41,29
Nincs adat	16	1,06
Digitalis generáció	**N**	**%**
Alfa generáció	0	0,00
Z generáció	284	18,73
Y generáció	306	20,18
X generáció	509	33,58
Baby boom	388	25,59
Veteránok	29	1,91
Tartózkodási hely	**N**	**%**
Egyéb	237	15,63
Város	421	27,77
Megye jogú város	331	21,83
Budapest	527	34,76
Iskolázottság	**N**	**%**
Általános iskola	166	10,95
Középiskola	461	30,41
Főiskola/egyetem	889	58,64
Eszközök (többválasztós kérdés)	**N**	**%**
Számítógép	922	60,82
Laptop	1261	83,18
Tablet	652	43,01
Okostelefon	1421	93,73
Okosóra	411	27,11
Okoskarkötő	178	11,74
Okos háztartási eszköz	395	26,06
Eszközök használata naponta (óra - munkahely)	**N**	**%**
Nem válaszolok	67	4,42
Nem használok informatikai eszközöket	252	16,62
Kevesebb, mint 3 órát	325	21,44
Legalább 3, de kevesebb, mint 6 órát	273	18,01
Legalább 6, de kevesebb, mint 9 órát	442	29,16
Legalább 9 órát	157	10,36
Eszközök használata naponta (óra - szabadidő)	**N**	**%**
Nem válaszolok	71	4,68
Nem használok inofrmatikai eszközöket	6	0,40
Kevesebb, mint 3 órát	482	31,79
Legalább 3, de kevesebb, mint 6 órát	610	40,24
Legalább 6, de kevesebb, mint 9 órát	230	15,17
Legalább 9 órát	117	7,72

Biztonságtudatosságra vonatkozó szakmai kérdések és a válaszok

A részletes adatokat a 6. táblázat mutatja be.

Az IT biztonsággal kapcsolatos hírolvasásra vonatkozó kérdésünk esetében 2021-ben a válaszadók kicsit több, mint harmada (35,36%) azt válaszolta, hogy „Rendszeresen", míg a válaszadók kicsit több, mint fele (52,57%) pedig azt jelölte be, hogy „Csak akkor, ha szembejön vele egy hírportálon, amit éppen olvas".

A válaszadók legnagyobb része megtudta mondani, hogy kihez kell fordulni (NAIH – 37,99%) abban az esetben, ha adatbiztonsági incidens éri őket, azonban nem elhanyagolható azon válaszadók száma sem, akik NBSZ-NKI-t jelölték meg (24,41%). A válaszadók több, mint egyharmada vagy rosszat jelölt meg (2,77%), vagy egyáltalán nem tudta a választ (34,83%).

A biztonsági frissítéssel kapcsolatban a válaszadók túlnyomó többsége az automatikus frissítést preferálja (64,91%), azonban jelentős számú azok aránya is, akik csak akkor frissítenek, ha van rá idejük (27,31%). A válaszadók 7,78% vagy egyáltalán nem frissít, vagy csak akkor, ha már működési gondot tapasztal a gépén.

A válaszadók kicsivel több, mint 60% törekszik különböző jelszavak használatára, míg közel egyharmad (31,93%) minél kevesebb jelszót szeretne megjegyezni.

A vírusirtót szoftvert használó és azt rendszeresen frissítők aránya közel 80% volt, függetlenül attól, hogy fizetős, vagy ingyenes verziót használt-e a válaszadó. A válaszadók közel 20%-ának nem volt fontos, hogy megfelelő, naprakész vírusírtó legyen a készülékén.

A levélcsatolmányokkal kapcsolatban a válaszadók 72,10%-a tudatosan viselkedett, mert elsődlegesen azt vett figyelembe, hogy honnan érkezett a levél. Az esetek közel egynegyedében (24,74%) a válaszadók a döntést a levél tartalma alapján hozták meg.

A zsarolóvírusok ismerete általában jellemző volt a válaszadókra, szinte pontosan a válaszadók kétharmada (66,42%) fejezte be jól a megkezdett mondatot. A fennmaradó egyharmadnyi válaszadó vagy pontatlanul tudta, vagy nem ismerte, hogy mit jelent, a fogalom.

A nyilvános wifi használatra vonatkozóan általában jellemző, hogy a többség (53,83%) semmilyen tevékenységre nem használja, ezzel szemben 16,75% ezeken a hálózatokon keresztül internetes szolgáltatásokat is igénybe vesz.

Végül az álprofil képzéssel kapcsolatban a válaszadók többségénél (60,95%) a minimális adatmegosztás volt jellemző

6. táblázat - 1: A 2021--es lakossági biztonságtudatossági országos felmérés szakmai kérdésekre adott válaszok száma és aránya (saját szerkesztés)

	2021	
****1. Ön milyen gyakorisággal olvas IT biztonsággal kapcsolatos híreket?**	**N**	**%**
Egyáltalán nem olvasok ilyen témájú híreket.	170	11,21
Csak akkor, ha szembejön velem egy hírportálon, amit épp olvasgatok.	797	52,57
Csak akkor, ha valamelyik híresség is érintett benne.	13	0,86
Rendszeresen.	536	35,36
****3. Kérem, nevezze meg, hogy melyik szervezethez fordulhat, amennyiben Ön adatbiztonsági incidensben érintett!**	**N**	**%**
Nemzeti Incidenskezelési Hatóság	25	1,65
Nemzeti Adatbiztos	17	1,12
Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet	370	24,41
Nemzeti Adatvédelmi és Információszabadság Hatóság	576	37,99
Nem tudom	528	34,83
****6. Ön milyen gyakorisággal végez biztonsági frissítést eszközein?**	**N**	**%**
Soha.	35	2,31
Amikor már nem tudom rendesen használni az eszközt.	83	5,47
Amint kijönnek a frissítések, és van rá időm.	414	27,31
Amint kijönnek a frissítések, mert be van állítva az automatikus frissítés.	984	64,91
****7. A különböző online felületeken eltérő jelszavakat használ, vagy törekszik a minél kevesebb jelszó megjegyzésére?**	**N**	**%**
Nem tudom.	14	0,92
Törekszem minél kevesebb jelszó megjegyzésére.	484	31,93
Eltérő jelszavakat használok.	930	61,35
Nem válaszolok.	88	5,80
****11. Használ-e a számítógépén/laptopján vírusirtó szoftvert?**	**N**	**%**
Nem tudom.	64	4,22
Nem.	101	6,66
Igen, ingyenes verziót, de nem foglalkozom a frissítéssel.	133	8,77
Igen, ingyenes verziót, amit rendszeresen frissítek.	750	49,47
Igen, fizetős verziót, ami magától frissül.	438	28,89
Nem válaszolok.	30	1,98

6. táblázat - 2: A 2021--es lakossági biztonságtudatossági országos felmérés szakmai kérdésekre adott válaszok száma és aránya (saját szerkesztés)

	2021	
****13. Kérjük, fejezze be a mondatot! Az e-mail üzenetekkel érkező csatolmányokat Ön…**	**N**	**%**
azonnal megnyitja. (2020: "mindig megnyitja" szerepelt a válaszok között)	25	1,65
a levél tartalmától függően megnyitja (pl.: számlabefizetéssel kapcsolatos értesítők, banktól beérkező levelek, stb.).	375	24,74
kizárólag akkor nyitja meg, ha megbízható forrásból érkezett a levél.	1093	72,10
soha nem nyitja meg.	23	1,52
****14. Kérjük, fejezze be a mondatot! Zsarolóvírusnak nevezzük azokat a rosszindulatú programokat, amelyek…**	**N**	**%**
nem tudom.	123	8,11
ellopják a felhasználók jelszavait.	386	25,46
titkosítják a számítógépes eszközön tárolt adatokat.	1007	66,42
****18. Nyilvános Wi-Fi használat esetén milyen tevékenységeket szokott végezni az eszközein? (2020: Egyszeres választás, 2021-2022: Több választ is megjelölhet.)**	**N**	**%**
Bejelentkezés online szolgáltatásokba (pl.: e-mail fiók ellenőrzése, netbank használata, közösségi média felületek használata, stb.).	254	16,75
Böngészés hírportálokon.	641	42,28
Dokumentumok, fájlok letöltése.	128	8,44
Nem használok nyilvános Wi-Fi hálózatot.	816	53,83
Nincs válasz.	4	0,26
****19. Elképzelhetőnek tartja-e, hogy egy közösségi oldalon valaki az Ön nevében profilt hozzon létre (lemásolja a profilját)?**	**N**	**%**
Igen, elvégre elég sok nyilvánosan elérhető adatot, képet és információt osztok meg magamról.	380	25,07
Nem, mégis ki akarna engem megszemélyesíteni?	212	13,98
Nem, mert minimális adatot osztok meg magamról és azok hozzáférését is szigorúan korlátozom.	924	60,95

Khi2 próbák eredményei

A kutatás tárgyát képező 2021-es évben megvizsgáltam a lehetséges összefüggéseket a különböző független és függő változók között.

A szignifikancia vizsgálatok eredményét egy mátrixban tüntettük fel. A mátrix elrendezése logikailag ugyanolyan, mint egy kereszttábla esetében, vagyis az első oszlopban (amely a sorokat határozza meg) találhatok a függetlennek tekintett, míg a felső sorban (vagyis az oszlopok meghatározásaként) a függő változók.

A mátrixban a szignifikancia szinteket a színek erősségével jeleztük: a legenyhébb szín esetében éppen eléri a p értéke a szignifikancia szintet, míg a legerősebb színek esetén (zöld és sárga) a p értéke kisebb, mint 0,001 ($p<0,001$). A két szín használatának oka, az, hogy zölddel jelöltük azt, ha a nominális vagy ordinális változók nagyobb értékei között lehet a kapcsolat, míg sárga színnel a fordított/inverz összefüggésre utalunk.

Egy konkrét példa: 2021-ban a nem és az IT hírek olvasása közötti kereszttábla és összefüggés vizsgálat (7. táblázat):

7. táblázat: „Nyers" kereszttábla, amely a 2021-as adatokkal a nem és az IT hírek olvasási gyakoriságának megoszlását mutatja be esetszámmal és gyakorisággal (saját szerkesztés)

Crosstab - Kereszttábla						
				IT hírek olvasási gyakorisága - di		
Vizsgálat éve				Nem, vagy esetlegesen olvas	Rendszeresen olvas	Total
2021	Neme	Férfi	Count	465	409	874
			% within Neme	53,20%	46,80%	100,00%
		Nő	Count	505	121	626
			% within Neme	80,70%	19,30%	100,00%
	Total		Count	541	970	530
			% within Neme	49,5%	64,70%	35,30%

$p<0,001$

Vagyis ebben az esetben a nem, mint független változó (vagy befolyásoló változó) (nominális, férfi:1, nő:2) és az IT hírek olvasási gyakorisága (nem vagy esetlegesen:0, rendszeresen:1) között erős szignifikancia mutatható ki ($p<0,001$): fordított a kapcsolat (ezért került sárgával jelzésre), mert a férfiak esetében jellemzőbb a rendszeres hírolvasás.

Áttekintettük a különböző változók és biztonságtudatosság közötti lehetséges kapcsolatokat (8. táblázat,) és az eredmények közül az alábbiakat emelem ki:

1. a nem (A01) tekintetében szinte egyértelműnek tűnik az összefüggés: a férfiak biztonságtudatosabbak, és ez statisztikai összefüggést mutat az eszközök magasabb számával, a gyakoribb eszköz használattal, a rendszeres IT biztonsági hírek olvasásával, valamint a biztonságtudatos viselkedési mintákkal (vírusirtóhasználat, jelszóhasználat, kattintás tudatosság, nyilvános wifi használat, stb.)
2. a generációk (A02) tekintetében nem olyan egyértelmű a mintázat, mint a nem esetében. Itt összefüggést lehet találni a tájékozottsággal, a biztonsági frissítések tudatosságával és a vírusirtó használatával. A többi biztonságtudatos minta nem mutatott egyértelmű és konzekvens életkorral/generációval összefüggő sajátosságot.
3. a tartózkodási hely (A03) szerepe sem teljesen egyértelmű: 2021-ben a kapott válaszoknál nem találtunk olyan összefüggést, amely legalább valamilyen tendenciaként megfogalmazható lenne (pl. azt várhatnánk, hogy a nagyvárosokban több eszközt használnak, vagy több időt töltenek számítógép előtt, de erre utaló összefüggés nem mutatható ki).
4. iskolai végzettség (A04) esetében egyértelműbb a kép: a magasabb iskolai végzettségű kategóriák válaszadói gyakrabban adtak biztonságtudatos válaszokat. Emellett az iskolai végzettség összefüggésben van az ezen eszközökkel munkában töltött idővel.
5. az eszközök száma (B01) és a munkában az eszközökkel töltött idő (B02) összefüggést mutatnak: a több, mint 3 eszközzel rendelkezők, és akik legalább 6 órában a munkaidejükből számítástechnikai eszközt is használnak, azokra jellemzőbb a biztonságtudatos viselkedés.
6. a legerősebbnek tűnő összefüggés az IT hírek olvasási gyakorisága (C01) és a biztonságtudatos viselkedés között van, vagyis aki rendszeresen olvas ilyen híreket, ott szinte minden esetben, kivétel nélkül biztonságtudatos viselkedésre utaló válaszokat kaptunk

A válaszlehetőségek kapcsolatát is megvizsgáltuk, ez elsősorban a kérdések és válaszok koherenciájának vizsgálatát segíti. Ez azt jelenti, hogy az, aki az egyik biztonságtudatossági kérdésre adott válasz alapján biztonságtudatos viselkedést jelölt

meg, az más, ugyanebbe a kategóriába (D kérdés csoport, lásd 8. táblázat) tartozó kérdés esetén is nagyobb arányban jelölte meg a biztonságtudatosnak tekinthető választ.

8. táblázat: Khi négyzet próba eredményei a független változók (A-B-C) és a biztonságtudatossági szempontok (D) tekintetében – 2021-es adatok alapján (saját szerkesztés)

			A01_Nem	A02_Generáció	A03_Tartózkodási hely 1.	A03_Tartózkodási hely 2.	A04_Iskolai végzettség 1.	A04_Iskolai végzettség 2.	B01_Eszközök száma	B02_Eszközök használata	C01_IT hírek gyakorisága	C02_Szervezeti incidens bejelentése	D01_Biztonsági frissítés	D02_Jelszavak - eltérő	D03_Vírusirtó használat	D04_Mondat:csatolmány	D05_Mondat:zsarolóvírus	D06_Nyilvános wifi használat	D07Álprofilképzés
2021	A01_Nem	Férfi--Nő		ns	ns	ns	<0,001	ns	0,027	<0,001	<0,001	0,005	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	ns
	A02_Generáció	AlfaZy--XBabyV			0,01	<0,001	<0,001	<0,001	ns	ns	ns	<0,001	<0,001	ns	<0,001	ns	ns	ns	ns
	A03_Tartózkodási hely	1. Egyéb,Város--MJVBudapest					ns	ns	ns	<0,001	ns	ns	ns	ns	ns	ns	<0,001	ns	ns
		2. Egyéb,Város,MJV--Budapest					<0,001	ns	ns	ns	ns	ns	ns	ns	ns	ns	ns	ns	ns
	A04_Iskolai végzettség	1. Általános--Középiskola, Felsőfokú							ns	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	ns	<0,001
		2. Általános,Középiskola--Felsőfokú							ns	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	ns	0,031
	B01_Eszközök száma	Legfeljebb 3--Több, mint 3								<0,001	<0,001	<0,001	ns	<0,001	0,009	0,03	0,003	ns	0,001
	B02_Eszközök használata	Kevesebb, mint 6 óra-Legalább 6 óra									<0,001	<0,001	ns	<0,001	<0,001	<0,001	<0,001	0,015	0,01
	C01_IT hírek gyakorisága	Nem rendszeres--Rendszeres										<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001
	C02_Szervezeti incidens bejelentése	Nem v rosszul tudja--Tudja											<0,001	<0,001	<0,001	0,001	<0,001	ns	ns
	D01_Biztonsági frissítés	Nem v nem tudatosan--Tudatos												<0,001	<0,001	<0,001	<0,001	0,001	0,01
	D02_Jelszavak - eltérő	Nem tudatos jelszóhasználó--Tudatos													<0,001	<0,001	<0,001	<0,001	<0,001
	D03_Vírusirtó használat	Hiányos végpontvédelem--Tudatos														<0,001	<0,001	0,022	ns
	D04_Mondat:csatolmány	Adathalászat magas kock--alacsony kock															<0,001	<0,001	0,007
	D05_Mondat:zsarolóvírus	Nem ismeri--Ismeri																<0,001	<0,001
	D06_Nyilvános wifi használat	Magas kockázat--alacsony kockázat																	<0,001
	D07_Álprofilképzés	Magas kockázat--alacsony kockázat																	

színskála p értékek alapján

pozitív

p<=0,001

0,001<p<=0,01

0,01<p<0,05

negatív/fordított

p<=0,001

0,001<p<=0,01

0,01<p<0,05

5. Megbeszélés

5.1. Digitális egészségügyi ökoszisztéma

Az egészségügyben az adatforradalom időszakát éljük. Adatvezérelt paradigmaváltás zajlik az egészségügyben: még az elején vagyunk, de már látható – más szektorból átvett tapasztalatok alapján – hogy az adatnak különös jelentősége és értéke van. Az adatfeldolgozás, adathasznosítás kulcsfontosságú az egészségnyereségek maximalizálása érdekében. Az adat középpontba állítása azért is fontos, mert a XXI. századi innovációs kezdeményezések egyik legfontosabb alapanyaga, olyan értéke van, hogy a modern ipari kémkedés már leginkább erre irányul (Security Service MI5, 2023).

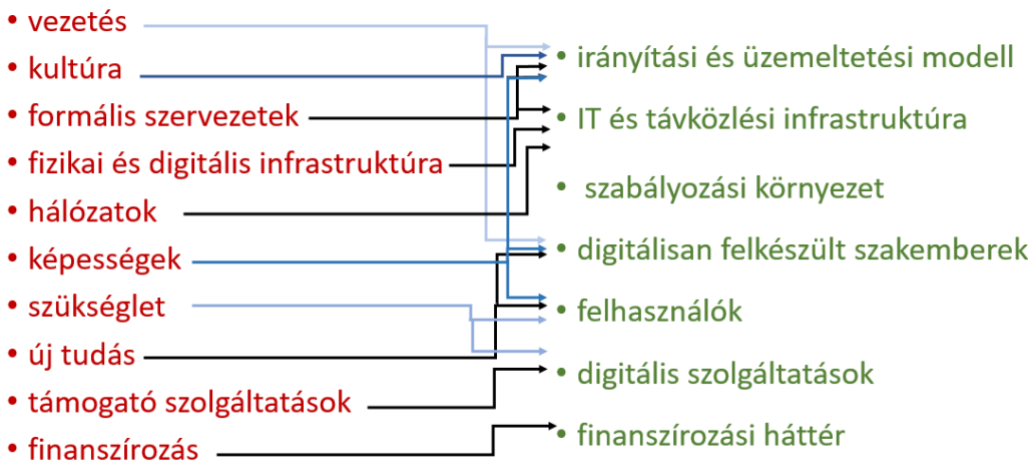
A kiberbiztonság kiemelt fontosságú terület, mivel az egészségügyi szektor jelentős kockázatoknak van kitéve, és egyre gyakoribb célpontja a kibertámadásoknak (Szócska & Joó, 2018). A személyes egészségügyi adatok bizalmas természete megköveteli a legszigorúbb adatvédelmi intézkedések alkalmazását, hogy biztosítsák azok védelmét és megfelelő kezelését, különösen a hálózatok világában, a kibertérben, és ez az egyik alapja annak, hogy a szuverén, befolyásolásmentes egészségügyi döntések születhessenek mind egyéni, mind csoportos, illetve tágabb értelemben nemzeti szinten is.

Az egészségügy az egyik legjelentősebb bizalmi alapú szolgáltatás, ahol a páciensek és az ellátók közötti kapcsolat a bizalomra és az adatok felelős kezelésére épül. A magyar digitális egészségügy az általános nemzeti szintű digitalizációhoz képest jobb nemzetközi értékelésű, a magyar egészségügyben, illetve a digitális egészségügyi fejlesztések alapján keletkező adatvagyon jelentős stratégiai előnyt és lehetőséget jelent nemzeti szinten, amely az egészségügy eredményesebb, hatékonyabb, igazságosabb működése érdekében használható. Az ehhez szükséges jogszabályi környezet megteremtése Magyarországon is megkezdődött.

Amint azt az 1. fejezetben bemutattam, az ökoszisztémák sajátossága, hogy azok elemeit azonos módon kell fejleszteni, egyébként megbomlik az ökoszisztéma egyensúlya, és az új helyzet aránytalanságokat, magasabb költséget, rosszabb minőséget jelent. Modellünk megalkotását részben ez, a kiegyensúlyozott fejlesztésre törekvés motiválta, illetve az a felismerés, hogy a digitális egészségügyi ökoszisztéma egyik legfontosabb eleme az egészségügyi adat.

Saunders és munkatársai 2022-ben publikáltak egy, az általunk 2021-ben publikálthoz hasonló digitális egészségügyi ökoszisztéma modellt, amely 10 elemet tartalmaz (Saunders et al., 2022). Az ő modelljük kapcsán fontos kiemelni, hogy a kanadai Albertában használt digitális egészségügyi ökoszisztéma modellt írták le, míg mi egy általánosan használható, de magyar tapasztalatokra építő modellben gondolkoztunk. A két modell elemei megfeleltethetők egymásnak, ahogy azt a 10. ábra bemutatja. A modellek összehasonlítása során elhagytuk azokat az entitásokat, amelyek nehezen voltak meghatározhatók vagy leírhatók, és olyan elemeknek feleltettük meg, amelyek komplexen magukban hordozzák a Saunders féle modell elemeit, és jól körülírhatók. Példaként említhetjük az általunk használt „irányítási és üzemeltetési modell" fogalmat, amely a konkrét szervezeti megoldástól (formális szervezetek) a szervezeti kultúrán keresztül a vezetés jellemzőit is magukban hordozzák.

A két modell közötti fontos különbség, hogy mi a digitális egészségügyi ökoszisztéma modellünk fontos részének tekintettük a szabályozási környezetet, míg Saunders erről nem tesz külön említést.



10. ábra: A Saunders-féle és a kutatás során megalkotott digitális ökoszisztéma modell megfeleltetése (saját szerkesztés)

Az egészségügy tekintetében teljeskörűen szükség lenne az informatikai fejlesztés és üzemeltetés új irányítási és üzemeltetési modelljének kialakítására, hiszen jelentős mértékben megváltozott a szektoron belül a szolgáltatások összetétele, de változott a

szolgáltatók tulajdonviszonya is: elég ha csak a magánegészségügyi szolgáltatók számának elmúlt években bekövetkezett, szinte exponenciális növekedésére gondolunk.
A centralizáció és decentralizáció szintén kiemelt területe a hatékony irányítási és üzemeltetési modellnek: ennek megfelelő szintjének és egyensúlyának kialakítása kulcsfontosságú ebben a forráshiányos helyzetben. Miközben az eszközök és különösen a képzett emberi erőforrás a legnagyobb hiány az egészségügyi ágazat információbiztonsági területén, ezek centralizációjával együtt szükséges azt is biztosítani, hogy a szolgáltatások megfelelő színvonalúak legyenek. A teljes mértékben centralizált rendszerek – jellemzően, a felhasználótól való nagy távolság miatt - nem képesek a végfelhasználói igényeket jó minőségben és gyorsan kiszolgálni.
Az infokommunikációs fejlesztések megvalósításakor elengedhetetlen, hogy a legteljesebb mértékben érvényesüljenek adatvédelmi szempontok: a személyes adatok védelme és a célhoz kötöttség elve. Ez azt jelenti, hogy kizárólag az érintett páciensek vagy az arra jogosult személyek férhetnek hozzá a kezeléshez szükséges adatokhoz. Az egészségügyben az informatikai és a kapcsolódó távközlési rendszerek biztonságának megteremtése és folyamatos fejlesztése kiemelten fontos, és ennek során az adatbiztonságot mindig elsődleges szempontként kell kezelni. Ez a megközelítés az egyik kulcseleme annak a modellnek, amely biztosítja a digitális egészségügyi ökoszisztéma kiegyensúlyozott és fenntartható fejlődését.
A digitális képességek fejlesztésének szükségességét nemcsak az Európai Bizottság hangsúlyozza a Digitális Kompetenciákról szóló keretrendszer bevezetésével (Vuorikari et al., 2022), hanem kifejezetten nemzeti szintű egészségügyi jó példák is vannak (NHS Health Education England, 2023).
A digitális egészségügy finanszírozásához rendelkezésre álló források változatosak, amelyek többsége köz- vagy kvázi közforrásokból származik. Ide tartozik például a központi költségvetés egészségügyre vagy infokommunikációra fordítható része, amely alapvető szerepet játszik a fejlesztések támogatásában (Stroetmann et al., 2011). Az előzőekhez hasonlóan, megfelelő üzleti modell kialakításával pénzügyi szereplőket (pl. magán, állami biztosító társaságok) vagy állami ügynökségek (pl. technológiai, innovációs) is be lehet vonni a finanszírozásba, kihasználva azt a lehetőséget, hogy az állam jelentős, a fejlesztések érdekében felhasználható adatvagyonnal rendelkezik, míg a biztosítók, vagy innovációs ügynökségek rendelkeznek a megfelelő piaci ismerettel. A

források felhasználása, azok célhoz kötöttsége változatos képet mutat. Feldolgoztuk a tudományos publikációkban elérhető digitális egészségügyi fejlesztések irodalmát, és ott is arra a megállapításra jutottunk, hogy általában nem jellemző, hogy egységes fejlesztési keretrendszer mentén, kiegyensúlyozottan történnek a fejlesztések (Vida et al., 2021). Az egészségügy digitális átalakulásának finanszírozásában kiemelkedő szerepet játszik az Európai Unió, amely az elmúlt két évtizedben Magyarországgal együtt (társfinanszírozásban) jelentős, százmilliárd forintos nagyságrendű fejlesztési beruházást valósított meg. Ezek a projektek a fenntartható, személyre szabott és integrált digitális egészségügyi szolgáltatások, eszközök és megoldások fejlesztését célozták, azonban sok esetben túlzottan is a technológiai fejlesztésre koncentráltak és nem biztosították a digitális egészségügyi ökoszisztéma szerinti kiegyensúlyozott fejlesztéseket.

Az adatközpontú digitális egészségügyi ökoszisztéma modell lehetővé tette, hogy definiáljuk a mesterséges intelligencia algoritmusok előállításának folyamatát, az ún. mesterséges intelligencia gyártósort (Balogh et al., 2022). A korábbi gyakorlati munkák tapasztalatai alapján elmondható, hogy az egészségügyi mesterséges intelligencia kutatások többsége technológiai vagy etikai szempontokra összpontosít, és kevés az olyan rendszerszintű vizsgálat, amely a jövőbeli integrációra figyel, illetve ahol a fejlesztés már a kezdetektől ilyen szempontok figyelembevételével történne.

A felsorolt kockázatok ellenére kijelenthető, hogy az egészségügyi digitális ökoszisztéma kiépítése – vagyis a digitális egészségügyi megoldások átgondolt, stratégiai fejlesztése, valamint széleskörű szakmai és társadalmi elterjesztése – jelentős közösségi értékeket teremthet. Ez a folyamat nemcsak az egészségügyi szolgáltatások hatékonyságát növeli, hanem számottevő össztársadalmi előnyökkel is jár, amelyek hosszútávon fenntartható fejlődést biztosíthatnak (Szabó et al., 2021).

Kutatásom alapján egyértelműen megfogalmazható és az elemei is meghatározhatók egy digitális egészségügyi ökoszisztéma modellnek, amely modell használata révén lehetőség van a digitális egészségügyi rendszer kiegyensúlyozott fejlesztésére és működésének biztosítására. Ezen modell központi eleme az egészségügyi adat, amely stratégiai szerepe is definiálható **(K1.1 kutatási kérdés megválaszolása).**

5.2. Biztonságos innovatív adathasznosítás

Az egészségügyi adatok mellett más adatok is jelentős értékkel rendelkeznek egy korszerű ökoszisztémában, és ezek az egészségügy és az egészségügyi rendszer számára is fontosak, közvetetten vagy közvetlenül egészségnyereséggé fordíthatók. A különböző rendszerekben, az egészségügytől függetlenül képződő nagy adatbázisok összekapcsolásával és innovatív eszközökkel az egészségügyi folyamatokat/rendszert/döntéseket lehet támogatni. A kész adatokkal a rendszerek gyors implementációt és döntéstámogatást biztosítanak. A jelenleg rendelkezésre álló lehetőségek kihasználásához azonban több problémát is meg kell oldani, pl. interoperabilitási kérdések vagy a kutatás tárgyát képező adat- és információbiztonsági kérdések.

A kidolgozott módszertanunk egy olyan jó gyakorlatot és ez alapján egy olyan biztonságos eljárást jelenthet, amely révén lehetőség van az üzleti-akadémiai-privát együttműködésekben rejlő lehetőségek kihasználására, különösen a veszélyhelyzetekben. Természetesen a kidolgozott biztonságos módszertan és az adathasznosítás során használt modell alkalmas lehet a „normál életben" létrejövő, közhaszon és magán haszon egyensúlyára épülő hasznosítások kialakítására is.

A mobiltelefonok fontos szerepet töltöttek be a COVID-19 járvány kapcsán: az általuk generált adatokkal jól követhetőek voltak azok a szereplők, akikhez köthető volt a vírus terjedése (Grantz et al., 2020).

Kidolgozott, és publikált módszertanunkban (Szócska et al., 2021) bemutattuk, hogy az egészségügyi adattudomány – amely a működés során keletkező nagy adatbázisok összekapcsolásával és innovatív eszközök alkalmazásával, hogyan járulhat hozzá egy reziliensebb, a külső körülményekhez rugalmasan alkalmazkodó egészségügyhöz.

Bár nem létezik egységes nemzetközi ajánlás arra vonatkozóan, hogyan tehető az egészségügy ellenállóvá és alkalmazkodóképessé, úgy véljük, hogy az infokommunikációs technológiák fejlődése és a másodlagos adathasználat innovatív alkalmazása – ahogyan azt a jelenlegi példák is mutatják – jelentősen javíthatja az

egészségügyi rendszerek hatékonyságát. Ezáltal növelhető a társadalmi reziliencia, vagyis a környezeti változásokhoz való rugalmas alkalmazkodás képessége.

Az itt bemutatott módszertan mellett egy tanulmányunkban más innovatív adathasznosítási lehetőséget is bemutattunk: például a hálózatelemzési eszköztár hogyan használható oltásellenességi mozgalmak kimutatására, és adott esetben ellenkampány tervezésére (Gaál et al., 2021).

Számos példa igazolja, hogy az innovatív adat felhasználás, az adatok elemzése hatékony eszközként szolgálhat a különböző környezeti kihívások kezelésében. A krónikus, nem fertőző betegségek esetében például a betegút menedzsment integráns részét képezhetik, és ezáltal a megelőzés kulcsfontosságú tényezőjévé válnak.

Összefoglalva elmondható, hogy a kidolgozott módszertannal sikerült olyan egyszerű és hatékony döntéstámogató alkalmazást fejleszteni, amely a mobilcellaadatok (CDR) felhasználásával kapcsolatos biztonsági és technikai kérdések mindegyikére választ ad. Ugyanakkor a CDR adatainak felhasználása nem az egyetlen lehetőség az emberek mozgási aktivitásának vizsgálatára. Az okostelefonok, amelyek GPS-funkcióval is rendelkeznek, pontosabb helymeghatározást biztosítanak, mint a cellainformációk. Ez a megoldás azonban korlátokkal is jár, mivel az előfizetőknek rendelkezniük kell GPS-képes eszközzel, a helymeghatározást be kell kapcsolniuk, és engedélyt kell adniuk a helyadatok használatához, ami csökkentheti az adatokhoz való hozzáférés lehetőségét.

A megjelent közleményünkben részleteiben hasonlítottuk össze a két, tudomásunk szerint jelenleg elérhető módszertant. Ebből az összehasonlításból a jelenlegi dolgozatban a legfontosabbakat emelem ki (9. táblázat) (Szócska et al., 2021).

9. táblázat: A CDR alapú és GPS alapú mozgás aktivitási módszertanok összehasonlítása (saját szerkesztés (Szócska et al., 2021) alapján)

Értékelési szempont	CDR alapú módszer	Okostelefon alapú módszer
Helyadatok	Cellaállomás („cellular base station")	Műhold és cellaállomás
Nyomkövetési pontosság	Jobb népességlefedettség	Jobb helymeghatározási pontosság az egyéni okostelefon-felhasználók számára
Személy helye	Alacsonyabb (kb. száz métertől kilométerekig), függ az állomás sűrűségétől és a környezettől	Magasabb (néhány méter műholdas pozicionálással)
Népességlefedettség	Magasabb	Alacsonyabb
Mobilitás elemzése személyes jellemzők szerint	Nagyon korlátozott	Igen
Megvalósíthatóság	Könnyebb és kevésbé költséges	Drágább
Személyes adatvédelem és adatvédelmi szabályok	Biztosított az anonim és aggregált adatokkal. A mobiltelefon-felhasználóktól nem igényel jóváhagyást (a jóváhagyást a szolgáltatásra történő regisztrációkor adják meg)	Az okostelefon-felhasználóktól jóváhagyást igényel
Mikor kell használni?	Jobb lehetőség a tömeges népességmozgás monitorozására nagy léptékű országos vagy regionális korlátozások esetén.	Jobb az egyének vagy kisebb népességcsoportok nyomon követésére célzott beavatkozások, például kontaktus nyomozás vagy karantén monitorozás céljából.

Elvégzett kutatásunk alapján egyértelműen igazolást nyert, hogy megteremthető egy olyan biztonságos innovatív adathasznosítási környezet és módszertan, amely az adat-, információ- és kiberbiztonsági feltételeknek megfelelve jól használhatók az egészségügyi, egészségbiztonsági döntések előkészítéshez, és a döntésekben és lehetőséget biztosítanak az egészségügyön kívüli adatok becsatornázásra az egészségügyet érintő döntések kapcsán is **(K2.1 kutatási kérdés megválaszolása)**. Meglátásom szerint a kutatásban megfogalmazott módszertannal további adatkörökre lehet kibővíteni az egészségügyi (egyéni, intézményi, vagy rendszerszintű) döntéseket megalapozó és támogató elemzéseket, ezzel kihasználva az adatok másodlagos hasznosításából eredő hasznokat.

5.3 Zsarolóvírusok az egészségügyben

A zsarolóvírus támadások elleni küzdelem, a megelőzés és a károk elhárítása a kiberbiztonság talán legnagyobb kihívásai közé tartoznak. 2020-ban megjelent tanulmányunkban részletesen összefoglaltuk a zsarolóvírusokkal kapcsolatos legfontosabb ismereteket (Palicz et al., 2020). Ezek közül érdemes kiemelni az alábbiakat:

1. a támadások jellegzetesen történnek: a leggyakoribb rendszerbe kerülési módok közé tartozik az adathalászat (phishing), a távoli asztalon keresztüli (RDP – Remote Desktop Protokoll) rendszerbe kerülés, és a szoftversérülékenység kihasználása.
2. jellemző vagy tipikus esetek közé tartozik, amikor a felhasználó valamilyen rosszindulatú állományt aktivál a gépén és ezen keresztül jutnak be a kiszemelt gépbe, majd hálózatba. Egészségügyi példához hasonlítva azt mondhatjuk, hogy a betegbiztonság kapcsán használt svájci sajt-modell itt is „működik”: általában több, egymást követő, vagy egymáshoz kapcsolódó sérülékenység, vagy nem megfelelő intézkedés (pl. egyszerű felhasználó az indokoltnál magasabb jogosultsággal rendelkezik) okozza a rendszer leállásához vezető problémát.
3. a rosszindulatú, titkosító kódot aktiválva – általában a zsarolóvírusra jellemzően – bizonyos könyvtárak titkosítása elindul, a fájlok hozzáférhetetlenné válnak, jellemző kiterjesztést kapnak, és bekerül egy olyan állomány, amely tartalmazza a legfontosabb üzenetet: az adatok titkosításra kerültek, és csak abban az esetben van lehetőség a hozzáférő (titkosítást feloldó) kód megkapására, ha meghatározott kriptovaluta megvásárlása és átutalása megtörténik. Fontos megjegyezni, hogy az esetek egy részében az utalást követően megkapott kódok nem működnek jól, vagyis hiába fizet valaki, a titkosítás feloldása nem sikerül.
4. a titkosítás mellett a zsarolóvírusok újabb generációja már arra is képes, hogy előzetesen elindítson egy adatszivárgást, amely révén olyan, akár üzletileg vagy személyesen érzékeny adatok kerülhetnek ki, amelyek nemcsak a szervezet, hanem az egyén számára is kompromittálóak lehetnek, így a zsarolás több szinten vagy pontos is történhet (gondoljunk például egy pszichiátriai intézményre, ahol a kezeltek részletes adatai kikerülnek).

5. mint sok más esetben (de az egészségi állapotra vonatkozóan általában), itt is igaz: a megelőzés a leghatékonyabb módja a biztonságos állapot fenntartásának, és ebben elsődleges a felhasználók biztonságtudatosítása

A zsarolóvírus támadások folyamatosan történnek, és számuk folyamatosan emelkedik. Ennek hátterében az áll, hogy a legjobb pénzügyi megtérüléssel járó kiberbűnözési forma közé tartozik, és manapság már ez is hozzáférhető szolgáltatásként (RaaS – Ransomware-as-a-Service).

A fentiekben bemutatott esetekből kettőt 2021-ben publikáltunk (Palicz, Sas, et al., 2021), míg a doktori munkához kapcsolódva további két eset feldolgozására került sor. Ezen esetekből az alábbi általános következtetések vonhatók le:

1. A hazai és nemzetközi adatok és esetek nehezen hozzáférhetők, gyakran nem tudományos, hanem laikus, sajtóinformációk alapján lehet tájékozódni
2. A zsarolóvírusok által okozott támadások az egészségügyi intézmények esetében kiemelt jelentőségűek, elsősorban a hozzáférés és a sértetlenség (integritás) sérülése miatt, valamint a bekövetkező üzletmenet folytonosság sérülése miatt
3. Hazai tapasztalatok alapján az intézmények nincsenek megfelelően felkészülve az ilyen eseményekre, nem rendelkeznek megfelelő preventív képességgel, illetve a baj bekövetkezte esetén esetlegesek a történések, leginkább személyes tapasztalatokon múlik, hogy hogyan kezelik a havariát
4. Az egészségügyben dolgozókat kiemelten kell kezelni a biztonságtudatosítás érdekében. Ez részint a „laikus" egészségügyi felhasználóra vonatkozik, másrészt az informatikai és információbiztonsági területen dolgozókra: az ő esetükben külön képzések, tréningek indítására lenne szükség.
5. Az ellátási/beszállítói láncot külön rizikóként kell kezelni: ez az egészségügy esetében, tekintettel a rendkívül komplex folyamatokra, az azokat támogató informatikai alkalmazásokra, vagy éppen orvosi eszközökre, rendkívül összetett, és hosszadalmas kockázatfeltáró és megelőző tevékenységet igényel.

A hazai esetek alapján fontos megállapítás, hogy mind az eseménykezelési eljárásokat mind azok dokumentálását - tudományos és oktatási feldolgozhatóság érdekében is - javítani kell.

2022. végén a Journal of American Medical Association-ben (JAMA) jelent meg az első nagy összefoglaló tanulmány, amely 2016-2021 között amerikai kórházakban előfordult 374 zsarolóvírus esetet dolgoz fel. Ennek kapcsán fontosnak tartom kiemelni, hogy maga a publikáció helye is jelzi, hogy a korszerű egészségügyi ellátás folytonosságának biztosításában milyen jelentősége van a zsarolóvírus támadásoknak. A cikk arra is rámutat, hogy ezeknek az eseteknek a megfelelő rendszerszintű gyűjtése és feldolgozása (mind az egyedi esetek tanulságainak levonása, mind a sokaság statisztikai feldolgozása) milyen fontos jelentőséggel bír (Neprash et al., 2022).
Szintén a JAMA-ban jelenet meg, de már 2023-ban az a tanulmány, amely kimutatta, hogy zsarolóvírus támadások ideje alatt, és azt követően a támadással nem érintett, de szomszédos kórházak sürgősségi osztályain is a betegek számának, a mentők érkezésének, a váróteremben töltött időnek, a nem ellátott betegek számának, a betegek teljes tartózkodási idejének, és az akut stroke ellátási mutatóinak jelentős kedvezőtlen irányú változása volt tapasztalható (Dameff et al., 2023). Ez a tanulmány azt is jelezte, hogy az egészségügyben a zsarolóvírusok jelentős fennakadásokat okoznak a nagyobb, regionális vagy megyei kórházakban, és olyan havária helyzetként kezelendők, ami összehangolt tervezési és reagálási erőfeszítéseket tesz szükségessé. Hasonló következtetésre jutott egy sürgősségi ellátásokkal foglalkozó lapban megjelent kvalitatív tanulmány is (van Boven et al., 2024).

Az elvégzett kutatásom alapján egyértelmű, hogy a zsarolóvírus támadások „üzleti” (ebben az esetben klinikai működési) következményeinek jobb megítélhetősége és értékelhetősége érdekében, az esetek egyszerű leírása mellett az alábbi szempontokat kell még áttekinteni. Ezek egyrésze kifejezetten egészségügy specifikus:

- milyen kórházban történt az eset (országos intézet, megyei/vármegyei, városi, egyéb ellátó), milyen típusú ellátást végez az intézmény, (fekvőbeteg vagy járóbeteg ellátás, aktív akut ellátás, aktív nem akut ellátás, krónikus, rehabilitációs, egyéb, stb.), milyen ellátási területtel rendelkezik, milyen progresszivitási szinten, kritikus/létfontosságú infrastruktúrának számít-e az eset?
- hogyan zajlott pontosan az eset, és milyen gyenge pontokat lehetett azonosítani, amelyek egy kórházi működés során zsarolóvírus támadással kihasználhatók? (hogyan került be a rosszindulatú kód, mi volt a szervezeten belüli életútja, milyen

szervereket, hálózati eszközöket, és végpontokat ért el, az eszközökön mit okozott, milyen hatással volt azok működésére)

- milyen mértékű volt a támadás jelentősége az alap és támogató folyamatokra, hogyan befolyásolta az „üzleti" tevékenységet (business impact analysis) – milyen mértékben érintette a betegellátást (milyen osztályokat, egységeket érintett, hány munkatársa, az adott osztály/egység működése mennyire kritikus az egészségügyi intézmény szempontjából, milyen konkrét működési problémát okozott, egyének, csoportok, kisebb egységek, osztályok, klinikák szintjén, hány munkatárs munkája vált érintetté),
- milyen diagnosztikai, terápiás, vagy egyéb adminisztratív folyamatot (szakmai és nem szakmai támogató folyamatok, dokumentálás, időpont szervezés, pénzügyi stb.) érintett a támadás
- milyen jó/rossz gyakorlat és tanulság vonható le következtetésként, amely más kórházak számára is hasznosítható lehet (milyen felkészültségűnek ítélte a kórház önmagát, rendelkeztek-e megfelelő tervekkel, azokat gyakorolták-e, milyen azonnali és középtávú teendők következtek ezekből, stb.).

Kutatásom alapján - figyelembe véve a publikációinkat követően megjelent nemzetközi kvalitatív és kvantitatív tanulmányokat – egyértelműen kimondható, hogy a zsarolóvírus támadások jelentős hatással vannak az egészségügyi szolgáltatók működésére, az informatikai rendszerek érintettsége változatos volt, a kórházak komplex folyamataiban a beszállítói láncok érintettsége is jelentős fennakadást okozhat (**K3.1 kutatási kérdés megválaszolása**). Az egészségügyi incidensek adatainak rögzítése a későbbi tudományos feldolgozás szempontjából nem megfelelő. Az egészségügyi intézményekben bekövetkezett incidensek bejelentésekor, vagy azt követően minél rövidebb időn belül szükséges lenne rögzíteni a kutatás során meghatározott adatokat, amelyek feldolgozása, elemzése jobban segítheti az események hatásainak megértését, ezáltal segítheti a felkészülést és a reagálási képességet **(K3.2 kutatási kérdés megválaszolása)**. A rögzítés célja elsődlegesen a tudásbázis létrehozása, és a későbbiekben ezek esetszintű illetve statisztikai feldolgozhatósága lenne.

5.4. Lakossági biztonságtudatosság

A hazai kibertér biztonságtudatosságát vizsgáló országos felmérésünk során átfogó képet kaptunk a lakosság viselkedéséről ezen a területen. Ez az első ilyen jellegű kutatás, amit több éven át, következetesen, gyakorlatilag azonos módszertannal végeztünk. A 2020-as évben több mint 1000 fő, míg 2021-ben már több mint 1500 fő töltötte ki az elektronikus kérdőívet. Az új kutatási kérdőívünkben, amelyet 2023-ban vezettünk be, az eddigi eredmények alapján megtartottuk a biztonságtudatossággal kapcsolatos kérdés-válaszokat, de kibővítettük ágazati besorolással, valamint olyan kérdésekkel, amely alapján az attitűd jobban vizsgálható. Emellett azt is vizsgáljuk az új kérdőívben, hogy a fenyegetettség összefüggésben van-e a biztonságtudatossággal.

A kérdőíves kutatásunk egyik legfontosabb limitációja, hogy a kérdőívek kiküldése nem reprezentatív mintának történt, emiatt az adatfeldolgozásból nem tudunk a teljes sokaság jellemzőire sem következtetni. Annak ellenére, hogy nem reprezentatív a minta, a felmérésünk eredményei hasonló tendenciákat mutatnak, mint a hazai és nemzetközi eredmények. A szociodemográfiai tényezők közül leginkább a nem és az iskolai végzettség van összefüggésben a biztonságtudatos magatartással. A település típusa, illetve a generáció vagy éppen az életkor vegyes képet mutat. Az életkor esetében megfigyeltük, hogy a fiatalabb generációkra az jellemző, hogy ugyan sokkal magabiztosabbak a virtuális világban, mint a többi generáció, azonban magasabb a kockázatvállalási hajlandóságuk is: kevésbé figyelnek a frissítésekre, vagy éppen a naprakész vírusírtók használatára. Ez a megállapítás azért fontos, mert annak az összefüggését vizsgálni kell (utánkövetés, vagy más vizsgálatokkal), hogy ez generációs vagy inkább életkori sajátosság. Illetve azt is érdemes vizsgálni, ezek a magatartási formák befolyásolhatók-e az iskolai képzés révén, legyen szó akár közoktatásról, akár felsőfokú képzésről. Amennyiben ez inkább generációs sajátosság, akkor ezek a jellemzők a későbbiekben is megmaradnak ebben a generációban, függetlenül az életkoruktól és iskolai képzésüktől. Ez néhány év múlva, amikor kiterjedten lesznek jelentős információs rendszer használók, komoly fejtörést okozhat a kiberbiztonsággal foglalkozó szakembereknek.

A kutatásunk eredményei alapján az egyik legfontosabb megállapítás, hogy a D csoport kérdései-válaszai erős korrelációt mutatnak, ami arra utal, hogy van egy meghatározott magatartásminta, amely jellemző a biztonságtudatosságra. Ez összecseng azzal, amit a

gyakorlatban is tapasztalunk, és amit rendszeresen kommunikálunk: bizonyos magatartások/válaszlépések jelentősen javíthatják a biztonságtudatosságot és csökkenthetik az információbiztonsági események kockázatát. A kutatás szerint azok, akik rendszeresen frissítik szoftvereiket, használnak automatikus vírusírtót, erős és eltérő jelszavakat alkalmaznak, és óvatosan kezelik az emailben érkező csatolmányokat, általában biztonságtudatosabban viselkednek. Ezek a magatartások szorosan összefüggnek: aki az egyik esetben biztonságtudatosan lép, az valószínűleg más esetekben is a biztonságos lépést fogja választani.

Ez az összefüggés több fontos gyakorlati jelentőséggel is bír. Egyrészt ezekből a válaszokból képezhető olyan paraméter, amelyek összességében jellemzik az egyén biztonságtudatos magatartását, így egyfajta mérőszám keletkezik, amellyel lehet jellemezni ezt a magatartást, illetve az időbeli változás, a mérhetőség szempontjából is fontos. Emellett további mérésekkel, jellemzőkkel tovább érzékenyíthető, finomítható ez a magatartásminta. Ilyen érzékenyítő tényező lehet például a mobileszközökön vagy notebookon használt PIN vagy biometrikus azonosítás (ki mit használ), a multifaktoros azonosítás választása, vagy a saját eszközök és hálózatok biztonságát növelő technológiák.

Emellett a kutatásunk egy másik fontos megállapítása az, hogy az IT biztonsági hírek olvasásának nagy jelentősége van a biztonságtudatos magatartásmintában. Az látható, hogy ez szintén erős összefüggést mutat a biztonságtudatos magatartással: aki rendszeresen olvas ilyen típusú híreket, arra a biztonságtudatos választás jellemző. Az a jelenlegi kutatás és elvégzett elemzések alapján nem dönthető el, hogy ez oki tényező-e, vagy a biztonságtudatos magatartás része. Ez további statisztikai és célzott kvalitatív és kvantitatív kutatásokkal tisztázható.

A fentiek gyakorlati szempontból azért fontosak, mert ezen sajátosságok alapján (szociodemográfiai tényezők, biztonságtudatossági magatartásmintázat, stb.) azonosíthatóvá válnak a sérülékeny csoportok. Ez egy-egy munkaköri kiválasztásnál, vagy éppen a szervezeten beüli speciális képzések meghatározásánál ez jelentőséggel bír. Ezek a képzések intézményi szinten is relevánsak lehetnek. Például, aki rendszeresen végez biztonsági frissítéseket, és óvatosan használja a jelszavait, kevésbé valószínű, hogy áldozata lesz kiberbiztonsági incidensnek. Ezek a paraméterek technikailag is monitorozhatók, ezzel csökkentve az emberi tényező és az önbevallás hatását. Vagyis egy

munkahelyi környezetben meg tudom mérni, hogy a kiberbiztonsággal foglalkozó honlapokon mennyi időt tölt valaki, illetve az is mérhető, monitorozható, hogy milyen biztonsági beállításokat használ valaki, rendszeresen frissíti-e az operációs rendszert, vagy a jelszavai megfelelnek-e bizonyos előírásoknak, és azokat rendszeresen cseréli-e. Ezeknek a jellemzőknek a meghatározása feltétele lehet bizonyos munkakör betöltésének, illetve ezzel kapcsolatban speciális képzések is kifejleszthetők.

Összességében, ezek a megállapítások további kutatásokat igényelnek a terület mélyebb megértése érdekében.

Lakosság körében végzett kutatásunkban, nagy válaszadói szám feldolgozásával bemutattuk, hogy a bizonyos szociodemográfiai tényezők (férfi nem, magasabb iskolai végzettség) pozitív összefüggést mutatnak a biztonságtudatos magatartással, míg más tényező esetében (lakóhely, generációs besorolás, informatikai használati szokások) ez az összefüggés nem egyértelmű **(H4.1. hipotézis részben nyert igazolást)**.

6. Következtetések

6.1. A kutatás jelentősége és egyedisége

Az egészségügy adatgazdagsága és működési sajátságai miatt indokolt az egészségügyön belül is foglalkozni az információbiztonsággal, illetve speciálisan a kiberbiztonsággal is. Itt érdemes megemlíteni az Amerikai Orvosszövetség (AMA) 2019-es mondatát, amelyben kijelentették: „Cybersecurity is not just a technical issue; it's a patient safety issue" – vagyis a „Kiberbiztonság nem pusztán egy technikai probléma, ez egy betegbiztonsági kérdés" (Robeznieks, 2019). Különösen igaz ez a XXI. században, amikor a digitális átalakulás teljesen átalakítja az egészségügyet. Ahogy a XIX. században, Semmelweis korában a kézmosás jelentett a higiénés területen jelentős előrelépést, napjainkban ugyanezt az előrelépést a kiberhigiéne terjesztése kell, hogy jelentse.

Hazai viszonylatban az egészségügyi információ és kiberbiztonsággal kapcsolatban publikációk csak elszórtan találhatók, és ezek is főként a biztonságtudományi területen koncentrálódnak.

Tekintettel a téma jelentőségére, az egészségügy számára is érthetővé és hozzáférhetővé kell tenni a kiberbiztonsági ismereteket, mivel ez közvetlenül befolyásolja az egészségügyi intézmények működését, valamint a betegek és dolgozók biztonságát. Ebben az összefüggésben a kutatásaim során feltett kérdések megválaszolásra kerültek, illetve a felállított hipotézisek részben vagy teljesen igazolást nyertek, és számos önálló kutatási eredményt is elértem.

A digitális egészségügyi ökoszisztéma modellje jól meghatározható, és az alkotóelemek/szereplők közötti szoros kapcsolat miatt a rendszer egészének fejlesztése kiegyensúlyozott és átgondolt beavatkozásokat igényel. Az elkövetkező időszak fejlesztéseiben ennek a kiegyensúlyozottságnak kiemelt jelentőséget kell kapnia: a magyar egészségügyi rendszer nem lesz képes rendszerszinten alkalmazni az új technológiákat, ha nem az ökoszisztéma alapú megközelítés kerül a középpontba. A kiegyensúlyozatlan beavatkozások allokációs hatékonysági problémát okoznak a rendszerben. Bizonyos területekre (ökoszisztéma elemekre) túlzó mértékben kerülnek források, miközben a más elemek elmaradnak.

Az egészségügy fejlesztésében és a döntéshozatalban nem csak az egészségügyi adatokat, hanem más, az egészségügyet érintő adatokat is figyelembe kell venni, különösen válsághelyzetekben: ez olyan többlet információkat hordoz, amelyeket a döntéselőkészítésben és döntéshozatalban is használni kell, hiszen ez új rendszerképességet jelenthet, illetve hozzájárulhat a társadalom, vagy egy társadalmi alrendszer rezilienciájának növeléséhez. Ennek felhasználása csak biztonságos környezetben, szabályozottan történhet.

Az egészségügyi zsarolóvírus támadások kiemelten fontosak, és megfelelő módszertan kidolgozása szükséges a jobb megértésük, az eredményes felkészülés és megelőzés, valamint a hatékony kezelésük érdekében.

A biztonságtudatosság növelése érdekében hazai szinten is szükség van a lakosság számára szóló kampányok és beavatkozások tervezésére, amelyekhez eddig még nem történt kormányzati támogatású felmérés. Az egészségügyi intézményben dolgozók és vezetők körében is szükséges lenne a kiberbiztonsággal kapcsolatos felmérések és interjúk készítése, hogy átfogó képet kaphassunk a hazai egészségügyi kiberbiztonság állapotáról és fejlesztési lehetőségeiről.

Összefoglalóan írható, hogy valamennyi kutatási területen olyan egyedi eredményeket sikerült bemutatnom, amelyek a hazai egészségügyi kiberbiztonsági területen teljesen újak.

6.2. A kutatás limitációi

Az egyes kutatási területeken külön-külön számos korláttal szembesültem, amelyeket fontos figyelembe venni az eredmények értelmezésekor.

A digitális ökoszisztéma leírása során felmerült egyik nehézség, hogy az alkalmazott elméleti megközelítések és keretek túlnyomórészt nemzetközi példákon alapultak, amelyek nem mindig illeszkednek a magyar egészségügyi rendszer sajátosságaihoz, különösen, ha figyelembe vesszük, hogy az egészségügyi rendszerek működése, és különösen a fejlesztések, változtatások kapcsán a kulturális vonatkozások nagy hangsúlyt kapnak. Az ökoszisztéma elmeinek, szereplőinek és folyamataiknak részletes feltérképezése nem minden esetben lehetett teljes, elsősorban erőforrásbeli korlátok miatt. Az emberi tényezők és a technológiai folyamatok közötti kapcsolatok mélyebb

vizsgálata szintén csak korlátozott mértékben valósult meg, míg a gyorsan változó adatvédelmi és szabályozási környezet további kihívásokat jelent az ökoszisztéma modell aktualizálásában.

A mobiladatok hasznosítása során a legnagyobb kihívást az adatvédelmi szabályozások, különösen a GDPR korlátozásai jelentették, amelyek az adatok hozzáférhetőségét és feldolgozhatóságát jelentősen befolyásolták. Az interoperabilitási problémák és az adatminőség eltérései tovább nehezítették az elemzést, míg a viselkedési minták és mozgási adatok kontextusának hiánya, illetve az aggregáltság foka az eredmények torzításához vezethetett. Ezek a korlátok befolyásolják a mobiladatok felhasználásának lehetőségeit az egészségügyi rendszerek és folyamatok fejlesztése érdekében.

A zsarolóvírus-kutatás esetében az adatgyűjtés jelentette a legkomolyabb limitációt: az érintett szervezetek gyakran nem hozzák nyilvánosságra az incidenseket, ami retrospektív elemzésekre, másodlagos adatokra és információkra való támaszkodást tett szükségessé. Ezáltal az eredmények pontossága és általánosíthatósága korlátozott lehet. Emellett fontos kiemelni, hogy a kritikus infrastruktúrák esetében a zsarolóvírusok okozta üzletmenete folytonosság fenntartása az elsődleges cél (nagyon helyesen), ezért a mélyebb elemzéseket lehetővé tevő adatgyűjtések és részletesebb feldolgozások és elemzések csak ritkán valósulnak meg. Azok is elsősorban gyakorlati szempontúak, a tudományos mélység és alaposság – érthető okok miatt – nem napi követelmény. A sérülékenységek hátterében álló emberi tényező szerepe és a pszichológiai manipuláció („social engineering”) szintén nehezen deríthető ki, illetve nehezen számszerűsíthető, ami tovább bonyolítja a probléma átfogó vizsgálatát, holott ez az egyik legfontosabb „belépési pont” a rendszerekbe. Bár az esetek mélyebb megértésére kvalitatív módszereket, például interjúkat is alkalmaztam, ezek általában csak korlátozott következtetések levonására alkalmasak, különösen mert jelentős idő telt el az esemény és a feldolgozás között, másrészt pedig nem teljeskörűen lehetett minden korabeli résztvevőt és érintettet bevonni az esetfeldolgozásba.

A lakossági biztonságtudatosságot célzó felmérés során az egyik legfőbb limitáció az, hogy a minta jellemzői alapján korlátozottan lehet következtetéseket levonni a teljes populációra. A válaszadói minta reprezentativitása korlátozott lehetett, különösen az életkor vagy a digitális írástudás tekintetében. Az önbevalláson alapuló adatok torzíthatják az eredményeket, mivel a résztvevők hajlamosak saját

biztonságtudatosságukat idealizált módon bemutatni. Emellett fontos limitáció az is, hogy ez egy pillanatfelvételnek megfelelő keresztmetszeti képet adott, és nem tette lehetővé az adatok időbeli változásainak követését. Ezek az elemzések és információk azonban elengedhetetlenül szükségesek ahhoz, hogy célzott fejlesztési programok induljanak a biztonságtudatosítás területén.

6.3. A kutatás gyakorlati hasznosíthatósága

A kutatások és fejlesztések számos szereplő munkáját támogatják az egészségügyi területen. Elsősorban az egészségügyi politikai döntéshozók, kutatók, intézményvezetők és hatóságok profitálhatnak a kutatás eredményeiből.

A digitális egészségügyi ökoszisztéma leírása nagyban segítheti a kiegyensúlyozott, fenntartható fejlesztések kereteinek megalkotását. Önmagában nem elegendő pl. az infrastruktúra fejlesztés, vagy digitális szolgáltatások, és alkalmazások előállítása, hanem ahhoz, hogy fenntarthatók legyenek a fejlesztések, a többi ökoszisztéma elemet is fejleszteni kell. Szintén fontos hasznosíthatósága ennek a megközelítésnek, hogy ezt egy kisebb területen is lehet alkalmazni. Például általában az információbiztonság esetében is érdemes az ökoszisztéma fogalmát meghatározni, de az egészségügyön belül is lehetnek speciális vonatkozásai ennek a kisebb ökoszisztémának, mint ahogy azt a mesterséges intelligencia fejlesztésekre vonatkozóan is megemlítettem.

A biztonságos innovatív adatfeldolgozás kapcsán alkalmazott módszertani fejlesztéseknek köszönhetően új lehetőségek nyílnak meg, például a közismert GPS, vagy a CDR adatok és egyéb, az egészségügyi döntéshozatalban hasznosítható információk integrálása. Emellett egy olyan rendszer prototípusát alakítottuk ki, amely számos veszélyhelyzetben alkalmazható, illetve más tudományterületek bevonásával ki is terjeszthető.

Az egyik legfontosabb általánosan is használható eredmény, hogy az egészségügy, mint kritikus infrastruktúra területén, sikerült hiánypótló eredményeket elérni. Továbbá, a kutatás során számos saját ötlet és innováció is megvalósult, amelyek a tudás gyakorlati alkalmazását segítik elő.

A zsarolóvírusok elleni védekezésben kidolgozott új esetfeldolgozási módszertan jelentős előrelépést jelenthet az események megértése és a következmények megítélése terén. A módszertan alapja egy átfogó és strukturált megközelítés, amely célzottan az egészségügyi intézmények sajátosságaira és a zsarolóvírusok jellegzetességeire összpontosít. Az új módszertan segítheti az egészségügyi intézmények és hatóságok közötti kommunikációt, a tapasztalatok feldolgozását, és ez alapján a reagálást és a helyreállítást is egy esetleges támadás után. Emellett ezek az esetek jól felhasználhatók az egészségügyi felsőfokú képzésben, az egészségügyi dolgozók élethossziglani továbbképzésében, valamint különböző érzékenyítő és tudatosító tréningeken.
A lakossági adatfelvétel és feldolgozás kapcsán fontos kiemelni, hogy a kérdőív folyamatos fejlesztésével lehetőség van még árnyaltabban megismerni a biztonságtudatossággal kapcsolatos ismereteket és attitűdöt, illetve a későbbiekben lehetőség szerint a különböző ágazati sajátosságok beépítésével ágazatspecifikus megismerés válik lehetővé, amely alapján pontos beavatkozások tervezhetők érzékenyítésre vagy éppen a tudatosság szintjének növelésére. Ezt a fejlesztési munkát már elkezdtük a Nemzeti Kibervédelmi Intézettel. A 2023-as felmérésben már ágazati összehasonlításra is lesz lehetőség, és várhatóan 6000 választ tudunk feldolgozni.

A kérdőíves feldolgozással lehetőség van kockázatos célcsoportok azonosítására, és a kockázatok alapján specifikus képzések kialakítására a csoportok számára. Emellett a fejlesztések révén ki lehet alakítani olyan kérdőívet is, amelyben már nemcsak csoportos, hanem egyéni kockázatok is azonosíthatók, és például egy-egy munkakör betöltésénél, vagy éppen egy munkahelyi továbbképzésnél személyre szabható a kiválasztás, vagy a belső képzési programok. Ezen a területen a tovább fejlesztésre lehetőség lesz azáltal is, hogy az áldozattá válás területén indítunk közös projektet a Magyar Bankszövetséggel és a Nemzeti Kibervédelmi Intézettel.

Arra építve, hogy az információbiztonsági hírek olvasása kritikusan fontos, 2022. áprilisától elérhetővé tettük az Egészségügyi Kiberbiztonsági Szemlét, amelynek célja, hogy az ágazatban dolgozók számára nyújtson korszerű, naprakész ismereteket, információt. A Szemlét rendszeresen eljuttatjuk valamennyi egészségügyi intézménybe, ezzel is támogatva a szektor kiberbiztonsági felkészültségét. A létrejött hálózat, amely

információbiztonsági és informatikai szakemberekből, egészségügyi dolgozókból, kórházi és más egészségügyi szolgáltatókban dolgozó munkatársakból áll, segít a szektor mobilizálásában is. Ennek köszönhetően 2023 őszén példátlan sikerrel rendezte meg a Nemzeti Kibervédelmi Intézet az egészségügyi intézmények HunEx nevű kibervédelmi gyakorlatát.

Az új technológiák tekintetében ki kell emelni a mesterséges intelligencia és a biztonság összefüggéseit. Ezt támogatjuk a Nemzeti Labor kereteiben létrehozott Mesterséges Intelligencia Radar-ral, amely követi, hogy biztonsági szempontból milyen feltételeknek felelnek meg ezek az alkalmazások - kiberbiztonsági kihívásokat és a fejlesztések állapotát az elkövetkező években.

A kutatások eredményei több hazai és nemzetközi szakmai és kutatási együttműködés elindulását is ösztönözték, amelyekben aktív résztvevőként és kezdeményezőként is jelen vagyok. Példaként említhetem az ENISA által 2024. novemberében a Semmelweis Egyetemen nemzetközi előadókkal és résztvevőkkel megrendezett 9. e-Health Cybersecurity Konferencát, az Egészségbiztonság Nemzeti Labor Adatvezérelt Egészség Divízióját, ahol a terület vezetőjeként dolgozom, illetve részt vettem az ECHO projektben is, amely az Európai Unió H2020 kutatási programján belül az egyik támogatott kiberbiztonsági projekt volt.

7. Összefoglalás

Kutatásomban az egészségügy digitális átalakulásához kötődően vizsgáltam meg az adat- és információbiztonság aspektusait.

Elsődlegesen egy olyan modellt alkottam, amely segítheti a digitális fejlesztéseket kiegyensúlyozottá tenni: a digitális egészségügyi ökoszisztéma modelljének bevezetése, és az elemeinek meghatározása abban segít, hogy az egyes elemek egyensúlyának megteremtése révén egy működőképes, fenntartható és forrásallokációs szempontból hatékony digitális rendszer jöjjön létre. A modellben az egészségügyi adat kap kiemelt szerepet: ennek van és lesz az elkövetkező időszakban a legnagyobb szerep és értéke.

A kutatásomban azt is bemutattam, hogy az egészségügyi adatok mellett más adatok is bevonhatók az egészségügyi döntéshozatalba, különösen veszélyhelyzet esetén. A biztonságos innovatív adathasználat megteremtésével bemutattam, hogy mobilszolgálatók által biztosított cellatorony adatokkal olyan mutatók alakíthatók ki, amelyek képesek döntés előkészítésére, vagy egy-egy beavatkozás monitorozására,

Az egészségügyi adatok bizalmasságát, rendelkezésre állását és sértetlenséget napjainkban leginkább a zsarolóvírus támadások veszélyeztetik. Hazai esetek feldolgozásával sikerült bemutatnom, hogy a sikeres felkészülésnek és védekezésnek az egyik fontos része a megfelelő adatgyűjtés és adatfeldolgozás. Ehhez a jelenlegi formákon változtatni szükséges, szélesebb körűnek kell lennie az adatfelvételnek, és az adatok kutathatósága mellett kiemelt fontosságú a tudományos és egészségügyi szakmai disszemináció.

A fenti információbiztonsági események kapcsán az egyik legfontosabb szempont, hogy ezeket az eseményeket lehetőség szerint megelőzzük, amelyhez célcsoport specifikus biztonságtudatosítás szükséges. A magas kockázatú célcsoport sajátosságainak meghatározáshoz országos lakossági felmérést végeztünk és a beérkezett több, mint 1500 választ feldolgoztuk. Munkánk során kimutattuk, hogy a szociodemográfiai tényezők közül a nem és az iskolai végzettség befolyásolja leginkább a biztonságtudatos magatartást. Emellett a kutatás azt is kimutatta, hogy a biztonságtudatosság jellegzetes magatartásmintázattal jár, és ebben meghatározó volt, hogy a válaszadó milyen olvasottsággal rendelkezik az információbiztonság területén.

A bemutatott kutatásokkal az egészségügyi kiberbiztonság területén új kutatási eredményeket és tudást hoztam létre.

7. Summary

In my research, I examined aspects of data and information security in the context of healthcare's digital transformation.

My primary focus was to create a model that can help balance digital development: introducing a model of the digital health ecosystem and defining its elements will help to create a workable, sustainable, and resource-allocative digital system by balancing the elements. Health data is a key element of the model: it has and will have the greatest role and value in the period ahead.

In my research, I have also shown that other data than health data can be included in health decision-making, especially in emergencies. By creating a secure innovative use of data, I have shown that cell tower data provided by mobile service providers can be used to develop indicators that can be used to prepare a decision or monitor an intervention,

Today, the confidentiality, availability, and integrity of healthcare data are most at risk from ransomware attacks. By working on domestic cases, I have been able to show that one important part of successful preparedness and defense is proper data collection and processing. This requires a change in the current patterns, a wider collection of data, and, in addition to the researchability of the data, the dissemination of scientific and health professional information is of paramount importance.

One of the most important aspects of the above information security incidents is to prevent them as far as possible, which requires target group-specific security awareness. To identify the specificities of the high-risk target group, a nationwide population survey was conducted and the more than 1500 responses received were processed. Our work has shown that, among sociodemographic factors, gender and educational attainment are the most important influences on safety-conscious behavior. In addition, the research also showed that security awareness is associated with a characteristic pattern of behavior and that the respondent's literacy in information security was a determinant of this.

The presented research has generated new research findings and knowledge in the field of health cybersecurity.

8. Irodalomjegyzék

Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security Requirements and Challenges of 6G Technologies and Applications. Sensors (Basel), 22(5). https://doi.org/10.3390/s22051969

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). Moving beyond cyber security awareness and training to engendering security knowledge sharing. Information Systems and e-Business Management, 21(1), 123-158. https://doi.org/10.1007/s10257-022-00575-2

Alsharif, M., Mishra, S., & AlShehri, M. (2021). Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science and Engineering, 40(3), 1153-1166. https://doi.org/10.32604/CSSE.2022.019938

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219-238. https://doi.org/10.3390/jcp1020012

Bakacsi, G. (2015). A szervezeti magatartás alapjai - Alaptankönyv Bachelor hallgatók számára. (pp. 75-79). Semmelweis Kiadó.

Balogh, J., Szócska, M., Palicz, T., Kontsek, E., Pollner, P., Varga, G., Ugrin, I., Davidovics, K., & Joó, T. (2022). A mesterséges intelligencia alapú megoldások fejlesztése és bevezetése az egészségügyben – kézműves manufaktúrától a gyártósorig? IME - Az egészségügyi vezetők szaklapja, 21(2), 56-63. https://doi.org/10.53020/ime-2022-206

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers and Security, 111, 102490. https://doi.org/10.1016/J.COSE.2021.102490

Benis, A., Tamburis, O., Chronaki, C., & Moen, A. (2021). One Digital Health: A Unified Framework for Future Health Ecosystems. Journal of Medical Internet Research, 23(2), e22189. https://doi.org/10.2196/22189

Bloomberg, J. (2018). Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril. Retrieved 2019 August 28 from

https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/

Bognár, B., & Bonnyai, T. (2019). Kritikus infrastruktúrák védelme. (pp. 37). Dialóg Campus.

Bucci, S., Schwannauer, M., & Berry, N. (2019). The digital revolution and its impact on mental health care. Psychology and Psychotherapy: Theory, Research and Practice, 92(2), 277-297. https://doi.org/10.1111/papt.12222

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2020). Cyber-Angriff auf Uniklinik Düsseldorf: BSI warnt vor akuter Ausnutzung be-kannter Schwachstelle Retrieved 2020 October 20 from https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

CEB United Nation System. (2022). Digital & Technology Network (DTN) Session Report. Retrieved 2024 August 20 from https://unsceb.org/sites/default/files/2022-12/20221209%20DTN%20Meeting%20Report.pdf

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2021). A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture. IEEE Internet Things Journal, 8(13), 10248-10263. https://doi.org/10.1109/jiot.2020.3041042

Chen, M., & Decary, M. (2020). Artificial intelligence in healthcare: An essential guide for health leaders. Healthcare Management Forum, 33(1), 10-18. https://doi.org/10.1177/0840470419873123

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. Health Services Research, 54(5), 971-980. https://doi.org/10.1111/1475-6773.13203

Cybersecurity and Infrastructure Security Agency (CISA). (2021). What is Cybersecurity? | CISA. Retrieved 2022 December 10 from https://www.cisa.gov/uscert/ncas/tips/ST04-001

Császár, A., Halmos, B., Palicz, T., Szalai, C., & Romics, L. (1997). Interpopulation effect of ACE I/D polymorphism on serum concentration of ACE in diagnosis of

sarcoidosis. Lancet, 350(9076), 518. https://doi.org/10.1016/s0140-6736(05)63108-x

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Education and Information Technologies, 27(4), 4729-4752. https://doi.org/10.1007/s10639-021-10806-7

Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., Hemmen, T. M., Clay, B. J., & Longhurst, C. A. (2023). Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. JAMA Network Open, 6(5), e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

Diaz, N. (2022). Google developing AI smartphone healthcare tools. Retrieved 2022 November 9 from https://www.beckershospitalreview.com/disruptors/google-developing-ai-smartphone-healthcare-tools.html

Ellahham, S. (2020). Artificial Intelligence: The Future for Diabetes Care. The American journal of medicine, 133(8), 895-900. https://doi.org/10.1016/J.AMJMED.2020.03.033

Ellahham, S., Ellahham, N., & Simsekler, M. C. E. (2020). Application of Artificial Intelligence in the Health Care Safety Context: Opportunities and Challenges. American Journal of Medical Quality, 35(4), 341-348. https://doi.org/10.1177/1062860619878515

Európai Bizottság. (2012). Elektronikus egészségügyi cselekvési terv a 2012–2020 közötti időszakra – innovatív egészségügyi ellátás a 21. században Európai Bizottság, Brüsszel. Retrieved 2020 March 9 from https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012DC0736&from=PL

Európai Bizottság. (2014). A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a hatékony, hozzáférhető és alkalmazkodóképes egészségügyi rendszerekről. Retrieved 2020 March 9 from https://ec.europa.eu/health/sites/health/files/systems_performance_assessment/docs/com2014_215_final_hu.pdf

European Comission. (2012). EU Task Force on eHealth: Redesigning health in Europe for 2020. Publication Office of European Union, Luxembourg. Retrieved 2020 March 9 from https://digital-strategy.ec.europa.eu/en/library/eu-task-force-ehealth-redesigning-health-europe-2020

European Union Agency for Cybersecurity (ENISA). (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. In (pp. 22). https://doi.org/10.2824/324042

Fausto, A., Gaggero, G. B., Patrone, F., Girdinio, P., & Marchese, M. (2021). Toward the integration of cyber and physical security monitoring systems for critical infrastructures. Sensors (Basel), 21(21). https://doi.org/10.3390/S21216970

Frey, L. J. (2018). Data integration strategies for predictive analytics in precision medicine. Personalized Medicine, 15(6), 543-551. https://doi.org/10.2217/pme-2018-0035

Frisinger, A., & Papachristou, P. (2024). Bridging the voice of healthcare to digital transformation in practice – a holistic approach. BMC Digital Health, 2(1), 12. https://doi.org/10.1186/s44247-024-00066-z

Gaál, P., Joó, T., Palicz, T., Pollner, P., Schiszler, I., & Szócska, M. (2021). Adattudományi innováció az egészségügy környezeti kihívásainak kezelésében: a nagy adatállományok hasznosításának jelentősége és lehetőségei a járványkezelésben. Scientia et Securitas, 2(1), 2-11. https://doi.org/10.1556/112.2021.00014

GBD 2021 Anaemia Collaborators. (2023). Prevalence, years lived with disability, and trends in anaemia burden by severity and cause, 1990-2021: findings from the Global Burden of Disease Study 2021. Lancet Haematology, 10(9), e713-e734. https://doi.org/10.1016/s2352-3026(23)00160-6

Gémes, C. (2018). A kibertér szereplői. Hadmérnök, XIII.(3), 13. http://hadmernok.hu/183_30_gemes.pdf

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. Healthcare (Basel), 10(2), 327. https://doi.org/10.3390/healthcare10020327

Godin, K., Stapleton, J., Kirkpatrick, S. I., Hanning, R. M., & Leatherdale, S. T. (2015). Applying systematic review search methods to the grey literature: a case study examining guidelines for school-based breakfast programs in Canada. Systematic Reviews, 4(1), 138. https://doi.org/10.1186/s13643-015-0125-0

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. JAMA Network Open, 2(3), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Grantz, K. H., Meredith, H. R., Cummings, D. A. T., Metcalf, C. J. E., Grenfell, B. T., Giles, J. R., Mehta, S., Solomon, S., Labrique, A., Kishore, N., Buckee, C. O., & Wesolowski, A. (2020). The use of mobile phone data to inform analysis of COVID-19 pandemic epidemiology. Nature Communications, 11(1). https://doi.org/10.1038/s41467-020-18190-5

Greevy, H. (2022). Healthcare's Ultimate Guide to Gmail: Is Gmail HIPAA compliant? Retrieved 2023 October 22 from https://www.paubox.com/blog/is-gmail-hipaa-compliant

Győrffy, Z., Békási, S., Szathmári-Mészáros, N., & Németh, O. (2020). Possibilities of telemedicine regarding the COVID-19 pandemic in light of the international and Hungarian experiences and recommendations. Ovosi Hetilap, 161(24), 983-992. https://doi.org/10.1556/650.2020.31873

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/https://doi.org/10.1016/j.heliyon.2017.e00346

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research, 23(4), e21747. https://doi.org/10.2196/21747

Herzog, A. R., & Bachman, J. G. (1981). Effects of questionnaire length on response quality. Public Opinion Quarterly, 45(4), 549-559. https://doi.org/10.1086/268687

Hong, Y., Kim, M.-J., & Roh, T. (2023). Mitigating the Impact of Work Overload on Cybersecurity Behavior: The Moderating Influence of Corporate Ethics—A Mediated Moderation Analysis. Sustainability, 15(19), 14327. https://www.mdpi.com/2071-1050/15/19/14327

Husák, M., Jirsík, T., & Yang, S. J. (2020). SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security ARES 2020, Virtul Event, Ireland. https://dx.doi.org/10.1145/3407023.3407062

Inan, O. T., Tenaerts, P., Prindiville, S. A., Reynolds, H. R., Dizon, D. S., Cooper-Arnold, K., Turakhia, M., Pletcher, M. J., Preston, K. L., Krumholz, H. M., Marlin, B. M., Mandl, K. D., Klasnja, P., Spring, B., Iturriaga, E., Campo, R., Desvigne-Nickens, P., Rosenberg, Y., Steinhubl, S. R., & Califf, R. M. (2020). Digitizing clinical trials. npj Digital Medicine, 3(1). https://doi.org/10.1038/s41746-020-0302-y

James F. Moore. (1993). Predators and Prey: A New Ecology of Competition. Harvard Business Revew, 1993 May-June. https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition

Janofsky, A. (2019). Smaller Medical Providers Get Burned by Ransomware. Wall Street Journal. Retrieved 2020 8 March from https://www.wsj.com/articles/smaller-medical-providers-get-burned-by-ransomware-11570366801

Kataria, S., & Ravindran, V. (2020). Electronic health records: A critical appraisal of strengths and limitations. Journal of the Royal College of Physicians of Edinburgh, 50(3), 262-268. https://doi.org/10.4997/JRCPE.2020.309

Kim, L. (2020). Cybercrime, ransomware, and the role of the informatics nurse. Nursing, 50(3), 63-65. https://doi.org/10.1097/01.NURSE.0000654064.67531.C5

Ködmön, J., & Csajbók, Z. E. (2015). Információbiztonság az egészségügyben. Orvosi Hetilap, 156(27), 1075-1080. https://doi.org/10.1556/650.2015.30196

Krasznay, C., & Hámornik, B. P. (2018). Analysis of Cyberattack Patterns by User Behavior Analytics. Academic and Applied Research in Military and Public Management Science, 17(3), 101-113. https://doi.org/10.32565/aarms.2018.3.7

Magyar Országgyűlés. (1997). 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről *. Retrieved 2022 March 28 from https://net.jogtar.hu/jogszabaly?docid=99700047.tv

Magyar Országgyűlés. (2011). 2011. évi CLIV. törvény a megyei önkormányzatok konszolidációjáról, a megyei önkormányzati intézmények és a Fővárosi Önkormányzat egyes egészségügyi intézményeinek átvételéről - Hatályos Jogszabályok Gyűjteménye. Retrieved 2020 October 8 from https://net.jogtar.hu/jogszabaly?docid=a1100154.tv

Magyar Országgyűlés. (2013). 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról - Hatályos Jogszabályok Gyűjteménye. Retrieved 2022 March 28 from https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

Magyarország Kormánya. (2013). 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Retrieved 2020 October 8 from https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf

Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020). An Investigation of Biometric Authentication in the Healthcare Environment. Array, 8, 100042-100042. https://doi.org/10.1016/J.ARRAY.2020.100042

Mikesy, G., Palicz, T., & Sinka, L. A. E. (2020). COVID-19 menedzsment ajánlás a telemedicina használatáról. In L. A. E. Sinka (Ed.), COVID-19 kórházi menedzsment-ajánlásaink (pp. 115-120). Semmelweis Egyetem Egészségügyi Menedzserképző Központ.

Mirsky, Y., Mahler, T., Shelef, I., & Elovici, Y. (2019). CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning USENIX Security Symposium, https://doi.org/10.48550/arXiv.1901.03597

Mitchell, M., & Kan, L. (2019). Digital Technology and the Future of Health Systems. Health Systems & Reform, 5(2), 113-120. https://doi.org/10.1080/23288604.2019.1583040

Munné, R. (2016). Big data in Public Sector in New Horizons for a Data-Driven Economy. In J. M. Cavanillas, E. Curry, & W. Wahlster (Eds.), (pp. 195-208). https://doi.org/https://doi.org/10.1007/978-3-319-21569-3

Nadkarni, S., & Prügl, R. (2021). Digital transformation: a review, synthesis and opportunities for future research. Management Review Quarterly, 71(2), 233-341. https://doi.org/10.1007/s11301-020-00185-7

Németh, L. (2019). Újabb dimenziók az EESZT használatával. Orvosi Hetilap, 160(4), 160-160. https://doi.org/10.1556/650.2019.4m

Nemzeti Média- és Hírközlési Hatóság (NMHH). (2020). A Nemzeti Média- és Hírközlési Hatóság mobilpiaci jelentése, Tárgyidőszak: 2015. IV. - 2019. IV. negyedév. Retrieved 2020 9 October from https://nmhh.hu/dokumentum/211976/NMHH_mobilpiaci_jelentes_2015Q42019Q4.pdf

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum, 3(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

NHS Health Education England. (2023). Profession and Service Specific Digital Capabilities Frameworks. Retrieved 2023 October 23 from https://digital-transformation.hee.nhs.uk/building-a-digital-workforce/digital-literacy/digital-capabilities-frameworks

Nomura, A., Noguchi, M., Kometani, M., Furukawa, K., & Yoneda, T. (2021). Artificial Intelligence in Current Diabetes Management and Prediction. Current Diabetes Reports, 21(12), 61. https://doi.org/10.1007/s11892-021-01423-2

Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. Procedia Computer Science, 181, 173-181. https://doi.org/https://doi.org/10.1016/j.procs.2021.01.118

Nyikes, Z. (2019). Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel - Doktori értekezés [PhD, Óbudai Egyetem]. http://www.lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Nyikes_Zoltan_ertekezes.pdf

Oroszi, E. D. (2020). Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasz-náló támadási technikák és megelőzésük. Dunakavics, VIII.(V), 5-20. http://dunakavics.uniduna.hu/Online_2005.pdf

Paez, A. (2017). Gray literature: An important resource in systematic reviews. Journal of Evidence-Based Medicine, 10(3), 233-240. https://doi.org/10.1111/jebm.12266

Palicz, T., Bencsik, B., & Szócska, M. (2021). Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai. Scientia et Securitas, 2(1), 78-87. https://doi.org/10.1556/112.2021.00001

Palicz, T., Bonnyai, T., Bencsik, B., Pinter, L., Dombradi, V., Joo, T., Bor, O., & Hornyik, Z. (2022). Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei. Belügyi Szemle, 70(2), 395-418. https://doi.org/10.38146/BSZ.2022.2.11

Palicz, T., & Joó, T. (2020). Az infrastuktúra-védelem és az információbiztonság kapcsolata. In (pp. 21-31).

Palicz, T., Sas, T., Szabó, Z., Tóth, T., Tisóczki, J., Bencsik, B., & Joó, T. (2021). Magyar kórházakban előfordult zsarolóvírus támadások esetei. IME - Az egészségügyi vezetők szaklapja, XX(1), 32-38. https://www.imeonline.hu/tmp/38d29c031eab81ea57816be32bb9708b.pdf

Palicz, T., Sas, T., Tisóczki, J., Bencsik, B., & Joó, T. (2020). „Pénzt vagy életet!"– Zsarolóvírusok az egészségügyi informatikai rendszerekben. Orvosi Hetilap, 161, 1498-1505. https://doi.org/10.1556/650.2020.31788

Palicz, T., Vártok, J., & Szócska, G. (2003). A folyamat-újraszervezési (BPR) projektek tatpasztalatai az egészségügyben. IME - Az egészségügyi vezetők szaklapja, II(2), 17-22. https://www.imeonline.hu/tmp/423e82a83b6b5ff52bfb5c848bf2aedf.pdf

Puzis, R., Farbiash, D., Brodt, O., Elovici, Y., & Greenbaum, D. (2020). Increased cyber-biosecurity for DNA synthesis. Nature Biotechnology, 38(12), 1379-1381. https://doi.org/10.1038/s41587-020-00761-y

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health*, *8*. https://journals.sagepub.com/doi/abs/10.1177/20552076221081716

Robeznieks, A. (2019). Cybersecurity: Ransomware attacks shut down clinics, hospitals. Retrieved 2021 October 8 from https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals

Roth, C. B., Papassotiropoulos, A., Brühl, A. B., Lang, U. E., & Huber, C. G. (2021). Psychiatry in the Digital Age: A Blessing or a Curse? International Journal of Environmental Research and Public Health, 18(16), 8302. https://doi.org/10.3390/ijerph18168302

Russell Ritenour, E. (2020). Hacking and Ransomware: Challenges for Institutions Both Large and Small. American Journal of Roentgenology, 214(4), 736-737. https://doi.org/10.2214/AJR.19.22620

SaberiKamarposhti, M., Ng, K.-W., Chua, F.-F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon, 10(10), e31406. https://doi.org/https://doi.org/10.1016/j.heliyon.2024.e31406

Sasse, N. M., & Flechais, I. (2005). Usable Security: Why Do We Need It? How Do We Get It? L. Cranor & S. Garfinkel (Eds.), Security and Usability: Designing secure systems that people can use (pp. 13-30). O'Reilly

Saunders, C., Currie, D., Virani, S., & De Grood, J. (2022). Navigating the Systemic Conditions of a Digital Health Ecosystem in Alberta, Canada: Embedded Case Study. JMIR Formative Research, 6(12), e36265. https://doi.org/10.2196/36265

Security Service MI5. (2023). Five Eyes intelligence partners launch outreach drive to secure innovation. Retrieved 2023 October 22 from https://www.mi5.gov.uk/news/five-eyes-launch-drive-to-secure-innovation

Senyo, P. K., Liu, K., & Effah, J. (2019). Digital business ecosystem: Literature review and a framework for future research. International Journal of Information Management, 47, 52-64. https://doi.org/10.1016/J.IJINFOMGT.2019.01.002

Shipman, S. L., Nivala, J., Macklis, J. D., & Church, G. M. (2017). CRISPR–Cas encoding of a digital movie into the genomes of a population of living bacteria. Nature, 547(7663), 345-349. https://doi.org/10.1038/nature23017

Stroetmann, K., Artmann, J., Stroetmann, V., Protti, D., Dumortier, J., Giest, S., Walossek, U., & Whitehouse, D. (2011). European Countries on their journey towards national eHealth infrastructures. Európai Bizottság, Információs Társadalmi és Médiaügyi Főigazgatóság, Publications Office. https://doi.org/doi/10.2759/47528

Szabó, H. (2021). Kiberbiztonság a koronavírusjárvány idején. A COVID-19 nemzetbiztonsági aspektusai. Rendvédelem - A Belügyi Tudományos Tanács online folyóirata(1), 52-70. https://epa.oszk.hu/03300/03353/00017/pdf/EPA03353_rendvedelem_2021_1_052-070.pdf

Szabo, Z. A., Szócska, M., Palicz, T., Szerencses, V., & Joó, T. (2021). A digitális egészségügyi ökoszisztéma fogalmának és elemeinek nemzetközi és hazai áttekintése. InfTárs - Információsó Társadalom, XXI(3). https://doi.org/https://dx.doi.org/10.22503/inftars.XXI.2021.3.3

Szádeczky, T., & Szőke, G. L. (2018). A bizalmasság és a nyilvánosság aktuális kihívásai az információbiztonság tükrében. ProFuturo(2), 24-41. https://doi.org/10.26521/Profuturo/2018/2/4716

Szalai, C., Császár, A., Czinner, A., Palicz, T., Halmos, B., & Romics, L. (1999). Genetic investigation of patients with hypercholesterolemia type IIa. Clinical Genetics, 55(1), 67-68. https://doi.org/10.1034/j.1399-0004.1999.550114.x

Szerencsés, V., Palicz, T., Joó, T., Demeter-Fülöp, V., Ugrin, I., & Lám, J. (2021). A Covid19 járvány során hozott egészségügyi intézkedések és hatásaik Magyarországon és Ausztriában. Belügyi Szemle, 69(1), 123-142. https://doi.org/10.38146/bsz.2021.1.6

Szócska, M., & Joó, T. (2018). Health Security Issues. G. Finszter & I. Sabjanics (Eds.), Security Challanges in the 21st Century (pp. 335-347). Nordex Non-Profit Ltd. – Dialóg Campus Publishing. https://www.bm-tt.hu/assets/letolt/secchal21.pdf

Szócska, M., Joó, T., Gál, A. L., Lőrincz, O., Auer, A., & Palicz, T. (2019). A hálózatkutatás alkalmazhatósága a közszolgáltatások fejlesztésében. A. Auer & T. Joó (Eds.), Hálózatok a közszolgálatban (pp. 9-25). Dialóg Campus, Budapest.

Szócska, M., Pollner, P., Schiszler, I., Joo, T., Palicz, T., McKee, M., Asztalos, A., Bencze, L., Kapronczay, M., Petrecz, P., Toth, B., Szabo, A., Weninger, A., Ader, K., Bacskai, P., Karaszi, P., Terplan, G., Tuboly, G., Sohonyai, A., . . . Gaál, P. (2021). Countrywide population movement monitoring using mobile devices generated (big) data during the COVID-19 crisis. Scientific Reports, 11(1), 5943. https://doi.org/10.1038/s41598-021-81873-6

Szócska, M., Réthelyi, J., & Normand, C. (2005). Managing healthcare reform in Hungary: challenges and opportunities. British Medical Journal, 331(7510), 231-233. https://doi.org/10.1136/bmj.331.7510.231

Szombathy, T., Szalai, C., Barna, K., Palicz, T., Romics, L., & Császár, A. (1998). Association of angiotensin II type 1 receptor polymorphism with resistant essential hypertension. Clinica Chimica Acta, 269(1), 91-100. https://doi.org/10.1016/s0009-8981(97)00184-8

Tham, Y. C., Husain, R., Teo, K. Y. C., Tan, A. C. S., Chew, A. C. Y., Ting, D. S., Cheng, C. Y., Tan, G. S. W., & Wong, T. Y. (2022). New digital models of care in ophthalmology, during and beyond the COVID-19 pandemic. British Journal of Ophthalmology, 106(4), 452-457. https://doi.org/10.1136/BJOPHTHALMOL-2020-317683

Tobias, B., Kujber, V., Kosa, J., & Palicz, T. (2022). Digitalizáció szerepe a genetikai vizsgálatokban: döntéstámogató rendszer fejlesztése a hazai genetikai tanácsadás segítésére. IME - Az egészségügyi vezetők szaklapja, 21(4). https://doi.org/https://doi.org/10.53020/IME-2022-405

Tóth, T., Palicz, T., & Szócska, M. (2020). A magyar egészségügyi szakemberek digitális technológiákkal kapcsolatos attitüdjének vizsgálata. IME - Az egészségügyi vezetők szaklapja, XIX(2), 44-48. https://www.imeonline.hu/tmp/43afe7990b1d2c4953882dfaa9dcb0bf.pdf

Ugrin, I., Dombrádi, V., Joó, T., Nagyjánosi, L., Palicz, T., Varga, G., Lakatos, B., Szerencsés, V., & Lám, J. (2022). Élethosszan át tartó oltási stratégia mint eszköz a pandémiák elleni védekezésben Magyarországon. Orvosi Hetilap, 163(14), 535-543. https://doi.org/10.1556/650.2022.32408

van Boven, L. S., Kusters, R. W. J., Tin, D., van Osch, F. H. M., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C., & Barten, D. G. (2024). Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals. Annals of Emergency Medicine, 83, 46-56. https://doi.org/10.1016/j.annemergmed.2023.04.025

Vida, Z., Vissi, B., Palicz, T., & Lám, J. (2021). Smart & Safe - intézményi digitalizációs stratégia a betegbiztonság szemszögéből. Orvosi Hetilap, 162(47), 1876-1884. https://doi.org/10.1556/650.2021.32289

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes. In. Publications Office of the European Union, Luxembourg. https://doi.org/https://dx.doi.org/10.2760/115376

Vuorikari, R., Punie, Y., Carretero Gomez, S., & Van Den Brande, G. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. https://doi.org/10.2791/607218

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in Digital Health, 4, 862221. https://doi.org/10.3389/fdgth.2022.862221

World Health Organization. (2000). The World Health Report, Health Systems: Improving Performance. Retrieved 2020 April 9 from https://cdn.who.int/media/docs/default-source/health-financing/whr-2000.pdf?sfvrsn=95d8b803_1&download=true

World Health Organization. (2019). WHO guideline: recommendations on digital interventions for health system strengthening. World Health Organization, Geneva. Retrieved 2020 March 10 from https://iris.who.int/bitstream/handle/10665/311941/9789241550505-eng.pdf

World Health Organization. (2020). Global strategy on digital health 2020 – 2025. World Health Organization, Geneva. https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

Zhang, J., Van Gorp, D., & Kievit, H. (2023). Digital technology and national entrepreneurship: An ecosystem perspective. The Journal of Technology Transfer, 48(3), 1077-1105. https://doi.org/10.1007/s10961-022-09934-0

9. Saját publikációk jegyzéke

(készült a Semmelweis Egyetem Központi Könyvtára által 2024. július 1-én kiadott igazolás alapján)

9.1. Értekezés témájához kapcsolódó saját publikációk:

1. Balogh Judit, Szócska Miklós, **Palicz Tamás,** Kontsek Endre, Pollner Péter, Varga Gergely, Ugrin Irina, Davidovics Krisztina, Joó Tamás. A mesterséges intelligencia alapú megoldások fejlesztése és bevezetése az egészségügyben –kézműves manufaktúrától a gyártósorig?
IME 21: 2 pp. 56-63. (2022) Szakcikk (Folyóiratcikk)

2. **Palicz Tamás,** Bonnyai Tünde, Bencsik Balázs, Pintér Levente, Dombrádi Viktor, Joó Tamás, Bor Olivér, Hornyik Zsuzsanna. Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei
BELÜGYI SZEMLE / ACADEMIC JOURNAL OF INTERNAL AFFAIRS: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA (2010-) 70: 2 pp. 395-418. (2022) Szakcikk (Folyóiratcikk)

3. Tobiás Bálint, Klujber Valéria, Kósa János, **Palicz Tamás.** Digitalizáció szerepe a genetikai vizsgálatokban: döntéstámogató rendszer fejlesztése a hazai genetikai tanácsadás segítésére
IME 21: 4 pp. 40-48. (2022) Összefoglaló cikk (Folyóiratcikk)

4. Ugrin Irina, Dombrádi Viktor, Joó Tamás, Nagyjánosi László, **Palicz Tamás,** Varga Gergely, Lakatos Botond, Szerencsés Viktória, Lám Judit. Élethosszan át tartó oltási stratégia mint eszköz a pandémiák elleni védekezésben Magyarországon [Lifelong vaccination strategy as a tool against pandemics in Hungary]
ORVOSI HETILAP 163: 14 pp. 535-543. (2022) Összefoglaló cikk (Folyóiratcikk)

5. Gaál Péter, Joó Tamás, **Palicz Tamás,** Pollner Péter, Schiszler István, Szócska Miklós. Adattudományi innováció az egészségügy környezeti kihívásainak kezelésében: a nagy adatállományok hasznosításának jelentősége és lehetőségei a járványkezelésben
SCIENTIA ET SECURITAS 2: 1 pp. 2-11. (2021) Szakcikk (Folyóiratcikk)

6. **Palicz Tamás,** Bencsik Balázs, Szócska MiklósKiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai
SCIENTIA ET SECURITAS 2: 1 pp. 78-87. (2021) Összefoglaló cikk (Folyóiratcikk)

7. **Palicz Tamás,** Sas Tibor, Szabó Zoltán, Tóth Tamás, Tisóczki József, Bencsik Balázs, Joó Tamás. Magyar kórházakban előfordult zsarolóvírus támadások esetei
IME 20: 1 pp. 32-38. (2021) Szakcikk (Folyóiratcikk)

8. Szabó Zoltán Attila, Szócska Miklós, **Palicz Tamás,** Szerencsés Viktória, Joó Tamás. A digitális egészségügyi ökoszisztéma fogalmának és elemeinek nemzetközi és hazai áttekintése [Global and national overview of the digital health ecosystem]
INFORMÁCIÓS TÁRSADALOM: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT 21: 3 pp. 47-66. (2021) Összefoglaló cikk (Folyóiratcikk)

9. Szerencsés Viktória, **Palicz Tamás,** Joó Tamás, Lám Judit, Demeter-Fülöp Virág, Ugrin Irina. A Covid19 járvány során hozott egészségügyi intézkedések és hatásaik Magyarországon és Ausztriában
BELÜGYI SZEMLE / ACADEMIC JOURNAL OF INTERNAL AFFAIRS: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA (2010-) 69: 1 pp. 123-141. (2021) Szakcikk (Folyóiratcikk)

10. Szócska Miklós, Pollner Péter, Schiszler István, Joó Tamás, **Palicz Tamás,** McKee Martin, Asztalos Áron, Bencze László, Kapronczay Mór, Petrecz Péter, Tóth Benedek, Szabó Ádám, Weninger Attila, Áder Krisztián, Bacskai Péter, Karaszi Péter, Terplán Győző, Tuboly Gábor, Sohonyai Ádám, Szőke József, Tóth Ádám, Gaál Péter
Countrywide population movement monitoring using mobile devices generated (big) data during the COVID-19 crisis
SCIENTIFIC REPORTS 11: 1 Paper: 5943, 9 p. (2021) Szakcikk (Folyóiratcikk)

11. Vida Zoltán, Vissi Borbála, **Palicz Tamás,** Lám Judit. Smart & Safe – intézményi digitalizációs stratégia a betegbiztonság szemszögéből [Smart & Safe –digitalisation strategy from a patient safety perspective]
ORVOSI HETILAP 162: 47 pp. 1876-1884. (2021) Szakcikk (Folyóiratcikk)

12. **Palicz Tamás,** Sas Tibor, Tisóczki József, Bencsik Balázs, Joó Tamás. „Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben ["Your money or your life!"–Ransomwares in healthcare information systems]
ORVOSI HETILAP 161: 36 pp. 1498-1505. (2020) Összefoglaló cikk (Folyóiratcikk)

13. Tóth Tamás, **Palicz Tamás,** Szócska Miklós. A magyar egészségügyi szakemberek digitális technológiákkal kapcsolatos attitűdjének vizsgálata
IME 19: 2 pp. 44-48. (2020) Szakcikk (Folyóiratcikk)

14. Mikesy Gergely, **Palicz Tamás,** Sinka Lászlóné Adamik Erika. COVID-19 menedzsment ajánlás a telemedicina használatáról
In: Belicza Éva, Lám Judit, Safadi Heléna, Sinka Lászlóné Adamik Erika (szerk.) COVID-19 kórházi menedzsment-ajánlásaink
Budapest, Magyarország: Semmelweis Egyetem Egészségügyi Menedzserképző Központ (2020) pp. 115-120. Szaktanulmány (Könyvrészlet)

15. **Palicz Tamás,** Joó Tamás. Az infrastuktúra-védelem és az információbiztonság kapcsolata
In: Deák, Veronika (szerk.) Az IBTV. gyakorlata: Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2020, Budapest, Magyarország: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet (2020) 50 p. pp. 21-32. Oktatási anyag része (Könyvrészlet)

16. Szócska Miklós, Joó Tamás, Gál András Levente, Lőrincz Orsolya, Auer Ádám, **Palicz Tamás.** A hálózatkutatás alkalmazhatósága a közszolgáltatások fejlesztésében
In: Auer Ádám, Joó Tamás (szerk.) Hálózatok a közszolgálatban Budapest, Magyarország: Dialóg Campus Kiadó (2019) 247 p. pp. 9-25. Szaktanulmány (Könyvrészlet)

9.2. Értekezés témájától független saját publikációk

1.Kilim Oz, Olar Alex, Joó Tamás, **Palicz Tamás,** Pollner Péter, Csabai István. Physical imaging parameter variation drives domain shift
SCIENTIFIC REPORTS 12: 1 Paper: 21302, 11 p. (2022) Szakcikk (Folyóiratcikk)

2.Schutzmann Réka, Nistor Katalin, Albert Fruzsina, **Palicz Tamás.** A szociális vezetőképzés: körkép a hazai és európai uniós képzési kínálatról
SZOCIÁLPOLITIKAI SZEMLE 7: 1 pp. 89-104. (2021) Összefoglaló cikk (Folyóiratcikk)

3.Kovács Réka, Aszalós Zoltán, Cserháti Zoltán, **Palicz Tamás**. Krónikus beteg munkavállalók támogatása, munkahelyi betegségmegelőzés: Az Európai Unió Chrodis Plus közös fellépésének munkahelyek számára kínált jógyakorlatai
IME 20: 4 pp. 38-44. (2021) Szakcikk (Folyóiratcikk)

4.Bálity Csaba, Cserháti Zoltán, Lám Judit, **Palicz Tamás,** Safadi Heléna. Humán szolgáltatások képzési programjainak értékelési rendszere
IME 19: 3 pp. 9-14. (2020) Szakcikk (Folyóiratcikk)

5.Antal Zsuzsanna, Cserháti Zoltán, **Palicz Tamás,** Lám Judit. Intézményi menedzsmentfejlesztő továbbképzés vezető szakdolgozók részére
IME 19: 4 pp. 21-26. (2020) Szakcikk (Folyóiratcikk)

6.Szócska Miklós Károly, Pollner Péter, Schiszler István, Joó Tamás, **Palicz Tamás,** McKee Martin, Magyar Telekom Nyrt, Telenor Magyarorszag Zrt, (Kollaborációs szervezet); Sohonyai, Ádám, Szőke József, Tóth Ádám, Gaál Péter. Putting (Big) Data in Action: Saving Lives with Countrywide Population Movement Monitoring Using Mobile Devices during the COVID-19 Crisis
Paper: DOI: 2020.09.21.20194019, 16 p. (2020)

7.Joó Tamás, **Palicz Tamás,** Szócska Miklós. A népegészségügyi termékadó dohánytermékekre való kiterjesztésének lehetősége
IME 17: 7 pp. 30-33. (2018) Szakcikk (Folyóiratcikk)

8.Palicz Tamás, Vártok Józsefné, Szócska Gábor. A folyamat-újraszervezési (BPR) projektek tapasztalatai az egészségügyben
IME 2: 2 pp. 17-22. (2003) Szakcikk (Folyóiratcikk)

9.Szócska Gábor, **Palicz Tamás,** Vártok Józsefné, Karádi István. Minőségügyi fejlesztés a gyakorlati orvosképzésben az ellátás minőségéért: Az oktatás mint a gyógyítófolyamatok minőségét meghatározó eljárás
LEGE ARTIS MEDICINAE 9: 4 pp. 322-327. (1999) Szakcikk (Folyóiratcikk)

10.Szombathy Tamás, Szalai Csaba, Barna Katalin, **Palicz Tamás,** Romics László, Császár Albert. Association of angiotensin II type 1 receptor polymorphism with resistant essential hypertension
CLINICA CHIMICA ACTA 269: 1 pp. 91-100. (1998) Szakcikk (Folyóiratcikk)

11.Szalai Csaba, Császár Albert, **Palicz Tamás,** Halmos Balázs, Czinner Antal, Romics László. Pontmutációk kimutatása familiáris hypercholesterinaemiás betegekben
MAGYAR BELORVOSI ARCHIVUM 50: 3 pp. 263-268. (1997) Szakcikk (Folyóiratcikk)

10. Köszönetnyilvánítás

Ezúton szeretném kifejezni köszönetemet cs**a**ládo**m**nak, feleségemnek és gyermekeimnek, akik végig türelemmel támogatták a **d**oktori kutatásom és az értekezés me**g**írása során.

Köszönetet mondok témavezetőimnek, Dr. Szócska Miklósnak, Dr. Joó Tamásnak, valamint közvetlen kollegáimnak: Dr. Lám Juditnak, Farkas Beátának és Dr. Gaál Péternek, hogy biztattak, és megteremtették a lehetőséget a kutatás végzéséhez.

Köszönöm Dr. Pollner Péternek, hogy sok esetben gyakorlati szempontokra, a mindennapok kihívására ráirányította a figyelmem.

Szintén köszönettel tartozom Dr. Bencsik Balázsnak, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet korábbi, és Szabó Lajosnak, az NKI jelenlegi igazgatójának, hogy felismerték a téma jelentőségét, és szakmailag is támogatták az ebben végzett kutatásokat és a kutatásokból fakadó gyakorlati lépéseket.

Emellett köszönet illeti minden volt és mostani egyetemi és nem egyetemi munkatársamat, akik tapasztalatukkal, a közös munkában szerzett élményekkel hozzájárultak ahhoz, hogy legyen inspirációm a doktori kutatás végzéséhez.