A csökkentett paraméteres biometrikus hitelesítés jelentősége kórházak kritikus informatikai infrastruktúráiban

Tisóczki József

Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
Pest Megyei Flór Ferenc Kórház, Kistarcsa, Magyarország
E-mail: tisoczki.jozsef@uni-obuda.hu

Beérkezett: 2022. szeptember 1.; elfogadva: 2023. január 31.

Összefoglalás

Jelen tanulmány a kritikus infrastruktúrák körébe tartozó létfontosságú egészségügyi rendszerelemek informatikai adatvédelmét és a felhasználók informatikai munkavégzési folyamatainak könnyítését célzó újfajta technológiai megoldás kutatási folyamatának első mérföldkövét kívánja bemutatni. Kutatásunk céljául egy újszerű biometrikus azonosítási rendszer megvalósítását tűztük ki. Jelen tanulmányban bemutatásra kerülnek az alapvető fogalmak, a betegbiztonságot veszélyeztető, informatikai rendszerek *(Muha 2008)* elleni támadási trendek. A tanulmány ismerteti a létfontosságú rendszerelemek körébe sorolt fekvőbeteg-ellátási intézmények informatikai szakrendszereit használó személyekkel készített mélyinterjúk elemzéseit. Ezen eredmények megalapozzák a csökkentett paraméterezésű biometrikus hitelesítési technológia megvalósíthatóságának lehetőségét, alátámasztja annak létjogosultságát, valamint a magyarországi létfontosságú rendszerelemek körébe sorolt egészségügyi ellátó intézményekben olyan biometrikus hitelesítéssel támogatott folyamatok kidolgozását, amelyek nagymértékben képesek lesznek a stratégiai jelentőségű egészségügyi adatvagyon védelmét szolgálni. A tanulmány választ ad arra a kérdésre is, hogy mi az összefüggés a csökkentett biometriával támogatott rendszerhasználat, valamint a malware, ransomware és más jellegű támadások, adatszivárgások között. A technológia kidolgozása, majd bevezetése közvetett módon képes lesz támogatni az eltérő tudásszintekkel, eltérő kiberrezilienciával rendelkező fejlesztők, felhasználók és üzemeltetők kórházi informatikai szakrendszereinek eltérő üzletmeneteit.

Kulcsszavak: betegbiztonság, csökkentett paraméteres biometrikus hitelesítés, informatikai biztonságtudatossági attitűd, egészségügyi kiberbiztonság, kiberreziliencia

The significance of biometric authentication with reduced parameters in critical IT infrastructures at hospitals

József Tisóczki

Óbudai University Doctoral School on Safety and Security Sciences, Budapest, Hungary
Flór Ferenc Hospital of Pest County, Kistarcsa, Hungary

Summary

This paper presents the first milestone in a research process aimed at protecting the IT privacy of a critical health system element of critical infrastructure and facilitating the IT workflow of users. The objective is to implement a novel biometric identification system. The paper introduces the basic concepts and the trends of attacks against IT systems that threaten patient security. The paper presents an analysis of in-depth interviews with users of IT systems in inpatient care facilities classified as critical system components. The results provide a basis for the technological implementation of a reduced-parameter biometric authentication option and support its justification. The development of processes supported by biometric authentication will be able to provide a high level of protection for strategic health data assets. The study also answers the question of the correlation between reduced biometrics-enabled system usage and malware, ransomware attacks. The development and implementation of the technology will indi-

rectly be able to support the use and development/maintenance of business processes of hospital IT systems with different levels of knowledge, cyber resilience. The protection of health IT systems must be strengthened with modern technological solutions beside human education.

Keywords: patient security, reduced-parameter biometric authentication, IT security awareness attitude, cyber security in healthcare, cyber resilience

Előszó

Tisóczki József kutatási témakörének meghatározását egy komoly problémafelvetéssel indította. Az orvosi-egészségügyi ellátó rendszerek és a biometrikus azonosítási eljárások külön-külön is komoly kihívásokat jelentenek napjainkban. A 2020 márciusától bekövetkezett Covid-járvány a kórházi ellátó intézményekre nagyon komoly nyomást, szakmai kihívást jelentett. Folyamatos leterheltség, a betegellátás problémakörei és a szinte szó szerinti 24 órás munkában állás a kórházi adminisztrációban nehézségeket okozott. Ezt a hosszú időn keresztüli feszített munkát tetézték a kibertérből érkező adathalász- és zsaroló vírusos támadások, a kiberfenyegetettség olyan fokúvá vált, amire megoldásokat nehezen találtak a szakemberek. A pályázó kutatómunkájában azt vállalta fel, hogy a kórházi kritikus információs infrastruktúrák védelme érdekében eljárási módszereket dolgoz ki a biometrikus azonosítás és eljárás területén a biztonságos adattárolás és -feldolgozás érdekében. A kutatási eredmények széles körben hozzájárulhatnak ahhoz, hogy a kórházi kritikus rendszerek használata során még erőteljesebben kizárható legyen a humánum által elkövetett hibák előfordulása.

Kutatási eredményei megfontolásra javasoltak, bár tudjuk, minden szigorítás, minden eljárásmód a biztonságra irányul, mégis a kritikus időpillanatokban, eljárásokban épp olyan fontos területet képviselnek, mint maga a betegellátás.

Prof. dr. Rajnai Zoltán
témavezető,
Óbudai Egyetem Biztonságtudományi Doktori Iskola
Óbudai Egyetem Bánki Donát
Gépész és Biztonságtechnikai Mérnöki Kar

A Pest Megyei Flór Ferenc Kórház (PMFFK) örömmel vette, hogy egyik munkatársa a doktori PhD-kutatási tevékenysége mellett a kórházi kritikus informatikai infrastruktúrák biztonságos alkalmazása témakörben biztonságos alkalmazások vizsgálatával is foglalkozik. A vállalat a kórházi ellátó rendszerek vizsgálatához hardver- és hálózati hozzáférés oldalról nemcsak támogatást nyújtott, hanem folyamatosan figyelemmel kísérte a pályázó munkáját. A biometrikus azonosítás feladataiban munkatársunk kapcsolatot épített ki az Alkalmazott Biometria Intézettel (ABI), és ez a közös támogatás nemcsak egyedi esetté vált, hanem meggyőződésünk, hogy a Kórház és az ABI között hosszú távú szakmai együttműködés is kialakulhat.

A pályázó nagy szakmai hozzáértéssel vizsgálta a kritikus ellátó rendszer informatikai biztonsági oldalait és aspektusait, kérdőíves felmérést végzett, amelyekből adatokat nyert ki, és megoldási javaslataival támogatást adott az informatikai biztonság erősítéséhez. Aktív kutatómunkáját szakmai véleményekkel, az eljárásrendek alkalmazhatóságának véleményezésével támogattuk. Az együttműködés során a pályázó, a vállalati szakértő és a kutatási témavezető kölcsönösen támogatták egymást, jól kiegészítették egymás képességeit. Ezt az együttműködést éppúgy, mint a kutató munkáját kiemelkedőre értékeltem.

Kovács Éva
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar
Pest Megyei Flór Ferenc Kórház, Kistarcsa

Bevezetés

A biztonságos betegellátás nonstop rendelkezésre állásához az informatikai rendszerek megfelelő szintű védelme alapfeltétel. Jelen tanulmány a kritikus infrastruktúrák körébe tartozó létfontosságú egészségügyi rendszerelem informatikai adatvédelmét és a felhasználók informatikai munkavégzési folyamatainak könnyítését célzó, egy újszerű személyi azonosítási rendszer megvalósítására fókuszál. A tanulmányban bemutatásra kerül a csökkentett paraméterű biometrikus azonosítás létjogosultsága. A kutatás időszerűségét több tényező, körülmény is indokolja. A mesterséges intelligencia (MI) eddig is rendkívül hatékony megoldásokat eredményezett, fejlődése exponenciális, megállíthatatlan. 1992-ben lett a nagyközönség számára bemutatva a Da Vinci névre keresztelt robotrendszer, melynek fejlettsége túltett a ZEUS-on *(Jasztrab 2017)*. A gépi tanulás, különösen a komplex többrétegű neurális hálózatok *„mély tanulása”*, a Deep Learning fejlesztések újabb szoftverképességek és új eszközök létrehozását vetítik előre. Az IoT eszközök fejlődése és használata is forradalmi léptékű. Az egészségügyi ellátások területén egyre több MI támogatott folyamat és eszköz található. Ilyen többek között a Semmelweis Egyetem sebészeti ellátásában 2022 tavaszán rendszerbe állított *Da Vinci sebészeti robot* is *(semmelweis.hu)*. A hazai egészségügy több területén alkalmaznak mesterséges intelligencia (MI) által támogatott adatfeldolgozási folyamatokat. Hazánkban is használatban vannak, illetve bevezetés alatt állnak MI-alkalmazások *(Balogh et al. 2022)*. Az információbiztonság területén dolgozó szakemberek a kibertámadások számosságának emelkedése mellett a kritikus infrastruktúrák elleni egyre komplexebb támadási formákkal szembesülnek. A zsarolóvíru-

sok, malware, social engineering és egyéb támadások komplexebb és nagyobb számosságú megjelenését erősíti a Sophos Ltd. 2022-es felmérése is *(1. ábra)*. Ugyanakkor ezek a támadási vektorok nem csak a kritikus rendszerek ellen irányulnak. Az egyéni, otthoni felhasználók is egyre nagyobb mértékben szembesülnek a személyes adataik megszerzésére irányuló tevékenységekkel, adatmanipulációs kísérletekkel, személyes adatok, banki adatok megszerzésére irányuló tevékenységekkel. Napjainkra a kibertámadások, az elvárt felhasználói viselkedési formák, az IT rendszerek robbanásszerű fejlődése már a közbeszéd részévé lett. Tapasztalataim alapján a kórházak informatikai rendszereinek IT technológiai fejlettsége pár éve még elmaradt az egyéb létfontosságú rendszerelemek (LÉR) körébe tartozó infrastruktúrák lehetőségeihez képest. Az elmúlt évek nagyszabású egészségügyi informatikai fejlesztései azonban ezt a trendet megfordították. Új szerverparkok üzembe állítása, kliens oldali teljes hardware- és software-cserék valósultak meg. Gyakorlati tapasztalataim azonban azt erősítik, hogy a technológiai fejlesztések ellenére az egészségügyi informatikai infrastruktúrák kitettsége nem csökkent, mindösszesen a támadási vektorok változtak. A támadási formák módosulását növelte a Covid19 veszélyhelyzet okozta munkavégzési formára történő áttérés. Mára a vállalatok jelentős része hibrid munkateret biztosít alkalmazottai részére. A távoli munkavégzést, az ún. *„home-office"* feladatellátást csakis biztonságos IT kiszolgáló környezetben, megfelelő felhasználói biztonságtudatosság, kiberreziliencia *(Hausken 2020)* megléte mellett lenne szabad folytatni.

Helyzetismertetés, problémafelvetés

Fogalommagyarázat

A tanulmány egyik célkitűzése a kutatás eddigi eredményeinek bemutatása mellett, hogy a publikációban szereplő jelentősebb fogalmakat is ismertesse. A fogalmak bemutatása során az Óbudai Egyetem Biztonságtudományi Doktori Iskolában (ÓE BDI) elsajátított ismeretanyag önálló megfogalmazása mellett hivatkozásokat is megadok.

Biometrikus azonosítás: Az ember egyedi biológiai jellemzőjének vagy jellemzőinek mesterséges intelligenciával támogatott, összetett digitalizált adatfeldolgozói folyamata, mely a nevezett személy azonosítását és/vagy hitelesítését végrehajtja. Egyedi biológiai jellemző lehet az ujjlenyomat, az írisz (szivárványhártya) mintázata, a tenyér érhálózatának térképe, de akár az arckép, a beszédhang, de a szívverés is *(biometrikus.hu)*.

Covid19: Vírusos légúti, illetve légzőszervi megbetegedés, amelyet a SARS-CoV-2 nevű koronavírus okoz *(semmelweis.hu)*. Az Egészségügyi Világszervezet 2020. március 11-én hirdette ki a betegség okozta világjárvány megjelenését.

Kritikus információs infrastruktúra: „Azok az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amely működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrák működőképességét jelentősen csökkentené." *(Muha 2007; 2015)*

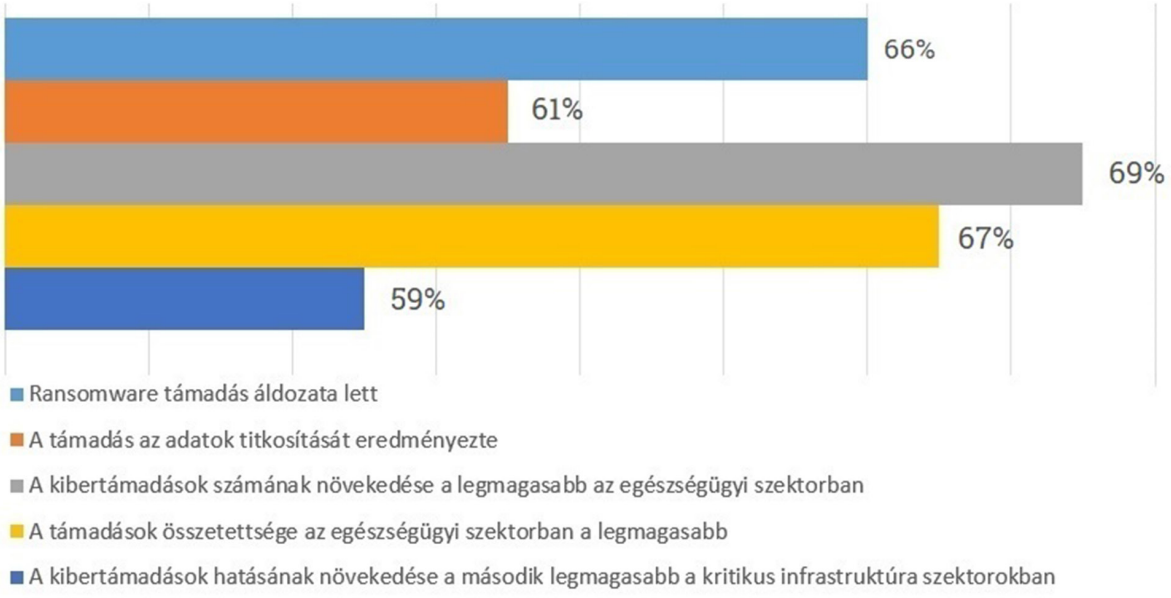
Kritikus munkakör: Az üzemeltető által azonosított azon munkakör, amelynek ellátásával biztosított a létfontosságú rendszerelem üzemfolytonos működése.

Mesterséges intelligencia: „Nehéz pontos definíciót adni, mivel magát az intelligenciát sem könnyű pontosítani." *(Ekler-Pásztor 2020)* Az EU Bizottságának megfogalmazásában: „A mesterséges intelligencia (MI) olyan rendszerekre utal, amelyek intelligens viselkedést mutatnak az alábbiak révén. Elemzik környezetüket, és bizonyos fokú önállósággal cselekszenek meghatározott célok elérése érdekében."

Social Engineering: A Social Engineering pszichológiai befolyásolást jelent *(www.securinfo.hu)*. Az informatikai rendszerekhez is köthető fogalom annak a fajta támadásnak a meghatározását sűríti egy kifejezésbe, amikor a támadó nem technológiai sebezhetőségeket használ ki, hanem arra törekszik, hogy megtévesszen egy felhasználót. A megtévesztés eredményeként a jogosultsággal rendelkező felhasználó a jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít számára a saját, vagy szervezete egy vagy több rendszerébe történő belépésre, kimondottan a pszichológiai befolyásolást végző személy megtévesztő viselkedése miatt.

A probléma feltárása

A betegellátási folyamatokban az időtényező sok esetben az emberéletet meghatározó paraméter! Az egészségügyi személyes adat, különleges személyes adat. Az egészségügyi szakrendszerekben tárolt adatok megbízhatósága, hitelessége és rendelkezésre állása az egészségügyi ellátási folyamatokban nélkülözhetetlen. A kritikus egészségügyi informatikai infrastruktúrákban a kitettség egyre növekvő jelenléte, annak exponenciálitása figyelhető meg *(Sophos 2022)*. A támadások számossága és komplexitása évek óta növekvő tendenciát mutat. Az orosz–ukrán háború kitörése óta a trendek nagymértékű emelkedése tapasztalható *(NKI 2022)*. Itt fontos megjegyezni, hogy a kritikus egészségügyi infrastruktúrákban a Sophos Ltd. 2022. június 4-én tette közzé *„A zsaroló-vírusok helyzete az egészségügyben"* című jelentését *(Sophos 2022)*. Az idei év kutatásában 31 országból 5600 informatikai szakember, köztük 381 egészségügyi szakember vett részt. Megállapításaik szerint a legnagyobb mértékben, 69%-kal, az egészségügyi szektorban nőtt a kiberfenyegetettség. Az észlelt kibertámadások komplexitása 67%-os emelkedést mutat. Az *1. ábrán* a Sophos 2022. évi jelentésében szereplő adatok felhasználásával foglaltam össze a főbb mutatókat. Az *1. ábra* egyértelműsíti a



1. ábra Az egészségügyi szektor kiberkitettségének emelkedése 2022-ben

Forrás: saját szerkesztés a Sophos Ltd. adatai alapján (2022)

szektort egyre inkább terhelő feladatot. Az egészségügyi ágazat technológiai és humán erőforrás kitettségén keresztül megvalósuló különleges személyes adataink kitettségét.

A 7/24 órás biztonságos betegellátás biztosításához az informatikai szakrendszerek nonstop rendelkezésre állására és adatintegritására van szükség. A biztonságos betegellátás sérülhet, ha a beteg egészségügyi ellátásához kapcsolódó egészségügyi adatrekordok épp egyik szükséges eleme valamilyen ok – például külső támadás, adatmanipuláció, SQL injection stb. – miatt módosul, vagy elérhetetlenné válik. Veszélyben vannak az egészségügyi adataink. Magyarország egészségügyi adatvagyona hatalmas és stratégiai jelentőségű. E különleges személyes adatok elvárt biztonsági szintjének biztosítása kiemelt prioritású feladat. Egyrészt a kibertér felől érkező támadásokat kell elhárítanunk. Nagy veszélyt jelentenek az ún. social engineering támadások *(Oroszi 2021)*. Az ilyen jellegű pszichológiai manipulációs támadásokkal a támadó fél képes lehet megszerezni egy adott rendszer hitelesítési kulcsát. Ez az információ rossz kezekben kaszkád folyamatokat fog indítani. Sajnos a zsarolóvírus-támadásoknak több hazai kórház is áldozatává vált *(Palicz et al. 2020)*. Erről szerzőtársaimmal egy korábbi tanulmányunkban adtunk ismertetést. Másrészt szembesültünk egy újonnan megjelent feladattal a hazai Covid19 pandémia fekvőbetegeket ellátó kórházi egységeinél. Ezeken az izolált betegápolási területeken, érthető módon, az egészségügyi ellátó személyzet teljes testet fedő védőfelszerelést használ. A védőeszközök a teljes testet olyannyira elfedik, hogy jellemzően ők maguk sem ismerik fel egykönnyen egymást. Emiatt védőruházatukat feliratozták *(2. ábra)*.

2017. november 1-én indult az Elektronikus Egészségügyi Szolgáltatói Tér (EESZT). Az EESZT indulásával egyidejűen EIDAS (európai) kompatibilis eSzemélyi igazolvány vagy hard token használata volt szükséges az Elektronikus Egészségügyi Szolgáltatói Térhez történő autentikációkhoz. Ugyanakkor újra kell értékelnünk – a már megtapasztalt pandémiás ellátási gyakorlatra fókuszálva – az eSzemélyi igazolvány ezen folyamatokban

2. ábra Covid19-betegellátás teljes testet fedő védőfelszerelésben

Fotó: dr. Ruszkai Zoltán osztályvezető főorvos, PMFFK (2021)

történő fizikai használatát, melynek az adatbiztonságra, közvetetten pedig a biztonságosságra vonatkozó pozitív voltát nem kérdőjelezzük meg. Az EESZT autentikációra mára már mobil applikáció is használható. Ehhez azonban ismét egy fizikai eszközt kell igénybe venni, nevezetesen egy smart telefont. Összességében kijelenthetjük, hogy (EESZT) bevezetése nagyban hozzájárult a pandémia sikeres kezeléséhez, segíti a biztonságos betegellátási folyamatokat. Ugyanakkor a SARS-CoV-2-pandémia számos új helyzetet eredményezett, így az egészségügyi informatikai rendszerek (HIS) használata során is. Az izolált ellátási zónákba – pl. Covid intenzív ellátó osztály – mindenképp be kell vinni egy fizikai azonosító eszközt a kétfaktoros autentikáció megvalósításához.

Kutatási célkitűzés

Kutatási projektünk célja egy új, a medikai informatikai szakrendszerek adatkezelési folyamataiban megjelenő, újszerű autentikációs lehetőség kidolgozása, mely a hazai egészségügyi adatvagyon megbízhatóságát és rendelkezésre állását emeli, sérülékenységét csökkenti, illetve a csökkentett paraméterezésű biometria alkalmazásával megvalósuló azonosítás és hitelesítés üzleti folyamatokba integrálása segítségével. Kutatási bázisaink az Óbudai Egyetem Alkalmazott Biometria Intézete (ABI) és a Pest Megyei Flór Ferenc Kórház (PMFFK). Célkitűzésünk konvergál Magyarország Nemzeti Kiberbiztonsági Stratégiájában *(1139/2013. (III. 21.) Korm. hat.)* és a Nemzeti Biztonsági Stratégiában *(1035/2012. (II. 21.) Korm. hat.)*, valamint a 2020. április végén megjelent új Nemzeti Biztonsági Stratégiában *(1163/2020. (IV. 21.) Korm. hat.) (Kovács 2020)* megfogalmazott védelmi célokkal. Kutatásunk az egészségügyi adatvagyon mint stratégiai jelentőségű kritikus adathalmaz védelmi képességeinek erősítéséhez kíván hozzájárulni.

A biometrikus hitelesítés

A biometrikus hitelesítés előnye, hogy egyértelmű módon az adott személyt azonosítja. Tehát nem tudás- vagy tulajdonlásalapú közvetett jellemzőket vizsgál. Ilyen közvetett jellemzők például a PIN-kód vagy a beléptető kártya, vagy a felhasználónév-jelszópáros használata. Ezek alkalmazása számos előnnyel bír, de ugyanakkor számos hátránya is van, így például a social engineering, keylogger, fizikai eltulajdonítás és még számos kitettség. Ennek kivédésére kerültek bevezetésre az egyre szélesebb körben megvalósuló, ún. kétfaktoros autentikációs megoldások, illetve a komplex erős jelszóhasználat és a jelszavak használhatóságának időkorlátjai. Az ún. biometrikus hitelesítés használatával lényegesen magasabb biztonsági szintet tudunk megvalósítani. A biometrikus azonosításnak számos fajtáját ismerjük. A különböző azonosítási formák működése minden esetben a rendszer, az emberi szervezet vagy a viselkedésforma egy

Ssz.	szempont	biometrikus azonosítási módszer									
		ujj		kéz		arc		írisz		ér	
		M	+	M	+	M	+	M	+	M	+
5.	Együttműködési igény.	a	a	b	b					c	c
6.	Elfogadottság.										
7.	Belső biometrikus jellemző mérése.	d	d	d	d	d	d				
9.	Érintés nélküli technika.										
10.	Azonosítási idő.										
11.	Biometrikus adatmennyiség-csökkenés.		e								
	Alkalmazhatóság (összefoglalás).			f	f	h	h				

Jelmagyarázat:
M: alkalmazás maszkban
+: alkalmazás maszkban és kesztyűben
: optimális
: nem optimális, de nem kizáró
: nem elfogadható
a: a detektor felületét mentesíteni kell minden felhasználó után
b: nem tüskés pozicionálás esetén, különben „a”
c: érintés nélküli megoldásokban, különben „a”
d: külső biometrikus jellemző mérése történik
e: polarizált fénnyel történő detektálás esetén az azonosítás megkísérelhető
f: nem tüskés pozicionálás esetén
h: azonosításra nem, hitelesítésre lehet alkalmas

3. ábra Azonosítási módszerek

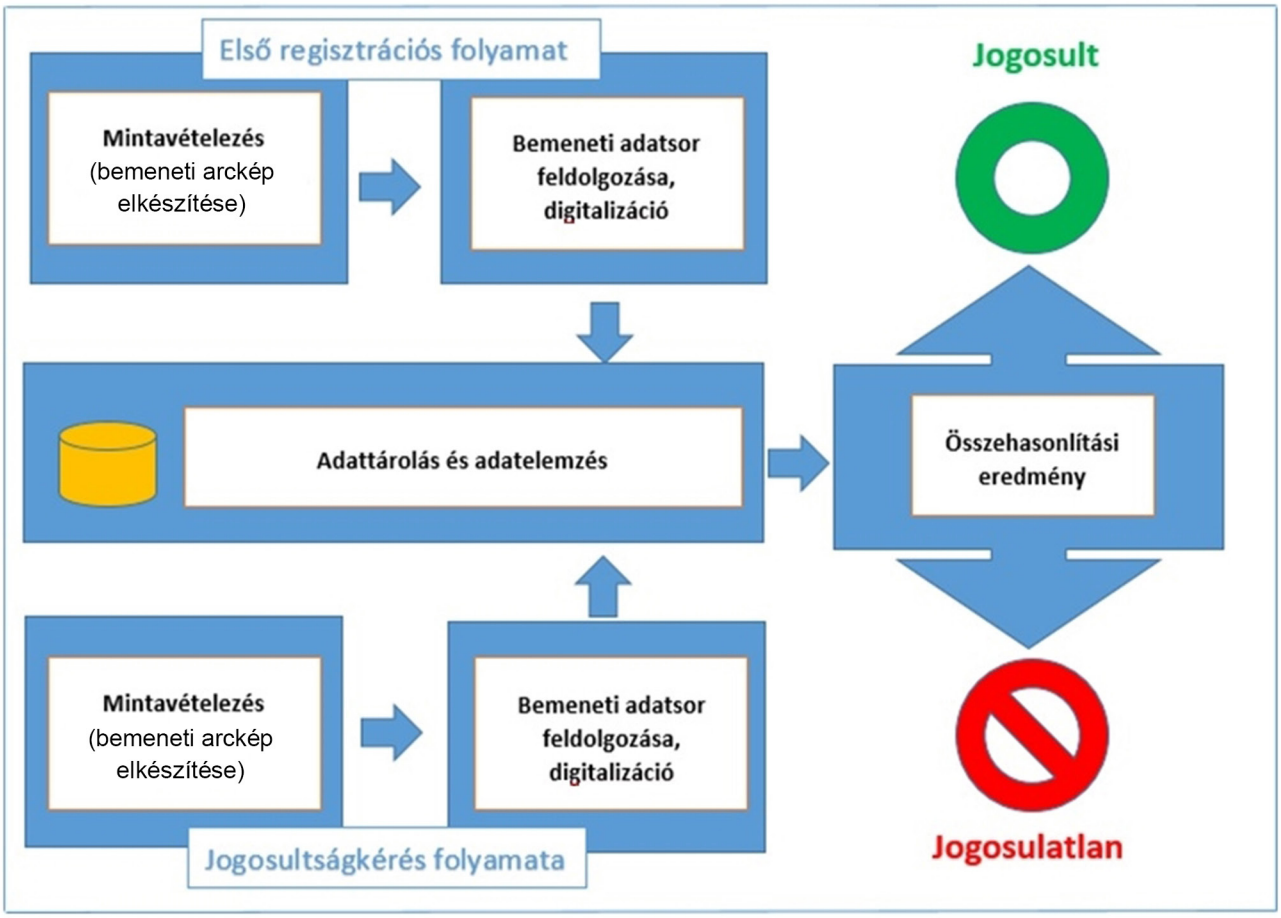
Forrás: saját fordítású ábra Kovács–Kovács (2022) alapján

vagy több egyedi mintáját rögzíti. A rendszer az egyedi mintát digitális adattá konvertálja és adatbázisban tárolja. Megkülönböztetjük az első regisztrációs folyamatot, valamint a használat során jelentkező use-case eseteket *(Rexha–Shala–Xhafa 2018)*. Hitelesítés során az aktuálisan levett mintát összevetjük ebben az adatbázisban korábban eltárolt mintákkal. 1:1 megfelelőség esetén ellenőrzést, más néven hitelesítést vagy azonosságmegerősítést végzünk (1:n kapcsolat esetén azonosításról beszélünk) *(Kovács–Ujhegyi 2021)*. Ezzel megállapítható az azonosság érvényessége. Amennyiben a rendszer össze tudja rendelni az aktuális mintát egy ellenőrző mintával, ismert a személy azonossága, és a hitelesítés rendben van, míg ellenkező esetben a személyazonosság invalid. A biometria azonosítási módszereinek védőruházatban történő alkalmazhatóságát, a biometriai azonosítási módszerek összevetését Kovács Tibor és Kovács Éva vizsgálták, majd megállapításaikat a *3. ábrán* látható táblázatban tették közzé *(Kovács–Kovács 2022)*. A mátrix azt láttatja, hogy maszkban, illetve maszk és kesztyű együttes használata esetén az adott biometrikus azonosítási módszerek egy nevesített szempont alapján milyen valószínűséggel alkalmazhatók. **Zöld:** optimális; **Sárga:** nem optimális, de nem kizáró; **Piros:** nem elfogadható. Az „a–h" opciók egyéb feltételeket közölnek.

A megvalósítandó ***csökkentett paraméteres biometrikus hitelesítés,*** az élettani technikának az arcfelismerését felhasználva, csak a szem és az orr életkorral sem változó paramétereit veszi alapul. A biometrikus hitelesítési folyamat a *4. ábrán* felrajzolt egyszerű sémán követhető nyomon.

Felhasználók és rendszerek

A kórházakhoz kapcsolódó járó- és fekvőbeteg-ellátások folyamataiban a felhasználókat tevékenységük alapján négy fő csoportba sorolhatjuk. Egyrészt a szoftverek felhasználóira mint orvosokra, nővérekre és adminisztrátorokra, valamint a gazdasági, műszaki támogató szakmaterületek dolgozóira. Egy másik súlyozottan kockázatos felhasználói csoport a rendszeradminisztrátorok csoportja és a felhasználói alkalmazásokat fejlesztők csoportja. Ugyanakkor a felsorolást ki kell terjeszteni a gépi automatizmusokra is, úgymint rendszerekbe integrált gépi hozzáférésekre. Ilyenek lehetnek az egészségügyi ellátási folyamatok mesterséges intelligenciával (MI) támogatott szakrendszerei, de az önálló gép-gép adatcsere



4. ábra Arcfelismerő rendszer sémája

Forrás: saját szerkesztés

interfészek is, az MI támogatott folyamatok. Az MI jellemzően diagnosztikus kiértékeléseket végez, segítve a különböző orvosi diagnózisok felállítását. Jelen felsorolásból kizártam a háziorvosi, védőnői, Országos Mentőszolgálat (OMSZ) és hospice szolgáltatásokat, valamint a működést koordináló, ellenőrző és finanszírozó szervezeteket, mint például az Országos Kórházi Főigazgatóságot (OKFŐ). Az 5 GHz-es hálózatok és a „Tárgyak Internetének" (IoT) egyre nagyobb térnyerése az egészségügyben is megjelenik és növekszik *(Krasznay 2020)*. Ez a folyamat egyrészt segít, de mellette újabb kihívásokat is támaszt. Ezek a gép-gép kapcsolatok újabb biztonsági kihívások elé állítják a kritikus informatika üzemeltetését és a jogszabályalkotókat is.

A Face ID *(Yan–Pan–Xu 2015)* automatikusan igazodik a felhasználó megjelenésében bekövetkezett változásokhoz, például amikor sminket használ, vagy ha megnőtt az ember arcszőrzete. Az Apple iPhone 15.x operációs rendszert vizsgálva kijelenthető, hogy számos biometriai jellemzőt képes megbízható módon azonosítani, valamint Artifical Intelligence (AI) megoldásaival biztonságos hitelesítést ad, elenyésző hibaráta mellett *(Yan–Pan–Xu 2015)*.

A csökkentett adatmennyiség alapján történő személyazonosság megállapítása újszerű megoldást jelenthet akár kriminalisztikai, katonai vagy terrorista felderítési-azonosítási szempontból is, de tömegszerencsétlenségek esetén megvalósítandó gyors személyazonosítási lehetőséggel is kecsegtet. Kutatásunk a pandémiás környezetben betegellátási tevékenységet ellátó, védőfelszerelésbe öltözött orvosok, nővérek azonosítása tekintetében egy adatbiztonságot növelő, munkaterhelést csökkentő lehetőséget kínál. Ugyanakkor a biometrikus adatok tárolása, kezelése és továbbítása különleges biztonsági védelmet kíván, mivel azok egyediek, nem lecserélhetők és nem pótolhatók *(Győrffyné Holló 2022)*.

A biometrikus adatokra épülő azonosítási, hitelesítési eljárások alkalmazása napjainkban már nem újszerű technikai megoldás. Mindennapos alkalmazásuk már napjaink egyik ismert technológiai megoldásává lépett elő. Gondoljunk csak az arcfelismeréssel történő mobiltelefon-használatokra. Kutatásunk újszerűsége, hogy a csökkentett mintavételezésen alapuló azonosításra fókuszál.

Alkalmazott vizsgálati módszertan

Jelen ismertetett kutatás megkezdése előtt, majd a folyamat közben is széles körű irodalomkutatást, a releváns információk és adatok összegyűjtését, azok rendszerezését végeztem el. Behatároltam a releváns hazai és európai uniós, folyamatosan változó jogszabályi környezetet. Vizsgáltam a vonatkozó szabványokat és ajánlásokat. A szakirodalom elemzésének körébe tartozott a vonatkozó technológiai megoldások és a témában eddig megjelent tanulmányok áttekintése, másodelemzése. Gyakorlati mintavételezéseket végeztünk az Óbudai Egyetem Alkalmazott Biometria Intézetében (ÓE ABI). Az eredmények ismertetését egy következő tanulmányban tervezem. Kvalitatív felmérések elvégzésére került sor, melyekben személyes interjúkat készítettem a különböző szerepköröket betöltő informatikai rendszerek felhasználóival. A kérdésekre adott válaszokat rendszereztem, a kapott eredményeket értékeltem. A kvalitatív eredmények alapján kvantitatív felmérés előkészítése történt, mely előkészítette a reprezentatív nagymintán történő vizsgálatot a szignifikancia bizonyíthatóságára.

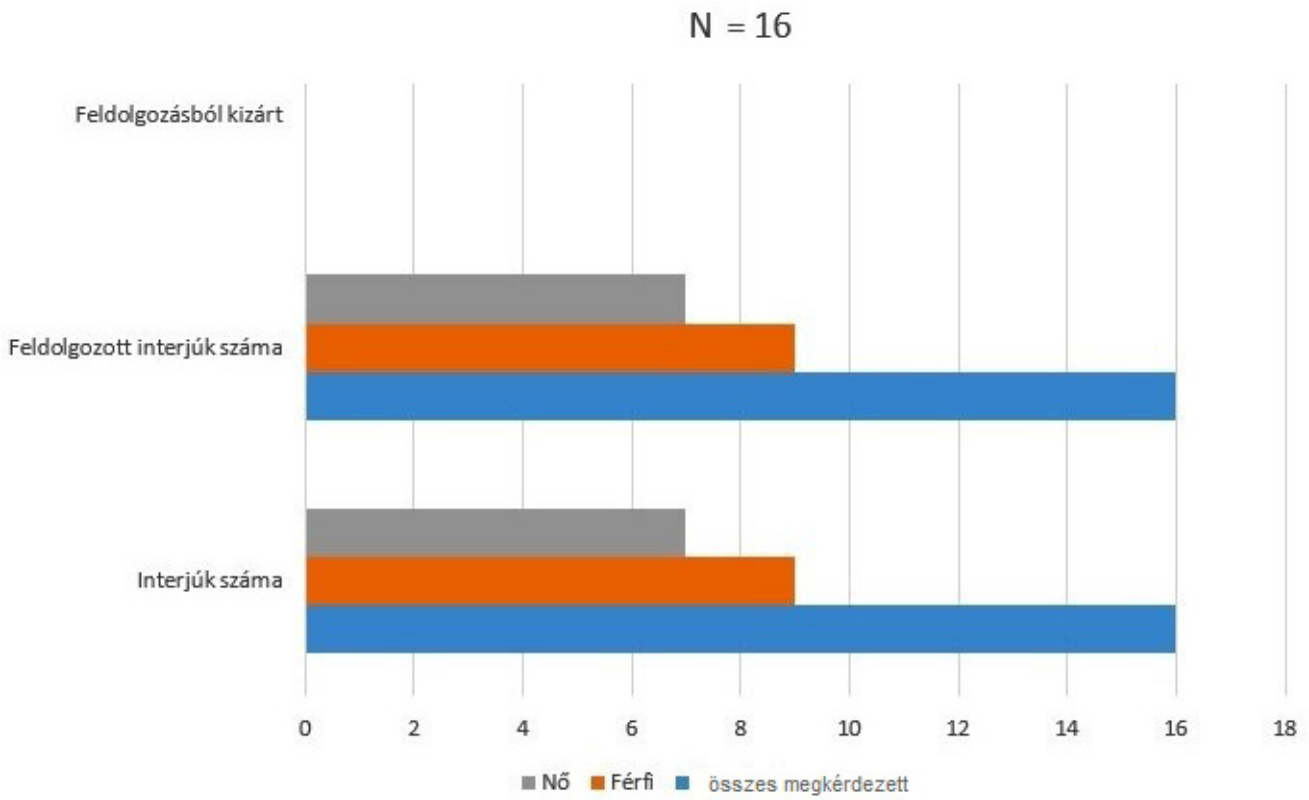
Interjúk

A kutatás szakirodalom-kutatásra és mélyinterjúk készítésére alapozott. Célcsoportjaim lehetőség szerint hazai és nemzetközi környezetben is szakmai gyakorlattal rendelkező, informatikai rendszerekhez köthető aktorok csoportjai. Meghatározásra kerültek a csoportok, majd felkérés útján a személyes interjúkat vállaló alanyok kijelölése történt meg. Hátráltató tényezőként volt jelen a Covid19 pandémia. Az adatszerzés adatfelvételezéssel, személyes interjúk elkészítésével történt.

A megvalósított feltáró kutatás mintavételezésének összeállítása során arra törekedtem, hogy a kvalitatív feldolgozás kis elemszámú (N = 16) mintája a nemek, az életkorok és szakmaterületek, valamint képzettségek figyelembevételével valósuljon meg *(5. ábra)*. Egy rétegzett mintavételezés történt, súlyozottan az orvosszakmára koncentráltan. A koncentrált kiválasztással olyan meghatározott csoportokból történt meg a kijelölés, akik alapvető hatással vannak a kutatás ezen szakaszában vizsgált feltevésekre.

Vizsgálatomat személyes mélyinterjúk rögzítésével végeztem, kórházi ellátási folyamatokban jelenleg is aktív egészségügyi szolgálati jogviszonyban állók körében. Az alapsokaság a betegellátási folyamatokban dolgozó orvosok, nővérek, illetve a támogató szakmaterületek dolgozói mint az informatikai rendszereket üzemeltetők és fejlesztők köréből került kiválasztásra. Felmérésemben 16 fő (9 férfi és 7 nő) válaszát rögzítettem. Előzetesen tájékoztattam az interjú alanyait, személyük és az adott válaszok anonimitására, önkéntességére, a válaszok összegzett módon történő felhasználására. Az interjúk kérdéseit nyitott és zárt, kötelezően, illetve szabad döntés alapján megválaszolható kérdésekként tettem fel. Az interjúk során egy rövid, 10-15 perces kötetlen beszélgetést követően tettem fel a nyitott és a zárt kérdéseket. Ezeket előzetesen megfogalmaztam, és olyan sorrendben tettem fel őket, hogy az előző válaszok kontrollálhatók legyenek.

Az interjúk 21 megválaszolandó kérdést tartalmaztak. Ebből 18 zárt, kötelező kérdés, 1 pedig nyitott, nem kötelező volt. Ezzel a válaszadó saját kötetlen megjegyzést adhatott. A zárt kérdések között alternatív és szelektív válaszlehetőségek közül választhattak az alanyok. Kérdéseim összeállítása során arra is figyeltem, hogy választ kapjak arra, hogy az információbiztonságot befolyásoló tényezőket mennyire ismerik a felhasználók, és milyen



5. ábra A mérés alanyainak számossága és nemek szerinti megoszlása

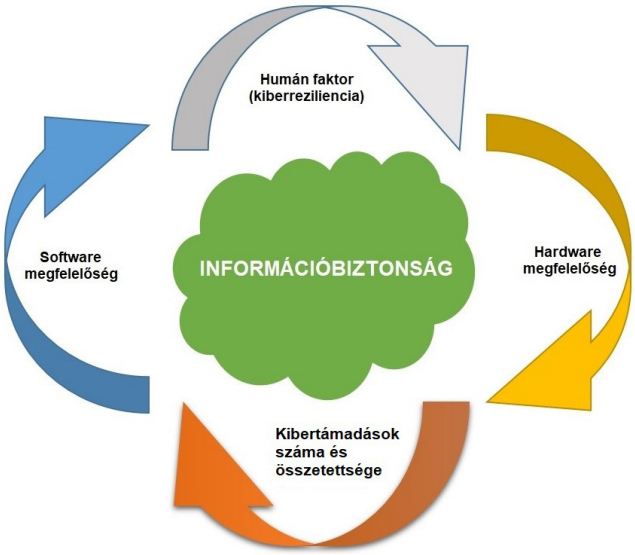
Forrás: saját készítés

mértékben ismerik a biztonságot befolyásoló tényezőket. *(6. ábra)*. A felhasználói rendszerek humán aktora jelenti az információbiztonság egyik legkritikusabb pontját *(Rajnai 2017)*.

A felvett interjúk kérdéskörét négy fő részre tagoltam. Az első részben személyes jellegű kérdéseket tettem fel. Ezek a válaszadó nemére, életkorára, munkaköreire és végzettségeire fókuszáltak. Az interjúk másik kérdésköre az informatikai rendszerismereteket térképezte fel. Ezek a válaszok az alanyok saját önértékelését tartalmazzák, egzakt mérés ezen adatok esetében nem történt. Az interjúk harmadik része az alanyok információbiztonsági tudatosságát kívánta feltérképezni. A negyedik kérdéskör – nem utolsósorban – a biometriával kapcsolatos ismeretszintre, a technológia elfogadottságára kérdezett rá. Egy nyitott kérdést tettem fel, ahol a válaszadó szabadon megfogalmazhatta véleményét. Az interjúkat az 2020–2021-es évek során, a Covid19 nehezítette körülmények között végeztem el. Az adatok elemzéséhez, a válaszok feldolgozásához, diagramok készítéséhez szimplán Excel-programot használtam.

Az interjúk kérdései

Az interjú kérdései: Neme / Életkora / Korábbi beosztások / Jelenlegi beosztás / Végzettség / Informatikai képzettsége (önmaga által megadott) / Informatikai rendszerismerete (önmaga által megadott) / Kiberbiztonsági ismeretszintje (önmaga által megadott, de nem mért) / Saját jelszóképzési és kezelési ismeretszintje (önmaga által megadott, de nem mért) / Telefonos információközlési limitszintje (önmaga által megadott, de nem mért) / EESZT, mobiltoken használata / Biomet-



6. ábra Az információbiztonságot befolyásoló tényezők

Forrás: saját készítés

riához kapcsolódó ismeretszintje (önmaga által megadott, de nem mért) / Támogatná a biometrikus adatainak rögzíthetőségét, felhasználhatóságát? / Rendelkezik érvényes útlevéllel? / Rendelkezik okostelefonnal? / Telefonján hogyan lép be? / Volt korábban azonosítási incidense? / Röviden mi volt az incidens tárgya? / Felderített, mi volt az incidens oka? / Részt vállalna gyakorlati tesztelésben? (anonimitás biztosításával) / A válaszadó egyéb észrevétele, megjegyzése.

Kvalitatív vizsgálat

A betegbiztonság és a betegjogok – a betegek magánéletének védelme – szorosan összefügg a beteginformációkkal *(Ahlfeldt 2008),* az ún. e-health rekordokkal (EHR) *(GYEMSZI 2012)*. Feltételezésem, hogy az információbiztonság, a felhasználók viselkedésmintái, attitűdjei szoros összefüggésben állnak egymással, közöttük korreláció mutatható ki. Jelen kutatásomban az összefüggések nagy mintán történő vizsgálatának előkészítése fog megvalósulni, e hipotézist a reprezentatív vizsgálat keretében fogom felmérni és elemezni. A hazai létfontosságú egészségügyi ellátórendszerek informatikai szakrendszereihez köthető felhasználók kiberbiztonsági attitűdvizsgálatát, mélyinterjúk készítésével a 2020–2021-es években rögzítettem. A vizsgálat kezdete a Covid19-pandémia kezdetével közel egy időben indult. A kapott eredmények megalapozzák a rá épülő csökkentett paraméteres biometrikus hitelesítési lehetőség kidolgozásának szükségszerűségét, mint könnyített hitelesítési technológiai megoldás kidolgozását.

A válaszok különböző szempontok alapján történő megoszlásai

A kutatás 16 adatfelvételéből az adatrögzítés, feldolgozás, elemzés során egy sem került kizárásra.

Az alapsokaság Magyarország egészségügyi ellátásában, ezen belül kórházakban informatikai rendszerekhez is kapcsolódó munkavállalók önkéntes csoportja. Összesen 16 interjú készült. A válaszok nemek szerinti megoszlása, a férfiak/nők aránya 9/7 fő. A férfiak átlagélet-kora 43,6 év, míg a nőké 44,3 év. Tehát a nemek életkor szerinti megoszlása közel azonos. A személyes jellemzőket vizsgálva 10 orvos, 3 nővér, 1 fő recepciós, 1 fő gazdasági területen foglakoztatott személy, illetve 1 fő IT rendszergazda adott választ. Az orvosok felülreprezentáltsága a mintában szándékolt, mivel az EESZT-ben tárolt betegadatok kezelésére a jogszabályok alapján ők jogosultak.

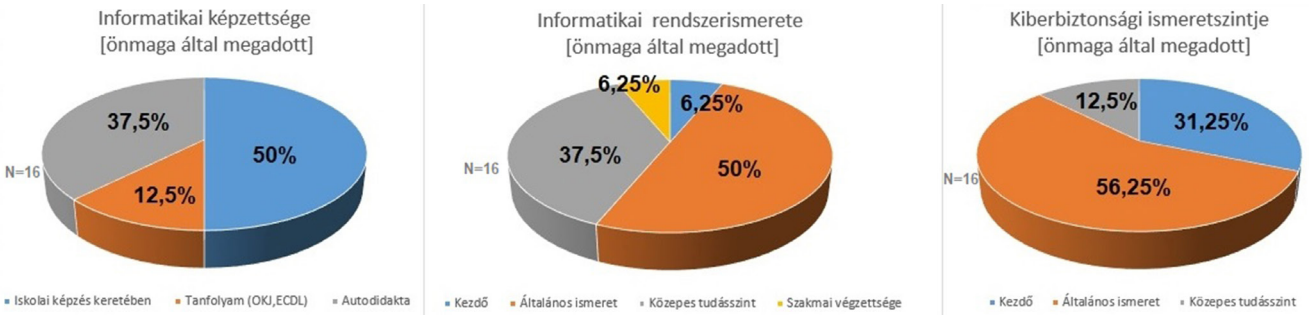
A válaszadók informatikai ismeretszintje

A válaszadók megadták, hogy az informatikai képzettségüket milyen formában szerezték meg. Ez lehetett formális, illetve non-formális képzési forma. Megbecsülték az informatikai rendszerekre vonatkozó ismeretszintjüket is. A kiberbiztonsági ismeretszint szintén önbevallás alapult. A *7. ábra* jól láttatja, hogy az informatikai képzettség megszerzése tekintetében a válaszadók pontosan fele, 50%-a formális iskolai képzést jelölt meg. OKJ/ECDL tanfolyamot 12,5% végzett el, meglepő módon az autodidakta képzettség megszerzésének aránya 37,5%-ot mutat.

Az előző képzettséggel szinte teljesen egybecseng az informatikai rendszer ismeretre adott válaszok aránya. Itt 1 fő szakmai végzettséget adott meg. Kiberbiztonság tekintetében meglepő a közel 1/3-os kezdő tudásszint arány.

Az információbiztonsági tudatosság

Az információbiztonsági tudatosságra adott válaszok kérdéscsoportban vizsgáltam a válaszadók információbiztonsággal összefüggésbe hozható attitűdjeit, a saját jelszóképzési és azok kezelési megoldásait *(8. ábra)*. A számos tudatosító képzés és a felhasználók 75%-a megfelelő szintre történő önértékelése ellenére a beszélgetésekben felszínre került, hogy a kórházi szakrendszerekben előírt jelszószabályokat nem tudják megkerülni, viszont a privát életükben gyenge és több helyen is ugyanazokat a jelszavakat alkalmazzák. Jelszómenedzser alkalmazásokat nem használnak, azok alkalmazási lehetőségeit nem ismerik. Egy új fogalmat szeretnék használ-



7. ábra IT képzettség, rendszerismeret és kibertudatosság megoszlásai

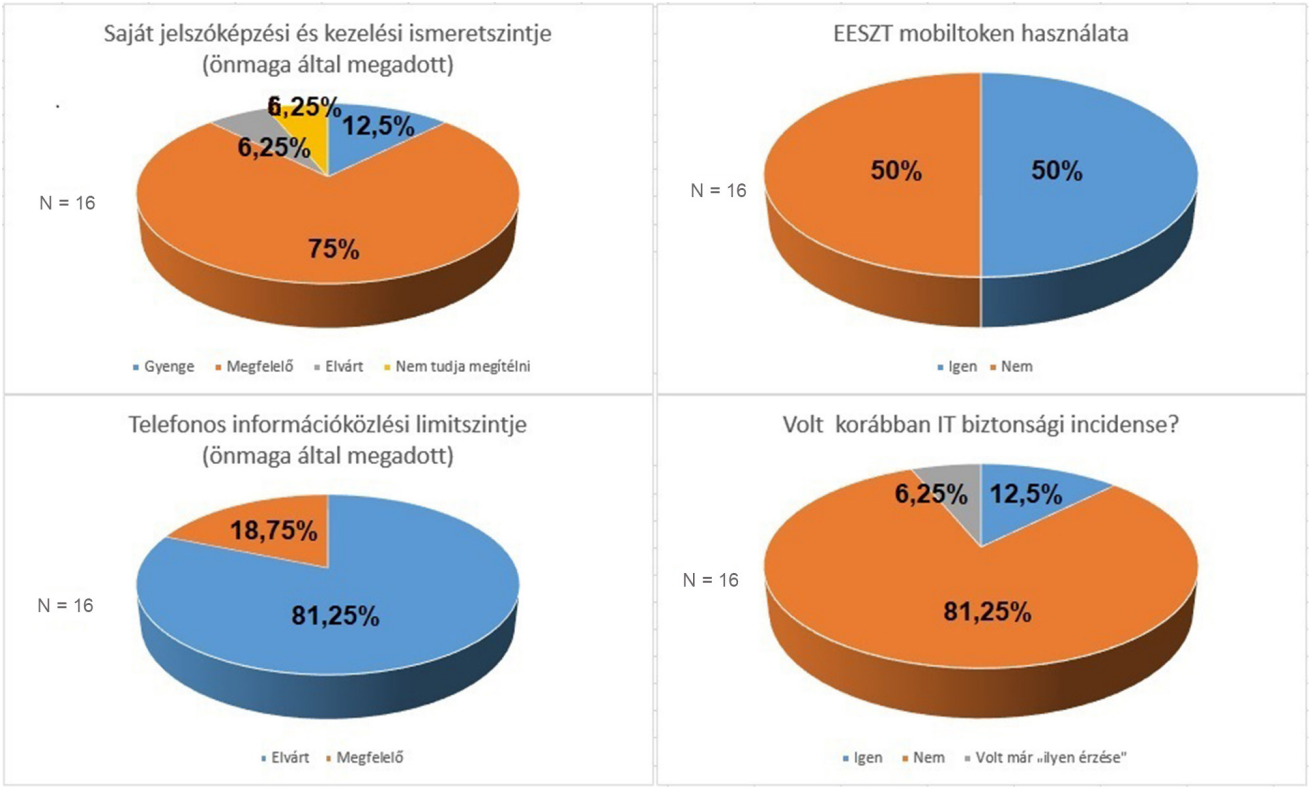
Forrás: saját szerkesztés

ni az egészségügyi dolgozói munkavállalók egyfajta adatmegosztására, munkafolyamataik során megosztott személyes jelszavaik munkatársaikkal történő megosztására. Erre a tényszerűségre az *információkulcs megosztást* alkalmazom. Fontos tény, hogy ez a magatartásmód minden jogszabályban és szabályzatban foglaltakkal ellentétes, az információbiztonságot veszélyeztető tényező. Ebben a pontban a személyes beszélgetések során, munkahelyi körülmények között „elkövetett" jelszóátadásokat, írásos feljegyzésekben és adott esetben telefonos megkeresésekre adott válaszadási hajlandóságot vizsgáltam. A válaszadók 80-20% arányban az elvárt és a megfelelő értékeket adták meg *(8. ábra)*. Vizsgálatom elemzése során az EESZT mobiltoken használat 50-50%-os arányt mutatott. Személyes tapasztalataimra alapozva azonban a mobiltelefon vs. eSzemélyi használatára vonatkozó érték napjainkra már 90-95% arányszámra becsülhető a mobiltoken javára. A „volt-e már korábban IT incidens elszenvedője" kérdésre két fő (12,5%) igennel válaszolt. Elmondásuk alapján egyikük a mobiltelefonján nem tudott belépni, ezt márkaszervizben orvosolták. A másik válaszadó esetében a számítógép merevlemeze sérült (nem tudta megadni, hogy szoftveres vagy hardverhiba lépett fel). Sajnos ő adatvesztést szenvedett el. Biztonsági mentéssel nem rendelkezett. Mindketten a magánéletükben élték meg az incidenseket. Egy fő adott egy nem egyértelmű választ, hogy az otthoni számítógépe rettenetesen lelassult, a megoldást az operációs rendszer újratelepítése jelentette.

Biometriával kapcsolatos ismeretek, attitűdök

Ebben a kérdéscsoportban számos fontos szempont jelent meg. Így például a biometriához való felhasználói viszonyulás, úgy technikai oldalról, mint etikai, jogi megközelítésből. A biometrikus azonosításról az összes felhasználó már hallott, legalábbis filmekben látott ilyen megoldásokat. Az arány 87,5 / 12,5%-os. Arra a kérdésemre, hogy támogatnák-e a biometrikus adataik felhasználását, a válaszadók több mint 2/3 része feltételekkel támogatná. A következő kérdésekre adott válaszaik alapján azonban az látható, hogy megfelelő garanciák mellett biztonságos azonosítási lehetőségnek látják a biometrikus azonosítást. Ezt támasztja alá, hogy útlevéllel mint biometrikus adatot is tároló okmánnyal 81,25% rendelkezik, mobiltelefonjaik használata során a válaszadók 50%-a alkalmazza a biometriát *(9. ábra)*.

Egy pilot tesztelési folyamat esetén a válaszadók 62,5%-a, garanciák biztosítása mellett részt vállalna a csökkentett paraméterű biometrikus azonosítási folyamat tesztelési folyamatában.

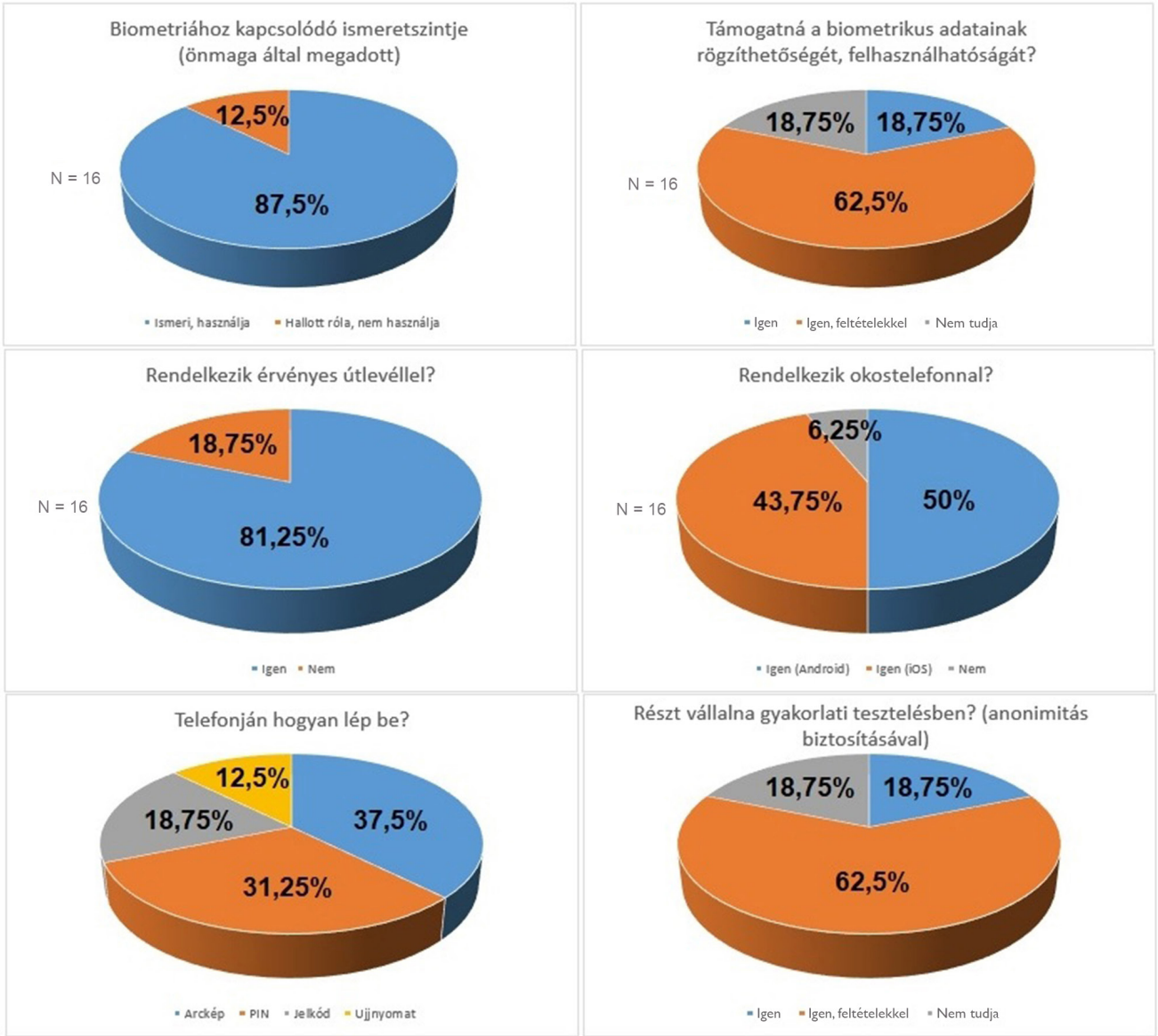


8. ábra Információbiztonsági tudatosságra adott válaszok megoszlásai

Forrás: saját szerkesztés

Összefoglalás és következtetések

A tanulmányban bemutatásra került a csökkentett paraméterű biometrikus azonosítás létjogosultsága. A tématerületen ilyen hazai vizsgálat korábban nem történt. A biztonságos betegellátás nonstop rendelkezésre állásához az informatikai rendszerek megfelelő szintű védelme alapfeltétel. Egyrészt a kibertér felől érkező támadásokat kell folyamatosan elhárítanunk. Bevezetőmben utaltam rá, hogy magyarázattal fogok szolgálni arra, hogy a csökkentett paraméterű biometrikus azonosítás miként lesz képes a kibertámadásokkal szembeni védekezést segíteni. A válasz egyszerű. A tárolt biometrikus azonosító nem visszafejthető, kompromittálódása nem valószínű. Ugyanakkor ha egy social engineering támadás következtében a felhasználó név-jelszó azonosítója kompromittálódik (akár kétfaktoros autentikáció során beékelődik egy második mobilkészülék) a támadó sikerrel jár. Ez a kitettség a biometrikus azonosítás autentikációs folyamatokba történő integrálásával csökkenthető. Kombinálható is lehet a jelenleg alkalmazott hitelesítési folyamatokban, a kétfaktoros azonosítás második faktoraként. Másrészt szembesültünk egy újonnan megjelent problémával is. A hazai Covid19 pandémia fekvőbetegeket ellátó kórházi egységeinél, nevezetesen a teljes testet elfedő védőruházatban történő munkavégzéshez kapcsolódó informatikai rendszerekbe történő belépések nehézségeivel. A betegellátók munkáját a csökkentett paraméterezésű biometrikus azonosítási megoldás nagyban tudja segíteni. A válaszadók megadták, hogy az informatikai képzettségüket, ismereteiket milyen formában szerezték meg. A helyzet teljes valid feltárására szimulációs felmé-



9. ábra Biometriával kapcsolatos ismeretekre, attitűd kérdésekre adott válaszok megoszlásai

Forrás: saját szerkesztés

rést kellett volna alkalmazni, amely nem becsült, hanem mért, egzakt eredménnyel szolgálhatott volna. A kis elemszámú mintán az N = 16 elvégzett vizsgálat válaszainak áttekintése azt sugallja, hogy az információbiztonsági tudatosság, a felhasználók viselkedésmintái, végzettségük, preferenciáik szoros összefüggésben állnak egymással. Ezt azonban egy nagy mintán elvégzett reprezentatív felmérés igazolni tudja. Egy reprezentatív felmérés a különböző informatikai tudásszintek és a kiberreziliencia, valamint az életkor összefüggéseire számszerű adatokkal fog szolgálni. Jelen vizsgálat egy feltáró kutatás volt. A mélyinterjúk során szerzett tapasztalatokat felhasználva a vizsgálatot egy nagy elemszámú (N = 700–1000) reprezentatív felmérés keretében – az anonimitás biztosításával – még szükséges elvégezni. A reprezentatív kutatásnak fel kell dolgozni a hazai orvostársadalom informatikai képzettségi és a kritikus egészségügyi központi betegellátó rendszerekhez való kapcsolódási attitűdjeit. Természetesen az egészségügyi ellátási területekhez kapcsolódó más végzettséggel és munkakörökkel rendelkezőket is be kell vonni a vizsgálatba. Kiemelt módon szükséges fókuszálni az informatikai rendszereket fejlesztő közreműködőkre, valamint a rendszereket üzemeltetőkre. A felmérés jól strukturált és minden szükséges információra kiterjedő online kérdőívek segítségével egyszerűen elvégezhető lesz. A nagy elemszámú minta kiértékelése meg tudja alapozni a rá épülő egészségügyi környezetben megvalósítható csökkentett paraméteres biometrikus hitelesítési lehetőségek technológiai kidolgozását, mely a mesterséges intelligencia bevonásával lesz megoldható. A jelenleg rendelkezésre álló vizsgálati eredmények összevetése és folytonos követése a vonatkozó tudományos szakirodalommal jogi és etikai szempontból is megalapozza a kutatás következő mérföldkövének elvégzését. Ugyanakkor fontos tényező, hogy egy egészségügyi informatikai alkalmazásnak a teljes életciklusában védettnek kell lennie a fejlesztéstől a selejtezésig a mindennapos használati eseteken át. Nem szabad szem elől téveszteni, hogy a személyes egészségügyi adatok különleges személyes adatoknak minősülnek. A hazai egészségügyben a csökkentett biometriai azonosítás és hitelesítés bevezetése az üzleti folyamatokba, majd azok nonstop alkalmazása számos szempontból is jelentős eredményekkel kecsegtet. Ugyanakkor nem feledhetjük, hogy a legújabb és legjobbnak értékelt technológia sem helyettesítheti az embert. Az egészségügyi informatikai rendszerek védelmét a humán edukáció mellett modern technológiai megoldásokkal is erősíteni kell.

Köszönetnyilvánítás

Köszönettel tartozom az Óbudai Egyetem vezetésének, prof. dr. habil. Kovács Levente rektor úrnak, prof. dr. Gulácsi László tudományos rektorhelyettes úrnak, témavezetőmnek, prof. dr. Rajnai Zoltánnak, a Pest Megyei Flór Ferenc Kórház főigazgatójának, dr. Trombitás Zoltán úrnak, Kovács Éva vállalati szakértőnek, valamint az interjú alanyainak a kutatás első mérföldkövéhez nyújtott támogatásért. Prof. dr. Kovács Tibor vállalati szakértőnek, aki számos hasznos ismerettel, véleményével segítette munkámat.

A 1007824. számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a KDP-2020 pályázati program finanszírozásában valósult meg.

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Irodalomjegyzék

Ahlfeldt, R. (2008) Information Security in Distributed Healthcare, Exploring the Needs for Achieving Patient Safety and Patient Privacy. PhD-értekezés, University of Skövde

Balogh, J., Szócska, M., Palicz, T., Kontsek, E., Pollner, P., Varga, G., … Joó, T. (2022) A mesterséges intelligencia alapú megoldások fejlesztése és bevezetése az egészségügyben – kézműves manufaktúrától a gyártósorig? IME: Interdiszciplináris Magyar Egészségügy/Informatika és Menedzsment az Egészségügyben, Vol. 21. No. 2. pp. 56–63. https://doi.org/10.53020/IME-2022-206

Ekler, P., Pásztor, D. (2020) Alkalmazott mesterséges intelligencia felhasználási területei és biztonsági kérdései – Mesterséges intelligencia a gyakorlatban, Scientia et Securitas, Vol. 1. No. 1. pp. 35–42. https://doi.org/10.1556/112.2020.00006

Győrffyné Holló K. (2022) A biztonságtudatosság hiánya, mint kockázati tényező vizsgálata, különös tekintettel az adatvédelmi és információbiztonsági szabályok alkalmazására. Doktori értekezés. Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Doktori Iskola

Hausken, K. (2020) Cyber resilience in firms, organizations and societies. Internet of Things, Vol. 11. https://doi.org/10.1016/j.iot.2020.100204

Jasztrab, J. Sz. (2017) A katonaorvosi pályaelhagyás. Doktori (PhD) értekezés. Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola

Kovács, L. (2020) A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. Honvédségi Szemle, Vol. 148. No. 5. pp. 3–18. https://doi.org/10.35926/HSZ.2020.5.1

Kovács, T., & Ujhegyi, P. (2021) Csökkentett paraméterű biometrikus azonosítási lehetőségek a kritikus infrastruktúrák és a speciális objektumok védelménél. Biztonságtudományi Szemle, Vol. 3. No.1. pp. 137–146.

Kovács, É., Kovács, T. (2022). Identification and Authentication Potentials Based on Limited Biometric Data. In: Kovács, T.A., Nyikes, Z., Fürstner, I. (eds) Security-Related Advanced Technologies in Critical Infrastructure Protection. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-2174-3_34

Krasznay, Cs. (2020) Kiberbiztonsági kompetencia hálózatok Európában – K+F+I lehetőségek a következő évtizedben. Scientia et Secu-

ritas, Vol. 1. No. 1. pp. 43–48. https://doi.org/10.1556/112.2020.00007
Muha, L. (2007, 2015) A kritikus infrastruktúrák védelme. RelNet Technológia Kft.
Oroszi, E. D. (2021) Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük. Dunakavics, Vol. VIII. No. V. pp. 5–20.
Palicz, T., Sas, T., Tisóczki, J., Bencsik, B., & Joó, T. (2020) „Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben ["Your money or your life!" – Ransomwares in healthcare information systems]. Orvosi Hetilap, Vol. 161. No. 36. pp. 1498–1505. https://doi.org/10.1556/650.2020.31788
Rajnai, Z. (2017) Információbiztonság Tudatosság. A XXII. Fiatal műszakiak tudományos ülésszak előadásai. Műszaki Tudományos Közlemények, Vol. 7. pp. 37–42. https://doi.org/10.33895/mtk-2017.07.02
Rexha, B., Shala, G., Xhafa, V. (2018) Increasing Trustworthiness of Face Authentication in Mobile Devices by Modeling Gesture Behavior and Location Using Neural Networks. Future Internet, Vol. 10. No. 2. Article 17. https://doi.org/10.3390/fi10020017
Yan, Z., Pan, C., & Xu, Z. (2015) The Study on the Identity Verification between the on-Site Face Image and the ID Photo. In Proceedings of the Information Science and Management Engineering III - ISME, SciTePress, pp. 130–133. https://doi.org/10.5220/0006020401300133

Webhelyek

BM OKF Szabályozás, jogszabályok. https://www.katasztrofavedelem.hu/33331/szabalyozas-jogszabalyok [Letöltve: 2022. 07. 29.]
EESZT Elektronikus Egészségügyi Szolgáltatási Tér. https://regi.ugyintezes.magyarorszag.hu/szolgaltatasok/eeszt.html [Letöltve: 2022. 07. 20.]
EESZT Lakossági (2022) https://www.eeszt.gov.hu/ [Letöltve: 2022. 07. 25.]
Európai Bizottság: Európai digitális személyazonosság, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_hu [Letöltve: 2022. 06. 23.]
GYEMSZI IRF Rendszerelemzési Főosztály (2012) EHR (electronic health record) rendszerek Európában. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwifq6XVmvL5AhVslosKHSezDswQFnoECAQQAQ&url=https%3A%2F%2Fera.aeek.hu%2FHealthOnline%2Fkepek%2Fho%2Fanyagok%2Fehr.doc&usg=AOvVaw2B1zf4CIAMG0uoMECQhKDs [Letöltve: 2021. 04. 22.]
Milyen személyes adatok minősülnek különleges adatnak? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_hu [Letöltve: 2022. 04. 25.]
Muha, L. (2008) Az informatikai biztonság egy lehetséges rendszertana 1. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiz_6uUo_L5AhXokIsKHSlgDTUQFnoECAIQAQ&url=http%3A%2F%2Freal.mtak.hu%2F11147%2F1%2F1228872.pdf&usg=AOvVaw0DdgpF_vNAK7OzEgIKEe1s [Letöltve: 2021. 12. 25.]
Nemzeti Kibervédelmi Intézet (NKI) (2022) https://nki.gov.hu/it-biztonsag/hirek/az-ukrajnat-celzo-kibermuveletek-eddigi-tanulsagai/ [Letöltve: 2022. 08. 01.]
Sophos (2022) Ransomware-Report 2022: Gesundheitswesen. https://news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/ [Letöltve: 2022. 07. 25.]
COM(2018)237 – Communication Artificial Intelligence for Europe; https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vknuqttbx4zb [Letöltve: 2022. 11. 25.]
https://sealog.hu/tudastar/fogalomtar/social-engineering [Letöltve: 2022. 11. 26.]
https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278 [Letöltve: 2022. 11. 30.]
https://drive.google.com/drive/folders/18sr29JM_BwaRTzbIfUOKyvftYqiRd8dD [Letöltve: 2022. 12. 03.]
https://onestore.nokia.com/asset/212587?did=D000000003506&gclid=EAIaIQobChMIieW-qc_k-wIVC3YYCh3nYwAAEAAYAyAAEgK7RPD_BwE [Letöltve: 2022. 12. 03.]
https://semmelweis.hu/hirek/2023/01/20/szenior-akademia-fokuszban-a-tav-a-robot-es-az-ursebeszet/ [Letöltve: 2022. 12. 03.]
https://semmelweis.hu/hirek/2022/06/25/bejarason-adtak-at-a-da-vinci-robotsebeszeti-rendszert-a-semmelweis-egyetemen/ [Letöltve: 2022. 12. 03.]
https://biometrikus.hu/biometrikus-azonositas-jelentese/ [Letöltve: 2022. 12. 03.]
https://semmelweis.hu/koronavirus/mit-tehetunk/altalanos-informaciok-a-covid-19-megbetegedesrol/ [Letöltve: 2022. 12. 04.]
https://www.securinfo.hu/termekek/it-biztonsag/1295-social-engineering-tamadasi-technikak-avagy-a-vegso-megoldas-a-felhasznalo.html [Letöltve: 2022. 12. 04.]

Jogszabályok

https://eur-lex.europa.eu/eli/reg/2016/679/oj
41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://net.jogtar.hu/jogszabaly?docid=a1200166.tv
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845
1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2012/19., 1378–1397. https://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020/81., 2101–2119. https://njt.hu/jogszabaly/2020-1163-30-22 [Letöltve: 2022. 07. 30.]
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://net.jogtar.hu/jogszabaly?docid=a1200166.tv