ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

SZŰCS KATA REBEKA

Mobil alkalmazásokkal kapcsolatos felhasználói biztonság

Témavezető: Dr. habil. Reicher Regina Zsuzsánna

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. Augusztus 10.

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Dr. Tick Andrea

Titkár:

Dr. Saáry Réka

Tagok:

Prof. Dr. Czakó Erzsébet

Dr. habil. Kiss Gábor

Dr. Póser Valéria

Bírálók:

Dr. Számadó Róza

Dr. Eisingerné dr. Balassa Boglárka

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott **Szűcs Kata Rebeka kijelentem**, hogy a **Mobil alkalmazásokkal kapcsolatos felhasználói biztonság** című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2024.08.30.

Szűcs Kata Rebeka
aláírás

TARTALOMJEGYZÉK

BEVEZETÉS: MOBIL KORSZAK, MOBIL APPLIKÁCIÓK 1
Témaválasztás indoklása, tudományos probléma megfogalmazása 2
Célkitűzések, kutatási módszerek, kutatás felépítése 3
1. MOBIL EGÉSZSÉG ALKALMAZÁSOK 8
1.1. Egészségtudatosság terjedése 8
1.2. Befolyásoló technológia 12
1.3. Megészség appok- COVID-19 és hozzá kapcsolódó applikációk 14
2. APPLIKÁCIÓK BIZTONSÁGÁNAK VIZSGÁLATA 19
2.1. Fogalmi keretek: biztonság és adatvédelem 19
2.2. Mobil alkalmazásokra vonatkozó fenyegetések 23
2.2.1. Alkalmazással kapcsolatos fenyegetések 24
2.2.2. Web-alapú fenyegetések 27
2.2.3. Vezeték nélküli kapcsolat fenyegetései 29
2.2.4. Hozzáféréssel kapcsolatos fenyegetések 32
3. FELHASZNÁLÓI BIZTONSÁG, A KÉRDŐÍV ELMÉLETI HÁTTERE 38
3.1. Kutatási munkák, pilot kutatás 38
3.2. Felhasználói biztonsági attitűdök és motivációk 42
3.3. Megoldási javaslatok a felhasználói biztonsági kockázatok csökkentésére 45
3.3.1. Szabályozás szükségessége 46
3.3.2. Megfontolások applikáció fejlesztésnél 52
3.3.3. Mit tehet a felhasználó? 55
3.4. Felhasználói szempont kiegészítése- Applikációk értékelése 59
4. REPREZENTATÍV KUTATÁS EREDMÉNYEI 62
4.1. Az egészség és életmód appok és azzal kapcsolatos adatok megítélésének vizsgálata 64
4.2. A kérdőív általános összefüggései 66
4.3. Biztonságtudatosság és biztonságérzet kapcsolata 71
4.4. Viselkedési attitűdelemmel kapcsolatos elemzés 77
4.5. Klaszterek további elemzése 82
4.6. Ellenőrző, kiegészítő kérdések elemzése, egészséggel kapcsolatos appok kérdések 88
4.7. Csoportok attitűdjeinek összefoglalása 91
ÖSSZEGZETT KÖVETKEZTETÉSEK- ÚJ TUDOMÁNYOS EREDMÉNYEK 93
AJÁNLÁSOK 100
IRODALOMJEGYZÉK 101
TÁBLÁZATJEGYZÉK 114
ÁBRAJEGYZÉK 115

MELLÉKLETEK 116
KÖSZÖNETNYILVÁNÍTÁS 131

BEVEZETÉS: MOBIL KORSZAK, MOBIL APPLIKÁCIÓK

Manapság az életünket egyre inkább befolyásolja az internet és a mobil eszközök megjelenése. Számokkal alátámasztva ez még inkább érzékelhető. A Digital 2021 jelentés szerint [1] világszinten a teljes népességnek (7,83 milliárd fő) 66,6%-ának van mobiltelefonja és 59,5% használ internetet, mely számok egy növekvő tendencia részei. Világszinten az Android felhasználók átlagosan 4 óra 10 percet töltenek a telefonjaik használatával naponta, egy másik vizsgálat szerint pedig egy tipikus felhasználó 3 órát és 39 percet tölt átlagosan az internetezéssel a mobiltelefonjáról. Bár a laptopon keresztüli forgalom még szintén jelentős (41%), a 2020 decemberében kiszolgált weboldalak 56%-át mobiltelefonokon futó böngészőkön kérték. A mobil technológia fejlődésével az eredeti és elsődleges funkció, a hangtovábbítás, telefonálás mára kiegészült számtalan egyéb funkcióval, többek között egyéb kommunikációs formákat, banki ügyintézést, fényképezést és videózást is lehetővé téve. Nem csak a szoftverek, de a hardver fejlődése is még kényelmesebbé tette a mobilozás élményét a felhasználóknak, így könnyedén vált a mindennapok részévé. Ez a jelenség a szolgáltatók szempontjából is új lehetőségeket hozott, ugyanis az eszközök erősen személyhez köthetőek, így lehetőséget adnak a szorosabb elköteleződés kialakításához, az akár visszamenőleg történő, mélyrehatóbb megismeréshez, azonosításhoz és rendkívüli pontosságú marketingtevékenységekhez is [2]. Magyarországon 2022 negyedik negyedévében 100 főre 141 mobiltelefon-előfizetés jutott [3], a mobil adatforgalom pedig közel harmadával nőtt egy év alatt [4]. A háztartások 76,7%-ában használtak szélessávú mobilinternetet [5]. A szokásokat tekintve a lakosság 83,4%-a használta az internetet naponta többször vagy folyamatosan, további 12%-uk pedig a jelentések szerint naponta egyszer szinte minden nap [6]. Az EU-27 országaiban az internetezők aránya (a 16-74 éves lakosság százalékában) 89% volt 2021-ben (ami megegyezik a hasonlóan számolt magyar átlaggal) [7].

A felgyorsult világ része tehát, hogy a nap minden percében legyen elérhető a felhasználó, de az is, hogy a felhasználó számára legyenek bármikor, azonnal elérhetők az információk, szolgáltatások a digitális térben. Ezt nagyban megkönnyítik az applikációk, melyek az élet szinte minden területéhez segítséget nyújthatnak. 2023-ban a Google Play Store-ban 2,87 millió, az Apple App Store-ban 1,96 millió applikáció volt elérhető letöltésre a felhasználóknak. Ezen appok letöltési statisztikáira számos forrás eltérő adatokat közöl [8], az azonban bizonyosnak látszik, hogy világszinten százmilliárdos nagyságrendről beszélhetünk. Várhatóan ezek a számok is tovább nőnek a jövőben. Érdekes módon az alkalmazásokból

származó bevételek 98%-a világszerte ingyenes alkalmazásokból származik és csak az emberek töredéke hajlandó fizetni a letöltésekért. Ez azonban nem jelenti azt, hogy a felhasználás során a későbbiekben ne használnának egyéb mobilalkalmazás-bevételszerzési stratégiákat, például alkalmazáson belüli hirdetéseket és alkalmazáson belüli vásárlásokat (*in-app advertising, in-app purchases*). Bár a felhasználók sok applikációt töltenek le, gyakran törlik is őket, általában ugyanis egy adott időszakban egyszerre csak egy adott mennyiségűt (kb. 10 darabot) használnak minden nap, könnyen megválnak a rosszul tervezett, nem használt, nem bevált applikációktól [9]. Az applikációk számtalan kategóriában elérhetők, a teljesség igénye nélkül például: közösségi média, játék, oktatás, életmód, üzlet, szórakozás, utazás, pénzügy, zene, hírek, vásárlás és egészség témában is. A hatalmas mennyiségű és típusú elérhető app és ezek felhasználói tömegeik mind hozzájárulnak az adatrobbanáshoz. Az applikációk néhány mérőszámát ismerve láthatóvá válik, hogy milyen sokféle adatot szolgáltathatnak a felhasználókról. Gyűjthető például az elkötelezettség hossza, a fókuszált elkötelezettség ideje, a felhasználói preferenciák, a kattintási ráta, vagy hogy mikor kezd el hanyatlani a használat mennyisége [10]. A Google például a saját adatvédelmi tájékoztatója szerint az alábbi fő kategóriákban gyűjt adatokat: felhasználók tettei, amiket a felhasználó létrehoz, valamint felhasználóhoz tartozó személyes adatok. Mindezeket a tájékoztató szerint a felhasználói élmény javítására, például a keresések eredményeinek személyre szabására és relevanciájának növelésére, automatikus kitöltésre (online dokumentumoknál), ajánlásokra használják [11].

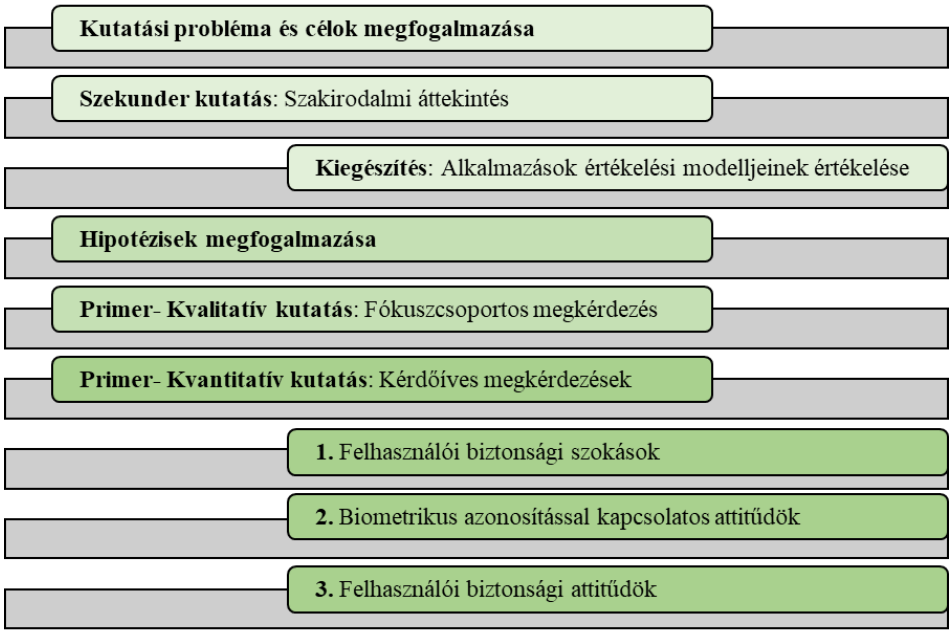
Témaválasztás indoklása, tudományos probléma megfogalmazása

Napjainkban az internet és az okostelefonok tehát érzékelhetően életünk szerves részévé váltak. A mobil technológia befolyásolja többek között az életminőségünket, viselkedésünket és döntéseinket. Ezen trendek hatással vannak az egészségügyre, egészségtudatosságra is, új lehetőségeket teremtve a technológia jobb kihasználására. Ezt támogatja az egészségtudatosság terjedése is, amely hozzájárult az egészség témájú mobil appok létrejöttéhez. Ez mind számtalan lehetőséget, ugyanakkor veszélyt is rejt, így jogosan figyelhető meg egy biztonságtudatossági trend is. A rengeteg alkalmazás hatalmas mennyiségű adat gyűjtését, kezelését, rendszerezését és hasznosítását is magával hozta, amely igen fontos kérdéseket és feladatokat vet fel mind adatvédelmi és magánszféra védelmi, mind biztonsági szempontból. Ezt egészíti ki a személyes érdeklődésem a téma iránt, fontos számomra a magánélet védelme és biztonság kérdése (mely egyre gyakrabban kerül napirendre a jelenkorban), valamint rengeteg applikációt használok a mindennapokban. A kutatásom során szakmai tapasztalataim

is segítettek, melyeket kiberbiztonsági szakemberként szereztem. Megfigyelésem szerint annak ellenére, hogy a biztonság népszerű téma lett, mely fontos a felhasználóknak, sok esetben hiányzik az ehhez kapcsolódó tudatosság és vagy érdeklődés az átlagfelhasználóknál, akik önkéntesen saját adataikkal fizetnek az alkalmazások használatáért. Előfordulhat, hogy a kényelmi funkciók használatáért cserébe biztonsági vagy adatvédelmi szempontból kevésbé jó döntéseket hoznak, bár lehet ez nem is érdekli őket. Ezt a jelenséget írja le például az adatvédelmi, vagy magánélet védelmi paradoxon (privacy paradox), mely létezésével nem minden kutató ért egyet. Az online viselkedéssel kapcsolatos legújabb kutatások eltéréseket tártak fel a felhasználói hozzáállás és a viselkedés között, vagyis bár a felhasználók azt állítják, hogy nagyon aggódnak a magánéletük miatt, ennek ellenére nagyon keveset adnak személyes adataik, magánszférájuk védelmére [12]. Disszertációm célja az volt, hogy a szakirodalom megismerése után megvizsgáljam és elemezzem a fent leírt jelenséget, vagyis megérteni, hogy hogyan írható le a felhasználók biztonsági attitűdje és milyen tényezők járulnak ehhez hozzá, mik befolyásolják. Célom megvizsgálni azt is, hogy egyáltalán fontos-e ez a téma, a biztonság a felhasználóknak, vagyis olyan témának tekintik-e, amelyre figyelmet kell fordítaniuk a mindennapokban. Ezáltal szándékom az ezzel kapcsolatos tudatosság növelése is, mivel a biztonság nem csak a technológiai fejlődés előre lépéseivel, hanem a biztonságra vonatkozó attitűdök és viselkedés jobb megértésével is fejleszthető. Mert hiába a legmodernebb biztonsági szolgáltatások és intézkedések, ha végül az emberi láncszem gyengeségét kihasználva sikerrel járnak a támadók.

Célkitűzések, kutatási módszerek, kutatás felépítése

A kutatás első, általános célja a felhasználói biztonsági attitűdök megértése volt. Ennek alapja a szakirodalmi áttekintés során megismert elméleti háttér és az ezek alapján megalkotott modell, mely segítségével később az alábbi kérdések megválaszolását segítő kérdőívet is megalkottam. A későbbiekben részletezett magyar lakosságra reprezentatív kutatást számos kisebb megalapozó pilot kutatás előzte meg, mobil egészség alkalmazások és a biztonság témaköreiben, szakirodalmi rendszerezés, fókuszcsoportos megkérdezés és kérdőíves kutatási módszereket felhasználva, melyeket a későbbiekben mutatok be. A kutatási folyamatot az 1. ábrán látható módon építettem fel. Az egyes elemeket a későbbiekben még részletesebben is bemutatom.



1. ábra Kutatási folyamat. Saját szerkesztés

A kutatásom témája az egészség témájú mobil applikációkkal kapcsolatos biztonság volt. A tanulmányaim során szekunder kutatással és primer kisebb kutatásokkal teszteltem a feltevéseim egyes részeit a finomítás érdekében (például korábbi kisebb mintás lekérdezések és fókuszcsoportos beszélgetések, melyeket később kifejtek [13]) és megállapítottam, hogy a felhasználói csoportosítás valószínűleg nem az applikációk témájától függ, hanem az azokkal kapcsolatos attitűdök alapján tehető meg. Ezt figyelembe véve a kérdőívben végül nem kapott hangsúlyt az egészség applikációk használata, csak néhány kérdést tettem fel az ilyen típusú alkalmazásokkal kapcsolatban. Ezért a második kutatási kérdésem ezt a feltevést vizsgálja.

A vizsgálat alapja a biztonsági attitűd összetevői közötti kapcsolat feltételezése volt. A logika az, hogy a felhasználók biztonságtudatossága és a biztonságérzete eredményezik a biztonsági viselkedést. A kognitív és affektív komponenseket figyelembe véve négy felhasználói csoport várható, amelyek mátrix struktúrában írhatók le. Az elméleti mátrix sorai azt mutatják, hogy a felhasználók ismerik-e, tudással rendelkeznek-e a biztonságról (a kognitív komponens), az oszlopok pedig azt, hogy a felhasználók törődnek-e a biztonsággal (az érzelmi komponens). Összefoglalva az alábbiakban található a négy várható csoport.

- Olyan felhasználók, akik fontosnak tartják és vannak biztonsági ismereteik,
- Olyan felhasználók, akik törődnek a biztonsággal, de nem tudnak róla túl sokat,
- Olyan felhasználók, akik nem törődnek a biztonsággal, bár vannak ismereteik róla,
- Olyan felhasználók, akik nem tartják fontosnak és nincsenek is biztonsági ismereteik.

A csoporthovatartozás alapján a biztonságra irányuló viselkedési komponenst is felmérem, megvizsgálva a három attitűdkomponens kapcsolatát. Ennek a logikának a használata segíthet a felhasználók biztonsági hozzáállásának jobb megértésében, ami hasznos lehet a felhasználók, az alkalmazásszolgáltatók és a szabályozók számára is. Az attitűd elemeinek kérdőíven keresztüli meghatározásához két másik, a témakörhöz tartozó pszichológiából ismert elméletet is használtam, a védelemmotivációs elméletet (Protection-motivation theory, PMT) és a tervezett cselekvés elméletét (Theory of Planned Behavior, TPB). A későbbiekben mindegyik modellt ismertetem.

A fentiek felmérése kvantitatív módszerrel, nevezetesen kérdőívvel történik. A szakirodalmi kutatáson alapuló kérdőív összeállítás után egy szolgáltató, az Ipsos Instant Research Service segítségével online történt a lekérdezés, lehetővé téve, hogy a minta reprezentatív legyen a magyar népességre nem, életkor, régió és település mérete szerint. (Fontos kiemelni, hogy nem vettem igénybe az említett szolgáltató segítségét a felmérés elkészítéséhez, kizárólag a lekérdezéshez.) A kérdőív három fő részből áll. Az első rész a biztonság különböző aspektusait vizsgálja, hogy illeszkedjenek az attitűdmodell első két összetevőjéhez, igénybe véve a már említett védelemmotivációs és tervezett cselekvés modellek elemeit, beleértve az ellenőrzést, a tudást, a képességet, a tudatosságot, az energiabefektetést, a biztonság kérdésének értékelését, az észlelt kockázatot és a bizalmat. Ez metrikus skála segítségével történt, a későbbi főkomponensek és klaszterek létrehozása érdekében. A főkomponens elemzés célja az elvárt attitűd elemek megjelenésének visszaigazolása volt, mely aztán a későbbiekben a klaszterelemzés alapjaként használok.

A felmérés második részének célja a válaszadói attitűdök viselkedési komponensének vizsgálata volt. A biztonság növelésére irányuló intézkedéseket egy egyszerű intézkedési lista segítségével vizsgáltam, mely a korábbi kutatásokon alapul [14], [15]. Fontos megjegyezni, hogy a viselkedést önbevallással vizsgáltam, így a kitöltők nem biztos, hogy a valós viselkedésüknek megfelelően nyilatkoznak, valamint a kontextust sem képes felmérni ez a módszer. Általános kép kialakításához viszont megfelelő lehet. Ezen kívül még kétféle feleletválasztós kérdés került a kérdőívbe: az egyik, amely az alkalmazástelepítéskor túlzott hozzáférési engedélyek jóváhagyásának motivációját vizsgálja, a másik pedig az alkalmazás kiválasztásánál fontos tényezőkre kérdez rá. Mindkettőben szerepel a biztonság is, de vannak más válaszlehetőségek is, mint például az alkalmazások funkcionalitása vagy esztétikai szempontok. Utóbbi kérdések segítenek a felhasználói viselkedés és motivációk további elemzésében.

A kérdőív harmadik része néhány ellenőrző, visszacsatoló kérdést tartalmaz, valamint néhány kérdés erejéig kitér arra is, hogy a felhasználók hogyan viszonyulnak az egészséges életmódhoz és az önkövető applikációkhoz. Ahogy már említettem, kutatásaim megkezdésekor ezen appokra koncentráltam, de mivel az előzetes kutatások alapján arra a következtetésre jutottam, hogy a biztonsági aspektusai ezeknek is hasonlóak, mint bármelyik másik funkciójú alkalmazásnak, így egy általánosabb kutatást folytattam le. Szűrőkérdés (sem a mobilalkalmazás-használatra vonatkozóan, sem az egészségappokra vonatkozóan) szándékosan nem került a kérdőívbe, hiszen internet- és alkalmazáshasználati szokásaitól függetlenül minden felhasználónak megvan a véleménye (és mivel a kérdőívet online töltötték ki, és a minta bizonyos szempontok szerint reprezentatív a magyar lakosságra nézve, valószínűleg van valamilyen tapasztalatuk ezen a területen, ahogy azt a mobil- és internethasználati statisztikák is kimutatták). Az eredményeket az SPSS szoftverrel (29-es verzió – ingyenes próbaverzió) elemeztem.

Összefoglalva a jelen írás a következő kutatási kérdésekre kíván választ adni és az alábbi hipotéziseket vizsgálja.

1.Kutatási kérdés: A felhasználók biztonsági szempontból ugyanúgy kezelik az egészség témájú applikációkat, mint bármilyen más témájú alkalmazást?

> **H1**: A felhasználók alkalmazás használatában biztonsági szempontból különbség van az egészség témájú applikációk és bármilyen más témájú alkalmazás között.

2.Kutatási kérdés: Hogyan írható le a válaszadók biztonsági attitűdje? (Melyből következtetéseket vonhatunk le a magyar lakosság biztonsági attitűdjeire.)

Jelen kutatás a felhasználók biztonsággal kapcsolatos attitűdjének elemzését tűzte ki célul, mely vonatkozik a biztonsági attitűd irányára és erősségére is, a csoportok egymáshoz képesti értékeit figyelembe véve.

> **H2**: A korábbi biztonsági incidenssel kapcsolatos negatív tapasztalatok befolyásolják az alkalmazásokba vetett bizalmat.

2.1. Kutatási kérdés: Csoportosíthatók-e a résztvevők biztonságtudatosságuk és biztonságérzetük alapján?

A kutatási kérdésre való válaszkeresés során a hipotézisek elemzésén felül célom statisztikai elemzési módszereket használva először a kérdésekből való főkomponenselemzés elvégzése,

hogy igazoljam az attitűdelemek kérdőívben való megjelenését. Ezután célom klaszterelemzést is végezni a kialakult főkomponensek mentén, hogy megismerjem a lehetséges felhasználói csoportosításokat biztonsági attitűd szempontból.

> **H2.1**: A nagyobb mértékű biztonságtudatosság nagyobb mértékű biztonsági kockázatérzettel jár együtt.

2.2. Kutatási kérdés: Hogyan hat a biztonságtudatosság és a biztonságérzet alapján meghatározott csoporthovatartozás a biztonságra irányuló viselkedésre?

A kutatási kérdés kapcsán a hipotézisek vizsgálata mellett célom még az attitűdelemek kapcsolatát leíró modellalkotás is, mely összefoglalja a kutatásom során feltárt elemeket, és azok kapcsolatát.

> **H2.2a**: A biztonságtudatosság befolyásolja a biztonsági viselkedést. Minél magasabb a biztonságtudatossága egy felhasználónak, annál több biztonsági intézkedést tesz.
> **H2.2b**: A biztonságérzet befolyásolja a biztonsági viselkedést. Minél inkább érzi a felhasználó a biztonsági kockázatokat, annál több biztonsági intézkedést tesz.

2.3. Kutatási kérdés: Hogyan jellemezhetők a létrejött csoportok?

> **H2.3a**: Akik biztonságtudatosabbak, azok jobban lépést tartanak a technológiai fejlődéssel, mint a kevésbé biztonságtudatosak.
> **H2.3b**: Az IT területen jártas válaszadók biztonságtudatosabbak, mint a területen nem jártas válaszadók.
> **H2.3c**: Az IT területen jártas válaszadók alacsonyabb szintű biztonsági kockázatot észlelnek, mint a területen nem jártas válaszadók.

3.Kutatási kérdés: Mi alapján választanak a felhasználók applikációkat? Melyek a választási szempontok és ezek hogy függenek össze a biztonságtudatossággal és biztonsággal kapcsolatos érzelmekkel? (Mintegy biztonsági cselekvésként értelmezve az alkalmazásválasztást is.)

> **H3**: A biztonság az elsődleges választási szempontok közé tartozik az applikációk választásánál.

1. MOBIL EGÉSZSÉG ALKALMAZÁSOK

A mobil applikációk egyik népszerű kategóriája az életmód és egészség témájú applikációk. Annak ellenére, hogy végül nem a téma szerint szűrtem a nagy kutatási kérdőívemet, az alábbi fejezetben az egészségtudatossági trend és annak lehetőségei után bemutatom az egészség témájú mobil applikációkat. Ismertetem ezek lehetséges pozitív és negatív hatásait, valamint röviden kitérek a COVID-19 nyújtotta új helyzetre és az azzal kapcsolatos mobil app megoldásokra.

1.1. Egészségtudatosság terjedése

A mobil egészség kialakulását és terjedését napjainkban nem csak a mobil eszközök és internet térnyerése, hanem az egészségtudatosság népszerűségének növekedése is támogatja. Egyre inkább előtérbe kerül az egészség és az egészséges életmód a mindennapokban, a hobbik választásánál, vagy a médiában, közbeszédben. Megfigyelhető, hogy míg korábban ez szimplán az ember egészséges állapotát jelentette, manapság egy holisztikus jóllétre gondolunk, nem csak fizikai, de mentális és érzelmi értelemben való egészség a cél. Látható ez az egészség definíciójának alakulásából is: az 1950-es években csak a betegség hiányát jelentette, ma már komplexebben értelmezendő, „már nemcsak a test és a lélek harmóniájáról van szó, hanem az értelem, a család, a foglalkozás és a tanulás is megjelennek, mint a komplex egészség összetevői” [16, p. 1]. A közösségi média korában az egészség, edzés, kidolgozott test és szépülésre fordított idő is olyan luxus, amit az emberek szívesen mutatnak meg egymásnak, vágnak fel vele. Erre a tényre egész iparágak, vállalatok és vállalkozások épültek napjainkra. Az egészségtudatos trend növekvő létszámú követő csoportja a Natural Marketing Institute szegmentációs modellje szerint a LOHAS *(lifestyle of health and sustainability)* csoport is. Tagjaik tudatos fogyasztók, érzékenyebbek a környezet és társadalom problémáira és felelősséget is vállalnak ezekért. Korai elfogadók az új trendekkel, az autentikus értékek, fenntarthatóság, belső értékek, belső egészség és az egészségtudatosság fontos számukra [17]. Megfigyelhető az is, hogy ez leginkább egy korcsoporthoz köthető (bár véleményem szerint egyre gyakrabban figyelhető meg ennek minden más korcsoportra való hatása is). Leginkább az Y generáció, a millenárisok, érintettek egy felmérés szerint, 72%-uk költene anyagi javak helyett inkább élményekre és törődik naponta a saját jólétével [18].

A technológia és mobil applikációk fejlődése többek között az egészségügyre és egészségtudatosságra is hatással van. A mobil egészségügy vagy megészség (*mHealth*) egy gyorsan növekvő, egészségügyet és infokommunikációs technológiákat összekötő ágazat, mely

magába foglalja az egészségüggyel kapcsolatos szolgáltatásokra, valamint megelőzésre is alkalmas mobil applikációkat. Ezek gyakran kezelnek személyes adatokat is [19, p. 2]. Az EU mobil egészségről szóló Zöld könyve szerint [20, p. 3] az megészség mobil eszközök által támogatott orvosi és közegészségügyi gyakorlat, melynek részei az életmód és wellness mobil applikációk, az okoseszközök, okos orvostechnikai eszközök is. Ezen applikációk alkalmasak lehetnek az egészségügy segítésére, esetleges reformjára is.

A PWC (PricewaterhouseCoopers) felmérése szerint [21] a mobil eszközök beépítése magában a gyógyításban nem hoz nagy újítást, csak annak módjában. Segíthet leküzdeni az adminisztrációs és távolság miatti problémákat. A nagy távolságok miatt nehézkes orvosi ellátással rendelkező régiókban a távgyógyításban jó lehetőségeket rejthet ez a technológia, de az adminisztrációs előnyök mindenhol érzékelhetők. Minden eddiginél kényelmesebben, személyre szabottabban és szorosabban követhető a beteg. Az egy helyen tárolt, bármikor, bárhonnan elérhető, akár valós idejű adatok lehetővé teszik az egyes betegek történetének gyorsabb megismerését, mely elősegíti a gyors és pontosabb döntéshozatalt, több szakorvos jobb együttműködését, mely holisztikusabb kezelést tesz lehetővé, de akár a könnyebb helyettesítést is orvosok között. Az okos eszközök által lehetővé tett folyamatos monitorozásból származó adatok lehetőséget adnak egyrész a beteg számára saját értékei megfigyeléséhez, tudatos befolyásolásához, valamint az ápolói számára egy bizonyítékokon alapuló ellátásra (amely nem csak a beteg megérzéseire, beszámolóira támaszkodik). Ez személyre szabottabbá, jobb minőségűvé, jobban szervezetté és fenntarthatóvá is teheti az ellátást. Segíthet abban is, hogy kiszűrje az esetleges fölösleges látogatásokat az orvosnál, ha előzetesen az adatok alapján azt az egészségügyi személyzet úgy látja, ezzel is csökkentve a terheltséget. A betegeknek is lehetősége nyílik a felelősségvállalásra és szerepvállalásra a saját ellátásukban, például maguk megfigyelésével, a mérésekkel, diéta vagy egyéb célok betartásával, ami amúgy a tudatosságuk növeléséhez is hozzájárul. Érvényesül még ezen kívül a mobil technológia legnagyobb előnye is, a kényelem. Távolról is sok mérés elvégezhető, ajánlások tehetők, sok szolgáltatás egy kattintással elérhető. A receptírás, időpontegyeztetés és megfelelő ügyelet, gyógyszertár megtalálása is könnyebb feladat így, melyet hazánkban már napjainkban is tapasztalhatunk [20]. Az adatosítási előnyök is érvényesülhetnek: azzal, hogy hatalmas mennyiségű adatot gyűjtünk és egyre inkább digitalizálva érhetők el ezek, lehetőség nyílhat ezek új, jobb felhasználására is. Az elérhető adatok összességéből akár új információk, felfedezések érhetők el. Kellő fenntartással kell azonban ezeket is kezelni, melyre a *Google Flu Trends* jó példa. Az internet terjedésével általánossá vált, hogy a betegek először online

néznek utána saját tüneteiknek, az ott található információ alapján igyekeznek meghatározni az orvosi ellátás szükségességét, a lehetséges gyógymódokat. A Google úgy vélte [22], hogy az egyes kulcsszavakra való keresésekből is kiderülhet az influenzajárvány kialakulása előbb, mint a megbetegedésekről szóló adatokból, ez azonban végül nem eredményezett használható, a valóságnak megfelelő előrejelzéseket a kezdeti pozitív kilátások ellenére, így a projekt le is állt. Szintén a betegek online támogatására és az abból való adatnyerésre példa a *Patientslikeme.com* (szabadon fordítva „hozzám hasonló betegek"), ahol a hasonló betegségben szenvedők megoszthatják egymással a tapasztalataikat, állapotuk és gyógyszeres kezelésük alakulását. Az itt feltöltött adatokat anonimizálva végül kutatóknak továbbítják, akik ezekből igyekeznek új tudásra szert tenni a betegek tapasztalatai alapján.

A mobil egészség applikációk segíthetnek az egészségügy problémáinak enyhítésében is. A korlátozott pénzügyi és egyéb erőforrások, az öregedő társadalom és az egészségtelen életmód mind növelik az egészségügy terheltségét. A mobil egészség applikációk segíthetnek az egészségtudatosság népszerűsítésében, motiválhatják a megfelelő pozitív viselkedést, tehát a prevencióban szerepük lehet. A fejlett országokban tehát segíthet a költségcsökkentésben, személyre szabásban és minőségjavításban, fejletlen országokban, régiókban pedig segíthet, hogy az egészségügyi szolgáltatás elérhetővé váljon. Fontos azonban ezek mellett megjegyezni, hogy a mobil egészség nem helyettesíti, inkább csak kiegészíti a személyes ellátást. Azonban ezen előnyök érvényesítéséhez szükséges lehet az ellátásban megszokott gyakorlatok átgondolására, megváltoztatására több szempontból is. Első sorban fontos, hogy az ellátást biztosító személyzet ismerje a technológia által nyújtott lehetőségeket. Arra is gondolni kell, hogy a meglévő rendszerekbe hogyan integrálhatók ezek az adatok, információk, ami már egy nagyobb erőforrásigényű kérdés. Bár időtakarékos, a mobil alapú ellátásra is kellene valamennyi időt szánni, amely a jelenlegi leterheltség mellett nehezen képzelhető el, hiszen a személyes ellátás egyértelműen prioritást élvez. Ez anyagi elszámolási kérdéseket is von maga után, jelenleg ugyanis egyes nemzeti jogszabályok továbbra is előírják, hogy orvosi tevékenység csak a beteg és az orvos fizikai jelenlétével végezhető el, megakadályozva az megészség megoldások megtérítését. Felmerülhetnek olyan kérdések is, hogy ha például egy applikáció fizetős, azt a TB téríti-e, stb. Fontos problémakör még a felelősség kérdése is: ha komolyabb egészségügyi szolgáltatásokra veszünk igénybe mobil megoldásokat és a betegnek ebből baja származik, az több okból is történhet. Előfordulhatnak nem valóságnak megfelelő adatok, például a mérőeszköz meghibásodása miatt, rossz diagnózis a rossz adatok miatt, esetleg az applikációban rejlő hiba miatt, vagy a beteg eleve rosszul végzett mérései miatt. Ez

alapján jól látható, hogy a nem csak megelőzésre, életmódra koncentráló applikációknál kifejezetten komoly veszélyek is rejlenek a jó lehetőségek mellett. Utolsó kockázatként kiemelném a sztenderdek hiányát is. Számtalan applikáció érhető el ezen a területen, melyek fejlesztésénél sok esetben nem világos, átlátható, hogy milyen szakmai szempontokat vettek figyelembe. Sokszínűségük pedig az egészségügyi dolgozók általi hasznosítást is megnehezíti [20]. Ezt az egészségügyi hatóságok bevonásával fejlesztett és jóváhagyott applikációk bevezetése és a használatukról szóló megállapodás segítheti. A definícióknál említett adatmegosztással kapcsolatos adatvédelmi és biztonsági kérdésekre a későbbiekben még hosszabban kitérek.

Az megészség applikációk leginkább ismert csoportja a hobbi célú, megelőzésre irányuló appok, melyek az egészséges életmód kialakításában és a jó szokások fenntartásában segítenek, nem csak a kialakult betegségek kezelésében. Ezen appok az élet több területén képesek adatokat gyűjteni, szokásokat alakítani, monitorozni, emlékeztetőket, összefoglalókat küldeni, információt biztosítani. Jellemző rájuk, hogy sokszor a közösség erejét is használják: vagy közösségi médiára oszthatóak az elért eredmények vagy az egyes appokon belül létrehozhatók közösségek, melyek tagjai egymást motiválhatják, láthatják egymás eredményeit, közös kihívásokat (*challenge*) hozhatnak létre. Itt is jellemző tehát a *social web* korában megfigyelhető, angolul *prosuming*-nak nevezett jelenség, amely a *produce*, előállítani és *consume*, fogyasztani szavakból áll, utalva arra, hogy a felhasználók egyszerre előállítói és fogyasztói az elérhető tartalmaknak [23]. Az applikációs boltokban böngészve az életmód és fitnesz kategóriában is számos appot találhatunk. Az alábbiakban a teljesség igénye nélkül az ilyen applikációval támogatható területeket sorolom fel. Léteznek diéta és testsúly témájú, edzést segítő és követő, vízivást segítő, dohányzásról való leszokást segítő, alvást segítő és követő, női egészséggel kapcsolatos, valamint hangulatkövető applikációk. A megalapozó kutatások során ezen alkalmazásokról szakirodalmi összefoglalókat is készítettem [24]. Bár egyre több applikáció érhető el magyar nyelven is, általánosan megfigyelhető, hogy az appok nyelve leginkább az angol. Az is szembetűnő, hogy bár a fent említett applikációk, és általában a legtöbb app ingyenesen tölthető le, majdnem mindegyiknél elérhetők fizetős prémium funkciók. Az applikációk legtöbbjénél a szép tervezés, külső és könnyen átlátható adatvizualizáció figyelhető meg, mely megkönnyíti a használatot. Érdemes megemlíteni a fenti appokon túl az okostelefonokon gyártónként elérhető egészségnek dedikált egészség (*Fitness, Health*) gyűjtőappokat is, melyek sok fenti app kategóriát helyettesíthetnek, rendszerezhetnek, egészíthetnek ki. Az Apple készülékekben elérhető Health app-ban például a következő

kategóriák érhetők el: aktivitás, adatok, menstruációs ciklus követés, szív (pulzus, EKG), mentális egészség, mobilitás, táplálkozás, légzés, alvás, tünetek, egyéb. Jól látható tehát, hogy az összes funkció használatával, esetleg más appok adatainak integrálásával átfogó, részletes információhoz, kimutatásokhoz juthatunk hozzá, melyeket az egészségünk követésére, megőrzésére használhatunk, valamint orvosaink rendelkezésére is bocsáthatjuk. Ezt még kiegészítheti az Apple Watch használatával gyűjtött adatok sora, mely még átfogóbb képet adhat a felhasználónak egészségügyi állapotáról.

1.2. Befolyásoló technológia

Vajon befolyásolhatják-e, megváltoztathatják-e valóban a felhasználók viselkedési szokásait ezek az applikációk? Ennek sikerességét támogatja a meggyőző, vagy befolyásoló technológia (*persuasive technology*), ami bármilyen interaktív technológia, melynek célja a felhasználók attitűdjeinek vagy viselkedésének megváltoztatása [25, p. 1]. Az interakció kulcsfontosságú, hiszen a felhasználó visszajelzései, szükségei, helyzete szerint alakítható a folyamat. A technológia és internet fejlődésével egyre több példájával találkozhatunk. Ebbe a kategóriába tartozik például egy épp elhajtó autók sebességét mérő tábla, amely a visszajelzéssel, villogással és színekkel igyekszik a vezetőt lassabb tempóra bírni, de akár az online vásárlás során feltűnő, kifejezetten a vásárlónak szóló ajánlatok is, melyeket az online bolt az előző tranzakciók és böngészések preferenciái alapján állít össze, ösztönözve a vevőt a további terméket vásárlására. Az interakciók segítségével, például egy fent említett dohányzásról való leszokást segítő applikáció a rendelkezésre álló statisztikák, valamint a felhasználó saját, addigi betáplált adataiból, az eddig elszívott szálak mennyiségéből, a visszaesésből, sikeres napok számából stb., meg tudja határozni, hogy mikor milyen beavatkozás szükséges a felhasználó motiválásához, alternatív cselekvések ösztönzéséhez, dicsérethez. Ahhoz az esethez képest, hogy egy ember próbálná meg a leszokásról meggyőzni a társát, egy gépnek van néhány előnye is: sokkal kitartóbb, mint embertársai, így akkor is mer szólni, amikor azok már feladták volna a próbálkozást. Az anonimitást is lehetővé teszi, ezért a felhasználók sokkal könnyebben és lehetséges, hogy őszintébben is vallanak nekik például az egészségükkel, vagy az elszívott szálak mennyiségével kapcsolatban. A gépek képesek sokkal több adatot is tárolni és kezelni, mint az emberek, így esetenként azokat használva még inkább meggyőzőek lehetnek, valamint bevethetnek többféle befolyásolásra alkalmas eszközt, nem csak a tényeket, de akár vizualizációt, videókat, képeket, szimulációkat, stb. is. Ezen kívül a technológiai sajátosságokból adódóan nagyobb mennyiségben és a világ bármelyik pontján egy eszköz segítségével elérhetők, ami lehetővé teszi akár nagy tömegek segítését is egy időben.

B. J. Fogg szerint [25] ahhoz, hogy a befolyásolás módjait megértsük, először a számítástechnika három lehetséges szerepét kell megértenünk: eszköz, média és társadalmi szereplő. Eszközként funkcionálva a gépek számos módon befolyásolhatják az embereket: megkönnyíthetik a célmagatartás végrehajtását, a felhasználókat egy folyamaton keresztül vezethetik, számításokat vagy méréseket végezhetnek, amelyek motiválják. Szenzoros médiumként funkcionálva az embereket azáltal győzheti meg, hogy szimulációkkal teremti meg az interakció lehetőségét és jó élményeket, környezetet nyújt a szituáció átlátására és megoldására. Amikor szociális, társadalmi szerepet töltenek be, akkor az ember társas kapcsolataira igyekszik hatni: meggyőzik a felhasználókat ugyanazokkal az elvekkel, amelyeket az emberek mások befolyásolására használnak, például pozitív visszajelzésekkel jutalmazva őket, vagy társas támogatást nyújtva. Fogg [25] az alábbi hét meggyőző technológiai eszköztípust azonosította. Redukció (*reduction*): úgy segít, hogy az összetett tevékenységet, ami a cél eléréséhez szükséges, egyszerűbb, kisebb számú lépésre bontja le. Így csökkenthető a kognitív terhelés és könnyebben elérhetőnek tűnik a cél. Támogatja azt is, hogy a mai felgyorsult világban, ahol a figyelem és összpontosítás csak rövid időn keresztül érhető el, gyorsabban menjen át az üzenet a felhasználónak, így növelve az elkötelezettséget és a kitartást. *Tunneling*: (kb. alagút módszer) célja, hogy a felhasználót következetesen végig vezesse a folyamaton irányított útmutatással. Lépésről lépésre igyekszik megmutatni a helyes viselkedést. Jó példa lehet erre, ha egy futást segítő applikáció az elérni kívánt hosszabb távot lebontja kisebb, könnyebben teljesíthető mennyiségekre, így a felhasználónak lehetősége van a fokozatos fejlődésre, a hosszútáv elérésére. Személyre szabás (*tailoring*): napjainkban egyre inkább jellemző, célja, hogy segítsen kiszűrni a felhasználó számára releváns információt a nagy halmazból. Ezen kívül növelheti a felhasználó kötődését is az apphoz. Javaslat (*suggestion*): ha az applikáció jókor, jól célzott javaslatokat tesz a meglévő preferenciák és célok alapján, nagy valószínűséggel megfogadja azokat a felhasználó. Előfordulhat például, hogy egy mozgást követő applikációnak táplálkozással kapcsolatos „testvér” alkalmazása is van. Ha az egyiket használja a felhasználó, érdemes lehet ajánlani neki a másikat is, hiszen az egészségtudatosságát, esetleg céljait is ismerjük már az első használatnál megadott válaszai alapján, amiből következtethetünk az ajánlás sikerességére. Önellenőrzés (*self monitoring*): valós idejű adatokat szolgáltat a felhasználónak saját magáról, ezzel befolyásolva viselkedését. Ezt támogathatja még a vizualizáció és gamifikáció is, segítve a kívánt viselkedés elérését. Megfigyelés (*surveillance*): míg az önellenőrzési stratégia a felhasználó fókuszát saját magára irányítja, a megfigyelési stratégia a fókuszt a többi felhasználóra helyezi, kihasználva az

emberekben természetesen jelenlevő versenyszellemet. Kondicionálás (*conditioning*): egyszerű stratégia, mely a kívánt magatartást erősíti meg valamilyen jutalommal.

Ugyanakkor Fogg azt is kiemeli, hogy ezek az eszközök csak akkor működhetnek, ha a felhasználó eleve motivált a viselkedése megváltoztatásában, valamint ha ezek a feladatok minél könnyebben elvégezhetők. Ebben az esetben a jól időzített, személyre szabott kis lökések pozitív befolyásúak lehetnek, hatásosak lehetnek a céljai elérése során.

A fenti felsorolást Oinas-Kukkonen és Harjumaa szerzőpáros elsődleges feladattámogató módszereknek (*primary task support*) nevezi, annyi különbséggel, hogy a javaslatokat az azokkal kapcsolatos elvárások miatt (legyen hasznos) inkább egy másik kategóriába helyezi. (A megfigyelést és kondicionálást az ő csoportosításuk elveti és helyette két másik módot, a szimulációt (lehetőséget adnak a várható eredmények jobb elképzelésére, ok-okozat megértésére) és a próbát (amikor lehetőség nyílik a kívánt cél gyakorlására, kipróbálására) említik.) Ezen kívül még három csoportot hoztak létre gyakorlati szempontból, követve Fogg gondolatmenetét is, amelyek alkalmasak a technológia segítségével történő befolyásolásra: a dialógus támogatást (*dialogue support*), a rendszer hitelesség támogatást (*system credibility support*) és a szociális támogatást (*social support*) [26].

Összességében tehát megfigyelhető, hogy az ember-ember kapcsolatban hatásos befolyásoló eszközök technológiával való támogatása segít ezen applikációk sikerességét is elérni. Mobil eszközökön ez annak sajátosságaiból adódóan is könnyebb: például azzal, hogy internetkapcsolattal rendelkezik, a felhasználók összekötésével közösség hozható létre. Azzal, hogy folyton a felhasználónál van az eszköz, lehetőség nyílik a folyamatos mérésre, visszajelzésre és motiválásra is. A képernyők fejlődésével az egyre szebb felület kialakítására is jobb lehetőségek nyílnak. Azonban a lehetőségek mellett itt is érdemes megfontolni a kockázatokat, lehetséges veszélyeket. Fontos, hogy etikus, jó szándékkal járjanak el a készítők az alkalmazások ilyen szemléletű kialakításakor, ugyanakkor szakértőket kell igénybe venni ahhoz, hogy a szakmai szempontok szerint helyesnek, egészségesnek vélt viselkedések rögzülését segítse a felhasználókban.

1.3. Megészség appok- COVID-19 és hozzá kapcsolódó applikációk

Az egészséggel kapcsolatos applikációk másik nagy csoportja a komolyabb témájú, egészségügyet támogató applikációk. Ezek funkciói többek között a diagnosztikai és kezelési támogatás, a távoli adatgyűjtés a betegekről, a távfelügyelet, a krónikus betegségek kezelése, a telemedicina, a betegségek és járványok követése, támogatása, a betegek oktatása,

tudatosságuk növelése, az egészségügyi dolgozók kommunikációja és képzése, valamint az egészségügyi ellátási lánc menedzsment. A fentiekhez hasonlóan ezek az appok is alkalmasak értesítések küldésére, motivációra, a pozitív viselkedés megerősítésére, gyűjthetnek adatokat is a jobb és pontosabb döntések érdekében, használhatnak vizualizációt stb. Jelen fejezet a COVID-19 világjárvány idején készült, így kézenfekvő és aktuális a járvánnyal kapcsolatos applikációk említése is.

A 2019 végén megjelent súlyos akut légúti tünetegyüttest okozó koronavírus 2 (SARS-CoV2), valamint az általa okozott megbetegedés, a koronavírus-betegség 2019, rövidítve a COVID-19 [27, p. 1], melyet az Egészségügyi Világszervezet (WHO) 2020 márciusában világjárvánnyá nyilvánított [28], jelentős változásokat hozott a mindennapokba. Viszont a tömeges megbetegedések lassítására, kontrollálására, visszaszorítására, követésére, a karanténban lévők felügyeletére, a népesség informálására, akár az otthoni munkavégzésre, tanulásra és az otthon töltött idő élvezetesebb eltöltésére is segítséget jelenthetnek a mobil és digitális kor megoldásai a korábbi járványokhoz képest. Természetesen ez önmagában nem újdonság, de minden eddigi járványhoz képest most a legfejlettebb a technológia, most kapcsolódnak a legtöbben a digitális világhoz, ami elősegítheti a sikereket. 2020 első felének egyik legnépszerűbb témája az érintkezéskövetés technológiával való támogatásának kérdése volt. Amíg a járvány a kezdeti szakaszban volt, a már megerősítetten COVID-19 fertőzött betegeknél a hagyományosan bevált, manuális érintkezéskövetést alkalmazták. Ez gyakorlatilag azt jelenti, hogy az igazolt beteget kikérdezik, hogy az elmúlt időszakban (kb. 7-10 nap), kivel töltött el több időt, kivel érintkezett közelről, mivel ezeknek az embereknek nagyobb az esélye, hogy elkapták tőle a vírust. Miután azonosították a kitett kontaktokat, azon személyeket is szorosan figyelemmel kell kísérni, esetleg karanténra ítélni [29]. Ez a folyamat viszonylag kis esetszámnál is idő- és erőforrásigényes, valamint az emlékezetre támaszkodik, ami nem mindig megbízható. Ezen kívül problémás még, hogy csak azokat az érintkezéseket tudja követni, amelyeknél a két érintkező ismeri egymást, ami nem mindig fedi a valóságot (például hosszabb eladó-vevő kontaktus). A járvány felgyorsulásával azonban érdemes megfontolni a technológia alkalmazását is, hogy nagyobb mennyiségű embernél hatékonyan lehessen ugyanezt a feladatot ellátni. E célra jöttek létre az érintkezéskövető, vagyis *contact tracing* applikációk is. Ezek pedig nem csak a terjedés megfékezésben, a járvány lassításban segíthetnek, ami az egészségügyi ellátás folyamatosságát, leterheltségének elosztását tudja biztosítani, hanem hozzájárulhatnak a terjedés módjának jobb megértéséhez is. A globális és lokális szinten a járványt érintő döntéshozatalban is támogatást nyújthat az ilyen módon begyűjtött adatok

elemzése [30]. Fontos azonban megemlíteni, hogy az applikációkkal segített érintkezéskövetéshez szükséges mobil eszközök a társadalom egy része számára nem érhetők el, így például a gyermekek, idősek, hátrányos helyzetűek, esetleg néhány típusú fogyatékossággal élő számára ezek továbbra sem jelentenek megoldást. Kérdéses az elfogadottság adatvédelmi és biztonsági szempontok miatt is, ami problémát jelenthet, mert egy Oxford University által végzett kutatás [31] szerint a hatékonyság érdekében a népesség 60-75%-ának kellene használnia az érintkezéskövető applikációkat.

Az alapkoncepció az érintkezéskövető applikációknál az, hogy általában Bluetooth segítségével követi az app a közeli, hosszabb ideig tartó érintkezéseket a felhasználók között, jegyzi azokat, majd egy felhasználó fertőződésének beigazolódása esetén értesíti az elmúlt időszakban vele érintkezett felhasználókat, akik ezután figyelemmel kísérhetik saját állapotukat, esetleg teszteltethetik magukat, tájékozódhatnak a betegségről, valamit gátolhatják a továbbfertőzést karanténban maradással [32]. A COVID-19 járvány során először Szingapúrban jelent meg ilyen app TraceTogether néven [33], mely tokencserével működik Bluetooth segítségével közeli telefonok között. A tokenek időben változó véletlen karakterláncok, a felhasználóhoz társítva. Megbetegedés esetén az egészségügy képviselői lekérdezik az appban tárolt adatokat, például a tokeneket, amiket a többi telefonról gyűjtött, így értesítik az érintetteket. Mivel a kormány vezeti az adatbázist, amely a tokeneket telefonszámokhoz és felhasználókhoz köti, így a felhasználóknak nem kell egymás előtt felfedni magukat [32]. Ennek a magyar megfelelője a Vírus radar, amely szintén mobil eszközök titkosított, anononimizált adataival, távolságméréssel (Bluetooth segítségével) igyekszik felfedni a bizonyítottan fertőzött emberek kapcsolatait. A felhasználó megfertőződése esetén értesítheti a járványügyi szakembereket, akik az adatmegosztás után értesíthetik az érintett kontaktokat. A tájékoztató szerint a felhasználónak csak a mobilszámát tárolja az állam, melyhez véletlenszerű kódot kapcsolva biztosítják az anonimitást [34].

Egy másik lehetőség a házi karantén felügyelet mobil eszközökkel való támogatása is. Erre példa lehet a Házi Karantén Rendszer applikáció, amely a regisztrált és jóváhagyott, hatóságilag karantén alá vetett felhasználókat ellenőrzi, hogy betartják-e az előírt karantént. A rendszer véletlenszerű időpontokban távellenőrzési kérdéseket küld a felhasználóknak, akiknek 15 perc áll rendelkezésükre, hogy az appban ezt végrehajtsák. A távellenőrzéskor a felhasználónak fotót kell készíteni magáról, fontos, hogy a lokáció hozzáférés engedélyezve legyen, ugyanis ez alapján igazolható a karantén betartása. Ezután pedig lehetősége van egy egészségügyi állapotfelmérőt is kitölteni, ha szeretné. A távellenőrzés elmulasztásakor az app

automatikusan értesíti az ORFK-t, akik megteszik a szükséges lépéseket. Ha a karanténnak vége, a felhasználó e-mailt kap, törölheti az alkalmazást és 60 nap után automatikusan törlik az adatbázisból is [35].

Az egyik legfőbb, sokakat foglalkoztató kérdés az adatok tárolása és feldolgozása ezekkel a megoldásokkal kapcsolatban, amely lehetséges decentralizált vagy centralizált (backend szerver) módon. Decentralizált megoldás esetén a személyes adatok, valamint az alkalmazás által generált azonosítók a felhasználó mobilján maradnak. Ezzel a módszerrel a felhasználók az adataikat tehát maguknál tarthatják, rendelkezhetnek felőlük, és elveszik a központi, állami hozzáférés a személytelenített adatokhoz. Ez azért nem szerencsés, mert az ilyen appokon gyűjtött adatok nem csak a megfékezésben, lassításban segíthetnek, de lehetőséget adhatnak jobb minőségű, valós idejű statisztikák létrehozására, segíthetnek jobban megérteni a terjedés módját, javíthatják a járványt érintő döntéshozatalt. Főleg a jelenlegi helyzetben, amikor egy eddig ismeretlen viselkedésű vírus terjed, az ezekből az adatokból nyerhető információk rendkívül értékesek. Épp ezért az EU ajánlása szerint ezt a megoldást például önkéntes adatmegosztással lehetne kombinálni, vagyis ha a felhasználó pozitív, megadhat adatokat, amiket önkéntesen elküldhet a központi adatbázisba. A másik lehetőség a centralizált megoldás, melynél az alkalmazás az országos közegészségügyi szerv által birtokolt, kezelt háttér-kiszolgálón keresztül működik, az azonosítók tárolása, párosítása is ott történik. Az EU ajánlás természetesen itt is az, hogy a felhasználók ne legyenek azonosíthatók ezen adatok alapján, csupán az alkalmazás által generált tetszőleges azonosítók legyenek a szerveren. Ez a mód is párosítható lehet önkéntes személyes adatmegosztással. Bármelyik megoldásba integrálható további funkció, ezeken keresztül a felhasználó akár tájékoztatást, segítséget is kaphat a betegséggel kapcsolatban a hatóságoktól. Bármelyik módot is választják a tagállamok, az EU célja az ajánlások kiadásával az, hogy egy országhatárokon átívelő rendszert segítsenek létrehozni, nem csak az értékes adatbázis létrehozása miatt, hanem hogy a jövőben mihamarabb újra tudjanak indulni a tagállamok közti folyamatok, szabad áramlások (személyek, áruk, szolgáltatások és tőke). Fontos azonban, hogy ezen appok használata legyen önkéntes, az appok legyenek az adott nemzet egészségügyi szerve által elfogadottak és annak segítségével kidolgozottak (hogy a megfelelő adatokat gyűjtsék és megfelelő tájékoztatást tudják adni). Hangsúlyt kell fektetni arra is, hogy adatvédelmi szempontból és EU jogi előírásoknak megfelelően hozzák létre ezeket és csak addig maradjanak használatban amíg az feltétlenül szükséges [30].

A fentieken kívül még alkalmazhatók applikációk a betegek állapotának, gyógyulásának nyomon követesére, ha azok otthonukban esnek át a betegségen, esetleg már hazatértek a kórházból, de szükség van utókövetésre. Ezt segíthetjük például okostelefonhoz párosított okosórával is, melyek képesek lehetnek pulzusmérésre, alvás minőség mérésére, akár testhőmérséklet megfigyelésére is. Ilyenek például az USÁ-ban már elterjedt Apple Health Check applikáció, a *Siri give me guidance* (Siri adj útmutatást), ami keretében Siri tünetekkel kapcsolatos útmutatást tud adni, de Alexa is képes az idősebb lakosság kérdésekkel való napi figyelésére és szűrésére (*My Day for Seniors*). Ezeket az adatokat egészségügyi dolgozóknak is továbbíthatják [36]. Amint már említettem, ilyen applikációk alkalmasak lehetnek tájékoztatásra is, ami segíthet enyhíteni az egészségügy leterheltségét, ugyanis sok kérdés merülhet fel egy járvánnyal kapcsolatban. Az Életmentő applikációban is található már egy link, amely a hivatalos kormány által létrehozott koronavirus.gov.hu oldalra vezet, ahol a felhasználó választ találhat kérdéseire.

Egyes feltevések szerint Kína sikerét a COVID-19 járványra adott hatékony válaszában nem csak a korábbi SARS során szerzett tapasztalat segítette, hanem a már bevált, megfigyelésre kiépített és berendezkedett infrastruktúra és az ebből rendelkezésre álló hatalmas adathalmaz [33]. Az adatokban rejlő lehetőségeket már jóval korábban felismerték többek között a hatalmas technológiai óriások is, mint például a Google, a Facebook vagy az Apple. Számtalan ilyen vállalat kíván a járvány elleni harcban is részt venni, felfedve az eddig nem mindig hivatalosan elismert adatgyűjtéseket is. Az előbb említett három cég az applikációikban követi a felhasználóik mozgását, ezekről aztán anonimizálva készítettek nyilvánossá tett összefoglalókat, táblázatokat és adnak információt a zárlat alatt lévő emberek mozgásáról (Google és Apple Maps- térkép applikációk), a Facebook pedig önkéntesen kitölthető teszttel és lokáció adatokkal próbálja megbecsülni a betegek számát egy-egy helyen az USA-ban [37]. Tehát jelen helyzetben is megfigyelhető az adatosítás és a gyűjtött adatokból történő hasznos információ létrehozásának szándéka.

Összefoglalva a járvány elleni küzdelemben jó lehetőségeket adhatnak a mobil applikációk is, de amíg a használatuk nem általánosan elterjedt, nem várható tőlük igazán nagy eredmény. A már felületesen említett adatvédelmi, biztonsági kérdésekre a későbbiekben részletesen kitérek. A járvány kitörése utáni időszakban a kutatásom részeként áttekintést készítettem a COVID és a biztonságos mobilhasználat témakörében [38].

2. APPLIKÁCIÓK BIZTONSÁGÁNAK VIZSGÁLATA

Az alábbi szakaszban a mobil applikációkon történő adatmegosztás biztonsági és adatvédelmi kérdéseit vizsgálom három fő szempontból: szabályozási, alkalmazásfejlesztői és felhasználói szempontokból. A fogalmi keretek tisztázása után bemutatom a lehetséges kockázatokat, majd a következő fejezetben az említett négy fő szempont szerinti kockázatokra adható javasolt válaszokat is, különös tekintettel a felhasználói részre, hiszen jelen írás fókusza a felhasználók tudatossága és biztonsághoz való hozzáállása.

2.1. Fogalmi keretek: biztonság és adatvédelem

A kibertér a „minket körülvevő elektronikus világ, amely a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese” [39, p. 242]. Ahhoz, hogy a kibertér továbbra is működhessen és fejlődhessen, szükséges a bizalom megtartása, melyet az azt alkotó elemek, mint az információs rendszerek és az azokban tárolt, kezelt és továbbított adatok, információk biztonságának növelésével lehet elérni. A kiberbiztonság ezzel összhangban politikai, jogi, gazdasági, valamint tudatosságnövelő, oktatási eszközökkel igyekszik a kibertér kockázatait elfogadható szintre csökkenteni. Ennek egy eszköze az elektronikus hálózati és információs rendszerek biztonsága, melyet tágan és szűken is értelmezhetünk. Tágan értelmezve ez „az adatok, információk kezelésére használt eszközök (hardver, hálózat), eljárások (szoftver, folyamatok), személyek együttesét fedi le, szűkebb értelemben csak az elektronikus hírközlő hálózatokat, az adatok kezelését végző eszközöket és az ezeken továbbított adatokat jelenti” [39, p. 242]. A digitális adatok tekintetében „az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos” [40, p. 145].

Az informatikai rendszerekkel és általában az adatokkal kapcsolatos biztonsági (*security*) követelmények a bizalmasság (*confidentiality*), sértetlenség (*integrity*) és a rendelkezésre állás (*availability*). A bizalmasság az az elvárás, hogy az adatokat csak az arra jogosultak, a jogosultság mértékéig használhatják, férhetnek hozzá, tehát az adatvédelmi elvárásoknak megfelelően kezelhetik azokat. Akkor sérül, ha illetéktelenek férnek hozzá az adatokhoz, akiknek nem lett volna erre joga. A sértetlenség jelentése, hogy az adat (tartalma és

tulajdonságai) nem változik meg, esetleg az arra jogosultak változtatják tervezett módon. Ebbe a kategóriába tartozik a hitelesség és a letagadhatatlanság kritériuma is. Előbbi az adat tartalmára és forrására, utóbbi a származását, az azt ért folyamatok ellenőrizhetőségét jelenti. A sértetlenség tehát például akkor nem érvényesül, ha az adatok nem valósak, esetleg jogosulatlanul módosítják, akár megsemmisítik őket. (A sértetlenség elve nem csak adatokra, információkra, de rendszerekre és szervezetekre is érbényes.) A rendelkezésre állás pedig az a tulajdonság, mely szerint az adatok, információk elérhetőek, az arra jogosultak azokat használhatják. Ez akkor sérülhet, ha az adatok, hozzá kapcsolódó szolgáltatások részlegesen vagy teljes mértékben nem használhatók, nem érhetők el [41]. E három tényezőre a CIA-triádként is hivatkoznak az angol kulcsszavak első betűinek összevonásával.

Tágabban értelmezve a „biztonság egyrészt a veszély és fenyegetések hiányát, másrészt a veszély és a fenyegetések elhárításának képességét jelenti" [42], azonban mivel ez soha nem tökéletesen elérhető állapot, inkább tekinthető percepcionális kérdésnek, „vagyis azt, hogy az egyén és közösség mit gondol a biztonságról, az objektív biztonság (biztonsági helyzet) és a szubjektív biztonság (biztonságérzet, percepció) együttesen határozza meg, s koránt sem biztos, hogy ez a két megközelítés mindig egybeesik" [42]. A biztonságtudatosság definiálása azonban már nehezebbnek bizonyul, ugyanis nem elérhető egységes, széles körben használt definíció. A tudatosság fogalmából kiindulva megalkotható a biztonságtudatosság fogalma is. Az ISACA (Information Systems Audit and Control Association) fogalommeghatározása nyomán ennek jelentése Tarjáni fordításában „értesültnek lenni, figyelembe venni, tudatosnak és jól informáltnak lenni egy olyan szakmai tárgykörben, mely magába foglalja az adott témakör tudását és megértését és az annak megfelelő cselekvést" [43]. Tehát a biztonságtudatosság a biztonságot, esetünkben biztonságos alkalmazáshasználatot érintő tudást, informáltságot jelenti. A következőkben a reprezentatív kutatás során megjelenő fogalom lesz még a biztonságérzet fogalma, mely „valakinek azzal a tudattal járó érzése, hogy biztonságban van" [44].

Az adatbiztonság „az informatikai rendszerekben az adatok kezelésének megfelelő minőségét jellemző állapot", vagyis „az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere". Máshogy fogalmazva „az informatikai rendszerekben az adatok kezelésének megfelelő minőségét jellemző állapot" [45, p. 25]. Az Információbiztonsági törvény [2013. évi L. törvény 1. § (1) bekezdés 26. pont] szerint a kiberbiztonság nem más, mint „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint

technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez" [46].

A következő fejezetben a mobil alkalmazásokkal kapcsolatos veszélyeket ismertetem, melyhez szükséges még néhány kapcsolódó fogalom tisztázása. A 2013. évi L. Törvény szerint a fenyegetés „olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát". A sérülékenység pedig „az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat." A kockázat pedig a fenyegetettség mértékét mutatja meg [47].

A fenti fogalmak kapcsán fontos még megemlíteni a letagadhatatlanságot (*non-repudiation*), mely jogi fogalom, és az az elleni védekezést jelenti, hogy az egyén hamisan tagadhassa egy adott cselekvés végrehajtását. Lehetővé teszi annak meghatározását, hogy egy adott személy végrehajtott-e egy bizonyos műveletet, például információt hozott létre, jóváhagyott valamit, vagy üzenetet küldött vagy kapott. Az e-kereskedelem és az elektronikus tranzakciók mai világában lehetőség nyílik mások személyi adataival való visszaélésre vagy egy cselekvés megtagadására, például az online vásárlásra, majd annak későbbi megtagadására. Fontos, hogy minden résztvevő bízzon az online tranzakciókban. A letagadhatatlan módszerek biztosítják, hogy az emberek felelősek legyenek az általuk lebonyolított tranzakciókért [48].

Ahogy arra többek között Shoshana Zuboff is felhívta a figyelmet a The Age of Surveillance capitalism című könyvében [49], napjainkban sok vállalat a felhasználókat megfigyelve, adataikat megszerezve, felhasználva, azokat értékesítve boldogul. Így gyakori témává vált manapság a biztonságon felül a magánélet, személyes adatok védelme is (*privacy*). Ez azt a jogot is jelenti, hogy az adat, információ tulajdonosa (vagyis akiről szól) dönthet róla, hogy ki és hogyan használhatja fel, adhatja tovább azokat, amik beazonosíthatóan róla szólnak [50]. Ez az elvárás különösen jogosnak tűnik az egészségügyi adatokkal szemben, amik magasabb szintű biztonságot kellene, hogy élvezzenek.

Azonban felmerülhet a kérdés, miért is fontos mindez, ha nincs az embernek rejtegetnivalója. 1967-ben Alan Westin írta könyvében, a Privacy and Freedom-ban [51], hogy az adatvédelemnek négy fő funkciója van: személyes autonómia, érzelmi ki-/elengedés, önmagunk értékelése és az intim kommunikáció lehetősége. Daniel J. Solove professzor pedig

a következő funkciókat azonosította [52]: korlátozza a kormány és nagyvállalatok hatalmát, tiszteletben tartja az egyéneket, lehetővé teszi az embereknek, hogy ők alakítsák a hírnevüket, fenntartja a megfelelő társadalmi határokat, bizalmat épít, erősít, irányítási, kontroll lehetőséget ad az egyénnek, biztosítja a gondolati és szólásszabadságot, biztosítja az egyéni szabadságot a társadalmi és politikai tevékenységekhez is, szükség esetén változtatásra, második esélyre is lehetőséget ad, valamint azt is jelenti, hogy nem kell magyarázkodnunk, tetteinket igazolni másoknak.

A megjelenő, fentebb ismertetett mobil egészség applikációk, és az azokkal járó tömeges megfigyelés elterjedése ezt az amúgy nem új kérdéskört, főleg a COVID-19 témájú appok kapcsán ismét nagyon népszerűvé tette. Érdemes figyelembe venni, hogy a személyes adatokhoz való jog egyszeri feladása után igen nehéz ezt az állapotot visszafordítani (bár a törvények már előírják az adatok törlését, ha már nem szükségesek), így a vészhelyzetnek sem szabad elég indoknak lenni a jogok figyelmen kívül hagyására. Ezt a jelenséget nevezhetjük *surveillance creep*-nek [53], vagyis a felügyelet lassú elterjedésének és állandósulásának, amely a lehetséges igazságtalanságokon túl pszichológiai hatással is lehet a népességre, előidézheti az ellenőrzöttség érzését, csökkentheti az egyéni autonómiát és a motivációra és jólétre is negatív hatással lehet. Érdekes kérdés marad tehát az is, hogy ha a veszély elmúlik, használatban maradhatnak-e az akkor bevezetett követési, ellenőrzési módszerek. Véleményem szerint ezt végül a társadalmi állásfoglalás döntheti el, egyes országokban ezek a jogok fontosabbak, mint máshol. Az viszont biztosnak látszik, hogy érdemes ilyen rendszereket anonimizálva elérhetően tartani, hiszen a jogok betartásával ezek a megoldások értékes lehetőségeket tartogatnak megelőzésre, gyors reakcióra, döntéshozatalra és a jövőbeli trendek megértésére is.

A fogalomhoz kapcsolódik még az adatvédelmi vagy magánéletvédelmi paradoxonként (*privacy paradox*) ismert az a jelenség [12], mely során a felhasználók hajlamosak a magánéletet veszélyeztető online magatartásra, ami végül kettősséget eredményez a magánélethez való hozzáállás és a viselkedés között. Egy bizonyos fokú kockázatérzékelés a magánélet védelmével kapcsolatos stratégiák nagyobb ismeretét vonja maga után, de úgy tűnik, ez nem elegendő motiváció az ilyen stratégiák alkalmazásához. Így, bár sok felhasználó elméleti érdeklődést mutat magánélete védelme iránt, és fenntartja a pozitív hozzáállást a magánélet védelmét szolgáló magatartáshoz, ez ritkán fordul tényleges védelmező magatartásba. Bár a felhasználók tisztában vannak az interneten fellépő adatvédelmi

kockázatokkal, hajlamosak privát információkat megosztani kiskereskedelmi értékekért és személyre szabott szolgáltatásokért cserébe.

2.2. Mobil alkalmazásokra vonatkozó fenyegetések

A mobil appokkal kapcsolatos veszélyek számbavétele nehéz feladat, ugyanis naponta ismerhetünk meg új fenyegetéseket és sérülékenységeket. Az ellenük való védekezéshez azonban elengedhetetlen ezek ismerete. Ennek egy átlátható és kedvelt módja a különböző *threat intel* szolgáltatások, éves, havi toplisták és ilyen területtel foglalkozó hírportálok, közösségi média követése. Toplistákat és jelentéseket sok szervezet ad ki, elérhető például alkalmazáskészítőknek az OWASP (the Open Web Application Security Project) ajánlása, de jó példa erre az ENISA (European Union Agency for Network and Information Security) évente megjelenő Threat Landscape Report című kiadványa is (Jelentés a fenyegetésekről). Ezen kívül a különböző biztonsági szolgáltatók is (például Cisco, Palo Alto, stb.) is adnak ki hasonló jelentéseket, összefoglalókat. Hasznos lehet még, főleg alkalmazás fejlesztői (és támogatói) szempontból a MITRE ATT&CK keretrendszer, amely egy olyan tudásbázis, ami leírja a támadók taktikáit és technikáit, amelyeket a támadás teljes életciklusa során használnak. A keretrendszer a szervezet biztonsági helyzetének megerősítésére szolgál és megoldási javaslatokat is kínál az egyes támadásokra. Az ATT&CK for Mobile Android és iOS operációs rendszerekben előforduló támadásokra koncentrál.

A mobil alkalmazásokat érintő veszélyeket a már említett nehézségek ellenére az alábbi csoportok szerint ismertetem, bár fontos megjegyezni, hogy sok más lehetséges csoportosítás is létezik.

- Alkalmazással kapcsolatos fenyegetések,
- Web-alapú fenyegetések,
- Vezeték nélküli hálózati fenyegetések,
- Hozzáféréssel kapcsolatos fenyegetések.

Gyakoriak az olyan fenyegetések, melyek több kategóriába is tartozhatnak egyszerre. A fejezet során főleg a felhasználói szempont érvényesül. Végül a mobil egészség applikációk és a koronavírusra vonatkozó egyéb kockázatokat is említem, mert bár kicsit eltérő kategória, mint az eddig felsoroltak, ugyanúgy fontos részei a teljes képnek.

2.2.1. Alkalmazással kapcsolatos fenyegetések

Az alkalmazással kapcsolatos fenyegetések értelemszerűen azok a fenyegetések, melyek az alkalmazásokkal kapcsolatosak. Az alkalmazások gyakran a mobileszközök sebezhetőségének gyökerei. Ebbe a kategóriába az alábbi főbb forrásokat sorolhatjuk [54].

- Fertőzött applikációk [55]: bár mindenképpen a legbiztonságosabb applikáció beszerzési forrásoknak tekinthetők, előfordulhat, hogy a nagy alkalmazásáruházakból (mint a Google Play, vagy Apple App Store) letöltött appok fertőzöttek. A Google terminológiáját használva ezek összefoglalva a potenciálisan ártalmas alkalmazások (*Potentially harmful applications*-PHA), melyek veszélyeztethetik a felhasználókat, a felhasználói adatokat vagy az eszközöket. Ezeket az alkalmazásokat általában rosszindulatú programnak, malware-nek nevezik. (Azért potenciális, mert bár bizonyos típusokon- ahol például nem a legújabb operációs rendszer van telepítve- biztosan problémát okoz, sok eszközre ártalmatlan lehet.)
- Sideloaded applikációk: a sideloading helyi file átvitelt jelent két eszköz között (wifi, bluetooth, esetleg memóriakártya segítségével). Androidnál ez általában egy alkalmazáscsomag APK formátumú telepítését jelenti egy Android-eszközre [56]. Ezeket a csomagokat általában nem a Google Play-ről, hanem számítógépren keresztül egyéb weboldalakról töltik le, csak akkor telepíthetők, ha az „ismeretlen források” használata engedélyezve van a biztonsági beállításoknál. IOS-nél pedig IPA formátumú file telepítését jelenti az Apple eszközre, szintén nem az Apple Store-on keresztül. Az iOS modern (nem jailbrake-elt) verzióinál az alkalmazások forrásait mind az Apple-nek, mind a felhasználónak megbízhatónak kell találnia [57]. Összefoglalva tehát a nem megfelelő, nem ellenőrzött forrásból való, nem jóváhagyott applikációk is hordozhatnak magukban veszélyt.
- Zero day application malware: ebbe a kategóriába tartoznak a nulladik napi támadások, amelyek olyan sebezhetőséget használnak ki, ami még nem került nyilvánosságra, nem ismert, így nincs arra irányuló biztonsági intézkedés. A zero day bármelyik későbbi kategóriára is jellemző lehet.

A fent felsoroltaknál az applikációkon keresztül érkezik tehát a fenyegetés, amely változatos formát ölthet. A legfontosabb gyűjtőkategória ezek közül a már említett rosszindulatú program, vagy malware. Ez minden olyan kód, amely veszélybe sodorhatja a felhasználót, a felhasználó adatait vagy az eszközt. Általában ezen programoknak az alábbiak közül valamelyik lehet a célja [58]. Kompromittálja a felhasználó eszközének integritását, irányítást nyer a felhasználó

eszköze fölött, távvezérelt műveletek támadók számára történő engedélyezésével a fertőzött eszközök elérése, használata vagy más módon történő kihasználása, személyes vagy hitelesítő adatok hozzájárulás nélküli továbbítása, nyilvánosságra hozatala. Ezen kívül spam vagy parancsok terjesztése a fertőzött eszközről más eszközök vagy hálózatok befolyásolására, valamint felhasználó megtévesztése.

Például az Avast egyik riportja szerint [59] csaknem 15 millió letöltést ért el összesen 47 olyan applikációt, amelyről kiderült, hogy rosszindulatú adwareket (reklámokat megjelenítő malware) tartalmaznak. Ezek mind a HiddenAds trójai család részei, amely biztonságos és hasznos alkalmazásoknak álcázza magát, de valójában csak tolakodó hirdetések megjelenítésére szolgál a felhasználó számára. Agresszíven jelenítik meg azokat az előugró ablakokat, amelyekre való kattintás után rögtön díjat számolnak fel a felhasználónak további funkciók használatáért, akár olyan hirdetéseket megjelenítve, amelyek a teljes képernyőt lefoglalják. Gyakori, hogy ezek az alkalmazások játékoknak vannak álcázva, majd a letöltés után bizonyos idővel mutatják meg valódi arcukat. Érdekesség, hogy ezeket az appokat gyakran Tiktokon vagy Instagramon is reklámozzák, így növelve a hitelesség érzetét. A Kaspersky riportja szerint [60] 2020-ban a koronavírus témájú csalások is jellemzőek voltak, például a GINP banki trójai olyan alkalmazásnak mutatta magát, amely COVID-19-fertőzött személyeket keresett, de közben az áldozatot arra késztették, hogy a bankkártya-adataikat 0,75 eurós díj megfizetésének ürügyén adják meg, amivel aztán visszaélésre is lehetőség volt. A technika szempontjából web injekciót alkalmaztak: bizonyos események észlelésekor a banki trójai megnyit egy ablakot, amely egy weblapot jelenít meg a bankkártya adatainak kérésével. Az oldal aztán bármilyen kivitelű, ürügyű lehet.

Az ENISA Threat Landscape beszámolója szerint [61] a malware-k családja továbbra is az első számú vezető fenyegetés. Mobil esetében például növekvőben van a kifejezetten banki adatok lopására létrehozott, eredetire nagyon hasonlító hamis mobil bankoló applikációk száma. Növekedést mutatott a fájl nélküli rosszindulatú programok (fileless malware) csoportja is, amelyek nem tartalmaznak könnyen kiszűrhető, futtatható fájlokat, hanem a telepítés után, amikor már biztonságosnak gondolja őket a rendszer, a támadó távolról rosszindulatú kódot juttat be, vagy rosszindulatú makrókat tartalmazó fájlt töltet le, amely megindítja a támadást. A felhasználói szempont miatt a malware-ket röviden felsorolom csak. Applikációk esetében lehetséges malware típus a hátsó ajtó (backdoor), amely olyan kód, ami lehetővé teszi a nem kívánt, potenciálisan káros, távvezérelt műveletek végrehajtását egy eszközön. Tehát tudatosan hagynak maguknak a rosszindulatú szereplők egy bejáratot, amivel később könnyebben véghez

vihetik céljukat [58]. Jellemző malware a trójai (*trojan*) programok csoportja. Ezek jóindulatúnak látszó programok, melyek nemkívánatos műveleteket hajtanak végre a felhasználóval szemben. Mindig van egy ártalmatlan és egy káros oldala, például előfordulhat, hogy egy játék applikáció emelt díjas SMS-eket küld a felhasználó jóváhagyása, tudta nélkül. Ez a felépítés megkönnyíti a gyanútlan felhasználóhoz való eljuttatást. Az applikációkhoz köthető malware-knél még fontos megemlíteni a magasabb szintű jogosultsággal való visszaélést (*elevated privilege abuse*), amely sérti a rendszer integritását az alkalmazás sandbox-ának feltörésével, jogosultságok megszerzésével, esetleg az alapvető biztonsági funkciókhoz való hozzáférés megváltoztatásával vagy letiltásával. Például olyan alkalmazások, amelyek a módosításokkal megakadályozzák, hogy eltávolítsák őket [58]. Jellemző malware még a vírus, amely egy olyan rosszindulatú program, amely egy programhoz, fájlhoz vagy dokumentumhoz kapcsolódik, és lehetővé teszi az egyik számítógépről a másikra való terjedését. A malware-k csoportjába tartozik még a férgek (worms) csoportja. A féreg hasonló a vírushoz, és néha a vírus alosztályának tekintik. Csakúgy, mint egy vírus, gépről gépre terjed, de a féreg képes emberi tevékenység nélkül terjedni. A féreg általában kihasználja a gyengeségeket, például az operációs rendszer sebezhetőségét vagy a gyenge jelszavakat, hogy elterjedjen a hálózatokon. A következő kategória ebben a csoportban a spyware, vagyis kémprogram. Ez egy olyan rosszindulatú program, amely a felhasználók tevékenységét figyeli azok tudta vagy beleegyezése nélkül. Ezek a kémkedési tevékenységek magukban foglalhatják a leütések naplózását (*keylogging*), a tevékenység figyelemmel kísérését és az adatgyűjtést, valamint az adatlopás egyéb formáit. A kémprogramokat általában trójai programként vagy szoftveres sebezhetőségek kihasználásával terjesztik [62]. Utolsóként említem a ransomware-t, vagyis a zsarolóvírusok egyre növekvő előfordulású csoportját. Ez egyfajta rosszindulatú program, amely korlátozza a fertőzött eszköz vagy hálózat fájljaihoz való hozzáférést. Azáltal kerül be az eszközre, hogy a felhasználó véletlenül letölt egy valós fájlnak álcázott trójai programot, vagy ha egy hamis hirdetésre kattint, amely átirányítja őt egy rosszindulatú webhelyre. Miután a rosszindulatú programot letöltötték, üzenet jelenik meg, amelyben az áldozatot törvénytelenségek elkövetéssel vádolják, majd a fájlokat titkosítják és lezárják a telefont. A fizetés feldolgozása után (melyhez gyakran a Bitcoin-t használnak), a támadó kódot küld a telefon feloldásához vagy az adatok visszafejtéséhez [63].

Végül egy későbbiekben is gyakran említendő veszélyforrás az emberi hiba. Ebbe a kategóriába tartozik minden olyan hiba, amely nem feltétlenül rossz szándékból került az alkalmazásokba, mégis hagy a rosszindulatú szereplőknek például hátsó ajtót, vagy olyan

adatot gyűjt, amire nincs jogosultsága stb. Ezen hibákat a későbbiekben bemutatott ajánlások betartásával jelentősen vissza lehet szorítani.

2.2.2. Web-alapú fenyegetések

Amint már a statisztikákból látható volt, az internetelérések sok esetben történnek mobil eszközökről, így a web-alapú fenyegetések igen jelentős csoportját képviselik a mobil appokkal kapcsolatos veszélyeknek. Ide tartoznak a webes felületeken, a böngészőn, a weboldalon vagy bővítményeken keresztül fertőző programok, valamint a webes szolgáltatások és alkalmazások gyengeségeit kihasználó fenyegetések, melyek sokszor átfedésben vannak az előző pontban említettekkel, így egyes részek akár össze is moshatók. Ezen fenyegetéseknek is számtalan formája ismert, melyeket egy átlag felhasználó nehezebben kerülhet el, mint az előző pontban említetteket, ezért ezeket jelen dolgozatban csak részletezés nélkül említem. Azonban ezekre is vannak megfelelő védekezési módszerek, melyeket a későbbiekben ismertetek [64]. Ilyen típusú támadások lehetnek például: SQL injection, Cross site scripting (XSS), Cross site request forgery (CSRF), Denial of service (DoS), OS command injection, LDAP injection és ezzel kapcsolatban is megjelenhetnek zero day támadások.

Mivel ezeket a támadásokat egy átlagos felhasználó nehezen veheti észre, más módszerekkel kell védekezni ellenük. Amit azonban könnyebben elkerülhet a felhasználó, az az alábbi két típus, melyek amúgy a többi kategóriában is jellemzőek és igen kártékonyak. Ezek az emberi hibára alapoznak, melyhez fontos tisztázni a social engineering fogalmát. „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer- a technológia használatával vagy anélkül- képes az embereket információszerzés érdekében kihasználni” [65]. Tehát minden olyan technika, amely célja, hogy rossz szándékkal rávegye a felhasználót információk felfedésére vagy valamilyen konkrét cselekvésre. Ez pszichológiai manipulációval valósítható meg, akár személyesen vagy például telefonon, de egyre inkább a technológia felhasználásával. Ilyen pszichológiai eszközök például a tekintély, a hiány, a kölcsönösség elve vagy a társadalmi bizonyíték. Valójában napjainkban a legtöbb kibertámadás használja ezt a technikát valamilyen módon [66]. Robert B. Cialdini Hatás című könyvéből idézve [67, p. 37] a social engineering során kihasznált emberi hibák a következőképp írhatók le. „Az együttműködés elnyerésének folyamatát, azt, amikor az egyik embert ráveszik, hogy eleget tegyen a másik kívánságának, sokszor csak úgy érthetjük meg, ha figyelembe vesszük az ember automatikus, egyszerűsített reakciókra való hajlamát. Kultúránkban a legtöbb egyén rendelkezik egy sor olyan tulajdonsággal, amely másokat

együttműködésre késztet, vagyis mindenki sok olyan információt hordoz, aminek alapján eldönthetjük, mikor helyes és kifizetődő az illető kívánságát teljesítenünk. Minden ilyen kiváltó tulajdonságot a befolyásolás hatófegyvereként használhatunk, hogy ezáltal rávegyünk másokat a kívánságaink teljesítésére." Az ilyen típusú támadások tehát úgy tudnak hatékonyak lenni, hogy kihasználják az emberi viselkedés nem tudatos elemeit. Ezen kívül a segítőkészségre és konfliktuskerülésre is építenek. A Proofpoint Human Factor jelentése szerint [68] majdnem minden támadáshoz valamilyen emberi interakcióra volt szükség, például egy mellékletet kellett megnyitni, vagy egy linkre kattintani. A legjelentősebb social engineering eszköz az e-mail, melyen keresztül a támadások érkezhetnek. Ahhoz, hogy ezek a támadások egyre inkább sikeresek legyenek, hozzájárul a nagymértékű, egyre pontosabb személyre szabás is, ami a hihetőséget növeli. Bár ebben az alkategóriában említem, ugyanúgy használhatnak az első pontban említett, applikációval kapcsolatos veszélyek is ilyen technikákat annak érdekében, hogy a letöltővel elhitessék, hogy az applikáció nem rosszindulatú.

A social engineering-et használják (többek között) az alábbiak is.

- Phishing (adathalászat): ezek olyan social engineering technikákat használó e-mailek, amelyek célja, hogy rávegyék az áldozatot, hogy megossza személyes adatait, egy rosszindulatú programot töltsön le (jóindulatúnak álcázva), vagy például pénzt utaljon illetékteleneknek. Az ENISA fenyegetettségi riportja szerint [69] az adathalászat a malware-k terjesztésének 90%-áért volt felelős, az adatokhoz való illetéktelen hozzáféréssel kapcsolatos incidensekhez pedig 72%-kal járult hozzá. Ezek célja tehát lehet adatlopás, kémkedés, zsarolás is. Sokszor ezek az e-mailek sürgős tennivalókat tartalmaznak, esetleg fenyegető esemény bekövetkezésével igyekeznek gondolkozás nélkül tettekre rávenni a fogadót (például azonnal változtassa meg jelszavát az alábbi linkre kattintva, stb.).
- Spam: bár egyre csökken a népszerűsége, az ENISA 10-es listájában [69] még mindig szerepel a spam-ek csoportja. Ezek olyan kéretlen üzenetek, melyeket botnetek segítségével juttatnak el felhasználókhoz. (A botnet több internethez csatlakoztatott eszköz, amelyek mindegyike egy vagy több botot futtat. Ezek olyan robotok, melyek automatikus feladatokat futtatnak az interneten. Ilyen technikával működnek például a DoS támadások is.) Szerencsére a spamszűrő szolgáltatások egyre fejlettebbek, így képesek már jobban szűrni ezt a típust. Hátrányuk még a személyre szabás viszonylagos hiánya is, így felhasználói szempontból könnyebben felismerhetők.

A fent említett módokkal szintén terjeszthetők malware-k, melyek a már ismertetett sokféle módon károsíthatják a célpontokat.

2.2.3. Vezeték nélküli kapcsolat fenyegetései

A következő nagyobb csoport a vezeték nélküli hálózati csatlakozással kapcsolatos fenyegetések. Ebben a csoportban (bár az előző ponttal a határai szintén nem élesen különválaszthatók) a vezeték nélküli kapcsolatokkal megjelenő veszélyeket ismertetem, a használat gyakorisága miatt a wifi kapcsolatokra fókuszálva.

Ezt a témát két szempontból érdemes vizsgálni. Egyrészt, ha a felhasználó csatlakozik egy elérhető hálózathoz, másrészt, ha a felhasználó osztja meg saját vezeték nélküli hálózatát. Előbbi magától értetődően azt jelenti, hogy a felhasználó csatlakoztatja mobil eszközét egy vezeték nélküli hálózatra. Utóbbi, a mobil hotspot-internetmegosztás, amely az okostelefonok alapfelszereltsége, lehetővé teszi a wifi-kompatibilis eszközök számára az internet elérését a hozzájuk való csatlakozással. Ez a folyton úton lévő felhasználóknak jó opció lehet mobilitásuk növelésére. Gyakori például laptop vagy táblagép telefonhoz való kapcsolódása. Itt a telefon töltöttsége, a sávszélesség és rendelkezésre álló adatforgalom mennyiségének csökkenésén kívül szintén megjelennek az alábbiakban említett biztonsági kockázatok.

War walking vagy war driving során (célja, hogy feltérképezze séta vagy vezetés közben az elérhető vezeték nélküli hálózatok fizikai helyét), számtalan sebezhető hálózatot találhatunk, melyekről sok adat érhető el nyilvánosan. Ezek pedig a használóik számára is kockázatot jelenthetnek, még titkosítás esetén is. Jellegükből adódóan ezek a hálózatok több irányból történő támadásnak is ki vannak téve, ugyanis a vezetékes LAN-októl eltérően a vezeték nélküli LAN-felhasználó nem korlátozódik egy vállalat fizikai területére vagy egyetlen hozzáférési pontra. A vezeték nélküli LAN hatótávolsága messze kiterjedhet az iroda vagy az épület fizikai határain kívülre, ezáltal lehetővé téve az illetéktelen felhasználók számára a nyilvános helyekről való hozzáférést, például parkolóból vagy a szomszédos irodákból. A nem védett WAP-ot (*wireless access point*- vezeték nélküli elérési pont) célzó támadónak csak a cél közelében kell lennie, és a hálózatra való betöréshez már nincs szüksége speciális képességekre, de a védetteknél is van mód a támadásra. Az alábbiakban a támadásokat két fő csoportra osztom céljuk szerint: a hálózatra való bejutást célzó támadásokra, valamint a hálózati lehallgatást célzó támadásokra.

Hálózatra való bejutást célzó támadások: ezek célja a hálózatra való bejutás. Miután a támadó már a hálózaton van, számtalan lehetősége van károkozásra: adatok ellopása, törlése, módosítása, esetleg rosszindulatú programok, támadások indítása, stb.

- Piggybacking [70]: Ha nem sikerül biztosítani a vezeték nélküli hálózatot, bárki használhatja a kapcsolatot, aki a hozzáférési pont hatótávolságában van. A hozzáférési pont tipikus beltéri sugárzási távolsága 50-100 méter. A szabadban ez a hatótávolság akár 300 méter is lehet. Tehát a nem biztosított, nem védett vezeték nélküli hálózat sok hívatlan felhasználó számára is megnyithatja az internetkapcsolatot. Előfordulhat, hogy csak az ingyen internetkapcsolat vonzza ezeket a szereplőket, azonban azok a bejutást követően képesek lehetnek illegális tevékenységek folytatására, az internetes forgalom megfigyelésére és rögzítésére vagy személyes fájlok ellopására is.
- Hamis hozzáférési pont (*rouge access point*) [71]: egy olyan vezeték nélküli hozzáférési pont, amelyet egy biztonságos hálózatra telepítettek, a helyi hálózati rendszergazda kifejezett engedélye nélkül, akár jó szándékú alkalmazott, akár rosszindulatú támadó adta hozzá. Ez mindkét esetben a biztonsági intézkedések elmaradásával járhat, amik egyértelmű támadási felületet biztosítanak.
- Gonosz iker támadás (*evil twin attack*) [70]: egy gonosz ikertámadás során a támadó információkat gyűjt egy nyilvános hálózati hozzáférési pontról, majd beállítja a rendszerét annak megszemélyesítésére (tehát egyfajta social engineering támadásról van szó). Az támadó a valós hozzáférési pont által generáltnál erősebb sugárzási jelet használ; akkor a gyanútlan felhasználók az erősebb jelhez csatlakoznak. Mivel az áldozat a támadó rendszerén keresztül csatlakozik az internethez, a támadó könnyen használhat speciális eszközöket az áldozat által az interneten küldött adatok olvasására. Ezek az adatok tartalmazhatnak hitelkártyaszámokat, felhasználónév és jelszó kombinációkat, valamint egyéb személyes adatokat.
- Közbeékelődéses támadás (*man in the middle*) [72]: gyűjtőnév az olyan támadásokra, amely közbeékelődéssel elfogja és kompromittálja a kommunikációt két rendszer között. Például egy http tranzakció során a cél az ügyfél és a szerver közötti TCP kapcsolat. Különböző technikák alkalmazásával a támadó az eredeti TCP-kapcsolatot két új kapcsolatra osztja fel, az egyiket az ügyfél és a támadó között, a másikat pedig a támadó és a szerver között. Miután a TCP kapcsolatot elfogták, a támadó egy proxy, amely képes elolvasni, beilleszteni és módosítani az elfogott kommunikáció adatait. Itt pedig a már említett kockázatok érvényesülhetnek, a személyes adatok ellopásától a

rosszindulatú programok beágyazásáig számtalan lehetőséggel. A támadóknak több lehetőségük van, például vizsgálhatnak csomagokat a kommunikációból (*sniffing*), rosszindulatú csomagokat adhatnak a kommunikációba (*packet injection*), vagy eltéríthetik a munkameneteket (*session hijacking*). Tehát a közbeékelődéses támadásoknak sok fajtája létezhet, a teljesség igénye nélkül például: IP spoofing, DNS (Domain Name Server) spoofing, SSL (Secure Socket Layer) stripping és hijacking, ARP (Address Resolution Protocol) spoofing és webolal hamisítás, amikor az eredetihez megszólalásig hasonló weboldalt hoz létre a támadó (esetleg annak elérését megtámogatva DNS spoofing-gal), a hitelesítési részletek ellopására vagy rosszindulatú programok terjesztésére, amelyek hátsó ajtó hozzáférést biztosítanak számukra akár a vállalati hálózathoz, vagy személyazonosság-lopáshoz is használhatók. A spoofing összefoglalva tehát hamisítás egy nem megbízható forrásból származó kommunikáció megbízhatóként való álcázására.

Hálózat lehallgatását célzó támadások: ezek célja hasonló a fentiekhez, de megelégszenek a lehallgatással, forgalom figyelésével, sokszor a hálózatra való bejutás nélkül.

- Forgalomfigyelés (*sniffing, eavesdropping*) [73]: a lehallgatás, más néven szippantás vagy szimatolása hálózaton áthaladó adatcsomagok figyelésére szolgál. A forgalmat rossz szándék nélkül is sok hálózati és biztonsági elemző vizsgálja. Azonban ez a támadóknak is jó eszköz lehet. Egy ilyen támadás során a csomagok monitorozásával (vagy akár módosításával vagy törlésével) a hallgatózó sokféle adathoz férhet hozzá. A legtöbb vezeték nélküli hozzáférési pont rendszeresen sugározza a szolgáltatáskészlet-azonosítóit (SSID) bárkinek, aki hallgatja, ez pedig a nem megfelelő védelmi intézkedések (például alapértelmezett jelszó megváltoztatása) akár hozzáférést is jelenthet a hálózathoz. Előfordulhat, hogy egy valós felhasználó csatlakozását figyelik meg a hálózatkor, vagy annak egy pénzügyi tranzakcióját, mely esetben a felhasználónév, jelszó, vagy banki adatok is ellophatók, de akár el tudja lopni a hálózati szerverről megnyitott fájlokat is a lehallgató. (Ideális esetben ezeket a csomagokat titkosítják, hogy a lehallgató ne tudja megfejteni az adatokat. Általában akkor fordul elő, amikor a felhasználó olyan hálózathoz csatlakozik, amelyben a forgalom nem biztonságos vagy nincs titkosítva. Az adatokat egy nyílt hálózaton keresztül továbbítják, ami lehetőséget ad a támadónak különböző módszerek segítségével történő elfogására. A lehallgatási támadásokat gyakran nehéz észrevenni. A kibertámadások

más formáival ellentétben a hiba vagy a figyelő eszköz jelenléte nem befolyásolhatja hátrányosan az eszközök és hálózatok teljesítményét.)

2.2.4. Hozzáféréssel kapcsolatos fenyegetések

Az utolsó, de szintén jelentős nagyobb csoport, amit bemutatok, az a hozzáféréssel kapcsolatos fenyegetések csoportja. Ezen csoportosítás megértéséhez érdemes tisztázni a hozzáférés-vezérlés fogalmát. „A hozzáférés-vezérlés olyan biztonsági mechanizmusok gyűjteménye, mely meghatározza, hogy a felhasználók mit tehetnek a rendszerben, azaz milyen erőforrásokhoz férhetnek hozzá és milyen műveleteket hajthatnak végre” [74, p. 67]. Az alábbi négy feladata van [74].

1. Azonosítás (*identification*): a rendszer résztvevőit egyedi azonosítókkal kell ellátni a megkülönböztethetőség és elszámoltathatóság érdekében (így a rendszerben történt események konkrét felhasználókhoz köthetők). Röviden ez megmutatja, hogy ki próbál hozzáférni a rendszerhez.
2. Hitelesítés (*authentication*): ennek során a felhasználó bizonyítja, hogy valóban az, akinek állítja magát, tehát hitelesíti az önmagáról állítottak valódiságát. A hitelesítés több módon történhet, lehetséges tudásalapú, tulajdonalapú, tulajdonságalapú és vegyes típusú. Tudásalapú: melyhez valami olyanra van szükség, amit a felhasználó tud. A legismertebbek ezen kategóriában a jelszavak, jelkódok, PIN kódok. Tulajdonalapú/ birtoklásalapú: olyan módok tartoznak ide, amelyek során a felhasználónak rendelkeznie kell valamivel, ami a hitelesítést segíti. Ide tartoznak a tokenek, belépőkártyák, egyszerhasználatos jelszavak (OTP-*one time password*) de akár a kulcs is. Tulajdonságalapú: a felhasználó valamely tulajdonsága segíti a hitelesítést, tehát a biometrikus tulajdonságok képezik a hitelesítés alapját. Lehetnek tulajdonság vagy viselkedés alapúak. A legismertebbek az ujjnyomat, írisz, arc vagy például a hangfelismeréssel való hitelesítés. Vegyes/ többfaktoros: a fentiek közül legalább kettő együttes használata a nagyobb biztonság érdekében.
3. Hozzáférés-engedélyezés (*access approval*), más szóval felhatalmazás (*authorization*): ha az azonosítás-hitelesítés sikeres, akkor megkapja a felhasználó a hozzáférést.
4. Audit (elszámolás- *accountability*): ez a pont a hozzáférések felügyeletét, naplózását jelenti elszámoltathatósági okokból.

A fentiek alapján a hozzáféréssel kapcsolatos fenyegetéseket a hitelesítés típusai szerint vizsgálom, így a számtalan veszély közül az alábbi csoportokat mutatom be: jelszóval kapcsolatos fenyegetések, lopás, biometrikus hitelesítéssel kapcsolatos fenyegetések.

A jelszó kérdése mindig is meghatározó volt biztonsági szempontból. Mivel nagyon elterjedt, sok támadási mód ismert. Az első ilyen az adathalászat, mely a legegyszerűbb módszer a jelszavak megszerzésére. Jellemzően egy megbízható személy vagy szervezet nevében, sokszor e-mailben kéri a támadó, hogy a felhasználó például jelentkezzen be, változtassa meg jelszavát, fizessen be sürgősen egy számlát. Ezekben az e-mailekben hamis bejelentkezési oldalakra vezető linkek találhatók (amelyek valósnak vannak álcázva). Ha ezeken bejelentkezik a felhasználó, a belépési adatait ellophatja a támadó. A social engineering máshogy is támogathatja a jelszavak feltörését: például ha bármilyen módon az áldozatról sikerül személyes adatokat, preferenciákat, kötődéseket kideríteni, előfordulhat, hogy a könnyebb megjegyezhetőség érdekében személyes jelszavakat is könnyebb feltörni. Gyakori ugyanis, hogy a felhasználók a gyermekük születésnapját vagy például kutyájuk nevét is felhasználják jelszavaikban. Ebbe a kategóriába sorolhatók még a brute force támadások, jelszó szórás (*password spraying*), dictionary attack, szivárványtábla támadás (*rainbow table attack*), hitelesítő adatok kitöltése (*credential stuffing*), valamint keylogger támadások [75]. A dictionary attack során szótári szavakat használ a támadó, mely már nem csak karaktereket, de egész szavakat, azok kombinációját próbálja végig, de itt is figyelembe veszi a támadó a leggyakrabban használtakat. A leetspeak-re (mely során a jelszóból néhány betűt egy hozzá hasonló számra változtatunk) is fel vannak már készülve a támadók, így a biztonságot az sem növeli sokkal [76]. A hitelesítő adatok kitöltése során a kikerült hitelesítő adatokat a támadók kipróbálhatják még számtalan másik felhasználói fiókon, amíg találatot nem kapnak, kihasználva azt, hogy általában egy felhasználónak több fióknál is lehet azonos felhasználóneve és jelszava. A dark weben sok ilyen adat érhető el akár ingyenesen vagy pénzért [75].

Mivel már szerepelt az előbbiekben, a közbeékelődéses támadást itt már csak említem, hiszen a forgalom vizsgálatával szintén hozzá lehet férni a hitelesítő adatokhoz.

A következő nagyobb kockázati csoport az egyszerű lopás, vagyis ha az eszköz illetéktelen kezekbe kerül. A támadás egyszerűsége miatt ezt a pontot nem részletezem, azonban fontos megemlíteni, hogy értelemszerűen ez az azonosítás-hitelesítés feletti kontroll elvesztését is jelenti. Mivel hatalmas mennyiségű személyes adatot tárolnak a felhasználók a mobiljaikon,

így az eszközök elvesztése, lopása anyagi károkon túl problémát okozhat (nem megfelelő védelmi intézkedések hiányában) adatvesztéssel, személyes adatok ellopásával, kikerülésével, rendszerekhez, programokhoz való illetéktelen hozzáféréssel, vállalati környezetben akár reputációt érő veszteséggel és súlyos bírságokkal (például a GDPR, *General Data Protection Regulation* miatt) kiegészülve. Egy Deloitte által végzett kutatásban [77], ahol szakértő IT elemzők próbáltak meg kinyerni adatokat mobil lopott és gyári visszaállított, törölt (használtan eladott) eszközökről, kiderült, hogy nem megfelelő védelem esetén a felhasználóról nagyon sok adat kideríthető az eszköze alapján, például a személyazonossága, e-mail címe, sok esetben akár hitelesítési adatok is, amelyek később visszaélésre adhatnak lehetőséget. Ezekkel az adatokkal lehetséges akár személyazonosság lopás, amikor a megszerzett adatokat törvénytelen célokra, például spamküldésre, zsarolásra, kapcsolatoktól való pénzkicsalásra, esetleg az áldozat nevében történő hitelfelvételre, internetes vásárlásokra használják. Előfordulhat az is, hogy hozzáférnek a mobilra telepített banki vagy bevásárló appokhoz a lopással, a megjegyzett bejelentkezési és fizetési adatokkal így is érheti kár az áldozatot. Extrém esetekben akár az áldozat személyes biztonsága is veszélybe kerülhet, hiszen a mobil eszközéről kideríthetők a gyakran látogatott helyek vagy akár az otthoni címe is.

Az utolsó nagy csoport a biometrikus hitelesítéssel kapcsolatos fenyegetések csoportja. Mielőtt ezeket összefoglalom, röviden ismertetem a folyamat logikáját. A biometrikus hitelesítés általában két fő részből áll. Az első szakasz a felhasználó biometrikus jellemzőinek regisztrálása, valamint ezen információk digitalizálása és mentése. A második rész maga a hitelesítés, amikor a rendszer új mintát vesz és összehasonlítja az adatbázisban található mintákkal. Ha a két minta egyezik, a hozzáférést megadják. Vagyis ezek a feliratkozási és a felismerési fázisok. E folyamat során a regisztrált biometrikus adat lényegében egy számítógépes kódrészlet, amelyet a jövőben referenciaként használnak. Az első rész szigorúan szabályozható például szervezeti környezetben, így a minta felvételekor a tulajdonos személye ellenőrizhető. A második szakaszban azonban az eredeti identitás már nem támadható meg, a rendszer csak a meglévő adatokkal keres egyezést. (Ez bizonyos szempontból azt is jelenti, hogy nem helyes az az elképzelés, hogy a biometria önmagában biztonságosabb, mint más módszerek.) Az egyik fontos különbség az, hogy például a jelszavaktól eltérően a biometrikus adatok nem igényelnek pontos egyezést, amikor a két mintát összehasonlítják. A rendszerek úgy állíthatók be, hogy elfogadják az ésszerű bizonyosságot, amely elég biztonságos, de képes felismerni a felhasználót abban az esetben is, ha például az ujja túl nedves vagy száraz. Az elfogadási szintet küszöbértéknek is nevezzük (az élő és a tárolt minták hasonlóságának

mérésére szolgál). Ez általában 100%-nál alacsonyabb értékre van beállítva, hogy rugalmasan felismerje ugyanazon testrész különböző állapotait, azonban szem előtt kell tartanunk, hogy a küszöbérték csökkentése a biztonsági szintet is csökkentheti. Egy másik példa, ha az adatbázis hatalmas, akkor jobb, ha a küszöbértéket magasabb százalékra beállítani, így nem hozunk létre hamis pozitív eredményeket.

A kutatásaim során két biometrikus hitelesítéssel kapcsolatos publikációm is született kisebb kérdőíves kutatásokkal, melyekből kiderült, hogy a kitöltők körében népszerű módszerről van szó, és főleg a telefonjaikon használják (annak feloldásához, nem specifikusan alkalmazásokhoz) [78]. Az is kiderült, hogy a válaszadók átlagosan kedvelik a biometrikus hitelesítést és biztonságosnak is találják, azonban már kisebb arányban válaszolták, hogy fizetnének is ennek segítségével [79].

Az Apple iPhone készülékek biometrikus hitelesítésének rendelkezésre álló módszerei az ujjnyomat és az arcfelismerés, amit Touch ID-nak és Face ID-nak neveznek. Az Apple szerint [80] annak valószínűsége, hogy egy véletlenszerű ember a populációból feloldhassa az iPhoneunkat, 1: 50 000 Touch ID-val vagy 1:1 000 000 Face ID-val. A Touch ID lehetővé teszi a felhasználók számára, hogy a kódok helyett ujjnyomatukkal oldják fel telefonjukat. A felhasználó engedélyezheti, hogy ezt használják az App Store, az iTunes Store, az Apple Pay és az Apple Books vásárlásai is, valamint egyre több pénzügyi szolgáltató applikációjához is használható (például banki appok). Kiegészítésként azért funkció beállításához és módosításához (és néhány más esetben) jelszóra is szükség van. (Érdekesség, hogy a technológia folyamatosan tanul a felhasználó ujjlenyomatáról, kibővíti az ujjnyomat-térképet, mivel további átfedő részek kerülnek hozzáadásra, amikor a felhasználók ujjaik különböző szögeivel próbálnak hozzáférni [81].) A Face ID lehetővé teszi a felhasználónak, hogy feloldja telefonját vagy belépjen az alkalmazásaiba a telefonra történő egyszerű nézéssel. Az arcazonosítót a Touch ID-hez hasonlóan lehet használni. Sok okostelefon beépített hangfelismeréssel is rendelkezik, például a Siri az iPhone-nál, de ezek még nem elég kifinomultak ahhoz, hogy hitelesítésre lehessen őket használni. Sok zavaró tényező lehet a környezetben (háttérzaj, a szoba akusztikája), amelyek miatt ezt a technikát nehéz azonosításra használni. Ennek kombinálása például egy jelkóddal javíthatja a biztonságot. Egyes online fórumokon vannak olyan történetek, amelyek alapján ritkán beenged a felhasználón kívül mást is a rendszerbe, ha a hangjuk hasonló (például ha a tulajdonos azonos nemű testvére próbál hozzáférni), melyek szintén alátámasztják ezt az állítást. Ezek a funkciók elérhetők más gyártók okostelefonjain is, ahol szintén a rendszerbe vagy egyes applikációkba való belépésre

használhatók, csak esetleg más fantázianevük van. A gyártó mérete miatt Android-os megoldásokból kiemelném például a Samsung Pass-t [82], egy személyazonosság-kezelés szolgáltatást (*identity management as-a-service*), amely biztonságos hozzáférést tesz lehetővé biometrikus hitelesítéssel (ujjnyomatot, íriszt és arcfelismerést használva).

Mint minden módszer, a jó híre és megbízhatósága ellenére ez is rejthet kockázatokat, veszélyeket [83, p. 260]. A rendszerhibákat okozó biztonsági fenyegetések a biometrikus adatok esetében négy kategóriába sorolhatók: szolgáltatásmegtagadás (*denial of service*): mely azt jelenti, hogy egy jogosult felhasználó nem tud hozzáférni a rendszerhez. Behatolás (*intrusion*), ami azt jelenti, hogy illetéktelen felhasználó lép be a rendszerbe. Elutasítás (*repudation*): azt jelenti, hogy egy jogosult felhasználó belép a rendszerbe, majd letagadja azt, állítva, hogy jogosulatlan felhasználó lépett be helyettük. Funkció kúszás (*function creep*): akkor jelenik meg, ha egy biometrikus rendszert kihasználnak, és az adatokat az eredetileg tervezettől eltérő alkalmazás elérésére használják, így összekapcsolható a felhasználó tudta nélkül két nyilvántartásban szereplő eltérő azonosítója. (Például egy bank adatbázisából nyert ujjnyomat-sablonnal fel lehet keresni az illető egészségügyi nyilvántartásait egy orvosi adatbázisban.)

A fenyegetések forrása alapján megkülönböztethetünk belső korlátokat és támadásokat [83, p. 280]. Az első hamis egyezéseket és hamis nem egyezéseket jelent (a tárolt sablon és belépési kisérletkor vett minta között), amikor a rendszer rosszul megválasztott beállítások miatt illetéktelen embereket enged be, vagy jogosultakat nem engedi be. Az utóbbiak, a támadások, további csoportokra oszthatók, nevezetesen belső és külső fenyegetésekre, amelyek célja a rendszer kihasználása, azzal való visszaélés. Ezek a támadások a már vázolt azonosítási folyamat bármelyik szakaszában megjelenhetnek, így a feliratkozás és a felismerés során is többféle módon támadhatnak meg egy rendszert. Összefoglalva tehát láthatjuk, hogy az ilyen típusú rendszereknél is lehetségesek a támadások és visszaélések. Ashbourn szerint a biometrikus adatok jó azonosítási forrást jelenthetnek, azonban nem tekinthetők egyedinek. (Emberek mintái között nagy lehet a hasonlóság.) Ez azt jelenti, hogy a hamis pozitív elfogadás kockázata valós, egy személy a hitelesítésekor helytelen mintához párosítható. Elméletileg az idő múlásával egyre több minta összegyűjtésével csökkenhet ez a kockázat, így a tárolt és az élő minta közötti elfogadható különbség küszöbértéke ennek megfelelően módosítható. A küszöbérték csökkentése viszont alacsonyabb szintű biztonságot és ezért a rendszerbe vetett bizalmat jelent, ezért nehéz megtalálni az egyensúlyt [84].

A biometrikus megoldások kockázatainál még fontos kiemelni, hogy a támadások megcélozhatják magukat a biometrikus adatokat is, nem csak a rendszert, amit azokkal védeni próbálnak. Tehát általában magasabb szintű biztonságot kell biztosítani a mentett mintának is, mivel ha ezek az adatok veszélybe kerülnek, definíció szerint is nehezebb módosítani és újra felhasználni őket ugyanarra a célra. A későbbiekben még röviden említem a gyártók által biztosított védelmet az okostelefonokon tárolt biometrikus adatok esetén.

Utolsóként pedig egy személyes adatvédelemre, magánélet védelmére kockázatot jelentő pontot említenék. Ugyanis ahhoz, hogy például a Siri vagy a Google Asszisztens mindig készen álljon a parancsok feldolgozására és teljesítésére, folyamatosan „hallgatóznia" kell. Minden gyártó igyekszik biztosítani felhasználóit, hogy ezekkel az adatokkal nem élnek vissza, de a kockázat valós.

A korábban említett többfaktoros hitelesítéssel a fenti kockázatok előfordulási esélye csökken, mert több lépcsőben és módszerrel történik a hitelesítés, megnehezítve a támadók feladatát.

Érdemes megemlíteni, hogy a COVID-19 világjárvány során sok olyan támadás és átverés jelent meg, amelyek módszerben nem feltétlenül jelentenek újdonságot, de tematikájukat a jelen helyzetre szabták, ezért hatásosak tudnak lenni. Dr. Stacey Wood californiai professzor szerint az, hogy ebben az időszakban a felhasználók sebezhetőbbek, három pszichológiai okra vezethető vissza: növekvő szorongás, depresszió, társadalmi igények (mint a validáció és a szeretet iránti igény), valamint a pénzügyi jólét kérdése. Értelemszerűen a világjárvány mindhárom területet érinti, hiszen sok ember veszti el szeretteit, dolgozik többet, esetleg otthonról, van egyedül, esetenként elveszítette a munkáját, ami anyagi nehézségekhez vezet, stb. Ezek a faktorok mind rontják az ember védekezőképességét az átverésekkel szemben. Nehezíti az ellenállást az is, hogy a fenyegetések sok esetben erre a helyzetre építve hihető történeteket találnak ki [85]. Ezt kihasználva és a számos pszichológián alapuló social engineering technikát használva még sikeresebbek lehetnek a támadások. A McAfee Labs jelentése szerint [86] percenként átlagosan 375 új fenyegetést észlelt, növekedést tapasztalva a COVID-19 témájú adathalász kampányok, rosszindulatú alkalmazások, rosszindulatú programok esetében. Az új mobilokkal kapcsolatos rosszindulatú programok 71%-kal nőttek 2019 júliusa és 2020 júliusa között. Mivel a fogyasztók egyre többet támaszkodnak mobil eszközeikre különféle feladatok elvégzésében, biztonsági szokásaikat is eszerint kell módosítaniuk. Gyakoribbak lettek a koronavírussal kapcsolatos regisztrált domainek, melyek sok esetben valódi megbízható oldalak, sok esetben viszont rosszindulatúak (spam

kampányokhoz, adathalászatra vagy malware terjesztésre létrehozva). Megjelentek a spamkampányokban, adathalász e-mailekben is a koronavírus témájúak, valamint a főleg kórházakat, intézményeket érintő zsarolóvírusok is [87].

3. FELHASZNÁLÓI BIZTONSÁG, A KÉRDŐÍV ELMÉLETI HÁTTERE

Az alábbi fejezetben a megelőző kutatások bemutatása után a magyar lakosságra reprezentatív nagyobb lekérdezéshez használt kérdőív összeállításának elméleti hátterét mutatom be. A biztonsági attitűdök megértéséhez az attitűd elmélet logikáját használtam, kiegészítve a védelemmotivációs elmélettel és a tervezett cselekvés elméletével. Ezek segítségével a biztonságtudatossággal és biztonságérzettel kapcsolatos kérdéseket tettem fel. Ezt követően a kérdőívben az attitűd harmadik pillérjére, a viselkedésre vonatkozó kérdések kerültek, melyek alapjait az alábbi javaslatok adják.

3.1. Kutatási munkák, pilot kutatások

A fejezetben leírt kutatási munkákra már a célkitűzéseket taglaló fejezetben is utaltam, melyeket a dolgozat elején található 1. ábra foglalja össze. Fontos megjegyezni, hogy az alábbi kutatások segítették a reprezentatív kutatás létrehozását, de nem tartozik hozzájuk hipotézis.

A primer kutatásaimat a témában a mesterszakon kezdtem meg, ahol online kérdőív segítségével 549 kitöltőt kérdeztem egészség alkalmazások használata és biztonság témakörében. Ebből kiderült többek között az, hogy a válaszadók körülbelül fele használ egészség témájú alkalmazásokat és van róluk pozitív véleménnyel. Megfigyeltem, hogy a válaszadók kora befolyásolta, hogy mennyire féltik személyes adataikat, valamint hogy mennyire zavarja őket, ha hozzáférnek vállalatok azokhoz. Összességében látható volt, hogy az idősebbek bizonytalanabbak az alkalmazásokban megosztott adataik biztonságának tekintetében, valamint kevésbé érzik azokat biztonságban a fiatalabb kitöltőkhöz képest. Ezzel párhuzamosan a fiatalabbak kevésbé is érezték az adataikat értékesnek. A teljes minta 63%-a állította, hogy nem tudja, mi történik a személyes adataival, amiket az alkalmazásokban megoszt. Ez érdekes azzal összevetve, hogy 86%-uk soha vagy csak ritkán olvassa el a tájékoztatókat, melyből arra következtethetünk, hogy ez nem is érdekli a felhasználókat [88].

A kutatás következő lépése egy kvalitatív, fókuszcsoportos megkérdezés volt az alkalmazásválasztási motivációkról. A megkérdezés logikája lemodellezve követi azt, ahogy egy felhasználó számára kiderülnek az egészség témájú alkalmazásról az információk a valós

alkalmazás választásnál és használatnál. Ez azért érdekes, mert a mélyebb, biztonságot érintő kérdésekre alkalmazások választásánál, de néha még a használat közben sem lát rá a felhasználó (hacsak nem kifejezetten érdeklődő a témában), melyet korábbi kutatásaimban kapott válaszok is alátámasztottak. Ezért véleményem szerint nem az alkalmazások tényleges biztonsága a fő kérdés felhasználó szempontból, hiszen azt elfogadják úgy, ahogy elérhető, hanem a felhasználók biztonsági attitűdje, melyet a fő kutatási kérdőívemben vizsgálok.

A fókuszcsoportos kutatásban 28 fő vett részt. (A résztvevők közül 6 nő és 22 férfi. A férfiak a mobil egészség alkalmazásoknak nem a tipikus célközönsége, mely segítségével elfogulatlanabb válaszok születhettek. A résztvevők a 20-as éveikben jártak, amely megfelel az előző kutatásaim szerint az ilyen típusú alkalmazások célcsoportjának.) A kutatás során az alkalmazásboltokban elérhető 8 legnépszerűbb fitnesz témájú (6 diéta, valamint 2 sport aktivitást követő) alkalmazás közül kellett a válaszadóknak az ingyenes funkciókat figyelembe véve választani (ugyanis a korábbi kutatásaim alapján a válaszadók 81%-a soha nem használ fizetős alkalmazást, további 17% is csak ritkán [88]. A megkérdezés öt szakaszban, három fordulóval zajlott.

1. Általános beszélgetés a fókuszcsoportos megkérdezés menetét illetően, majd az egészség alkalmazásokról, mely során felmértem a résztvevők hozzáállását és tudását az ilyen típusú alkalmazásokkal kapcsolatban. Ezeket általában ismerték, jónak tartották és nagyjából felük használt is ilyen kategóriába eső alkalmazást.
2. Az első fordulóban a résztvevőknek választaniuk kellett a 8 alkalmazásból csak képernyőfotók és értékelési pontszámok alapján, valamint a választásukra indoklást is kellett adni. (Ez modellezi, hogy mi az, ami először elérhető a felhasználónak, amikor egy alkalmazást szeretne választani.)
3. A második fordulóban megmutattam az alkalmazások funkcióit a résztvevőknek és újra választaniuk kellett, valamint a választásukat megindokolni.
4. A harmadik, utolsó fordulóban pedig megmutattam az alkalmazások hozzáférési engedélykéréseit és újra választásra és indoklásra kértem őket.
5. Ezután még általános beszélgetés következett a tapasztalatokkal kapcsolatban.

A kutatás során megfigyelhető volt, hogy az elérhető alkalmazás értékelés főleg akkor számít, ha rossz vagy ha nem ismerik az alkalmazást. Az is számított a választásnál, hogy korábban hallottak- e már az alkalmazásról: ha jókat hallottak, nem befolyásolta őket a választásban egyéb szempont (kivéve ha feltűnően negatív volt). Az egyszerű használatot és átláthatóságot,

vizualizációt sugalló képernyőfotók is segítenek meggyőzni a választókat (design és vonzó színek is). Funkciót tekintve a holisztikus hozzáállást (egy alkalmazás több területre), a motiváló közös kihívásokat és a GPS-t emelték ki, de csak 5 résztvevő változtatta meg a véleményét a funkciók megismerése során. Tehát az értékelés, képernyőfotók és előzetes ismeretek a legtöbb válaszadónál elegendőek voltak a választáshoz. A harmadik körben az engedélykérések hatására sem változott 25 válaszadó véleménye, azonban 5 az összehasonlítás hatására olyan alkalmazást választott, amire korábban nem esett volna a választása, azért, mert kevesebb hozzáférési engedélyt igényelt. Sokakat aggasztottak a túlzó engedélykérések, nem látták indokoltnak például a média és kontaktokhoz való hozzáféréseket sem, azonban a legtöbben azt állították, hogy nem befolyásolja a döntésüket a való életben sem, hogy mihez kér hozzáférést az alkalmazásuk. Azt is állították, hogy többek között azért nem tartják kockázatosnak a választásokat, mert hamar letörlik az alkalmazásokat, ha nem váltják be a hozzájuk fűzött reményeket. A lezáró beszélgetésben a résztvevők megerősítették, hogy az alkalmazásokat általában elfogadják azok elérhető formájában, bízva abban, hogy azok biztonságosak és védik a felhasználók adatait, ugyanakkor megfigyelhető volt az ezzel kapcsolatos bizonyosság hiánya is [13].

A kvalitatív szakasz után a kvantitatív kutatási szakasz két megalapozó, valamint egy nagyobb, reprezentatív kérdőíves kutatásból áll. Ennek első eleme egy online kérdőíves kutatás volt a felhasználói védekezési szokásokról. Ezt megelőzően összefoglaltam a lehetséges védekezési módokat és kockázatokat a szakirodalom és saját szakmai tapasztalataim alapján, majd 124 fős mintára vonatkozóan vizsgáltam ezen szokások alakulását. (A minta 65%-a nő, 45%-a budapesti, több, mint fele Y generációhoz tartozó, 31%-a a Z generációhoz tartozó volt. Összesen 43%-uk hallgató, és 30%-uknak volt informatikai területen való jártassága.) Megvizsgáltam, hogy a válaszadók melyik fenyegetésről tudják, hogy mit jelent, melyből arra következtettem, hogy bár sok fenyegetést ismernek, az ENISA toplistán szereplők közül sokról nem hallottak. Megtudtam, hogy átlagosan 12 karakter hosszúságú jelszót választanak (e-mail fiókjukhoz), valamint hogy körülbelül kétharmaduk ritkán vagy soha nem változtatja, azonban 21%-uk félévente vagy kevesebb időnként változtatja meg jelszavát. A válaszadók 72%-a személyéhez nem köthető jelszót választ, azonban 81%-uk azt több helyen is felhasználja (ez például a munkahelyi és magánéletben használt jelszó összemosása esetében a vállalati kitettséget is növeli). Kiderült, hogy a válaszadók 67%-a mindig bekapcsolva tartja a Wi-Fi-t, 15%-a a Bluetooth-t, valamint 17%-uk használ VPN-t, de 16%-uk nem tudja mi az. A válaszadók 45%-a automatikus operációsrendszer frissítéseket, 41%-uk automatikus

alkalmazás frissítéseket használ. A kitöltők 67%-a rendszeresen ellenőrzi az alkalmazások beállítását, valamint 66%-uk az alkalmazás hozzáféréseket is (például kamera, mikrofon). Megtudtam, hogy 44%-uk használ tűzfalat vagy antivirus programokat. Érdekes módon 8% gondolja, hogy a bankja elkérheti e-mailben személyes adatait (további 2% nem biztos benne), valamint 3%-uk általában megnyit ismeretlen forrású mellékletet is (6% nem biztos benne), melyek mind kockázatokat rejtenek. Összességében tehát a kérdőívből kiderült, hogy bár vannak ismert és kevésbé ismert részletek, de a legtöbb válaszadó általában jól tájékozott a biztonság területét tekintve, és igyekszik ezt a mindennapi alkalmazás használat során is figyelembe venni [14], [15].

A kvantitatív kutatás második eleme egy szintén felhasználói szokásokról szóló megalapozó online kérdőíves kutatás volt a felhasználók biometrikus azonosításhoz való szokásairól és hozzáállásáról, mert ez egy igen népszerű téma a biztonságon belül napjainkban. A reprezentatív, nagyobb kérdőívben nem kapott kitüntetett szerepet a biometrikus azonosítás, mivel biztonsági attitűd szempontból nem tartottam kiemelkedőnek a szerepét. Ismét kérdőíves online megkérdezés keretein belül, ezúttal 224 fő válaszait vizsgáltam. (A kitöltők 66%-a férfi, 53%-uk fővárosi, valamint 54%-uk hallgató. A kitöltők fele a Z generáció tagja, 33%-uk az Y generációhoz tartozik.) A kitöltők nagy része leginkább az ujjnyomat, szem-, valamint arcfelismerő technológiákat ismerte (mind 83% fölötti arányban a kitöltők számához képest). Megtudtam, hogy a kitöltők 76%-a használt biometrikus azonosítást és van róla pozitív véleménnyel, valamint bízik is benne. Arra a kérdésre, hogy mennyire szívesen fizetnének is vele, már a 10-es skálát tekintve (1-egyáltalán nem fizetne vele, 10- szívesen fizetne) csak átlagosan 6-os szintű válaszok érkeztek. A válaszokból arra lehetett következtetni, hogy a kitöltőknek valószínűleg nem állt elegendő információ a rendelkezésükre a technológiát illetően ahhoz, hogy fizetésre is megbízhatónak ítéljék a módszert. Kiderült, hogy a válaszadók leginkább okostelefonjaikon használják (70%), leginkább arra, hogy feloldják lezárt eszközeiket (70%), de 30% használja még alkalmazásokba való belépésre és ugyanúgy 30% mobil fizetésre. Összességében tehát megfigyelhető volt, hogy ebben a témakörben a kitöltők jártasak, valamint hogy használják is rendszeresen a technológiát és nagyrészt bíznak is benne [78], [79].

A fentieket gyakorlati szempontból kiegészítendő, de inkább szakirodalmi kutatás részének tekinthetően, az applikációk értékelési rendszereit és az azokban rejlő lehetőségeket is vizsgáltam, melynek a későbbiekben külön fejezetet szentelek, így azt itt nem részletezem.

Hasonlóan, a reprezentatív kérdőíves megkérdezéssel történt kutatást is a későbbiekben fejltem ki részletesen.

3.2. Felhasználói biztonsági attitűdök és motivációk

Az alábbi fejezet arra a kérdésre keresi a választ, hogy hogyan alkalmazható az attitűd elmélete és fogalma a biztonság témakörében. A felhasználói biztonsági attitűdöt befolyásoló tényezők feltárásához az attitűdvizsgálatok logikáját és elméletét használtam. Számos definíció létezik, de George Katona (pszichológus) szerint „az attitűdök általánosított nézőpontjainkat reprezentálják, amelyek képessé tesznek bennünket arra, hogy bizonyos szituációkat kedvezően, másokat pedig kedvezőtlenül értékeljünk” [89]. Az attitűd három összetevője, amely a jelen felmérés összeállításánál is alapul szolgált: (1) a kognitív vagy ismereti komponens (hit és tudás), (2) az affektív komponens (érzelmek) és (3) a konatív, vagy más néven viselkedés-tendencia komponens. Gyakori, hogy az attitűd érzelmi összetevője befolyásolja az általános attitűdöt. A tudatos véleményformálás során a kognitív és affektív elemek harmóniájának megteremtése érdekében a felhasználók kellő információ nélkül is az érzelmekhez igazíthatják a megfelelő összetevőket [90].

Az attitűdök egymással is kölcsönhatásban vannak, és így komplex egészet alkotnak [91]. Ez azt is feltételezi, hogy bizonyos fokú konzisztenciának kell lennie közöttük. Mivel kapcsolatban állnak egymással, van köztük bizonyos fokú kompatibilitás, különben konfliktusba kerülnének egymással. Emellett az attitűd tanulható is. Az attitűdök többek között a valósággal kapcsolatos saját tapasztalataink, környezetünk, valamint a tömegkommunikációból, akár reklámokból szerzett információk alapján alakulnak ki. Közvetlen és közvetett élettapasztalatokból egyaránt származhatnak. Mivel az attitűdök tanulhatók, minél tovább fennmaradnak, annál erősebbek lesznek, vagy legalábbis annál ellenállóbbak a változásokkal szemben [92]. Eszerint az újonnan kialakult attitűdök könnyebben változnak és kevésbé stabilak, mint az azonos erősségű régiek [93].

Az attitűd tényezőinek, így a biztonságtudatosságra és viselkedésre ható tényezőknek a vizsgálatát további elméletek összetevőivel bontottam részekre, az alábbi elméleteket felhasználva. Bár eredetileg egészségügyben használták, jelen kutatáshoz is érdekes elemeket ad a védelemmotivációs elmélet (Protection-motivation theory, PMT), mely szerint az emberi védekezés alakulása két tényezőn alapul: a fenyegetés értékelésén és a megküzdés értékelésén. A fenyegetés értékeléskor az egyén felméri a helyzete súlyosságát, míg a megküzdés értékelése közben azt vizsgálja, hogyan reagálhat a helyzetre. A fenyegetettség értékelése tovább

bontható: a fenyegető esemény észlelt súlyosságát és az előfordulás vélt valószínűségét, sebezhetőségét elemzi. Ezekhez kapcsolódik a jutalom, amely a viselkedés megkezdésének vagy folytatásának pozitív aspektusaira utal. A fenyegetés értékelésének eredményét tehát az előbbi két tényező különbsége adja. A megküzdés értékelése az észlelt válaszhatékonyságból (vagyis az egyén azon elvárásából áll, hogy a cselekvés elvégzése eltávolítja a fenyegetést), és az észlelt önhatékonyságból (vagyis abból a meggyőződésből, hogy valaki képes az ajánlott cselekvési módok sikeres végrehajtására) áll. E két elemet a válaszköltséghez lehet hasonlítani, hogy az észlelt válaszhatékonyságot megkapjuk. A válaszköltség megmutatja, hogy mik az ajánlott viselkedés költségei a felhasználónak. Vagyis ebben a tényezőben az egyén képességeit és az erőfeszítéseit írhatjuk le [94]. Az elméletet többek között az alábbi tanulmányban használták információs rendszerek felhasználói biztonságának vizsgálatára [95]. Az elmélet értékes eredményeket mutathat nemzetenkénti összehasonlító vizsgálatoknál is [96], melyhez a jelen írás is hozzájárul, a magyar szempont elemzésével.

Összefoglalva, a védelemmotivációs modell, vagyis a védelemmotivációt alakító tényezők az alábbi módon írhatók le.

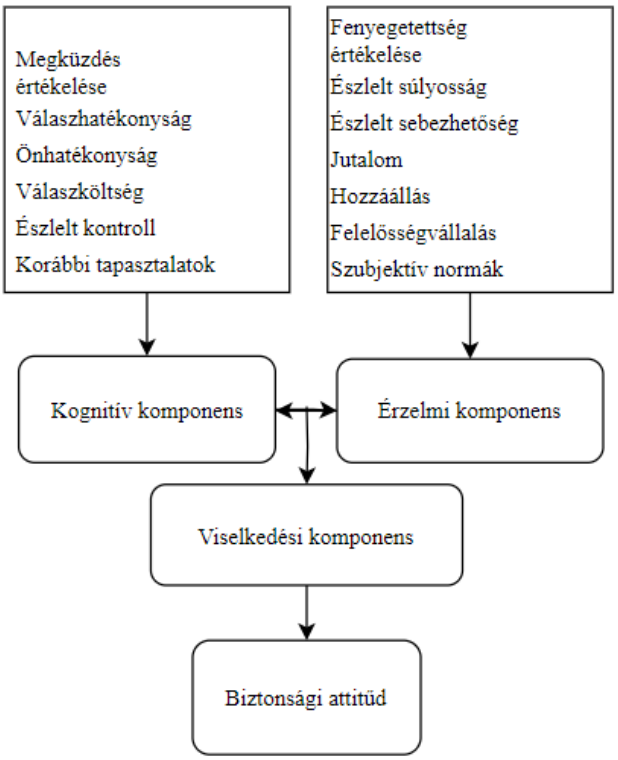
(Észlelt Súlyosság és Sebezhetőség) – Jutalom = Fenyegetettség Értékelése
(Észlelt Válaszhatékonyság és Önhatékonyság) – Válaszköltség = Megküzdés Értékelése

A tervezett cselekvés elmélete (Theory of Planned Behavior, TPB) szerint cselekvési szándékot, majd a tényleges cselekvést a viselkedéssel kapcsolatos attitűdök, a szubjektív normák és az észlelt viselkedési kontroll befolyásolja. Vagyis a felhasználói biztonság kérdésére értelmezve ez azt jelenti, hogy a biztonságra irányuló szándékot, majd cselekedeteket a biztonsággal kapcsolatos attitűd, az azzal kapcsolatos társadalmi elvárások és a biztonságra irányuló cselekvés észlelt nehézsége határozza meg [97]. Fontos megjegyezni, hogy az itt megjelenő attitűd egy álatalánosabb hozzáállást jelöl, nem a fent elemzett részletes kibontású attitűd fogalomra vonatkozik. Későbbi munkájában Ajzen [98] tovább definiálja az észlelt viselkedési kontrollt, két összetevőre, az észlelt önhatékonyságra és az észlelt kontrollálhatóságra bontva azt. Előbbi arra vontakozik, hogy önmaga szerint mennyire hatékonyan tudja az adott cselekvést elvégezni a felhasználó, utóbbi pedig a felhasználó által érzett kontrollt mutatja. Mivel több kutatás is úgy találta, hogy a szubjektív normák hatása a legkisebb az előrejelezhető tervezett cselekvésre, a kérdőívben ez a komponens kapta a legkisebb szerepet [99], [100]. Az eredeti modellt további elemekkel, mint a pszichológiai tulajdon (*psychological ownership*) és korábbi tapasztalat egészítették ki, melyek

hozzájárulnak a biztonságra irányuló cselekedetek értelmezéséhez. (Ezen kívül a kiegészített modellben a szubjektív norma mellett a leíró norma is, előbbi a felhasználó meggyőződése arra vonatkozóan, hogy mások akarják-e, hogy biztonságra irányuló viselkedést mutassanak, utóbbi pedig arra utal, hogy a felhasználó mit gondol arról, hogy más felhasználók hogyan gondoskodnak az eszközeinek védelméről. Azonban a már említett okok miatt egyik norma szempont sem jelenik meg a végleges kérdőívben [101].) További kutatásokban [102] megjelenik a biztonsággal kapcsolatos tudatosságon túl a felhasználó informatikai fejlettsége és az akár társadalomba, akár technológiába vetett bizalma is, mint biztonsági viselkedést befolyásoló tényezők. Ezen tényezőkről a kérdőívbe szintén került kérdés.

A fenti elméletekben tehát megfigyelhetők bizonyos párhuzamok, melyeket a kérdőív összeállításánál is figyelembe vettem. Az alábbiakban az attitűd elmélet elemeit a védelemmotivációs elmélet és a tervezett cselekvés elméletének elemeivel vetettem össze. Feltételezésem szerint a kognitív és érzelmi komponensek, vagyis hogy mit tud és mit érez a biztonságról a felhasználó, az az alábbi önbevalláson alapuló tényezőktől függ. Fontos megemlíteni, hogy bár a biztonságról való tényleges tudás is mérhető lenne, a személyes attitűddel kapcsolatban inkább a felhasználó saját maga által értékelt tudása a mérvadó, hiszen az attitűd alakulása belső folyamat. Az ezekhez kapcsolódó viselkedési komponenssel együtt a három tényező alkotja a felhasználó biztonsági attitűdjét.

A kutatási logikát a 2. ábra mutatja be. A minőség érdekében számos különböző biztonsággal kapcsolatos tanulmányt vettem figyelembe, amelyek az általam is használt PMT és TBP modellekre épültek. Ezeket saját gondolatmenetem és az attitűdelemek mentén kiegészítve használtam fel a kérdőív kialakításánál [103], [101], [104], [105], [106], [107]. Ennek érdekében más kutatók egyes kérdéseit, akik a modellt alkalmazták vizsgálataik során, átvettem és beépítettem a kérdőívembe. Az átvett kérdésekre jellemzők, hogy nem az attitűdelméletre, hanem az említett modellekre vonatkoznak. Az első számú mellékletben találhatók a kérdőív kérdései, melyben az egyes kérdések mellett a vonatkozó modell elemeket, valamint a vonatkozó szakirodalmat is feltüntettem. A felhasználók biztonságtudatossága három fő módon mérhető: (1) kérdőívekkel történő felmérés, mely során a felhasználó saját bevallása szerint értékelik a tudatosságát, (2) valódi viselkedés elemzése alapján, esetleg (3) kérdéses helyzet szimulációja alapján történő felméréssel. A jelen kutatás az első csoportba tartozik, vagyis a saját bevalláson alapuló tudatosságot és viselkedést méri.



2. ábra Kutatási logika- Saját szerkesztés

Egyes tanulmányok szerint [108] azonban ezek mindig kontextus függők is (így például ez a jelen írás egyik korlátja is, mely általánosságban vizsgálódott és nem vette figyelembe a kontextust). Bár a kérdőív biztonságra való koncentrálása torzíthatta az eredményt, egy tanulmány szerint a mobil technológia alkalmazása általánosságban, valamint különösen a munkahelyen, pozitívan befolyásolta a munkavállalók explicit biztonsági ismereteit, valamint a biztonsági kultúrájukat (viselkedési szempontból és a biztonsággal kapcsolatos attitűdök tekintetében) [109]. Ez tehát egyszerűsítve azt felételezi, hogy a mobil eszközök használata már önmagában magasabb biztonságtudatossággal jár együtt.

3.3. Megoldási javaslatok a felhasználói biztonsági kockázatok csökkentésére

Az alábbi fejezetben a korábban ismertetett veszélyek mértékének csökkentésére vonatkozó javasolt megoldásokat mutatom be. Először szabályozási, majd applikáció gyártói, szolgáltatói, végül egyéni felhasználói szempontokat figyelembe véve, megvizsgálva, hogy az értékláncban résztvevő szereplők hogyan tudnak hozzájárulni a biztonságosabb applikációhasználathoz. Mivel vállalati környezetben is egyre gyakoribb a munkavállaló saját mobil eszközének használata (BYOD), a vállalati biztonsági szempontokat is említhetném, a téma lazán való kapcsolódása miatt azonban ezt nem teszem. Az alábbi felsorolás a kérdőívben a viselkedési

attitűd komponenshez kapcsolódó kérdések alapjául szolgált. Fontos megemlíteni, hogy bár a szabályozásra, valamint az alkalmazásfejlesztési eljárásokra a felhasználónak kevesebb ráhatása van, az ezekről való tudás növelheti a biztonságtudatos alkalmazáshasználatot.

3.3.1. Szabályozás szükségessége

A technológiai fejlődést nehéz szabályozással is lekövetni, sok esetben csak később válik nyilvánvalóvá, hogy milyen veszélyeket is rejthetnek az újítások. Az internet szabályozása megosztó kérdés: a idealista felfogás szerint a tömegkommunikáció és nyilvánosság egy minőségileg jobb, önszabályozó tömegdemokrácián alapuló platformot hozhat létre, melyben az állami szabályozásnak nincs helye. A realisztikusabb, népszerűbb elképzelés szerint azonban szükséges a szabályozás, hiszen az interneten keresztül is megoszthatók törvénytelen tartalmak, az interneten keresztül bonyolított kommunikációnak is lehet valós térben érzékelhető hatása. „Az internet nem jogmentes terület, az internetes kommunikációban tanúsított emberi magatartások és formák a jogi szabályozás tárgyát képezhetik. Alkotmányossági szempontból tehát az új technológiák által nyújtott tereken és felületeken, valamint kommunikációs csatornákon – így az interneten zajló nyilvános kommunikációban érvényesítendők az Alaptörvényben rögzített alapvető jogok és kötelezettségek” [39, p. 186]. A szabályozásnak számtalan új kihívásra kell választ találnia: nem csak a hatalmas mennyiségű adat gyűjtésének, kezelésének szabályait, hanem például az ennek segítségével történő személyre szabásból adódó szűrőbuborék-problémát, vagy az álhírek szűrését is meg kell oldani. Bármilyen témájú applikáció használatával nagy mennyiségű személyes adat keletkezik, mely tudatos rossz szándék hiányában is lehetőséged adhat hibákra, visszaélésre.

A mobil appoknál megjelenő adatvédelmi kockázatok két fő területről származnak: a személyes mobil eszközökön futó szoftverek, applikációk jellegéből, valamint a mobilapp fejlesztési és elosztási környezet sajátosságaiból. Az ENISA (European Union Agency For Network and Information Security) szerint [110] többek között az alábbi faktorok adják a kockázatokat. Mobileszközökben tárolt adatok és szenzorok sokfélesége: mivel a mobil eszközeink életünk részét képezik, nagy mennyiségű személyes adatot tárolnak, amely további hatalmas mennyiségű, az elérhető szenzorok segítségével (pl. GPS, mikrofon, kamera) létrejött adattal egészülnek ki. Személyes eszközökről van szó, melyek mindig a felhasználóval vannak. Sokféle azonosítóval is rendelkeznek (hardver azonosítók, mint például IMEI, MEID/ESN, UDID, Wifi MAC cím, valamint konfigurációk, metaadatok, stb.), melyek újabb lehetőségeket nyitnak a követésre és profilozásra. Ebbe a kategóriába tartozik a *device fingerprinting* (kb. eszköz ujjlenyomatának meghatározása), mely az előbb említett azonosítók, az operációs

rendszer, a böngésző típusa és verziója, valamint a nyelvi beállítások és IP cím segítségével igyekszik a felhasználó profilját megalkotni és a felhasználót online követni. Ez a módszer egyébként egyes kutatások szerint akár 97%-os megbízhatósággal alkalmas a felhasználó azonosítására [111], így jól belátható kockázatokat rejt. A mobil eszközök magától értetődően mobilok, hordozhatók és mindig csatlakoznak is hálózatokhoz, amely egyrész a követést, másrészt a megfigyelést és a potenciálisan érzékeny személyes adatokra való következtetést is lehetővé teszi. Korlátozott fizikai biztonság: a kis méretből és mobilitásból fakadóan ezek az eszközök könnyedén ellophatók és megrongálódhatnak, ami újabb biztonsági és adatvédelmi kockázatok forrása lehet. Ezen kívül nehézséget okozhat az is, hogy az eszközhöz fizikailag sokan hozzáférhetnek a felhasználón kívül is. Korlátozott felhasználói felület: a kényelem érdekében kisebb méretű képernyők meglepő kockázatokat is jelenthetnek. Egy kutatás szerint például a mobil eszközökön létrehozott jelszavak sokkal gyengébbek, mint más eszközökön létrehozottak [112], de az is belátható, hogy a felhasználó kevésbé tudja kényelmesen elolvasni és átlátni például az adatvédelmi és adatkezelési tájékoztatókat, így könnyebben járulhat hozzá olyanhoz, amit alapos átolvasás után lehet, hogy nem tenne. Applikáció fejlesztők korlátai: a mobil app fejlesztésnél a biztonság és adatvédelem csak egy a sok megoldandó probléma közül és sok esetben a fejlesztők nincsenek tisztában az ezekkel kapcsolatos elvárásokkal. Sok esetben -a legjobb szándékkal együtt is- a komplex kihívások miatt a vonatkozó előírások és szabályok betartása nehéz feladat. Harmadik féltől származó szoftverek használata: az előző pontot magyarázza az is, hogy az appfejlesztők gyakran dolgoznak harmadik féltől származó, már elkészített funkciókkal, könyvtárakkal a felhasználó követésére, elkötelezettségének mérésére, melyeket ha több app használ együtt, az adatok akár összeköthetők a harmadik félnél. Applikációk piaca: az appokat legtöbbször az alkalmazásboltokból töltik le a felhasználók. Ezek a területek azonban nem egységes szabályok alapján működnek, ki szigorúbban, ki engedékenyebben hagyja, hogy szinte bárki applikációt oszthasson meg rajtuk keresztül, amely sok lehetséges kockázatot rejt. Az is fontos szempont, hogy az alkalmazás boltok hozzáférnek a felhasználó által letöltött alkalmazások listájához, amiből következtetni lehet a felhasználó életének egyes aspektusaira. Felhő alapú tárhelyek: az applikációknál, főleg a *quantified self* mozgalmat támogató appoknál jellemző a felhőn való adattárolás, melyből szintén kockázatok származnak. Itt a szolgáltató oldaláról fontos a megfelelő adatvédelem és a felhő biztonsága. Online közösségek: sok applikáció ad lehetőséget arra, hogy a felhasználó önkéntesen megossza adatait más felhasználókkal összehasonlítás, motiváció céljából. Ez bár a felhasználó saját akaratából történik, szintén adatvédelmi és biztonsági kockázatokkal jár.

Az egyre gyakrabban, néha botrányokkal nyilvánosságra került visszaélések csökkentésére és a felhasználói adatgyűjtés és felhasználás átláthatóságának növelésére jött létre néhány éve a következőkben bemutatott GDPR (2016/679 EP), magyarul Általános Adatvédelmi Szabályozás, amely szabályozza a személyes adatok védelmét jogalkotási szinten és amely közvetlenül alkalmazandó a tagállamokban, és meghatározza azokat a feltételeket, amelyek mellett az uniós polgárok üzleti célokból kezelhetik a személyes adatokat [113]. A szabályozás szerint személyes adatnak minősül minden olyan adat, amely alapján egy ember közvetetten vagy közvetlenül azonosítható, ilyenek a külső fizikai, kulturális, társadalmi jellemzők, például név, cím, e-mail cím, fénykép, egészségügyi információk, jövedelem, szexuális irányultság vagy politikai nézetek. (Ezek közül néhány speciális kategóriába tartozik, ami azt jelenti, hogy még érzékenyebbnek számítanak (például biometrikus azonosító adatok, szexuális orientáció vagy egészségügyi információk, a faji, etnikai, vallási és politikai hovatartozás), ezért ezekre még szigorúbbak a szabályok [114].) Ezek alapján belátható, hogy minden vállalat és minden applikáció is kezel személyes adatokat, így a GDPR hatálya alá esnek: mindenkire vonatkozik, aki az EU területén működik, aki EU-s polgárok adatait gyűjti, tárolja, feldolgozza, tartózkodási helytől függetlenül [115]. Ez azért fontos, mert az online térben tisztázza az elvárásokat.

A szabályozás alapján a személyes adatokat a következő elvek szerint kell kezelni [116]:

- Jogszerűség, tisztességes eljárás és átláthatóság: a személyes adatok kezelését az érintettek számára átláthatóan, emellett jogszerűen és tisztességesen kell végezni.
- Célhoz kötöttség: csak meghatározott, egyértelmű és jogszerű célból gyűjthető, ezen célokkal összeegyeztethetően kezelhető személyes adat.
- Adattakarékosság: az adatkezelési célok figyelembevételével csak a szükséges adatok gyűjthetők.
- Pontosság: az adatoknak naprakésznek és pontosnak kell lennie.
- Korlátozott tárolhatóság: csak annyi ideig tárolhatók, ameddig a célok elérését segítik. Ennél hosszabb ideig csak közérdekű archiválás, tudományos és történelmi kutatás, valamint statisztikai célok érdekében lehet eltérni.
- Integritás és bizalmas jelleg: a kezelés során érvényesülnie kell ezen elveknek is, akár technikai, akár szervezési megoldások segítségével.
- Elszámoltathatóság: az adatkezelő felelős a szabályozásnak való megfelelésért és ennek igazolásáért is.

Mit jelent az adatot törvényesen, jogszerűen gyűjteni és feldolgozni? A kulcs a világos, átlátható kommunikáció és beleegyezés kérése. A szervezeteknek világosan kommunikálniuk kell, hogy kik ők, miért kérnek adatokat, meddig tárolják és kiknek továbbíthatják azokat. Meg kell szerezniük az felhasználók egyértelmű, megerősítő beleegyezését is ahhoz, hogy feldolgozhassák ezeket az ügyféladatokat. Az ügyfeleknek tudniuk kell, hogy adataikat például profilalkotási vagy marketing célokra használják-e fel [117]. Ha viszont a felhasználótól olyan adat gyűjtésére kérnek engedélyt, ami nem felel meg a célhoz kötöttség és pontosság elvének, akkor a kifejezett hozzájárulása ellenére sem szabályos annak gyűjtése. Ajánlott az adatkezelési hozzájárulások kérését különválasztani az applikációval kapcsolatos egyéb beleegyezést kérő nyilatkozatoktól. Az adatgyűjtés törvényes indoklásait lehetnek, ha szerződés teljesítéséhez, a szervezet jogi kötelezettségeinek teljesítéséhez szükséges, vagy ha a szervezet vagy a nyilvánosság érdeke [118]. Ez alatt például egy kamera alkalmazás jogos hozzáférését értjük az eszköz kamerájához és a mentés érdekében annak memóriájához. (Azonban például a marketingtevékenység, a reklámozás nem számít szigorúan szükséges tevékenységnek, így erre más szabályok vonatkoznak.) Az alkalmazásszolgáltatók általában az engedélyarchitektúra (*permission architecture*) alapján férhetnek hozzá az eszköz, felhasználó és szenzoros adatokhoz. Ez a következő módokon történhet a gyakorlatban. Lehet az operációs rendszer által megszabott engedélyarchitektúrát használni (elérhető API-k), amelyeknél a fejlesztőnek az operációs rendszer előírásainak kell megfelelni. Ebben az esetben maga az operációs rendszer gondoskodik róla, hogy a felhasználót informálva az jóváhagyja a hozzáféréseket, amely hozzájárulhat az átláthatóbb és szabályozásnak megfelelő működéshez. Lehetőség van a felhasználóktól direkt interakciókkal is engedélyeket kérni. Sok esetben azonban problémás helyzeteket eredményezhet, ha harmadik fél szolgáltatásait is igénybe veszik, ugyanis nem jellemző az azokra vonatkozó külön engedélyek kérése. Ezeken túl a metaadatok és felhasználói viselkedés vizsgálata is személyes adatokhoz való hozzáférésnek számít [110]. A felhasználó számára ajánlott az átláthatóság biztosítása érdekében több helyen is elérhetővé tenni az adatgyűjtésre vonatkozó leírásokat: az applikációban az adatvédelmi irányelvek leírásánál, külön linken, a hozzáférés engedélyezéseknél, valamint az applikációban már használatkor is. Fontos megemlíteni a gyermekeket is, ha egy szervezet 16 évesnél fiatalabb személytől gyűjt adatokat (vagy, mivel tagállamonként változhat, egyes tagországokban akár 13 évesnél), akkor szülői beleegyezéssel kell rendelkeznie [117]. Ez applikációk esetében tovább bonyolítja a helyzetet. Az értékláncban általában nem csak a felhasználó és a vállalat vesz részt, így komplexebb szerepleírásokat is tartalmaz a szabályozás. Többek között definiálja az érintett, az adatkezelő, az adatfeldolgozó, valamint az adatvédelmi

tisztviselő (Data protection offcer- DPO) szerepeket, valamint rendelkezik a felügyeleti hatóságról is [114], [119]. Az érintetteknek joguk van hozzáférni (egy szervezetnél tárolt) adataikhoz, módosítani őket, vagy megosztani őket egy másik céggel. Joguk van kérni az adatkezelőket (akiknek meg kell kérniük az adatfeldolgozót), hogy töröljék az érintettre vonatkozó összes információt. Mint már említettem, joguk van tudni, hogy adataikat profilalkotási és marketing célokra használják-e, melyeket meg is tagadhatnak. Mivel az adatszivárgások, lopások már viszonylag gyakori jelenségek, az is szabályozott, hogy ilyen helyzet esetén az érintettet mihamarabb, de legkésőbb 72 órán belül a felfedezése után, értesíteni kell [117]. Szerepeket tekintve általában az elsődleges adatkezelő az alkalmazásszolgáltató, ha a felhasználók adatait saját célra dolgozza fel. Sok esetben az app szolgáltató ugyanaz, aki az appot fejleszti is, mely esetben szintén adatkezelőként jár el (de az is előfordul, hogy az szolgáltatók megbíznak a fejlesztéssel külsős cégeket). Több adatkezelő is lehet abban az esetben, ha az applikációban olyan adatközpontú funkciókat használnak, melyek harmadik féltől származnak, így náluk is megjelennek az adattal kapcsolatos kötelezettségek. Ezen kívül pedig az operációs rendszer is gyűjthet adatokat, így az azokat szolgáltatók is adatkezelőknek tekinthetők. Adatfeldolgozók az előbb említett példában lehetnek a szolgáltató által megbízott app fejlesztők, de ebbe a csoportba tartoznak például a későbbiekben is említett felhőszolgáltatók, akik az app szolgáltatók felügyelete alatt dolgozzák fel a felhasználók adatait [110]. Mint látjuk, a rendelet több olyan kérdéssel foglalkozik, amelyek korábban kissé ködösek voltak, és egyértelmű jogokat és felelősségeket ad az érdekelt feleknek. A szervezeteknek azonban nem csupán az átláthatóság miatt kell megfelelniük, más motivátorok is vannak: súlyos pénzbírsággal sújthatják őket mulasztás esetén, akár az éves globális forgalom 4% -áig, vagy 20 millió euróig, attól függően, hogy melyik a nagyobb, nem is beszélve hírnevükről, amelyet negatívan befolyásolhatnak az ilyen események. (A többszintű megközelítés miatt alacsonyabb összegű bírság is meghatározható a különböző megsértett pontok esetében.) [120] Hazánkban a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) jár el a GDPR-ban foglaltakkal kapcsolatban, a hatóságnál lehet a témában tájékozódni, adatvédelmi tisztségviselőt vagy incidenst is bejelenteni.

Természetesen országonként is vannak erre vonatkozó előírások. Magyarországon az Alaptörvény előírja a személyes adatok védelméhez való jogot, de az ezzel kapcsolatos részletek a 2011. évi CXII. Törvény tartalmazza az információs önrendelkezési jogról és az információszabadságról [121], melyet a GDPR megjelenése után összhangba is hoztak azzal (2018). Érdemes még megemlíteni a hamarosan életbelépő ePrivacy rendeletet, ami az

elektronikus hírközlési adatvédelmi irányelv (2002/58/EK irányelv) felváltója lehet [122]. Ennek központjában az elektronikus kommunikációs szolgáltatók állnak, célja az adatvédelem és a kommunikáció bizalmasságának elősegítése a felhasználók (vállalati és magán) védelme érdekében. Ez tehát valamivel szélesebb körű szabályozás, vonatkozik például a kommunikáció metaadataira vagy a felhasználó készülékének adataira is, de a tervezet célja a sütikre vonatkozó előírások tisztázása, szigorítása is. Mivel az említett esetekben is történik személyes adatkezelés is, a GDPR-ral összehangolt tervezetről van szó, melyekben a hatóságok hatásköre összeérhet. Fontos kulcsszó a biztonság szemléletű tervezés (*security by design*), ami azt jelenti, hogy bármely termék, szolgáltatás, folyamat, stb. fejlesztésének kezdetétől fogva a szervezeteknek szem előtt kell tartaniuk az adatvédelmet, a biztonságot és a GDPR-t, ami megkönnyíti a megfelelést és csökkenti a biztonsági események kockázatát (amelyek magukban foglalják a személyes adatok elvesztését vagy törlését, valamint a személyes adatok jogosulatlan megosztását vagy hozzáférését). A rendelet megjelenésétől kezdve tehát már az app ökoszisztéma résztvevőire kötelezően vonatkoznak az itt ismertetettek. Alkalmazásokra vonatkozóan tehát az alapvető kérdés, hogy dolgoz-e fel személyes adatot, melyre a válasz nagy valószínűséggel lesz igen. Az fentiekben láthattuk, hogy nem csak a felhasználó, de az eszköz adatai is személyes adatnak számítanak, így ez még biztosabb. Csak ha ezen adatokat teljesen anonimizálják, akkor nem vonatkozik rájuk a GDPR. Egy másik megoldás az álnevesítés (pszeudonimizáció), mely „a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni” [123]. A felhasználókról szóló képek és metaadatok nem érzékeny adatok, hacsak nem fednek fel a felhasználóról olyan információkat, amelyek már a speciális kategóriába tartoznak (például látható a képről az etnikai hovatartozás, akár egészségügyi helyzet), mely esetben védelmet igényelnek. Hasonló a helyzet a helyadatoknál, figyelembe kell venni a feldolgozásnál az szükségesség és arányosság kérdését, ezért a legtöbb mobil operációs rendszer már lehetővé teszi a helyadatok használatának átlátható kezelését és engedélyezését a felhasználó részéről.

Biztonságot tekintve a fent leírt adatvédelemre vonatkozó szabályozásokkal szemben inkább csak ajánlásokat találhatunk, melyekből viszont számtalan áll rendelkezésre. Ezek főleg az

applikációk készítői számára elérhető irányelveket tartalmaznak a gyakori hibák kiküszöbölésére, azonban ezek használata, kombinálása az ő döntésük.

3.3.2. Megfontolások applikáció fejlesztésnél

Applikációk fejlesztésénél a már korábban leírt okok miatt számtalan készen elérhető kódrészletet kaphatnak a fejlesztők, melyek hatással vannak a biztonsági kérdésekben való döntésekre is. Ugyanakkor a már említett biztonság szemléletű tervezés is fontos szerepet játszik, a lehető legkorábbi lépésektől a biztonságot folyamatosan szem előtt tartva érdemes az alkalmazást alakítani. Ezen kívül a fejlesztők segítségére lehetnek még bizonyos szabványok és ajánlások is, melyekből számtalan szervezet megoldásai közül választhat a fejlesztő. Szabványok közül a hazánkban egyik legismertebb az ISO (*International Organization for Standardization*), vagyis Nemzetközi Szabványügyi Szervezet, mely számos területen, a biztonság és az egészség témájú appok kapcsán is szolgál opcionálisan megvásárolható standard megoldásokkal és leírásokkal. Létrehozták többek között az ISO/TR 17522:2015, Egészségügyi informatika — Mobil/okoseszközök egészségügyi alkalmazásaira vonatkozó rendelkezések című jelentést, mely az okoseszközökön alapuló egészségügyi ellátással kapcsolatos fejlesztésekről és szabványokról szól [124], elérhető az ISO/TR 21835:2020 Egészségügyi informatika — Naponta generált személyes egészségügyi adatok, amely a mobil egészséggel kapcsolatos adatgyűjtésről és adathasznosításról szól. A dokumentációban további számos a témában releváns standard hivatkozása található [125]. Elérhető még a 2021-ben létrehozott ISO/TS 82304-2:2021-t, Egészségügyi szoftver – 2. rész: Egészségügyi és wellness alkalmazások is [126]. A világ számos egészségügyi szervezete által meghatározott alkalmazásokra vonatkozó irányelveket és követelményeket egyesítve és azokra építve biztosítja az appok biztonságosságát, megbízhatóságát és hatékonyságát. Elérhetők mobil applikációra vonatkozó például biztonságot, tesztelést leíró standardok a NIST (*National Institute of Standards and Technology*) ajánlásában [127] is, mely USA központú szervezet. Biztonsággal foglalkozik még például a már említett OWASP szervezet is [128], mely egy online közösség, amely ingyenes, nyilvánosan elérhető cikkeket, módszertanokat, dokumentációt és technológiákat készít a webalkalmazások biztonsága érdekében. A nyílt forráskódú összetevők a szoftverfejlesztés szerves részévé váltak, ezek biztonságközpontú fejlesztése a szervezet célja. Számos anyag érhető el a fejlesztők számára mobil alkalmazásokkal kapcsolatban is, szintén nem csak készítés, de tesztelés témában is. A fentieken kívül kifejezetten egészségügyi applikációkkal, esetleg azon belül konkrét betegségekkel foglalkozó appokkal kapcsolatos ajánlások is elérhetők, például a WHO vagy

egyéb nemzetközi szervezetek, egyes országok egészségügyi szervezetei, de akár nagy mobil szolgáltatók vagy egyetemek által javasolt irányelvekkel.

Értelemszerűen már az applikációk készítésénél figyelembe kell venni a fent említett szabályokat és a folyamat elejétől azok tudatában kell dolgozni. A strukturált átgondolást és tervezést segíti a GDPR által adatkezelőnek előírt adatvédelmi hatásvizsgálat (*data protection impact assessment* vagy DPIA), amely a személyes adatok gyűjtéséből és feldolgozásából származó kockázatokat azonosítja. Akkor kötelező, ha az adatkezelés „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve" [129]. Bár a rendelet nem fejti ki részletesen, de a leírások alapján a DPIA szükséges, ha az adatkezelő a gyűjtött adatokat profilozásra, értékelésre (például profilalkotásra is) használja, amelyre az éritettel kapcsolatos döntések épülnek, vagy ha nagy mennyiségben kezel különleges kategóriába tartozó adatokat (például egészségügyi adatok), esetleg nyilvános helyet figyel meg módszeresen, nagy méretben [129]. Appoknál, főleg egészségügyi téma esetében tehát nagy valószínűséggel szükség lesz erre. Alkalmazható a logika akár kódrészletekre, harmadik féltől származó könyvtárakra is. Ahogy már említettem, a kezdetektől fontos megtenni, de a fejlesztés és fejlődés során újra és újra el lehet végezni, ha változások vannak a technikai design-ban vagy az adatgyűjtésben. Kivitelezést, módszereket tekintve sok javaslat létezik különböző szervezetektől és kutatóktól, azonban mindnek vannak közös pontjai, melyek a már említett ENISA ajánlás alapján a következők [110].

- Adatvédelmi alapelvek tiszteletben tartása: a már előzőekben említett elvek betartását jelenti. Az appok csak az igazolható célnak megfelelő adatokat, csak jogszerűen és átláthatóan kérhetik, gyűjthetik, és szükséges az érintettek hozzáférési, helyesbítési és törlési jogainak biztosítását elősegítő funkciók létrehozása is.
- Az alkalmazás / szolgáltatások / rendszer kontextusának leírása: szükséges a feldolgozási rendszer, a célok, a gyűjtött, feldolgozott, továbbított adatok, támogató eszközök és ezekkel kapcsolatos kockázati források meghatározása.
- Fenyegetettségek felmérése: a nem megfelelő adatgyűjtésből, feldolgozásból származó kockázatok elemzését jelenti, mint például a személyes adatok vétlen megsemmisítése, elvesztése, illetéktelenek számára való hozzáférhetősége (például ha a felhasználó nem tud róla, hogy adatait harmadik félnek is továbbítják, melyből sok botrányos példát láthattunk korábban a hírekben).
- Kockázatértékelés: minden nem kívánatos eseményre, amiket az előző pontban meghatároztak, ki kell számolni az előfordulás valószínűségét és a lehetséges hatásai

súlyosságát. Érdemes kiemelt figyelmet szentelni a kockázatos események adatvédelmi, személyiségi jogokat érintő hatásainak a DPIA elemzés során annak funkciójából adódóan.

- Kockázatkezelés: a kockázatok azonosítása és értékelése után meg kell határozni a lehetséges módokat azok minimalizálására, kiiktatására például technikai és szervezési lehetőségek segítségével. A nem elkerülhető, fennmaradó kockázatokat pedig, valamennyi éritett számára világossá kell tenni, ideértve a felhasználót is.

Ha már elkészült az alkalmazás az ajánlások, standardok és biztonság szemléletű fejlesztés figyelembevételével, következő lépésként publikálják azt. Az Apple híres a szigorúan ellenőrzött technológiai ökoszisztémáról, amely egyedülálló kontrollt biztosít a vállalat számára a szolgáltatások és a biztonság felett. Minden alkalmazás szigorú Apple-jóváhagyási folyamaton megy keresztül, hogy ne tudjanak az appok jogosulatlanul bizalmas információt gyűjteni, és hogy ne férjenek hozzá olyan rendszerelemekhez, ahová más típusú rendszerekben bejuthatnak. Gyakorlatilag minden szakértő egyetért abban, hogy az iOS lezárt jellege megoldott néhány alapvető biztonsági problémát, és hogy ezeknek a korlátozásoknak az alkalmazásával az iPhone-nak sikerül szinte minden megszokott rosszindulatú szereplőt távol tartania. (Amikor azonban a hackereknek sikerül betörniük, az Apple rendkívüli védelme végül a támadókat védi, ugyanis ezen szigorú hozzáférés korlátozások miatt nagyon nehéz felfedezni, hogy hol rejtőznek. Ha viszont a rendszer bizonyos szintű nyitása mellett döntenének, értelemszerűen megnyílik az ajtó a rosszindulatú szereplők számára is, amit kihasználhatnak. Ezen kívül köztudott, hogy a vállalat rég óta szeretné elkerülni, hogy a felhasználóit például kiadja a kormányoknak vagy például az FBI-nak, amely szintén a nyitás ellen szól [130].) Bár kevésbé szigorú rendszer, de a Google Play is nagy figyelmet fordít arra, hogy elkerülje a fertőzött, rosszindulatú appok publikálását. Ezt többek között a Google Play Protect, alkalmazásboltba beépített malware védelemmel igyekeznek elérni, amely gépi tanuláson alapul és minden nap automatikusan ellenőrzi az összes Android-telefonon található alkalmazást, és megakadályozza a káros alkalmazások telepítését [131]. Ez a szűrés kiegészül még az Androidra épülő gyártói kiadások által végzett plusz biztonsági szűréssel is, például a Xiaomi esetében egy alkalmazás letöltésénél nem csak a Google Play Protect, de a Xiaomi MIUI is végez szűrést.

3.3.3. Mit tehet a felhasználó?

A felhasználó oldaláról javasolt védekezési, biztonságnövelési lépéseket a veszélyek sorrendjében ismertetem, vagyis alkalmazással kapcsolatos, web-alapú, vezeték nélküli hálózatokkal és végül hozzáféréssel kapcsolatos fenyegetések szerint.

Elsők tehát az alkalmazással kapcsolatos lehetőségek. A felhasználóknak a fenyegetések tudatában érdemes elkerülni az olyan alkalmazásokat, amik nem hivatalos applikációáruházakból származnak, ezeknél ugyanis megnő a fertőzöttség veszélye. A sideloading és a feltört applikációk, valamint a nem megfelelő konfigurációval rendelkező eszközök kerülése jó kezdő lépés lehet. Ahogy már említettem azonban, az áruházakban elérhető appok sem feltétlenül biztonságosak, az onnan történő rosszindulatú programot vagy hátsóajtót tartalmazó applikációk elkerülésére a legjobb megoldás a tájékozódás lehet. A megbízhatóságra utalhat például egy applikáció neve, ha ismertebb vállalat alkalmazása vagy ismertebb fejlesztők kiadványa. Azonban például a letöltések száma vagy rangsorokban elfoglalt hely alapján nem határozható meg a biztonság, előfordul, hogy megbízhatónak, hitelesnek tűnő applikációról sok letöltés után derül ki, hogy valójában rosszindulatú programot tartalmazott. Érdemes megtekinteni a véleményeket, a kevés vélemény, esetleg rossz funkcionalitásról, sok rejtett pluszköltségről szóló hozzászólás is jelezhet problémát (például adware jelenlétére utalhat). Mivel sokszor szükség van az appnak jogosultságra, hogy végrehajtsa például trójaiként a feladatát, fontos mindig ellenőrizni, hogy letöltéskor az applikációnak milyen engedélyeket adunk, valamint érdemes megnézni, hogy mi áll az adatvédelmi tájékoztatóban és milyen általános felhasználási feltételekhez járulunk hozzá. Ezeket az engedélyeket már az alkalmazás telepítése után is érdemes néha átfutni és felülvizsgálni, ugyanis sok applikációnál például alapértelmezett, hogy használhatja a kamerát, lokációt vagy mikrofont, ami beláthatóan szintén kockázatot jelenthet. A felülvizsgálat során azokat érdemes engedélyezni, amik az applikáció funkcióinak kihasználásához beláthatóan szükségesek. Akár a vírusirtók használata is ajánlott lehet, bár a gyakorlatban ez a legkevésbé elterjedt védekezési módszer mobil eszközöknél (nem vállalati környezetben). Gyakran nehéz észrevenni, hogy az okoseszköz megfertőződött. Erre utalhat, ha például a mobil elkezd látszólag ok nélkül lelassulni, ha több idő kell az appoknak, hogy betöltsenek, ha gyorsabban merül az akkumulátor, ha feltűnően gyakrabban lát a felhasználó felugró hirdetéseket, ha esetleg olyan alkalmazást fedez fel telefonján, amit nem is ő töltött le, vagy olyan adatforgalmat vesz észre, amelyet nem ő generált, esetleg ha váratlanul magas telefonszámlája érkezik. Az egyéb és nulladiknapos sebezhetőségeket kihasználó támadások esetében a legegyszerűbb

védekezés a gyakori frissítés. Magát az operációs rendszert és az applikációkat is rendszeresen, az új verziók megjelenésekor vagy bizonyos időközönként érdemes frissíteni, ezen új verziók célja ugyanis a feltárt sebezhetőségek, problémák kiküszöbölése. Összefoglalva tehát az applikációkkal kapcsolatos védekezési lehetőségek a következők. Ha egy rossz döntés következtében mégis például zsarolóvírust tölt le a felhasználó, érdemes a fontosabb fájlokról minden esetben biztonsági mentést készíteni erre az esetre, hogy ezek probléma esetén se vesszenek el.

- Hivatalos alkalmazásáruházak használata,
- Körültekintő alkalmazás letöltés,
- Vírusirtó használata,
- Rendszeres és gyakori frissítések,
- Appok hozzáféréseinek kritikus engedélyezése és ellenőrzése,
- Biztonsági mentés készítése.

A következő nagy csoport a web-alapú fenyegetések volt, melyeket ahogy már említettem, az átlagos felhasználó nehezen tudja észrevenni. Viszont szinte minden esetben az emberi hiba is szükséges ezek sikerességéhez, ezért az alábbiakban a social engineering támadások (például adathalászat és spam segítségével való fertőzés) elleni javasolt védekezést mutatom be. Mivel legtöbbször ezek a támadások e-mailen keresztül érkeznek, erre koncentrálok, de fontosnak tartom megemlíteni a közösségi médiát is, hiszen azt is gyakran használják a felhasználók és szintén jó lehetőséget ad a támadóknak. Az erős spamszűrők segíthetnek megszűrni, hogy milyen levelek érkeznek a felhasználóhoz. Ha valamilyen nem megfelelő tartalom átjut, például a Gmail-ben, ha átmozgatja a felhasználó spam kategóriába az e-mailt, ezt követően megkérdezi a rendszer, hogy az összes hasonló tartalmút oda mozgassa-e azon túl, ami további segítség lehet a szűrésre. Ha viszont mégis átjut egy rosszindulatú e-mail, az alábbi intő jeleket érdemes figyelni. A levél tartalmát tekintve gyakori a sürgetés, hirtelen cselekedetet elváró felszólítás, nagyon közeli lejáratú akció, olyan válaszra adott kérdés, amit fel sem tett a felhasználó, esetleg adománygyűjtés. Ezek mind azt segítik, hogy a címzett vagy jószándékkal vagy gyorsan, a valósság kérdésének logikus átgondolása nélkül kattintson például egy adott linkre vagy töltsön le egy fájlt. Tehát egy pillanatra érdemes lenyugodni és átgondolni a kapott sürgős kérést. Gyanús lehet a sok helyesírási hiba, magyartalan fogalmazás is. Mivel ezek a támadások gyakran külföldről érkeznek, így előfordulhat, hogy fordítóprogramokat használnak, és bár ezek minősége egyre jobb, még mindig könnyen kiszúrhatók egy nyelvet jól ismerő számára. A túl általános megszólítás is utalhat erre, bár ez önmagában nem

használható jelként. Mindig gyanakvásra adhat okot, ha adategyeztetést, jelszóváltoztatást kér tőlünk egy szolgáltató e-mailen keresztül, vagy ha bárki értesít, hogy valamit nyertünk. Előbbinél például a szolgáltatóval érdemes telefonon egyeztetni, hogy valós-e a kérés vagy a saját honlapjukról megtenni a kért lépéseket, nem az e-mailben kapott linkre kattintva. Csatolmányoknál érdemes átgondolni, hogy a címzett vár-e csatolmányt és számít-e egyáltalán olyan e-mailre, amiben a csatolmány érkezett. Bár ezek egyszerű kérdések, gyakran az emberi kíváncsiság miatt figyelmen kívül hagyják őket a felhasználók. A levél tartalmán túl gyanús esetekben árulkodó lehet a feladó címe, ahhoz képest megjelenített neve is. Előfordul, hogy a kettő nem egyezik, a megjelenített név például egy bank neve, a valós cím azonban teljesen más. Lehetséges az is, hogy bár a kettő egyezik, de apró hibák vannak az e-mail címben, ami jelzi, hogy nem az a feladó, akit a támadó szeretne elhitetni (például helpdesk@gooogle.com, ami egy sietős, figyelmetlen felhasználónak akár fel sem tűnik). A valós és megjelenített link összehasonlítása is hasznos lehet, ugyanis ott is elrejthető például egy egyértelműen rosszindulatúnak tűnő link. Levelezést tekintve, ha vállalati szempontból vizsgáljuk, fontos a magán és vállalati célú levelezések különválasztása. (Bár általában belső szabályozás tiltja is, de a magán levelezésen való fájlmegosztás is kockázatos lehet.) Az ilyen típusú támadások felismerését megnehezíti a támadások növekvő mértékű személyre szabása. Ennek egyik jó forrása lehet a közösségi média, melyen a nyilvánosan elérhető megosztott adatok a támadók számára is értékesek lehetnek. A platformok és felhasználók, valamint az egyes felhasználó ismerősei közötti bizalmat kihasználva egyrészt onnan szerezhető információkkal is, de magán a platformon is lehetséges a támadás a már említett módokon. Ezt elkerülendő érdemes a profilt nem nyilvánossá tenni, és minél kevesebb adatot megadni magunkról (mert az ismerősök kevésbé biztonságos profilján keresztül még elérhetőek lehetnek fontos információk). Például a felhasználó helyzetmegosztásából kiderülhet, hogy hol tartózkodik épp, az érdeklődési kör megadásával pedig a támadók „témaválasztása” lehet könnyebb. Azoknak a támadóknak pedig, akik jól értenek a kommunikációhoz és a befolyásoláshoz, ezek már elegendők lehetnek egy sikeres támadáshoz. Vállalati szempontból külön jó információforrásnak számíthat a LinkedIn, ezért azt is körültekintően érdemes használni. Összefoglalva tehát az alábbi intő jeleket kell figyelni a támadások elkerülése érdekében.

- Beérkező üzenet tartalma: témák lehetnek sürgető felhívások, jótékonyság, jelszócsere, adategyeztetés, jellemzőek a helyesírási hibák, általános megszólítások
- Üzenet egyéb tulajdonságai: gyanús feladó, gyanús linkek és csatolmányok. Megjelenített információ nem egyezik a valós információval.

- Közösségi média: személyre szabás forrása, ezért a lehető legkevesebb adatot érdemes megosztani.

Mindezek mellett fontos megjegyezni, hogy az emberi hibák sok esetben az alapvető jóindulatból származnak, az áldozatok sokszor nem is feltételeznek rossz szándékot a másik oldalon, főleg ha az kedvesen közeledik. Számtalan olyan videó érhető el például Youtube-on is, ahol néhány perces kedélyes csevegés után több részletben a felhasználók megosztják az interjúztatóval a jelszavukat. Tudatossággal és a fenti módszerek ismeretével azonban ez a kockázat jelentősen csökkenthető.

A következő nagy csoport a vezeték nélküli kapcsolatok fenyegetései volt. Felhasználó szempontjából néhány egyszerű lépéssel is növelhető a biztonság. Ebben a kategóriában két szempontból védekezhet a felhasználó: egyrészt védheti a saját vezeték nélküli hálózatát, másrészt a biztonságot szem előtt tartva csatlakozhat más hálózatokhoz. A nyilvánosan elérhető routerekről többek között az SSID (*service set identifyer*) is elérhető a nyilvánosság számára. Ez alapértelmezetten az eszköz modelljének gyártó által adott neve, melyekhez az interneten elérhető a beállított alapértelmezett jelszó is. Azonban ehhez gyakran meg sem kell nézni a típust, az admin, Admin, valamint password és jelszó próbálkozásokkal szinte biztosan sikerrel járhatunk. Tehát az SSID és a jelszó megváltoztatásának elmulasztásával bárki csatlakozhat a felhasználó saját hálózatára, amivel a már említett támadások sorát teszi lehetővé. Kevésbé praktikus, de megoldás lehet a whitelisting (fehér lista) is, mely esetben a felhasználó meghatározhatja, hogy ki csatlakozhat a hálózatához. A saját mobil eszközön megnyitott hotspot-ot tanácsos csak a legszükségesebb ideig bekapcsolva tartani, valamint erős jelszóval védeni azt. A másik oldalt vizsgálva, vagyis amikor a felhasználó csatlakozik mások hálózatához, fontos a körültekintés. Nyilvánosnak akkor nevezhetünk egy kapcsolatot, ha az nem titkosított vagy ha a jelszó bárki számára elérhető. Az ezen keresztül áramló kommunikáció könnyedén kompromittálható. Mivel egyes mobil operációs rendszerek csak az SSID valamint jelszó egyezését figyelik automatikus csatlakozás esetében, más azonosítókat, például MAC címet nem, így a támadók a megjegyzett nyilvános hálózatokhoz való csatlakozókat magukhoz csalhatják azok tudta nélkül. Innentől pedig beláthatóan könnyű befolyásolni vagy lehallgatni a kommunikációt, ami rajtuk keresztül folyik. Sok esetben a kényelem jegyében alapbeállítás az automatikus csatlakozás, növelheti a biztonságot ennek kikapcsolása, vagy csatlakozás helye szerinti korlátozása. Gyakori védekezési módszer a VPN (*virtual private network*), vagyis virtuális magánhálózat használata, amivel a forgalom már titkosított. [132] Előfordulhat azonban, hogy az alkalmazásboltokban ingyenesen elérhető

VPN menedzserek a már említett beépített hátsóajtóval vagy rosszindulatú fertőzéssel ellátott applikációk, így mindenképp érdemes megbizonyosodni a megfelelő forrásról.

Hozzáféréssel kapcsolatos fenyegetések ellen értelemszerűen a megfelelő erősségű, nem felhasználóhoz köthető PIN, Passcode és jelszó beállítás jelenthet védelmet. Ezeket erősítheti még az okostelefonon elérhető biometrikus funkciók használata is. A már említett korábbi, kutatásaimat megalapozó, egyetemi hallgatók körében történő vizsgálatom alapján a legismertebb kategóriák a biometrikus azonosítás kapcsán az ujjnyomat, a szem mintázatán alapuló megoldások és az arcfelismerés. A kitöltők saját bevallásuk szerint szeretik használni ezt a módszert, kényelmesnek és biztonságosnak tartják [79].

Végül érdemes a legújabb fenyegetésekkel tisztában lenni és követni a híreket, hiszen a tudás megvédhet az esetleges rossz döntésektől, csakúgy, mint a kritikus gondolkodás. Fontos azonban a fentieken túl azt is kiemelni, hogy az adatmegosztás mindig kockázatokkal jár, amik sokszor vissza nem fordítható károkhoz vezethetnek, így mindig érdemes megfontoltan cselekedni, 100% biztonság ugyanis sajnos nem érhető el. Erre megoldást jelenthet a pótolhatatlan adatok biztonsági mentése, mely bár nem minden okozott káron segít, enyhítheti a negatív hatásokat.

Adatvédelmi szempontból a felhasználóknak érdemes megismerni egy adott alkalmazás felhasználói feltételeit, adatvédelmi nyilatkozatait és az esetleges mobilon megnyitott weboldalakkal kapcsolatos süti tájékoztatókat is. Ezek ismerete ugyanis megvédheti a felhasználót az általa nem kívánatos adatmegosztástól, annak továbbításától.

3.4. Felhasználói szempont kiegészítése- Applikációk értékelése

Az alkalmazás boltokban egyes témákra keresve a felhasználó számára elérhető nagy számú találatból kiválasztani a legmegfelelőbbet nehéz feladat. Felmerülhet a kérdés, hogy mi alapján érdemes dönteni. A felhasználók számára legtöbbször viszonylag egyszerűsített döntéssegítő adatok állnak rendelkezésre, például a korábbi felhasználók értékelései (csillagszámban kifejezve és szövegesen), az alkalmazás boltban elért helyezése, valamint néhány applikációból elérhető képernyőfotó és összefoglaló a funkciókról. Ezek mindegyike befolyásolható, hogy kedvezőbb színben tüntesse fel a kínált appot. Nehezebb azonban eldönteni, hogy vajon ezek biztonságosak-e, adatkezelési szempontból vagy egészségügyi szakmai szempontból megfelelnek-e. A kritikus szempontok azonosítására és az azok figyelembevételével készíthető applikáció értékelésre már számos kutató próbált megoldást találni. Az alábbiakban a véleményem szerint legkiemelkedőbbeket említem a teljesség igénye nélkül, melyek

szempontrendszere megfelel az általam fontosnak tartott szempontoknak. Ezek az értékelő rendszerek különösen fontosak lehetnek a hobbi témájú egészséggel kapcsolatos applikációknál, ugyanis ezekre nem vonatkoznak annyira szigorú előírások, mint a komolyabb témájú appokra. Ezért, bár a legtöbb említett rendszer a komoly egészségügyi appokra vonatkozik, javasolt lehet a hobbi célú alkalmazásoknál (akár nem egészség témakörben is) ezeket használni a minőség és megbízhatóság érdekében. Érdekes, hogy a biztonság és adatvédelem kérdése nem minden modellben jelenik meg annak ellenére, hogy napjaink megkerülhetetlen kérdése lett, különösen egészségügyi adatokra vonatkozóan. Fontos, hogy nem mindegyik felhasználói szempontú elemzésnek készült, mégis úgy gondolom, hogy a végfelhasználóknak is érdemes lenne az alábbiakat ismerni és az alkalmazás választás és használat közben is figyelembe venni.

- Mobilalkalmazás értékelési skála (*MARS- Mobile App Rating Scale*) [133],
- Mobil egészség applikáció megbízhatósági ellenőrző lista (*MHAT- Mobile Health App Trustworthiness Checklist*) [134], [135],
- Átláthatóság a bizalomért (*T4T- Transparency for Trust*) [136],
- Mobil egészség applikációk standard javaslata [137].

Összefoglalva, e modellek javasolt összegzéseként a következő területeket kell felmérni annak megállapításához, hogy egy alkalmazás elég jó-e a használathoz, melyeket egy gyakorlati elemzésen keresztül bemutatva publikáltam. Az alábbi szempontrendszereket a kérdőív készítése során is felhasználtam [138].

- Használhatóság, beleértve a funkciót, az elkötelezettséget, az esztétikát. Ebben a kategóriában a cél annak vizsgálata, hogy az alkalmazás könnyen használható, intuitív, szórakoztató, tetszetős, testreszabható, megfelel-e a célnak és a célközönségnek stb.
- Tartalom, beleértve az átadott információ minőségét, előnyöket, háttér kutatást, megfelelőséget és alkalmasságot. Ez a kategória tartalmazhat kérdéseket a mérésekről, az alkalmazás tartalmát megalapozó kutatásokról, az alkalmazás alátámasztott előnyeiről stb.
- Biztonság, adatvédelem, átláthatóság. Ez megmutathatja az alkalmazás használatának lehetséges kockázatait, a felhasználók védelme érdekében hozott biztonsági intézkedéseket, valamint az adatkezeléssel kapcsolatos, adatvédelmi kérdéseket, az adatvédelmi szabályzat megírását, az alkalmazás hogyan védi a felhasználói adatokat stb.

- Kiadók: hasznos lehet a felhasználók számára, ha több információval rendelkeznek az alkalmazásszolgáltató szervezetéről, annak hírnevéről, márkájáról, esetleges üzleti érdekeiről, valamint az alkalmazás szerzőiről, esetleg fejlesztési jellemzőiről.
- Technikai támogatás és frissítések: melyek általában létfontosságúak az alkalmazás használhatóságához.
- Technológia: az alkalmazásnak jól kell működnie, nem pazarolhat erőforrásokat stb.

A fentiekből tehát látható, hogy milyen sokszínű szempontrendszereket lehet figyelembe venni egy alkalmazás letöltése előtt, valamint annak használatakor. Sajnos, bár mindegyik értékes a felhasználónak, ezen információk sok esetben nem érhetők el, nem elég átláthatók, amely hiány szintén beszédes lehet a felhasználónak. Annak tudatában, hogy ezek a szempontok léteznek és érdemes lehet őket, vagy a rájuk utaló jeleket keresni, máris tudatosabb applikáció használók lehetünk. Bár a már említett szabályozások nagy mértékben védik a felhasználókat, önmaguk védelmében saját felelősségük sem elhanyagolható.

A fenti módszereket gyakorlatban egy alkalmazáson tesztelve megállapítható, hogy az említett szempontokról rengeteg hasznos információ deríthető ki az adatvédelmi szabályzatokból és felhasználási feltételekből, így azok megismerése sokat tehet a felhasználói tudatosságért. Érdekes eredményeket hozhat az alkalmazás tudományos hátterének vagy gyártó, szolgáltató cégének vizsgálata is, melyek sokszor hosszas kutatás után lelhetők csak fel [138]. (Ami például egy egészséggel, fitnesszel kapcsolatos alkalmazás esetén sok kérdést felvet.) Bár az értékelő rendszerek egyfajta kombinációjának vagy bármely egyéni értékelő rendszernek a használata nagy mennyiségű információval szolgálhat a felhasználóknak az alkalmazás minőségéről, a valóságban általában nem vesznek figyelembe ilyen sok szempontot, mielőtt a letöltik az alkalmazást. A reálisabb megközelítés az lenne, ha ezeket az értékeléseket a szolgáltatók végezhetnék el, amelyek eredményei akkor jelennének meg, amikor egy alkalmazást bemutatnak a felhasználóknak (például az információs oldalakon vagy az alkalmazást, szolgáltatást támogató webhelyeken). Egy másik megoldás lehet, hogy az ilyen típusú alkalmazásokat ajánló, például egészségügyi személyzet elvégzi az értékelést, és az eredmények alapján ad ajánlásokat. Még ha ezek az alkalmazások nem is túl komoly egészségügyi alkalmazások, komolyabb kritériumokkal történő értékelésük értékes információkat ad a felhasználóknak, és növeli a megbízhatóságot, ha elérhetők [138].

4. REPREZENTATÍV KUTATÁS EREDMÉNYEI

Az alábbiakban a korábbi kutatások és a megalkotott hipotézisek alapján létrehozott kérdőíves kutatásom eredményeit mutatom be, mely három fő részből áll. A kérdőívet a szakirodalom, korábbi kutatásaim és a saját gondolatmenetem szerint, az attitűdelemek mentén alakítottam ki, a következő kuatatások figyelembevételével [103], [101], [104], [105], [106], [107].

- 1. Biztonsági attitűd kognitív és érzelmi elemeire vonatkozó metrikus skálát alkalmazó kérdések, melyek a védelemmotivációs és tervezett cselekvés modellek elemeit is tartalmazzák, beleértve az ellenőrzést, a tudást, a képességet, a tudatosságot, az energiabefektetést, a biztonság kérdésének értékelését, az észlelt kockázatot és a bizalmat. (A dolgozat 3.2 fejezetében kifejtettek alapján, a területen elérhető hivatkozott kutatások figyelembevételével kialakított kérdések, melyek az 1. mellékletben található 1-15. kérdések.) Ez a szakasz szolgált a főkomponens elemzés, valamint az az alapján történő klaszterelemzés alapjául.
- 2. Viselkedési attitűdelemre vonatkozó kérdések, melyek önbevalláson alapulnak. (A dolgozat 3.3 fejezetében kifejtettek alapján létrehozott kérdések és válaszlehetőségek, melyek alapja a szakirodalmi kutatás, valamint saját szakmai tapasztalatom. Az 1. mellékletben található 28-30. kérdések.) Az első szakasz segítségével kialakított klasztereket a második szakaszban található kérdések segítségével elemeztem tovább, megismerve így a kitöltők teljes biztonsági attitűdjét.
- 3. Ellenőrző, visszacsatoló kérdések, valamint néhány egészséges életmód alkalmazásra vonatkozó kérdés. (1. mellékletben található 16-27, valamint 31. kérdések.) A harmadik szakasz kérdéseinek elemzésével elmélyíthettem a létrehozott klaszterek megismerését, valamint visszaigazolhattam a kapott válaszok konzisztenciáját is. A mobil egészség témájú kérdések a témához való hozzáállást, a használatot, majd az abból származó viselkedés módosítását, végül a COVID-hoz való viszonyt vizsgálják a felhasználóknál.

Az alábbiakban, a kutatási kérdések sorrendjét követve, a minta és kérdőív általánosabb bemutatása után először megvizsgálom, hogy helyes-e a feltevésem, miszerint az egészség és életmód appok ugyanolyan felhasználói megítélés alá esnek biztonság szempontjából, mint más applikációk (hiszen azok különlegesen szenzitív, egészségre vonatkozó adatokat is tartalmazhatnak). Ezután a kognitív és affektív attitűdelemekkel kapcsolatos főkomponens elemzést mutatom be, melyek alapjai a kérdőív elején található skálás kérdések. A főkomponensek azonosítása után a kapott komponensek mentén a kitöltőket csoportokra

osztom, majd a csoportokat az attitűd harmadik pillére, vagyis az önbevallott viselkedés mentén is elemzem. Ezután további elemzéseket végzek a felhasználói csoportok jobb megismerésére demográfiai és egyéb szempontok szerint. Kitérek néhány ellenőrző kérdésre, melyek célja a válaszok konzisztenciájának ellenőrzése és végül néhány egészség és életmód alkalmazással kapcsolatos kérdésre is.

A felmérésben 525 magyarországi kitöltő vett részt (online, a már említett Ipsos Instant research igénybevételével). A válaszadók 18 és 65 év közöttiek (munkaképes korúak), átlagéletkoruk 43,5 év (medián 44 év). A magyar lakossághoz képesti reprezentativitás megállapítására illeszkedésvizsgálatokat végeztem Khí-négyzet próbák segítségével. A nullhipotézis minden esetben az, hogy a két minta, tehát a magyar lakosság és a lekérdezésből származó minta, eloszlása adott szempontból megegyezik egymással. A KSH adataival [139] összevetve a Khí-négyzet próba eredménye a korcsoportokra vonatkozóan $p<0,001$, mely szerint a H0-t elutasítjuk 5%-os szignifikancia szint mellett, ami azt jelenti, hogy a minta korcsoport szerint nem reprezentatív a magyar lakosságra. Az 1. táblázatban az arányok megoszlása látható a mintában és a lakosságban a KSH 2022-es adatai alapján, melyen megfigyelhető, hogy arányaiban a két idősebb korosztályban történt arányfelcserélés a megkérdezett mintában a lakossági arányokhoz képest.

Korcsoport	Minta aránya	Lakossági arány
18-26	16%	15%
27-35	16%	18%
36-44	20%	21%
45-53	18%	23%
54-65	30%	23%

1. táblázat Korcsoportok megoszlása a mintában és a népességben. Saját szerkesztés

A válaszadók körülbelül fele nő (48%), fele férfi (52%), ami hasonló a magyar lakosság arányához. Az illeszkedésvizsgálat során megállapítottam, hogy a Khí-négyzet próba eredménye ($p=0,417$), mely szerint elfogadjuk a nullhipotézist, a két minta eloszlása egyezik. [140] Körülbelül egyharmaduk, 35%-uk Budapesten (fővárosban) vagy megyeszékhelyen él, további 33%-uk városokban, 32%-uk pedig községekben (szintén Magyarország lakosságához hasonlóan [141] a Khí-négyzet próba eredménye szerint ($p=0,208$), ahol a H0-t elfogadjuk.) A válaszadók majdnem egyharmada (31%) Budapestről vagy Pest megyéből származik. A második legtöbb kitöltőt (15%) az Észak-alföldi régió adta, a harmadikat (13%) a Dél-alföldi régió. A többi régió aránya 9 és 11% között mozog. A régió szerinti megoszlás esetében a Khí-négyzet próba eredménye $p=0,057$, mely szerint az eloszlások megegyeznek [142]. A kitöltők

kevesebb mint fele, 42%-uk főiskolai, egyetemi végzettségű vagy posztgraduális képzésben részesült, további 34%-uk pedig érettségit szerzett gimnáziumban vagy középiskolában. Ötödük, azaz a válaszadók 20%-a rendelkezik az informatikai területhez kapcsolódó végzettséggel vagy foglalkozással.

Összefoglalva, az illeszkedésvizsgálatok során megállapítható volt, hogy a reprezentativitás a KSH 2022-es adataihoz hasonlítva nemre, régióra és település méretére teljesül, de hasonló kor szerint is. Ezeket a 2. mellékletben található számítások igazolják.

4.1. Az egészség és életmód appok és azzal kapcsolatos adatok megítélésének vizsgálata

Amint korábban említettem, az előzetes vizsgálatok alapján feltevésem az volt, hogy hasonlóan viszonyulnak biztonság szempontból az egészség és a más egyéb applikációkhoz a felhasználók, melyet az 1. kutatási kérdésként azonosítottam. Az említett fókuszcsoportos megkérdezés során a megkérdezetteknek mobil egészség alkalmazásokból kellett választania több körben, majd megosztania a választási szempontjaikat. Azt találtam, hogy általában az alkalmazások hírneve, a saját előzetes ismereteik, elérhető vélemények és az alkalmazás külső jegyei alapján választanak. Befolyásoló még az elérhető funkciók listája is (melyekből túl sok is negatívan hathat a választásra). Azonban nem befolyásolta a választásokat az alkalmazások engedélykérése, nem vettek figyelembe biztonsággal kapcsolatos szempontokat a választás során saját bevallásuk szerint [13]. A feltevés tehát a következő volt.

> **H1**: A felhasználók alkalmazás használatában biztonsági szempontból különbség van az egészség témájú applikációk és bármilyen más témájú alkalmazás között.

Az állításomat úgy teszteltem, hogy a kérdőív elején található skálás kérdéseket (1-15. kérdések az 1. mellékletben) összevetettem azon válaszadókkal, akik használnak és akik nem használnak egészséggel kapcsolatos alkalmazásokat. A Mann-Whitney U próba segítségével vizsgálva egyik kérdésnél sem volt szignifikáns az eltérés (eredmények a 6. mellékletben), kivéve a „fontos számomra, hogy ha a közösség érdeke úgy kívánja, akár lemondjak személyes adataim feletti kontrollomról (például COVID alatt)” (1. melléklet/14.) kérdésre adott választ. Esetében a próba eredménye ($p= 0,030$) volt, vagyis szignifikáns összefüggés van a kérdés válaszai és az egészséggel kapcsolatos alkalmazás használat között. Akik nem használnak ilyen appokat, jellemzően nagyobb mértékben nem értenek egyet ezzel az állítással (bár leginkább ez jellemző a mintára általánosan is). Ez tehát azt jelenti, hogy ezen kívül a válaszadók hasonlóan viszonyultak a kérdésekhez akkor is, ha használtak és ha nem használtak ilyen

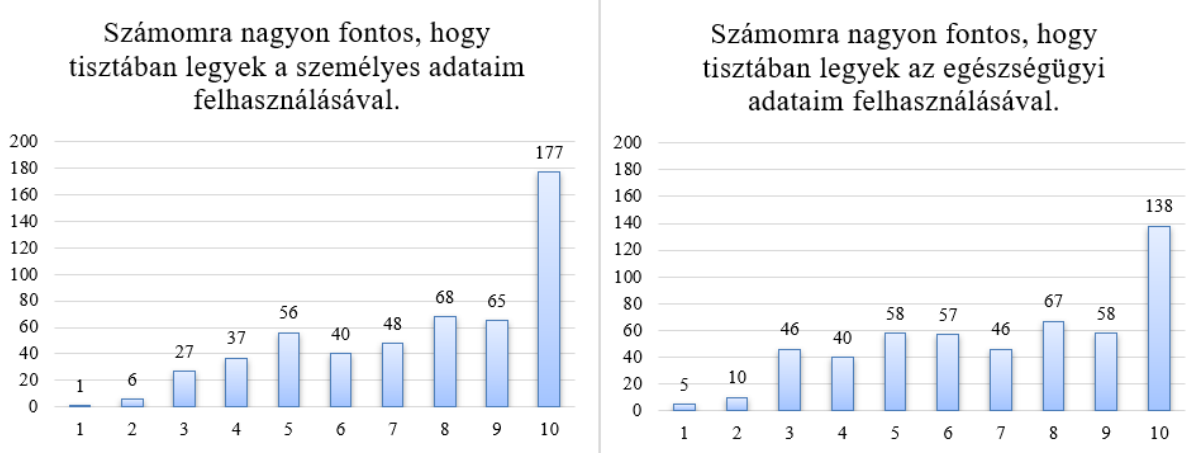
appokat (vagyis ugyanúgy használják az alkalmazásokat biztonsági szempontból). Az olvashatóság érdekében a 3. mellékletben található ábrán a kérdésekre adott átlagos válaszok láthatók az egészség app használattal összevetve, amiből megállapítható, hogy a legtöbb kérdésnél valóban nagyjából egyeznek a válaszok átlagai mindkét esetben. Érthető módon a COVID-hoz, mint megosztó témához, nem egyértelmű a kitöltők viszonya. Figyelembe véve, hogy ez egy elég speciális témakör, úgy tekintem, hogy a többi kérdésnél megfigyelhető eredmények igazolják az első hipotézisemet.

Az egészséggel kapcsolatos adatokhoz való hozzáállást még egy módon elemeztem, ugyanis a skálás kérdések között néhány kérdés különbséggel a válaszadók két kérdésre is válaszoltak (1. melléklet/ 4. és 13. kérdések):

- Számomra nagyon fontos, hogy tisztában legyek a személyes adataim felhasználásával.
- Számomra nagyon fontos, hogy tisztában legyek az egészségügyi adataim felhasználásával.

Mint látható, a különbség a két kérdés között az egészségügyi hangsúly. A két kérdés esetében normalitásvizsgálattal megállapítottam, hogy a válaszok nem követnek normális eloszlást, ezért a nem paraméteres Wilcoxon próbát használtam. Az eredmény szerint ($p<0,001$) a két kérdésre adott válaszok eloszlása szignifikánsan különbözik egymástól. Az alábbi 3. ábrán láthatók a válaszok alapján alkotott hisztogramok, melyek függőleges tengelyén a gyakoriság, vízszintes tengelyén pedig a válaszlehetőségek értékei látszanak. A második kérdésnél, vagyis az egészségügyi adatok esetében a válaszok jobban megoszlanak, mint a személyes adatoknál. Ebből tehát arra lehet következtetni, hogy az egészségügyi adatok a válaszadókat jobban megosztó adatok. A személyes adatoknál érdekes módon sokkal több válaszadó értett egyet, hogy nagyon fontos nekik az állítás, az egészségügyi adatoknál ezek az arányok elmaradtak a másik kérdéshez képest. Ez tehát azt jelenti, hogy a személyes adatok esetében sokkal inkább védelmezőnek tűntek a felhasználók, mint az egészségügyi adataikkal (mely egyfajta személyes adat). Mivel az előző kérdésben inkább a fitnesz témájú applikációkról volt szó, a két eredmény kiegészítheti egymást (hiszen azokba nem kerülnek bele túl érzékeny egészségügyi adatok). Összefoglalva tehát látható, hogy az egészségügyi adataikat nem tekintik érzékenyebb adatoknak a felhasználók, mint általában a személyes adataikat. Ez egy másik szempontból, de szintén alátámasztja a feltevésemet, miszerint a felhasználók alkalmazás használatában biztonsági szempontból nincs különbség az egészség témájú

applikációk és bármilyen más témájú alkalmazás között (tehát H1-et elvetem, vagyis elfogadom a H0-t).



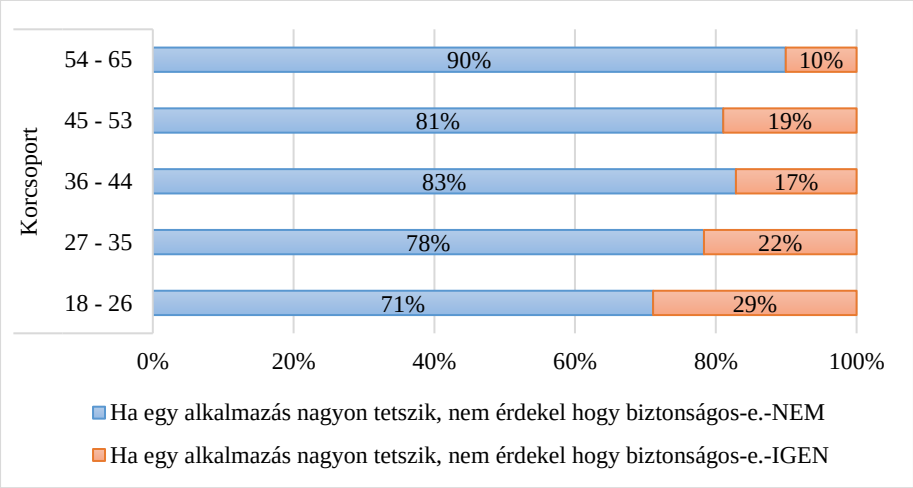
3. ábra Személyes adatok felhasználása vs. egészségügyi adatok felhasználása hisztogramok. Saját szerkesztés

Ez alátámasztja a logika helyességét, hogy nem szükséges egészség témájú alkalmazásokra szűrni a kérdőívet.

4.2. A kérdőív általános összefüggései

A következőkben a válaszadói biztonsági attitűdök vizsgálata előtt néhány érdekesebb összefüggést mutatok be a kérdőívből. Először néhány egyszerű kérdést, majd a biztonsági incidensek hatását vizsgálom, végül néhány COVID témájú kérdést elemzek.

Először a „ha egy alkalmazás nagyon tetszik, nem érdekel hogy biztonságos-e” (1. melléklet/16.) kérdésre adott válaszokat vetettem össze a korral, majd az iskolai végzettséggel. A kérdés és a kor kapcsán az volt a feltevésem, hogy minél idősebb a kitöltő, annál inkább érdekli a biztonság, mert a fiatalabbak biztosabban mozognak a technológia világában.

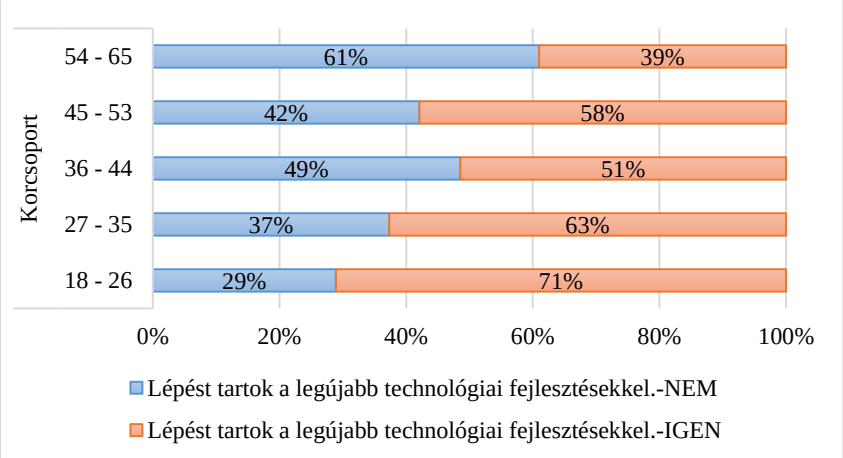


4. ábra „Ha egy alkalmazás nagyon tetszik, nem érdekel hogy biztonságos-e.” kérdés korcsoport szerint. Saját szerkesztés

A hipotézisemet Khí-négyzet próbával vizsgáltam, melynek eredménye p=0,006, vagyis elfogadom, hogy szignifikáns összefüggés van a kor és a biztonság fontosságának megítélése között a kérdésben foglaltak szerint. Ahogy az a 4. ábrán is látható, a fiatalabbak nagyobb arányban értettek egyet a kérdéssel az idősebb válaszadókhoz hasonlítva.

Ugyanezt a kérdést az iskolai végzettséggel is összevetettem és szintén Khí-négyzet próbával teszteltem. Az eredmény szerint p<0,001, vagyis szignifikáns összefüggés van az iskolai végzettség és a biztonság fontosságának megítélése között a kérdés szerint. (A kérdésnél a mintaelemszám miatt a 8 általános vagy alacsonyabb iskolai végzettségű és a szakmunkásképző, szakiskola (érettségi nélkül) végzettségű csoportot összevonva vizsgáltam, érettségi nélküli csoportként.) Míg az érettségi nélküli csoportnál a válaszadók 29%-a értett egyet azzal, hogy ha egy alkalmazás tetszik neki, nem érdekli, hogy biztonságos-e, addig ugyanez az arány a gimnáziumi és szakközépből származó érettségivel rendelkezőknél már csak 20%, a főiskolai és egyetemi végzettségűeknél pedig 10%. Tehát a magasabb iskolai végzettségűek kevésbé értenek egyet az állítással, mint az alacsonyabb iskolai végzettségű válaszadók.

Ezután azt vizsgáltam, hogy a válaszadók saját bevallásuk szerint lépést tartanak-e a legújabb technológiai fejlesztésekkel, követik-e az ezzel kapcsolatos híreket (1. melléklet/18.). A kérdést kor és nem kapcsolatai szerint vizsgáltam. A feltevésem szerint a fiatalabb korosztályok nagyobb mértékben gondolják magukat technológia követőnek, ahogy az a 5. ábrán látható. A Khí-négyzet próba eredménye p<0,001 szerint szignifikáns összefüggés van a kor és a technológiai fejlesztésekkel való lépéstartás között. Érdekes, hogy az előző kérdésnél és ennél is a 45-53 éves korosztálynál a mintázat kissé megtörik, az ő korcsoportjuk jobban hasonlít a 27-35 év közötti korosztály válaszaira, mint idősebb társaikéra.



5. ábra Technológiai lépéstartás kor szerinti megoszlása. Saját szerkesztés

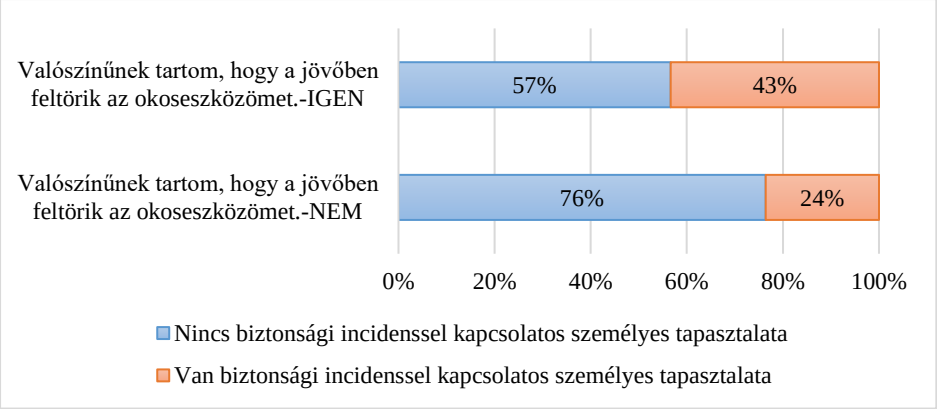
A kérdés és a nem kapcsolatát is vizsgáltam Khí-négyzet próba segítségével, mely eredménye szerint (p=0,002) szignifikáns összefüggés van a nem és a technológiai lépéstartás között. A férfiak 60%-a, a nők 47%-a tart saját bevallása szerint lépést a legújabb technológiai fejlődésekkel.

A „valószínűnek tartom, hogy a jövőben feltörik az okoseszközömet" (1. melléklet/19.) kérdést is vizsgáltam, először nem szerint. A feltevésem az volt, hogy a nők nagyobb arányban tartják valószínűnek, hogy feltörik az eszközeiket. A Khí-négyzet próba eredménye szerint, p=0,054, ezt elvetem, azonban egy megengedőbb 10%-os szignifikancia szint mellett az eredmény szignifikáns lehetne. Ezután a kérdést összevetettem az IT területen szerzett végzettség vagy munkatapasztalat meglétével (1. melléklet/27.). A Khí-négyzet próba szerint p=0,004, vagyis szignifikáns összefüggés van aközött, hogy a válaszadó valószínűnek tartja-e, hogy feltörik a jövőben az okoseszközét és az IT jártassága között. Az IT jártassággal rendelkezők nagyobb arányban tartják valószínűnek ezt (45%), míg az IT jártassággal nem rendelkezőknél kevesebben (30%).

A kutatási terv során logikai sorrendben kialakított második fő kutatási célomhoz, vagyis a válaszadók biztonsági attitűdjének leírásához tartozó első feltevésem, H2 szerint a korábbi negatív tapasztalatok befolyásolják az alkalmazásokba vetett bizalmat, melyet az alábbiakban vizsgálok először ugyanehhez a kérdéshez kapcsolódóan.

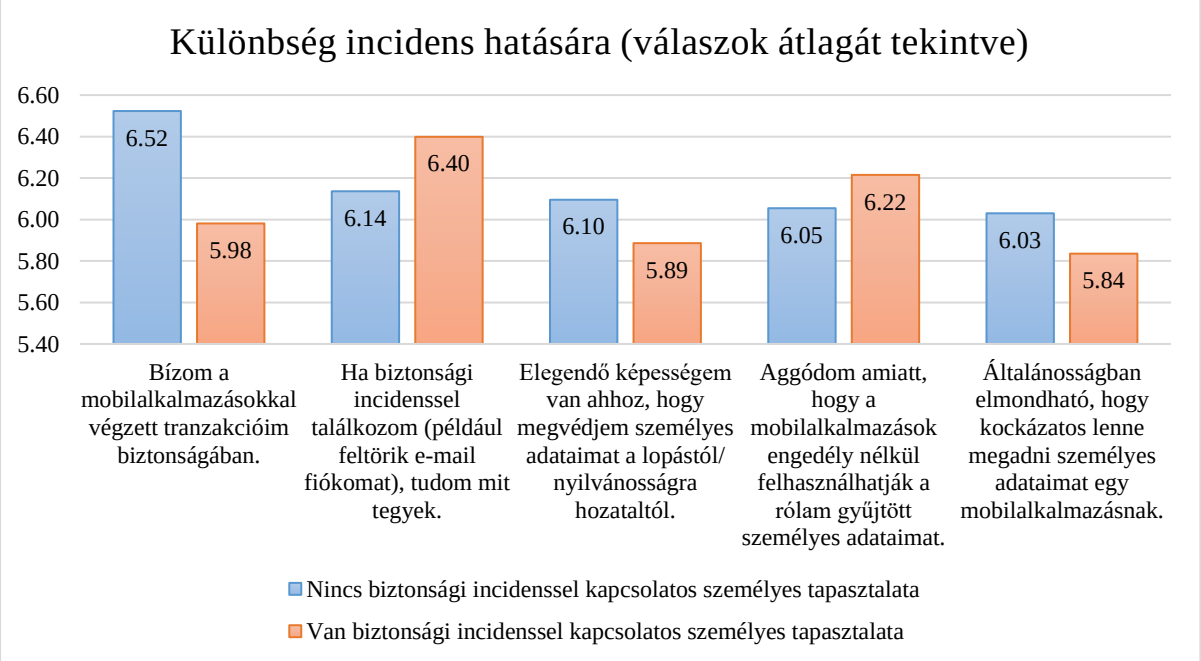
> **H2**: A korábbi biztonsági incidenssel kapcsolatos negatív tapasztalatok befolyásolják az alkalmazásokba vetett bizalmat.

Az előbbi kérdést összevetettem azzal, hogy volt-e a válaszadónak biztonsági incidenssel kapcsolatos tapasztalata. (Van biztonsági incidenssel kapcsolatos személyes tapasztalata? Például feltörték e-mail fiókját, közösségi média fiókját vagy online vásárlás során banki adatait ellopták.- 1. melléklet/31.) A feltevésem szerint, akinek van negatív tapasztalata, az nagyobb valószínűséget lát arra, hogy feltörik az eszközét a jövőben is. A Khí-négyzet próba eredménye szerint p<0,001 szignifikáns összefüggés van a korábbi tapasztalat és a kérdésre adott válasz között. Azok között, akik valószínűnek tartják eszközeik jövőbeli feltörését, nagyobb arányú a biztonsági incidens tapasztalattal rendelkezők száma (43%), mint akik ezt nem tartják valószínűnek (24%). Az eredményeket az 6. ábra szemlélteti.



6. ábra A jövőbeli feltörés kockázatának megítélése a negatív biztonsági incidens tapasztalat hatására. Saját szerkesztés

A következő, 7. ábrán néhány skálás kérdés átlagos válaszai látszanak rossz tapasztalattal rendelkező és nem rendelkező kitöltők esetén a további elemzés érekében. Látható, hogy akinek nincs biztonsági incidenssel kapcsolatos tapasztalata, az a kérdésekre adott válaszok átlagát tekintve jobban bízik a mobilalkalmazás tranzakcióiban, kevésbé aggódik az engedély nélküli adatgyűjtéssel kapcsolatban és nagyobb kockázatot érez. Érdekes módon a tapasztalattal rendelkezők nagyobb arányban tudják, hogy mit tegyenek ilyen helyzetekben, viszont kevésbé érzik magukat képesnek személyes adataik védelmére (ez adódhat abból is, hogy végül mégis áldozatul estek).

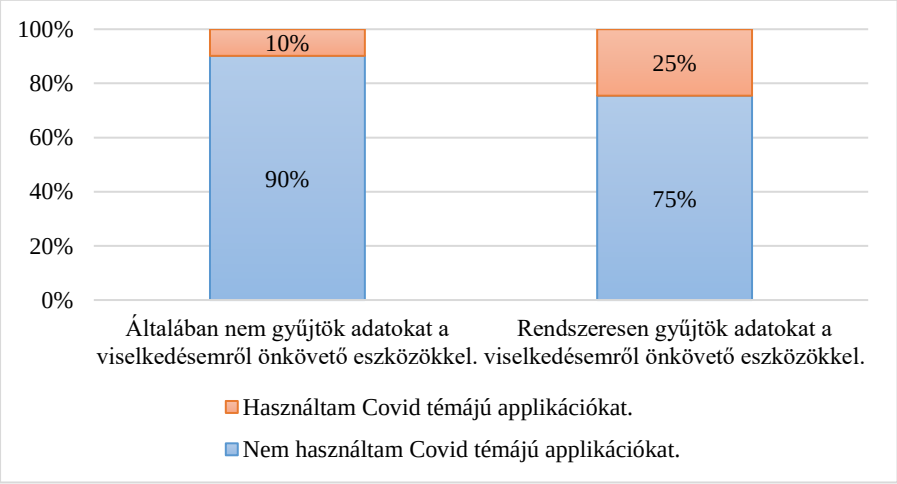


7. ábra Biztonsági incidenssel kapcsolatos tapasztalat hatása egyes válaszok átlagára. Saját szerkesztés

A szükséges normalitás vizsgálatok után a Mann-Whitney U próba szerint a felsorolt kérdések közül a „bízom a mobilalkalmazásokkal végzett tranzakcióim biztonságában” esetében

szignifikáns az eredmény (p=0,030), vagyis megállapítható, hogy szignifikáns különbség van az appok tranzakcióiba vetett bizalomban biztonsági incidenssel kapcsolatos tapasztalat hatására, a H2 hipotézist elfogadom. A részletes számításokat a 7. melléklet tartalmazza.

Az utolsó elemzett kérdéskör a COVID-dal kapcsolatos. Az első kérdés ebben a kategóriában a „COVID miatt lemondtam néhány korábban fontos jogomról" (1. melléklet/ 25.) volt, mellyel a válaszadók 71%-a nem értett egyet. Ez nem is mutatott szignifikáns összefüggést demográfiai szempontokkal, tehát egységesen inkább nem értenek egyet ezzel a válaszadók. A kérdést azonban összevetettem azzal is, hogy használt-e a válaszadó COVID témájú applikációkat (1. melléklet/ 26. kérdés). A Khí-négyzet próba eredménye szerint, p<0,001, szignifikáns összefüggés van a COVID miatti jogokról való lemondás megítélése és a COVID alkalmazás használat között. Az ilyen alkalmazást használók 64%-a értett egyet az állítással, miszerint lemondott néhány korábban fontos jogáról, míg az ilyen applikációkat nem használóknál ez az arány mindössze 23%. Összesen a válaszadók 16%-a használt ilyen alkalmazásokat, de ez egyik demográfiai szempontból sem mutatott szignifikáns összefüggést. Megfigyelhető volt azonban, hogy aki a „rendszeresen gyűjtök adatokat a viselkedésemről önkövető eszközökkel" kérdéssel (1. melléklet/23.) egyetértett, nagyobb arányban használt COVID témájú alkalmazásokat, melyet a 8. ábrán szemléltettem. Az összefüggést Khí-négyzet próbával is vizsgáltam, melynek eredménye szerint (p<0,001) szignifikáns összefüggés van a két kérdésre adott válasz között.



8. ábra Önkövetési szokások és COVID alkalmazások használatának kapcsolata. Saját szerkesztés

Tehát összefoglalva azok használták az ilyen alkalmazásokat, akik amúgy is használnak hasonló típusú alkalmazásokat, de elképzelhető, hogy túlságosan korlátozónak érezték azokat,

mert náluk nagyobb arányban gondolták a válaszadók, hogy lemondtak korábban fontos jogaikról.

4.3. Biztonságtudatosság és biztonságérzet kapcsolata

A következőkben a biztonsági attitűddel kapcsolatos elemzéseket mutatom be. A 2.1. számú kutatási kérdésem az volt, hogy csoportosíthatók-e a résztvevők biztonságtudatosságuk és biztonságérzetük alapján, melyek az attitűd egy-egy pillérjének felelnek meg (ezen kívül a harmadik a viselkedési pillér lesz). A kutatási kérdéshez az alábbi hipotézis tartozott.

> **H2.1**: A nagyobb mértékű biztonságtudatosság nagyobb mértékű biztonsági kockázatérzettel jár együtt.

A vizsgálatot az elméletek alapján kialakított 15 skálás kérdésre (1. melléklet/1-15.) futtatott főkomponenssel kezdtem meg, amely az első két attitűdtényezőre, azaz a saját bevallású biztonsági ismeretekre és a felhasználók témával kapcsolatos érzéseire vonatkozó kérdéseket tartalmazott. A cél az volt, hogy alátámasszam a kérdések összetartozását a fenti tényezők szerint. (A főkomponens analízist Promax rotációval, Kaiser normalizálással alkalmaztam, és a forgatás 6 iterációban történt.) Az főkomponens analízis érvényesnek bizonyult, mivel a KMO (Kaiser-Mayer-Olkin Measure of Sampling Adequacy) értéke 0,888, amely szerint az alkalmazott változócsoport alkalmas főkomponens elemzésre. A Bartlett-teszt eredménye ($p<0,001$) szintén alátámasztja az módszer használatát az előre beállított paraméterekkel (vagyis a változók között korreláció van). A kommunalitás táblázat az összes kérdésre 0,5-nél nagyobb értékeket mutatott, ami azt jelenti, hogy minden kérdés bekerülhet a modellbe. Három főkomponens figyelhető meg, melyek összesített varianciája 67,32%, azaz a létrejött három főkomponens az eredeti változók 67,32%-át magyarázza. A 4. mellékletben található (4/1.) ide tartozó táblázatban az átláthatóság érdekében csak a 0,4-nél magasabb értékeket ábrázoltam.

Mivel a „számomra nagyon fontos, hogy tisztában legyek a személyes adataim felhasználásával," (1. melléklet/4.) kérdésnél a faktorsúly két komponensnél is viszonylag magas értéket adott (0,544 az egyes és 0,474 a kettes komponens esetében), az elemzést e kérdés nélkül is lefuttattam. Az utolsó kérdésnél viszont jelentősebb mértékű a két komponenshez való tartozás közötti különbség (több mint 0,2), ezért a kérdést az elemzésben hagytam. (Jelen esetben is a főkomponens analízist Promax rotációval, Kaiser normalizálással alkalmaztam, és a forgatás 6 iterációban történt.) Így, a 14 skálás kérdéssel, eredményként a KMO=0,873, a Bartlett-teszt értéke pedig $p<0,001$. Vagyis a főkomponens elemzésre továbbra

is alkalmasak a kérdések. Az analízis ismét három olyan tényezőt azonosított, amelyek az eredeti változók eltéréseinek 67,24%-át magyarázzák.

		1	2	3
1.	Jól ki tudom használni a technológiát személyes adataim biztonságának védelme érdekében,	0,913		
2.	Elegendő képességem van ahhoz, hogy megvédjem személyes adataimat a lopástól/ nyilvánosságra hozataltól,	0,908		
3.	A mobileszközökön szükséges biztonsági intézkedések megtétele teljes mértékben az én kontrollom alatt áll,	0,840		
4.	Az adatvédelmi nyilatkozatok miatt úgy gondolom, hogy személyes adataimat az appok bizalmasan kezelik,	0,757		
5.	Ha biztonsági incidenssel találkozom (például feltörik e-mail fiókomat), tudom mit tegyek,	0,743		
6.	A mobilalkalmazások használata előtt tudatosan beállítom a biztonságra vonatkozó beállításokat (például hogy mihez férhet hozzá egy app),	0,743		
7.	Bízom a mobilalkalmazásokkal végzett tranzakcióim biztonságában,	0,643		
8.	Aggódom amiatt, hogy a mobilalkalmazások engedély nélkül felhasználhatják a rólam gyűjtött személyes adataimat,		0,877	
9.	Általánosságban elmondható, hogy kockázatos lenne megadni személyes adataimat egy mobilalkalmazásnak,		0,817	
10.	Számomra nagyon fontos, hogy tisztában legyek az egészségügyi adataim felhasználásával,	0,403	0,625	
11.	Komoly problémát jelentene nekem, ha valaki az engedélyem vagy tudtom nélkül hozzáférne a telefonomon lévő bizalmas információhoz,		0,617	
12.	A biztonság és adatvédelem kérdése túlértékelt,			0,833
13.	Fontos számomra, hogy ha a közösség érdeke úgy kívánja, akár lemondjak személyes adataim feletti kontrollomról (például COVID alatt),			0,674
14.	Túl sok befektetett energiával jár a mobileszközöm védelmét szolgáló biztonsági intézkedések megtétele,		0,417	0,674

2. táblázat Második komponens mátrix, saját szerkesztés SPSS-ből. (Extraction Method: Principal Component Analysis, Rotation Method: Promax with Kaiser Normalization, Rotation converged in 5 iterations)

A 2. táblázatban látható a kommunalitás táblázat. A komponensenkénti értékeket jelen esetben is 0,4 fölött ábrázoltam. Ebben az esetben is néhány kérdés több komponensnél is megjelenik, de mivel a különbségek itt is jelentősebbek (0,2 fölöttiek), ezért ezek a kérdések az elemzés részei maradtak.

Összefoglalva, a kiválasztott 14 kérdésből három tényező azonosítható.

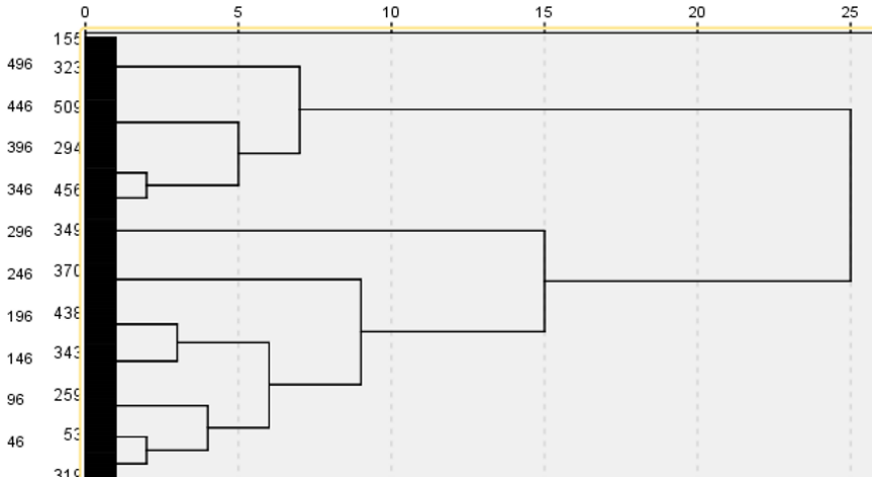
1. Biztonságtudatosság, a kontrollba vetett bizalom: (2. táblázatban található 1-7. kérdések) ez a tényező megmutatja, hogy a felhasználó saját bevallása szerint tudja-e, hogyan védje meg adatait, úgy gondolja-e, hogy kontrollálja azt és tudja-e, mit kell tenni biztonsági incidens esetén. Ez az attitűdelmélet figyelembevételével igazítható az önbevallott biztonsági tudás fogalmához, vagyis a kognitív komponenshez.

2. Észlelt kockázat: (2. táblázatban látható 8-11. kérdések) ez a tényező azt mutatja meg, hogy a felhasználók aggódnak-e az adataik biztonsága és védelme miatt. Az attitűd összetevőit tekintve ez lehet az affektív komponens.

3. A biztonság megítélése: (2. táblázatban található 12-14. kérdések) ez a tényező azt mutatja meg, hogy a felhasználók túlértékeltnek vagy fontos témának tartják-e a biztonságot és a személyes adatok védelmét, és hogy túl sok erőfeszítést igényel-e adataik védelme. Az attitűd megközelítését tekintve ez is az affektív komponens részének tekinthető, de az előző ponttól eltérő szemszögből.

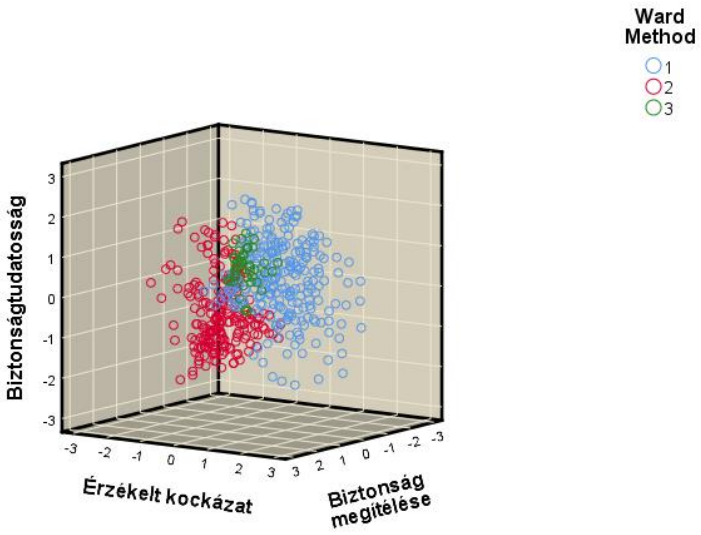
A 2. és 3. tényező összefoglalva biztonságérzetként azonosítható. A belső konzisztencia és belső megbízhatóság ellenőrzésére további számításokat végeztem. A Cronbach-alfa értéke az adatok közötti korreláció mértékével párhuzamosan nő. Ezért nevezik az együtthatókat belső konzisztenciának vagy a teszt belső megbízhatóságának is [143]. A Cronbach-alfa az első csoportnál 0,91, a második kérdéscsoportnál 0,79, a harmadik komponensnél 0,65, ami azt jelzi, hogy ezek a kérdések csoportonként valóban összetartoznak.

Miután megbizonyosodtam arról, hogy a fent azonosított tényezők összhangba hozhatók az attitűdelmélettel, a felhasználókat csoportokba osztottam a három felismert tényező alapján. A főkomponensek azonosítására építve, a különböző tényezőkre adott válaszaik alapján klaszterelemzés segítségével felhasználói csoportok kialakítása volt a következő lépés. A hierarchikus klasztermódszerek közül a Ward-féle eljárást használtam (négyzetes euklideszi távolsággal). A 9. ábrán látható dendrogram kivonat szemlélteti a megfigyelési egységek egyesítését. Annak érdekében, hogy az összevonás utolsó lépései jobban láthatóak legyenek, az ábra magasságát jelentősen csökkentettem, átláthatóbbá téve annak lényegét.



9. ábra Képernyőkép az SPSS-ből, dendrogram a Ward módszer segítségével, szerző által átméretezett

Megvizsgáltam összevonási táblázat eredményeit is (agglomeration schedule), amelyben az együtthatók utolsó hat értékét vonaldiagrammal ábrázoltam az SPSS-ben, a "könyökkritérium" [144] alkalmazhatóságát vizsgálva. (Ezt az opciót a 4. melléklet 4/2. ábrán látható diagram alapján elutasítottam, mert „könyök” nem volt egyértelműen megfigyelhető, a további elemzést alapját ezért a dendrogramon látható adatok képezték.) A dendrogramot figyelembe véve a 2 és 4 közötti klaszterszámokat új változóként elmentve, varianciaanalízis segítségével további elemzéseket végeztem az egyes klaszterek jellemzőinek vizsgálatára a megfelelő számú klaszter meghatározásához. A kétklaszteres megoldást elutasítottam, mert nem ad elég részletes elemzést a mintáról.



10. ábra Klaszterábrázolás - 3D Scatter. SPSS segítségével saját szerkesztés

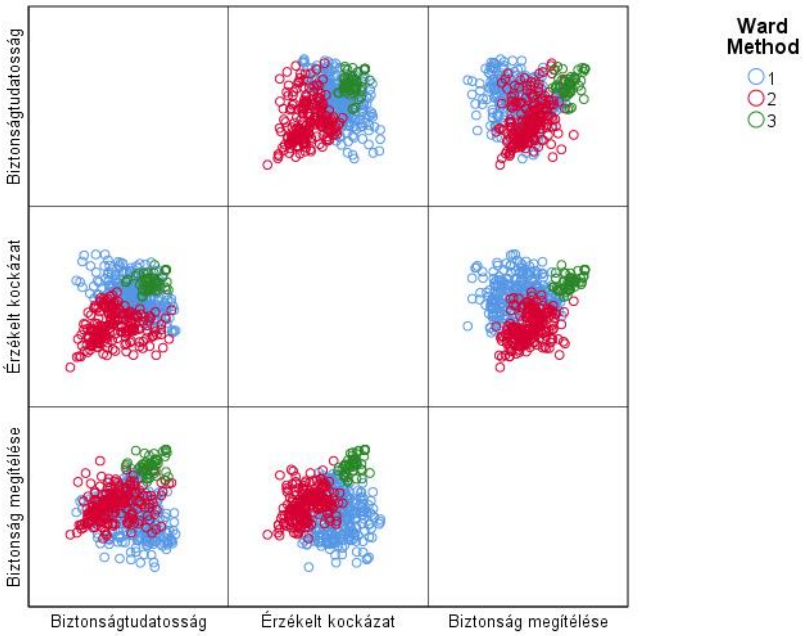
A háromklaszteres megoldás esetében a válaszadók fent azonosított tényezőkhöz való hozzáállása az alábbiak szerint oszlik meg. (A 4. melléklet 4/3. táblázat megmutatja a klaszterekre jellemző főkomponensenkénti átlagot és szórást, valamint a klaszterelemek számát.) Ezen eredmények alapján a három klaszter ábrázolható 3D Scatter diagramon (10. ábra) is, melyen jól látható ezek elkülönülése.

1. Tudatos: Az első klaszter tagjai (N=256, 1, csoport a 4. melléklet 4/3. táblázatban, valamint kék csoport a 10. ábrán) azt állították, hogy rendelkeznek bizonyos fokú tudással a biztonságról, emellett éreznek biztonsági kockázatot, és a biztonság témáját pozitívan ítélik meg, nem tartják túlértékeltnek. Következésképpen ezt a csoportot „tudatosnak” lehet elnevezni, mivel magas szintű tudatossággal rendelkeznek, de abban is eléggé biztosak, hogy tudják, mit kell tenniük a biztonság érdekében.

2. Nyugodt: A klaszter tagjai (N=217, a 4. melléklet 4/3. táblázat 2. csoportja, valamint piros csoport a 10. ábrán) saját bevallásuk szerint nem tartják magukat biztonságtudatosnak, és a többi csoporthoz képest náluk a legalacsonyabb az észlelt biztonsági kockázat. Náluk a biztonság értékelése már kissé negatív, kicsit túlértékeltnek tartják azt, ezért is nevezhetjük őket a „nyugodtak” csoportjának.

3. Magabiztos: A harmadik csoport különleges, mert mindhárom komponens ebből a csoportból kapta a legerőteljesebb válaszokat, ami azt jelenti, hogy nagyon tudatosnak tartják, magas a kockázat észlelésük, ugyanakkor a biztonságot a többi csoporthoz képest nagyon túlértékeltnek tartják. Ez egyfajta önbizalomra utalhat, ami azt sugallja, hogy a „magabiztos” csoportnak címkézhetjük őket. Ötvenkét válaszadó került ebbe a csoportba (a 4. melléklet 4/3. táblázat 3. számú csoportja, zöld csoport a 10. ábrán).

A 11. ábrán (a három klaszteres megoldás esetében megfigyelt) a klasztermátrix segítségével minden elem egyszerre csak két tengely viszonylatában kerül ábrázolásra, így még láthatóbbá téve az egyes klaszterek közti különbséget. (A 4. melléklet 4/4. ábrán az egyes főkomponensenként és klaszterenként jellemző átlagokat ábrázoltam a könnyebb átláthatóság és értelmezhetőség érdekében, így az egymáshoz viszonyított csoportjellemzők is nyilvánvalóbbá válhatnak.)



11. ábra Klasztermátrix. SPSS segítségével saját szerkesztés

A szintén ugyanazt a módszertant követő négyklaszteres megoldásnál (Ward-módszer négyzetes euklideszi távolsággal a fent azonosított főkomponensek alapján) az előző megoldáshoz képest egy negyedik csoportot figyelhetünk meg, amely a három klaszteres megoldás első csoportját (a „tudatosokat") osztja két részre: a 4. melléklet 4/5. ábra 1. számú csoportjára, illetve a 4. számú csoportra, amelyek 203, illetve 53 válaszadóból állnak.

E felosztás első csoportja a háromklaszteres megoldás első csoportjához, vagyis a „tudatosokhoz" hasonlít mindhárom szempontból, ahol a csoporttagok körében magas a tudatosság és az észlelt kockázati szint, valamint ezzel összhangban pozitívan ítélik meg a biztonság témakörét. A negyedik csoport saját bevallása szerint biztonságtudatosabb (a csoportok közül a leginkább), ami segítheti őket abban, hogy alacsonyabb szintű kockázatot érezzenek, ugyanakkor úgy gondolják, hogy a biztonság összességében életük fontos része. Ezt a csoportot például „határozottnak" nevezhetnénk. Ez azt jelenti, hogy az egyetlen megfigyelhető különbség a „tudatos" és a „határozott" csoportok között az észlelt kockázat mértéke.

Figyelembe véve az így hozzáadott csoport méretét (N=53), amely újabb kis létszámú csoportot hozna létre, valamint azt, hogy a négyklaszteres megoldás nem ad nagyon eltérő csoportot a háromklaszteres megoldáshoz képest, a háromklaszteres megoldás mellett döntöttem, tehát a „tudatos", „nyugodt" és „magabiztos" csoportosítás mellett. Fontos megjegyezni, hogy bár az lenne az ideális, ha nem lenne csak 52 tagú csoport („magabiztosak"), megtartottam őket, mert annyira egyedi véleményük van a kérdésekről más csoportokhoz képest, valamint más klaszterszám esetén is együtt álltak, így érdemesnek tartottam külön vizsgálni őket. Az eredményeket a szakmai elfogadás érdekében publikáltam is [145]. A létrejött csoportok különböznek a biztonságtudatosságuk és biztonságérzetük mentén, mely például a főkomponensenként és klaszterenként jellemző átlagokat megjelenítő ábrán is látható. A két tényezőt egyidejűleg figyelembevéve alkottam meg a csoportokat. Az előzetesen elvárt 4 csoport helyett azonban csak 3 csoportot sikerült azonosítani (melyet a 3. táblázat foglal össze). 1. Olyan felhasználók, akik fontosnak tartják és vannak biztonsági ismereteik: a „tudatos" csoport. 2. Olyan felhasználók, akik törődnek a biztonsággal, de nem tudnak róla túl sokat: „nyugodt" csoport. 3. Olyan felhasználók, akik nem törődnek a biztonsággal, bár vannak ismereteik róla: „magabiztos" csoport. Olyan felhasználók, akik nem tartják fontosnak és nincsenek is biztonsági ismereteik: ilyen csoportot nem sikerült azonosítanom, még a további klaszterezési lehetőségek elemzésével sem. (Ez természetesen a kérdőív torzítása is lehet, de a napjainkban gyakran megjelenő biztonsággal kapcsolatos tudatossági trend jele is lehet.)

		Érzelmi attitűd komponens	
		Törődik a biztonsággal	Nem törődik a biztonsággal
Kognitív attitűd komponens	Van biztonsági ismerete	**Tudatos csoport**	**Magabiztos csoport**
	Nincs biztonsági ismerete	**Nyugodt csoport**	

3. táblázat Felhasználói csoportok összefoglalása. Saját szerkesztés

A H2.1 feltevést a következő fejezetben vizsgálom a számítások összetartozása miatt.

4.4. Viselkedési attitűdelemmel kapcsolatos elemzés

A következő rész a három klasztert vizsgálja tovább. A főkomponens- és klaszterelemzésekhez kiválasztott kérdések az attitűdlogika első két komponensét tartalmazták: az önbevallott biztonsági ismereteket és a válaszadók biztonsággal kapcsolatos érzéseit. Az eredményeket a harmadik komponens, azaz a különböző klaszterek biztonság növelésére irányuló tevékenységeik tekintetében is vizsgálom. Ehhez a fejezethez tartozik a 2.2. kutatási kérdés, amely arra keresi a választ, hogy hogyan hat a biztonságtudatosság és és a biztonságérzet alapján meghatározott csoporthovatartozás a biztonságra irányuló viselkedésre.

A felmérésben háromféle viselkedési kérdés szerepelt. A kérdőív második szakaszában az első kérdésben tizenöt potenciális intézkedés közül választhattak a kitöltők, amelyek növelhetik a biztonság szintjét (1. melléklet/30. kérdés). Megállapítható, hogy az első klaszter, a „tudatosok” átlagosan 7-et, a második klaszter, vagyis a „nyugodtak” átlagosan 5-öt, a harmadik, vagyis a „magabiztosak” csoportja pedig átlagosan 3-at alkalmazott. Az 4. táblázat megmutatja, hogy az egyes klaszterek hány százaléka választotta ki a megfelelő viselkedéstípust (az egyes klaszter elemszámához képesti százalékos arányban). (Több válaszlehetőséget is meg lehetett jelölni, így a táblázatban nem értelmezhető az oszloponkénti összesítés.) A válasz-lehetőségenkénti összesített válaszok, vagyis a klaszterek figyelembevétele nélküli eredmények az első oszlopban találhatók.

	Összesen (%) (N=525)	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)	Khí-négyzet próba eredménye
Applikációkat kizárólag hivatalos alkalmazásboltból töltök le. (Például Play Áruház vagy App Store)	67.62	**75.78**	**64.06**	**42.31**	0.000
Vírusírtót használok.	53.33	**60.55**	**48.39**	38.46	0.002
Alkalmazásaimat rendszeresen frissítem.	48.19	**54.69**	**44.24**	32.69	0.005
Elolvasom az adatkezelési tájékoztatókat.	40.57	45.31	33.18	**48.08**	0.014
Bonyolult jelszavakat választok.	40.19	49.61	32.72	25.00	0.000
Ismerem a személyes adatkezeléssel kapcsolatos szabályozásokat, jogaimat. (Például GDPR)	37.71	41.41	32.72	**40.38**	0.139
Személyes adatok kiadása előtt meggyőződnék a weboldal vagy alkalmazás hitelességéről.	36.76	46.88	30.88	11.54	0.000
Biztonsági mentéseket készítek. (Például dokumentumokról, fotókról)	36.00	45.70	30.88	9.62	0.000
Az alkalmazások engedélykérését rendszeresen felülvizsgálom. (Például ellenőrzi milyen alkalmazások használhatják a helyadatait, fényképeit.)	33.90	42.19	28.57	15.38	0.000
Felismernék egy adathalász e-mailt annak tulajdonságairól.	33.71	44.14	26.27	13.46	0.000
Személyemhez nem köthető jelszót választok.	33.71	41.02	28.11	21.15	0.002
Biometrikus azonosítást használok. (Például ujjnyomat- vagy arcfelismerés)	32.19	37.89	31.34	7.69	0.000
Körültekintően átnézem elfogadás előtt a javasolt süti (cookie) beállításokat.	29.14	36.72	23.04	17.31	0.001
Követem az internetes csalásokról szóló híreket.	27.05	35.16	21.20	11.54	0.000
Jelszavaimat rendszeresen frissítem.	19.81	23.83	17.51	9.62	0.035

4. táblázat Klaszterenkénti és összesített biztonsági intézkedések, valamint kereszttábla elemzés eredményei. Saját szerkesztés

Az első oszlop tehát a teljes mintára vonatkozó válaszarány. Az átláthatóság érdekében a fenti táblázatban az arányokat intézkedésenként és klaszterenként mindig a zöld (alacsony esetében fehér) szín különböző árnyalataival emeltem ki. A csoportonkénti első három leggyakoribb válasz pedig félkövérrel látszik. Az utolsó oszlopban pedig a kereszttábla elemzés eredményei láthatók, az adott intézkedést a klasztertagsággal összevetve. Ez tehát azt jelenti, hogy egy kivételével az összes eredmény szignifikánsan eltér a különböző klaszterek esetében. A szabályozások és jogok ismeretét láthatóan hasonló hozzáállással kezeli mindegyik csoport. Ezen kívül megfigyelhető, hogy az első két csoport eredménye valóban összhangban van azzal, amit a felmérés első felében állítottak. A „tudatosok” csoportja a legtöbb esetben a klaszter méretéhez képest a legnagyobb arányban választotta ki a módszereket, melyeket saját bevallása szerint hasznosít a biztonsága növelésére, a nyugodtak csoportja pedig valóban kevesebbet válogat ezekből. Érdekes módon a „magabiztosként” azonosított harmadik csoport, akik magas biztonsági kockázatot észlelő, nagy biztonságtudatosságú embereknek vallották magukat, a másik két klaszterhez képest a legkevesebbet választotta ezek közül az intézkedések közül. Ez annak megerősítéseként értelmezhető, hogy biztonságfelfogásuk szerint ez nem annyira fontos számukra. Bár ez nem zárja ki annak lehetőségét, hogy ezek az emberek valóban magabiztosak, mindenképpen érdekes, hogy nem alkalmaznak túl sok védőintézkedést (legalábbis a kérdőívben elérhetők közül). A jelenség egyik lehetséges magyarázata, hogy látják, de vállalják is a technológiának, például a mobilalkalmazások használatának kockázatait, ezért nem törődnek túlságosan az intézkedésekkel (pl. a már említett privacy paradox miatt). Egy másik lehetséges magyarázat, hogy a felhasználók számára elérhető biztonságot elégségesnek

gondolják saját intézkedések megtétele nélkül is. (Ezt támaszthatja alá, hogy a tudatossági főkomponenst alkotó egyik kérdés például az, hogy bízik-e a felhasználó a mobilalkalmazásokkal végzett tranzakciói biztonságában, mely komponensnél a „magabiztosak" csoportja a legmagasabb szintet vallotta magáénak a három csoport közül.)

Látható, hogy a három legnagyobb arányban választott intézkedés megegyezik a „tudatos" és a „nyugodt" klaszthereknél. Ezek magukban foglalják az alkalmazások csak megbízható forrásból történő letöltését, a vírusirtó használatát és az alkalmazásfrissítések rendszeres telepítését. A „magabiztos" klaszter esetében csak a hivatalos alkalmazásboltokból való app letöltés szerepel az első három intézkedésben az előzőekből, a másik kettő a felhasználási feltételek elolvasása és az adatvédelmi jogaik (például GDPR) ismerete. Ez azt sugallhatja, hogy az 1, és 2, klaszter jobban támaszkodik a technológia által biztosított biztonságra, a 3, klaszter viszont jobban bízik önmagában, ha a biztonságról van szó.

Ezek a válaszok természetesen megjelennek az összes válaszadóra (525 fő) vetített arányoknál is, a legnépszerűbb a teljes mintát tekintve a hivatalos alkalmazásbolt használata (67,62%), a vírusírtó használata (53,33%), az alkalmazások rendszeres frissítése (48,19%), az adatkezelési tájékoztatók elolvasása (40,57%) és a bonyolult jelszavak választása (40,19%) volt.

A biztonsági intézkedésekből az SPSS segítségével egy score-t is készítettem. Az összes kérdőívben felsorolt biztonsági intézkedésből az egyes kitöltők által választottak darabszámát összeadtam (biztint_total változó). Ezek alapján végeztem regresszió analízist, hogy megállapítsam, hogy a biztonsági intézkedések számosságát hogyan befolyásolja az egyes főkomponensekhez való viszonyulás. (A későbbiekben majd ehhez még a kor, nem és az IT területen való jártasság kérdését is hasonlítom.)

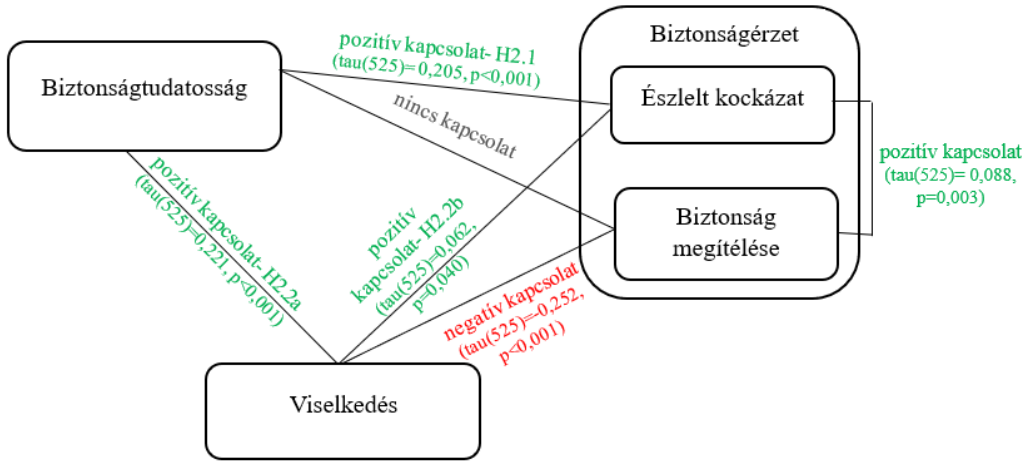
Az ide vonatkozó hipotézisek a következők voltak.

> **H2.2a**: A biztonságtudatosság befolyásolja a biztonsági viselkedést. Minél magasabb a biztonságtudatossága egy felhasználónak, annál több biztonsági intézkedést tesz.
> **H2.2b**: A biztonságérzet befolyásolja a biztonsági viselkedést. Minél inkább érzi a felhasználó a biztonsági kockázatokat, annál több biztonsági intézkedést tesz.

Ahhoz, hogy a továbbiakban használható vizsgálati módszereket meghatározzam, normalitás vizsgálat szükséges. A program segítségével a három főkomponensre, valamint a biztonsági intézkedések számára futtattam normalitásvizsgálatot, mely eredményei az 5. mellékletben láthatók. Mivel a rendelkezésre álló minta 525 elemű, a Kolmogorov-Smirnov teszt

használható. (A Saphiro-Wilk teszt ugyanis a magasabb elemszámoknál nem annyira megbízható.) A H0-ban szereplő állítás az, hogy az adott változó szerinti eloszlás nem tér el szignifikánsan a normális eloszlástól. Jelen esetben a fentiek szerint ez a biztonság megítélésén kívül (mely esetben p=0,200) ez nem teljesül, tehát a kitöltők által használt biztonsági intézkedések száma, a biztonságtudatosságuk, valamint az észlelt kockázatuk nem követ normális eloszlást. Mivel a változók kapcsolatát egybevetve vizsgálom, nem paraméteres korrelációs vizsgálatokat használok a továbbiakban.

A vizsgálathoz a Kendall-tau rangkorrelációs együtthatót választottam, mely eredményeit a 8. melléklet ábrázolja (8/1.). (Mivel a főkomponensek standardizált változók, nem paraméteres korrelációs módszerekkel vizsgálhatók.) A 12. ábrán a vizsgálatok alapján felállított összefoglaló modell látható, mely az egyes biztonsági attitűdelemek kapcsolatát írja le az alábbiak szerint. A kitöltők által tett összes biztonsági intézkedés száma szignifikáns kapcsolatban van a korábbiakban meghatározott három főkomponenssel. Pozitív gyenge kapcsolat figyelhető meg (p<0,001) a biztonsággal kapcsolatos tudatosság és a megtett biztonsági intézkedések számossága között. Tehát a magasabb biztonságtudatosság több intézkedéssel jár együtt, amely igazolja a H2.2a feltevést. Gyenge a kapcsolat a biztonsági intézkedések száma és az észlelt biztonsági kockázat mértéke között (p=0,040). Eszerint a H2.2b hipotézist elfogadom azzal a megkötéssel, hogy a kapcsolat gyenge. Gyenge negatív kapcsolat figyelhető meg a biztonság kérdésének megítélése és a megtett biztonsági intézkedések száma között (p<0,001), vagyis minél inkább túlértékeltnek gondolja a kitöltő a biztonság kérdését, annál kevesebb biztonsági intézkedést tesz.



12. ábra Biztonsági attitűdelemek kapcsolata. Saját szerkesztés

A fenti hipotézisek maguktól értetődőnek tűnhetnek, ugyanakkor fontosnak tartottam statisztikailag is alátámasztani és attitűdelemek közti összefüggéseként kezelni ezen felvetéseket. A főkomponensek kapcsolatát tekintve megfigyelhető, hogy a biztonságtudatosság és az észlelt kockázat között gyenge pozitív korreláció van, azaz magasabb tudatosság nagyobb mértékű észlelt kockázattal jár együtt ($p<0,001$), mely a H2.1 hipotézist alátámasztja. Az észlelt kockázat és a biztonság megítélése között szignifikáns, de gyenge kapcsolat figyelhető meg ($p<0,001$). A biztonságtudatosság és a biztonság megítélése között pedig nem mutatható ki kapcsolat a kérdőív alapján.

A következőkben vizsgáltam az informatikai végzettség vagy informatikához kapcsolódó munka (1. melléklet/ 27. kérdés) és a meghozott biztonsági intézkedések kötötti kapcsolatot. Ebben az esetben is normalitásvizsgálatot végeztem, hogy az alkalmazható módszert meghatározzam. Az eredmény itt is azt mutatja, hogy a normalitás nem teljesül, így ebben az esetben is nem paraméteres próbával vizsgáltam tovább a kérdést. (A számítás eredményeit az 5. melléklet tartalmazza.) Ismét a Mann-Whitney U próbát alkalmaztam, mely segítségével megállapítható ($p=0,522$), hogy itt sem figyelhető meg szignifikáns eltérés az IT jártassággal rendelkezők és nem rendelkezők biztonsági intézkedéseinek számossága között.

A fenti összefüggések további feltárása érdekében ezután többszempontos varianciaanalízist végeztem, melyben a nem és az informatikai háttér (munka vagy végzettség) interakcióját, valamint külön a nemet, informatikai hátteret, életkort, valamint a korábban meghatározott három főkomponenst elemeztem. Az eredményeket a 8. melléklet tartalmazza (8/2.). A varianciaanalízis feltétele a Levene-teszt, mely a szóráshomogenitást vizsgálja (test of homogenity of variances). A teszt nullhipotézise, hogy a szórások nem egyenlők, melynek elvetése azt jelenti, hogy a szóráshomogenitás teljesül, Itt tehát ($p=0,149$) a H0-t elvetjük, vagyis a feltétel teljesül. Bár a nem és az IT-jártasság közötti interakció vizsgálata érdekes lehetőségnek tűnt, nem hozott szignifikáns eredményt. A táblázatban található szignifikanciaszintek alapján megállapítható, hogy a nemnek, az első főkomponensnek, tehát a biztonságtudatosságnak, valamint a harmadik főkomponensnek, tehát a biztonság megítélésének van szignifikáns hatása a megtett biztonsági intézkedések számára. (A tesztek nullhipotézise, hogy a változók között nincs kapcsolat, Mivel p ezekben az esetekben kisebb, mint 0,05, a nullhipotézist elvethetjük, tehát van kapcsolat a változók között.) Érdemes azért kiemelni, hogy az R négyzet mutató értéke 0,248, ami azt jelenti, hogy ezek a változók csak 24,8%-ban magyarázzák a biztonsági intézkedések számát, amely szintén alátámasztja, hogy számos más tényező is befolyásolhatja azt.

4.5. Klaszterek további elemzése

Az azonosított klaszterek jobb megismerése érdekében további elemzéseket végeztem. A 2.3. kutatási kérdésre keresi a választ az alábbi fejezet, hogy hogyan jellemezhetők a létrejött csoportok. A demográfiai jellemzőkkel kapcsolatban nem fogalmaztam meg hipotéziseket, de szintén érdekes információkat rejthetnek. A számítások ábrázolásait a 9. melléklet tartalmazza.

Először megvizsgáltam, hogy a klaszterhez való tartozás és az iskolázottság között van-e összefüggés. Mivel a 8 általános vagy alacsonyabb iskolai végzettséggel rendelkező csoportok elemszáma klaszterenként 5 fő alá csökkent, a csoportot összevontam a szakmunkásképzőt, szakiskolát (érettségi nélkül) végzett csoporttal. Együtt ezeket érettségi nélküli csoportnak neveztem el SPSS-ben. Az összefüggést kereszttábla elemzés segítségével vizsgáltam. A H0 szerint a két változó független egymástól. A próba eredménye (p=0,091) szerint 0,05-os szignifikancia szint mellett ugyan nem mutatható ki összefüggés, de egy megengedőbb, 10%-os szignifikancia szinttel szignifikáns kapcsolat lenne az iskolázottság és a klasztertagság között.

A csoportok arányaiban megfigyelve látható (melléklet 9/1.), hogy az eddig „magabiztosnak” nevezett csoportban a válaszadók 40%-a érettségi nélküli. Érdekes, hogy további 31%-nak viszont főiskolai, egyetemi vagy posztgraduális végzettsége is van. A két másik csoport iskolázottsági arányai azonban láthatóan nem térnek el egymástól nagy mértékben. A nemet vizsgálva a kereszttábla elemzés eredménye (p=0,777) szerint nincs összefüggés a nem és a klasztertagság között. (A részletes számítások a mellékletben találhatók.)

A klasztereket ezután korcsoportonként is megvizsgáltam. A Khí-négyzet próba eredményét (p=0,044) figyelembe véve szignifikáns kapcsolat van a klasztertagság és a korcsoportba való tartozás között. A mellékletben (9/2.) klaszterek korcsoportonkénti megoszlása látható. Feltűnő, hogy a „nyugodtak” csoportjában a legnagyobb a fiatalabb kitöltők aránya, 23%-uk 26 év alatti, további 14%-uk pedig 35 év alatti (utóbbi a korosztály szerinti legkisebb arány a többi klaszterhez viszonyítva). Ugyanezt a két korcsoportot tekintve a „tudatosok”, majd a „magabiztosak” követik őket egyre csökkenő arányokkal. Az előbbiekkel össze-egyeztethetően a „nyugodtaknál” a legkisebb az idősebb kitöltők aránya, egészen a 45-től 65 évig terjedő korcsoportokban. A „tudatosok” és a „magabiztosak” 36 éven túli korcsoportok tekintetében hasonlónak tűnnek, a „tudatos” csoportban nagyobb arányú a legidősebb kitöltők aránya (54-65 év közöttiek).

A következő demográfiai szempont a lakhely volt, először régió, majd település mérete szerint vizsgáltam a klaszterbeli tartozást kereszttábla elemzéssel. Bár a Khí-négyzet próba eredménye (p=0,046) szignifikáns összefüggést mutatott volna a régió és a klaszter tagság között, két csoportban 5 fő alatt volt a kitöltők száma, így ez nem tekinthető megfelelően alátámasztott eredménynek. Jelen esetben a régiók további összevonását sem láttam jó megoldásnak, mert az torzította volna az eredményeket. A 9. mellékletben (9/3. ábrán) látható a klaszterek régiónkénti megoszlása. A „tudatos" csoport legnagyobb arányban az ország középső régióiból származik. A Nyugat-Dunántúlon élők legnagyobb arányban a „nyugodtak" csoportját erősítik. A „magabiztosak" között a legmagasabb az észak-magyarországi kitöltők aránya, valamint a dél-alföldiek aránya is a többi klaszterhez képest. A település méretét és klasztertagságot kereszttábla elemzéssel vizsgálva (p=0,965) nem figyelhető meg szignifikáns összefüggés. Ez a megoszláson is látható, nagyjából egyezik a csoportonkénti megoszlás az összesített megoszlással település méret tekintetében.

A következőkben a havi nettó jövedelmet vizsgáltam, mely (p=0,771) nem mutatott szignifikáns összefüggést a klaszter tagsággal. A 9. mellékletben található 9/4. táblázatban látható ezek megoszlása csoportonként (színezéssel kiemelve a magasabb értékeket). Bár nem szignifikáns, de megfigyelhető, hogy a „tudatos" csoportban kissé nagyobb a magasabb fizetések aránya, míg a „magabiztos" csoportban alacsonyabb a többi klaszterhez viszonyítva.

Az internetes vásárlási gyakoriságot is összevetettem a klasztertagsággal. A gyakoriságot ordinális skálaként értelmezve Kruskal-Wallis tesztet végeztem, mely eredménye p=0,067, mely szigorúan véve nem szignifikáns, azonban egy megengedőbb, 10%-os szignifikancia szintnél már szignifikáns eredménynek számítana. A 9. mellékletben (9/5.) klaszterenként látható a vásárlási gyakoriság. Megállapítható, hogy a „tudatos" csoport vásárol a legnagyobb arányban havi többször is interneten keresztül. Elég magas az arány a „nyugodtak csoportjában is, bár ők már nagy arányban válaszolták, hogy többször, negyedévente vásárolnak ilyen módon. A „magabiztosak" csoportjában a legmagasabb a soha és ritkán interneten vásárlók aránya.

Az alábbiak két technológiai felkészültséget vizsgáló kérdés és a klaszterek kapcsolatát vizsgálják, melyekhez a 2.3. kutatási kérdéshez kapcsolódó hipotéziseket társítottam.

> **H2.3a**: Akik biztonságtudatosabbak, azok jobban lépést tartanak a technológiai fejlődéssel, mint a kevésbé biztonságtudatosak.

H2.3b: Az IT területen jártas válaszadók biztonságtudatosabbak, mint a területen nem jártas válaszadók.

H2.3c: Az IT területen jártas válaszadók alacsonyabb szintű biztonsági kockázatot észlelnek, mint a területen nem jártas válaszadók.

Az 5. táblázatban az egyetértő válaszok az azonosított felhasználói csoportok, majd a teljes minta arányában figyelhetők meg. Bár a technológiai fejlődést követés (1. melléklet/18. kérdés) viszonylag nagy arányban jellemző a válaszadókra, hiszen a kitöltők fele értett egyet az állítással, a „magabiztosak" csoportjában kiemelkedően sokan tartanak lépést a technológiai fejlődéssel. A másik két csoport szokásai hasonlóak ilyen szempontból. Kereszttábla elemzéssel és Khí-négyzet próbával vizsgálva (p=0,002) szignifikáns összefüggés figyelhető meg a klasztertagság és a technológia követési szokások között. Tekintve a csoportalkotásnál figyelembe vett biztonságtudatosságot, a H2.3a hipotézist elfogadom, tehát valóban igaz, hogy akik tudatosabbak, jobban lépést tartanak a technológiai fejlődéssel.

Az informatikai végzettség vagy munka kapcsolatát már a fentiekben is elemeztem, azonban a klaszterekre és az egész mintára vetítve is érdekes megvizsgálni a válaszokat ezzel kapcsolatban. (A végzettség vagy tapasztalat meglétét IT területen jártasságnak nevezem.) A minta ötöde (20,00%) jártas informatikai területen saját bevallása szerint. A „magabiztosak" csoportjában a legnagyobb (majdnem egyharmad) a csoportok közül ezen válaszadók aránya. Az eredményeket az 5. táblázat tartalmazza. Kereszttábla elemzéssel és Khí-négyzet próbával vizsgálva (p= 0,031) megállapítható, hogy szignifikáns összefüggés van az IT jártasság és a klasztertagság között. Ismét a csoportkialakítási logikában szereplő biztonságtudatosságot figyelembe véve tehát megállapítható, hogy a H2.3b hipotézist, miszerint az IT területen jártas válaszadók biztonságtudatosabbak, elfogadom a próba eredménye alapján. A H2.3c hipotézist, miszerint az IT területen jártas válaszadók alacsonyabb szintű biztonsági kockázatot észlelnek, elvetem, mert a csoportosításnál figyelembe vett észlelt biztonsági kockázat a „magabiztos" csoportnál volt a legnagyobb saját bevallásuk szerint, ugyanakkor náluk a legnagyobb az IT jártasság aránya. Ez tehát egy fordított irányú kapcsolatra enged következtetni a feltevésemhez képest. Összefoglalva a két kérdés alapján tehát a technológiai felkészültség szignifikánsan összefügg a klasztertagsággal.

	Összesen (%) (N=525)	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)	Khí-négyzet próba eredménye
Lépést tartok a legújabb technológiai fejlesztésekkel.	53.71%	50.00%	52.53%	76.92%	0,002
Végzettségem vagy munkám IT területhez kapcsolódik.	20.00%	16.80%	20.74%	32.69%	0,031

5. táblázat Technológiai és IT felkészültség klaszterenként és összesen, valamint kereszttábla elemzés eredményei. Saját szerkesztés

Végül a korábbi biztonsági incidenssel kapcsolatos tapasztalatok (1. melléklet/31. kérdés) és a klasztertagság összefüggését vizsgáltam. A kereszttábla elemzés szerint (p=0,113) nem figyelhető meg szignifikáns összefüggés a két tényező között. Általánosságban azonban elmondható, hogy a rossz tapasztalat befolyásolja a kérdőívre adott válaszokat, ahogy azt a fentiekben vizsgáltam.

A kérdőív következő kérdése az alkalmazástelepítéskor túlzó hozzáférési engedélyek jóváhagyása mögötti lehetséges motivációkat vizsgálta. A „ha egy alkalmazás túl sok hozzáférési engedélyt kér a telepítés után, akkor hagyom jóvá, ha…” (1. melléklet/28.) kezdetű mondat lehetséges befejezéseiből a résztvevők kiválaszthatták a rájuk igaz állításokat. (Azt, hogy mi számít túl soknak, a válaszadóra bíztam.) A 6. táblázat foglalja össze a klaszterenkénti válaszokat (a klaszterelemszámok arányában). Az első oszlopban a teljes mintához viszonyított válaszarányok találhatók. Az előzőekhez hasonlóan a válasz-lehetőségenkénti arányokat legmagasabb arányokat zölddel és arányaival ábrázoltam, a legalacsonyabbakat pedig fehér színnel, valamint félkövéren jelöltem a csoportonkénti első három választást az átláthatóság érdekében. Az utolsó oszlopban a Khí-négyzet próbák eredményei láthatóak az adott sor és a klasztertagság összefüggésében, hogy megállapítható legyen, mely eredményből lehet következtetéseket levonni. Amint az látható, az első és a második klaszter, vagyis a „tudatos” és a „nyugodt” csoportok esetében megegyezik a három legnagyobb arányú válasz. Ezek alapján leginkább azért fogadnak el engedélykéréseket alkalmazások telepítésekor, mert bíznak a hivatalos alkalmazásboltokban, nincs korábbi rossz tapasztalatuk, és úgy gondolják, hogy ezek ésszerű kérések, tehát az alkalmazás használatához szükséges funkciókat segítik.

Ha egy alkalmazás telepítés után túl sok hozzáférési engedélyt kér, azokat akkor hagyom jóvá, ha:	Összesen (%) (N=525)	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)	Khí-négyzet próba eredménye
megbízom az alkalmazásboltban, ahonnan letöltöm az appot.	53.33	**55.08**	**54.84**	**38.46**	0.077
korábban semmilyen problémát nem észleltem hasonló eset miatt.	36.00	**36.33**	**35.02**	**38.46**	0.888
úgy érzem, hogy ezek jogos kérések.	28.19	**33.20**	**25.81**	13.46	0.009
nagyon szeretném az alkalmazás nyújtotta funkciókat használni.	16.95	17.58	17.05	13.46	0.770
nem értem miért kéri.	13.14	11.72	12.90	**21.15**	0.184
azokat túl sokáig tart elolvasni.	10.48	7.81	12.90	13.46	0.150

6. táblázat Hozzáférés engedélyezés motivációi klaszterenként és összesen, valamint kereszttábla elemzés eredményei. Saját szerkesztés

A „magabiztosak” esetében az első két legnagyobb arányú válaszlehetőség megegyezik a fentiekkel, azonban a harmadik legtöbbet választott opció az volt, hogy akkor is jóváhagyják ezeket az engedélykéréseket, ha nem értik, miért kérik tőlük. Ez azt sugallhatja, hogy nem aggasztják őket az engedélykérések, és egyetértenek a szolgáltatók, alkalmazás-fejlesztők javaslataival. Az egyetlen szignifikáns összefüggést jelző válaszlehetőség a kérések jogosságára (és a klasztertagságra) vonatkozott ($p=0,009$). Megfigyelhető, hogy a „tudatos” csoport ért ezzel a leginkább egyet, a „magabiztosak” csoportja pedig a legkevésbé.

E két szakasz után látható, hogy viselkedési szempontból az első és a második klaszter nem különbözik túlságosan. A klaszterek létrehozásakor az első csoport szinte az ellentétének tűnt a második csoportnak a biztonságtudatosság fokát és a kockázat- és biztonságérzékelést tekintve, így nagyon érdekes, hogy végül viszonylag egyformán gondolkodnak a biztonsági viselkedésről. Fontos megjegyezni, hogy mivel az egész kérdőív a biztonságról és annak vonatkozásairól szólt, a válaszadók úgy érezhették, hogy a kitöltés során úgy kell tenniük, mintha a biztonság lenne a legfontosabb szempont számukra, ami például a funkciónál is fontosabb.

Ezt a lehetőséget támasztja alá egy harmadik kérdés, amely az alkalmazás választásának okait vizsgálja (1. melléklet/ 29. kérdés), mely eredményeit a 7. táblázat foglalja össze. A 3. kutatási kérdés is ezt a témakört vizsgálja: mi alapján választanak a felhasználók applikációkat, melyek a választási szempontok és ezek hogy függenek össze a biztonságtudatossággal és biztonsággal kapcsolatos érzelmekkel, melyhez az alábbi hipotézis tartozik.

> **H3**: A biztonság az elsődleges választási szempontok közé tartozik az applikációk választásánál.

A korábbi logikát követve az első oszlopban a teljes mintára vonatkozó válaszarányok látszanak, a csoportonkénti legnépszerűbb három választás pedig félkövérrel van ábrázolva. Az utolsó oszlopban ismét a Khí-négyzet próbák eredményei láthatók, melyek a soronkénti válaszokat és a klasztertagságot vetik össze. Összességében az összes válaszadó 74%-a számolt be arról, hogy a biztonság fontos szempont egy alkalmazás kiválasztásakor, de ez nem feltétlenül tükröződik viselkedésükben, ahogyan az fentebb látható. Ez alapján a H4 hipotézist igazoltam, a biztonság fontos szempont a felhasználóknak alkalmazások választásánál. Érdemes megjegyezni, hogy mivel a teljes kérdőív témája a biztonság volt, a válaszadókat ez befolyásolhatta a biztonság fontosságának megítélésekor. A jövőbeni kutatások egy lehetséges

irányaként a kérdőív kialakításánál érdemes lehet ezt a kérdést például sorrendben előrébb venni a befolyásolás csökkentése érdekében.

A második legnépszerűbb válasz a személyes adatok megbízható kezelése. A kérdőív ugyan nem tért ki arra, hogy ezt honnan tudják megállapítani a kitöltők, de a korábbi válaszok alapján többek között az alkalmazásboltok megbízhatóságába és az appok frissítésébe vetett bizalom adhatja meg erre a kérdésre a választ. Ezen kívül az adatkezelési és felhasználási tájékozók adhatnak erről több információt, melyet a felhasználók 41%-a szokott elolvasni (a klaszterenkénti megoszlást a korábban elemzett 4. táblázatban ábrázoltam).

Alkalmazás választásánál számomra fontos, hogy az app:	Összesen (%) (N=525)	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)	Khí-négyzet próba eredménye
biztonságos legyen.	74.48	**85.94**	**66.36**	**51.92**	0.000
megbízhatóan kezelje személyes adataimat.	45.33	**61.72**	32.72	17.31	0.000
milyen csillagos értékelést kapott.	43.24	45.70	**41.94**	**36.54**	0.420
jó szöveges értékeléseket kapjon.	42.10	46.09	**39.63**	**32.69**	0.128
elérhető legyen magyarul.	41.71	**50.00**	35.02	28.85	0.001
jó hírnevű legyen.	26.67	29.30	27.65	9.62	0.013
sok letöltéssel rendelkezzen.	25.71	26.95	25.35	21.15	0.675
örömet okozzon.	25.14	26.56	25.81	15.38	0.228
megmagyarázza, hogy milyen tudományos kutatáson alapul.	18.48	20.31	17.05	15.38	0.550
motiváljon.	17.14	17.97	16.59	15.38	0.868
esztétikus legyen.	16.38	13.67	19.82	15.38	0.194
elől legyen a találati listában, ha az adott témakörre keresek az alkalmazásboltban.	15.81	13.67	16.59	23.08	0.219
valaki ajánlja nekem.	13.33	14.45	12.44	11.54	0.751

7. táblázat Szempontok alkalmazások választásakor klaszterenként és összesen, valamint kereszttábla elemzés eredményei. Saját szerkesztés

Amint látható, a biztonság az első szignifikáns összefüggést jelző válaszlehetőség. Itt a biztonságtudatosságnak megfelelően a „tudatos” csoport választotta ezt a legmagasabb mértékben, a „nyugodt” a középső a két másik csoporthoz képest, és a „magabiztosakat” érdekelte a biztonság legkevésbé alkalmazás választási szempontként. A személyes adatok bizalmas kezelése is szignifikánsan összefügg a klasztertagsággal. E kérdés jóval megosztóbb volt, mint az előző, ugyanis a csoportokra vonatkozó arányok egymáshoz viszonyítva nagyon eltérőek. A „magabiztosak” nagyon kevesebb, mint egyötödét érdekli ez a szempont alkalmazás választásnál. (Természetesen ennek lehet az is az oka, hogy a válaszadók bizonytalanok, hogy ezt hogyan lehet megtudni- melyre már az applikációk értékelése fejezetben utaltam.)

A következő szignifikáns összefüggést jelző válaszlehetőség az, hogy az applikáció legyen elérhető magyarul (p=0,001). Ebből arra következtethetünk, hogy a „tudatos” csoport, ahol a válaszadók 50%-a jelölte ezt fontos szempontnak, fele valószínűleg nem tud angolul. A „nyugodtaknál” már 35%, míg a „magabiztosaknál” csak 29%, vagyis utóbbiak legnagyobb

arányban fogadják el az applikációkat angolul is a kitöltők közül. Az utolsó szignifikáns összefüggést alkalmazások választásánál a klasztertagsággal az app jó hírneve mutatta (p=0,013), Itt látható, hogy a „tudatosoknak" a leginkább fontos ez, a „magabiztosaknak" pedig legkevésbé.

A kutatás korlátjaként fontos megemlíteni, hogy ezek a kérdések a felhasználók átlagos rendszeres önbevallású viselkedését mérik fel, a tényleges viselkedést ebben a kérdőívben nem vizsgáltam, hogy az eredmények ne legyenek túl specifikusak egy adott alkalmazás használatával kapcsolatban. A jövőben azonban ez a tanulmány logikájának potenciális folytatása lehet, azonban az attitűd elmélete szempontjából (melyet a kognitív disszonancia torzíthat), az önbevalláson alapuló logika is megfelelő lehet.

4.6. Ellenőrző, kiegészítő kérdések elemzése, egészséggel kapcsolatos appok kérdések

A következő szakaszban a már említett ellenőrző, visszacsatoló, valamint a néhány egészséges életmódhoz és önkövető applikációkhoz kapcsolódó kérdést elemzem.

Először az azonosított főkomponenseket egy-egy ellenőrző kérdéssel vetem össze, alátámasztva ezzel a válaszok konzisztenciáját. „Az alkalmazások használatakor mindig automatikusan elfogadom az engedélykéréseket" (1. melléklet/17.) mondatot a biztonságtudatossággal vizsgálom. A megfelelő módszer meghatározásához ismét normalitás vizsgálatot végeztem (Kolmogorov-Smirnov teszttel), mely szerint az egyetértő válaszok esetében az eloszlás normális (p=0,2) (részletes számítás a 2. mellékletben), azonban az egyet nem értők esetében nem az (p=0,008), így a további vizsgálatoknál a Mann-Whitney U próba használható. A próba nullhipotézise, hogy ugyanolyan a biztonságtudatosak azok, akik automatikusan elfogadják az engedélykéréseket, mint azoknak, akik nem. A próba eredménye (p=0,006) szerint a nullhipotézist elvetjük, vagyis valóban különbözik a két csoport biztonságtudatossága.

A következő ellenőrző kérdést, vagyis hogy „valószínűnek tartom, hogy a jövőben feltörik az okoseszközömet" (1. melléklet/19.), az észlelt kockázattal vetettem össze. Ismét normalitás vizsgálattal határozom meg a használható módszert. A Kolmogorov-Smirnov teszt alapján az egyetértőknél a normalitás (részletes számítások a mellékletben) nem valósul meg (p=0,002), de az egyet nem értőknél megvalósul (p=0,086). Ezek alapján ismét a Mann-Whitney U próba használható. A próba eredménye (p=0,183) szerint a nullhipotézist, vagyis hogy egyformán érzik a kockázatot azok, akik valószínűnek tartják az eszközük jövőbeni feltörését azokkal akik

nem tartják valószínűnek, elfogadjuk. Nincs a kettő csoport között szignifikáns különbség. Ez azt jelenti, hogy a válaszadók az elemzések alapján nem biztos, hogy az adott kérdésre konzisztens válaszokat adtak. Bár az észlelt kockázattal (és a biztonság megítélésével) nem függ össze az ellenőrző kérdés, kimutathatóan együtt jár a biztonságtudatossággal (Mann-Whitney U próba esetében $p<0,001$).

Az utolsó főkomponenssel kapcsolatos ellenőrző kérdés a „ha egy alkalmazás nagyon tetszik, nem érdekel, hogy biztonságos-e” (1. melléklet/16. kérdés), melyet a biztonság megítélésével vetettem össze. A normalitásnál ismét a Kolmogorov-Smirnov teszt eredményét vizsgálom, mely szerint az eloszlás nem tér el szignifikánsan a normális eloszlástól (a számítás részletei a mellékletben találhatók). Ezért a továbbiakban használható módszer meghatározásához szóráshomogenitás vizsgálatra van szükség. A 8. mellékletben (8/3.) látható a Levene-teszt eredménye, melynek nullhipotézise, hogy a szórások nem egyenlők. Ezt jelen esetben ($p=0,563$) elvetjük, tehát a szóráshomogenitás teljesül. Ez azt jelenti, hogy a 2 mintás t-próba használható. A próba eredménye esetünkben az „egyenlő szórásokat feltételezve” sor a releváns, ahol a szignifikancia szint $p<0,001$, vagyis a két csoportnak, akiket érdekel és nem érdekel a biztonság, ha egy alkalmazás tetszik nekik, valóban eltér a biztonsági megítélésük. A 8. táblázatban az ellenőrző kérdések és válaszaik aránya látszik először az azonosított felhasználói csoportok, majd a teljes minta arányában.

Az első kérdés az alkalmazások engedélykéréseinek elfogadását vizsgálta, mely szerint a válaszadók 44,19%-a automatikusan elfogadja azokat. A táblázatban is látható, hogy az egyes azonosított klaszterek a korábbi leírásoknak megfelelően válaszoltak, a „magabiztosaknál” a legnagyobb, a „tudatosoknál” a legkisebb a kérdésre adott megerősítő válaszok aránya. Az összes válaszadó közel egyharmada (32,95%) tartja valószínűnek, hogy feltörik okos eszközét. Ez az észlelt kockázat egyik összetevőjeként is értelmezhető, mely a „magabiztosaknál” volt eredetileg a legmagasabb, amit az alábbi válaszok is alátámasztanak. Azonban érdekes, hogy míg a klaszterek besorolásánál a „nyugodt” csoportnál volt a legkisebb az észlelt kockázat mértéke, a kérdésre ők adták a második legnagyobb arányú pozitív választ.

Az utolsó ellenőrző kérdés azt vizsgálja, hogy a biztonság szempont-e az alkalmazáshasználatkor. Tekintve, hogy az összes válaszadó mindössze 17,90%-a állította, hogy nem érdekli a biztonság, ha egy alkalmazás tetszik neki, a fenti állítás, miszerint alkalmazás választásakor ez 74,48%-uknak fontos, nagyjából konzisztens válaszokat mutat. Ismételten fontos megemlíteni, hogy az, hogy az egész kérdőív a biztonság témakörét dolgozza

fel, a válaszadókat befolyásolhatta a biztonság fontosabbnak ítélésében. A klaszterenkénti válaszok megoszlásánál ismét megfigyelhető, hogy az egyes csoportok a fentieknek megfelelően nyilatkoztak a kérdés kapcsán. A „magabiztosakat" érdekelte a legkevésbé a biztonság, a „tudatosokat" pedig a leginkább a válaszaik alapján.

	Összesen (%) (N=525)	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)
Az alkalmazások használatakor mindig automatikusan elfogadom az engedélykéréseket.	44.19%	32.81%	53.46%	61.54%
Valószínűnek tartom, hogy a jövőben feltörik az okoseszközömet.	32.95%	28.91%	35.94%	40.38%
Ha egy alkalmazás nagyon tetszik, nem érdekel hogy biztonságos-e.	17.90%	7.42%	26.27%	34.62%

8. táblázat Ellenőrző kérdések klaszterenként és összesen. Saját szerkesztés

A kérdőív utolsó szakaszában az egyéb, egészség és fitnesz applikációkkal kapcsolatos kérdések szerepeltek (1. melléklet/20-26. kérdések). Az itt felsorolt kérdések sorrendje a használat, és annak során felmerülő kérdések logikai sorrendjét követte, kiegészítve néhány COVID témájú kérdéssel. Az egyéb, egészség és fitnesz applikációkkal kapcsolatos kérdésekre adott válaszokat a 9. táblázat mutatja be a megalkotott klaszterekre és a teljes mintára vonatkozóan. Az utolsó oszlopban ismét a kereszttábla elemzések során kapott Khí-négyzet próba értékei láthatók. Érdekes, hogy 5%-os szignifikancia szinten csak három állítás van szignifikáns kapcsolatban a klasztertagsággal, azonban egy megengedőbb 10%-os szignifikancia szinten további két állítás jelezne még kapcsolatot. Az jól látható, hogy az egészséges életmód a válaszadók nagy részének fontos (85,53%), 61,14%-uk használ is valamilyen ehhez kapcsolódó alkalmazást. (Érdekes módon 18 kitöltő állította, hogy nem fontos nekik az egészséges életmód, de használnak alkalmazásokat az egészségük vagy fittségük megőrzése érdekében.) A már említett megengedőbb szignifikancia szint mellett megállapítható lenne, hogy a „magabiztosak" használnak a legnagyobb arányban ilyen appokat, a „tudatosok" pedig a legkevésbé. Az egészség és fitnesz appokba vetett hit a válaszadók 43%-ánál jelenik meg. Azok közül, akik használnak ilyen appokat 87%-uk hisz is abban, hogy ezek segíthetnek megelőzni a jövőbeni betegségeket. A kitöltők 42%-a gyűjt magáról adatokat, viszont csak 29%-uk módosítja ezek alapján a viselkedését. Szintén megengedőbb szignifikancia szint mellett megállapítható lenne, hogy az önkövetés leginkább a „magabiztosak" csoportjára jellemző a mintából, a legkevésbé pedig a „tudatosok" csoportjára. A viselkedés módosítására vonatkozó kérdésre a három klaszter tagjai szigorúbb szignifikancia szint mellett is szignifikánsan különböző válaszokat adtak, leginkább a „magabiztosak" csoportja módosítja ezek alapján a viselkedését, míg a „tudatosok" csoportja

a legkevésbé. A kitöltők kevesebb, mint negyede gondolta úgy, hogy korábban lemondott a COVID miatt korábbi jogairól. A leginkább a „magabiztosak” érezték a lemondást, a legkevésbé pedig a „tudatosok”, mely összefüggés szignifikánsnak bizonyult. COVID témájú applikációkat a teljes minta 16%-a használt, legnagyobb arányban a „magabiztosak”, legkisebb arányban pedig ismételten a „tudatosok” csoportja. A különbség a klaszterek között szintén szignifikáns.

	Összesen (%) (N=525)	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)	Khí-négyzet próba eredménye
Fontos számomra az egészséges életmód.	85.33%	86.72%	82.49%	90.38%	0.240
Alkalmazásokat használok a jó egészség/fittség megőrzése érdekében.	61.14%	37.89%	45.62%	53.85%	0.055
Úgy gondolom, hogy az egészség és fitnesz alkalmazások segíthetnek a jövőbeni betegségek megelőzésében.	42.67%	59.38%	60.37%	73.08%	0.173
Rendszeresen gyűjtök adatokat a viselkedésemről önkövető eszközökkel (például pulzus, lépésszám vagy útvonal követése okos órával vagy okos telefonnal).	41.90%	38.67%	42.40%	55.77%	0.073
Magatartásomat folyamatosan módosítom az önkövető eszközöktől kapott adatok/visszajelzések alapján.	29.33%	17.19%	26.27%	38.46%	0.001
A Covid miatt lemondtam néhány korábban fontos jogomról.	23.05%	21.88%	33.18%	50.00%	0.000
Használtam Covid témájú applikációkat (például Vírusradar vagy Házi Karantén).	16.00%	11.72%	16.13%	36.54%	0.000

9. táblázat Egészséggel és önkövetéssel kapcsolatos kérdések klaszterenként és összesen, valamint kereszttábla elemzési eredmények. Saját szerkesztés

Összességében megállapítható, hogy az alábbi kérdések alapján leginkább a „magabiztosak” használják az egészség és fitnesz témájú appokat és nekik a legnagyobb a hitük is ebben. A második helyen ilyen összefüggésben a „nyugodtak” csoportja áll, végül a legkevésbé a „tudatosokra” jellemző ezek kihasználása.

4.7. Csoportok attitűdjeinek összefoglalása

Összefoglalva a válaszadók biztonsági attitűdjét a 10. táblázat tartalmazza. A jelölések minden esetben egy háromfokú skálán jelenítik meg az egyes elemekhez tartozó csoportonkénti értéket, figyelembe véve a mintán belüli másik két csoport értékeit.

Attitűd	Kognitív elem	Érzelmi elem		Viselkedési elem
	Biztonságtudatosság	Észlelt Kockázat	Biztonság megítélése	Biztonsági intézkedések száma
Tudatos	Közepes	Közepes	Pozitív	Magas
Nyugodt	Alacsony	Alacsony	Semleges	Közepes
Magabiztos	Magas	Magas	Negatív	Alacsony

10. táblázat Eredmények összesítése

A „tudatos” felhasználók csoportja magas, de a mintát tekintve közepes szintű biztonság-tudatossággal rendelkezik, közepes szintű kockázatot is észlel, pozitívan ítéli meg a biztonság kérdését és ennek megfelelően az általuk megtett biztonsági intézkedések száma a mintán belül

a legmagasabb. Demográfiai szempontból tagjaik igen hasonlóak a „nyugodt” csoport tagjaihoz, például iskolázottság tekintetében. Ebben a csoportban a legnagyobb az idősebb válaszadók aránya (ugyanakkor ez nem jelentősen tér el a „magabiztos” csoport arányaitól). Kiemelhető, hogy ők vásárolnak a leggyakrabban interneten, gyakrabban Közép-magyarországiak és magasabb fizetésekkel rendelkeznek (bár utóbbiak közül egyik sem szignifikáns). Saját bevallásuk szerit a mintán belül ők tartanak legkevésbé lépést a technológiai fejlesztésekkel és náluk a legkisebb az IT területen jártas válaszadók aránya. Számukra alkalmazás választásánál leginkább fontos szempont, hogy egy alkalmazás biztonságos legyen és megbízhatóan kezelje az adataikat, valamint hogy elérhető legyen az alkalmazás magyarul, tehát a „tudatos” csoport fele valószínűleg nem tud angolul. Ők fogadják el a legkevésbé automatikusan az engedélykéréseket, ugyanakkor ők is tartják a legkevésbé valószínűnek, hogy feltörik a jövőben az okoseszközeiket. Ők használnak arányaiban a legkevésbé egészség és fitnesz alkalmazásokat, ez igaz a COVID témájú applikációkra is. A „nyugodt” csoport látszólag alacsonyabb szintű biztonságtudatosságot mutat, ők érzik a legalacsonyabb szintű biztonsági kockázatot és a biztonságot semlegesen ítélik meg. Ennek ellenére a biztonságot célzó viselkedésük hasonló a „tudatos” társaikéhoz. A mintát tekintve második helyen állnak a megtett biztonsági intézkedések számát tekintve. Ebben a csoportban a legmagasabb a fiatalok aránya. Hasonló az iskolázottságuk a „tudatosok” csoportjához. A mintán belül náluk a legmagasabb a Nyugat-dunántúliak aránya, de a többi arányban hasonlítanak például a „tudatos” csoporthoz. A legtöbb válasz esetében a csoport tagjai a középutat képviselik, egyik irányba sem dőlnek túlságosan. Ilyen például a technológiával való lépéstartás, az IT jártasság, az egészség appokkal kapcsolatos kérdéseknél vagy az alkalmazásválasztásnál megjelölt szempontok aránya. Számukra utóbbinál a biztonság, valamint a csillagos és szöveges értékelések a legfontosabb szempontok. A „magabiztos” csoport rendelkezik saját bevallása szerint a legmagasabb szintű biztonságtudatossággal, és a legmagasabb észlelt kockázati szinttel is, miközben a biztonságot összességében negatívan ítéli meg. Ugyanakkor a többi klaszterhez képest ez a csoport tesz a legkevesebb biztonsági intézkedést, tehát igen különlegesek biztonsági attitűdjüket tekintve. Itt a legmagasabb az érettségi nélküliek aránya (bár eközben harmaduknak főiskolai vagy egyetemi diplomája van). Több IT jártasságú ember is a csoport tagja, akik követik a technológiai fejlődést. A csoportban a legmagasabb az Észak-magyarországi régióból származó válaszadók aránya, a többi esetben hasonlítanak a „tudatos” csoportra (Dél-Dunántúl kivételével, ahol ezen eltérés arányaiban megtalálható). Havi nettó jövedelem tekintetében, bár nem szignifikáns az összefüggés, ennél a csoportnál a legmagasabb a legkisebb sávot megjelölők aránya. Ők vásárolnak a legkisebb

arányban interneten. Számukra alkalmazásválasztásnál számít a biztonság, valamint a csillagos és szöveges értékelés, akár csak a „nyugodt” csoportnál, ugyanakkor majdnem mindegyik szempontot arányaiban kevesebben választották a csoporton belül, mint más csoportok kitöltői. Őket érdekli a legkevésbé, ha egy alkalmazás lehet, hogy nem biztonságos, nagy arányban el is fogadják automatikusan az engedélykéréseket, ha tetszik nekik az alkalmazás. Ugyanakkor a teljes mintát tekintve ők gondolják a legvalószínűbbnek, hogy a jövőben feltörik okoseszközeiket. Ők használnak leginkább egészség appokat és önkövető eszközöket, és ezek alapján ők is változtatják a mintán belül legnagyobb arányban a viselkedésüket. Ők használtak a legnagyobb arányban COVID témájú applikációkat, és ők is érzik úgy a legnagyobb arányban, hogy a COVID miatt lemondtak néhány korábban fontos jogukról.

ÖSSZEGZETT KÖVETKEZTETÉSEK- ÚJ TUDOMÁNYOS EREDMÉNYEK

A következő kutatási kérdésekkel és hipotézisekkel kezdtem a dolgozatot, melyekre összefoglalva az alábbiakban látható eredményeket találtam.

1.Kutatási kérdés: A felhasználók biztonsági szempontból ugyanúgy kezelik az egészség témájú applikációkat, mint bármilyen más témájú alkalmazást?

A kutatási témám az egészséggel és életmóddal kapcsolatos alkalmazások biztonsági vetületeit, az azokkal kapcsolatos felhasználói biztonsági attitűdöket vizsgálta, azonban a szakirodalmi áttekintés és az egyes elemeket megalapozó kisebb kutatások során úgy tűnt, hogy a biztonsági attitűd szempontjából az alkalmazás témája nem lesz mérvadó. A kérdőív ennek figyelembevételével nem kifejezetten az ilyen témájú alkalmazásokról szól. A **H1** szerint: A felhasználók alkalmazás használatában biztonsági szempontból különbség van az egészség témájú applikációk és bármilyen más témájú alkalmazás között. Ez azért fontos, mert az ilyen típusú alkalmazások különleges besorolású személyes adatokat, egészségügyi adatokat tartalmazhatnak. A feltevést két módon is vizsgáltam a dolgozatban, és alátámasztottam, hogy biztonsági attitűd szempontból nincs különbség az alkalmazások között (tehát H1-et elvetettem). Először is az attitűd két pilléréről, a biztonságtudatosságról és a biztonsággal kapcsolatos érzelmekről, szóló kérdéseket összevetettem az egészség alkalmazást használók és nem használók körében. A válaszokban nem volt megfigyelhető szignifikáns eltérés a két esetben. A második módja az állítás tesztelésének a személyes adatok felhasználásáról való tudás fontosságát vetette össze az egészségügyi adatokéval. Ezesetben megfigyelhető volt, hogy a válaszadók a személyes adataikat jobban féltették, mint az egészségügyi adataikat. Ez

szintén alátámasztja, hogy az alkalmazásba bekerülő egészséggel kapcsolatos adatok nem befolyásolják a biztonsági attitűdöt.

1. tézis: A felhasználók alkalmazás használatában biztonsági szempontból nincs különbség az egészség témájú applikációk és bármilyen más témájú alkalmazás között.

2.Kutatási kérdés: Hogyan írható le a válaszadók biztonsági attitűdje? (Melyből következtetéseket vonhatunk le a magyar lakosság biztonsági attitűdjeire.)

A kutatási kérdésre való válaszkeresés alapja a biztonsági attitűd összetevői közötti kapcsolat feltételezése volt. A logika szerint a felhasználók biztonsági ismeretei és a biztonsággal kapcsolatos érzéseik eredményezik a biztonsági viselkedésüket. A magyar lakosság biztonsági attitűdjére való következtetést a minta bizonyos szempontok szerinti reprezentativitása teszi lehetővé (nemre, régióra és település méretére teljesül, de hasonló a megoszlás kor szerint is). A **H2** hipotézist alátámasztva az elemzések során megállapítottam, hogy szignifikáns különbség van az appok tranzakcióiba vetett bizalomban biztonsági incidenssel kapcsolatos korábbi negatív tapasztalat hatására. Tehát a biztonsággal kapcsolatos attitűd egyik befolyásoló tényezője a korábbi negatív tapasztalat.

2. tézis: A korábbi biztonsági incidenssel kapcsolatos negatív tapasztalatok befolyásolják az alkalmazásokba vetett bizalmat.

A tézis egyrészt betekintést nyújt a személyes biztonsági attitűd kialakulásának hátterébe, másrészt személyre szabottá teheti például szervezetek számára a szabályzatok és tréningek fejlesztését is ezen szempont felmérésével, figyelembe véve, hogy a korábbi incidenssel kapcsolatos tapasztalattal nem rendelkező kollégák valószínűleg nagyobb kockázatot jelentenek biztonsági szempontból.

2.1. Kutatási kérdés: Csoportosíthatók-e a résztvevők biztonságtudatosságuk és biztonságérzetük alapján?

A kutatási kérdés megválaszolása során két statisztikai elemzésből származó új tudományos eredmény jött létre: a kérdőívből származó főkomponensek, valamint az ezek figyelembevételével készült klaszterek.

3. tézis: A felhasználók csoportosíthatók biztonsági attitűdjeik szerint.

Statisztikai összefüggésvizsgálat- főkomponens elemzés: A létrehozott kutatási modell alapján, melyben az attitűdelmélet, valamint a ennek gazdagításához a védelemmotivációs és

tervezett cselekvés elméleteket foglalta magában, a kérdőív első szakaszában található kérdések kifejezetten a tudással és érzelmekkel kapcsolatos attitűd összetevőire koncentráltak. Ezt főkomponens elemzéssel alátámasztottam, és három tényezőt azonosítottam: biztonságtudatosság, észlelt kockázat és biztonság megítélése- utóbbi kettőt az érzelmi attitűdkomponensként, biztonságérzetként értelmezve.

Statisztikai összefüggésvizsgálat- klaszterelemzés: Az azonosított főkomponenseket felhasználva alkottam meg a felhasználói csoportokat klaszterelemzéssel. A kognitív és affektív komponenseket figyelembe véve négy felhasználói csoportot vártam, amelyek mátrix struktúrában írhatók le. Az elméleti mátrix sorai azt mutatják, hogy a felhasználók ismerik-e, tudással rendelkeznek-e a biztonságról (a kognitív komponens), az oszlopok pedig azt, hogy a felhasználók törődnek-e a biztonsággal (az érzelmi komponens). Az elvárt csoportokból hármat sikerült azonosítani („tudatos", „nyugodt", „magabiztos"). Olyan csoportot, akik nem tartják fontosnak a biztonságot és nincsenek is biztonsági ismereteik, a minta alapján nem sikerült azonosítani, mely alátámasztja a biztonság témakörének napjainkban megfigyelhető népszerűségét (3. táblázat). A felhasználók kognitív és affektív attitűdelemek szerinti csoportosítása lehetővé teszi azok jobb megismerését, valamint a későbbiekben a biztonsággal kapcsolatos viselkedésük elemzését is. A létrehozott csoportokat a 4.8 fejezetben jellemeztem is. A biztonsági attitűd szerinti csoportosítás lehetőséget adhat személyre szabott tréningprogramok kialakítására, célzottabb vállalati kommunikációra, jobb szabályzatok kialakítására is. Ezen felül segít jobban megérteni az emberi viselkedést és annak lehetséges hátterét is. Alapot adhat akár vállalaton belüli dolgozók biztonsági attitűdjét vizsgáló felméréshez is, mely segít meghatározni a vállalati biztonsági kultúra állapotát és a lehetséges javító lépéseket is.

A **H2.1, valamint a H2.2a és H2.2b** hipotéziseket az elemzések során alátámasztva, azokat összevonva megállapítottam a 4. tézist, melyet a 12. ábra is bemutat.

4. tézis: A biztonsági attiűd elemei közötti kapcsolat leírható az alábbiak szerint.

- **A nagyobb mértékű biztonságtudatosság nagyobb mértékű biztonsági kockázatérzettel jár együtt.**
- **A biztonságtudatosság befolyásolja a biztonsági viselkedést. Minél biztonságtudatosabb a felhasználó, annál több biztonsági intézkedést tesz.**
- **A biztonságérzet befolyásolja a biztonsági viselkedést. Minél inkább érzi a felhasználó a biztonsági kockázatokat, annál több biztonsági intézkedést tesz.**

A biztonságtudatosság és az észlelt kockázat között gyenge pozitív korreláció van, azaz a nagyobb biztonságtudatosság nagyobb mértékű észlelt kockázattal jár együtt. Vagyis a biztonsággal kapcsolatos tudással rendelkezés logikus módon a felhasználókban tudatosítja az ezzel járó lehetséges kockázatokat is, ahelyett, hogy magabiztosságukat növelve csökkentené a kockázatérzetet. Ezek alapján érdemes a felhasználói tudatosság növelésére fókuszálni például vállalati, de magánéleti vonatkozásban is, hiszen így a felhasználó kockázatérzete is növelhető, ami óvatosabb használatra sarkallhatja.

Attitűdelemekből történő modellalkotás: A kutatási kérdés megválaszolása során új tudományos eredménynek tekinthető az azonosított attitűdelemek közötti kapcsolatot leíró modell létrehozása is, mely ábrázolja az elemek egymáshoz viszonyított kapcsolatát a válaszadói attitűdök alapján (12. ábra). A kognitív és affektív komponensek figyelembevételével alkotott csoportosítás alapján a kutatási kérdés a biztonságra irányuló viselkedési komponenst is felméri, megvizsgálva a három attitűdkomponens kapcsolatát a válaszadók csoportjaira. Bár az összefüggések triviális állításoknak tűnhetnek, fontosnak tartottam az attitűdelemek vizsgálata során ezek tudományos igényességgel történő alátámasztát, ezért helyet kaptak a dolgozatban. A modell bemutatja, hogy az egyes elemek hogy működnek együtt és hogyan befolyásolják egymást, ami szintén segítheti a személyreszabást a biztonság növelését célzó például vállalati intézkedések során.

Pozitív gyenge kapcsolat figyelhető meg a biztonsággal kapcsolatos tudatosság és a megtett biztonsági intézkedések számossága között. Tehát a magasabb biztonságtudatosság több intézkedéssel jár együtt, amely igazolja a H2.2a feltevést. Ez tulajdonképpen a hétköznapi szóhasználatot tekintve a biztonságtudatosság definíciójának alátámasztásaként értelmezhető, biztonsági attitűd szempontból pedig a kognitív és viselkedési elemek kapcsolatának együttállásáról szól. Ez szintén alátámasztja a biztonságtudatosság növelő képzések és kezdeményezések fontosságát, mert a tudatosság növelése alátámaszható módon összefügg a megtett biztonsági intézkedések számával is, mely összességében növeli a felhasználó biztonságát is.

Gyenge a kapcsolat a biztonsági intézkedések száma és az észlelt biztonsági kockázat mértéke között. Eszerint a H2.2b hipotézist elfogadom azzal a megkötéssel, hogy a kapcsolat gyenge. A fentiekkel összhangban az érzelmi és viselkedési attitűdelem között is kimutatható kapcsolat, mely szintén erősíti, hogy a biztonsági kockázatok tudatosítása ösztönzően hathat a felhasználói biztonsági intézkedések megtételére, azok számának növelésére.

2.3. Kutatási kérdés: Hogyan jellemezhetők a létrejött csoportok?

A kutatási kérdés megválaszolására a klaszterelemzés során létrejött csoportokat demográfiai és egyéb szempontok alapján is elemeztem. Valamint a **H2.3a**, **H2.3b** és **H2.3c** hipotéziseket is vizsgáltam, melyeket az 5. tézis foglal össze (a H2.3c hipotézis elvetésével).

5. tézis: A technológiai jártasság és az IT területen való jártasság befolyásolja a biztonsági attitűdöt az alábbiak szerint.

- **Akik biztonságtudatosabbak, azok jobban lépést tartanak a technológiai fejlődéssel, mint a kevésbé biztonságtudatosak.**
- **Az IT területen jártas válaszadók biztonságtudatosabbak, mint a területen nem jártas válaszadók.**
- **Az IT területen jártas válaszadók magasabb szintű biztonsági kockázatot észlelnek, mint a területen nem jártas válaszadók.**

Tekintve a csoportalkotásnál figyelembe vett biztonságtudatossági szintet, a H2.3a hipotézist elfogadom, tehát igaz, hogy akik tudatosabbak, jobban lépést tartanak a technológiai fejlődéssel, mint akik kevésbé azok. Bár ez szintén a köznapi beszéd szerinti tudatosság definíciójaként is értelmezhető, attitűdelemek szerinti elemzés segítségével is alátámasztható. A technológiai lépéstartást önbevallás alapján vizsgáltam, majd összevetettem a biztonságtudatosság szerinti csoportosítással. A tézisből arra lehet következtetni, hogy a biztonságtudatosság növelésének egyik lehetséges megoldása a technológiai hírek követése lehet, mely segíti, hogy a felhasználók tisztában legyenek az elérhető legújabb technológiákkal és az azokkal kapcsolatos lehetséges kockázatokkal.

A csoportkialakítási logikában szereplő biztonságtudatosságot figyelembe véve megállapítható, hogy a H2.3b hipotézist, miszerint az IT területen jártas válaszadók biztonságtudatosabbak, elfogadom. A fentieket szintén megerősítve megállapítható, hogy az IT területen való végzettség vagy tapasztalat is növelheti a biztonságtudatosságot. Ez szintén alátámasztja, hogy minél inkább rendelkezik a felhasználó tudással, annál inkább tudatos lesz az adott témában.

A H2.3c hipotézist, miszerint az IT területen jártas válaszadók alacsonyabb szintű biztonsági kockázatot észlelnek, elvetem. A 4. tézissel összhangban itt is megfigyelhető, hogy a területről való több tudás magasabb szintű kockázatérzettel jár együtt. Ez alátámasztja, hogy ha a

felhasználónak több tudása van a lehetséges kockázatokról, rossz kimenetelekről, akkor tudatosabban használja az alkalmazásokat.

3.Kutatási kérdés: Mi alapján választanak a felhasználók applikációkat? Melyek a fontos szempontok és ezek hogy függenek össze a biztonságtudatossággal és biztonsággal kapcsolatos érzelmekkel? (Mintegy biztonsági cselekvésként értelmezve az alkalmazásválasztást is.)

Az utolsó kutatási kérdésben az alkalmazásválasztás szempontjait vizsgáltam. Az összes válaszadót figyelembe véve a biztonság, a megosztott adatok megbízható kezelése és a csillagos és szöveges értékelések a válaszadók körében legnépszerűbb szempontok. Előbbi kettőnél a kérdőív ugyan nem tért ki arra, hogy ezt honnan tudják megállapítani a kitöltők, de a korábbi válaszok alapján többek között az alkalmazásboltok megbízhatóságába és az appok frissítésébe vetett bizalom adhatja meg erre a kérdésre a választ. Ezen kívül a felhasználói és adatvédelmi tájékoztatók is sokat segíthetnek az alkalmazás által készen elérhető biztonsági szint megértésében.

H3: A biztonság az elsődleges választási szempontok közé tartozik az applikációk választásánál.

A H3 hipotézist igazoltam, megalkotva a 6. tézist.

6. tézis: A biztonság az elsődleges választási szempontok közé tartozik az applikációk választásánál. Hozzátéve, hogy az egyéb említett lehetséges választási szempontok sokkal könnyebben észlelhetők a felhasználók számára, míg a biztonság ennél komplexebb utánajárást igényelne, mely lehetséges megoldásaira szintén kitértem a korábbiakban (3.4. fejezet).

A fenti eredményeket a 11. táblázat foglalja össze. A mobil alkalmazások célcsoportjainak, felhasználóinak attitűdjeit, valamint azok tulajdonságait meghatározva és a számukra fontosabb szempontokat megértve következtethetünk arra, hogy az alkalmazások használata közben milyen lesz a viselkedésük. A felhasználói csoport hovatartozások, így a dolgozat eredményei, gyakorlati megfontolások alapjául is szolgálhatnak akár az alkalmazásfejlesztők, akár a felhasználók, akár a munkáltatók számára. Az eredmények azt is alátámasztják, hogy a felhasználói biztonságtudatosság növelését célzó képzéseknek, tudatosító kampányoknak valódi szerepe lehet a felhasználói biztonság növelésében.

Kutatási Cél	Kutatási Kérdés	Feltevések	Eredmények	Tézisek
1. Meghatározni, hogy van-e különbség felhasználói biztonsági attitűd szempontból az egészség témájú és egyéb alkalmazások között.	**1.** A felhasználók biztonsági szempontból ugyanúgy kezelik az egészség témájú applikációkat, mint bármilyen más témájú alkalmazást?	**H1**: A felhasználók alkalmazás használatában biztonsági szempontból különbség van az egészség témájú applikációk és bármilyen más témájú alkalmazás között.	Elvetem.	**1. tézis: A felhasználók alkalmazás használatában biztonsági szempontból nincs különbség az egészség témájú applikációk és bármilyen más témájú alkalmazás között.**
2. Kérdőíves kutatással vizsgálni a válaszadók biztonsági attitűdjét.	**2.** Hogyan írható le a válaszadók biztonsági attitűdje? (Melyből következtetéseket vonhatunk le a magyar lakosság biztonsági attitűdjeire.)	**H2**: A korábbi biztonsági incidenssel kapcsolatos negatív tapasztalatok befolyásolják az alkalmazásokba vetett bizalmat.	Igazoltam.	**2. tézis: A korábbi biztonsági incidenssel kapcsolatos negatív tapasztalatok befolyásolják az alkalmazásokba vetett bizalmat.**
2.1. A válaszadók biztonságtudatosság és biztonságérzet alapján való csoportosítása.	**2.1.** Csoportosíthatók-e a résztvevők biztonságtudatosságuk és biztonságérzetük alapján?	Statisztikai összefüggésvizsgálat- Főkomponens elemzés		**3. tézis: A felhasználók csoportosíthatók biztonsági attitűdjeik szerint.**
		Statisztikai összefüggésvizsgálat- Klaszterelemzés		
		H2.1: A nagyobb mértékű biztonságtudatosság nagyobb mértékű biztonsági kockázatérzettel jár együtt.	Igazoltam.	**4. tézis: A biztonsági attiűd elemei közötti kapcsolat leírható az alábbiak szerint.** - A nagyobb mértékű biztonságtudatosság nagyobb mértékű biztonsági kockázatérzettel jár együtt. -A biztonságtudatosság befolyásolja a biztonsági viselkedést. Minél biztonságtudatosabb a felhasználó, annál több biztonsági intézkedést tesz. -A biztonságérzet befolyásolja a biztonsági viselkedést. Minél inkább érzi a felhasználó a biztonsági kockázatokat, annál több biztonsági intézkedést tesz.
2.2. A meghatározott csoportok biztonságra irányuló magatartásának vizsgálata.	**2.2.** Hogyan hat a biztonságtudatosság és a biztonsággal kapcsolatos érzések alapján meghatározott csoporthovatartozás a biztonságra irányuló magatartásra?	Attitűdelemekből történő modellalkotás		
		H2.2a: A biztonságtudatosság befolyásolja a biztonsági viselkedést. Minél magasabb a biztonságtudatossága egy felhasználónak, annál több biztonsági intézkedést tesz.	Igazoltam.	
		H2.2b: A biztonságérzet befolyásolja a biztonsági viselkedést. Minél inkább érzi a felhasználó a biztonsági kockázatokat, annál több biztonsági intézkedést tesz.	Igazoltam.	
2.3. Létrehozott felhasználói csoportok egyéb jellemzők mentén történő elemzése.	**2.3.** Hogyan jellemezhetők a létrejött csoportok?	**H2.3a**: Akik biztonságtudatosabbak, azok jobban lépést tartanak a technológiai fejlődéssel, mint a kevésbé biztonságtudatosak.	Igazoltam.	**5. tézis: A technológiai jártasság és az IT területen való jártasság befolyásolja a biztonsági attitűdöt az alábbiak szerint.** - Akik biztonságtudatosabbak, azok jobban lépést tartanak a technológiai fejlődéssel, mint a kevésbé biztonságtudatosak. -Az IT területen jártas válaszadók biztonságtudatosabbak, mint a területen nem jártas válaszadók. -Az IT területen jártas válaszadók magasabb szintű biztonsági kockázatot észlelnek, mint a területen nem jártas válaszadók.
		H2.3b: Az IT területen jártas válaszadók biztonságtudatosabbak, mint a területen nem jártas válaszadók.	Igazoltam.	
		H2.3c: Az IT területen jártas válaszadók alacsonyabb szintű biztonsági kockázatot észlelnek, mint a területen nem jártas válaszadók.	Elvetem.	
3. Felhasználói alkalmazás választási szempontok meghatározása.	**3.** Mi alapján választanak a felhasználók applikációkat? Melyek a választási szempontok és ezek hogy függenek össze a biztonságtudatossággal és biztonsággal kapcsolatos érzelmekkel?	**H3**: A biztonság az elsődleges választási szempontok közé tartozik az applikációk választásánál.	Igazoltam.	**6. tézis: A biztonság az elsődleges választási szempontok közé tartozik az applikációk választásánál.**

11. táblázat Eredmények összefoglalása

AJÁNLÁSOK

A kutatás eredményei számos területen használhatók. Egyrészt megalapozhatnak további kutatásokat, másrészt segíthetnek a felhasználók jobb megértésében, a tudatosság növelésében, és a biztonságos alkalmazáshasználat elterjedésében. Ezen kívül vállalati környezetben is jól használhatók a már említett módokon:

- Biztonságtudatossági programok és tréningek fejlesztése,
- Személyre szabott megközelítés, célzott kommunikáció,
- Szabályzatfejlesztés, irányelvek fejlesztése,
- Biztonsági kultúra felmérése és előmoztítása.

A jövőbeli kutatási irányok tovább konkretizálhatják a kérdéseket esetleg alkalmazás fókuszúan, vagy tovább vizsgálhatják a felhasználókat más szempontok, például egyéb alkalmazás használati vagy online viselkedési szokások szerint is, melyek még átfogóbb képet adhatnak az attitűdjüket meghatározó tényezőkről. Hiszen a biztonsági attitűd az adott helyzet függvénye is lehet. Ezeket akár kisérletekkel, akár a kérdőív kibővítésével lehet vizsgálni. Lehetséges logikus folytatás még a fentiek alapján történő fókuszcsoportos beszélgetés is, az azonosított felhasználói csoportok jobb megértésére. Az attitűdök még jobb megértése érdekében az alkalmazáshasználat lehetséges motivációit is érdemes vizsgálni, jelen dolgozat fókusza a felhasználói oldal ezen részét nem vizsgálta alaposabban.

A felhasználók jobb megértése az értéklánc minden résztvevőjének segíthet a biztonság növelésében. Felhasználói oldalról az attitűdök megértése segíthet a felhasználó saját maga által betöltött szerepének felismerésében, mely a gyenge pontok azonosítását is lehetővé teszi, kiemelve, hogy melyik területekre érdemes fókuszálnia biztonság tekintetében. Fontos lehet azt is felismerni, hogy bár számára a biztonság fontos, lehet, hogy több intézkedést is tehetne a biztonságos alkalmazáshasználat érdekében. Alkalmazás szolgáltatói, gyártói oldalról segítheti például annak meghatározását, hogy milyen intézkedéseket várnak el a felhasználók és ezeket hogyan lehet a felhasználó tudtára adni, hogyan lehet megmutatni, hogy egy alkalmazás biztonságos. Fontos a tudatosítás erről az oldalról is, például a lehetséges veszélyekre való figyelem felhívása. Szabályozói oldalról pedig a már megalkotott szabályok finomítása és a további tutatosítás a feladatok. Annak biztosítása azonban, hogy a felhasználók tudják, hogy mit jelent a biztonságos alkalmazáshasználat és meg is tegyék az ehhez szükséges lépéseket, minden szereplő feladata és közös érdeke.

IRODALOMJEGYZÉK

[1] S. Kemp, „DIGITAL 2021: GLOBAL OVERVIEW REPORT,” 27 01 2021. [Online]. Available: https://datareportal.com/reports/digital-2021-global-overview-report. [Hozzáférés dátuma: 06 03 2021].

[2] D. Horváth, N. Nyirő és T. Csordás, Médiaismeret Reklámeszközök és reklámhordozók- Első magyar nyelvű digitális kiadás, Budapest: Akadémiai Kiadó, 2016.

[3] KSH, „12.1.1.1. Az információ, kommunikáció főbb mutatói,” KSH (Hungarian Central Statistical Office), Budapest, 2022.

[4] KSH, „GYORSABB INTERNET MELLETT STAGNÁLT A VEZETÉKES NET ADATLETÖLTÉSI FORGALMA- Internethasználat, 2022. II. negyedév,” KSH (Hungarian Central Statistical Office), Budapest, 2022.

[5] KSH, „12.1.1.14. A háztartások internetkapcsolat típusainak aránya,” KSH (Hungarial Central Statistical Office), Budapest, 2022.

[6] KSH, „12.1.1.16. Az internethasználat gyakoriságának megoszlása,” KSH (Hungarian Central Statistical Office), Budapest, 2022.

[7] KSH, „12.1.3.4. Internethasználók aránya [a 16–74 éves népesség százalékában],” KSH (Hungarian Central Statistical Office), Budapest, 2021.

[8] L. McCormack, „Mobile App Download Statistics & Usage Statistics (2023),” https://buildfire.com, 01 06 2023. [Online]. Available: https://buildfire.com/app-statistics/. [Hozzáférés dátuma: 03 07 2023].

[9] A. Dogtiev, „Businessofapps.com,” 16 10 2017. [Online]. Available: http://www.businessofapps.com/data/app-statistics/#1.

[10] R. J. Sobhany, Mobilize, New York: Vanguard Press, 2011.

[11] Google.com, „Google.com,” 04 11 2017. [Online]. Available: https://privacy.google.com/your-data.html.

[12] S. Barth és M. D. de Jong, „The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review,” *Telematics and Informatics*, %1. kötet34, %1. szám7, pp. 1038-1058, 2017.

[13] K. R. Szűcs, „How do we choose our apps?,” In: Pal, Feher - Polgar (szerk.) FIKUSZ 2017 - Symposium for Young Researchers: Proceedings. Budapest, Magyarország : Óbudai Egyetem, Keleti Károly Gazdasági Kar (2017) 368 p. pp. 323-334. , 12 p., 2017.

[14] K. R. Szűcs, „MOBILE SECURITY BASICS TO IMPROVE PERSONAL AND CORPORATE SAFETY,” *NATIONAL SECURITY REVIEW : PERIODICAL OF THE MILITARY NATIONAL SECURITY SERVICE*, %1. szám2, pp. 56-72, 2019.

[15] K. R. Szűcs, „Biztonsági kockázatok csökkentése a mindennapokban,” *In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2*, pp. 247 p. pp. 82-94. , 13 p., 2019.

[16] K. Dudás, „Az egészségtudatos vásárlói magatartás jellemzői -szakirodalmi összefoglalás,” 01 12 2015. [Online]. Available: https://ktk.pte.hu/sites/ktk.pte.hu/files/images/szervezet/intezetek/mti/dudas_az_egeszsegtudatos_vasarloi_magatartas_jellemzoi_2015.pdf. [Hozzáférés dátuma: 01 03 2021].

[17] R. Z. Reicher és G. Rácz, „LOHAS témák megjelenése az offline és online,” in *Gazdaság & Társadalom* , Budapest, 2012.

[18] D. Weinswig, „Forbes.com,” 30 06 2017. [Online]. Available: https://www.forbes.com/sites/deborahweinswig/2017/06/30/wellness-is-the-new-luxury-is-healthy-and-happy-the-future-of-retail/#4d20b2d18323.

[19] G. Buttarelli és EDPS, „Opinion 1/2015 Mobile Health, Reconciling technological innovation with data protection,” European Data Protection Supervisor, EDPS, Brussels, 2015.

[20] European Commission, „GREEN PAPER- on mobile Health ("mHealth"),” 4 10 2014. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth. [Hozzáférés dátuma: 04 03 2021].

[21] PWC, „PWC,” 20 03 2014. [Online]. Available: https://www.pwc.com/gx/en/healthcare/mhealth/assets/pwc-emerging-mhealth-full.pdf.

[22] D. Lazer, R. Kennedy, G. King és A. Vespignani, „The Parable of Google Flu: Traps in Big Data Analysis,” Science, Vol. 343, Issue 6176, pp. 1203-1205, 14 03 2014. [Online]. Available: https://science.sciencemag.org/content/343/6176/1203. [Hozzáférés dátuma: 01 03 2021].

[23] G. Ritzer, P. Dean és N. Jurgenson, „The Coming of Age of the Prosumer,” American Behavioral Scientist, 07 03 2017. [Online]. Available: http://journals.sagepub.com/doi/abs/10.1177/0002764211429368.

[24] K. R. Szűcs, „Mobile health – on overwiew,” *BIZTONSÁGTUDOMÁNYI SZEMLE*, %1. kötetKülönszám, pp. 79-91, 2021.

[25] B. Fogg, Persuasive Technology- Using Computers to Change What We Think and Do, Stanford: Elsevier, 2003.

[26] H. Oinas-Kukkonen és M. Harjumaa, „Persuasive Systems Design: Key Issues, Process,” 01 03 2009. [Online]. Available: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3424&context=cais. [Hozzáférés dátuma: 01 04 2021].

[27] nnk.gov.hu, „A COVID-19 fertőzés legfontosabb jellemzői (1. sz melléklet – COVID-19 eljárásrend 2020. március 30.),” 30 03 2020. [Online]. Available: https://www.nnk.gov.hu/attachments/article/567/1_sz_mell%C3%A9klet_ismertet%C5%91_2020_03_30.pdf. [Hozzáférés dátuma: 05 04 2020].

[28] WHO, „WHO announces COVID-19 outbreak a pandemic,” euro.who.int, 12 03 2020. [Online]. Available: http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2020/3/who-announces-covid-19-outbreak-a-pandemic. [Hozzáférés dátuma: 01 04 2020].

[29] WHO, „Contact tracing,” who.int, 09 05 2017. [Online]. Available: https://www.who.int/news-room/q-a-detail/contact-tracing. [Hozzáférés dátuma: 28 03 2020].

[30] eHealth Network, „Mobile applications to support contact tracing in the EU’s fight against COVID-19,” 15 04 2020. [Online]. Available: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf. [Hozzáférés dátuma: 20 04 2020].

[31] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. l Parker, D. Bonsall és C. Fraser, „Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing,” Science- science.sciencemag.org, 31 03 2020. [Online]. Available: https://science.sciencemag.org/content/early/2020/04/09/science.abb6936.full. [Hozzáférés dátuma: 10 04 2020].

[32] H. Cho, D. Ippolito és Y. W. Yu, „Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs,” Cornell University, 30 03 2020. [Online]. Available: https://arxiv.org/abs/2003.11511. [Hozzáférés dátuma: 02 04 2020].

[33] Y. Huang, M. Sun és Y. Sui, „How Digital Contact Tracing Slowed Covid-19 in East Asia,” Harvard Business Review, 15 04 2020. [Online]. Available: https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia. [Hozzáférés dátuma: 16 04 2020].

[34] Vírusradar, „virusradar.hu,” [Online]. Available: https://virusradar.hu/. [Hozzáférés dátuma: 01 03 2021].

[35] Házi Karantén Rendszer, „hazikaranten.hu,” [Online]. Available: https://hazikaranten.hu/hogyan-mukodik-az-applikacio/. [Hozzáférés dátuma: 10 03 2021].

[36] A. Kapoor, S. Guha, M. K. Das, K. C. Goswami és R. Yadav, „Digital healthcare: The only solution for better healthcare during COVID-19 pandemic?,” Indian Heart Journal, 11 04 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7151273/. [Hozzáférés dátuma: 15 04 2020].

[37] A. Holmes, „Facebook, Google, and Apple are using data from millions of users to map COVID-19 and people's movements. Here are all the coronavirus maps and dashboards made by tech giants you can explore today,” businessinsider.com, 21 04 2020. [Online]. Available: https://www.businessinsider.com/explore-coronavirus-maps-made-from-facebook-google-apple-user-data-2020-4. [Hozzáférés dátuma: 21 04 2020].

[38] K. R. Szűcs és D. Maros, „Mobile Usage during COVID-19,” in *CANDO-EPE 2020 - Proceedings, IEEE 3rd International Conference and Workshop in Obuda on Electrical and Power Engineering*, Budapest, 2020.

[39] T. Klein és A. Tóth, Technológia jog – Robotjog – Cyberjog (online verzió), Budapest, 2019.

[40] L. Muha, „Az informatikai biztonság egy lehetséges rendszertana,” *BOLYAI SZEMLE- ISSN 1416-1443*, %1. kötet17 (4), pp. 137-156, 2008.

[41] L. Kovács, A kibertér védelme, Budapest: Dialóg Campus Kiadó, 2018.

[42] Uni-NKE.hu, „Közszolgálati Online Lexikon,” Nemzeti Közszolgálati Egyetem, [Online]. Available: https://lexikon.uni-nke.hu/szocikk/biztonsag-2/. [Hozzáférés dátuma: 01 06 2023].

[43] G. Tarján, „AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN- Doktori Értekezés,” 01 01 2020. [Online]. Available: https://phd.lib.uni-corvinus.hu/1090/1/Tarjan_Gabor_dhu.pdf. [Hozzáférés dátuma: 01 06 2023].

[44] Arcanum, „Arcanum Kézikönyvtár, A magyar nyelv értelmező szótára,” 01 01 2023. [Online]. Available: https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/b-1EF8E/biztonsagerzet-211A3/. [Hozzáférés dátuma: 01 06 2023].

[45] T. Szádeczky és G. L. Szőke, „A bizalmasság és a nyilvánosság aktuális kihívásai az információbiztonság tükrében,” *ProFuturo*, %1. kötet8, %1. szám2, pp. 24-41, 2018.

[46] L. Kovács, Kiberbiztonság és -stratégia, Budapest: Dialóg Campus Kiadó, 2018.

[47] Jogtár, „2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,” 01 01 2014. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv. [Hozzáférés dátuma: 24 03 2021].

[48] ISC2, „Official ISC2 CC Online Self-Paced Training”.

[49] S. Zuboff, The Age of Surveillance Capitalism- The Fight for the Future at the New Frontier of Power, London: Profile Books, 2019.

[50] S. Arora, J. Yttri és W. Nielsen, „PubMed,” 01 04 2017. [Online]. Available: http://pubmedcentralcanada.ca/pmcc/articles/PMC4432854/.

[51] A. Hess, „NYTimes.com,” 09 05 2017. [Online]. Available: https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html.

[52] D. Solove, „10 Reasons Why Privacy Matters,” TeachPrivacy, 20 01 2014. [Online]. Available: https://teachprivacy.com/10-reasons-privacy-matters/. [Hozzáférés dátuma: 01 04 2020].

[53] R. A. Calvo, S. Deterding és R. M. Ryan, „Health surveillance during covid-19 pandemic,” 06 04 2020. [Online]. Available: https://www.bmj.com/content/369/bmj.m1373. [Hozzáférés dátuma: 10 04 2020].

[54] Check Point, „Checkpoint- CHECK POINT SANDBLAST MOBILE,” 25 11 2018. [Online]. Available: https://www.checkpoint.com/downloads/products/sandblast-mobile-datasheet.pdf. [Hozzáférés dátuma: 20 09 2019].

[55] Google, „Potentially Harmful Applications (PHAs),” 01 03 2021. [Online]. Available: https://developers.google.com/android/play-protect/potentially-harmful-applications. [Hozzáférés dátuma: 01 03 2021].

[56] J. Hildenbrand, „Android Central- What is sideloading,” 02 02 2012. [Online]. Available: https://www.androidcentral.com/what-sideloading-android-z. [Hozzáférés dátuma: 20 09 2019].

[57] N. Statt, „The Verge- This illicit iPhone app store has been hiding in plain sight,” 20 02 2019. [Online]. Available: https://www.theverge.com/2019/2/20/18232140/apple-tutuapp-piracy-ios-apps-developer-enterprise-program-misuse. [Hozzáférés dátuma: 30 09 2019].

[58] Google, „Malware categories,” 01 03 2021. [Online]. Available: https://developers.google.com/android/play-protect/phacategories. [Hozzáférés dátuma: 01 03 2021].

[59] J. Vávra, „Avast researchers discover 47 apps on Play Store with intrusive ads and stealth features.,” Avast, 23 06 2020. [Online]. Available: https://blog.avast.com/avast-discovers-47-android-adware-apps-avast. [Hozzáférés dátuma: 02 05 2021].

[60] V. Chebyshev, „Mobile malware evolution 2020,” Securelist by Kaspersky, 01 03 2021. [Online]. Available: https://securelist.com/mobile-malware-evolution-2020/101029/. [Hozzáférés dátuma: 01 05 2021].

[61] ENISA, „Malware- ENISA Threat Landscape,” 01 01 2020. [Online]. Available: https://www.enisa.europa.eu/publications/malware. [Hozzáférés dátuma: 01 03 2021].

[62] ENISA, „Malware,” 01 01 2020. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware. [Hozzáférés dátuma: 01 03 2021].

[63] Norton, „What is mobile ransomware?,” Norton, 01 01 2020. [Online]. Available: https://us.norton.com/internetsecurity-mobile-what-is-mobile-ransomware.html. [Hozzáférés dátuma: 10 05 2021].

[64] Penta Security, „Top 7 Most Common Types of Cyberattacks on Web Applications in 2020,” 19 03 2020. [Online]. Available: https://www.pentasecurity.com/blog/top-7-common-types-cyberattacks-web-applications/. [Hozzáférés dátuma: 01 03 2021].

[65] K. Mitnick és W. Simon, A legendás hacker- A megtévesztés művészete, Budapest: Perfact-Pro, 2002.

[66] ENISA, „What is "Social Engineering"?,” 01 01 2021. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering. [Hozzáférés dátuma: 01 03 2021].

[67] R. B. Cialdini, Hatás- A befolyásolás pszichológiája, Budapest: HVG Könyvek, 2009.

[68] Proofpoint, „proofpoint.com,” 01 01 2019. [Online]. Available: https://www.proofpoint.com/us/resources/threat-reports/human-factor. [Hozzáférés dátuma: 05 12 2019].

[69] ENISA, „ENISA Threat Landscape Report 2018- 15 Top Cyberthreats and Trends,” European Union Agency for Network and Information Security (ENISA), Athens, 2018.

[70] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, „Security Tip (ST05-003)- Securing Wireless Networks,” CISA, 05 08 2020. [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST05-003. [Hozzáférés dátuma: 03 04 2021].

[71] Cisco Press, „Wireless Security,” 16 07 2004. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=177383&seqNum=5. [Hozzáférés dátuma: 03 04 2021].

[72] D. Balaban, „11 Types of Spoofing Attacks Every Security Professional Should Know About,” Security Magazine, 24 03 2020. [Online]. Available: https://www.securitymagazine.com/articles/91980-types-of-spoofing-attacks-every-security-professional-should-know-about. [Hozzáférés dátuma: 04 04 2021].

[73] Fortinet, „Eavesdropping,” 01 01 2020. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/eavesdropping. [Hozzáférés dátuma: 05 04 2021].

[74] L. Muha és C. Krasznay, Az elektronikus információs rendszerek biztonságának menedzselése, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[75] B. Canner, „The Top 7 Password Attack Methods (And How to Prevent Them),” Identity Management Solutions Review, 12 10 2019. [Online]. Available: https://solutionsreview.com/identity-management/the-top-7-password-attack-methods-and-how-to-prevent-them/. [Hozzáférés dátuma: 20 04 2021].

[76] V. Highfield, „ALPHR.com- The top ten password-cracking techniques used by hackers,” 26 06 2018. [Online]. Available: https://www.alphr.com/features/371158/top-ten-password-cracking-techniques. [Hozzáférés dátuma: 06 10 2019].

[77] Deloitte, „Mobile devices- Secure or security risk? Deloitte research highlights the dangers of data theft from mobile devices.,” 01 01 2020. [Online]. Available: https://www2.deloitte.com/ie/en/pages/risk/articles/mobile-devices-security.html. [Hozzáférés dátuma: 20 04 2021].

[78] K. R. Szűcs, A. Őszi és T. Kovács, „Mobile Biometric Solutions from Big Tech Companies,” *HADMÉRNÖK*, %1. kötet15, %1. szám3, pp. 5-16, 2020.

[79] K. R. Szűcs, A. Őszi és T. Kovács, „Mobile Biometrics and their Risks,” *HADMÉRNÖK,* %1. kötet15, %1. szám4, pp. 15-27, 2020.

[80] A. Mathew, „Subtlety is the Future of Biometric Authentication,” Counter Point , 04 10 2018. [Online]. Available: https://www.counterpointresearch.com/subtlety-future-biometric-authentication/. [Hozzáférés dátuma: 04 05 2021].

[81] Apple, „About Touch ID advanced security technology,” Apple, 11 09 2017. [Online]. Available: https://support.apple.com/en-bn/HT204587. [Hozzáférés dátuma: 03 05 2021].

[82] Samsung, „Samsung Pass,” Samsung, 01 01 2021. [Online]. Available: www.samsung.com/uk/apps/samsung-pass/. [Hozzáférés dátuma: 03 05 2021].

[83] A. K. Jain, A. A. Ross és K. Nandakumar, Introduction to biometrics, London: Springer, 2011.

[84] J. Ashbourn, Biometrics in the new world, London: Springer, 2014.

[85] T. Ford, „Business Daily- Boom time for scammers,” BBC, London, 2021.

[86] V. Varadaraj, „The Future of Mobile in a Post-COVID World & How to Stay Secure,” McAfee, 09 07 2021. [Online]. Available:

https://www.mcafee.com/blogs/mobile-security/the-future-of-mobile-in-a-post-covid-world-how-to-stay-secure/. [Hozzáférés dátuma: 14 01 2022].

[87] Interpol, „COVID-19 cyberthreats," Interpol.int, 01 01 2022. [Online]. Available: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats. [Hozzáférés dátuma: 05 01 2022].

[88] K. R. Szűcs és R. Z. Reicher, „Mobile Application Security," *Management, Enterprise and Benchmarking in the 21st Century*, pp. 510 p. pp. 357-364. , 8 p., 2017.

[89] . Á. Hofmeister-Tóth, A FOGYASZTÓI MAGATARTÁS ALAPJAI (THE FUNDAMENTALS OF CONSUMER BEHAVIOR), Budapest: Akadémiai Kiadó, 2014.

[90] G. Rekettye , T. Tóth és E. Malota , Nemzetközi marketing- Online version, Budapest: Akadémiai Kiadó, 2016, p. 116.

[91] J. K. Chan, „Understanding the Tourists' Attitudes toward Participating Nature-Based Tourism," *PROCEEDINGS FOR EURO-ASIA CONFERENCE ON ENVIRONMENT AND CORPORATE SOCIAL RESPONSIBILITY: TOURISM AND MANAGEMENT SESSION*, pp. 156-168, 2008.

[92] A. T. S. E. U. G. T. Y. K. Aydina, „Attitudes of Potential Consumers toward Country-of-Origin and Auto Brand Images," *Serbian Journal of Management*, %1. kötet2, %1. szám2, pp. 205 - 216, 2007.

[93] D. Ashenden, „In their own words: employee attitudes towards information security," *Information and Computer Security*, %1. kötet26, %1. szám3, pp. 327-337, 2018.

[94] R. W. Rogers, „Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation.," *Social Psychophysiology*, p. 153–177, 1983.

[95] J. Cox, „Information systems user security: A structured model of the knowing–doing gap," *Computers in Human Behavior*, pp. 1849-1858, 2012.

[96] Y. Chen és F. M. Zahedi, „Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China," *MIS Quarterly: Management Information Systems*, %1. kötet40, %1. szám1, pp. 205-222, 2016.

[97] I. Ajzen, „The theory of planned behavior," *The theory of planned behavior*, %1. kötet50, %1. szám2, pp. 179-211, 1991.

[98] I. Ajzen, „Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior," *Journal of Applied Social Psychology*, %1. kötet32, %1. szám4, pp. 665 - 683, 2002.

[99] C. J. Armitage és M. Conner, „Efficacy of the theory of planned behaviour: A meta-analytic review," *British Journal of Social Psychology,* %1. kötet40, %1. szám4, pp. 471 - 499, 2001.

[100] T. Dinev és Q. Hu, „The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems,* %1. kötet8, %1. szám7, pp. 386 - 408, 2007.

[101] N. Thompson, . T. J. McGill és X. Wang, „"Security begins at home": Determinants of home computer and mobile device security behavior," *Computers & Security,* pp. 376-391, 2017.

[102] R. Behardien és I. Brown, „Factors Influencing Smartphone End-User Security Behaviour – The Case of Young Adults in South Africa," in *2022 IST-Africa Conference (IST-Africa),* Ireland, 2022.

[103] B. Ali, R. N. Hamid és S. Rajiv, „Mobile application security: Role of perceived privacy as the predictor of security perceptions," *International Journal of Information Management,* %1. kötet52, %1. szám07, 2020.

[104] T. Chun-Yen, S. Wen-Ling, H. Fu-Pei, C. Yun-An, L. Chien-Liang és W. Hui-Ju, „Using the ARCS model to improve undergraduates' perceived information security protection motivation and behavior," *Computers & Education,* %1. kötet181, %1. szám05, 2022.

[105] H. Mark A., B. Robert és G. C. Amita, „Identifying factors influencing consumers' intent to install mobile applications," *International Journal of Information Management,* %1. kötet36, %1. szám3, 2016.

[106] B. Susanne, d. J. Menno D.T., J. Marianne, H. Pieter H. és R. Janina C., „Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics and Informatics,* %1. kötet41, %1. szám08, pp. 55-69, 2019.

[107] M. Kateryna és L. Christoph, „A quantum of self: A study of self-quantification and self-disclosure," *Computers in Human Behavior,* %1. kötet81, %1. szám04, pp. 102-114, 2018.

[108] A. Solomon, . M. Michaelshvili, R. Bitton, B. Shapira, L. Rokach, R. Puzis és A. Shabtai, „Contextual security awareness: A context-based approach for assessing the security awareness of users," *Knowledge-Based Systems,* %1. kötet246, 2022.

[109] A. J. Olak, I. Hejduk, W. Karwowskic, P. Tomczykd , J. Fazlagić, P. Gacf , H. Hejduk, S. Sobolewska, E. Çakıt és O. A. Alrehailii, „The relationships between the use of smart mobile technology, safety knowledge and propensity to follow safe practices at work," *International Journal of Occupational Safety and Ergonomics,* %1. kötet27, %1. szám3, pp. 911-920, 2021.

[110] ENISA, „Privacy and data protection in mobile applications- A study on the app development ecosystem and the technical implementation of GDPR," 01 01 2017. [Online]. Available: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications. [Hozzáférés dátuma: 21 03 2021].

[111] A. Kurtz, H. Gascon, T. Becker és K. Rieck, „Fingerprinting Mobile Devices Using Personalized Configurations," Proceedings on Privacy Enhancing Technologies 2016(1), 01 01 2016. [Online]. Available: https://www.researchgate.net/publication/282894103_Fingerprinting_Mobile_Devices_Using_Personalized_Configurations. [Hozzáférés dátuma: 21 03 2021].

[112] W. Melicher, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor és M. L. Mazurek, „Usability and Security of Text Passwords on Mobile Devices," 01 01 2016. [Online]. Available: https://www.andrew.cmu.edu/user/nicolasc/publications/M+-CHI16.pdf. [Hozzáférés dátuma: 21 03 2021].

[113] Z. Batyi, „kozlekedesvilag.hu," 30 04 2019. [Online]. Available: https://www.kozlekedesvilag.hu/2018/08/24/minden-amit-gdpr-rol-tudni-erdemes/.

[114] Á. Kéri és T. Kancsal, „Adatvédelem a gyakorlatban," HVG, Budapest, 2018.

[115] A. Denley, M. Foulsham és B. Hitchen, GDPR- How to achieve and maintain compliance, New York: Routledge, 2019.

[116] J. Zavodnyik , A Nemzeti Adatvédelmi és Információszabadság Hatóság általános adatvédelmi rendelettel (GDPR) kapcsolatos 2019-es értelmezései, Budapest: Akadémiai Kiadó, mersz.hu, 2020.

[117] European Commission, „Data protection- Better rules for small business," 01 05 2019. [Online]. Available: https://ec.europa.eu/justice/smedataprotect/index_en.htm.

[118] AV Adatvédelem, „adatvedelmiszolgaltato.hu," 30 04 2019. [Online]. Available: https://adatvedelmiszolgaltato.hu/gdpr-attekinto.

[119] P. Bhatia, „EU GDPR Academy," 20 04 2019. [Online]. Available: https://advisera.com/eugdpracademy/knowledgebase/key-roles-defined-in-eu-gdpr/.

[120] EU GDPR.ORG, „GDPR Key Changes," 21 04 2019. [Online]. Available: https://eugdpr.org/the-regulation/.

[121] Jogtár, „2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról," 01 04 2020. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv. [Hozzáférés dátuma: 01 04 2020].

[122] K. dr. Horváth , „A portugál elnökség nyilvánosságra hozta az ePrivacy Rendelet új tervezetét," JogiFórum.hu, 12 01 2021. [Online]. Available:

https://www.jogiforum.hu/blog-adatvedelem-10/2021/01/12/a-portugal-elnokseg-nyilvanossagra-hozta-az-eprivacy-rendelet-uj-tervezetet/. [Hozzáférés dátuma: 14 01 2022].

[123] Adatjog.hu, „GDPR fogalmak," 01 01 2021. [Online]. Available: https://adatjog.hu/gdpr-fogalmak. [Hozzáférés dátuma: 20 03 2021].

[124] ISO, „ISO/TR 17522:2015- Health informatics — Provisions for health applications on mobile/smart devices," ISO.org, 01 08 2015. [Online]. Available: https://www.iso.org/standard/59949.html. [Hozzáférés dátuma: 14 01 2022].

[125] ISO, „ISO/TR 21835:2020(en)- Health informatics — Personal health data generated on a daily basis," ISO.org, 01 06 2020. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:tr:21835:ed-1:v1:en. [Hozzáférés dátuma: 15 01 2022].

[126] European Commission, „mHealth label published," Digital-Strategy.ec.europa.eu, 25 08 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/mhealth-label-published. [Hozzáférés dátuma: 14 02 2022].

[127] NIST, „Vetting the Security of Mobile Applications: NIST Publishes SP 800-163 Revision 1," NIST.gov, 19 04 2019. [Online]. Available: https://www.nist.gov/news-events/news/2019/04/vetting-security-mobile-applications-nist-publishes-sp-800-163-revision-1. [Hozzáférés dátuma: 15 01 2022].

[128] OWASP, „OWASP mobile security," OWASP.org, 01 01 2022. [Online]. Available: https://owasp.org/www-project-mobile-security/. [Hozzáférés dátuma: 14 01 2022].

[129] Z. B. Kovacs , „Az adatvédelmi hatásvizsgálat I (Az adatvédelmi hatásvizsgálat elkészítése)," 19 02 2018. [Online]. Available: https://eugdpr.blog.hu/2018/02/19/az_adatvedelmi_hatasvizsgalat_az_adatvedelmi_hatasvizsgalat_elkeszitese. [Hozzáférés dátuma: 21 03 2021].

[130] P. Howell O'Neill, „Hackers are finding ways to hide inside Apple's walled garden-MIT Technology review," 01 03 2021. [Online]. Available: https://www.technologyreview.com/2021/03/01/1020089/apple-walled-garden-hackers-protected/. [Hozzáférés dátuma: 15 03 2021].

[131] Google, „Google Play Protect," 01 03 2021. [Online]. Available: https://developers.google.com/android/play-protect. [Hozzáférés dátuma: 01 03 2021].

[132] M. Rouse, „Search Networking- VPN (virtual private network)," Search Networking, 01 08 2019. [Online]. Available:

https://searchnetworking.techtarget.com/definition/virtual-private-network. [Hozzáférés dátuma: 30 09 2019].

[133] S. R. Stoyanov, . L. Hides, . D. J. Kavanagh, . O. Zelenko, D. Tjondronegoro és . M. Mani, „Mobile App Rating Scale: A New Tool for Assessing the Quality of Health Mobile Apps," *JMIR mHealth and uHealth,* %1. kötet3, %1. szám1, 11 03 2015.

[134] A. van Haasteren, F. Gille, M. Fadda és E. Vayena, „Development of the mHealth App Trustworthiness checklist.," *Digital Health. 2019 Jan-Dec;5:2055207619886463,* p. 01.

[135] A. van Haasteren, E. Vayena és . J. Powell , „The Mobile Health App Trustworthiness Checklist: Usability Assessment," *JMIR mHealth and uHealth,* %1. kötet8, %1. szám7, 21 7 2020.

[136] T. Wykes és . S. Schueller, „Why Reviewing Apps Is Not Enough: Transparency for Trust (T4T) Principles of Responsible Health App Marketplaces," *Journal of Medical Internet Research,* %1. kötet21, %1. szám5, 02 05 2019.

[137] P. Llorens-Vernet és . J. Miró , „Standards for Mobile Health–Related Apps: Systematic Review and Development of a Guide," *JMIR mHealth and uHealth,* %1. kötet8, %1. szám3, 3 3 2020.

[138] K. R. Szűcs és R. Z. Reicher, „Mobile Health Application Evaluation Possibilities," *SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY ORGANIZATION AND MANAGEMENT SERIES,* pp. 160 pp. 595-611. , 17 p., 2022.

[139] KSH, „22.1.1.3. Népesség korév és nem szerint, január 1.," KSH, 01 06 2023. [Online]. Available: https://www.ksh.hu/stadat_files/nep/hu/nep0003.html. [Hozzáférés dátuma: 01 06 2023].

[140] KSH, „22.1.1.2. A népesség száma és átlagos életkora nem szerint," KSH (Hungarian Central Statistical Office), Budapest, 2022.

[141] KSH, „22.1.2.4. Népesség településtípus szerint, január 1.*," KSH (Hungarian Central Statistical Office), Budapest, 2022.

[142] KSH, „22.1.2.1. A lakónépesség nem, vármegye és régió szerint, január 1.*," KSH, 01 06 2023. [Online]. Available: https://www.ksh.hu/stadat_files/nep/hu/nep0034.html. [Hozzáférés dátuma: 02 06 2023].

[143] . Á. Münnich, Á. Nagy és K. Abari , Többváltozós statisztika pszichológus hallgatók számára, Debrecen: Debrecen: Bölcsész Konzorcium, 2006.

[144] L. Sajtos és A. Mitev, SPSS Kutatási És Adatelemzési Kézikönyv, Budapest: Alinea Kiadó, 2007.

[145] K. R. Szűcs, A. Tick és R. Z. Reicher, „USING THE ATTITUDE THEORY TO DETERMINE SECURITY APPROACHES OF USERS,” *Serbian Journal of Management*, %1. kötet19, pp. 1 pp. 133-148. , 16 p. , 2024.

TÁBLÁZATJEGYZÉK

1. táblázat Korcsoportok megoszlása a mintában és a népességben. Saját szerkesztés 63
2. táblázat Második komponens mátrix, saját szerkesztés SPSS-ből. (Extraction Method: Principal Component Analysis, Rotation Method: Promax with Kaiser Normalization, Rotation converged in 5 iterations) 72
3. táblázat Felhasználói csoportok összefoglalása. Saját szerkesztés 77
4. táblázat Klaszterenkénti és összesített biztonsági intézkedések, valamint kereszttábla elemzés eredményei. Saját szerkesztés 78
5. táblázat Technológiai és IT felkészültség klaszterenként és összesen, valamint kereszttábla elemzés eredményei. Saját szerkesztés 85
6. táblázat Hozzáférés engedélyezés motivációi klaszterenként és összesen, valamint kereszttábla elemzés eredményei. Saját szerkesztés 85
7. táblázat Szempontok alkalmazások választásakor klaszterenként és összesen, valamint kereszttábla elemzés eredményei. Saját szerkesztés 87
8. táblázat Ellenőrző kérdések klaszterenként és összesen. Saját szerkesztés 90
9. táblázat Egészséggel és önkövetéssel kapcsolatos kérdések klaszterenként és összesen, valamint kereszttábla elemzési eredmények. Saját szerkesztés 91
10. táblázat Eredmények összesítése 91
11. táblázat Eredmények összefoglalása 99

ÁBRAJEGYZÉK

1. ábra Kutatási folyamat. Saját szerkesztés 4
2. ábra Kutatási logika- Saját szerkesztés 45
3. ábra Személyes adatok felhasználása vs. egészségügyi adatok felhasználása hisztogramok. Saját szerkesztés..... 66
4. ábra „Ha egy alkalmazás nagyon tetszik, nem érdekel hogy biztonságos-e.” kérdés korcsoport szerint. Saját szerkesztés..... 66
5. ábra Technológiai lépéstartás kor szerinti megoszlása. Saját szerkesztés 67
6. ábra A jövőbeli feltörés kockázatának megítélése a negatív biztonsági incidens tapasztalat hatására. Saját szerkesztés..... 69
7. ábra Biztonsági incidenssel kapcsolatos tapasztalat hatása egyes válaszok átlagára. Saját szerkesztés 69
8. ábra Önkövetési szokások és COVID alkalmazások használatának kapcsolata. Saját szerkesztés .. 70
9. ábra Képernyőkép az SPSS-ből, dendrogram a Ward módszer segítségével, szerző által átméretezett 73
10. ábra Klaszterábrázolás - 3D Scatter. SPSS segítségével saját szerkesztés 74
11. ábra Klasztermátrix. SPSS segítségével saját szerkesztés 75
12. ábra Biztonsági attitűdelemek kapcsolata. Saját szerkesztés 80

MELLÉKLETEK

1. Melléklet: Kérdőív

Szám	Kérdés	Attitűdelem/ Témakör	Szakirodalmi forrás
I.	Értékelje az alábbi állításokat 1-től 10-ig terjedő skálán. 1= Egyáltalán nem értek egyet., 10= Teljes mértékben egyetértek.		
1.	A mobileszközökön szükséges biztonsági intézkedések megtétele teljes mértékben az én kontrollom alatt áll.	Kognitív (kontroll)	[101]
2.	Jól ki tudom használni a technológiát személyes adataim biztonságának védelme érdekében.	Kognitív (megküzdés értékelése)	[104]
3.	Elegendő képességem van ahhoz, hogy megvédjem személyes adataimat a lopástól/ nyilvánosságra hozataltól.	Kognitív (megküzdés értékelése)	[104]
4.	Számomra nagyon fontos, hogy tisztában legyek a személyes adataim felhasználásával.	Érzelmi	[103]
5.	A mobilalkalmazások használata előtt tudatosan beállítom a biztonságra vonatkozó beállításokat (például hogy mihez férhet hozzá egy app).	Kognitív	
6.	Túl sok befektetett energiával jár a mobileszközöm védelmét szolgáló biztonsági intézkedések megtétele.	Kognitív (válaszköltség)	[101]
7.	A biztonság és adatvédelem kérdése túlértékelt.	Érzelmi (norma)	
8.	Bízom a mobilalkalmazásokkal végzett tranzakcióim biztonságában.	Érzelmi	[103]
9.	Aggódom amiatt, hogy a mobilalkalmazások engedély nélkül felhasználhatják a rólam gyűjtött személyes adataimat.	Érzelmi (fenyegetettség értékelése)	[106]
10.	Általánosságban elmondható, hogy kockázatos lenne megadni személyes adataimat egy mobilalkalmazásnak.	Érzelmi (fenyegetettség értékelése)	[103]
11.	Komoly problémát jelentene nekem, ha valaki az engedélyem vagy tudtom nélkül hozzáférne a telefonomon lévő bizalmas információhoz	Érzelmi (fenyegetettség értékelése)	[101]
12.	Az adatvédelmi nyilatkozatok miatt úgy gondolom, hogy személyes adataimat az appok bizalmasan kezelik.	Kognitív	[103]
13.	Számomra nagyon fontos, hogy tisztában legyek az egészségügyi adataim felhasználásával.	Érzelmi	
14.	Fontos számomra, hogy ha a közösség érdeke úgy kívánja, akár lemondjak személyes adataim feletti kontrollomról (például COVID alatt).	Érzelmi	
15.	Ha biztonsági incidenssel találkozom (például feltörik e-mail fiókomat), tudom mit tegyek.	Érzelmi	
II.	Értékelje az alábbi állításokat. A lehetséges válaszok: Egyetértek/ Nem értek egyet.		
16.	Ha egy alkalmazás nagyon tetszik, nem érdekel hogy biztonságos-e.	Visszacsatoló	
17.	Az alkalmazások használatakor mindig automatikusan elfogadom az engedélykéréseket.	Visszacsatoló	

18.	Lépést tartok a legújabb technológiai fejlesztésekkel	Technológiai felkészültség	
19.	Valószínűnek tartom, hogy a jövőben feltörik az okoseszközömet.	Visszacsatoló	[101]
20.	Fontos számomra az egészséges életmód.	Egészség alkalmazások	
21.	Alkalmazásokat használok a jó egészség/fittség megőrzése érdekében.	Egészség alkalmazások	
22.	Úgy gondolom, hogy az egészség és fitnesz alkalmazások segíthetnek a jövőbeni betegségek megelőzésében.	Egészség alkalmazások	
23.	Rendszeresen gyűjtök adatokat a viselkedésemről önkövető eszközökkel (például pulzus, lépésszám vagy útvonal követése okos órával vagy okos telefonnal).	Egészség alkalmazások	[107]
24.	Magatartásomat folyamatosan módosítom az önkövető eszközöktől kapott adatok/visszajelzések alapján.	Egészség alkalmazások	[107]
25.	A COVID miatt lemondtam néhány korábban fontos jogomról.	Egészség alkalmazások	
26.	Használtam COVID témájú applikációkat (például Vírusradar vagy Házi Karantén).	Egészség alkalmazások	
27.	Végzettségem vagy munkám IT területhez kapcsolódik.	IT jártasság	
	Kérem válaszoljon az alábbi kérdésekre. Több választ is megjelölhet.		
28.	Ha egy alkalmazás telepítés után túl sok hozzáférési engedélyt kér, azokat akkor hagyom figyelmen kívül/jóvá, ha:	Viselkedés	[105]
	· megbízom az alkalmazásboltban, ahonnan letöltöm az appot		
	· korábban semmilyen problémát nem észleltem hasonló eset miatt		
	· nem értem miért kéri		
	· azokat túl sokáig tart elolvasni		
	· úgy érzem, hogy ezek jogos kérések		
	· nagyon szeretném az alkalmazás nyújtotta funkciókat használni		
29.	Alkalmazás választásánál számomra fontos, hogy az app:	(Viselkedésként is értelmezhető)	[105], [13]
	· jó értékeléseket kapjon		
	· elől legyen a találati listában, ha az adott témakörre keresek az alkalmazásboltban		
	· milyen csillagos értékelést kapott		
	· sok letöltése legyen		
	· megmagyarázza, hogy milyen tudományos kutatáson alapul		
	· esztétikus legyen		
	· biztonságos legyen		
	· jó hírnevű legyen		
	· motiváljon		
	· örömet okozzon		

	· valaki ajánlja nekem		
	· elérhető legyen magyarul		
30.	Jelölje, hogy az alábbi biztonsági intézkedések közül melyeket alkalmazza általánosságban. Több választ is megjelölhet.	Viselkedés	[101], [106], [14], [15]
	Ismerem a személyes adatkezeléssel kapcsolatos szabályozásokat, jogaimat. (Például GDPR)		
	Elolvasom az adatkezelési tájékoztatókat.		
	Körültekintően átnézem elfogadás előtt a javasolt süti (cookie) beállításokat.		
	Applikációkat kizárólag hivatalos alkalmazásboltból töltök le. (Például Play Áruház vagy App Store)		
	Az alkalmazások engedélykérését rendszeresen felülvizsgálom. (Például ellenőrzi milyen alkalmazások használhatják a helyadatait, fényképeit.)		
	Alkalmazásaimat rendszeresen frissítem.		
	Vírusírtót használok.		
	Követem az internetes csalásokról szóló híreket.		
	Biztonsági mentéseket készítek. (Például dokumentumokról, fotókról)		
	Személyes adatok kiadása előtt meggyőződnék a weboldal vagy alkalmazás hitelességéről.		
	Felismernék egy adathalász e-mailt annak tulajdonságairól.		
	Bonyolult jelszavakat választok.		
	Személyemhez nem köthető jelszót választok.		
	Jelszavaimat rendszeresen frissítem.		
	Biometrikus azonosítást használok. (Például ujjnyomat- vagy arcfelismerés)		
31.	Van biztonsági incidenssel kapcsolatos személyes tapasztalata? (Például feltörték e-mail fiókját, közösségi média fiókját vagy online vásárlás során banki adatait ellopták)	Korábbi tapasztalat	
IV.			
	Kor (számsoron választható 18-65 év)	Demográfiai kategóriák	
	Nem	Demográfiai kategóriák	
	· Férfi		
	· Nő		
	Régió	Demográfiai kategóriák	
	· Dél-Alföld (Bács-Kiskun, Békés, Csongrád megye)		
	· Dél-Dunántúl (Baranya, Somogy, Tolna megye)		
	· Észak-Alföld (Hajdú-Bihar, Jász-Nagykun-Szolnok, Szabolcs-Szatmár-Bereg megye)		
	· Észak-Magyarország (Borsod-Abaúj-Zemplén, Heves, Nógrád megye)		

	· Közép-Dunántúl (Komárom-Esztergom, Fejér, Veszprém megye)		
	· Közép-Magyarország (Budapest és Pest megye)		
	· Nyugat-Dunántúl (Győr-Moson-Sopron, Vas, Zala megye)		
	Település mérete	Demográfiai kategóriák	
	· Budapest		
	· Megyeszékhely		
	· Város		
	· Község		
	Iskolázottság	Demográfiai kategóriák	
	· 8 általános vagy alacsonyabb iskolai végzettség		
	· Szakmunkásképző, szakiskola (érettségi nélkül)		
	· Gimnázium, szakközépiskola (érettségi)		
	· Főiskolai-, egyetemi diploma, posztrgraduális képzés		
	Mennyi az Ön havi nettó személyes jövedelme?	Kiegészítő kérdések	
	· 150.000 Ft vagy kevesebb		
	· 150.001 - 300.000 Ft között		
	· 300.001 - 500.000 Ft között		
	· 500.001 - 1.000.000 Ft között		
	· 1.000.001 Ft-nál több		
	· Nem szeretnék válaszolni		
	Ön milyen gyakran szokott interneten vásárolni?	Kiegészítő kérdések	
	· Soha		
	· Ritkábban		
	· Évente több alkalommal		
	· Többször, negyedévente		
	· Havonta többször		

2. Melléklet: Illeszkedésvizsgálatok

Korcsoport	fi		nPi	Khi2	2022 KSH	Pi
18-26	83	16%	80,730058	0,063825498	941821	15%
27-35	83	16%	96,385151	1,858816171	1124458	18%
36-44	105	20%	107,88589	0,077195766	1258629	21%
45-53	95	18%	118,61328	4,700881796	1383778	23%
54-65	159	30%	121,38562	11,65575591	1416121	23%

Szabadságfok: 4

Kritikus érték: 0,000

	fi		nPi	Khi2	2022 KSH	Pi
Férfi	272	52%	262,695	0,330	3064675	50%
Nő	253	48%	262,305	0,330	3060132	50%
	525			0,660		

Szabadságfok (kategóriák száma-1): 1

Kritikus érték: 0,417

Település mérete	fi		nPi	Khi2	2022 KSH	Pi
1=Budapest	85	16%	92,485896	0,605915572	1706851	18%
2,3 =Város Megyeszékhely	271	52%	275,44314	0,071671794	5083374	52%
4=Község	169	32%	157,07096	0,905972287	2898785	30%

Szabadságfok: 2

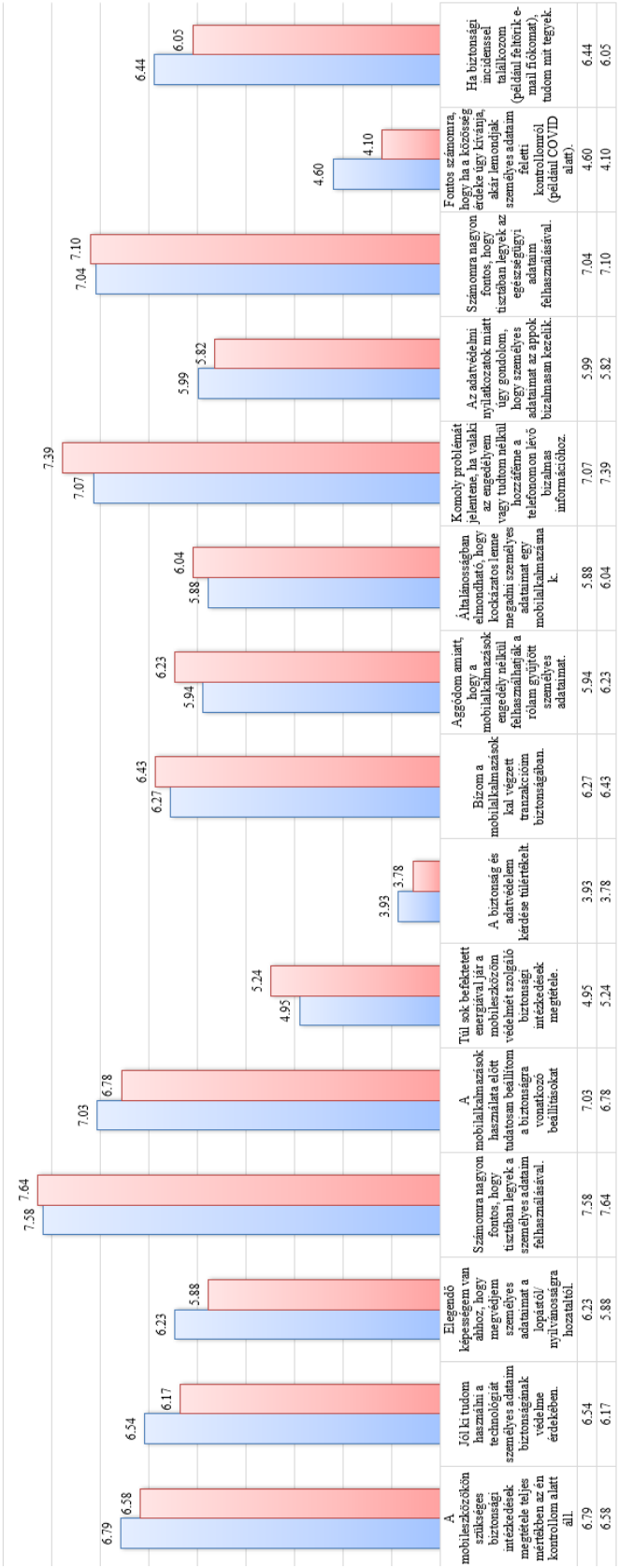
Kritikus érték: 0,208

Régió	fi		nPi	Khi2	2022 KSH	Pi
1=Közép-Magyarország (Budapest és Pest megye)	155	30 %	164,28311	0,524558446	3031887	31 %
2=Közép-Dunántúl (Komárom-Esztergom, Fejér, Veszprém megye)	55	10 %	57,235453	0,087310385	1056295	11 %
3=Nyugat-Dunántúl (Győr-Moson-Sopron, Vas, Zala megye)	49	9%	54,028995	0,468096674	997119	10 %
4=Dél-Dunántúl (Baranya, Somogy, Tolna megye)	44	8%	46,83213	0,171270447	864299	9%
5=Észak-Magyarország (Borsod-Abaúj-Zemplén, Heves, Nógrád megye)	66	13 %	59,715451	0,661395971	1102064	11 %
6=Észak-Alföld (Hajdú-Bihar, Jász-Nagykun-Szolnok, Szabolcs-Szatmár-Bereg megye)	80	15 %	77,146094	0,105576054	1423751	15 %
7=Dél-Alföld (Bács-Kiskun, Békés, Csongrád megye)	76	14 %	65,758769	1,594962977	1213595	13 %

Szabadságfok: 6

Kritikus érték: 0,057

3. Melléklet: Egészség app használat vs. biztonsággal kapcsolatos (kognitív és érzelmi komponenssel kapcsolatos) kérdésekre adott válaszok. Saját szerkesztés

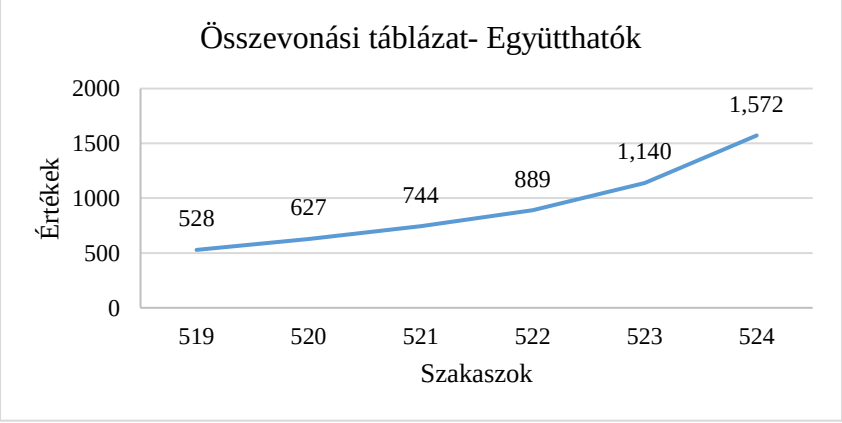


4. Melléklet: Főkomponens elemzés és klaszterelemzés kiegészítő táblázatai

4/1. Első komponens mátrix, saját szerkesztés SPSS-ből (Extraction Method: Principal Component Analysis, Rotation Method: Promax with Kaiser Normalization, Rotation converged in 6 iterations)

	1	2	3
Jól ki tudom használni a technológiát személyes adataim biztonságának védelme érdekében,	0,922		
Elegendő képességem van ahhoz, hogy megvédjem személyes adataimat a lopástól/ nyilvánosságra hozataltól,	0,919		
A mobileszközökön szükséges biztonsági intézkedések megtétele teljes mértékben az én kontrollom alatt áll,	0,845		
Az adatvédelmi nyilatkozatok miatt úgy gondolom, hogy személyes adataimat az appok bizalmasan kezelik,	0,777		
Ha biztonsági incidenssel találkozom (például feltörik e-mail fiókomat), tudom mit tegyek,	0,746		
A mobilalkalmazások használata előtt tudatosan beállítom a biztonságra vonatkozó beállításokat (például hogy mihez férhet hozzá egy app),	0,732		
Bízom a mobilalkalmazásokkal végzett tranzakcióim biztonságában,	0,660		
Számomra nagyon fontos, hogy tisztában legyek a személyes adataim felhasználásával,	0,544	0,474	
Aggódom amiatt, hogy a mobilalkalmazások engedély nélkül felhasználhatják a rólam gyűjtött személyes adataimat,		0,888	
Általánosságban elmondható, hogy kockázatos lenne megadni személyes adataimat egy mobilalkalmazásnak,		0,827	
Számomra nagyon fontos, hogy tisztában legyek az egészségügyi adataim felhasználásával,		0,618	
Komoly problémát jelentene nekem, ha valaki az engedélyem vagy tudtom nélkül hozzáférne a telefonomon lévő bizalmas információhoz,		0,603	
A biztonság és adatvédelem kérdése túlértékelt,			0,836
Fontos számomra, hogy ha a közösség érdeke úgy kívánja, akár lemondjak személyes adataim feletti kontrollomról (például COVID alatt),			0,669
Túl sok befektetett energiával jár a mobileszközöm védelmét szolgáló biztonsági intézkedések megtétele,		0,465	0,668

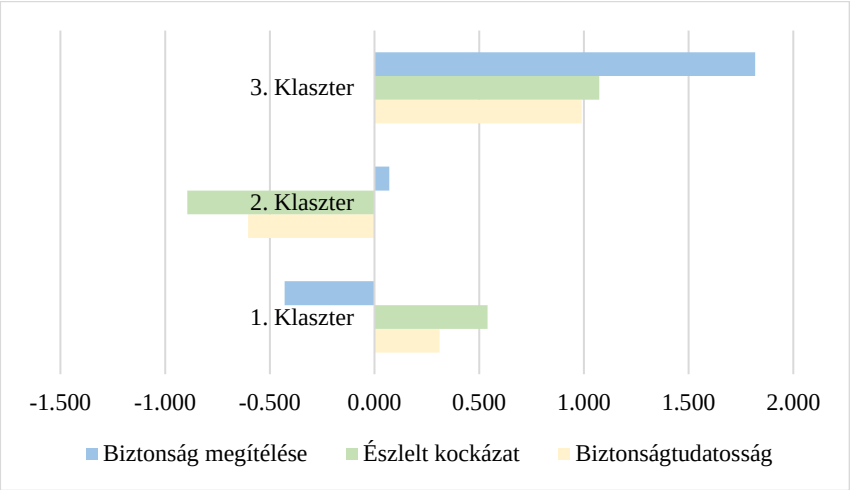
4/2. Kiegészítés: Összevonási táblázat, utolsó 6 együttható ábrázolása. Saját szerkesztés



4/3. Három klaszteres megoldás – A klaszterekre jellemző főkomponensenkénti átlagos és szórás, valamint a klaszterelemek száma. Saját szerkesztés

Klaszterek		Biztonság-tudatosság	Észlelt kockázat	Biztonság megítélése
1	Átlag	0,311	0,540	-0,429
	N	256	256	256
	Szórás	0,859	0,697	0,905
2	Átlag	-0,603	-0,894	0,070
	N	217	217	217
	Szórás	0,888	0,633	0,636
3	Átlag	0,989	1,074	1,819
	N	52	52	52
	Szórás	0,460	0,330	0,390
Összesen	Átlag	0,000	0,000	0,000
	N	525	525	525
	Szórás	1,000	1,000	1,000

4/4. Kiegészítés: Az egyes főkomponenseként és klaszterenként jellemző átlagok. Saját szerkesztés



4/5. Négy klaszteres megoldás – A klaszterekre jellemző főkomponensenkénti átlagos és szórás, valamint a klaszterelemek száma. Saját szerkesztés

Klaszterek		Biztonság-tudatosság	Észlelt kockázat	Biztonság megítélése
1	Átlag	0,065	0,766	-0,236
	N	203	203	203
	Szórás	0,764	0,571	0,887
2	Átlag	-0,603	-0,894	0,070
	N	217	217	217
	Szórás	0,888	0,633	0,636
3	Átlag	0,989	1,074	1,819
	N	52	52	52
	Szórás	0,460	0,330	0,390
4	Átlag	1,250	-0,327	-1,168

	N	53	53	53
	Szórás	0,467	0,392	0,503
Összesen	Átlag	0,000	0,000	0,000
	N	525	525	525
	Szórás	1,000	1,000	1,000

5. Melléklet: Normalitás vizsgálatok

	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Összes biztonsági intézkedés	0,130	525	0,000	0,929	525	0,000
Biztonságtudatosság	0,049	525	0,004	0,981	525	0,000
Észlelt kockázat	0,055	525	0,001	0,985	525	0,000
Biztonság megítélése	0,033	525	0,200*	0,991	525	0,003
*. Ez a valódi szignifikancia alsó határa.						
a. Lilliefors szignifikancia korrekció						

		Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Nem	**Statistic**	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Összes biztonsági intézkedés	**férfi**	0,137	272	0,000	0,940	272	0,000
	nő	0,140	253	0,000	0,915	253	0,000
a. Lilliefors szignifikancia korrekció							

Végzettségem vagy munkám IT területhez kapcsolódik.		**Kolmogorov-Smirnov**[a]			**Shapiro-Wilk**		
		Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Összes biztonsági intézkedés	**Igen**	0,166	105	0,000	0,906	105	0,000
	Nem	0,147	420	0,000	0,928	420	0,000
a. Lilliefors szignifikancia korrekció							

Az alkalmazások használatakor mindig automatikusan elfogadom az engedélykéréseket.		**Kolmogorov-Smirnov**[a]			**Shapiro-Wilk**		
		Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Biztonságtudatosság	**Egyetértek**	0,051	232	0,200*	0,986	232	0,025
	Nem értek egyet	0,062	293	0,008	0,975	293	0,000
*. Ez a valódi szignifikancia alsó határa.							
a. Lilliefors szignifikancia korrekció							

Valószínűnek tartom, hogy a jövőben feltörik az okoseszközömet.	**Kolmogorov-Smirnov**[a]			**Shapiro-Wilk**		
	Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**

Észlelt kockázat	**Egyetértek**	0,089	173	0,002	0,972	173	0,001
	Nem értek egyet	0,045	352	0,086	0,987	352	0,003
a. Lilliefors szignifikancia korrekció							

Ha egy alkalmazás nagyon tetszik, nem érdekel hogy biztonságos-e.		**Kolmogorov-Smirnov**[a]			**Shapiro-Wilk**		
		Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Biztonságtudatosság	**Egyetértek**	0,092	94	0,050	0,965	94	0,013
	Nem értek egyet	0,046	431	0,028	0,983	431	0,000
Észlelt kockázat	**Egyetértek**	0,102	94	0,017	0,965	94	0,012
	Nem értek egyet	0,048	431	0,019	0,986	431	0,000
Biztonság megítélése	**Egyetértek**	0,080	94	0,168	0,975	94	0,064
	Nem értek egyet	0,034	431	0,200*	0,990	431	0,005
*. Ez a valódi szignifikancia alsó határa.							
a. Lilliefors szignifikancia korrekció							

Ha egy alkalmazás nagyon tetszik, nem érdekel hogy biztonságos-e.		**Kolmogorov-Smirnov**[a]			**Shapiro-Wilk**		
		Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Biztonság megítélése	**Egyetértek**	0,080	94	0,168	0,975	94	0,064
	Nem értek egyet	0,034	431	0,200*	0,990	431	0,005
*. Ez a valódi szignifikancia alsó határa.							
a. Lilliefors szignifikancia korrekció							

6. Melléklet: Mann-Whitney próbák

	A mobileszközökön szükséges biztonsági intézkedések megtétele teljes mértékben az én kontrollom alatt áll.	Jól ki tudom használni a technológiát személyes adataim biztonságának védelme érdekében.	Elegendő képességem van ahhoz, hogy megvédjem személyes adataimat a lopástól/ nyilvánosságra hozataltól.	Számomra nagyon fontos, hogy tisztában legyek a személyes adataim felhasználásával.	A mobilalkalmazások használata előtt tudatosan beállítom a biztonságra vonatkozó beállításokat (például hogy mihez férhet hozzá egy app).	Túl sok befektetett energiával jár a mobileszközöm védelmét szolgáló biztonsági intézkedések megtétele.	A biztonság és adatvédelem kérdése túlértékelt.	Bízom a mobilalkalmazásokkal végzett tranzakcióim biztonságában.	Aggódom amiatt, hogy a mobilalkalmazások engedély nélkül felhasználhatják a rólam gyűjtött személyes adataimat.	Általánosságban elmondható, hogy kockázatos lenne megadni személyes adataimat egy mobilalkalmazásnak.	Komoly problémát jelentene nekem, ha valaki az engedélyem vagy tudtom nélkül hozzáférne a telefonomon lévő bizalmas információhoz.	Az adatvédelmi nyilatkozatok miatt úgy gondolom, hogy személyes adataimat az appok bizalmasan kezelik.	Számomra nagyon fontos, hogy tisztában legyek az egészségügyi adataim felhasználásával.	Fontos számomra, hogy ha a közösség érdeke úgy kívánja, akár lemondjak személyes adataim feletti kontrollomról (például COVID alatt).	Ha biztonsági incidenssel találkozom (például feltörik e-mail fiókomat), tudom mit tegyek.
Mann-Whitney U	32002,500	30780,500	31030,500	33549,500	31794,000	31489,500	33089,000	32632,000	31680,500	32547,500	31197,500	32545,500	33321,000	30036,000	30980,000
Wilcoxon W	77453,500	76231,500	76481,500	58749,500	77245,000	56689,500	78540,000	57832,000	56880,500	57747,500	56397,500	77996,500	58521,000	75487,000	76431,000
Z	-1,004	-1,717	-1,570	-0,097	-1,128	-1,301	-0,367	-0,633	-1,189	-0,682	-1,488	-0,683	-0,230	-2,160	-1,601
Asymp. Sig. (2-tailed)	0,315	0,086	0,116	0,923	0,260	0,193	0,713	0,527	0,234	0,495	0,137	0,495	0,818	0,031	0,109

a. Csoportosító változó: Alkalmazásokat használok a jó egészség/fittség megőrzése érdekében.

	Biztonságtudatosság
Mann-Whitney U	29 285,000
Wilcoxon W	56 313,000
Z	-2,725

Asymp. Sig. (2-tailed)	0,006
a. Csoportosító változó: Az alkalmazások használatakor mindig automatikusan elfogadom az engedélykéréseket.	

Mann-Whitney próba- ellenőrző kérdés a biztonságtudatossághoz.

	Észlelt kockázat
Mann-Whitney U	28 274,000
Wilcoxon W	90 402,000
Z	-1,331
Asymp. Sig. (2-tailed)	0,183
a.Csoportosító változó: Valószínűnek tartom, hogy a jövőben feltörik az okoseszközömet.	

Mann-Whitney próba- ellenőrző kérdés az észlelt kockázathoz.

7. Melléklet: Biztonsági incidenssel kapcsolatos negatív tapasztalat hatása a válaszokra

	Elegendő képességem van ahhoz, hogy megvédjem személyes adataimat a lopástól/ nyilvánosságra hozataltól.	Bízom a mobilalkalmazásokkal végzett tranzakcióim biztonságában.	Aggódom amiatt, hogy a mobilalkalmazások engedély nélkül felhasználhatják a rólam gyűjtött személyes adataimat.	Általánosságban elmondható, hogy kockázatos lenne megadni személyes adataimat egy mobilalkalmazásnak.	Ha biztonsági incidenssel találkozom (például feltörik e-mail fiókomat), tudom mit tegyek.
Mann-Whitney U	27 556,000	25 559,500	28 094,500	27 777,500	27 264,000
Wilcoxon W	40 117,000	38 120,500	95 622,500	40 338,500	94 792,000
Z	-0,907	-2,169	-0,567	-0,768	-1,093
Asymp. Sig. (2-tailed)	0,364	0,030	0,571	0,443	0,275

a. Csoportosító változó: Van biztonsági incidenssel kapcsolatos személyes tapasztalata? (Például feltörték e-mail fiókját, közösségi média fiókját vagy online vásárlás során banki adatait ellopták)

8. Melléklet: Egyéb számítások az attitűdelemekre vonatkozóan

8/1. Kendall-tau rangkorrelációs együttható vizsgálata a főkomponensek és az összes biztonsági intézkedés kapcsolatában. Saját szerkesztés

			Biztonsági tudatosság	Érzékelt kockázat	Biztonság megítélése	Összes biztonsági intézkedés
Kendall-tau	Biztonságtudatosság	Correlation Coefficient	1,000	0,205**	0,048	0,221**
		Sig. (2-tailed)	.	0,000	0,099	0,000
		N	525	525	525	525
	Észlelt kockázat	Correlation Coefficient	0,205**	1,000	0,088**	0,062*
		Sig. (2-tailed)	0,000	.	0,003	0,040
		N	525	525	525	525
	Biztonság megítélése	Correlation Coefficient	0,048	0,088**	1,000	-0,252**
		Sig. (2-tailed)	0,099	0,003	.	0,000
		N	525	525	525	525
	Összes biztonsági intézkedés	Correlation Coefficient	0,221**	0,062*	-0,252**	1,000
		Sig. (2-tailed)	0,000	0,040	0,000	.
		N	525	525	525	525
**. A korreláció 0,01-es szinten szignifikáns (2-tailed).						
*. A korreláció 0,05-ös szinten szignifikáns (2-tailed).						

8/2. Többszempontos varianciaanalízis a főkomponensek, a nem, az életkor, az IT jártasság és a nem és az IT jártasság interakciójának vonatkozásában. Saját szerkesztés

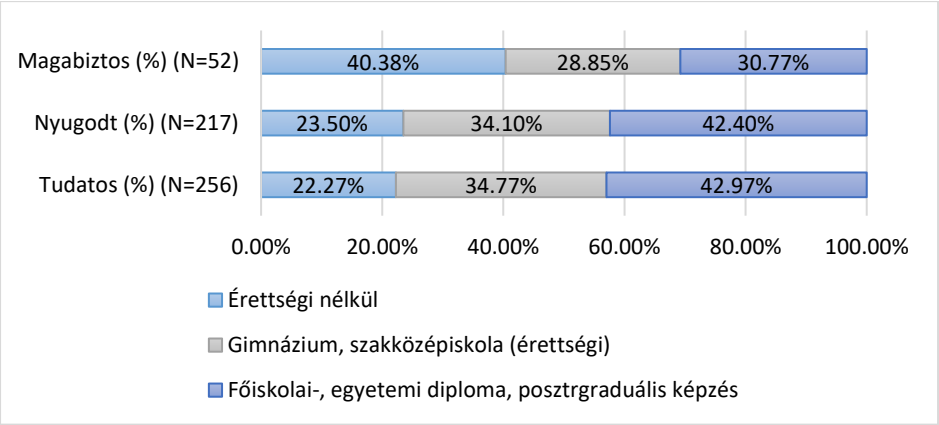
Függő változó: Összes biztonsági intézkedés	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1692,257[a]	7	241,751	24,306	0,000
Intercept	1 500,341	1	1 500,341	150,845	0,000
Nem* IT_jártasság	9,131	1	9,131	0,918	0,338
Nem	39,421	1	39,421	3,963	0,047
IT_jártasság	0,646	1	,646	0,065	0,799
Életkor	5,717	1	5,717	0,575	0,449
FAC1_1: Biztonságtudatosság	697,371	1	697,371	70,114	0,000
FAC2_1: Észlelt kockázat	14,020	1	14,020	1,410	0,236
FAC3_1: Biztonság megítélése	934,809	1	934,809	93,986	0,000
Error	5 142,192	517	9,946		
Total	23 886,000	525			
Corrected Total	6 834,450	524			
a. R Négyzet = 0,248 (Korrigált R Négyzet = 0,237)					

8/3. Levene-teszt és 2 mintás t-próba- ellenőrző kérdés a biztonság megítélésére. Saját szerkesztés

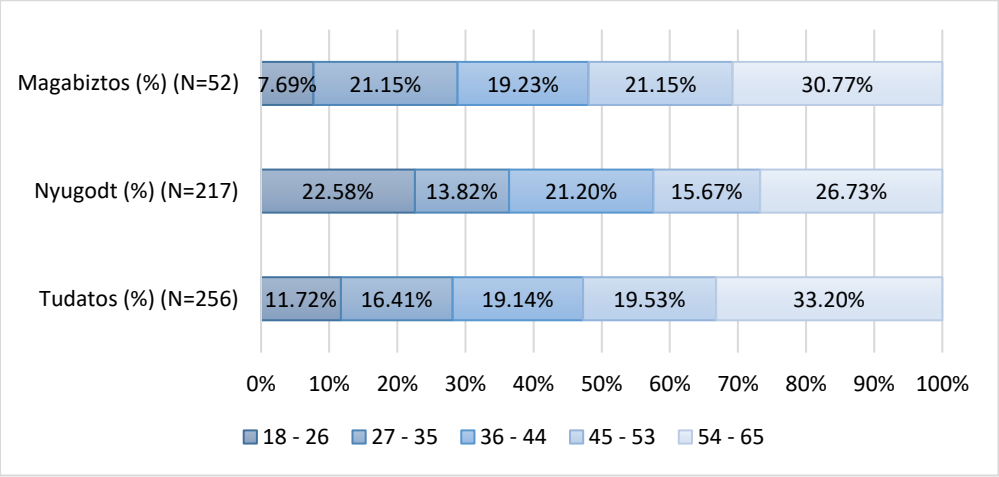
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Differen	Std. Error	95% Confidence Lower	95% Confidence Upper
Biztonság megítélése	Egyenlő szórásokat feltételezve	0,335	0,563	4,971	523	0,000	0.554	0.111	0.338	0.772
	Nem egyenlő szórásokat feltételezve			5,272	145,938	0,000	0.554	0.105	0.346	0.761

9. Melléklet- Klaszterek demográfiai szempontú elemzésének ábrázolásai

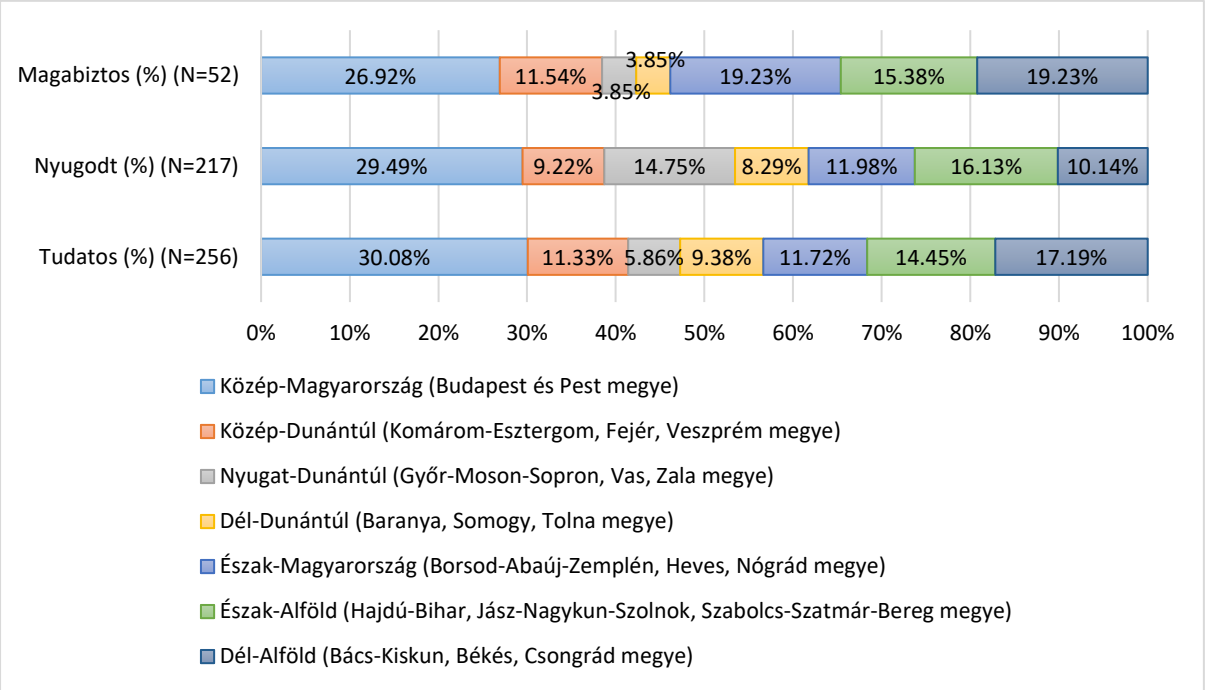
9/1. Klaszterek iskolázottságának megoszlása. Saját szerkesztés.



9/2. Klaszterek korcsoportonkénti megoszlása. Saját szerkesztés



9/3. Klaszterek régiónkénti megoszlása. Saját szerkesztés



9/4. Havi nettó jövedelem klaszterenként. Saját szerkesztés

Havi nettó jövedelem	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)
150.000 Ft vagy kevesebb	38.46%	38.46%	52.17%
150.001 - 300.000 Ft között	42.99%	45.60%	36.96%
300.001 - 500.000 Ft között	14.93%	13.74%	8.70%
500.001 - 1.000.000 Ft között	3.17%	1.65%	2.17%
1.000.001 Ft-nál több	0.45%	0.55%	0.00%
Összesen	100.00%	100.00%	100.00%

9/5. Internetes vásárlási gyakoriság klaszterenként. Saját szerkesztés

Ön milyen gyakran szokott interneten vásárolni?	Tudatos (%) (N=256)	Nyugodt (%) (N=217)	Magabiztos (%) (N=52)
Havonta többször	35.16%	32.26%	26.92%
Többször, negyedévente	21.48%	30.88%	15.38%
Évente több alkalommal	21.48%	16.59%	15.38%
Ritkábban	15.63%	11.06%	25.00%
Soha	2.73%	4.61%	9.62%
Nincs adat	3.52%	4.61%	7.69%
Összesen	100.00%	100.00%	100.00%

KÖSZÖNETNYILVÁNÍTÁS

Elsőként szeretnék köszönetet mondani a témavezetőmnek, Reicher Reginának a folyamatos támogatásáért, biztatásáért és iránymutatásért. Nélküle nem jöhetett volna létre ez az értekezés.

Köszönettel tartozom még a Doktori Iskola és az Óbudai Egyetem számos munkatársának is, többek között Velencei Jolánnak, Tick Andreának, Kolnhofer-Derecskei Anitának, Kovács Tibornak, Maros Dórának, Farkasné Hronyecz Erikának és Lévay Katalinnak a munkájáért is.

Végül köszönöm a családomnak, barátaimnak, csoporttársaimnak és kollégáimnak, hogy végig mellettem álltak és támaszaim voltak.