ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

SZŰCS KATA REBEKA

Mobil alkalmazásokkal kapcsolatos felhasználói biztonság

Témavezető: Dr. habil. Reicher Regina Zsuzsánna

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024.09.03.

Tartalomjegyzék

1 Summary

In an era where mobile phones are integral to daily life, the security of mobile applications has become a critical concern. My research focused on understanding users' security attitudes towards mobile applications, investigating the importance they place on security and the factors that influence their behaviour. The study began with a comprehensive literature review covering mobile application security and user attitudes. This foundation allowed me to formulate hypotheses on user security attitudes. To gather initial insights, I conducted a focus group interview examining how individuals select mobile applications. This was followed by pilot surveys that delved into user security behaviour and attitudes. Building on these findings, I designed a representative survey targeting the Hungarian population to assess user security attitudes comprehensively. I employed statistical methods, including principal component analysis, to identify the core components of security attitudes: **cognitive (security awareness), affective (sense of security), and behavioural intentions**. My analysis revealed that the affective component could be further divided into **perceived risk and security assessment**. Using these four principal components, I conducted a cluster analysis that categorized users into three distinct groups: **aware, calm, and confident**. Subsequent analysis of these groups from various perspectives led to the formulation of six key theses:

1. **Security Perspective Across Application Themes**: There is no significant difference in users' security behaviour between health-themed and other applications.
2. **Impact of Past Security Incidents**: Negative experiences with security breaches reduce trust in applications.
3. **User Grouping by Security Attitudes**: Users can be categorized based on their security attitudes.
4. **Relationships Among Security Attitude Elements**: - Increased security awareness correlates with heightened perceived security risk. - Security awareness influences security behaviour; more security-conscious users adopt more security measures. - The perception of security risks also drives users to take more security precautions.
5. **Influence of Technological and IT Proficiency**: - Users who are more technologically proficient are generally more security-aware. - IT-experienced users have higher security awareness and perceive greater security risks than those without IT experience.
6. **Security as a Primary Selection Criterion**: Security is a crucial factor when choosing applications (although it requires a more complex evaluation process than other aspects).

The findings of this research have broad implications. They provide a foundation for future studies, enhance understanding of user behaviour, and promote the adoption of safer mobile applications. Additionally, these insights can be applied in corporate settings to develop security awareness programs, personalize communication, establish regulations and guidelines, and foster a robust security culture.

2 A kutatás előzményei

Napjainkban az internet és az okostelefonok érzékelhetően életünk szerves részévé váltak. A mobil technológia befolyásolja többek között az életminőségünket, viselkedésünket és döntéseinket. Ez 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. 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.

3 Célkitűzések

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.

Összefoglalva a disszertációban az alábbi kutatási célokat határoztam meg.

1. Meghatározni, hogy van-e különbség felhasználói biztonsági attitűd szempontból az egészség témájú és egyéb alkalmazások között.

A kutatásom a mobil egészség alkalmazásokra fókuszált, azonban a fókuszcsoportos megkérdezés és a pilot kutatás során megállapítottam, hogy valószínűleg nem befolyásolja az alkalmazás témája a biztonsági attitűdöt. Az első célom tehát e feltevés vizsgálata volt.

2. Kérdőíves kutatással vizsgálni a válaszadók biztonsági attitűdjét.

    2.1. A válaszadók biztonságtudatosság és biztonságérzet alapján való csoportosítása.

    2.2. A meghatározott csoportok biztonságra irányuló magatartásának vizsgálata.

    2.3. Létrehozott felhasználói csoportok egyéb jellemzők mentén történő elemzése.

    2.4. Biztonsági attitűd elemei közötti kapcsolat leírása.

A fenti célokhoz a Vizsgálati módszerek pontban bemutatott magyar lakosságra reprezentatív kérdőív segítségével kerestem a válaszokat. Célom a válaszadók attitűd elemek mentén való vizsgálata, majd egyéb szempontok szerinti elemzése is, ezután az attitűdelemek egymással való kapcsolatának vizsgálata is.

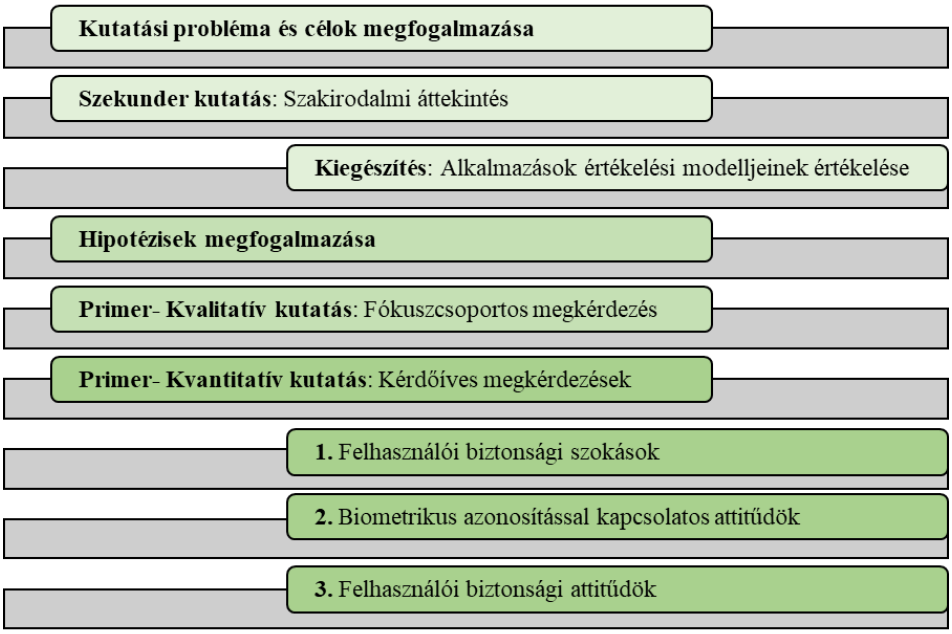
3. Felhasználói alkalmazás választási szempontok meghatározása.

A kutatási cél a bevezetőben említett kérdésre keresi a választ, miszerint egyáltalán fontos-e a biztonság a felhasználóknak, olyan témának tartják-e, amelyre érdemes figyelmet fordítaniuk.

4 Vizsgálati módszerek

A kutatás elsődleges célja tehát a felhasználói biztonsági attitűdök megértése volt. Ennek alapja a szakirodalmi áttekintés során megismert elméleti háttér és az ezek alapján megalkotott modell, mely segítségével később a kutatási kérdések megválaszolását segítő kérdőívet is megalkottam. A későbbiekben részletezett magyar lakosságra reprezentatív kutatást számos kisebb megalapozó kutatás előzte meg, mobil egészség alkalmazások és a biztonság témaköreiben, szakirodalmi rendszerezés, fókuszcsoportos megkérdezés és kérdőíves kutatási módszereket felhasználva. Ezeket kiegészítette egy alkalmazások értékelési modelljeit elemző kutatás, mely során megvizsgáltam, hogy milyen módszerek állnak a felhasználók rendelkezésére az alkalmazások értékelésére, valamint hogy az ott említett információk elérhetők-e számukra. A munka során tapasztaltakat később a reprezentatív kérdőív felépítése során is figyelembe vettem (például egyes szempontok beemelésével.) 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 szabályozások nagy mértékben védik a felhasználókat, önmaguk védelmében saját felelősségük sem elhanyagolható [4]. A kutatás felépítését az 1. ábra foglalja össze.



1. ábra Kutatás felépítése

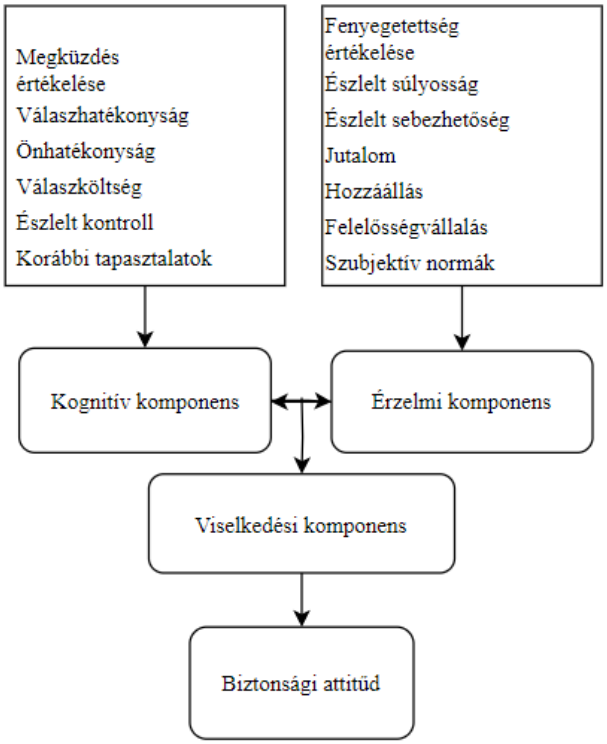
A primer kutatásaim két részre oszthatók: kvalitatív és kvantitatív kutatásokra. A kvalitatív egy fókuszcsoportos megkérdezés volt az alkalmazásválasztási motivációkról. A megkérdezés logikája lemodellezve követte azt, ahogy egy felhasználó számára kiderülnek az egészség témájú alkalmazásról az információk 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 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. A 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 [1].

A kvalitatív szakasz után a kvantitatív kutatási szakasz két megalapozó pilot, 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. Összességében 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 [2]. A megkérdezés eredményeit a későbbi reprezentatív lekérdezésben is felhasználtam a kérdőív kialakításához. 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 kérdőívben nem kapott kitüntetett szerepet a biometrikus azonosítás, mivel biztonsági attitűd szempontból nem tartottam kiemelkedőnek a szerepét.)

A kutatás utolsó szakasza, melyhez végül a tézisek is kapcsolódnak, a felhasználói biztonsági attitűdöket vizsgálta egy nagyobb mintás, magyar lakosságra bizonyos szempontból reprezentatív minta segítségével. A kérdőív kialakításában nagy szerepet játszottak a korábbi kutatások is. Bár a kutatásom témája az egészség témájú mobil applikációkkal kapcsolatos biztonság volt, tanulmányaim során a már említett szekunder kutatással és primer kisebb kutatásokkal teszteltem a feltevéseim egyes részeit a finomítás érdekében 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. 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). 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 kutatási logika a 2. ábrán látható.



2. ábra Kutatási logika

A fentiek felmérése kvantitatív módszerrel, nevezetesen kérdőívvel történik. A 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, a kognitív és érzelmi komponensekhez, 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. A lekérdezés 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 használtam.

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 [2]. 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. Az eredményeket az SPSS szoftverrel (29-es verzió – ingyenes próbaverzió) elemeztem.

5 Új tudományos eredmények

A kutatásom 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. Az volt a feltevésem, hogy 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.

1. tézis: A felhasználók alkalmazás használatában biztonsági szempontból nincs különbség az egészség témájú applikációk és bármilyen más témájú alkalmazás között. [1], [2], [3], [4], [5], [6]

A következőkben azt vizsgáltam, hogy 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). 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. [1], [2], [3], [4], [5], [6]

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.

A következőkben a válaszaszadók biztonságtudatosságuk és biztonságérzetük alapján való csoportosítási lehetőségeit vizsgáltam. 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. [1], [2], [3], [4], [5], [6]

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:

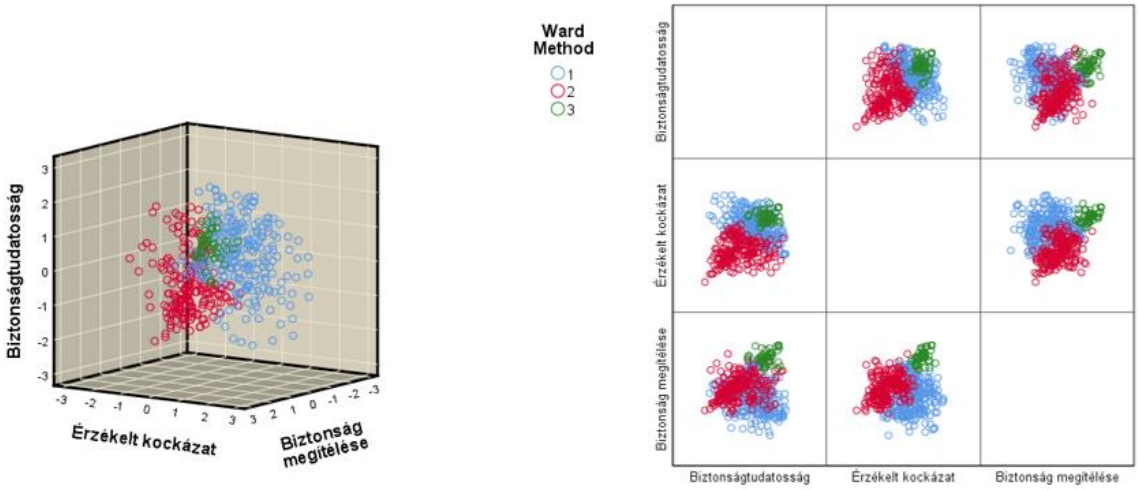
biztonságtudatosság, észlelt kockázat és biztonság megítélése- utóbbi kettőt az érzelmi attitűdkomponensként, biztonságérzetként értelmezve.

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"), melyeket az 1. táblázat foglal össze.

		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**	

1. táblázat Klaszterek

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. A klaszterek attitűdelemek szerinti megoszlása a 3. ábrán is látható 3D scatter és klasztermátrix ábrázolásban is.



3. ábra Klaszterábrázolás - 3D Scatter és Klasztermátrix. SPSS segítségével saját szerkesztés

A felhasználók kognitív és affektív attitűdelemek szerinti csoportosítása lehetővé teszi azok jobb megismerését, valamint a későbbiekben a biztonsággal kapcsolatos viselkedésük elemzését 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.

Összefoglalva a válaszadók biztonsági attitűdjét a 2. 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

2. táblázat Klaszterek jellemzése

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.

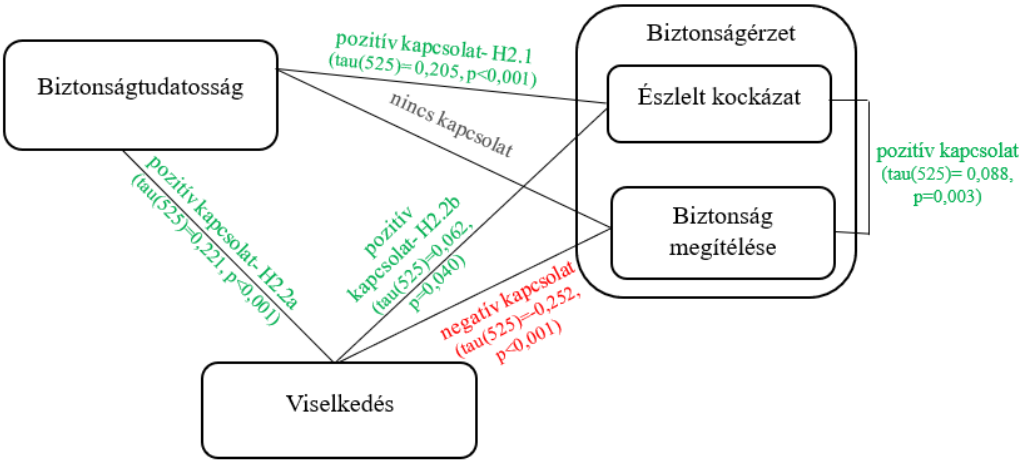
4. tézis: A biztonsági attiűd elemei közötti kapcsolat leírható az alábbiak szerint. [1], [2], [3], [4], [5], [6]

- **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 (4. 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.



4. ábra Biztonsági attitűdelemek kapcsolata

Pozitív gyenge kapcsolat figyelhető meg a biztonsággal kapcsolatos tudatosság és a megtett biztonsági intézkedések számossága között. Tehát a magasabb biztonságtudatosság több intézkedéssel jár együtt. 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. 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.

A klaszterelemzés során létrejött csoportokat demográfiai és egyéb szempontok alapján is elemeztem, vizsgáltam az önbevallott technológiai lépéstartás és IT jártasság biztonsági attitűdre gyakorolt hatását is.

5. tézis: A technológiai jártasság és az IT területen való jártasság befolyásolja a biztonsági attitűdöt az alábbiak szerint. [1], [2], [3], [4], [5], [6]

- **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, 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 az IT területen jártas válaszadók biztonságtudatosabbak. 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.

Az IT területen jártas válaszadók magasabb szintű biztonsági kockázatot észlelnek. 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.

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.

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). [1], [2], [3], [4], [5], [6]

A fenti eredményeket az 3. 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 attitűd 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.**

3. táblázat Kutatási eredmények összefoglalása

6 Az eredmények hasznosítási lehetősége

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.

7 Irodalmi hivatkozások listája/ 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. 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].

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

[15] 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.

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

[17] 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].

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

[19] 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].

[20] 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.

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

[22] 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].

[23] 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].

[24] 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].

[25] 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].

[26] 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].

[27] 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].

[28] 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].

[29] 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].

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

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

[32] 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].

[33] 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].

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

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

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

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

[38] 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].

[39] 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].

[40] 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.

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

[42] 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].

[43] ISC2, „Official ISC2 CC Online Self-Paced Training".

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

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

[46] 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.

[47] 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].

[48] 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].

[49] 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].

[50] 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].

[51] 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].

[52] 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].

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

[54] 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].

[55] 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].

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

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

[58] 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].

[59] 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].

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

[61] 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].

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

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

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

[65] 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].

[66] 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].

[67] 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].

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

[69] L. Muha és C. Krasznay, Az elektronikus információs rendszerek biztonságának menedzselése, Budapest: Nemzeti Közszolgálati Egyetem, 2014.
[70] 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].
[71] 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].
[72] 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].
[73] 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].
[74] 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].
[75] Samsung, „Samsung Pass,” Samsung, 01 01 2021. [Online]. Available: www.samsung.com/uk/apps/samsung-pass/. [Hozzáférés dátuma: 03 05 2021].
[76] A. K. Jain, A. A. Ross és K. Nandakumar, Introduction to biometrics, London: Springer, 2011.
[77] J. Ashbourn, Biometrics in the new world, London: Springer, 2014.
[78] T. Ford, „Business Daily- Boom time for scammers,” BBC, London, 2021.
[79] 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].
[80] 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].
[81] . Á. Hofmeister-Tóth, A FOGYASZTÓI MAGATARTÁS ALAPJAI (THE FUNDAMENTALS OF CONSUMER BEHAVIOR), Budapest: Akadémiai Kiadó, 2014.
[82] G. Rekettye , T. Tóth és E. Malota , Nemzetközi marketing- Online version, Budapest: Akadémiai Kiadó, 2016, p. 116.
[83] 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.
[84] 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.
[85] D. Ashenden, „In their own words: employee attitudes towards information security,” *Information and Computer Security*, %1. kötet26, %1. szám3, pp. 327-337, 2018.
[86] 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.
[87] J. Cox, „Information systems user security: A structured model of the knowing–doing gap,” *Computers in Human Behavior*, pp. 1849-1858, 2012.

[88] 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.

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

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

[101] 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.

[102] 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].

[103] 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].

[104] 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].
[105] Z. Batyi, „kozlekedesvilag.hu," 30 04 2019. [Online]. Available: https://www.kozlekedesvilag.hu/2018/08/24/minden-amit-gdpr-rol-tudni-erdemes/.
[106] Á. Kéri és T. Kancsal, „Adatvédelem a gyakorlatban," HVG, Budapest, 2018.
[107] A. Denley, M. Foulsham és B. Hitchen, GDPR- How to achieve and maintain compliance, New York: Routledge, 2019.
[108] J. Zavodnyik , A Nemzeti Adatvédelmi és Információszabadság Hatóság általános adatvédelmi rendelettel (GDPR) kapcsolatos 2019-es értelmezései, Budapest: Akadémiai Kiadó, mersz.hu, 2020.
[109] European Commission, „Data protection- Better rules for small business," 01 05 2019. [Online]. Available: https://ec.europa.eu/justice/smedataprotect/index_en.htm.
[110] AV Adatvédelem, „adatvedelmiszolgaltato.hu," 30 04 2019. [Online]. Available: https://adatvedelmiszolgaltato.hu/gdpr-attekinto.
[111] P. Bhatia, „EU GDPR Academy," 20 04 2019. [Online]. Available: https://advisera.com/eugdpracademy/knowledgebase/key-roles-defined-in-eu-gdpr/.
[112] EU GDPR.ORG, „GDPR Key Changes," 21 04 2019. [Online]. Available: https://eugdpr.org/the-regulation/.
[113] 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].
[114] 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].
[115] Adatjog.hu, „GDPR fogalmak," 01 01 2021. [Online]. Available: https://adatjog.hu/gdpr-fogalmak. [Hozzáférés dátuma: 20 03 2021].
[116] 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].
[117] 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].
[118] 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].
[119] 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].
[120] OWASP, „OWASP mobile security," OWASP.org, 01 01 2022. [Online]. Available: https://owasp.org/www-project-mobile-security/. [Hozzáférés dátuma: 14 01 2022].

[121] 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].

[122] 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].

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

[124] 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].

[125] 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.

[126] 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.

[127] 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.

[128] 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.

[129] 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.

[130] 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].

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

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

[133] 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].

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

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

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

[1] 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.

[2] 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.

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

[4] K. R. Szűcs és R. Zs. 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.

[5] K. R. Szűcs, A. Tick és R. Zs. Reicher, „APPLYING ATTITUDE THEORY TO DETERMINE USERSECURITY APPROACHES,” SERBIAN JOURNAL OF MANAGEMENT 19 : 1 pp. 133-148. , 16 p. 2024

[6] K. R. Szűcs- Biztonsági kockázatok csökkentése a mindennapokban, In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2., Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 82-94. , 13 p.

8.2 További tudományos közlemények (opcionális)

[7] 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.

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

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

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