

D I P L O M A M U N K A

Harangozó Valentin
2024



**Nemzeti Közsolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok Kar
Kiberbiztonsági Tanszék
Kiberbiztonsági mesterképzési szak**

**Az elektromobilitási eszközök kiberbiztonsági kockázatai,
különös tekintettel az e-rollerekre**

A konzulens:

**Dr. Bányász Péter
egyetemi docens**

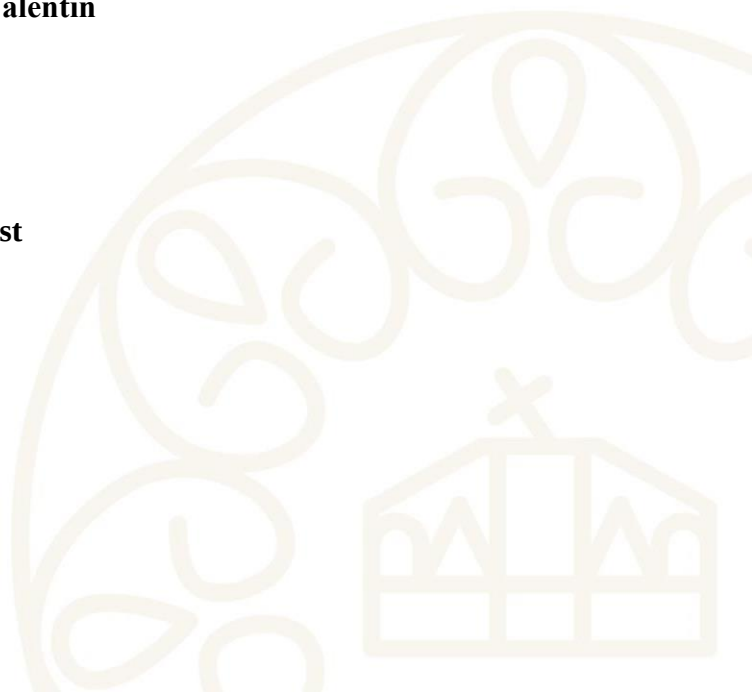
Szakfelelős:

**Dr. Krasznay Csaba
egyetemi docens**

Készítette:

Harangozó Valentin

**Budapest
2024**



TARTALOMJEGYZÉK

BEVEZETÉS	5
A téma helye, jelentősége, aktualitása	5
Tudományos probléma megfogalmazása	5
Kutatási célkitűzések, fontosabb kérdések	6
Kutatási hipotézisek megfogalmazása	7
Kutatás módszerek	8
1 JOGSZABÁLYI HÁTTÉR, JÁRMŰVEKKEL ÉS A KIBERBIZTONSÁGGAL KAPCSOLATOS FONTOSABB FOGALMAK	9
1.1 Járművek fogalma.....	9
1.2 Közlekedés fogalma	10
1.3 Kiberbiztonsági fogalmak.....	13
1.4 Jogszályi háttér	16
1.4.1 Adatvédelmi és adatkezelési jogszályok	16
1.4.2 Termékbiztonsági előírások	17
1.4.3 Kiberbiztonsági előírások.....	17
KÖVETKEZTETÉSEK	19
2 AZ ELEKTROMOBILITÁSI ESZKÖZÖK.....	20
2.1 Az elektromos járművek történeti áttekintése	20
2.2 Elektromobilitási eszközök típusai	22
2.2.1 Elektromos kerékpárok	22
2.2.2 Elektromos egykerekűek	24
2.2.3 Segway típusú járművek	25
2.2.4 Hoverboardok.....	26
2.3 Az elektromos rollerek	27
2.3.1 E-rollerek specifikációi	27
2.3.2 E-rollerek elterjedése.....	28
2.3.3 Közösségi megosztáson alapuló e-rollerek	29
KÖVETKEZTETÉSEK	30
3 KIBERBIZTONSÁGI TÁMADÁSOK, FENYEGETETTSÉGEK	31
3.1 A támadások módszertana	31
3.2 A támadások típusai.....	34
3.3 Kiberbiztonság a járműiparban.....	37
3.4 Kiberfenyegetettségek a járművek tekintetében.....	38

3.5	Kiberfenyegetettségek az elektromos roller tekintetében.....	41
	KÖVETKEZTETÉSEK	44
4	ELEMZŐ, VIZSGÁLÓ MUNKA	45
4.1	Kutatás	45
4.2	A kérdőív	45
4.3	A vizsgálat	47
4.3.1	A vizsgálat módszertana.....	47
4.3.2	Kérdőíves kutatás eredményei	48
	KÖVETKEZTETÉSEK	58
5	BIZTONSÁGI VIZSGÁLAT A VALÓSÁGBAN.....	59
5.1	Teszt végrehajtása.....	61
5.2	További tesztek végrehajtása.....	66
	KÖVETKEZTETÉSEK	68
	ÖSSZEGZETT KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK	69
	IRODALOMJEGYZÉK.....	72
	ÁBRAJEGYZÉK	76
	MELLÉKLETEK JEGYZÉKE	77
	RÖVIDÍTÉSEK JEGYZÉKE	91
	TÁBLÁZATOK JEGYZÉKE.....	92
	FÜGGELÉKEK JEGYZÉKE.....	93
	ANNOTÁCIÓ.....	97

BEVEZETÉS

A téma helye, jelentősége, aktualitása

Manapság egyre több közlekedési eszköz közül lehet választani, ha el szeretnénk jutni az egyik pontból a másik pontba. Az elektromobilitás forradalma felgyorsította a közlekedési eszközök átállását hagyományos üzemanyagokról elektromos energiafelhasználásra. Ennek következtében az elektromobilitási eszközök, mint környezetbarát, könnyű és praktikus eszközök elterjedése is rohamosan nő.

Az elektromobilitási eszközök megjelenése változásokat hozott a közlekedési paradigmában, ezzel együtt pedig komoly kihívások elé állította a kiberbiztonságot. A városi mobilitás átalakulása, melyet az e-rollerek térnyerése hajt, napjainkban kulcsfontosságú a fenntartható városi élet és a személyes közlekedés terén. Ezen eszközök térhódítása azonban a digitális világba való átmenettel együtt jár, és ezáltal kibertérbe helyezett veszélyeket hordoz magával. A kiberbűnözés folyamatosan fejlődik, és az e-rollerek által használt platformok és alkalmazások a potenciális célpontok között szerepelnek, ezáltal felvetve az adatlopás, a személyazonosság-lopás és más káros tevékenységek veszélyét.

Ezen körülmények közepette az e-rollerek kiberbiztonsági kockázatainak elemzése és kezelése kiemelkedő fontosságú. Az aktualitás ezen a területen éppen abban rejlik, hogy az elektromos közlekedés térnyerése egyidejűleg hozza magával a kiberbiztonsági kihívásokat, így különleges figyelmet igényel az adatvédelem és az eszközök online biztonságának megteremtése. Az elektromobilitási eszközök digitalizációja és a hozzájuk kapcsolódó hálózati funkciók által új kiberbiztonsági fenyegetések merülhetnek fel, melyekre eddig kevés figyelem irányult. Pontosan ezen sajátosságok és az ezekből felmerülő kiberbiztonsági problémák kérdésköre az, amely miatt a témát választottam.

Tudományos probléma megfogalmazása

Az elektromobilitás térnyerése jelentős áttörést hozott a közlekedés terén, azonban ez a modernizáció nem csupán előnyöket hozott magával. Az eszközök használatához szükséges digitális infrastruktúra és kapcsolódó alkalmazások adatainak tárolása és feldolgozása kiemelkedő figyelmet igényel a felhasználók személyes és üzleti adatainak védelme érdekében.

Az elektromobilitási eszközök kényelmes és könnyen elérhető eszközök, viszont problémafelvetésem szerint ezeken az eszközökön keresztül átvitt vagy azokon tárolt adatok gyakran érzékeny információkat is tartalmaznak, például GPS-koordinátákat, személyes profilokat és fizetési adatokat. Az ilyen adatok kezelése során felmerülő kockázatok a személyes és a pénzügyi szempontból akár súlyos veszélyt is jelenthetnek.

Az adatbiztonság és az adatvédelem mellett az e-rollerek fizikai biztonságát érintő problémák is kritikus fontosságúak. A hardveres és szoftveres biztonsági rések kihasználása, például a távoli hozzáférés vagy az eszközön található sebezhetőségek, potenciális támadási felületeket teremtenek a kiberbűnözők számára. Mindez hozzájárulhat az eszközök megbízhatatlanságához és azok bizalmatlanságához a felhasználók részéről. Ezért fontos, hogy az eszközök és az azokat kezelő platformok olyan biztonsági megoldásokkal, stratégiákkal rendelkezzenek, amelyek megfelelő védelmet nyújtanak a felhasználói adatoknak, valamint a fizikai és digitális fenyegetésekkel szemben is ellenállók.

Kutatási célkitűzések, fontosabb kérdések

A dolgozat célja, hogy részletesen feltárja a mindennapi közlekedésben megjelenő elektromobilitási eszközök kiberbiztonsági vonatkozásait, azonosítva a lehetséges kockázatokat és veszélyforrásokat. Kiemelt figyelmet kapnak az adatbiztonságot érintő kérdések, például az eszközön tárolt vagy átvitt személyes információk védelme, a távoli hozzáférés lehetőségei és az esetleges adatlopás veszélyei. Fontos kérdések között szerepel továbbá az eszközök fizikai biztonsága, a vezérlőrendszer sebezhetőségei és az esetleges támadási pontok az eszközön vagy a hozzá kapcsolódó szoftverekben.

A fontosabb kérdések körét vizsgálva kettő részre bontható a dolgozat, mivel egyik oldalról szeretném bemutatni a vizsgált elektromos eszközöknek a kiberbiztonsági fenyegetettségét, másik oldalról pedig szeretném megismerni és elemezni ezeket a közlekedési eszközöket felhasználók biztonságtudatossági szintjét. Továbbá a felhasználók szempontjából kiemelkedő fontosságú tényezők feltárását és az esetleges hiányosságok azonosítását az elektromos járművek kiberbiztonságának szempontjából. A dolgozat céljával összhangban annak érdekében, hogy a felhasználók és az elektromos járművek kiberbiztonsága közötti összefüggéseket feltárhassam és megvizsgálhassam, az alábbi kérdéseket fogalmaztam meg.

- Hol vannak az esetleges támadási pontok az eszközön vagy a hozzá kapcsolódó szoftverekben?
- Hogyan alakul a felhasználók tudatossága az elektromos járművek kiberbiztonsági fenyegetettségével kapcsolatban? Mennyire ismerik az adatvédelmi kockázatokat?
- Milyen mértékben alkalmazzák a felhasználók a biztonságos használat alapelveit az elektromos járművek esetében, mennyire figyelnek a frissítésekre és az alapvető biztonsági intézkedésekre?
- Milyen hatása van a kiberbiztonsági fenyegetettségeknek a felhasználói élményre és bizalomra az elektromos járművekkel kapcsolatban? Hogyan befolyásolja ez a döntést az ilyen eszközök használatáról vagy vásárlásáról?

Kutatási hipotézisek megfogalmazása

A kutatási téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

H1. Az elektromobilitási eszközök számos sebezhetőségi ponttal rendelkeznek.

H2. Az emberek részéről tapasztalható aggodalom az elektromobilitási eszközök kiberbiztonsági kockázatai miatt.

H3. Az elektromobilitási eszközökkel rendelkezők optimistábbak és pozitívabbak az elektromos mobilitási technológiákat illetően, mint azok, akik nem rendelkeznek ilyen eszközökkel.

H4. Az elektromobilitási eszközökkel kapcsolatos kiberbiztonsági tudatosságot befolyásolja a nem és az iskolai végzettség.

H5. A kiberbiztonság jelentőséggel bír a jármű gyártás, fejlesztés és szabályozás területén.

Kutatás módszerek

A kutatásom során többféle módszert alkalmaztam az elektromobilitási eszközök kiberbiztonsági kockázatainak feltárására és értékelésére.

Készítettem egy online kérdőíves kutatást, amelynek célja az volt, hogy megértsem az emberek attitűdjeit és aggodalmait az elektromobilitási eszközök kiberbiztonsági kérdéseivel kapcsolatban. A kérdőívben olyan témákra fókuszáltam, mint az eszközökkel kapcsolatos tapasztalatok, az aggodalmak szintje, és a technológia elfogadásával kapcsolatos hajlandóság.

Összegyűjtöttem, majd részletesen áttekintettem a hazai és nemzetközi szakirodalmakat az elektromobilitási eszközökkel és azok kiberbiztonsági kockázataival kapcsolatban.

Elvégeztem egy biztonsági tesztelést egy elektromos rolleren, hogy közvetlen tapasztalatokat szerezhsek az eszköz kiberbiztonsági sebezhetőségeiről. Ez a tesztelés tartalmazott olyan elemeket, mint a rendszeres frissítések telepítése, az eszközön található alkalmazások biztonságának értékelése és a potenciális kockázati tényezők azonosítása.

Az összes adatgyűjtést követően az összegyűjtött információkat analizáltam és összehasonlítottam, hogy átfogó képet kapjak az elektromobilitási eszközök kiberbiztonsági helyzetéről. A fentiek eredményeként alakítottam ki a kutatás végkövetkeztetéseit és ajánlásait.

1 JOGSZABÁLYI HÁTTÉR, JÁRMŰVEKKEL ÉS A KIBERBIZTONSÁGGAL KAPCSOLATOS FONTOSABB FOGALMAK

A szabályozások a járműgyártók, szolgáltatók és felhasználók számára meghatározzák az adatvédelmi, biztonsági és jogi követelményeket. Ide tartozik például az autonóm járművek tesztelésére és üzembe helyezésére vonatkozó jogszabályok, valamint a járművekbe épített szoftverek és hálózati kapcsolatok biztonsági követelményei. A járművekkel kapcsolatos kiberbiztonsági szabályozások célja a járművek elleni támadások megelőzése és kezelése, hogy minimalizálják az ilyen eseményekből eredő kockázatokat és veszteségeket. Az ilyen jogszabályok és fogalmak általánosan arra törekszenek, hogy a járműveket és azok digitális infrastruktúráját védelmező és megbízható keretrendszer biztosítsanak.

1.1 Járművek fogalma

Az élet minden területén hozzá kellett szoknunk a történelmi fejlődés során, hogy meghatározott keretek között tevékenykedhetünk. Ezen keretek és normák által irányítva élhetjük mindennapjainkat, és ezek szabályozzák cselekedeteinket. A jogrendszer rendkívül fontos szerepet tölt be ebben a folyamatban, hiszen minden tevékenységnek, minden területnek megvannak a maga sajátos szabályai és előírásai.

A jogalkotás részletesen szabályozza az emberek életét. Meghatározza, hogy mik a jogalanyok kötelezettségeik, jogaik és felelősségeik az adott területen. Ennek megfelelően a közúti közlekedés sem kivétel. A közlekedés szintén saját jogszabályrendszerrel rendelkezik, amely részletesen meghatározza, hogyan kell viselkednünk az utakon, milyen szabályok vonatkoznak a közlekedésre. Ezek a szabályok biztosítják a rendet és biztonságot az utakon. Ilyen jogszabály az is, amely a járműveket fogalmilag meghatározza és elkülöníti az egyes jármű kategóriákat, típusokat egymástól. Ezért a járművek fogalmának tisztázásához elengedhetetlen az 1/1975 (II.5.) KPM-BM együttes rendelet a közúti közlekedés szabályairól című jogszabály vizsgálata, mely szerint:

„Jármű: közúti szállító- vagy vontató eszköz, ideértve az önjáró vagy vontatott munkagépet is. A mozgáskorlátozottak közlekedésére szolgáló, emberi erővel tolt vagy hajtott kerekes szék és a gépi meghajtású kerekes szék - ha sík úton önerejéből 10 km/óra sebességnél gyorsabban

haladni nem képes, továbbá a gyermekkocsi és a talicska - azonban nem minősül járműnek. Az ilyen eszközökkel közlekedő személyek gyalogosoknak minősülnek.”¹

Az előbbieken meghatározott fogalom további szintekre bontható a KRESZ alapján, mivel az a járműveket három nagy kategóriába sorolja.

Melyek a következők:

- Gépjárművek: Amelyeket beépített motor (erőgép) hajt.
- Motoros nem gépjárművek: Amelyeknek beépített motorjuk van, azonban a jogszabály alapján nem minősülnek gépjárműnek.
- Nem motoros járművek: Amelyeknek nincsen saját motorja.

Fontos megjegyezni, hogy az elektromos közlekedési eszközök nagy része jelenleg nem rendelkezik teljes körű jogi szabályozással. Az elektromos rollerektől az elektromos kerékpárokon át egészen a kisebb elektromos járművekig sokféle formája van az elektromobilitásnak, melyeket jelenleg a segédmotoros kerékpárok csoportosításába sorolnak. Ez a besorolás azonban egyáltalán nem fedi le teljes mértékben az elektromobilitás sokféleségét és specifikus jellemzőit, és pontosan ezért a jogi szabályozottság pontosítása kiemelkedő jelentőséggel bír napjainkban.

1.2 Közlekedés fogalma

A legtöbb ember számára a közlekedés jelentése gyakran a célpontról célpontra történő eljutást jelenti valamilyen formájában. Azonban a közlekedés ennél sokkal bonyolultabb fogalmat takar, és annak meghatározásához közlekedéstudomány szempontjait kell figyelembe venni. A közlekedés, mint fogalom sokkal árnyaltabb, és számos összetevőt foglal magában.

„A közlekedés személyeknek és dolgoknak (árúknak, termékeknek) olyan helyválttatása, amely sajátos technikai eszközök igénybevételével, részint a közlekedésben dolgozók termelő munkája révén szabályszerűen és tervszerűen ismétlődve, részint nem termelő egyéni tevékenységként valósul meg.”²

¹ „1/1975. (II. 5.) KPM–BM együttes rendelet a közúti közlekedés szabályairól”

² Dr. Irk Ferenc és mtsai., *Közlekedésrendészeti Alapismeretek*, Egyetemi jegyzet (Budapest, 2013).

A fogalom alapján megállapítható, hogy a közlekedés nem csupán mozgást jelent, hanem egy összetett folyamatot, amely folyamatosan változik és fejlődik. Az emberek és dolgok mozgása az emberiség létezésével egyidős. Azonban az emberiség fejlődésével együtt az igények és szokások is átalakultak, ez pedig kihatással volt a közlekedési szükségletekre, ez a jelenség a mai közlekedésünkre is egyaránt igaz.

Az emberek társadalmi elvárásai folyamatosan változnak és a technológia gyors ütemben fejlődik. Azonban a közlekedési szabályok sokszor lemaradnak ezektől a gyors változásoktól. Az új társadalmi szokások és technológiai újítások bevezetése gyakran nehézségeket okoz a meglévő jogszabályoknak, különösen az olyan új közlekedési eszközök, mint az e-rollerek.

Az e-roller a modern mobilitás egyik jelentős formája, de a közlekedésben történő használatuk szabályozása még nem kapott megfelelő törvényi keretet. Ugyanez a helyzet a kiberbiztonság terén is, ahol az új eszközök, alkalmazások és digitális platformok rendkívül gyorsan fejlődnek. Emiatt a jogi szabályozásoknak időről időre nehézséget okozhatnak azzal, hogy megfelelő védelmet és irányelveket biztosítsanak az online biztonság területén.

Mindkét esetben a gyors technológiai változások miatt a jogi szabályozásnak nehéz lehet lépést tartani a fejlődéssel. Az elektromobilitás és a kiberbiztonság területén is kulcsfontosságú a szabályozás és a jogi keretek állandó frissítése és adaptálása ahhoz, hogy megfelelő védelmet és irányelveket biztosítson a változó környezetben.



1. ábra: A kiberbiztonság és a közlekedési innovációk összefüggései
(Saját szerkesztés, forrás: Innovációk a közlekedésben³)

Úgy gondolom, hogy a fenti folyamatára szemléletesen mutatja be a kiberbiztonság és a közlekedési innovációk összefüggéseit, amelyről a közlekedés fogalmának kifejtése során említést tettem.

Az új igények és elvárások megjelenése mind a közlekedési, mind a kiberbiztonsági szektorban kulcsfontosságú. A közlekedés terén az új eszközök, járművek iránti igények gyakran olyan technológiai innovációkhoz vezetnek, amelyek a közlekedési infrastruktúrát és a közlekedési eszközök piacát változtatják meg. Ugyanakkor a kiberbiztonság terén az új igények általában olyan biztonsági megoldások kereséséhez vezetnek, amelyek képesek megvédeni az új technológiákat és adatainkat az esetleges fenyegetésektől. Ez a folyamat, például az e-rollerek esetében, egyértelműen bemutatja, hogy az új közlekedési eszközök megjelenésével együtt a felhasználók igénylik az azokat a közlekedési eszközöket kiszolgáló alkalmazásokat is. Ugyanakkor ezzel párhuzamosan felmerül a szükség a kiberbiztonsági oldalon arra, hogy ezeket az alkalmazásokat is védjék, hiszen az adatbiztonság és a felhasználók védelme kiemelt fontosságú.

³ Fleischer Tamás, „Innovációk a közlekedésben: külföldi példák, hazai tanulságok”, 2008.

Ezt követi a technológiai fejlődés, amely a közlekedési eszközök és a kiberbiztonsági rendszerek terén egyaránt gyorsan történik. Az innováció és a fejlesztés olyan új megoldásokat hoznak létre, amelyek megváltoztatják az adott terület működését és hatékonyságát. Ebből következik a következő folyamat az eredménytermékek megjelenése. Új technológiák jelennek meg, új közlekedési eszközök kerülnek piacra, és előállnak új kiberbiztonsági megoldások is, ezáltal megváltoztatva mindkét területet.

A változó igényekre és az eredménytermékek megjelenésére adott válaszként a jogi szabályozásnak alkalmazkodnia kell, különben problémák merülhetnek fel mind technológiai, mind a közlekedésbiztonsági oldalon. A jogi kereteknek meg kell felelniük az új technológiák által felvetett kihívásoknak és a változó közlekedési igényeknek. A jogi szabályozást követően a felhasználók általi elfogadás és használat folyamata következik. Az új fejlesztések sikerét végső soron az emberek reakciói és elfogadása határozzák meg. Ez egyben visszacsatolás is a folyamatban, mivel a felhasználók visszajelzései további fejlesztésekre és finomításokra ösztönözhetik a rendszereket és az eszközöket.

Az egész folyamat ciklikus jellegű, hiszen az új igények megjelenése, a technológia fejlődése, a szabályozás és a felhasználói elfogadás mind visszahatnak az egész folyamatra. Ezt követően új fejlődési ciklusok indulnak el új igényekkel, amelyek további innovációra, fejlődésre és válaszok keresésére serkentik mind a közlekedési, mind a kiberbiztonsági területet.

1.3 Kiberbiztonsági fogalmak

A dolgozat fókuszában az elektromobilitási eszközök kiberbiztonsági kockázatainak mélyebb megértése áll. Ezért azt gondolom, hogy a közlekedés és járművek fogalmának ismertetése után ebben a kontextusban fontos az alapvető kiberbiztonsági fogalmak bemutatása is. A kiberbiztonsághoz kapcsolódó fogalmak közül azok kerülnek bemutatásra, amelyek az elektromobilitási eszközök kiberbiztonsági kockázatainak a dolgozat későbbi részben történő kifejtésének szempontjából fontosak lehetnek.

A dolgozat szempontjából talán a legfontosabb fogalom maga a kiberbiztonság, amelynek a definícióját az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény írja le.

„Kiberbiztonság 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.”⁴

Az elektromobilitás területén a kiberbiztonsági intézkedések célja az, hogy a járműveket kiszolgáló rendszerek és az azokhoz kapcsolódó adatok védelme mellett a zavartalan működést biztosítsák, miközben a felhasználók bizalma is megmarad. A kiberbiztonság tehát elengedhetetlen a fenntartható és biztonságos elektromobilitás kialakításához és fejlődéséhez.

Az előzőhöz hasonlóan szintén ilyen fontos fogalom az elektromobilitás szempontjából, maga az elektronikus információs rendszer,

„Elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese”⁵.

„Az elektronikus információs rendszerekhez tartoznak:

- *a számítástechnikai rendszerek és hálózatok;*
- *a helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;*
- *a rádiós vagy műholdas navigáció;*
- *az automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek stb.);*
- *a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.”⁶*

Az utóbbi kibővített felsorolás részletesen meghatározza azokat a rendszereket, amelyek az elektronikus információk kezelésére, tárolására és átvitelére szolgálnak, és különféle területeken használhatók. Jelentősége az elektromobilitás szempontjából kiemelkedő, hiszen

⁴ „2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, elérés 2024. április 8.

⁵ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, elérés 2024. április 8.

⁶ Muha Lajos és Krasznay Csaba, „Az elektronikus információs rendszerek biztonságáról vezetőknek”, NKE, Budapest, 2018.

ezek a közlekedési eszközök számítástechnikai rendszerek és hálózatok igénybevételével kommunikálnak más eszközökkel, és a működésük alapját ezek a rendszerek biztosítják.

„Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.”⁷

A bizalmasság jelentősége szintén kiemelkedő fontosságú, hiszen az elektromobilitás egyre inkább digitalizált és kapcsolódik az internethez, amelynek következtében az elektromos járművek és azok infrastruktúrája is adatokat generál, tárol, és ezeket továbbítja. Az elektromos járművekben és azokat kiszolgáló rendszerekben tárolt adatok - legyenek azok járművek műszaki adatai, navigációs információk, felhasználói preferenciák vagy akár személyes adatok - ezáltal különféle kiberbiztonsági fenyegetettségeknek vannak kitéve.

Fontos megemlíteni, hogy az adatvédelem a személyes adatok védelmére vonatkozik, ezzel szemben az elektronikus információs rendszerek biztonsága elsősorban az adatok és azokat kezelő rendszerek védelmét szolgálja. Ez kiterjedhet az elektronikus adatokra, az adatbázisokra, a szoftverekre és hardverekre, valamint azokra a hálózatokra és infrastruktúrákra, amelyekben ezek az adatok tárolódnak.

Szinén fontos fogalmak a hálózat biztonság és a vulnerabilitás. A hálózat biztonság az elektromobilitás szempontjából az elektromos járművek és azok infrastruktúrája által használt hálózatok védelme a külső támadások, például kiberbűnözők vagy rosszindulatú szoftverek ellen. Az elektromos járművek és azok infrastruktúrájának hálózatbiztonsága alapvető fontosságú az adatok integritásának és a rendszerek zavartalan működésének biztosítása érdekében. A vulnerabilitás pedig az elektromos járművek és azok rendszereinek sebezhetőségei, melyek lehetőséget adnak a támadásokra és a káros tevékenységekre. Ezek a sebezhetőségek lehetnek hardveres vagy szoftveres gyengeségek, esetleg rosszul beállított biztonsági protokollok, amelyek kihasználása veszélyt jelenthet az elektromos járművek biztonságára és adatvédelmére. A sebezhetőségek felfedezése és kezelése kritikus fontosságú, mivel ezeknek a hibáknak a kihasználásával a támadók illegális hozzáférést szerezhetnek, adatokat lophatnak vagy manipulálhatnak, vagy akár a járművek működését is zavarhatják. Ennek érdekében használják megoldásként például a következő fogalmat, amely a titkosítás. A

⁷ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról - Hatályos Jogszabályok Gyűjteménye.

titkosítás „*alapvető feladata matematikai módszereket alkalmazó algoritmusokkal és azok használatának pontos leírását tartalmazó – szigorúan betartandó – kriptográfiai protokollok segítségével biztosítani az üzenetek, illetve tárolt információk bizalmasságát, védettségét, hitelességét.*”⁸ Tehát a titkosítás lényege, az adatok vagy kommunikációk átalakítása oly módon, hogy azok csak a jogosult felek számára legyenek értelmezhetőek, ezzel megakadályozva az illetéktelen hozzáférést.

A kiberbiztonság, bizalmasság, adatvédelem, hálózatbiztonság, vulnerabilitás, titkosítás, alapvető fogalmak, amelyek hozzájárulnak az elektromobilitási eszközök és azok infrastruktúrájának védelméhez. Természetesen még sok olyan fogalom létezik, amelyek fontosak, azonban az elektromobilitási eszközök kiberbiztonsági fenyegetettségének szempontjából elegendő a fentieket megérteni és alkalmazni, illetve lehetővé teszi a dolgozatban a kiberbiztonsági kockázatok pontosabb azonosítását.

1.4 Jogsabályi háttér

Az elektromobilitási eszközök, mint az e-rollerek gyártóira és szolgáltatóira számos jogsabály vonatkozik információbiztonsági szempontból. Ezek a szabályozások az eszközök tervezésétől kezdve a felhasználók védelméig terjednek. Ezeknek a szabályoknak a célja, hogy az elektromos mobilitási eszközök adatvédelmi és kiberbiztonsági szempontból is megbízhatóak és biztonságosak legyenek a felhasználók számára. Ezáltal a jogi keretek megalkotása, nemcsak a gyártókra és szolgáltatókra, hanem közvetlenül a felhasználókra is hatást gyakorolnak.

A szabályozás kapcsán három különböző kategóriát is megkülönböztethetünk, amelyek az elektromobilitási eszközök jogsabályi háttérét alkotják.

1.4.1 Adatvédelmi és adatkezelési jogsabályok

Az e-rollerek gyártóinak és szolgáltatóinak be kell tartaniuk az adatvédelmi törvényeket, mint például Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről, tehát az általános adatvédelmi rendeletet, angolul röviden GDPR-t. Továbbá szintén be kell tartaniuk az adott országok saját adatvédelmi előírásait. Ezek a jogsabályok meghatározzák, hogyan

⁸ Muha Lajos és Krasznay Csaba, „Az elektronikus információs rendszerek biztonságáról vezetőknek”.

gyűjthetők, tárolhatók és kezelhetők a felhasználók személyes adatai, és biztosítják, hogy azok megfelelően védettek legyenek.

1.4.2 Termékbiztonsági előírások

Fontos, hogy az elektromos járművek gyártására és forgalmazására vonatkozó szabványok és biztonsági előírások szigorúak legyenek, hiszen ezek az előírások biztosítják, hogy az eszközök megfeleljenek a műszaki és biztonsági szabványoknak, minimalizálva ezzel a felhasználókra nézve jelentkező kockázatokat. Termékbiztonság terén az elektromos járművekre, beleértve az e-rollereket is, vonatkozó uniós szabályozás az EU 168/2013 számú rendelete a két- vagy háromkerekű járművek, valamint a négykerekű motorkerékpárok jóváhagyásáról és piacfelügyeletéről. Ez a rendelet meghatározza az egységes jóváhagyási előírásokat és szabványokat az új típusú járművek esetében, amelyek közé tartoznak az elektromos járművek is.

1.4.3 Kiberbiztonsági előírások

Egyre inkább előtérbe kerülnek olyan szabályozások, amelyek konkrétan a kiberbiztonsági védelemre helyezik a hangsúlyt. Ezek a szabályok foglalkoznak az eszközök hálózati kapcsolataival, a szoftverfrissítésekkel, a biztonsági rések gyors javításával és egyéb olyan intézkedésekkel, amelyek megakadályozhatják a kiberbűnözők támadásait. Az elektromos járművek kiberbiztonsági védelmére vonatkozó előírások között példaként említhető az ISO/SAE 21434 szabvány. Ez a szabvány az autóiparban a kiberbiztonság terén létrehozott nemzetközi iránymutatás, amely konkrétan az autók kiberbiztonsági kockázataira és az ezek elleni védelemre fókuszál. A szabvány célja, hogy keretet hozzon létre a közúti járműrendszerek kiberbiztonságához. *„A szabvány a kockázatértékeléstől, -kezeléstől a biztonsági ellenőrzésekig és a kockázatcsökkentési stratégiákig mindenre kiterjed.”*⁹

A fenti ISO szabvány mellett fontos megemlíteni Az Európai Parlament és a Tanács (EU) 2016/1148 irányelvet más néven hálózat- és információbiztonsági (angolul röviden NIS) irányelv, amely az uniós kibervédelmi szabályozás egyik fontos eleme. Ez az irányelv a hálózat- és információbiztonsági követelményeket határozza meg az Unióban.

⁹ Jain Anushtha, „ISO 21434: Meghatározás, megfelelőség, eszközök és tanúsítványok”, Visure Solutions (blog), elérés 2024. április 8., <https://visuresolutions.com/hu/blog/aut%C3%B3ipari/iso-21434/>.

A fenti irányelv a járművek kiberbiztonsági kérdéseivel foglalkozik annak általános biztonsági hatókörében, hogy megelőzze és minimalizálja az események és támadások hatását. Illetve a másik irányelv a 2022/2555 Network and Information Systems Directive 2 (angolul röviden NIS2) , amely a korábbi (EU) 2016/1148 NIS irányelv továbbfejlesztett változata. Mindkét irányelv felszólítja az alapvető szolgáltatásokat nyújtó szereplőket és a digitális szolgáltatókat, hogy tegyék meg a megfelelő és arányos technikai és szervezeti intézkedéseket az információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében.

Szintén a közúti szállítási ágazatra vonatkozóan az Európai Unió Kiberbiztonsági Ügynökség (továbbiakban ENISA) is dolgozott ki iránymutatásokat a kiberbiztonsági irányelvek végrehajtására vonatkozóan. Ilyen például az ENISA - Good Practices For Security Of Smart Cars, tehát az intelligens autók biztonságával kapcsolatos bevált gyakorlatok elnevezésű iránymutatása, amelyben az intelligens autók érintő kiberbiztonsági kihívásokat tárgyalta.¹⁰

Továbbá szintén meg kell említeni az ENISA ajánlásainak figyelembevételével az Európai Gépjárműgyártók Szövetségét (ACEA) is, akik meghatározták a csatlakoztatott és az automatizált járművek elleni kiberfenyegetettségekkel szembeni védelem alapelveit, amelyek a következők:

- A kiberbiztonsági kultúra ápolása
- Kiberbiztonsági életciklus elfogadása a járműfejlesztéshez
- A biztonsági funkciók értékelése tesztelési fázisokon keresztül: önellenőrzés és tesztelés
- Biztonsági frissítési házirend kezelése
- Az incidensre adott válasz és helyreállítás biztosítása
- Az iparág szereplői közötti információmegosztás javítása¹¹

Az alapelvek meghatározása mellett, hangsúlyozta a kiberbiztonsági követelmények végrehajtását a járműfejlesztési életciklus minden szakaszában.

¹⁰ „ENISA good practices for security of Smart Cars — ENISA”, elérés 2024. április 8., <https://www.enisa.europa.eu/publications/smart-cars>.

¹¹ „ACEA Principles of Automobile Cybersecurity”, ACEA - *European Automobile Manufacturers' Association* (blog), 2017. október 18., <https://www.acea.auto/publication/acea-principles-of-automobile-cybersecurity/>.

KÖVETKEZTETÉSEK

A kiberbiztonsági fogalmak és jogszabályi háttér áttekintése alapján megállapítható, hogy az elektromobilitási eszközök, mint például az e-rollerek, számos kiberbiztonsági kockázattal és fenyegetettséggel szembesülnek. A kiberbiztonság, adatvédelem, hálózatbiztonság és a hozzájuk kapcsolódó fogalmak fontos szerepet játszanak a felhasználók és a rendszerek védelmében, és elengedhetetlenek az elektromobilitás biztonságos fejlődéséhez és fenntarthatóságához.

A jogszabályi háttér elemzése azt mutatja, hogy az e-rollerek gyártóinak és szolgáltatóinak számos előírást kell betartaniuk, amelyek az adatvédelem, termékbiztonság és kiberbiztonság területét érintik. Az EU rendeletek és irányelvek mellett az ENISA és az ACEA ajánlásai is iránymutatást nyújtanak az elektromobilitási eszközök kiberbiztonságának javításához és a megfelelő védelmi intézkedések meghozatalához. A kiberbiztonsági intézkedéseket és jogszabályokat figyelembe véve nyílik lehetőség arra, hogy az elektromobilitási eszközök biztonságosabbá váljanak, minimalizálva ezzel a kiberbiztonsági kockázatokat és növelve a felhasználók bizalmát.

2 AZ ELEKTROMOBILITÁSI ESZKÖZÖK

Az elektromos járművek története és fejlődése a 19. századra nyúlik vissza, ám csak az utóbbi években váltak igazán elterjedtté. Az elektromos közlekedés térnyerése számos alternatív járművet hozott magával, mint az elektromos rollerek és kerékpárok. Ezek környezetbarát megoldások, bár még mindig vannak korlátai, mint például a hatótávolság és a töltési infrastruktúra hiánya. Az elektromobilitás jelenlegi helyzete azonban kedvező, az egyre szigorúbb környezetvédelmi szabályozások és a technológiai fejlődés ösztönzi az áttérést az elektromos járművekre.

2.1 Az elektromos járművek történeti áttekintése

A közlekedési eszközök, akár csak a mobiltelefonok, vagy számítógépek folyamatos fejlődés alatt állnak. A technológiai rendszerek innovációi folyamatosan adaptálásra kerülnek a járműiparba is. Ezért elkerülhetetlen volt az a jelenség, hogy a közlekedési eszközök csatlakozzanak a hálózatra. Egy átlag járműhasználó életében a választott jármű típusától függően más-más lehetőségek állnak rendelkezésre az internetes hálózathoz való csatlakozásra. Eleinte még csak maximum Bluetooth-os kapcsolatok létesítésre voltak képesek egyes járművek, például egy személygépkocsi kihangosító rendszere. Azonban az igények folyamatosan fokozódtak a felhasználói oldalról, így megjelentek a GPS rendszerek, az érintőképernyős fedélzeti számítógépek, és a mára már hétköznapiak számító TESLA önvezető járművek rendszerei.

Az elektromos járművek térhódítása már évekkal korábban elkezdődött¹², azonban a 2015-ös év környékére tehető főként, hogy az elektromos autózás hétköznapivá vált és berobbant a köztudatba Magyarországon. Ugyanis 2014. március 13-án a kormány bejelentette, hogy adókedvezményeket és támogatásokat ad az állampolgároknak, annak érdekében, hogy az elektromos autók elterjedhessenek Magyarországon. Az első nagyobb ugrás a zöld rendszámú járművek tekintetében 2016-ban történt. 2015-ben még csak 303 darab elektromos meghajtású jármű közlekedett az utakon, míg 2016 decemberében már ugyan ez a szám 1524 darab volt, ami ötszörös növekedést jelentett.¹³ A jelenlegi számok tekintetében a 2022-es évben minden

¹² Chuyuan Xu, „Research on Range Extended Electric Vehicle Based on Cruise”, *Journal of Physics: Conference Series* 2479, sz. 1 (2023. április 1.): 012012, <https://doi.org/10.1088/1742-6596/2479/1/012012>.

¹³ Z. TÓTH, „The electric vehicle penetration in Hungary.”, *International Journal of Engineering and Management Sciences Vol. 2.*, sz. No. 4. (2017), <https://doi.org/10.21791>.

rekordot megdöntött a zöldrendszámú autók átadása Magyarországon, köztük is a tisztán elektromos autók eladása nőtt a legnagyobb mértékben, és az év végén már 34 754 közlekedett az utakon. A legfrissebb adatok alapján pedig 2023. június végén 41 386 tisztán elektromos autó közlekedett az utakon Magyarországon, míg a zöld rendszámú autók száma már meghaladta a 74 000 darabot.¹⁴

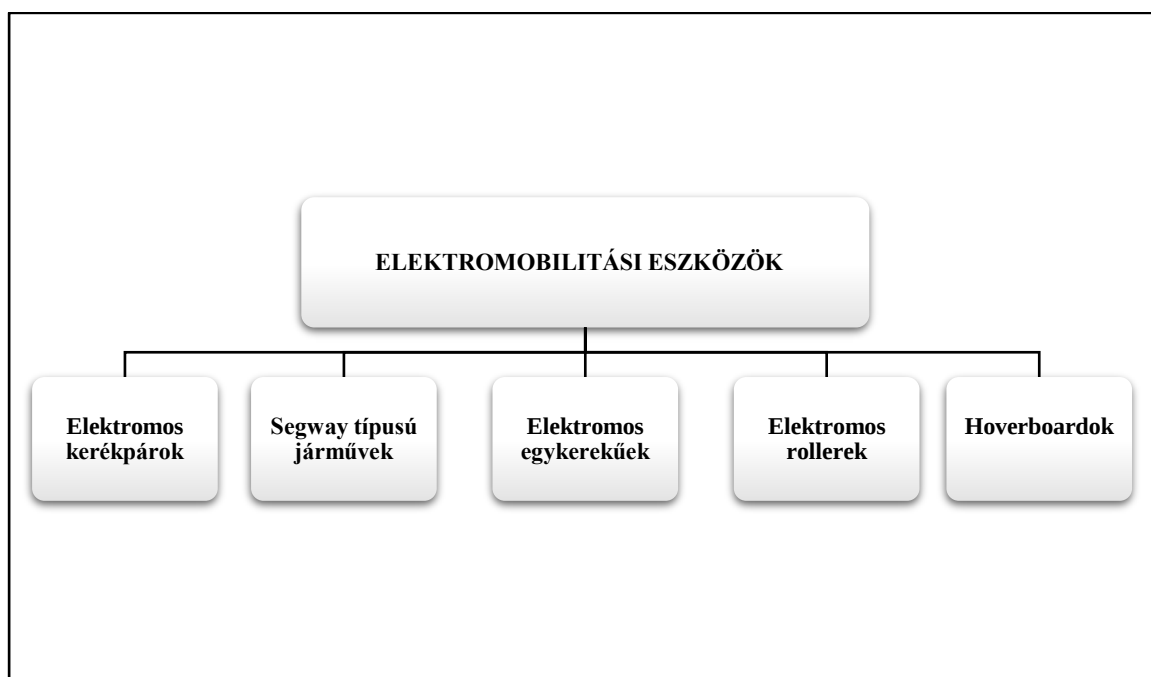
A fentiek alapján megállapítható, hogy az emberek környezettudatossá válása és a fenntartható mobilitásra való törekvés egyre nagyobb figyelmet kap. Ezt bizonyítja az a tény is, hogy az elektromos mobilitási eszközök száma is napról napra növekszik a közúti közlekedésben. Hiszen például az elektromos rollerek, hoverboardok¹⁵, segway¹⁶-ek kiváló alternatívát nyújtanak a környezetbarát közlekedés terén, a városi közlekedéshez a kompaktságuk miatt is hasznosak, illetve az egyre fejlettebb akkumulátorok és a jobb teljesítményű motorok lehetővé teszik, hogy ezek az eszközök hosszabb távokra is alkalmasak legyenek, és kényelmesebben használhatóak legyenek a felhasználók számára.

¹⁴ Pásztor Csaba, „Egyre magabiztosabban és többen villanyautóznak Magyarországon”, 2023. augusztus 2., <https://totalcar.hu/magazin/hirek/2023/08/02/egyre-magabiztosabban-es-tobben-villanyautoznak-magyarorszagon/>.

¹⁵ A hoverboard egy lapos, kétkerekű, kis elektromos jármű, melyet a talpunk lenyomásával irányíthatunk. Segítségével könnyedén kanyarodhatunk, gyorsulhatunk és lassulhatunk, mivel beépített giroszkóp és elektronika segíti mozgásunkat.

¹⁶ A Segway egy közlekedési eszköz, melyet a talpak és testsúly mozgásával irányítanak. Ez egy két kerekű jármű, amely elektromos meghajtással rendelkezik és van rajta kar, amely segíti az irányítást.

2.2 Elektromobilitási eszközök típusai



2. ábra: Elektromobilitási eszközök típusai

(Saját szerkesztés)

A hétköznapi közlekedési eszközök mellett megjelentek a kis helyigényű és kis energiafelhasználású, de rugalmas mobilitást szolgáló elektromos eszközök, ezeket nevezzük elektromobilitási közlekedési eszközöknek. A rengeteg újfajta elektromos eszköz mellett, megjelentek szinte teljesen új eddig nem ismert közlekedési eszközök is, például az e-roller vagy e-unicikli. Ezeknek az eszközöknek a közös tulajdonsága, hogy kapcsolatot kell létesíteniük egy okostelefonnal a kommunikáció és az információ áramlás fenntartásának érdekében. Az alábbiakban ezekről a közlekedési eszközök tulajdonságairól és jellemzőikről lesz szó.

2.2.1 Elektromos kerékpárok

Az elektromos kerékpárokon belül három fő típus különíthető el. A legelterjedtebb típusban az elektromos motor segít a láncos meghajtásban, angolul ezt a típust pedal-electricnek nevezik, melyből alakult ki a pedelec összevonású szó. A másik típusok tisztán az akkumulátor erejére támaszkodnak, ilyenkor kizárólag az elektromotor hajtja a kerékpárt. Az elektromos kerékpárok általában pedálozás mellett is működtethetők, és nagy hatótávolsággal rendelkeznek. Amennyiben az akkumulátor lemerülne, továbbra is használhatók hagyományos kerékpárként.

A fékrendszerük általában tárcsafékes, hasonlóan a fékkarok meghúzásával működik, mint a hagyományos kerékpárok fékjei.

„Pedelec: Az elektromos motor kizárólag a pedállal történő hajtásra segít rá, ez maximum 25 km/h sebességig működik. Azonban vannak olyan kínai gyártótól származó típusok is, amelyekben nincs semmi korlátozás, és megvásárolhatók Magyarországon.

S-pedelec: A motor szintén csak tekeréskor segít be a hajtásba, viszont már maximum 45 km/h sebességig működik. 300 W teljesítményig kerékpárnak minősül.

E-bike: Elektromos hajtásával önálló mozgásra is képes, pedálhajtás nélkül, gázkarral, vagy gombnyomásra. Ez a típus már kizárólag vezetői engedéllyel, biztosítással, és bukósisak viselése mellett használható.”¹⁷



3. ábra: E-bikehoz tartozó okosberendezés (forrás: Luxuo¹⁸)

Az elektromos kerékpárok egyre gyakrabban vannak felszerelve különböző informatikai berendezésekkel és eszközökkel azért, hogy javítsák a felhasználók élményét és biztonságát. Sok gyártó kínál okostelefonos alkalmazásokat az elektromos kerékpárokhoz, amelyek segítségével a felhasználók beállíthatják a sebességet, vagy például ellenőrizhetik az

¹⁷ „Minden, amit az alternatív közlekedési eszközökről tudni érdemes”, Magyar Autóklub, elérés 2024. április 8., <https://www.autoklub.hu/minden-amit-az-alternativ-kozlekedesi-eszkozokrol-tudni-erdemes/>.

¹⁸ Jonathan Ho, „5 Luxurious Designer Electric Bicycles”, LUXUO, 2017. június 19., <https://www.luxuo.com/cars/5-luxurious-designer-electric-bicycles.html>.

akkumulátor állapotát. Hasonlóan sok gyártó szereli fel ezeket az eszközöket GPS nyomkövetéssel, amelyek segítenek a felhasználónak nyomon követni az útvonalat, később pedig megtekinteni az utazás részleteit. Számos modern elektromos kerékpár rendelkezik olyan szenzorokkal, amik mérhetik a pedálozási erőt, sebességet és egyéb teljesítmény adatokat, ezek szintén segíthetnek a felhasználónak optimalizálni az edzéseit vagy az utazásait.

Az elektromos kerékpárok előnyei közé sorolható, hogy megfelelő figyelemmel használva jelentősen javíthatják a közlekedés biztonságát, kevesebb helyet foglalnak el az utakon, és csökkentik a tömegközlekedés zsúfoltságát. A pedelec típusú kerékpárok hátrányai közé sorolható pedig, hogy a súlyuk miatt nehezebb őket tárolni vagy szállítani. Emellett a technológia ára jóval magasabb, mint a hagyományos kerékpároknál. Illetve a nagyobb sebesség pedig súlyosabb baleseti kockázatot is hordozhat magában.

2.2.2 Elektromos egykerekűek

Az unicklik hagyományosan egy kerekes közlekedési eszközként ismertek, azonban az elektromos változatok megjelenése új lendületet adott az elterjedésüknek. Az elektromos unicklik olyan motoros egykerekűek, amelyeken nincsen kormány. Ehelyett a vezető testsúlya és testmozgása az irányítás alapja, mivel az egyensúlyt az előre vagy hátra mozgatott súlypont segítségével kell fenntartani. Ennek a stabil egyensúlynak a lényege egy beépített giroszkóp, ami függőlegesen tartja az eszközt, így lehetővé téve a vezető számára, hogy könnyedén és precízen irányítsa azt az egyensúlyozás révén.



4. ábra: Elektromos unicikli (forrás: Voltride¹⁹)

Az egyik legismertebb elektromos unicikli típus az Inmotion V5F, ami 14 colos kerékkel és közel 12 kg-os súllyal rendelkezik. Ezek a járművek általában nem rendelkeznek külön lengéscsillapítóval, ehelyett a gumibroncsok rugózási képessége teszi lehetővé az egyenletes és komfortosabb közlekedést. Az Inmotion V5F modellen lámpák találhatók mind elől, mind hátul, valamint akkumulátor töltöttség kijelző is szolgálja a felhasználók kényelmét és biztonságát.

Az elektromos uniciklik általában kisebb kibertámadási felülettel rendelkeznek és kevesebb érzékeny adatot tárolnak, ami csökkentheti a kiberbiztonsági kockázatot ezen eszközök tekintetében. Azonban fontos fenntartani és frissíteni kell az eszközök szoftverét és biztonsági rendszerét, hogy minimalizálják a potenciális fenyegetéseket, különösen azokat, amelyek a vezérlést, a kommunikációt és az esetleges személyes adatokat érintik.

2.2.3 Segway típusú járművek

A Segway az elektromos közlekedés egyik korai úttörője volt, és robbanásszerűen terjedt el a megjelenése után. Ezt a közlekedési eszközt a megjelenése idejéhez képest meglehetősen innovatív technológiával szerelték fel. A Segway teljes mértékben önegyensúlyozó elven

¹⁹ „InMotion V12HT – elektromos egykerekű készleten”, Voltride, elérés 2024. április 8., <https://www.voltride.hu/hu/egyeb-elektromos-jarmuvek/egykerekuek/inmotion-v12ht>.

működik, ami azt jelenti, hogy a beépített lézeres giroszkópok érzékelik, amikor a jármű elkezd dőlni. Ezek az adatok a kerekeket a megfelelő irányba és sebességgel hajtó elektromotorhoz továbbítódnak, így a Segway egy számítógép segítségével megtartja az egyensúlyát.



5. ábra: Segway (forrás: Robotsguide²⁰)

A Segway kerekei általában nagyobbak és nehezebbek az átlagosnál, ami miatt nem számít a legkompaktabb elektromobilitási eszköznek. A Segwayek felhasználása sokrétű például biztonsági szolgálatok gyors reakcióra képes eszközként alkalmazzák, emellett az idegenforgalmi helyeken a turisták is gyakran választják városnézéshez.

A Segwayek általában kevesebb érzékeny adatot tárolnak és kevésbé kapcsolódnak bonyolult hálózatokhoz, ezért alapvetően kisebb kibertámadási felülettel rendelkeznek. Az adatkapcsolatai és kommunikációs lehetőségei főként a Bluetooth-os kapcsolatra támaszkodik applikációval vagy más eszközökkel való összekapcsolódás során.

2.2.4 Hoverboardok

Ahogy korábban említettem, ma már szinte mindennek megvan a maga innovatív elektromos változata. A hoverboardok, melyeket gördeszkákhoz hasonlítva terveztek, mégis különlegesek, hiszen nincs rajtuk sem kormány, sem fékrendszer, a felhasználó csak a saját egyensúlyára számíthat a velük való közlekedés során. Az irányításuk, hasonlóan a Segwayekhez, álló helyzetben történik egy pedálszerű konzollal, amin állunk. A lábfej apró mozdatásával lehet

²⁰ „Segway”, ROBOTS: Your Guide to the World of Robotics, elérés 2024. április 8., <https://robotsguide.com/robots/segway>.

haladni előre vagy hátra, növelni vagy csökkenteni a sebességet, és a kanyarodáshoz egyszerűen csak a kívánt irányba kell dönteni a lábfejet.



6. ábra: Hoverboard (forrás: Scootershop²¹)

Ezek az eszközök rendelkeznek a legkevesebb kiberbiztonsági kockázattal, mivel nincs hozzájuk rendszeresen használt alkalmazás, és az egyetlen külső eszközzel történő kapcsolatuk Bluetooth-on keresztül működik, azonban ez a Bluetooth kapcsolat is csak arra szolgál, hogy a felhasználók a hoverboardokon lévő hangszórón keresztül zenét játszhassanak le, tehát nem kapcsolódnak internetes szolgáltatásokhoz vagy más külső hálózatokhoz.

2.3 Az elektromos rollerek

2.3.1 E-rollerek specifikációi

Az elektromos rollerek Magyarországon elég nagy arányban figyelhetők meg a közúti közlekedésben. Azonban e-roller és e-roller között is van különbség mindegyik típus más-más specifikációkkal rendelkezik. Kialakításuk is megegyezik a hagyományos rollerekkel, pár apró mégis fontos eltérésekkel. Rendelkeznek fellépő résszel, amelyek általában csuszásgátló bevonattal vannak ellátva és egyes gyártók vízhatlan anyagból is készítik ezeket a részeket, így még esős időjárásban is maximális biztonsággal használhatóak. A legtöbb típus két kerékkel

²¹ „Hoverboard IO HAWK CROSS 2.0”, SIP-Scootershop, elérés 2024. április 8., https://www.sip-scootershop.com/hu/product/hoverboard-io-hawk-cross-20_E10020CS.

van felszerelve, azonban megtalálható a piacon három és négy kerekű verzió is. A kerekeken található gumik is típusonként eltérőek lehetnek, hiszen vannak tömör gumis változatok, amelyek jobban ráznak és az úthibákat jobban meg lehet velük érezni, de vannak felfújható gumis változatok is, amelyek sokkal jobbak lengéscsillapítás szempontjából, azonban hajlamosak gyakran defektet kapni. Meg kell említeni, hogy egyes változatok rendelkeznek üléssel is, amelyek biztonsági és kényelmi szempontból jobbnak tekinthetők.

Az e-rollerek technikai adatait tekintve is számtalan különbség található egyes típusok között. Bizonyos típusok kijelzővel is rendelkeznek, amelyről megtudható a legtöbb információ a roller állapotával kapcsolatban, például a pillanatnyi sebesség vagy az akkumulátor töltöttségének állapota. A gyártók általában 25 km/órás végsebességre korlátozzák a típusok maximális sebességét, de található olyan típus is, amelynek a végsebessége elérheti a 120 km/órát is. Rendelkezhetnek még továbbá lopásgátlóval, tempomattal és egyéni sebességkorlátozó funkcióval is. Az átlagos hatótávolságuk az e-rollereknek 30-45 kilométer közé tehető, illetve az e-rollerek motorjainak az átlagos teljesítménye 250-300 Watt. A technikai fejlődés folyamatos az elektromos rollerek tekintetében is, hiszen vannak olyan típusok, amelyek rendelkeznek E-ABS rendszerrel.

2.3.2 E-rollerek elterjedése

Az elektromos rollerek elterjedése a technológiai fejlődéssel párhuzamosan haladt előre. Az elektromos hajtás és a villanymotor már 193 éve ismert, hiszen Jedlik Ányos 1828-ban elkészítette az első elektromágneses kölcsönhatáson alapuló forgókészüléket, a villanymotor őst.²² Azonban az igazi áttörést a nagy kapacitású lítium-ion akkumulátorok megjelenése jelentette, hiszen ezeknek köszönhető, hogy egyes modelleknél az akár 70 km-es hatótáv. Ugyanis ilyen akkumulátorok nélkül, az elektromos közlekedési eszközök nem rendelkezhetnének ilyen hosszú hatótávval. Az elektromos rollerek az elterjedésüket valójában nem az árúknak köszönhetik, mivel a mai napig elég drágáknak bizonyulnak ezek a közlekedési eszközök, az interneten található típusok között a legolcsóbbak olyan ötven és százezer forint körül mozognak, viszont további böngészés során felfelé egészen nagy terjedelmű skálán mozognak az árak, mivel lehet találni elektromos rollert, akár több millió forintért is, ami már akár egy személygépkocsi árával is megegyezik. Ezek alapján megállapítható, hogy az elterjedés nem az árúknak, hanem a körjük kialakított üzleti háttérnek tudható be. Ugyanis sok

²² „Technikatörténeti szemle 22. (1996) | Könyvtár | Hungaricana”, elérés 2024. április 8., https://library.hungaricana.hu/hu/view/ORSZ_KOZL_TechTortSzle_22/?pg=108&layout=s.

felhasználó nem a saját tulajdonában álló e-rollerrel közlekedik, hanem bérjáművekként használják őket. Magyarországon ezt az üzleti modellt alkalmazza a 2017-ben alapított lassan Európa legtöbb nagyvárosában megjelenő Lime nevű nemzetközi vállalat, illetve ilyen vállalatok még a Bird és a TIER is. Ez az üzleti modell azonban újabb kiberbiztonsági kihívásokat vet fel. Az elektromos rollerek megosztott használata azt jelenti, hogy a felhasználók széles körűen használják és hozzáférnek ezekhez a járművekhez, és ezáltal növekszik az esélye a biztonsági incidenseknek és visszaéléseknek. Ezenkívül a fizikai biztonság is jelentős kérdést vet fel. Ezek az elektromos rollerek nyilvánosan hozzáférhetők az utcákon és a köztereken, ami lehetőséget teremt a fizikai rongálásra, lopásra vagy akár a járművek manipulálására. Ezek a fenyegetések különösen akkor jelentkezhetnek, ha a rollereket nem megfelelően ellenőrzik vagy tartják karban a szolgáltatók.

2.3.3 Közösségi megosztáson alapuló e-rollerek

Magyarország fővárosában, Budapesten 2019-ben látványos változások történtek a közösségi roller használatában, ebben az évben történt áttörés, amikor az e-rollerek megjelentek a közúton. A Lime-S elektromos rollerek bevezetése nyitotta meg az utat a bérlet lehetőségéhez. A szolgáltatás rendkívül egyszerűen működik. Az okostelefonra letölthető alkalmazás segítségével bárki könnyen hozzáférhet az elektromos rollerekhez, majd a használat után bárhol leparkolhatja azokat. A kiválasztott rollert a kormányon található QR-kód segítségével lehet feloldani. Minden felhasználó rendelkezik egy virtuális pénztárcával, amelyre pénzt lehet tölteni, és ha elegendő egyenleg áll rendelkezésre, akkor már használható is az adott roller. A Lime-S rollerek akár 25 km/órás sebességet is elérhetnek, és egy feltöltéssel általában 30-50 kilométert lehet velük megtenni. A szolgáltatás dokkolóállomások nélkül működik, így a rollereket bárhol fel lehet venni és letenni. Minden rollerben GPS található, amely nyomon követi a használatot, így könnyen nyomon követhető, hogy hol hagyta el a felhasználó a járművet és mennyi ideig használta azt, ami alapján a szolgáltató kiszámlázza a használati díjat. A szolgáltató nem Magyarországon, hanem az Egyesült Államokban kezdte meg a rollerek bérbeadását.

Kiberbiztonsági szempontból fontos kiemelni, hogy többek között az okostelefonokra letölthető alkalmazás, amely segíti az elektromos rollerek bérletét, adatvédelmi kockázatokat is hordoz magában. Az alkalmazásnak hozzáférést kell biztosítania a felhasználó helyzetadatához, a fizetési információkhoz és egyéb személyes adatokhoz. Ezért kiemelten fontos, hogy a szolgáltató biztosítsa az adatok biztonságos kezelését és tárolását, valamint megfelelő védelmi

mechanizmusokat alkalmazzon az esetleges adatlopás vagy hackertámadások ellen. Ezekre a kockázatokra figyelemmel kell lenniük mind a szolgáltatónak, mind a felhasználóknak. A szolgáltatónak biztosítaniuk kell a szigorú adatvédelmi intézkedéseket és folyamatosan frissíteniük kell a biztonsági protokollokat a kiberbiztonsági fenyegetések ellen. A felhasználóknak pedig óvatosságnak kell lenniük az alkalmazások letöltésekor és az online fizetéseknél, valamint figyelniük kell a biztonságos jelszavakra.

KÖVETKEZTETÉSEK

Összegezve megállapítható, hogy az emberek keresik az alternatívákat a városi közlekedésre, és az elektromobilitási eszközök kényelmes, gyors és környezetbarát megoldást nyújtanak. Bár áruk magasabb lehet, az egyre növekvő választék és a fejlett funkciók vonzóvá teszik őket a közlekedők számára. Az elektromos rollerek már sok városban közösségi közlekedési eszközökként is megjelentek, hozzájárulva a fenntartható városi mobilitáshoz. Az e-rollerek elterjedése azonban nem mentes a kihívásoktól. A közúti biztonság és a közlekedési szabályok betartásának kérdései továbbra is felmerülnek, valamint a töltési infrastruktúra hiánya is korlátozhatja az e-rollerek használatát. Ugyanakkor a különböző típusú e-mobilitási eszközöknek jelentős előnyeik is vannak, például a rugalmasság, a könnyű szállíthatóság és a környezetbarát működés. Ezért ezek az eszközök továbbra is népszerű közlekedési eszközök maradnak, különösen a városi lakosok körében.

3 KIBERBIZTONSÁGI TÁMADÁSOK, FENYEGETETTSÉGEK

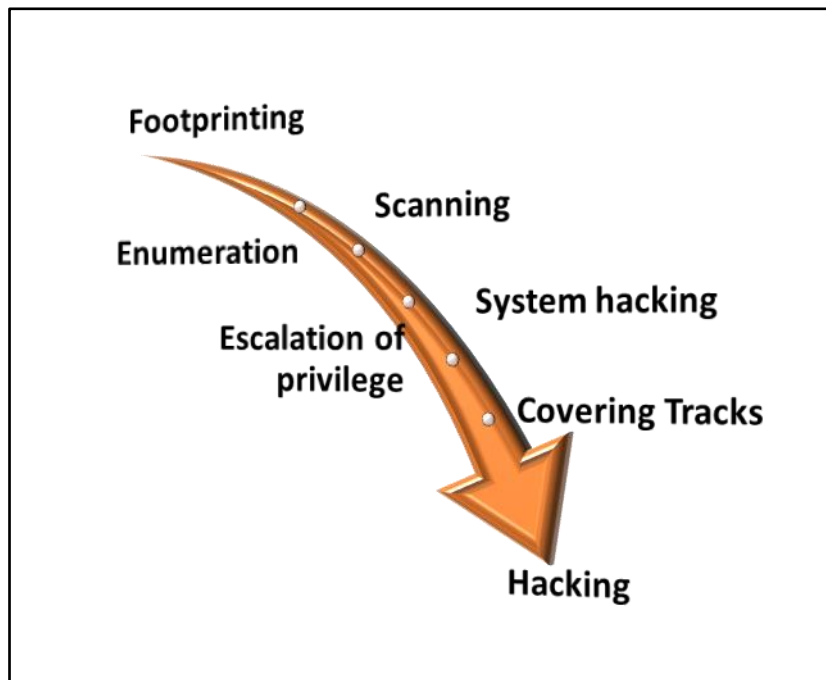
A digitalizáció és az internetes technológiák térnyerésével párhuzamosan a kiberbiztonsági támadások és fenyegetettségek egyre növekvő aggodalomra adnak okot világszerte. A modern társadalmak szinte minden területén jelen vannak az online platformok és digitális rendszerek, amelyek kiszolgáltatottá teszik azokat a kiberbűnözők, hackerek és más rosszindulatú szereplők számára. Ezek a támadások nem csupán gazdasági károkat okozhatnak, hanem súlyosan veszélyeztethetik az egyének és vállalatok személyes adatait, valamint kritikus infrastruktúrákat is.

3.1 A támadások módszertana²³

A kiberbiztonsági támadások ma már nem csak egyszerű fenyegetések, hanem a digitális világban működő szervezetek és egyének számára mindennapi kihívások. Ezek a támadások változatos módszerekkel és technikákkal támadják meg a rendszereket, hálózatokat és az emberek személyes információit. A kiberbiztonsági támadások széles skálán mozognak, különböző méretű és összetettségű szervezeteket célozva meg. Ezek a támadások gyakran átfednek egymással, és egyetlen módszer vagy védekezés sem elegendő az összes lehetséges fenyegetés ellen. Ezért elengedhetetlen az alapos megértés és folyamatos tanulás az új támadási módszerekkel szembeni védekezés érdekében.

Egy IT támadás felépítése sok esetben különbözhet, azonban felismerhető egyfajta általános felépítés. Ennek ismertetésére a Certified Ethical Hacker (CEH) kurzus 9. verziójának tanulási segédletében fellelhető folyamatleírás szolgál alapul.

²³ „CEH v9: Certified Ethical Hacker Version 9 Study Guide | Wiley”, Wiley.com, elérés 2024. április 8., <https://www.wiley.com/en-br/CEH+v9%3A+Certified+Ethical+Hacker+Version+9+Study+Guide-p-9781119419303>.



7. ábra: Egy IT támadás felépítése
(Saját szerkesztés, forrás: CEH v9²⁴)

Footprinting: Ez a lépés az inaktív adatgyűjtés szakasza. Általában az elsődleges passzív módon megszerezhető információk ide tartoznak. Azoknak az adatoknak a gyűjtése, melyek egy célzott támadás alapját képezhetik. Ide sorolhatók például a whois rekordok, melyek alapvető információkat kínálnak egy adott domainről. További információforrást jelenthet a különféle keresőmotorok célzott alkalmazása, a megfelelő keresőkifejezések kialakításához segítséget nyújthat az interneten elérhető Google Hacking Adatbázis (GHDB), ami egy gyűjtemény a keresőmotor célzott felhasználásának lehetőségeiről. Ezek mellett természetesen számos más módja is létezik a szükséges adatok megszerzésének.

Scanning: Ez a lépés a szkennelés folyamata. Ebben a fázisban a támadó felhasználja a korábban megszerzett információkat és sokkal részletesebb, precízebb felderítést végez különféle erre szánt eszközökkel, hogy feltérképezze az elérhető szolgáltatásokat és eszközöket. Itt lehetőség van információ gyűjtésre például az alkalmazott operációs rendszer típusáról, valamint megfelelő tapasztalattal a hálózati biztonsági megoldások egy részéről is. A topológia felderítése is lehetséges ezen eszközök segítségével, amely azt mutatja meg, hogy a

²⁴ „CEH v9: Certified Ethical Hacker Version 9 Study Guide | Wiley”, Wiley.com, elérés 2024. április 8., <https://www.wiley.com/en-br/CEH+v9%3A+Certified+Ethical+Hacker+Version+9+Study+Guide-p-9781119419303>

hálózati eszközök (például számítógépek, szerverek, router-ek stb.) hogyan vannak kapcsolódva egymáshoz a hálózaton keresztül.

Enumeration: Ebben a lépésben a támadó áttanulmányozza a korábbi lépések során szerzett információkat és mélyebb kutatásokkal jut el a rejtett adatokhoz, például felhasználói nevekhez, felhasználói csoportokhoz, alkalmazásokhoz, használt protokollokhoz és bannerekhez. Gyakran ebben a lépésben történik meg a jelszavak megszerzése is.

System Hacking: Ez az a lépés, ahol a rendszer feltörése következik. A korábbi lépések alapján a támadó konkrét lépéseket tervezhet meg. Kitalálhatja, milyen támadási módszereket alkalmazzon, például közvetítéses, injekciós támadást végezzen, malware-t használjon, túlterheléses támadást hajtson végre, vagy akár keyloggert használjon.

Escalation of privilege: Ebben a lépésben a felhasználói jogosultságok bővítése a cél. A korábbi támadások segítségével a támadó arra törekszik, hogy minél magasabb szintű hozzáféréssel és jogosultsággal rendelkezzen a célszámítógépen vagy rendszeren, hogy így később a valós tevékenységeket végrehajthassa.

Covering Tracks: Ez a lépés pedig, pedig az a szakasz, ahol a nyomok eltüntetése a fő cél. Ez különösen fontos egy célzott támadás során, mivel a támadó többet szeretne elérni, kevesebb információt kiszivároztatva. A tapasztalt támadó addig dolgozik, amíg képes a tevékenysége nyomait olyan módon eltüntetni vagy elrejteni, hogy azokra csak nagyon későn vagy egyáltalán ne lehessen rájönni.

A támadási fázisok áttekintése rávilágít arra, hogy a kiberbiztonság terén a védekezés nemcsak az egyes támadási pontok elleni védekezést jelenti, hanem a teljes támadási folyamat megértését és annak ellenőrzését. Az informatikai rendszerek biztonságának megőrzése érdekében kulcsfontosságú a proaktív hozzáállás és a folyamatos monitorozás, valamint a gyors reakcióképesség a támadásokra. Ennek következtében fontos, hogy részletesen megismerjük a támadási fázisok mellett, a konkrét kiberbiztonsági támadások leggyakoribb fajtáit, azok jellemzőit és hatásait.

3.2 A támadások típusai

Malware támadások

A rosszindulatú szoftverek, az angol malicious software, ismertebb nevén malware-ek, talán az átlagos felhasználóban a számítógépes világ sötét oldalának szinonimái. A malware-ek létrehozásának számos célja lehet, például az adatok eltulajdonítása, a rendszerek károsítása vagy a hálózatok megbénítása. Ahogy egy összetett célzott támadásnak, úgy a malware írásának is többféle indítéka lehet.

Ide soroljuk például az alábbiakat:²⁵

- Vírusok és trójai falovak: A vírus saját magát, vagy önmagának egy fejlettebb fajtáját másoló kód. Általában fájlokat, rendszerterületek fertőznek meg. A trójai falovak pedig valamilyen más programnak, vagy annak egy alkotórészének álcázzák magukat.
- Spammer programok: Kéretlen levelek küldésére képes program.
- Flooderek: Olyan módon képesek megnövelni a hálózati adatforgalmat, hogy azok szolgáltatásleálláshoz vezetnek.
- Billentyűzetnaplózók (keyloggerek): A billentyűzet leütéseket, más esetben a monitorképet, vagy más beviteli perifériák tevékenységét rögzítő malware.
- Rootkitek: Olyan kártékony programok, amelyek rendszergazdai jogosultságú, akár kernelszintű hozzáférést biztosítanak később a támadónak.
- Spyware: Internetes tevékenységet kutató programok, azaz titokban információkat gyűjtenek a felhasználók internetes szokásairól.
- „Ransomware (zsaroló vírus): Olyan malwarek, melyek visszaállítható vagy visszaállíthatatlan módon titkosítanak a célrendszerben, majd váltságdíjat kérnek a feloldó kulcs megadásáért.
- Kripto vírusok: A kriptovaluták lopására alkalmas kártékony kódok.
- Destructoware: A trójai falovak egy fajtája. A legitim szoftver valamilyen funkcióját kihasználva kifejezetten romboló hatást ér el.”²⁶

²⁵ Ször Péter, *A vírusvédelem művészete* (Bicske: SZAK Kiadó, 2010).

²⁶ Bodó Attila Pál és mtsai., *Célzott kibertámadások - Éves továbbképzés az elektronikus információs rendszer biztonságért felelős személy számára* (Nemzeti Közszoigálati Egyetem, 2022), <https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/18055>.

DoS/DDoS támadások

A Denial of Service (DoS) és a Distributed Denial of Service (DDoS) rövidítések olyan támadásformákat jelölnek, amelyek során a szolgáltatás megtagadására irányuló támadásokat valósítanak meg, illetve ezek elosztott túlterheléses változatát, általában botnetekkel szervezve. A DoS támadás lényege, hogy annyi kérést intéznek a célpont hálózatahoz vagy alkalmazásaihoz, amennyit azok nem képesek feldolgozni, így azok elérhetetlenné válnak. E célok elérése érdekében könnyen célpontként kiválasztható egy adott hálózat vagy webes szolgáltatás. A támadók gyakran azt várják, hogy a védelmi intézkedések miatt a célpont szakemberei elfoglalva legyenek, majd ekkor hajtják végre a tényleges támadást. A DoS támadás elleni védekezés alapvetően két módon történik, általában mindkettő egyszerre alkalmazva. Az egyik megoldás a nagy hálózati kapacitással rendelkező szolgáltatók igénybevétele, akik képesek szűrni a hálózati forgalmat. A másik megoldás a szervezet saját hálózati infrastruktúrájának megfelelő alkalmazás szintű szűrése, ami letiltja a gyanús, túlterhelést okozó kéréseket. A DoS és DDoS támadások célja, hogy túlterheljék a célpont infrastruktúráját, így azt elérhetetlenné téve a valódi felhasználók számára.²⁷

Social Engineering támadások

„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 – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”²⁸

A social engineering típusú támadások két fő kategóriába sorolhatók. Az egyik csoportba tartoznak az emberi kapcsolatokra épülő módszerek, amelyek közvetlen interakciót igényelnek a támadó és az áldozat között. A másik kategóriába pedig a számítógép-alapú technikák tartoznak, ahol a támadó az áldozattal való kapcsolatot közvetetten, valamilyen informatikai eszközön keresztül teremti meg.²⁹

A humánmódszerek közé sorolhatók például a következők:³⁰

²⁷ Bodó és mtsai.

²⁸ Dub Máté, „A social engineering támadások megelőzésének lehetőségei”, *Hadmérnök* 16, sz. 3 (2021. november 25.): 173–87, <https://doi.org/10.32567/hm.2021.3.10>.

²⁹ Muha Lajos és Krasznay Csaba, „Az elektronikus információs rendszerek biztonságáról vezetőknek”.

³⁰ Guenther M., „Social Engineering”, *Social Engineering Security Awareness Series*, 2001.

- segítség kérése,
- segítség nyújtása,
- kölcsönösség kihasználása,
- shoulder surfing – képernyő lelesése,
- tailgating – bejutás a bejáraton más embert követve, annak tudtán kívül,
- dumpster diving – információk felkutatása a hulladékban.

A számítógép-alapú támadások körébe sorolhatók pedig a következők:

- scam – hamisított weboldalak.
- adathalászat, amelyek lehetnek:
 - phishing – e-mailalapú,
 - vishing – voip-alapú,
 - smishing – sms-alapúak.

Egy social engineering támadás négy fázisból épül fel: információgyűjtés; kapcsolat kiépítése; kapcsolat kihasználása; támadás végrehajtása.³¹

A social engineering támadások során a támadó arra törekszik, hogy olyan információkhoz juthasson, amelyek nem állnak rendelkezésére, és ehhez általában emberekkel kell közvetlen kapcsolatba lépnie. A támadó olyan módszereket alkalmaz, amelyek során személyes információkat gyűjt a célponttal való interakció során. Gyakran beszélget, próbál bizalmat szerezni, és kedvező hangulatot teremt a célpont körül. A támadó az emberi viselkedésre támaszkodik, például az empátiára vagy a segítségnyújtásra, hogy elérje célját.³²

E támadási technikát egyaránt alkalmazzák a bűnözők, a terroristák és a hírszerzők céljaik elérése érdekében, ami rendkívül eltérő lehet, irányulhat információszerzésre, informatikai rendszer befolyásolására, dezinformálásra és számos egyéb tevékenységre.

³¹ Francois Mouton, Louise Leenen, és H. S. Venter, „Social engineering attack examples, templates and scenarios”, *Computers & Security* 59 (2016. június 1.): 186–209, <https://doi.org/10.1016/j.cose.2016.03.004>.

³² „The Art of Deception: Controlling the Human Element of Security | Wiley”, Wiley.com, elérés 2024. április 8., <https://www.wiley.com/en-us/The+Art+of+Deception%3A+Controlling+the+Human+Element+of+Security-p-9780471237129>.

3.3 Kiberbiztonság a járműiparban

A kibertámadások káros hatásai óriásiak lehetnek egy olyan iparágra, mint a kooperatív összekapcsolt és automatizált mobilitás.³³ 2022-ben megjelent egy fontos ENSZ javaslat, amely az elektromos járművek kiberbiztonságára vonatkozóan kettő javaslatot adott ki. A járművek kiberbiztonsági megfeleléséről (a proposal on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management systems), továbbá a járművek szoftverfrissítésére vonatkozó követelményekről (proposal on uniform provisions concerning the approval of vehicles with regards to software updates and software update management systems)³⁴.

Az ENSZ javaslatai azonban nem teljeskörűen fogalmaznak, inkább csak kijelölte a követendő irányvonalakat a tervezési, a gyártási és a gyártás utáni termék megfigyelési folyamatok tekintetében. A javaslat alapján a gyártóknak kiberbiztonsági irányítási rendszert (cybersecurity management system, CSMS) és szoftverfrissítés-kezelő irányítási rendszert (software update management system, SUMS) kell bevezetni. Fontos megjegyezni, hogy egyes tanulmányok szerint a jelenlegi kiberbiztonsági tudásmegosztási gyakorlatok nem megfelelőek a tényleges és az újonnan megjelenő fenyegetések kezelésére³⁵.

Azonban az ENSZ javaslata nagyban elősegíti a kiberbiztonsági növelését az elektromos járművek piacát tekintve, ugyanis 2022. július 6.-ot követően nem adható ki típusjóváhagyás az elektromos járművekre CSMS vagy SUMS nélkül és ami még fontosabb, hogy 2024. július 7.-ét követően pedig már nem lehet nyilvántartásba venni, olyan elektromos járművet, vagy az ahhoz tartozó olyan alkatrészt, amely nem felel meg az új kiberbiztonsági szabályozásoknak. Ami azért is fontos, mert a Zogby Analytics által készített HSB-felmérés szerint az elektromos járművekkel kapcsolatban megkérdezett személyek 23%-a biztonsági rendszerek sebezhetőségét említette legfőbb aggodalomnak.³⁶ A felmérésből az is kiderül, hogy a válaszadó személyek 53%-a Bluetooth-alapú technológiát használ. A kutatásban résztvevők

³³ Now Publishers, „Artificial Intelligence-Based Cybersecurity for Connected and Automated Vehicles”, 2022. 0 29., <https://www.nowpublishers.com/article/BookDetails/9781638280606>.

³⁴ Péter Bányász, Bettina Bóta, és Zágon Csaba, „A Social Engineering Jelentette Veszélyek Napjainkban” (Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019), 12–37, <https://doi.org/10.37372/mrtvtpt.2019.1.1>.

³⁵ „UN Regulation No 155 – Uniform Provisions Concerning the Approval of Vehicles with Regards to Cybersecurity and Cybersecurity Management System [2021/387]”, elérés 2024. április 8., <https://eur-lex.europa.eu/eli/reg/2021/387/oj>.

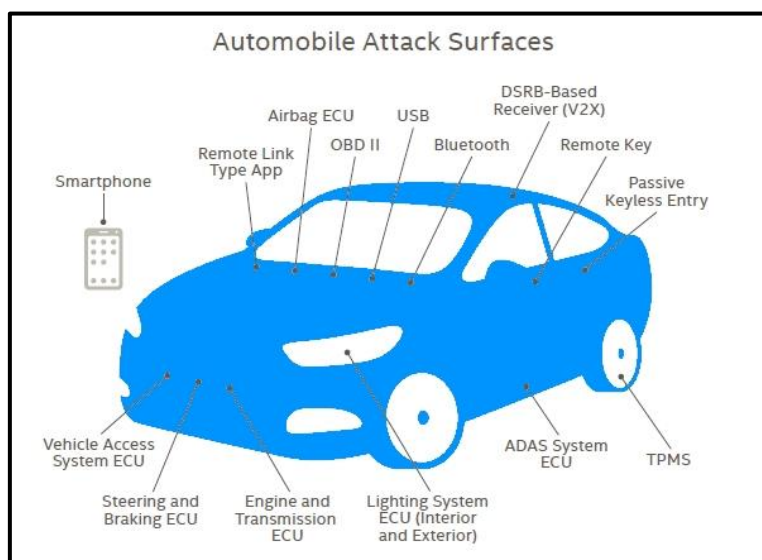
³⁶ Help Net Security, „Consumers Worry about the Cybersecurity of Connected Vehicles”, *Help Net Security* (blog), 2021. április 16., <https://www.helpnetsecurity.com/2021/04/16/cybersecurity-connected-vehicles/>.

42%-a nagy arányban veszik igénybe a különféle navigációs rendszereket, 39%-ban pedig a biztonsági szenzorokat. A megkérdezettek 36%-a pedig okostelefonos alkalmazáson keresztül csatlakozik az elektromos járművéhez, 24%-uk pedig Wi-Fi-n vagy mobil hotspotokon keresztül kapcsolódik az internethálózathoz menetközben.³⁷

A fentiek alapján megállapítható, hogy a villamosítás és az automatizált vezetés mellett az elektromos járművek kiberbiztonsága az egyik legfontosabb kihívás az járműipari fejlesztők, gyártók és az járműipari alkatrész gyártók számára, ezzel igazolva a H5 kutatási tézisémet, mely szerint a kiberbiztonság jelentőséggel bír a jármű gyártás, fejlesztés területén. A kiberbiztonsági irányítási rendszerek és szabályozások célja, hogy a jövőben megvédjék a teljes járművet, az infrastruktúrát és a berendezéseket a fenyegetések ellen.

3.4 Kiberfenyegetettségek a járművek tekintetében

A téma címéből adódóan a jövőbeli kiberfenyegetések nem csak a hétköznapi munkavégzések során lesznek jelen, hanem az elektromos járművek térhódítása miatt a gazdasági szektoron átívelve a mindennapi közlekedésben is megfognak jelenni.



8. ábra: Lehetséges támadási pontok egy jármű tekintetben (forrás: Spiceworks³⁸)

³⁷ Security.

³⁸ „Automotive Cybersecurity: Is Your Vehicle Safe From a Hack? - Security”, Spiceworks Community, 2016. augusztus 10., <https://community.spiceworks.com/t/automotive-cybersecurity-is-your-vehicle-safe-from-a-hack/517370>.

Az egyik ilyen kiberfenyegetettség a jövőben lehet a Vehicle-to-Vehicle kapcsolódás (továbbiakban: V2V). „Az elmúlt években az autóiipari és közlekedési rendszerek hatalmas erőforrásokkal fejlesztették ki az intelligens közlekedési rendszereket (ITS) és a kooperatív intelligens közlekedési rendszereket (C-ITS), valamint az őket összekötő V2X (Vehicle-to-Everything) technológiát”.³⁹ Az elektromos járművek képesek az előttük haladó másik elektromos járművel összekapcsolódni. A járművek közötti kommunikáció természetesen vezeték nélküli hálózat használatával jön létre, ez a funkció hasznos lehet például a haladás során is, ugyanis lehetővé teszi az autó sebességének csökkentését, ha a másik jármű közelebb kerül. Ebben az esetben a kiberfenyegetettség abban rejlik, hogy a támadó visszaélhet a vezeték nélküli hálózat által biztosított kommunikációs technológia hibáival, így könnyedén átveheti az irányítást és akár csökkentheti az autó sebességét, és malwarekkel fertőzheti meg ezt a kapcsolatot a járművek között, amely hatására a V2V rendszer egy lehetőséggé válik ahhoz, hogy megfertőzze a többi csatlakoztatott autót is.

A következő kiberfenyegetettség a „Controller Area Network”-ban (továbbiakban: CAN) rejlik, ugyanis a legtöbb jármű CAN vezérlőt használ, amely a jármű elektronikus vezérlőegységével (továbbiakban: ECU) kommunikál. Az ECU számos alrendszert működtet, például az ABS-t, azaz a blokkolásgátló fékeket, légzsákokat, sebességváltót, média és audiórendszert. Az ECU vezérli továbbá például a jármű motorjának elektronikáját, a sebességváltót, az elektromos zár, a légkondicionáló rendszer és a fényvezérlés moduljait és sok más alkatrészt is.⁴⁰

A járműben lévő hálózat összeköti az ECU-kat és továbbítja az adatokat közöttük. Ez a hálózat magában foglalja többek között a vezérlőterületi hálózatot, a helyi összekötő hálózatot angolul local interconnect network, (továbbiakban: LIN), ethernetet. A LIN egy alacsony sebességű hálózat, amelyet általában ajtózárahhoz, klímaberendezésekhez, biztonsági övekhez, napfénytetőhöz és tükörvezérlőhöz használnak.⁴¹ Az ECU könnyedén elérhető egy külső OBD-eszközzel is, amely mint egy „Backdoor” támadásként képes lesz a jármű vezérlőegységébe bejutva parancsokat adni, és vezérelni a különböző rendszereket-szolgáltatásokat. Fontos

³⁹ Pethő Zsombor, Szalay Zsolt, és Török Árpád, „Safety risk focused analysis of V2V communication especially considering cyberattack sensitive network performance and vehicle dynamics factors”, *Vehicular Communications* 37 (2022. július 1.): 100514, <https://doi.org/10.1016/j.vehcom.2022.100514>.

⁴⁰ Toth Andras, „Information security for electric cars in accordance with nist critical infrastructure cybersecurity framework”, 2017. január 1.

⁴¹ Katona Gergő, „Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése 1. rész”, *Hadmérnök* 18, sz. 3 (2023): 161–76, <https://doi.org/10.32567/hm.2023.3.11>.

megemlíteni, hogy a titkosítás hiánya is egy kiberbiztonsági kockázat, ugyanis CAN-csomagok nincsenek titkosítva, ezért a támadók könnyen elemezhetik a CAN-csomagokat.⁴² „*Sen Nie és társai kísérletileg bemutatták, hogyan vezérelhető az ECU távolról tetszőleges CAN-csomagok küldésével a legújabb firmware-rel frissített Tesla járműben. Tesztelték a Tesla S P85 és P75 modellek sebezhetőségét. Vezeték nélküli (Wi-Fi/celluláris) technológiával számos, a vizsgált járműben lévő rendszert, például integrált áramkört és átjárókat károsítottak meg, majd rosszindulatú CAN-üzeneteket fecskendeztek be.*”⁴³ A felfedezés után a Tesla járműveket az Over-the-air (röviden: OTA) mechanizmussal frissítették, és kódalírási védelmet alkalmaztak.⁴⁴

A jelenlegi jármű technológia lehetővé teszi, hogy az autókhoz csatlakoztassuk az okostelefonjainkat is, amellyel olyan funkciókat használhatunk az autókban, mint a telefonhívás, szöveges üzenetírás, vagy zenehallgatás, ilyen például az Apple CarPlay vagy az AndoridAuto. Ez azért veszélyes, mert a telefon és a jármű kapcsolata során egy előzetesen összeállított rosszindulatú program (például egy malware) azonnal kihasználja a biztonsági réseket a járművekben ezzel veszélyeztetve a járművezetőt, a járművezető adatait, és a közlekedés biztonságát is.

Kiberfenyegetésként említhető a jövőben az elektromos járművek széles elterjedését követően az autólopások módszerének megváltozása is. A legtöbb jármű távolról kulccsal nyitható és zárható már most is. Ezt használja ki az a potenciális támadó is, aki képes anélkül ellopni egy autót, hogy ahhoz bármilyen fizikai behatást alkalmazna. Ezt a fajta kibertámadást általában hackerek használják, és nem is kell hozzá sok felszerelés, emellett kifejezetten hatékony. Ebben az esetben a támadó blokkolja a jelet a jármű vezeték nélküli kulcsáról, amely során nyitva hagyja az autót, mindeközben a jármű válaszol a jelre, amellyel megtéveszti az autó tulajdonosát. A támadás lényege, hogy a kulcs és jármű kommunikációjához használt elektromágneses hullámokat blokkolja, így megakadályozva az autó bezárását. Például egy

⁴² Marko Wolf, Christof Paar, és André Weimerskirch, „Security in automotive bus systems”, *Proceedings of the Workshop on Embedded Security in Cars*, 2004.

⁴³ Katona Gergő, „Autonóm járművek kiberbiztonsági kihívásai (2. rész)”, Ludovika.hu, 2022. január 20., <https://www.ludovika.hu/blogok/cyberblog/2022/01/20/autonom-jarmuvek-kiberbiztonsagi-kihivasai-2-resz/>.

⁴⁴ Kyounggon Kim és mtsai., „Cybersecurity for autonomous vehicles: Review of attacks and defense”, *Computers & Security* 103 (2021. április 1.): 102150, <https://doi.org/10.1016/j.cose.2020.102150>.

kutatás során egy VW Group távirányító jelét továbbították, majd a járműből küldött jelet lehallgatták, így tetszőlegesen hozzáférhettek a járműhöz.⁴⁵

3.5 Kiberfenyegetettségek az elektromos roller tekintetében

Több kutatás alapján megállapítható, hogy az elektromos rollerek Magyarországon elég nagy arányban figyelhetők meg a közúti közlekedésben és a számuk folyamatosan növekszik. Ahogyan már korábban említettem az elektromos rollerek tekintetében beszélhetünk saját tulajdonú és közösségi megosztáson alapuló e-rollerekről. Mindegyik rollerben található egy globális helymeghatározó rendszer, amely nyomon követi az adott személy használatát. A globális navigációs műholdrendszer egy műholdalapú helymeghatározó, navigációs és időmérő (Position, Navigation and Timing, PNT) rendszer. Jelenleg számos GNSS van a kiépítés és a működés különböző szakaszaiban. Az amerikaiak által használt globális helymeghatározó rendszer vitathatatlanul a legismertebb. Mindazonáltal az európai vezetésű GALILEO, az orosz vezetésű GLONASS, a kínai BeiDou, az India által vezetett IRNSS és a japán QZSS mellett áll.⁴⁶ Együttes keretrendszerként a GNSS egy világszerte meghatározó és költséghatékony kültéri PNT-technológiává vált. Az egyes GNSS-technológiák alkalmazása elengedhetetlen egy elektromos jármű, mint például egy e-roller esetében, a pontos helymeghatározás érdekében. Továbbá a jövőben megalakuló intelligens közlekedési rendszerben az egyes járművek és forgalmi helyzetek meghatározásához is szükséges a szenzorok alkalmazása.⁴⁷ Azonban ez a helymeghatározó rendszer is rejt magában számos kockázatot, például egy rosszindulatú szándékkal rendelkező támadó stratégiailag kiválaszthatja és hamisíthatja egy vagy több e-roller helyzetét egy eldugott területre vagy olyan területre, ahol minimális az emberi jelenlét, hogy ezzel odacsalva a potenciális áldozatot.⁴⁸

Az elektromos rollerek kiberbiztonsági kockázatai főként a közösségi megosztáson alapuló e-rollerek tekintetében jelennek meg, hiszen ezek azok a szolgáltatók, akik a felhasználók adatait

⁴⁵ „Proceedings of the 25th USENIX Conference on Security Symposium”, Guide Proceedings, elérés 2024. április 8., <https://dl.acm.org/doi/proceedings/10.5555/3241094>.

⁴⁶ Sujoy Mandal, „Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region”, *Advances in Space Research*, 2018. január 1., https://www.academia.edu/88455421/Augmentation_of_GNSS_utility_by_IRNSS_NavIC_constellation_over_the_Indian_region.

⁴⁷ Gergő, „Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése 1. rész”.

⁴⁸ Nisha Vinayaga-Sureshkanth és mtsai., „Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems”, in *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security (CODASPY '20: Tenth ACM Conference on Data and Application Security and Privacy*, New Orleans LA USA: ACM, 2020), 31–35, <https://doi.org/10.1145/3375706.3380559>.

kezelik, ők felelnek a járművek karbantartásáért és azért is, hogy kiberbiztonsági szempontból sebezhetetlenek legyenek ezek a közlekedési eszközök. Azonban sajnos mégis vannak olyan gyengepontok, amelyek aggasztóak lehetnek. Egy feketekalapos hacker Bluetooth kapcsolaton keresztül a jármű közelében képes az e-rollerek firmware-jét letörölni és egy általa módosítottat felölteni arra, amivel például képes lehet, hogy növelje az előtte korlátozott sebességet. Erre megoldás lehet, hogy az e-rollerekre kizárólag jóváhagyott firmware-t lehessen telepíteni. Valamint, hogy a szolgáltatók vagy a gyártók korlátozzák a harmadik féltől származó alkalmazásokat, hogy hozzáférhessenek az e-rollerek firmware-jéhez.

Számos szolgáltató kínál mobil alkalmazást az elektromos rollerhez, azonban itt megjelenik egy következő kiberfenyegetettség az elavult alkalmazásbiztonság. Mai napokban már a legnépszerűbb elektromos autókhoz is léteznek speciális alkalmazások, amelyekkel a felhasználók rengeteg érdekes és hasznos információhoz juthatnak hozzá a saját autójukkal kapcsolatban. Ez igaz az elektromos rollerekre is, hiszen ezeknek a rollereknek a rendszere, főként Bluetooth-on vagy Wi-Fi kapcsolaton keresztül kommunikálnak. Azonban ahogy minden hálózati kapcsolat megtámadható, és ha nincsen megfelelő védelemmel ellátva, akkor fel is törhető. A hackerek olyan szoftvereket hoznak létre, amelyek megkerülhetik az alkalmazások kiberbiztonságát. Ennek eredményeképpen képesek betörni az alkalmazásba és átvenni az irányítást. A hackerek képesek arra, hogy saját kódot futtassanak az alkalmazásokon. Ami azt jelenti, hogy megváltoztathatja az alkalmazás működését, vagy teljesen leállíthatja annak működését. Az adattitkosítás hiánya szintén kiberfenyegetettség a jövőben. Számos szolgáltató esetében jelenleg az adatok átvitele HTTP használatával történik, ezeket frissíteni kell HTTPS-re. Pontosan azért, hogy a felhasználói adatok, az utazások adatai és a bejelentkezési adatok mind-mind titkosítva legyenek és ne lehessen hozzáférni ezekhez.

Ahhoz, hogy megértsük és hatékonyan kezeljük ezeket a kockázatokat, fontos áttekinteni és elemző módon megvizsgálni az e-rollerek lehetséges támadási pontjait. Ezért egy táblázatba szedve szemléltetem az e-rollerek legfőbb támadási pontjait, valamint ezek magyarázatát. A táblázat segítségével könnyen azonosíthatjuk az e-rollerek legkritikusabb biztonsági problémáit, és a későbbiekben javaslatokat lehet tenni a megfelelő megelőzési stratégiákra a felhasználók és az eszközök védelme érdekében.

1. táblázat: Az e-rollerek lehetséges támadási pontjai
**(Saját szerkesztés, forrás: Addressing Cybersecurity⁴⁹,
 Cyber Security Considerations⁵⁰)**

Támadási pontok	Magyarázat
Firmware manipuláció	A hackerek módosíthatják az e-rollerek firmware-jét, például növelhetik a sebességet vagy kikapcsolhatják a biztonsági funkciókat, ami veszélyeztetheti az e-rollerek felhasználóit.
Alkalmazásbiztonság megkerülése	Az alkalmazások biztonsági intézkedéseit megkerülve, lehetőség nyílik arra, hogy illetéktelenül hozzáférjenek az e-rollerek felhasználói adataihoz, például a felhasználók személyes információihoz vagy a közlekedési tevékenységeikhez kapcsolódó adatokhoz. Az adatok átvitele HTTP-n keresztül történik, ami kockázatot jelent. Az adatok titkosítása HTTPS használatával szükséges a biztonságos adatátvitel érdekében.
Adattitkosítás hiánya	Az adatok titkosításának hiánya lehetővé teszi a hackerek számára, hogy illetéktelenül hozzáférjenek az e-rollerek felhasználói adataihoz, például a felhasználók személyes információihoz vagy a közlekedési tevékenységeikhez kapcsolódó adatokhoz. Az adatok átvitele HTTP-n keresztül történik, ami kockázatot jelent. Az adatok titkosítása HTTPS használatával szükséges a biztonságos adatátvitel érdekében.
Bluetooth és WiFi kapcsolat	A Bluetooth kapcsolatok kihasználása lehetővé teszi a hackerek számára, hogy távolról kapcsolódjanak az e-rollerekhez, és manipulálják azok működését vagy akár ellopják azokat. Ha az e-roller alkalmazást használ, és az okostelefon Bluetooth vagy WiFi kapcsolaton keresztül kommunikál az eszközzel, ezek a csatornák sebezhetővé tehetik a rendszert.
Szoftverfrissítési sebezhetőség	A szoftverfrissítések során felmerülő sebezhetőségek lehetővé tehetik a hackerek számára, hogy kártékony szoftvereket telepítsenek az e-rollerekre, vagy akár illetéktelen hozzáférést szerezzenek azokhoz a frissítési folyamatok során.
Felhasználói hitelesítési problémák	Gyenge felhasználói hitelesítési mechanizmusok vagy hiányos bejelentkezési eljárások lehetőséget adnak a hackereknek arra, hogy illetéktelenül hozzáférjenek az e-rollerekhez.
Adatvédelmi problémák	Az e-rollerekről gyűjtött és tárolt felhasználói adatok védelmének hiánya komoly kockázatot jelent a felhasználók személyes információinak illetéktelen hozzáférése és felhasználása szempontjából, ami súlyos következményekkel járhat az érintettek számára.
Rendszerhiba és sérülékenység	Az e-rollerekben és azok működéséhez szükséges rendszerekben lévő hardver- és szoftverkomponensek sérülékenységei és rendszerhibái lehetővé tehetik a hackerek számára, hogy különféle támadásokat hajtsanak végre az e-rollerek ellen, beleértve a fizikai károkozást és a távoli irányítást.
Felhasználói adatlopás	A hackerek az alkalmazásokon keresztül hozzáférhetnek a felhasználói adatokhoz, például a személyes információkhoz vagy a banki adataikhoz, és ezeket illetéktelenül felhasználhatják vagy értékesíthetik, ami súlyos következményekkel járhat az érintettek számára.
Fizikai hozzáférés kockázata	A fizikai hozzáférés megszerzése az e-rollerekhez lehetővé teszi a hackerek számára, hogy fizikai károkat okozzanak az eszközökön, például azok megsemmisítésével vagy manipulálásával, ami veszélyeztetheti az e-rollerek felhasználóinak biztonságát és magánéletét.

⁴⁹ Nikolaos Argyropoulos és mtsai., „Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CAMEL”, *Transportation Research Procedia*, 23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus, 52 (2021. január 1.): 307–14, <https://doi.org/10.1016/j.trpro.2021.01.036>.

⁵⁰ Binod Vaidya és H.T. Mouftah, „Cyber Security Considerations for Automated Electro-Mobility Services in Smart Cities”, 2020, 457–73, <https://doi.org/10.1201/9780429329401-17>.

KÖVETKEZTETÉSEK

A kiberbiztonsági kockázatok áttekintése során megállapítható, hogy számos potenciális támadási pont létezik az elektromobilitási eszközök tekintetében, amelyek veszélyeztethetik akár az e-rollerek, akár más e-mobilitási eszköz felhasználóinak biztonságát és adatainak védelmét, ezzel igazolva a H1. kutatási hipotézisemet.

Fontos hangsúlyozni, hogy ezeket a kockázatokat lehet és kell is kezelni a megfelelő védelmi intézkedésekkel és gyakorlatokkal. Az e-rollerek tervezése és üzemeltetése során kiemelt fontosságú az adatvédelem és a felhasználók bizalmának megőrzése, ezért folyamatos figyelemmel kell kísérni a kiberbiztonsági kockázatokat és azokra hatékony válaszokat kell kidolgozni a felhasználók védelme érdekében. A biztonságos és kényelmes közlekedés érdekében a gyártók, szolgáltatók és felhasználók közös felelőssége, hogy az e-rollerek világa folyamatosan fejlődjön.

4 ELEMZŐ, VIZSGÁLÓ MUNKA

Az egyre fejlettebb technológiai eszközök és az internet térhódítása új dimenziókat nyitott meg a kibertérben folyó tevékenységeknek, mind a jószándékú, mind pedig a rosszindulatú szereplők számára. Az ilyen jellegű kihívások megértése és megfelelő kezelése érdekében alapos és átfogó kutatásokra van szükség. A kérdőíves kutatás az egyik leggyakrabban alkalmazott módszer az ilyen jellegű problémák feltárására és megértésére. A jelen kutatás célja a kiberbiztonsági kihívások feltárása és azok kezelésére javaslatok kidolgozása. A kérdőív segítségével részletesen elemzésre kerülnek azok a tényezők, melyek hatással lehetnek a kiberbiztonságra.

4.1 Kutatás

Az általam megfogalmazott és a problémát körülölelő kérdésekre adandó válaszokat az eddig folytatott internetes kutatások által előtárt adatokkal, valamint a jelen fejezetben bemutatni kívánt kutatási eredményekkel kívánom alátámasztani. Annak érdekében, hogy valóságghú és alapos következtetéseket vonhassak le, fontosnak tartottam egy olyan kutatási módszer kiválasztását, amely nem csupán friss eredményeket szolgáltat, hanem speciális járművek, így például az elektromos rollerek esetében is alkalmazható. Az előző részekben összegyűjtött adatok nagy része internetes forrásokból származott, és bár sok tudományos közlekedési cikk volt segítségül a munkámhoz, azonban konkrét írott szakirodalom az elektromos rollerek kiberbiztonságára vonatkozóan kevés számban állt rendelkezésemre.

4.2 A kérdőív

Az általam végzett kérdőíves kutatás a konkrét vizsgálathoz kapcsolódóan kvantitatív és nem reprezentatív. Az általam alkalmazott módszertant tekintve véletlenszerű mintavételen alapuló kérdőíves felmérés. A kérdőívben egyes, többszörös választásos és értékelő-skálás kérdéseket tettem fel.

A kutatásom először a kérdőív megtervezésével kezdődött. Az ideális objektumszám és a megfelelő kérdéstípusok meghatározása volt az első feladat, olyan szempont alapján, hogy az adott válaszok alkalmasak legyenek a vizsgálat során az informatikai elemzésre is. Ennek függvényében összesen 28 kérdést állítottam össze, amelyből 11 darab egyszeres választásos,

2 darab többszörös választásos, 14 darab értékelő-skálás és 1 darab nyitott kérdés. Az ideális kérdésszám meghatározása azon elvárások alapján kerültek megállapításra, hogy a kérdőíves kutatás megfelelően széles spektrumú legyen, illetve, hogy a kapott adatok és eredmények kezelhető mennyiségűek legyenek. A kérdőív megnyitását 2024. január 24-re időzítettem és a válaszok befogadása egészen március 28-ig zajlott, ekkor került lezárásra a kérdőív.

Az általam összeállított kérdőív az alábbiak szerint tagozódik:

- Demográfiai adatok: Az első részben demográfiai kérdések találhatók, amelyek segítségével a válaszadók neme, életkora, iskolai végzettsége és lakhelye kerülnek rögzítésre.
- Felhasználói szokások: Ez a rész arra irányul, hogy feltárja a válaszadók elektromobilitási eszközökkel kapcsolatos felhasználói szokásait, beleértve a saját eszköz birtoklását és használatát, valamint a közösségi megosztáson alapuló eszközök használati gyakoriságát.
- Közösségi hatások: Ebben a részben a válaszadók az elektromobilitási eszközök közösségi hatásait értékelhetik.
- Kiberbiztonsági tudatosság: A kérdőív ezen része arra irányul, hogy feltárja a válaszadók kiberbiztonsági tudatosságát és ismereteit az elektromos mobilitással kapcsolatban.
- Technológia elfogadással kapcsolatos hajlandóság: Az utolsó részben a válaszadók a technológia elfogadásával kapcsolatos hajlandóságát mérik fel a TAP-index segítségével, beleértve az optimizmust, jártasságot, függőséget és sebezhetőséget.

A technológia elfogadással kapcsolatos hajlandóság kifejezés azt jelenti, hogy mennyire hajlandóak az emberek elfogadni és alkalmazni az új technológiákat az életükben. A TAP-modell egy olyan módszer vagy skála, amely segít mérni az emberek ebben a téren mutatott hajlandóságát, és figyelembe veszi a támogató (optimizmus, jártasság), gátló (függőség és sebezhetőség) tényezőket.⁵¹

Az optimizmus faktor azt mutatja, hogy az egyén mennyire hisz abban, hogy a technológiai fejlesztések pozitív hatással lesznek az életére. A jártasság arra utal, hogy az egyén milyen

⁵¹ Berényi László és Deutsch Nikolett, „Technology Adoption among Higher Education Students”, *Vezetéstudomány / Budapest Management Review*, 2023. november 13., 28–39, <https://doi.org/10.14267/VEZTUD.2023.11.03>.

mértékben jártas a technológiák használatában és kezelésében. A függőség faktor azt méri, hogy az egyén mennyire függőséget alakított ki a technológiával való interakciójában. A sebezhetőség arra utal, hogy az egyén mennyire érzi magát sebezhetőnek a technológiai változásokkal szemben.

Ezek a faktorok különböző módon befolyásolják az emberek hajlandóságát az új technológiák elfogadására. A TAP-index segítségével ezeket a faktorokat mérve jobban megérthetjük, hogyan reagálnak az emberek az új technológiákra, és hogyan lehet ezeket a reakciókat befolyásolni vagy támogatni. Összességében a kérdőív átfogóan vizsgálja a válaszadók kiberbiztonsági tudatosságát és technológia elfogadásával kapcsolatos hajlandóságát az elektromobilitási eszközök tekintetében.

4.3 A vizsgálat

4.3.1 A vizsgálat módszertana

A dolgozatban két fő vizsgálati módszert alkalmazok annak érdekében, hogy átfogó képet kapjak az elektromos rollerek kiberbiztonsági aspektusairól. Az egyik vizsgálati módszer a kérdőíves kutatásom statisztikai elemzése. Ez a fázis a kérdőíves kutatás eredményeinek átfogó elemzését és bizonyos adatok összehasonlítását foglalja magában.

Az adatokat különböző statisztikai módszerekkel elemzem, beleértve az egyszerű leíró (deskriptív) statisztikai adatelemzést és az összefüggéseket vizsgáló statisztikai teszteket. Az az adatok kiértékelésre az IBM - Statistical Package for the Social Sciences (továbbiakban: SPSS) szoftvert használom. Az SPSS számos analitikai eszközt kínál az adatok elemzéséhez, amelyeket a dolgozatomban használni fogok többek között például a khi-négyzet próbát, a kereszttábla elemzést, a Kruskal-Wallis elemzést és egyéb statisztikai mutatókat is, mint például a minimum és maximum, illetve átlag mutatók. Ezek az elemzési módszerek és mutatók segítenek az adatok közötti összefüggések és különbségek feltárásában. Összességében tehát a statisztikai elemzési módszerekkel és az SPSS segítségével részletesen megvizsgálom a kérdőíves válaszokat, keresve a válaszok közötti korrelációkat és az esetleges összefüggéseket.

4.3.2 Kérdőíves kutatás eredményei

Demográfiai jellemzők

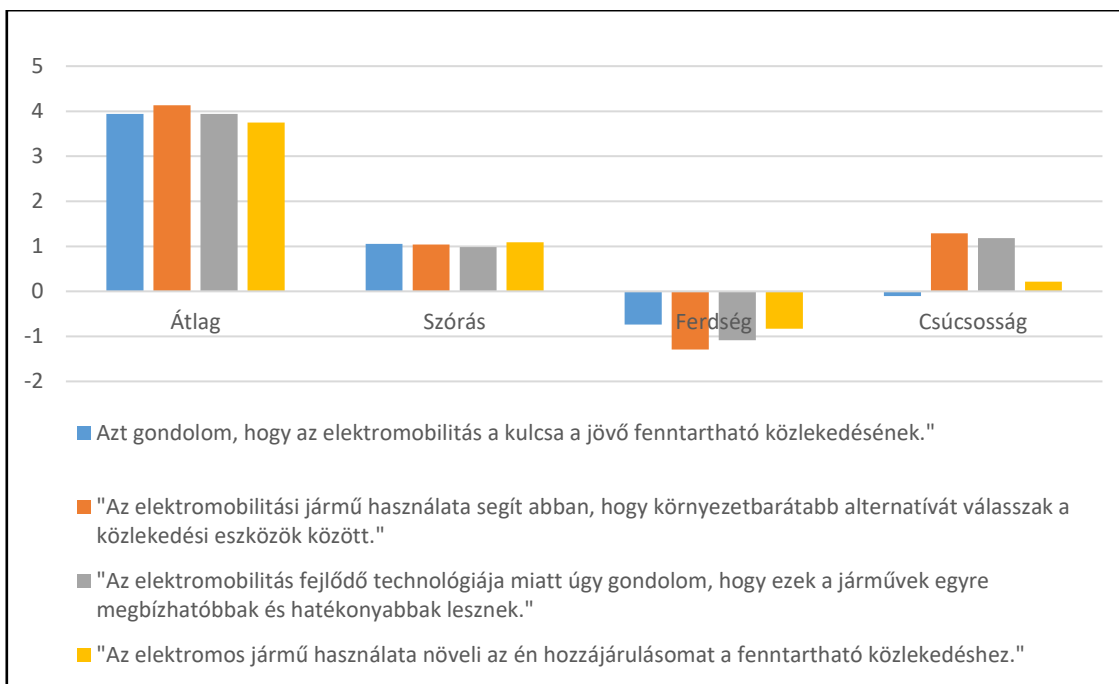
A kérdőíves kutatásban a demográfiai jellemzők felmérésével kapcsolatban felmértem a válaszadók nemi arányát, az életkori eloszlását és a válaszadók legmagasabb iskolai végzettségét. A kérdőívet kitöltő 117 személy 47%-a nő, míg 53%-a férfi volt.

Az életkorra vonatkozóan a válaszadók többsége a 18 és 25 év közötti korosztályba tartozik, ami 46,2%-os részesedést jelent a válaszadók között. Ezután a második legnagyobb arányt a 26 és 39 év közötti korcsoport képviseli 36,8%-os aránnyal. A 40 és 59 év közötti korosztály 15,4%-ot tesz ki a válaszadók közül, míg a 60 év feletti korcsoport mindössze 1,7%-os részesedéssel rendelkezik.

A legmagasabb iskolai végzettségre vonatkozóan a válaszadók legnagyobb része középfokú vagy annál magasabb végzettséggel rendelkezik. A válaszok alapján azok, akik az általános iskola 8. osztályát végezték el, 18,8%-ot tesznek ki. Ezzel szemben 12% a középfokú végzettséggel rendelkezők aránya érettségivel, míg 31,6% azoké, akik középfokú végzettséggel és szakmai végzettséggel rendelkeznek érettségivel. A felsőfokú végzettséggel rendelkezők csoportjában 27,4% azok aránya, akik alapképzés, BA vagy BSc fokozattal rendelkeznek. Ezzel szemben 6,8% azoké, akik mesterképzés, MA vagy MSc fokozattal rendelkeznek, és 1,7% azoké, akik tudományos fokozatot igazoló oklevelet (PhD, DLA) szereztek.

TAP modell leíró elemzése

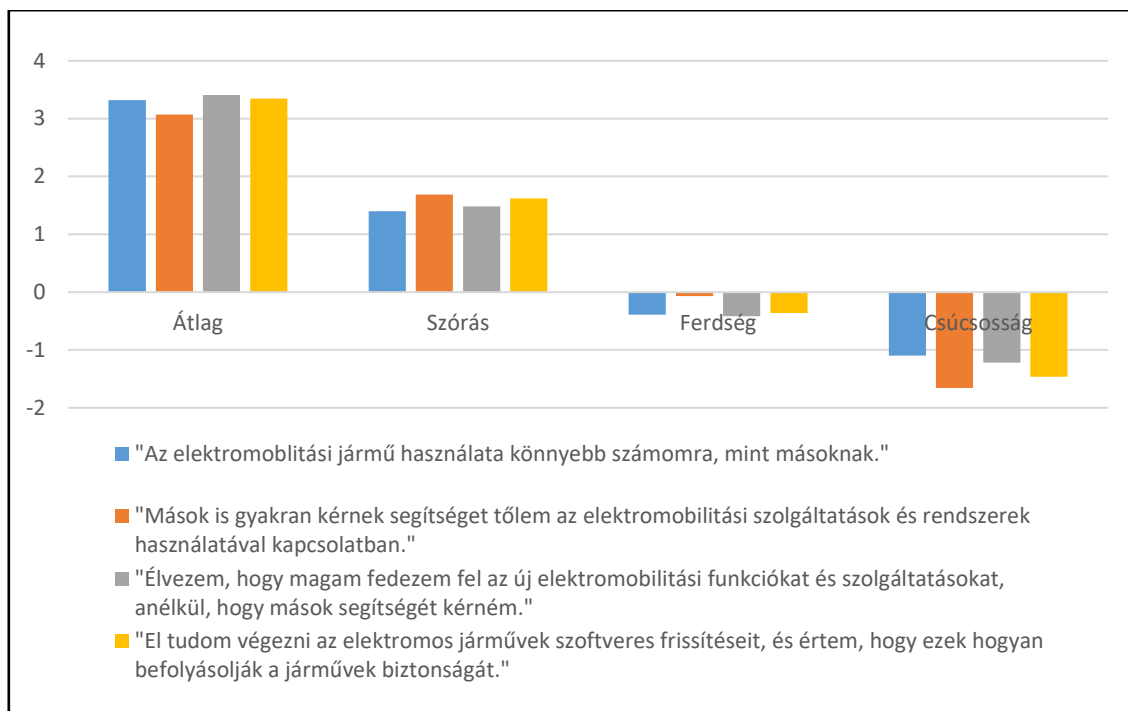
Az elektromobilitás elfogadását vizsgálva az optimizmus, jártasság, függőség és sebezhetőség négy dimenziója mentén fontos megfigyeléseket tehetünk. Az állításokra adott válaszok alapján az alábbi számadatok alapján végeztem leíró elemzést.



**9. ábra: A TAP-modell optimizmusra vonatkozó állításainak elemzése
(saját szerkesztés a kérdőív eredményei alapján)**

Az optimizmusra vonatkozó állítások

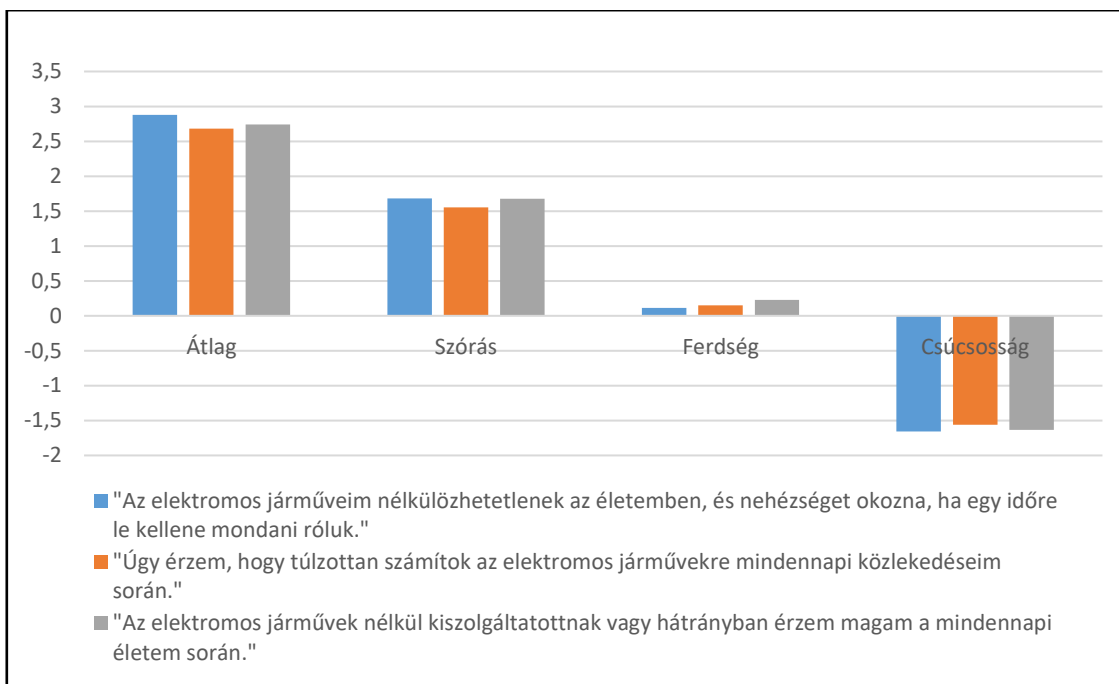
Az optimizmusra vonatkozó állítások esetében az átlagos pontszámok magasak voltak, az átlag értékek 3.75 és 4.13 között mozognak a 5 pontos skálán, ami azt mutatja, hogy a résztvevők pozitívan viszonyulnak az elektromobilitáshoz. Az átlagok közötti kis eltérések a válaszok eloszlását tükrözik, míg a szórás alacsony értékei azt jelzik, hogy a válaszok kevésbé térnek el egymástól. A torzítás és csúcsosság értékek közelítenek a nullához, ami azt sugallja, hogy az eloszlás közel van a normális eloszláshoz, de kissé lefelé görbült.



10. ábra: A TAP-modell jártasságra vonatkozó állításainak elemzése (saját szerkesztés a kérdőív eredményei alapján)

A jártasságra vonatkozó állítások

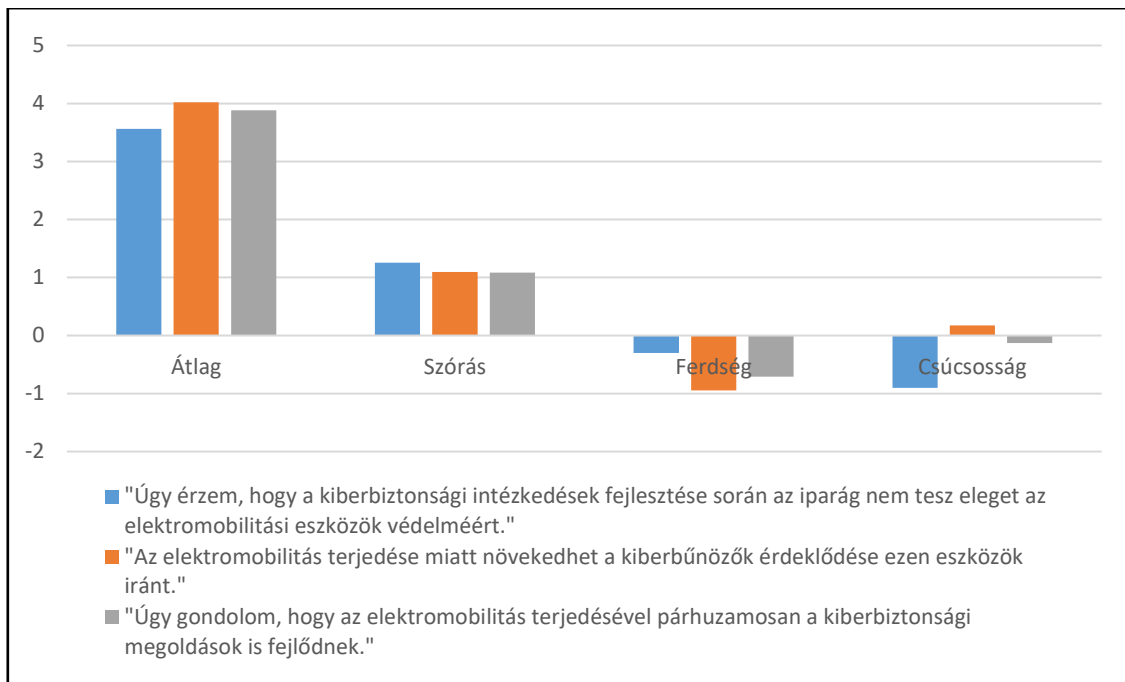
A jártasságra vonatkozó állításoknál az átlag pontszámok változatosabbak 3.07 és 3.41 közötti értékekkel, és a válaszok eloszlása szélesebb skálán mozgott. Magasabb szórás értékek figyelhetők meg, ami azt jelenti, hogy a válaszok nagyobb mértékben térnek el egymástól. A torzítás és a csúcsosság értékek közelítenek a nullához, ami azt sugallja, hogy az eloszlás kissé balra tolódik. Ez alapján arra lehet következtetni, hogy az emberek általánosságban közepesen érzik magukat jártasnak az elektromobilitási szolgáltatások és rendszerek használatában.



11. ábra: A TAP-modell függőségre vonatkozó állításainak elemzése (saját szerkesztés a kérdőív eredményei alapján)

A függőségre vonatkozó állítások

A függőségre vonatkozó állítások esetében az átlagos pontszámok alacsonyabbak voltak az értékek 2.68 és 2.88 között mozognak, ami azt jelzi, hogy az emberek nem érzik magukat túlzottan függőnek az elektromos járművektől mindennapi életük során. Az alacsony átlagok mellett magasabb szórás értékek figyelhetők meg 1.552 és 1.682 között, ami azt mutatja, hogy az emberek válaszai nagyobb mértékben térnek el az átlagtól. A torzítás értékek közelítenek a nullához vagy enyhén negatívak, a csúcsosság értékek pedig negatívak, ami azt jelzi, hogy az eloszlás kissé balra görbült.



12. ábra: A TAP-modell sebezhetőségre vonatkozó állításainak elemzése (saját szerkesztés a kérdőív eredményei alapján)

A sebezhetőségre vonatkozó állítások

Az átlagos pontszámok magasabbak a sebezhetőségre vonatkozó állításoknál, az értékek 3.56 és 4.02 között mozognak, ami azt jelzi, hogy az emberek aggodalmat éreznek a kiberbiztonsági kockázatok miatt. Ezzel igazolva a H2. kutatási hipotézisemet, miszerint az emberek részéről tapasztalható aggodalom az elektromobilitási eszközök kiberbiztonsági kockázatai miatt.

A szórás értékek itt is magasak voltak, ami azt mutatja, hogy a válaszok nagyobb mértékben térnek el az átlagtól. A torzítás és a csúcsosság értékek közelítenek a nullához vagy enyhén negatívak, ami azt jelzi, hogy az eloszlás kissé balra görbült.

Következtetés

Összegezve elmondható, hogy általánosságban pozitívan viszonyulnak az emberek az elektromobilitáshoz és a fenntartható közlekedéshez. Bár magas az optimizmus és a jártasság, közepes szintű a függőség, ugyanakkor magasabb a sebezhetőség érzete a kiberbiztonsági kockázatok miatt. Az eredmények alapján a technológiai fejlődéssel és a biztonsági

intézkedések javításával tovább növelhető lenne az emberek elfogadása az elektromobilitással kapcsolatban.

A nem és a végzettség összefüggése a tudatossággal

A kiértékelés célja az volt, hogy feltárja a résztvevők nemének és a végzettségeknek az összefüggéseit a kiberbiztonsági tudatosság között az elektromobilitási eszközök használatával kapcsolatban. A H4. kutatási hipotézisem vizsgálata érdekében meg keresztábra elemzéssel kiértékeltem, hogy a résztvevők neme összefüggést mutat-e azzal, hogy hallottak-e már arról, hogy az elektromobilitási eszközök használata során a biztonságuk és az adataik veszélyben lehetnek a kiberbiztonsági szempontok miatt, illetve ezt az elemzést végzettem el abban az aspektusban, hogy a tudatosság összefüggést mutat-e azzal, hogy a válaszadó rendelkezik-e legalább felsőfokú végzettséggel.

Nemek összefüggési

A chi-square tesztek és szimmetrikus mértékek elemzése a nem és a kiberbiztonsági veszélyek ismerete közötti kapcsolatot vizsgálta az elektromobilitási eszközök használatával kapcsolatban. Az eredmények azt mutatták, hogy van egy szignifikáns kapcsolat a nem és a kiberbiztonsági veszélyek ismerete között (Pearson Chi-Square: $\chi^2(1) = 5.445$, $p = 0.020$). Ez azt jelzi, hogy valószínűleg a nem befolyásolja az emberek tudását a kiberbiztonsági veszélyekről az elektromobilitási eszközök használata során. A Fisher pontos teszt tovább erősítette ezt az eredményt ($p = 0.027$, kétoldalas; $p = 0.017$, egyoldalas), megerősítve annak valószínűségét, hogy a nem és a kiberbiztonsági veszélyek ismerete közötti kapcsolat valós és szignifikáns.

A szimmetrikus mértékek, mint például a Phi és a Cramer's V is megerősítették a kapcsolatot, közepes erősségű szignifikáns összefüggést mutatva a nem és a kiberbiztonsági veszélyek ismerete között (Phi = 0.216; Cramer's V = 0.216). Ez azt jelzi, hogy a nem befolyásolja az emberek tudását és érzékenységét a kiberbiztonsági kockázatokra az elektromobilitási eszközök használata során, ezzel igazolva a H4. kutatási hipotézisem első részét. Összességében ezek az eredmények alátámasztják, hogy a nem jelentős tényező lehet az egyének kiberbiztonsági tudatosságában az elektromobilitási eszközök használata során.

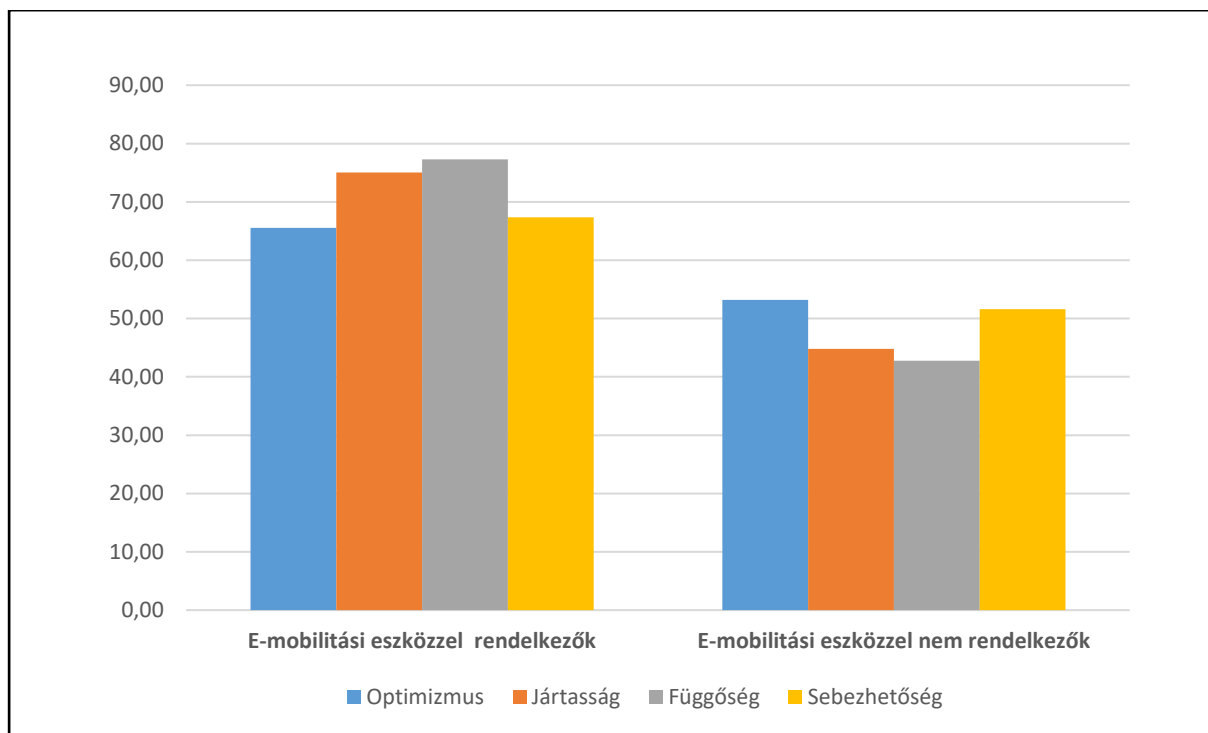
Végzettség összefüggései

Az elemzés során Chi-square tesztek és szimmetrikus mértékeket alkalmaztam annak érdekében, hogy feltárjam a "Van-e legalább felsőfokú végzettsége?" és a "Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során?" változók közötti összefüggést. Ezzel a végzettség és az elektromobilitási eszközök kiberbiztonsági veszélyeiről való tudás közötti lehetséges kapcsolatot vizsgáltam, és a következő eredményeket kaptam.

A Pearson Chi-Square teszt azt mutatta, hogy a két változó közötti kapcsolat nem szignifikáns ($\chi^2 = ,358$, $df = 1$, $p = ,550$). A Fisher's Exact Test eredménye szintén hasonlóan volt nem szignifikáns ($p = ,648$). Ezek az eredmények egyértelműen utalnak arra, hogy nincs szoros összefüggés a legalább felsőfokú végzettséggel rendelkezők köre és a kiberbiztonsági veszélyek ismerete között, ezzel megcáfolva a H4. kutatási hipotézisem második részét. A szimmetrikus mértékek, mint a Phi és Cramer's V, szintén alacsony értékeket mutattak (Phi = ,055; Cramer's V = ,055;) Ezek az értékek is alátámasztják azt a tényt, hogy nincs szignifikáns kapcsolat a vizsgált változók között.

A TAP modell és az e-mobilitási eszközökkel rendelkezők összefüggései

A vizsgált adatok alapján elemzést végeztem az optimizmus, jártasság, függőség és sebezhetőség faktorai mentén az elektromos mobilitási eszközökkel rendelkezők és azok között, akik nem rendelkeznek ilyen eszközzel.



13. ábra: A TAP-modell faktorainak összefüggései az elektromobilitási eszközök birtoklásával (saját szerkesztés a kérdőív eredményei alapján)

Az optimizmus vizsgálata során megállapítható, hogy az elektromobilitási eszközökkel rendelkezők átlagos rangja (68,78) magasabb volt, mint azoké, akik nem rendelkeztek ilyen eszközzel (50,32). A Kruskal-Wallis teszt kimutatta, hogy ebben a dimenzióban szignifikáns különbségek vannak a két csoport között (Chi-square = 9,535, df = 1, p = 0,002). Ezzel igazolva H3. kutatási hipotézisemet, mely szerint az elektromobilitási eszközökkel rendelkezők optimistábbak és pozitívabbak az elektromos mobilitási technológiákat illetően, mint azok, akik nem rendelkeznek ilyen eszközökkel.

A jártasság vizsgálata szintén jelentős különbségeket mutatott. Az elektromobilitási eszközökkel rendelkezők átlagos rangja magasabb volt (71,07) azokhoz képest, akik nem rendelkeztek ilyen eszközzel (48,29). A Kruskal-Wallis teszt eredménye szintén szignifikáns különbségeket mutatott ebben a dimenzióban (Chi-square = 13,816, df = 1, p < 0,001).

A függőség és sebezhetőség dimenzióiban is hasonló eredményeket kaptam. Mindkét esetben az elektromobilitási eszközökkel rendelkezők átlagos rangja magasabb volt, mint azoké, akik nem rendelkeztek ilyen eszközzel (függőség: 78,04 és 42,11; sebezhetőség: 72,56 és 46,97). Mindkét dimenzióban szintén szignifikáns különbségeket találtunk a két csoport között (függőség: Chi-square = 35,468, df = 1, p < 0,001; sebezhetőség: Chi-square = 18,229, df = 1, p < 0,001).

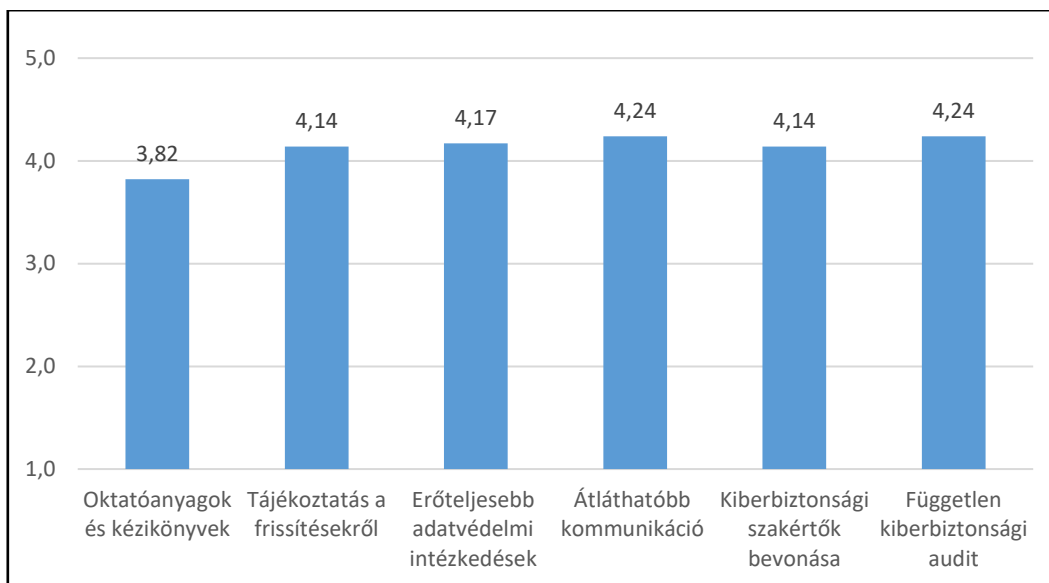
Ezek az eredmények alátámasztják azt a feltevést, hogy az elektromobilitási eszközökkel rendelkezők általában pozitívabb érzelmekkel, magabiztosabb jártassággal, kevésbé függőséggel és kevesebb érzékenységgel rendelkeznek a sebezhetőséggel szemben, ezzel ellentétben azok, akik nem rendelkeznek elektromos mobilitási eszközökkel, általában alacsonyabb rangokat kaptak az optimizmus, jártasság, függőség és sebezhetőség faktoraiban. Ez arra utal, hogy azok akik nem rendelkeznek saját elektromobilitási eszközökkel általában kevésbé pozitívak és magabiztosak az elektromos mobilitási technológiákkal kapcsolatban, valamint nagyobb mértékben érezhetik a függőséget és a sebezhetőséget azok használata során.

Lehetséges megoldásokkal kapcsolatos vizsgálatok

A kérdőíves kutatásomban megfogalmaztam hat lehetséges ajánlást az elektromobilitási eszközök kiberbiztonságának növelése és a kockázatok minimalizálása érdekében. Ezeket az ajánlásokat feltettem állításként a kérdőívet kitöltők részére, hogy milyen mértékben értenek egyet, és hogyan hatnának ezek az intézkedések az elektromobilitási eszközök kiberbiztonságára vonatkozóan. Az állítások sorrendben a következők voltak:

- Javítaná az emberek bizalmát, a részletes felhasználói oktatóanyagok és kézikönyvek készítése.
- Javítaná az emberek bizalmát, a rendszeres tájékoztatás a kiberbiztonsági frissítésekről és intézkedésekről.
- Javítaná az emberek bizalmát, az erőteljesebb adatvédelmi intézkedések bevezetése az eszközök és alkalmazásaik részére.
- Javítaná az emberek bizalmát, az átláthatóbb kommunikáció a gyártók részéről a biztonsági intézkedésekről és fejlesztésekről.
- Javítaná az emberek bizalmát, ha kiberbiztonsági szakértőket vonnak be az eszközök fejlesztésébe és tesztelésébe a megbízhatóság növelése érdekében.
- Javítaná az emberek bizalmát, ha az elektromobilitási eszközök gyártóinak termékei rendszeres független kiberbiztonsági auditokon vennének részt.

Az állításokat egy egytől ötig terjedő skálán értékelhették, amelyen az 1, hogy egyáltalán nem értek egyet, 5 pedig, hogy teljes mértékben egyetértek. A beérkezett válaszok átlagát megvizsgálva a következő diagramot készítettem el.



14. ábra: Megoldási javaslatokra adott válaszok átlaga
(Saját szerkesztés, forrás: kérdőíves vizsgálat eredményei)

Az eredmények alapján megállapítható, hogy a válaszadók egyetértenek az általam megfogalmazott ajánlásokkal kapcsolatban, és úgy vélik, hogy ezek hozzájárulhatnak az emberek bizalmának növeléséhez az elektromobilitási eszközök kiberbiztonsági szempontból. A legmagasabb átlagos pontszámot az állítások közül a "Javítaná az emberek bizalmát, ha az elektromobilitási eszközök gyártóinak termékei rendszeres független kiberbiztonsági auditokon vennének részt." állítás és a "Javítaná az emberek bizalmát az átláthatóbb kommunikáció a gyártók részéről a biztonsági intézkedésekről és fejlesztésekről." állítás kapta, míg a legalacsonyabbat a "Javítaná az emberek bizalmát, a részletes felhasználói oktatóanyagok és kézikönyvek készítése." állítás. Ez számomra érdekes, mert az emberek általában fontosnak tartják a részletes felhasználói oktatóanyagokat és kézikönyveket, mint az eszközök biztonságos és hatékony használatának eszközeit. Véleményem szerint, ez azért lehet, mert a válaszadók úgy gondolták, hogy bár az oktatóanyagok fontosak, azok nem elegendőek önmagukban a bizalom növeléséhez, és más intézkedésekre is szükség van a kiberbiztonság javítása érdekében. Ezért lehet, hogy a válaszadók inkább a konkrét, aktív intézkedéseket preferálták, mint például a szakértők bevonását. Láthatóan a válaszadók általában magasabb pontszámot adtak a proaktív intézkedésekkel kapcsolatos állításoknak, mint az átláthatóság és a felhasználói tájékoztatás terén történő fejlesztéseknek.

KÖVETKEZTETÉSEK

Az elemzések és összehasonlítások alapján megállapítható, hogy az elektromobilitási eszközök elfogadása és a kiberbiztonsági tudatosság szorosan összefügg egymással, ugyanakkor különböző demográfiai tényezők is befolyásolják ezeket a kérdéseket.

Az előbbiek alapján látható, hogy az emberek általánosságban pozitívan viszonyulnak az elektromobilitáshoz és a fenntartható közlekedéshez, azonban magasabb a sebezhetőség érzete a kiberbiztonsági kockázatok miatt. Ez arra utal, hogy bár az emberek látják az elektromobilitás előnyeit, még mindig aggodalmak merülnek fel a technológia biztonsága kapcsán.

Fontos felismerni az adatok alapján, hogy a társadalmi elfogadottság és a kiberbiztonsági tudatosság szorosan összekapcsolódik az elektromobilitási technológiák terén. Az intézkedéseket és a kommunikációt célszerűen kell kialakítani annak érdekében, hogy tovább növeljük az emberek elfogadását és bizalmát ezen a területen, miközben biztosítjuk a megfelelő kiberbiztonságot és tájékoztatást.

5 BIZTONSÁGI VIZSGÁLAT A VALÓSÁGBAN

A második vizsgálati módszer egy gyakorlati biztonsági tesztelést foglal magában, amely során egy valós környezetben tesztelem egy elektromos roller biztonsági mechanizmusait. A vizsgálat során célom megállapítani, hogy egy Bluetooth-os adatkapcsolati rendszeren keresztül lehet-e hozzá lehet-e férni az e-rollerek rendszeréhez, és módosíthatóak-e bizonyos gyárilag beállított biztonsági intézkedések. Az elektromos roller rendszerének biztonsági tesztelése lehetővé teszi számomra, hogy a valós életben megvizsgáljam a biztonsági intézkedések hatékonyságát és a rendszer esetleges sebezhetőségeit. Az ilyen tesztek által nyert eredmények segíthetnek a bemutatni, hogy általam megfogalmazott kiberbiztonsági fenyegetettségek valósak, illetve hogy az esetleges hiányosságokat szükséges azonosítani a szolgáltatóknak és gyártóknak, továbbá, hogy szükséges az elektromobilitási eszközök rendszerének és a hozzájuk társított applikációk továbbfejlesztése a felhasználók biztonságának javítása érdekében.

Ahogy korábban említettem a biztonsági tesztelésem célja, hogy megállapítsam, hogy egy elektromos rolleren vezeték nélküli adatkapcsolati kommunikáción keresztül hozzá lehet-e férni annak rendszeréhez, és módosíthatóak-e bizonyos gyárilag beállított biztonsági intézkedések, adatok.

A tesztelés laboratóriumi környezetén kívül egy valóságos környezetben történik, ahol valódi elektromos rollert használok. A tesztelés során használt elektromos roller egy Xiaomi gyártmányú Mi Essential típusú eszköz. Ennek az elektromos rollernek a főbb jellemzői: 20km-es hatótávval rendelkezik, maximum 20 km/h sebességgel képes haladni. A roller súlya: 12 kg, kerékmérete 8,5 col, és dupla fékrendszerrel (E-ABS és nagy hátsó tárcsafék) szerelt. Az akkumulátor típusa lítium-ion, 3 sebesség móddal rendelkezik gyalogos, normál és sport, a töltési ideje körülbelül 3,5 óra. A hozzárendelt gyártói applikáció a Mi Home, amellyel kezelhető a roller rendszere.

Ebben az alkalmazásban látható minden információ a saját rollerünkkel kapcsolatban, többek között a sorozatszám, a szoftver és hardver információk, illetve a megtett kilométer, akkumulátor töltöttség. Ez az alkalmazás Bluetooth kapcsolaton keresztül kommunikál az elektromos roller vezérlő egységével. Amit még fontos tudni, hogy ebben az alkalmazásban történik - amennyiben rendelkezésre áll újabb - az e-roller szoftverfrissítése, illetve fontos megjegyezni, hogy az adott e-roller típusok mind-mind sajátos funkciókkal rendelkeznek. Ez a konkrét típus egy belépő szériának minősül és a legalapabb funkciókkal rendelkezik, így

például nincsen rajta gyárilag elektronikus sebesség tartó funkció (tempomat). Az alkalmazás Android rendszerű eszközökre a Play Áruházból, IOS rendszerű eszközökre pedig az App Store-ból tölthető le, és az alkalmazáson belül csak az adott e-roller típusra vonatkozó beállítások szerkeszthetők vele, például korábbi szoftverek nem telepíthetők vele, plusz beállítások nem végezhetők el vele, tehát ez alapján zárt rendszerűnek mondható az alkalmazás.

A tesztelés során mindenképpen Android rendszerű eszközt fogok használni, ugyanis azok az alkalmazások amelyekkel megkerülhetők a gyári beállítások, kizárólag a Play Áruházból érhetők el. Ezek úgynevezett „third-party app”-ok, ami azt jelenti, hogy olyan egy harmadik féltől származó alkalmazások, amelyeket nem az e-roller gyártója készített. Nevezetesen van kettő ilyen alkalmazás, amelyet szeretnék bemutatni és használni ennek a folyamatnak a végrehajtására, az egyik ilyen alkalmazás a „ScooterHacking Utility”, a másik pedig az „m365 DownG”.

Minden elektromos rollernek saját vezérlő elektronikája van, és ezzel együtt ún. firmware-je (FW). Röviden ez mondja meg a rollernek, hogyan viselkedjen, milyen teljesítményt adjon le a motor, milyen gyorsan menjen az elektromos roller. Ha ezt az FW-t módosítják, azt nevezzük CFW-nek (custom firmware). A biztonsági tesztelés során használt elektromos rollerre gyári firmware van telepítve. A használt DownG alkalmazás verziószáma 36., a másik általam használt alkalmazás a ScooterHacking Utility verziószáma a 2.3.2.

Fontos megjegyezni, hogy minden e-roller rendelkezik négy olyan rendszerrel, amelyet érintenek ezek az alkalmazások az egyes szoftvermódosítások során.

Az e-ollerek esetében ez a négy rendszer a DRV, ESC, BSM és a BLE. A DRV az elektromos motor vezérlőjére utal, amely felelős az elektromos motor sebességének és irányának szabályozásáért a rollerben. A motorvezérlő szabályozza a motorhoz szállított energiát a roller vezérléseitől származó bemeneti jelek alapján. Az ESC az elektronikus sebességvezérlő rövidítése. Azzal szabályozza az elektromos motor sebességét, hogy szabályozza az ahhoz szállított energia mennyiségét. Értelmezi a roller vezérléseitől származó jeleket, és ennek megfelelően szabályozza a motor sebességét. A BSM az akkumulátorkezelő rendszer rövidítése, ami felelős a roller akkumulátorának kezeléséért, ideértve annak állapotának figyelését, a cellák kiegyenlítését és a túltöltés vagy túlmerülés elleni védelmet. A BMS szinte minden elektronikus eszközben megtalálható, sokféle szerepet játszik az e-ollereken belül. Ez

egy beépített rendszer, amely figyeli az akkumulátort és annak egyes akkumulátorcelláit, hogy diagnosztizálja, korrigálja és optimalizálja a járművet. Ezeket az adatokat a BMS folyamatosan gyűjti a zökkenőmentes működés és az optimalizált energiafogyasztás biztosítása érdekében. A BLE az angol "Bluetooth Low Energy" rövidítése. Az elektromos roller esetében ez a roller Bluetooth kapcsolatára utal, ami lehetővé teszi annak kommunikációját egy mobilalkalmazással vagy más eszközökkel. A BLE funkciók közé tartozhatnak a roller zárásának/nyitásának vezérlése, beállítások módosítása, a roller helyzetének nyomon követése és a diagnosztikai adatok biztosítása. Ennek a segítségével működik a gyártó által biztosított dedikált alkalmazás is, továbbá ez az a rendszer, amire elsődlegesen hatnak a fenti Play Áruházból letölthető alkalmazások.

Az elektromos rollerek, ahogy korábban említettem Bluetooth kapcsolaton keresztül kommunikálnak a külső eszközökön lévő alkalmazásokkal. A biztonsági tesztben érintett Xiaomi elektromos roller is a gyártó által fejlesztett MiHome alkalmazáson keresztül vezérelhető.

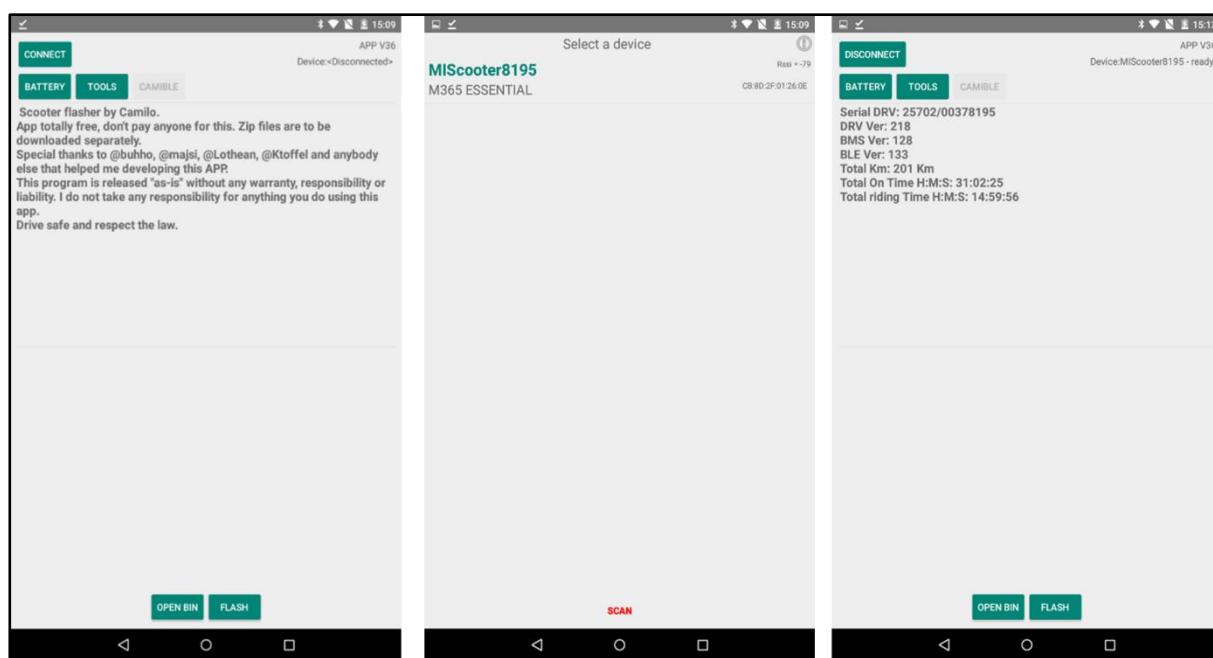
Fontos megjegyezni, hogy ezen a gyári applikáción van egy olyan lehetőség, hogy a saját e-rollerünket, amikor összekapcsoljuk Bluetooth-on keresztül, akkor elektronikusan le lehet zárni, majd azt fel lehet oldani a további használat érdekében. Amikor a roller elektronikusan lezárásra kerül, akkor az egyetlen rajta található funkció gombbal, kizárólag a lámpát lehet be és kikapcsolni, minden más funkció ilyenkor letiltásra kerül, a roller kijelzőjén kizárólag egy lakat szimbólum és amíg a Bluetooth eszközzel kapcsolatban van, addig egy Bluetooth szimbólum látható. Továbbá fontos, hogy az elektronikus lezárást követően a roller további mozgásra képes, azonban az elektromotor folyamatosan fékezi az első kerekét a rollernek. Az e-roller nyitásának és zárásának jelentősége lesz a teszt során.

5.1 Teszt végrehajtása

Az első teszt során azt az élethelyzetet szeretném bemutatni, amikor nem használom a MiHome alkalmazást és ezáltal nem is zárom le az elektromos rollert elektronikusan. Ebben az esetben a teszt célja a rollerre telepített firmware felülírásra egy olyan custom firmware-el, amelyen a gyári biztonsági intézkedések már felülírásra kerültek, így például a maximális sebesség 30 km/h-ra került beállításra, előtte nem rendelkezett elektronikus sebességtartó funkcióval, ez is beállításra került a CFW-ben, illetve az elektromotor indítási sebessége is csökkentésére került.

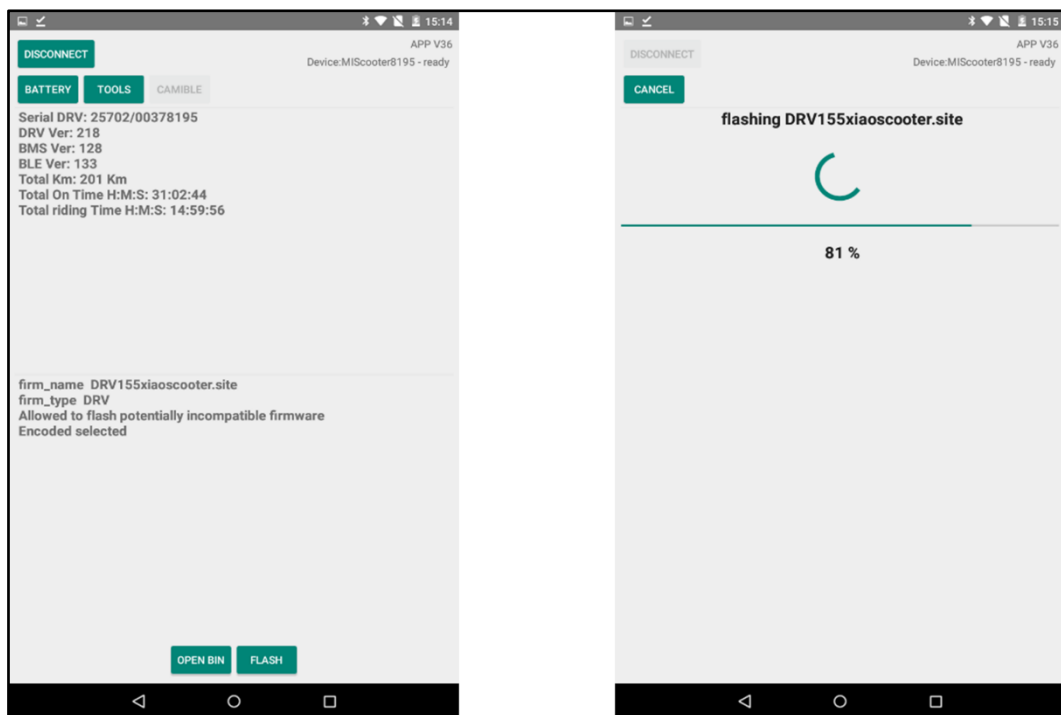
Ennek a CFW-nek az e-rollerre történő telepítésre a DownG alkalmazást fogom használni. Az alkalmazás megnyitása során a következő kezdőképernyő fogadja a felhasználót. Ez a kezdőfelület, ahol négy funkció gombot találhatunk, nekünk a kívánt művelet végrehajtásához először csatlakoztatni kell az elektromos rollert. A „Connect” gombbal átjutunk egy új felületre, ahol kiválaszthatjuk a módosítani kívánt e-rollert. Itt minden olyan e-roller megjelenik amelyik be van kapcsolva és az Andorid-os eszközöm Bluetooth hatótávjában észlelhető.

Miután a módosítani kívánt e-roller megjelenik a listában és kiválasztjuk, akkor egy új felületre kerülünk. Itt már láthatunk minden fontos információt a saját e-rollerünkről. Többek között látható az e-rollerünk széria száma, és a rajta található DRV, BMS, BLE verziószámokat, illetve az összes megtett utat kilométerben és időben is, azonban ez nem releváns a teszt szempontjából. Ami a teszt szempontjából fontos az az e-rolleren található DRV verziószám, amely jelen esetben 2.1.8. Ez a verziószám fog vélhetően módosulni az általam generált CFW verziószámára, ha sikeres lesz a teszt.



15. ábra: Az e-roller felfedezésének, kiválasztásának folyamata
(Saját felvételek, forrás: DownG alkalmazás)

A következő lépésben megnyitásra került a CFW az „OPEN BIN” gombbal, majd ezt követően ha betöltésre került a CFW a programba, akkor a „FLASH” gombbal elindítva megindul a felülírási folyamat.



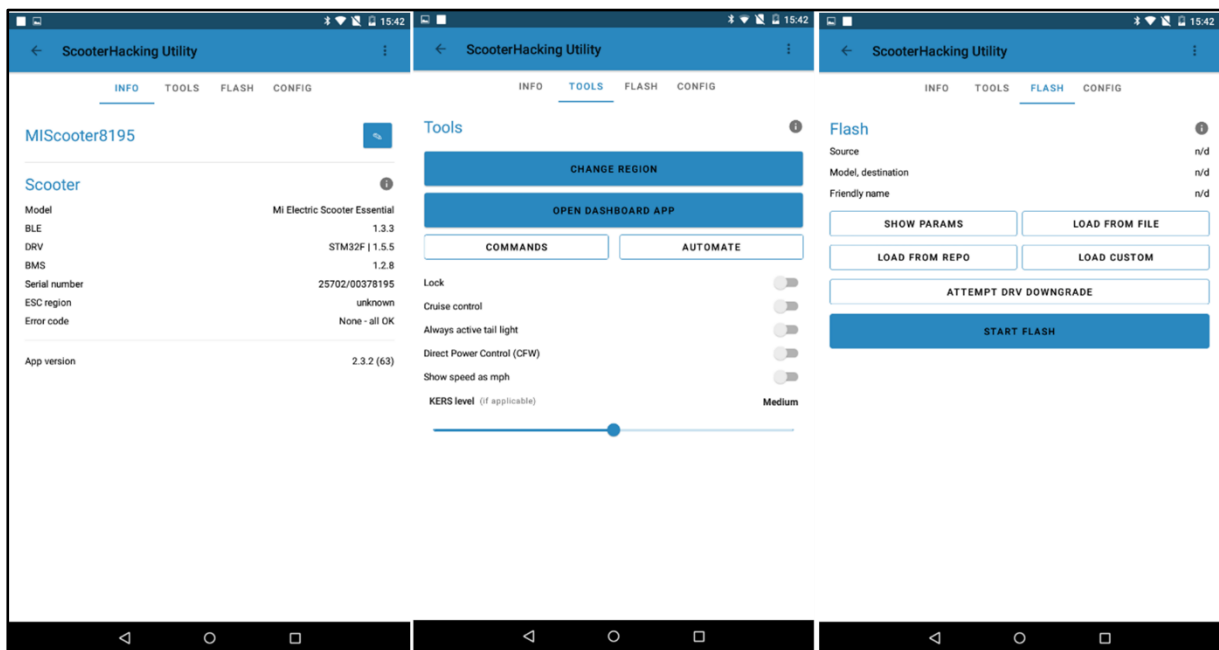
16. ábra: A CFW felülírásának folyamata
(Saját felvételek, forrás: DownG alkalmazás)

A folyamat nagyjából 1-2 percet vesz igénybe és egy százalékos folyamatjelző időközben az aktuális állapotról tájékoztat. Ennek a folyamatnak a során mindent meg kell tenni annak érdekében, hogy az e-roller Bluetooth hatótávon belül maradjon és ne kapcsoljon ki. A folyamat végét követően, amennyiben sikeres a felülírás, akkor a következő felület fogadja a felhasználót, amelyen látható, hogy az általam használt e-roller DRV verziószáma módosult 1.5.5.-re.



17. ábra: A módosult DRV számmal rendelkező e-roller
(Saját felvétel, forrás: DownG alkalmazás)

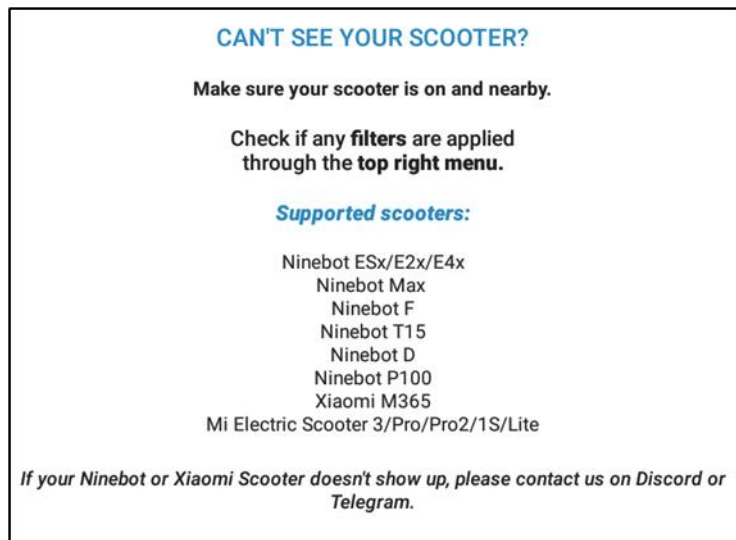
A felülírást követően megállapítottam, hogy az e-roller az általam generált CFW-vel hibakód nélkül működött tovább, és az eddig tempomattal nem rendelkező e-roller már ilyen funkcióval is rendelkezett, a maximális sebessége módosult 30 km/h-ra és az elektromotor indító sebessége is módosult a felülírással, amely összesen kettő percig tartott a DownG alkalmazás a használatával.



18. ábra: ScooterHacking Utility alkalmazás kezelőfelülete

(Saját felvételek, forrás: ScooterHacking Utility alkalmazás)

A fenti képeken szeretném bemutatni a ScooterHacking Utility alkalmazás kezelőfelületét, amelyet szintén az általam használt e-rollerrel kapcsolatam össze. Megállapítható, hogy ez az alkalmazás már sokkal több lehetőséget kínál az e-rollerrel kapcsolatos módosítások végrehajtásához. Fontos megjegyezni, hogy ez az alkalmazás már nem csak kizárólag Xiaomi e-rollerekkel kompatibilis. Az következő ábrán felsorolt e-roller típusok rendszerébe, hasonlóan könnyedén be lehet jutni ennek segítségével.



19. ábra: ScooterHacking Utility által támogatott e-rollerek
(Saját felvétel, forrás: ScooterHacking Utilitiy alkalmazás)

5.2 További tesztek végrehajtása

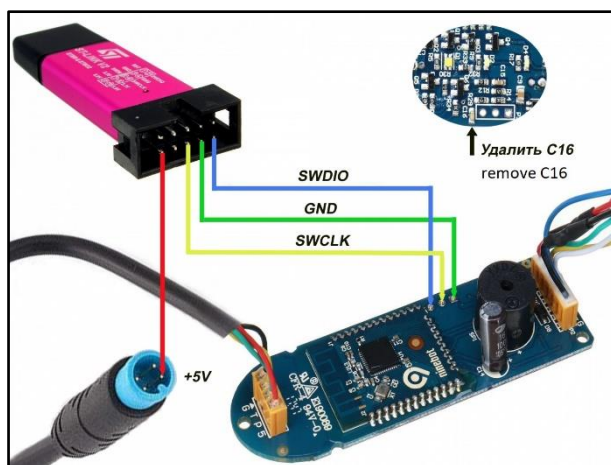
Az első tesztet követően azt vizsgáltam meg, hogy amennyiben egy e-roller a korábban ismertetett módon Bluetooth-al lezárásra kerül - ami a valóságban egy gyakran előforduló élethelyzet, hogy valaki elektromosan lezárja az e-rollerét, és amíg nem használja, addig elmegy annak közvetlen környezetéből - , akkor hogyan reagál egy ilyen alkalmazásra.

Az első esetben úgy hajtottam végre, hogy az az eszköz, amelyről lezártam az e-rollert a MiHome alkalmazással, ott maradt a roller Bluetooth hatótávolságán belül, és így folyamatos kapcsolat volt az eszköz és az e-roller között. Ebben az esetben az Androidos eszközre telepített alkalmazások egyikével sem lehetett észlelni az e-rollert. Tehát ebben az esetben az e-roller gyakorlatilag védett maradt és ez idő alatt, amíg egy másik Bluetooth kapcsolat aktív volt, akkor nem lehetett rajta végrehajtani változtatásokat.

A második esetben azonban a tesztet úgy hajtottam végre, hogy az az eszköz, amelyről a rollert lezártam a MiHome alkalmazással már a Bluetooth hatótávolságon kívül legyen, és ebben az esetben az e-roller kijelzőjén kizárólag egy lakat szimbólum jelenik meg. Ekkor az Androidos készülékre telepített alkalmazással azonnal észlelhetővé vált az e-roller, pedig az elektromos zárolás még mindig aktív volt. Azon felül, hogy az e-roller észlelhető volt, sikerült is bejutni az annak vezérlő rendszerébe és a zárolást feloldani a ScooterHacking Utility alkalmazással és képes lettem módosításokat végrehajtani az e-rolleren, akár tudtam csökkenteni a elektromotor

fékhátását, az indítási sebességet, a maximális sebességet, az elektromotor rendszer feszültségét, akár másik régióba regisztrálhattam az e-rollert stb. Tehát megállapítható, hogy amint nincsen élő Bluetooth kapcsolat az e-roller és egy másik eszköz között, akkor annak rendszerébe könnyedén be lehet jutni és azon belül változtatásokat végrehajtani.

További kutatásokat hajtottam végre különböző internetes forrásokon, amely alapján megállapítható, hogy a gyártó ezt a problémát már felismerte és ezért az újabb e-roller szériákat már egy frissített BLE verzióval adja ki és az 1.5.7. verziószámában már blokkolja a vezérlőegység a feloldási lehetőségeket, azonban további kutatásokkal megállapítottam, hogy ennek a védelmi intézkedésnek a megkerülésére már kettő módszer is létezik. Az egyik módszer alapja, hogy már árulnak külön megvásárolható utángyártott e-roller alaplaponkat, amelyeket beleépítve az e-rollerbe lehetőség nyílik annak szoftveres módosítására. A másik módszer lényege pedig, az úgynevezett ST-Link V2 használata, amely egy programozó eszköz, USB modul az STM32 és STM8 processzorcsalád programozásához⁵², és ennek használatával az elektromos roller BLE modulját tudják programozni.



20. ábra: ST-Link V2 összekötése a Xiaomi e-roller vezérlőegységével
(Forrás: TavIR⁵³)

⁵² „ST-Link V2 (STM8/STM32) programozó-debugger”, TavIR WebShop, 2023. szeptember 16., <https://shop.tavir.hu/termek/shop/kiegeszitok/programozo-avr-esp-stm32/st-link-v2-stm8-stm32-programozo-debugger/>.

⁵³ „Recovering a Xiaomi M365 with an ST-Link dongle”, 2019. október 27., <http://nelsonware.com/blog/2019/10/27/recovering-a-xiaomi-m365-with-an-st-link-dongle.html>.

KÖVETKEZTETÉSEK

Összegezve az elvégzett kutatás célja az volt, hogy feltárja az elektromos rollerek Bluetooth kapcsolaton keresztüli hozzáférhetőségének és manipulálhatóságának kiberbiztonsági fenyegetettségei. A kutatás során a gyakorlat biztonsági vizsgálattal igyekeztem szemléletesen bemutatni, hogy mennyire egyszerű az elektromos rollerek rendszerébe való belépés és annak rendszerében történő módosítások végrehajtása

Az eredmények alapján megállapítható, hogy a könnyű hozzáférhetőség súlyos kockázatokat jelent mind a kiberbiztonság, mind a közlekedésbiztonság, mind pedig az adatvédelem terén. A kiberbiztonsági szempontból az elektromos rollerek rendszereinek sérülékenysége lehetővé teszi a távoli vezérlést és a rendszerben tárolt adatokhoz történő hozzáférést, azok módosítását. Ez pedig potenciálisan komoly veszélyeket rejthet magában a felhasználók és a közlekedés résztvevői számára. Közlekedésbiztonsági aspektusból nézve az e-roller rendszerének manipulálhatósága könnyedén vezethet balesetekhez mind az e-roller vezetője, mind pedig más közlekedők számára. Ezáltal az ilyen típusú járművek veszélyessé válhatnak akár a közutakon, akár a gyalogos területeken egyaránt.

Végül úgy gondolom, hogy adatvédelmi szempontból is kiemelt figyelmet kell fordítani az elektromos rollerek rendszerének védelmére. Az elektromos rollerek vezérlőegységének manipulálása lehetővé teszi a rendszerfájlokhoz, a rendszerben tárolt adatokhoz való egyszerű hozzáférést, így például lehetőség nyílik személyes adatok, geolokációs adatok, útvonalak, vagy akár az eszköz használatára vonatkozó információk megismerésére, illetéktelen felhasználására.

ÖSSZEGZETT KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

Dolgozatom célkitűzése az volt, hogy feltárja a mindennapi közlekedésben megjelenő elektromobilitási eszközök kiberbiztonsági vonatkozásait, azonosítva a lehetséges kockázatokat és veszélyforrásokat, illetve, hogy ezzel összhangban feltárjam és megvizsgáljam a felhasználók és az elektromos járművek kiberbiztonsága közötti összefüggéseket. Az eredmények alapján számos ajánlás adható mind a felhasználók, mind a gyártók, felhasználók, vagy akár a fejlesztők számára. Úgy gondolom, hogy a felhasználók részére szükséges lenne további oktatási és tájékoztató kampányokat szervezni az eszközök szoftver és hardver-illesztőprogramjainak fontosságáról és a rendszeres frissítések szükségességéről. Ez növelhetné az emberek tudatosságát és hajlandóságát a kiberbiztonsági intézkedésekkel kapcsolatban, ami hozzájárulhatna az elektromobilitási eszközök biztonságosabb használatához.

Azonban ezen eredmények alapján hangsúlyozni kell a gyártók, fejlesztők és szabályozók felelősségét is a rendszerek biztonságának növelése és a kockázatok minimalizálása érdekében. A rendszeres biztonsági frissítések és a szigorúbb ellenőrzési mechanizmusok bevezetése elengedhetetlen az elektromobilitási eszközök biztonságának biztosítása érdekében. Lehetséges megoldási javaslatként merül fel, hogy a gyártók lehetőséget biztosítsanak a felhasználók számára a kétlépcsős hitelesítés alkalmazására az e-rollerekhez való hozzáférés során. Ez azt jelentené, hogy a felhasználóknak nemcsak a jelszavukkal kellene bejelentkezniük az alkalmazásba vagy az e-rollerek vezérlőfelületére, hanem egy második, például SMS-ben küldött vagy autentikációs alkalmazáson keresztül generált kód megadásával is megerősíteniük kellene az azonosításukat. Ezáltal még nehezebbé válna az illetéktelen hozzáférés, még akkor is, ha az egyik azonosítási tényezőt valakinek sikerülne megszereznie.

Úgy gondolom, hogy a fentiekben megfogalmazott ajánlások hatékony segítséget nyújthatnak a kiberbiztonság növelésében az elektromobilitás területén. Fontos felismerni és kezelni a kiberbiztonsági kihívásokat az e-rollerek és többi elektromos közlekedési eszközök esetében is. Az adatvédelmi intézkedések erősítése, a kiberbiztonsági szakértők bevonása és a rendszeres auditok lehetőséget teremtenek az emberek bizalmának növelésére és az eszközök biztonságának javítására. Továbbá, a felhasználók és a gyártók közötti együttműködés és felelősségvállalás elengedhetetlen az innováció és a biztonság egyensúlyának fenntartása érdekében.

KUTATÁSI EREDMÉNYEK

Kutatásom során az alábbi eredményeket fogalmaztam meg:

T1: Az elemzéssel igazoltam, hogy az elektromobilitási eszközök rendszerében számos sebezhetőségi pont van.

T2: Igazoltam, hogy az emberekben valóban aggodalom van jelen az elektromobilitási eszközök kiberbiztonsági kockázataival kapcsolatban.

T3: Megállapítottam, hogy az elektromobilitási eszközökkel rendelkezők körében valóban optimistább és pozitívabb attitűd tapasztalható az elektromos mobilitási technológiákkal kapcsolatban, mint azoknál, akik nem rendelkeznek ilyen eszközökkel.

T4: Az elektromobilitási eszközökkel kapcsolatos kiberbiztonsági tudatosságban a nem és az iskolai végzettség csak részben bizonyultak befolyásoló tényezőnek, ugyanis az iskolai végzettség igen, míg a végzettség nem bír befolyással.

T5: Megállapítottam, hogy a kiberbiztonság valóban jelentőséggel bír a járműgyártás, fejlesztés és szabályozás területén.

Ezen eredmények alapján megerősíthetjük, hogy az elektromobilitási eszközök kiberbiztonsági kérdései komoly figyelmet igényelnek mind a felhasználók, mind a gyártók, mind pedig a szabályozó hatóságok részéről. Az elektromos járművek és azokhoz kapcsolódó szoftverek sebezhetőségeinek azonosítása és az ezekből eredő kockázatok kezelése kiemelkedő fontosságúak a felhasználók és az egész közlekedési infrastruktúra biztonságának szempontjából. A megvizsgált eredmények alapján megállapítást nyert a dolgozatban, hogy a kiberbiztonsági fenyegetettségeknek a felhasználói élményre és bizalomra gyakorolt hatása jelentős. Az effajta fenyegetettségek csökkenthetik a felhasználók bizalmát az elektromos járművek iránt, és negatívan befolyásolhatják a döntésüket az ilyen eszközök használatáról vagy vásárlásáról. Ez pedig jelentős akadályt jelenthet az e-mobilitás terjedése szempontjából, ezzel együtt pedig az okos városok és az autonóm közlekedés fejlődése is lelassulhat.

Bár a téma sokoldalúsága, a digitális tér folyamatos fejlődése és az elektromobilitás térnyerése új kihívásokat és veszélyeket vet fel a kiberbiztonság terén, úgy gondolom és remélem, hogy a dolgozatom és az elvégzett kutatásom egy összegző jellegű iránymutatást adhat ebben a

kérdéskörben. Pontosan ezért szeretnék további jövőbeli kutatásokat is végezni, amelyek célja a jövőben kialakult kiberbiztonsági intézkedések, továbbá a megalkotott jogszabályok hatásainak a vizsgálata az elektromobilitás tekintetében.

Összességében a kiberbiztonsági kockázatok és az elektromobilitási járművek közötti összefüggés vizsgálata egy kiemelten fontos lépés volt a jövőbiztos mobilitás felé vezető úton. A dolgozatban az általam megfogalmazott javaslatokkal és a jövőben egy megfelelő szabályozási keret kialakításával, továbbá a kiberbiztonsági szakemberek bevonása a gyártók, a fejlesztők, illetve a szolgáltatók körébe nagymértékben segíthet abban, hogy az elektromobilitási járművek és azok felhasználói biztonságosabb környezetben vehessék igénybe ezeket az innovatív közlekedési eszközöket, ezzel hozzájárulva: egy fenntartható, biztonságos és technológiailag fejlett közlekedési jövőért.

IRODALOMJEGYZÉK

- 1/1975. (II. 5.) KPM–BM együttes rendelet a közúti közlekedés szabályairól
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- ACEA - European Automobile Manufacturers' Association. „ACEA Principles of Automobile Cybersecurity”, 2017. október 18. <https://www.acea.auto/publication/acea-principles-of-automobile-cybersecurity/>.
- Argyropoulos Nikolaos, Pouria Sayyad Khodashenas, Orestis Mavropoulos, Eirini Karapistoli, Anastasios Lytos, Paris Alexandros Karypidis, és Klaus-Peter Hofmann. „Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARMEL”. *Transportation Research Procedia*, 23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus, 52 (2021. január 1.): 307–14. <https://doi.org/10.1016/j.trpro.2021.01.036>.
- Bányász Péter, Bóta Bettina, és Zágón Csaba. „A Social Engineering Jelentette Veszélyek Napjainkban”, 12–37. Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. <https://doi.org/10.37372/mrttvpt.2019.1.1>.
- Berényi László, és Deutsch Nikolett. „Technology Adoption among Higher Education Students”. *Vezetéstudomány / Budapest Management Review*, 2023. november 13., 28–39. <https://doi.org/10.14267/VEZTUD.2023.11.03>.
- Bodó Attila Pál, Cser Orsolya Anikó, Gyaraki Réka Eszter, Kaczur Gábor, Lattmann Tamás, Solymos Ákos, Szabó Zsolt Mihály, Tikos Anita, Váczi Dániel, és Zámbó Nóra. *Célzott kibertámadások - Éves továbbképzés az elektronikus információs rendszer biztonságért felelős személy számára*. Nemzeti Közszerológati Egyetem, 2022. <https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/18055>.
- Pásztor Csaba. „Egyre magabiztosabban és többen villanyautóznak Magyarországon”, 2023. augusztus 2. <https://totalcar.hu/magazin/hirek/2023/08/02/egyre-magabiztosabban-es-tobben-villanyautoznak-magyarorszagon/>.
- Dub Máté. „A social engineering támadások megelőzésének lehetőségei”. *Hadmérnök* 16, sz. 3 (2021. november 25.): 173–87. <https://doi.org/10.32567/hm.2021.3.10>.
- „ENISA good practices for security of Smart Cars — ENISA”. Elérés 2024. április 8. <https://www.enisa.europa.eu/publications/smart-cars>.
- Dr. Irk Ferenc, Klobusitzky György, Dr. Major Róbert, és Dr. Varga Ádám. *Közlekedésrendészeti Alapismeretek*. Egyetemi jegyzet. Budapest, 2013.

- Katona Gergő. „Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése 1. rész”. *Hadmérnök* 18, sz. 3 (2023): 161–76. <https://doi.org/10.32567/hm.2023.3.11>.
- Guenther M. „Social Engineering”. *Social Engineering Security Awareness Series*, 2001.
- Guide Proceedings. „Proceedings of the 25th USENIX Conference on Security Symposium”. Elérés 2024. április 8. <https://dl.acm.org/doi/proceedings/10.5555/3241094>.
- Jonathan Ho. „5 Luxurious Designer Electric Bicycles”. LUXUO, 2017. június 19. <https://www.luxuo.com/cars/5-luxurious-designer-electric-bicycles.html>.
- Jain Anushtha. „ISO 21434: Meghatározás, megfelelőség, eszközök és tanúsítványok”. *Visure Solutions* (blog). Elérés 2024. április 8. <https://visuresolutions.com/hu/blog/aut%C3%B3ipari/iso-21434/>.
- Katona Gergő. „Autonóm járművek kiberbiztonsági kihívásai (2. rész)”. Ludovika.hu, 2022. január 20. <https://www.ludovika.hu/blogok/cyberblog/2022/01/20/autonom-jarmuvek-kiberbiztonsagi-kihivasai-2-resz/>.
- Kim Kyounggon, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, és Huy Kang Kim. „Cybersecurity for autonomous vehicles: Review of attacks and defense”. *Computers & Security* 103 (2021. április 1.): 102150. <https://doi.org/10.1016/j.cose.2020.102150>.
- Magyar Autóklub. „Minden, amit az alternatív közlekedési eszközökről tudni érdemes”. Elérés 2024. április 8. <https://www.autoklub.hu/minden-amit-az-alternativ-kozlekedesi-eszkozokrol-tudni-erdemes/>.
- Mandal Sujoy. „Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region”. *Advances in Space Research*, 2018. január 1. https://www.academia.edu/88455421/Augmentation_of_GNSS_utility_by_IRNSS_NavIC_constellation_over_the_Indian_region.
- Marko Wolf, Christof Paar, és André Weimerskirch. „Security in automotive bus systems”. *Proceedings of the Workshop on Embedded Security in Cars*, 2004.
- Mouton Francois, Louise Leenen, és H. S. Venter. „Social engineering attack examples, templates and scenarios”. *Computers & Security* 59 (2016. június 1.): 186–209. <https://doi.org/10.1016/j.cose.2016.03.004>.
- Muha Lajos és Krasznay Csaba. „Az elektronikus információs rendszerek biztonságáról vezetőknek”. *NKE*, 2018.
- Pethő Zsombor, Szalay Zsolt, és Török Árpád. „Safety risk focused analysis of V2V communication especially considering cyberattack sensitive network performance and

- vehicle dynamics factors”. *Vehicular Communications* 37 (2022. július 1.): 100514.
<https://doi.org/10.1016/j.vehcom.2022.100514>.
- Now Publishers. „Artificial Intelligence-Based Cybersecurity for Connected and Automated Vehicles”, 2022.12.29.
<https://www.nowpublishers.com/article/BookDetails/9781638280606>.
- Nelsonware. „Recovering a Xiaomi M365 with an ST-Link dongle”, 2019. október 27.
<http://nelsonware.com/blog/2019/10/27/recovering-a-xiaomi-m365-with-an-st-link-dongle.html>.
- ROBOTS: Your Guide to the World of Robotics. „Segway”. Elérés 2024. április 8.
<https://robotsguide.com/robots/segway>.
- Help Net Security. „Consumers Worry about the Cybersecurity of Connected Vehicles”. *Help Net Security* (blog), 2021. április 16.
<https://www.helpnetsecurity.com/2021/04/16/cybersecurity-connected-vehicles/>.
- SIP-Scootershop. „Hoverboard IO HAWK CROSS 2.0”. Elérés 2024. április 8.
https://www.sip-scootershop.com/hu/product/hoverboard-io-hawk-cross-20_E10020CS.
- Spiceworks Community. „Automotive Cybersecurity: Is Your Vehicle Safe From a Hack? - Security”, 2016. augusztus 10. <https://community.spiceworks.com/t/automotive-cybersecurity-is-your-vehicle-safe-from-a-hack/517370>.
- Ször Péter. *A vírusvédelem művészete*. Bicske: SZAK Kiadó, 2010.
- Fleischer Tamás. „Innovációk a közlekedésben: külföldi példák, hazai tanulságok”, 2008.
- TavIR WebShop. „ST-Link V2 (STM8/STM32) programozó-debugger”, 2023. szeptember 16.
<https://shop.tavir.hu/termek/shop/kiegeszitok/programozo-avr-esp-stm32/st-link-v2-stm8-stm32-programozo-debugger/>.
- „Technikatörténeti szemle 22. (1996) | Könyvtár | Hungaricana”. Elérés 2024. április 8.
https://library.hungaricana.hu/hu/view/ORSZ_KOZL_TechTortSzle_22/?pg=108&layout=s.
- Toth Andras. „Information security for electric cars in accordance with nist critical infrastructure cybersecurity framework”, 2017. január 1.
- UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387]. Elérés 2024. április 8. <https://eur-lex.europa.eu/eli/reg/2021/387/oj>.

- Vaidya Binod, és H.T. Mouftah. „Cyber Security Considerations for Automated Electro-Mobility Services in Smart Cities”, 457–73, 2020. <https://doi.org/10.1201/9780429329401-17>.
- Vinayaga-Sureshkanth Nisha, Raveen Wijewickrama, Anindya Maiti, és Murtuza Jadliwala. „Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems”. In *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, 31–35. New Orleans LA USA: ACM, 2020. <https://doi.org/10.1145/3375706.3380559>.
- Voltride. „InMotion V12HT – elektromos egykerekű készleten”. Elérés 2024. április 8. <https://www.voltride.hu/hu/egyeb-elektromos-jarmuvek/egykerekekuek/inmotion-v12ht>.
- Wiley.com. „CEH v9: Certified Ethical Hacker Version 9 Study Guide | Wiley”. Elérés 2024. április 8. <https://www.wiley.com/en-br/CEH+v9%3A+Certified+Ethical+Hacker+Version+9+Study+Guide-p-9781119419303>.
- Wiley.com. „The Art of Deception: Controlling the Human Element of Security | Wiley”. Elérés 2024. április 8. <https://www.wiley.com/en-us/The+Art+of+Deception%3A+Controlling+the+Human+Element+of+Security-p-9780471237129>.
- Xu Chuyuan. „Research on Range Extended Electric Vehicle Based on Cruise”. *Journal of Physics: Conference Series* 2479, sz. 1 (2023. április 1.): 012012. <https://doi.org/10.1088/1742-6596/2479/1/012012>.
- Tóth Z. „The electric vehicle penetration in Hungary.” *International Journal of Engineering and Management Sciences Vol. 2.*, sz. No. 4. (2017). <https://doi.org/10.21791>.

ÁBRAJEGYZÉK

1. ábra: A kiberbiztonság és a közlekedési innovációk összefüggései	12
2. ábra: Elektromobilitási eszközök típusai.....	22
3. ábra: E-bikehoz tartozó okosberendezés	23
4. ábra: Elektromos unickli	25
5. ábra: Segway	26
6. ábra: Hoverboard.....	27
7. ábra: Egy IT támadás felépítése	32
8. ábra: Lehetséges támadási pontok egy jármű tekintetben.....	38
9. ábra: A TAP-modell optimizmusra vonatkozó állításainak elemzése	49
10. ábra: A TAP-modell jártasságra vonatkozó állításainak elemzése	50
11. ábra: A TAP-modell függőségre vonatkozó állításainak elemzése.....	51
12. ábra: A TAP-modell sebezhetőségre vonatkozó állításainak elemzése	52
13. ábra: A TAP-modell faktorainak összefüggései az elektromobilitási eszközök birtoklásával	55
14. ábra: Megoldási javaslatokra adott válaszok átlaga	57
15. ábra: Az e-roller felfedezésének, kiválasztásának folyamata.....	62
16. ábra: A CFW felülírásának folyamata.....	63
17. ábra: A módosult DRV számmal rendelkező e-roller	64
18. ábra: ScooterHacking Utility alkalmazás kezelőfelülete	65
19. ábra: ScooterHacking Utility által támogatott e-rollerek	66
20. ábra: ST-Link V2 összekötése a Xiaomi e-roller vezérlőegységével	67

MELLÉKLETEK JEGYZÉKE

1.számú melléklet: A kérdőíves kutatáshoz összeállított kérdőív

2.számú melléklet: Kérdőív kiértékelése

1. számú melléklet: A kérdőíves kutatáshoz összeállított kérdőív.

1. Az Ön neme?

Nő

Férfi

2. Hány éves Ön?

18-25 év

26-39 év

40-59 év

60 év felett

3. Az Ön legmagasabb iskolai végzettsége?

8 általános iskolánál kevesebb

Általános iskola 8. osztálya

Középfokú végzettség érettségi nélkül, szakmai végzettséggel

Középfokú végzettség érettségivel

Középfokú végzettség érettségivel, szakmai végzettséggel

Felsőfokú végzettség (Alapképzés, BA, BSc)

Felsőfokú végzettség (Mesterképzés, MA, MSc)

Tudományos fokozatot igazoló oklevél (PhD, DLA)

4. Milyen településen él Ön?

Főváros

Vármegyeszékhely vagy megyei jogú város

Egyéb város

Község, Falu

5. Rendelkezik-e valamilyen informatikai képzettséggel?

Nem rendelkezem

Középfokú végzettséggel rendelkezem Felsőfokú végzettséggel rendelkezem

6. Rendelkezik saját elektromos mobilitási eszközzel? (Pl. e-roller, hoverboard, segway, e-unickli stb.)

Igen

Nem

7. Milyen rendszerességgel használja Ön az alábbi elektromobilitási eszközöket?

	Naponta	Hetente egyszer-kétszer	Hetente többször (min. 3 alkalommal)	Havonta 1-3 alkalommal	Ritkábban	Soha
E-roller	☐	☐	☐	☐	☐	☐
Hoverboard	☐	☐	☐	☐	☐	☐
Segway	☐	☐	☐	☐	☐	☐
E-unickli	☐	☐	☐	☐	☐	☐
Elektromos kerékpár	☐	☐	☐	☐	☐	☐
Elektromos gördeszka	☐	☐	☐	☐	☐	☐

8. Milyen gyakran használ Ön közösségi megosztáson alapuló elektromobilitási eszközt?

	Naponta	Hetente egyszer-kétszer	Hetente többször (min 3 alkalommal)	Havonta 1-3 alkalommal	Ritkábban	Soha
E-roller	☐	☐	☐	☐	☐	☐
Elektromos kerékpár	☐	☐	☐	☐	☐	☐

9. Mely területeken látja hasznosnak az elektromos mobilitást?

Városi közlekedés

Szállítás és logisztika

Tömegközlekedés kiegészítése

Turizmus

Rövid távú közlekedés (pl. bevásárlás, munkába járás)

Sport és szabadidős tevékenységek

Környezetvédelem és fenntarthatóság

10. Önnek milyen mértékben befolyásolja a döntését a kiberbiztonság egy elektromobilitási eszköz vásárlása esetén? Jelölje 1-től 5-ig terjedő skálán.

1: Egyáltalán nem befolyás

5: Nagy mértékbe befolyásolja

11. Információbiztonság szempontjából tudatosnak tartja-e magát?

Nem foglalkoztat az információbiztonság

Igen

Nem

12. Kiberbiztonsági szempontjából tudatosnak tartja-e magát?

Nem foglalkoztat a kiberbiztonság

Igen

Nem

13. Milyen szintűnek ítéli meg a kiberbiztonsági ismereteit?

Nem rendelkezek kiberbiztonsági ismeretekkel.

Alapszintű: Csak alapvető fogalmakat ismerek, de nincs mélyebb tudásom a témában.

Közepes szintű: Ismerem a kiberbiztonság alapjait, de van még mit tanulnom.

Haladó szintű: Részletes ismereteim vannak a kiberbiztonság terén.

Szakértő: Magas szintű és széleskörű tudásom van a kiberbiztonság terén, és tapasztalataim is vannak a gyakorlatban.

14. Milyen mértékben figyel oda az internetre kapcsolódó eszköze biztonságos használatára? (Pl. erős jelszavak használata)
Jelölje 1-től 5-ig terjedő skálán.

1: Nem törődöm a biztonsággal

2: Mindig odafigyelek a biztonságra.

15. Milyen gyakran frissíti az alábbiakat a kiberbiztonság javítása érdekében?

	Mindig azonnal frissíték	Általában frissíték, de időnként késlekedem vele	Ritkán frissíték, csak ha szükséges	Nem szoktam frissíteni
Alkalmazásokat	☐	☐	☐	☐
Eszközeinek szoftverét	☐	☐	☐	☐
Eszközeinek hardver- illesztőprogramjait	☐	☐	☐	☐

16. Hallott már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során?

Igen, hallottam róla, és figyelek a biztonságra használat közben.

Igen, hallottam róla, de nem igazán foglalkozom vele.

Nem, nem hallottam erről korábban.

17. Kiberbiztonsági szempontból milyen szintű az Ön bizalma az elektromobilitási közlekedési eszközökkel kapcsolatban? Jelölje 1-től 5-ig terjedő skálán.

1: Nagyon alacsony: Nem bízik az elektromobilitási eszközök kiberbiztonságában.

5: Nagyon magas: Teljes mértékben bízik az elektromobilitási eszközök kiberbiztonságában.

18. Ön szerint az alábbiak közül, melyek érinthetik az elektromos mobilitási eszközöket? Több válasz is megjelölhető.

Adatlopás és személyes információk veszélyeztetése

Távoli hozzáférésből származó információs támadások (hackelés)

Szoftverhibák és informatikai sebezhetőségek

Hamisított vagy biztonsági szempontból ellenőrizetlen alkalmazások

Wi-Fi vagy Bluetooth hálózatokon keresztül történő támadások

Távoli hozzáférésből származó fizikai támadások (pl. fékezésre kényszerítés)

19. Tapasztalt már kiberbiztonsági problémát az Ön által használt elektromos mobilitási közlekedési eszközökkel kapcsolatban?

Igen, tapasztaltam.

Nem, soha nem tapasztalta ilyet.

Nem használok ilyen eszközöket, így nem tapasztaltam.

20. Ha az előző kérdésre "Igen"-el válaszolt és megkívánja osztani, akkor kérem írja le mi történt.

21. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások arra vonatkoznak, hogy Önnek mennyire fontosak az alábbiak egy elektromos mobilitási eszköz kiválasztása során.

1= Egyáltalán nem értek egyet

2= Részben nem értek egyet

3= Egyet is értek, meg nem is

4= Részben egyetértek

5= Teljes mértékben egyetértek

Fontos, hogy az eszköz használatához álljanak rendelkezésre applikációk.

Fontos, hogy az eszközhöz tartozó applikációk könnyen kezelhetők legyenek

Fontos, hogy az eszköz használatához ne keljen megadni személyes adatokat.

Fontos, hogy az eszköz használatához ne keljen megadni pénzügyi adatokat.

22. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások arra vonatkoznak, hogy Önnek mennyire fontosak az alábbiak egy elektromos mobilitási eszköz kiválasztása során.

1= Egyáltalán nem értek egyet

2= Részben nem értek egyet

3= Egyet is értek, meg nem is

4= Részben egyetértek

5= Teljes mértékben egyetértek

Fontos, hogy az eszköz biztonságos használatához álljanak rendelkezésre szükséges oktatóanyagok.

Fontos, hogy az eszköz rendelkezzen informatikai biztonsági rendszerekkel (pl. hálózati védelem).

Fontos, hogy az eszköz álljon rendelkezésre rendszeresen elérhető szoftverfrissítés és biztonsági javítás.

Fontos, hogy az eszköz feleljen meg a kiberbiztonsági előírásoknak.

23. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások arra vonatkoznak, hogy az alábbi intézkedések hogyan hatnának az elektromobilitási eszközök kiberbiztonságával kapcsolatban.

1= Egyáltalán nem értek egyet

2= Részben nem értek egyet

3= Egyet is értek, meg nem is

4= Részben egyetértek

5= Teljes mértékben egyetértek

Javítaná az emberek bizalmát, a részletes felhasználói oktatóanyagok és kézikönyvek készítése.

Javítaná az emberek bizalmát, a rendszeres tájékoztatás a kiberbiztonsági frissítésekről és intézkedésekről.

Javítaná az emberek bizalmát, az erőteljesebb adatvédelmi intézkedések bevezetése az eszközök és alkalmazásai részére.

24. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások arra vonatkoznak, hogy az alábbi intézkedések hogyan hatnának az elektromobilitási eszközök kiberbiztonságával kapcsolatban.

1= Egyáltalán nem értek egyet

2= Részben nem értek egyet

3= Egyet is értek, meg nem is

4= Részben egyetértek

5= Teljes mértékben egyetértek

Javítaná az emberrel bizalmát, az átláthatóbb kommunikáció a gyártók részéről a biztonsági intézkedésekről és fejlesztésekről.

Javítaná az emberrel bizalmát, ha kiberbiztonsági szakértőket vonnak be az eszközök fejlesztésébe és tesztelésébe a megbízhatóság növelése érdekében.

Javítaná az emberrel bizalmát, ha az elektromobilitási eszközök gyártóinak termékei rendszerese független kiberbiztonsági auditokon vennének részt.

TECHNOLÓGIA ELFOGADÁSSAL KAPCSOLATOS HAJLANDÓSÁG

A következőkben a technológia elfogadással kapcsolatos hajlandóságot mérem fel. A technológiaelfogadásmodellek megjelenése kulcsfontosságú szerepet játszott abban, hogy tesztelni lehessen egy-egy technológiai innováció felhasználói fogadtatását, feltárva annak hibáit, hiányosságait. Az általam használt modell a Technológia Alkalmazására való Hajlandóság kérdőíve (Technology Adoption Propensity, röviden TAP). A TAP-index négy tényezőtől áll: optimizmus, jártasság, függőség és sebezhetőség. Az egyén TAP-pontszáma előre jelzi a technológiai lehetőségek felhasználásának és birtoklásának a szintjét.

25. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások a technológiával kapcsolatos optimizmust vizsgálják.

1= Egyáltalán nem értek egyet

2= Részben nem értek egyet

3= Egyet is értek, meg nem is

4= Részben egyetértek

5= Teljes mértékben egyetértek

Azt gondolom, hogy az elektromobilitás a kulcsa a jövő fenntartható közlekedésének.

Az elektromobilitási jármű használata segít abban, hogy környezetbarátabb alternatívát válasszak a közlekedési eszközök között.

Az elektromobilitási fejlődő technológiája miatt úgy gondolom, hogy ezek a járművek egyre megbízhatóbbak és hatékonyabbak lesznek.

Az elektromobilitási jármű használata növeli az én hozzájárulásomat a fenntartható közlekedéshez.

26. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások a technológiában való jártasságot vizsgálják.

Az elektromobilitási jármű használata könnyebb számomra, mint másoknak.

Mások is gyakran kérnek segítséget tőlem az elektromobilitási szolgáltatások és rendszerek használatával kapcsolatában.

Élvezem, hogy magam fedezzem fel az új elektromobilitási funkciókat és szolgáltatásokat, anélkül, hogy mások segítségét kérném.

El tudom végezni az elektromos járművek szoftveres frissítéseit, és értem, hogy ezek hogyan befolyásolják a járművek biztonságát.

27. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások a technológiától való függőséget vizsgálják.

1= Egyáltalán nem értek egyet

2= Részben nem értek egyet

3= Egyet is értek, meg nem is

4= Részben egyetértek

5= Teljes mértékben egyetértek

Az elektromos járműveim nélkülözhetetlenek az életemben, és nehézséget okozna, ha egy időre le kellene mondani róluk.

Úgy érzem, hogy túlzottan számítok az elektromos járművekre mindennapi közlekedésim során.

Az elektromos járművek nélkül kiszolgáltatottnak vagy hátrányban érzem magam a mindennapi életem során

28. Kérem, jelölje 1-től 5-ig terjedő skálán, mennyire ért egyet az alábbi állításokkal.

Az állítások a technológia általi sebezhetőséget vizsgálják.

1= Egyáltalán nem értek egyet

2= Részben nem értek egyet

3= Egyet is értek, meg nem is

4= Részben egyetértek

5= Teljes mértékben egyetértek

Úgy érzem, hogy a kiberbiztonsági intézkedések fejlesztése során az iparág nem tesz eleget az elektromobilitási eszközök védelméért.

Az elektromobilitás terjedése miatt növekedhet a kiberbűnözők érdeklődése ezen eszközök iránt.

Úgy gondolom, hogy az elektromobilitás terjedésével párhuzamosan a kiberbiztonsági megoldások is fejlődnek.

2. számú melléklet: Kérdőív kiértékelése

Crosstabs

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Az Ön neve? * Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során?	117	100,0%	0	0,0%	117	100,0%

Az Ön neve? * Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során? Crosstabulation

Count

		Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során?		Total
		1	2	
Az Ön neve?	1	53	9	62
	2	37	18	55
Total		90	27	117

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5,445 ^a	1	,020	,027	,017
Continuity Correction ^b	4,468	1	,035		
Likelihood Ratio	5,499	1	,019		
Fisher's Exact Test					
Linear-by-Linear Association	5,399	1	,020		
N of Valid Cases	117				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 12,69.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Phi	,216			,020
	Cramer's V	,216			,020
Interval by Interval	Pearson's R	,216	,089	2,369	,019 ^c
Ordinal by Ordinal	Spearman Correlation	,216	,089	2,369	,019 ^c
N of Valid Cases		117			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Van-e legalább felsőfokú végzettsége? * Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során?	117	100,0%	0	0,0%	117	100,0%

Van-e legalább felsőfokú végzettsége? * Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során? Crosstabulation

Count

		Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során?		Total
		1	2	
Van-e legalább felsőfokú végzettsége?	1	59	16	75
	2	31	11	42

Total	90	27	117
-------	----	----	-----

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,358 ^a	1	,550	,648	,352
Continuity Correction ^b	,136	1	,712		
Likelihood Ratio	,353	1	,552		
Fisher's Exact Test					
Linear-by-Linear Association	,355	1	,551		
N of Valid Cases	117				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 9,69.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Asymp. Std. Error ^a	Approx. T ^b	Approx. Sig.
Nominal by Nominal	Phi	,055			,550
	Cramer's V	,055			,550
Interval by Interval	Pearson's R	,055	,094	,594	,554 ^c
Ordinal by Ordinal	Spearman Correlation	,055	,094	,594	,554 ^c
N of Valid Cases		117			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Azt gondolom, hogy az elektromobilitás a kulcsa a jövő fenntartható közlekedésének.	117	1	5	3,94	1,053	-,736	,224	-,103	,444
Az elektromobilitási jármű használata segít abban, hogy környezetbarátabb alternatívát válasszak a közlekedési eszközök között.	117	1	5	4,13	1,038	-1,295	,224	1,289	,444
Az elektromobilitás fejlődő technológiája miatt úgy gondolom, hogy ezek a járművek egyre megbízhatóbbak és hatékonyabbak lesznek.	117	1	5	3,94	,985	-1,089	,224	1,182	,444
Az elektromos jármű használata növeli az én hozzájárulásomat a fenntartható közlekedéshez.	117	1	5	3,75	1,090	-,831	,224	,214	,444
Az elektromobilitási jármű használata könnyebb számomra, mint másoknak.	117	1	5	3,32	1,401	-,389	,224	-1,097	,444
Mások is gyakran kérnek segítséget tőlem az elektromobilitási szolgáltatások és rendszerek használatával kapcsolatban.	117	1	5	3,07	1,685	-,065	,224	-1,654	,444

Élvezem, hogy magam fedezem fel az új elektromobilitási funkciókat és szolgáltatásokat, anélkül, hogy mások segítségét kérném.	117	1	5	3,41	1,481	-,414	,224	-1,219	,444
El tudom végezni az elektromos járművek szoftveres frissítéseit , és értem, hogy ezek hogyan befolyásolják a járművek biztonságát.	117	1	5	3,35	1,621	-,363	,224	-1,463	,444
Az elektromos járműveim nélkülözhetetlenek az életemben, és nehézséget okozna, ha egy időre le kellene mondani róluk.	117	1	5	2,88	1,682	,114	,224	-1,656	,444
Úgy érzem, hogy túlzottan számítok az elektromos járművekre mindennapi közlekedéseim során.	117	1	5	2,68	1,552	,149	,224	-1,559	,444
Az elektromos járművek nélkül kiszolgáltatottnak vagy hátrányban érzem magam a mindennapi életem során.	117	1	5	2,74	1,678	,228	,224	-1,634	,444
Úgy érzem, hogy a kiberbiztonsági intézkedések fejlesztése során az iparág nem tesz eleget az elektromobilitási eszközök védelméért.	117	1	5	3,56	1,256	-,301	,224	-,902	,444
Az elektromobilitás terjedése miatt növekedhet a kiberbűnözők	117	1	5	4,02	1,098	-,947	,224	,173	,444

érdeklődése ezen eszközök iránt.									
Úgy gondolom, hogy az elektromobilitás terjedésével párhuzamosan a kiberbiztonsági megoldások is fejlődnek.	117	1	5	3,88	1,084	-,708	,224	-,128	,444
Valid N (listwise)	117								

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Magyar megnevezés	Idegen nyelvű megnevezés
ACEA	Európai gépjárműgyártók szövetségét	European Automobile Manufacturers' Association
CAN		Controller Area Network
CFW		Custom Firmware
C-ITS	Kooperatív intelligens közlekedési rendszerek	Cooperative Intelligent Transport Systems
DoS	Szolgáltatásmegtagadással járó támadás	Denial Of Service
ECU	A jármű elektronikus vezérlőegysége	Electronic Controller Unit
ENISA	Európai uniós kiberbiztonsági ügynökség	The European Union Agency for Cybersecurity
FW		Firmware
GDPR	Általános adatvédelmi rendeletet	General Data Protection Regulation
GNSS	Globális Navigációs Műholdrendszer	Global Navigation Satellite System
ITS	Intelligens közlekedési rendszerek	Intelligent Transport Systems
KRESZ	Közúti Rendelkezők Egységes Szabályozása - 1/1975. (II. 5.) KPM-BM együttes rendelet a közúti közlekedés szabályairól	
LIN		Local Interconnect Network
NIS	Hálózati és információs rendszerek biztonságáról szóló irányelv	The Directive On Security Of Network And Information System
NIS2	Hálózati és információs rendszerek biztonságáról szóló irányelv 2	Network And Information Systems Directive 2
OTA		Over The Air
SPSS		Statistical Package For The Social Sciences
TAP	Technológiai átvételi hajlandóság	Technology Adoption Propensity
V2V	Jármű és jármű közötti kommunikáció	Vehicle-To-Vehicle
V2X	Jármű és környezet közötti kommunikáció	Vehicle-To-Everything

TÁBLÁZATOK JEGYZÉKE

- 1. számú táblázat:** Az e-rollerek lehetséges támadási pontjai

FÜGGELÉKEK JEGYZÉKE

- 1. számú függelék:** A konzultációkon történő részvétel igazolása
- 2. számú függelék:** Szerzői jogi nyilatkozat
- 3. számú függelék:** Felhasználási nyilatkozat

1. számú függelék: A konzultációkon történő részvétel igazolása

3. függelék

A konzultációkon történő részvétel igazolása

A konzultációkon történő részvétel igazolása (diplomamunkához)

A hallgató neve:	Harangozó Valentin
A hallgató Neptun-kódja:	G0WFHT
Szak, szakirány megnevezése:	Kiberbiztonsági
Képzési szint (alap-/mesterképzés):	Mesterképzés
Munkarend (levelező/napnali):	Levelező
A dolgozat címe:	Az elektromobilitási eszközök kiberbiztonsági kockázatai, különös tekintettel az e-rollerekre
A dolgozat konzulensének neve:	Dr. Bányász Péter
A konzulens munkahelye, beosztása:	NKE ÁNTK Kiberbiztonsági Tanszék, egyetemi docens

1. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2023.10.19 (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)
Budapest, 2023. év október hó 19. nap

Dr. Bányász Péter

.....
Konzulens aláírása

2. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2024.02.23. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)
Budapest, 2024. év február hó 23. nap

Dr. Bányász Péter

.....
Konzulens aláírása

3. A hallgató a dolgozat készítésével kapcsolatos konzultáción részt vett. A konzultáció időpontja: 2024.03.08. (év/hónap/nap). A konzultáció formája: személyes / elektronikus. (Aláhúzni!)
Budapest, 2024. év március hó 8. nap

Dr. Bányász Péter

.....
Konzulens aláírása

Készült 2 eredeti példányban.

2. számú függelék: Szerzői jogi nyilatkozat

Szerzői jogi nyilatkozat (diplomamunkához a Neptun-rendszer felületén)

Büntetőjogi felelősségem tudatában nyilatkozom, hogy a benyújtott jelen szakdolgozat/diplomamunka saját szellemi tevékenységem eredménye, az abban hivatkozott nyomtatott és elektronikus szakirodalom felhasználása a szerzői jogokra vonatkozó jogszabályoknak megfelelően történt, a benne foglaltak más személyek jogszabályban rögzített jogait nem sértik.

Szerzői jogi nyilatkozat (diplomamunkához papír alapú)

Alulírott Harangozó Valentin (NEPTUN-kód: G0WFHT) büntetőjogi felelősségem tudatában kijelentem, hogy a „Az elektromobilitási eszközök kiberbiztonsági kockázatai, különös tekintettel az e-rollerekre.” című, a Nemzeti Közszerzői Egyetem Kiberbiztonsági Mesterképzési Szak képzésén benyújtott jelen diplomamunka saját szellemi tevékenységem eredménye, az abban hivatkozott nyomtatott és elektronikus szakirodalom felhasználása a szerzői jogokra vonatkozó jogszabályoknak megfelelően történt, a benne foglaltak más személyek jogszabályban rögzített jogait nem sértik.

Budapest, 2024. április 04.

.....
Hallgató aláírása



3. számú függelék: Felhasználási nyilatkozat

Felhasználási nyilatkozat (diplomamunkához)

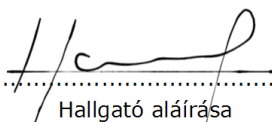
A hallgató neve:	Harangozó Valentin
Kar:	Államtudományi és Nemzetközi Tanulmányok Kar
Oktatási szervezeti egység:	Kiberbiztonsági Tanszék
Szak, szakirány:	Kiberbiztonsági mesterképzési szak
A dolgozat címe:	Az elektromobilitási eszközök kiberbiztonsági kockázatai, különös tekintettel az e-rollerekre.
A dolgozat elkészítésének éve:	2024.

I. Alulírott, mint a diplomamunka szerzője tudomásul veszem, hogy a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 50. § (6) bekezdése értelmében az elektronikus tanulmányi nyilvántartó rendszerben (Neptun-rendszer) tárolt szakdolgozatokat és diplomamunkákat – jogszabályban meghatározottak szerint titkosított részek kivételével – a tanulmányi rendszeren keresztül korlátozás nélkül hozzáférhetővé és kereshetővé kell tenni.

II. Alulírott, mint a diplomamunka szerzője, a szerzői jog kizárólagos jogosultjaként **hozzájárulok**, hogy a dolgozatom teljes szövegének elektronikus változatát a Nemzeti Közszerzési Egyetem Egyetemi Könyvtár által mőködtesett egyetemi repozitórium nyilvánosan szolgáltatassa:

korlátlan hozzáféréssel (teljes nyilvánossággal az interneten elérhetően)

Budapest, 2024. április 4.

.....

Hallgató aláírása

ANNOTÁCIÓ

A dolgozat célja az volt, hogy alaposan vizsgálja az elektromobilitási eszközök kiberbiztonsági vonatkozásait, azonosítva a lehetséges kockázatokat és veszélyforrásokat, valamint feltárja a felhasználók és az elektromos járművek kiberbiztonsága közötti összefüggéseket. A kutatás során részletesen elemeztem az eszközök potenciális sebezhetőségeit, beleértve az adatbiztonsági kockázatokat, a fizikai biztonság kérdéseit és a vezérlőrendszer sebezhetőségeit. Emellett a felhasználók technológia elfogadási hajlandóságát is megvizsgáltam.

A kutatás módszertanát többféle módszer alkotta. Elvégeztem egy online kérdőíves kutatást, hogy megérthessem az emberek attitűdjeit és aggodalmait az elektromobilitási eszközök kiberbiztonsági kérdéseivel kapcsolatban. Ezen felül áttekintettem a hazai és nemzetközi szakirodalmat az elektromobilitási eszközök kiberbiztonságával kapcsolatban, valamint biztonsági tesztelést hajtottam végre egy elektromos rolleren, hogy közvetlen tapasztalatokat szerezzek az eszköz kiberbiztonsági sebezhetőségeiről.

Az eredmények alapján megállapítottam, hogy az elektromobilitási eszközök valóban számos sebezhetőségi ponttal rendelkeznek. Igazoltam, hogy az emberek valós aggodalommal viszonyulnak ezeket az eszközöket érintő kiberbiztonsági kockázatokhoz. Különösen fontosnak tartották az adatbiztonság és a frissítések fontosságát. Megállapítottam, hogy a vizsgált emberek közül az elektromos járművekkel rendelkezők optimistábbak az elektromobilitási technológiákat illetően, és az elemzés alapján igazoltam, hogy a válaszadók neme befolyásolja a kiberbiztonsági tudatosságot.

Ezek az eredmények fontos következtetéseket vonnak maguk után. A felhasználók és a gyártók közötti együttműködés elengedhetetlen a kiberbiztonság növelése érdekében. További oktatási és tájékoztató kampányokra van szükség a felhasználók tudatosságának növelése érdekében, és a gyártóknak fokozott figyelmet kell fordítaniuk a biztonsági frissítésekre és ellenőrzésekre. Ezen intézkedések elősegíthetik, hogy az elektromobilitási járművek és azok felhasználói biztonságosabb környezetben vehessék igénybe ezeket az innovatív közlekedési eszközöket, ezzel hozzájárulva: egy fenntartható, biztonságos és technológiailag fejlett közlekedési jövőért.