INFORMATION SECURITY OF PASSENGER VEHICLES FROM THE PERSPECTIVE OF INFORMATION SECURITY EXPERTS

A SZEMÉLYGÉPJÁRMŰVEK INFORMÁCIÓBIZTONSÁGA AZ INFORMÁCIÓBIZTONSÁGI SZAKÉRTŐK SZEMSZÖGÉBŐL

HEGYI Henrietta[1]

Abstract

Internet-connected passenger vehicles face similar risks as mobile phones, but unauthorized access to vehicle systems can pose greater risks to users. Modern passenger vehicles are capable of connecting to the internet and receiving messages that contain various instructions. The aim of this study is to explore the information security challenges related to passenger vehicles and formulate recommendations regarding the practical application of the current regulatory environment. To understand this complex issue, a qualitative research methodology was employed through expert in-depth interviews. The proper state and practical implementation of regulations are key to protecting user data and minimizing the risk of unauthorized access. The recommendations presented in this study support the development of the regulatory environment in the field of automotive manufacturing..

Keywords

IoT, passenger vehicle, information security, security standards, cybersecurity

Absztrakt

Az internetre csatlakozó járművek hasonló veszélyekkel néznek szembe, mint a mobiltelefonok, de előbbiek meghibásodása nagyobb kockázatot jelenthet a felhasználók számára. A modern személygépjárművek képesek kapcsolódni az internethez és üzeneteket fogadni, amelyek különböző utasításokat tartalmaznak. A tanulmány célja a személygépjárművekkel kapcsolatos információbiztonsági kihívások feltárása és a jelenlegi szabályozási környezet gyakorlati alkalmazásával kapcsolatos javaslatok megfogalmazása. Ennek a komplex kérdéskörnek a megértéséhez kvalitatív kutatási módszertant alkalmaztunk, szakértői mélyinterjúk formájában. A szabályok megfelelő állapota és gyakorlati alkalmazása kulcsfontosságú a felhasználói adatok védelmében és az illetéktelen hozzáférés kockázatának minimalizálásában. A tanulmányban bemutatott javaslatok támogatják a szabályozási környezet fejlesztését a gépjárműgyártás terén.

Kulcsszavak

IoT, személygépjármű, szabványok, kiberbiztonság, információbiztonság

[1] hegyi.henrietta@uni-obuda.hu | ORCID: https://orcid.org/0000-0002-7731-840X | Doktori hallgató, Óbudai Egyetem | Doktori hallgató, Óbudai Egyetem.

BEVEZETÉS

Az internetkapcsolatra képes személygépjárművek hasonlóan a mobiltelefonokhoz, ki vannak téve az internetről érkező támadásoknak, miközben a személygépjármű rendszereihez való illetéktelen hozzáférés használatának célját tekintve nagyobb veszélyforrást jelenthet annak felhasználójára, mint egy mobiltelefon. A modern személygépjárművek a „Dolgok Internetéhez" (Internet of Things, IoT) hasonlóan képesek arra, hogy az internethez kapcsolódjanak és onnan különböző utasításokat tartalmazó üzeneteket fogadjanak. Egyre több gyártó tér át a gépjárművek belső hálózatának kulcsfontosságú elemei, a mikrokontrollerek (ECU – *electronic controller unit*) *firmware*[2] progjamainak (alapszoftver vagy vezérlőprogram) interneten keresztül való frissítésére is. Ezt a gyakorlatot FOTA/OTA szolgáltatásnak (*over-the-air* vagy *firmaware* esetében *firmware-over-the-air*[3]) nevezzük.

A személygépjárművek ma már a legkülönfélébb szenzorokkal, adatfeldolgozó egységekkel, rögzítőeszközökkel (pl. kamera) vannak felszerelve, melyek nagy mennyiségű információ összegyűjtésére szolgálhatnak. Az ilyen adatokból a felhasználó vagy egy csoport számos tulajdonságára, szokására lehet következtetni, mely szintén biztonsági kockázatokat rejt magában. Ugyan a gépjárműiparban a mind a gyártóknak, mind pedig a beszállítóknak szigorú biztonsági előírásoknak kell megfelelnie, az informatika gyors fejlődésének hatására ugyanezt a szigorú rendszert az elektronikus információbiztonság kapcsán már sokkal nehezebb működtetni. [1] Bár a legtöbb esetben a támadóknak nem érdekük a járműben tartózkodók életét veszélyeztetni, mégis van ok az aggodalomra, hiszen a rengeteg gyűjtött adatnak köszönhetően magas haszonnal kecsegtethet egy esetleges sikeres behatolás. [2] A megfelelő védelem kialakítása kapcsán problémát jelent, hogy a biztonsági értékelés gyakran szubjektív szempontok alapján történik – minél összetettebb rendszerről van szó, annál nehezebb pontos metrikát alkalmazni a kockázatok elemzésére. [3], [4]

Az információbiztonsági szakértők szubjektív ítéletei fontos szerepet játszanak a kiberfizikai rendszerek fenyegetéseinek értékelése és modellezése során. Például az egyes rendszerelemek sebezhetőségét többféle tényező alapján lehet leírni; ilyenek a bonyolultság, a technológiai érettség és a támadások segítésére rendelkezésre álló eszközök elérhetősége. Ezek az információk hasznosak a támadási kockázat meghatározásában, de nagy részüket nehéz automatikusan begyűjteni. Azonban a legtöbb szakértőben valamilyen mértékű bizonytalanság rejlik az értékelések terén. [5] A meglévő módszerek a fenti okokból kifolyólag nagymértékben függnek az értékelő tapasztalataitól, és a biztonsági mérőszámok általában legjobb esetben belső kockázatelemzési metódusok eredményeiként alakulnak ki. [6]

Jelen tanulmány célja, hogy feltárja a személygépjárművekkel kapcsolatos információbiztonsági kihívásokat és javaslatokat fogalmazzon meg a jelenleg használatban lévő szabványok és szabályozási környezet gyakorlati alkalmazásával kapcsolatban. A tanulmány célja továbbá az is, hogy javaslatokat fogalmazzon meg a szabályozási környezet tar-

[2] Hardverben - jellemzően csak olvasható memóriában (ROM) vagy programozható csak olvasható memóriában (PROM) - tárolt számítógépes programok és adatok, úgy, hogy a programok és adatok nem írhatók vagy módosíthatók dinamikusan a programok végrehajtása során.

[3] A folyamat során a szoftverfrissítés „a levegőn keresztül", azaz internet kapcsolat segítségével jut el a járműhöz, tehát nincs szükség például pendrive vagy egyéb fizikai eszköz csatlakoztatására.

talmára és alkalmazására vonatkozóan a személygépjárműipar területén, továbbá egy a kiberbiztonsági területen kevésbé gyakran alkalmazott módszertani megközelítéssel vizsgálja meg a témát, ezzel hozzájárulva a jövőbeli kutatási irányok meghatározásához.

A cikk kutatási kérdései a következők:

1. A hazai információbiztonsági szakemberek szerint megfelelő-e a jelenlegi információbiztonsági szabályozási környezet hatékonysága a személygépjárműiparban?
2. Milyen változtatásokkal lehetne hatékonyabbá tenni a személygépjárműiparban alkalmazott információbiztonsági szabványokat és szabályozási környezetet, hogy azok megfelelően védjék ne csak a gyártó, de a felhasználó adatait is?

A tanulmány a fenti problémára kvalitatív kutatás segítségével keresi a választ. A szakirodalmi elemzés a főbb információbiztonsági elméleti megközelítéseket, valamint leggyakrabban alkalmazott szabványokat elemzi. A kutatáshoz választott módszertan a mélyinterjú sajátosságait, valamint az átiratok elemzésére alkalmazott tartalomelemzési módszertant ötvözi.

SZAKIRODALMI ELEMZÉS

Az összekapcsolt autókkal kapcsolatos szolgáltatások adatainak feldolgozását szabályozó információbiztonsági irányelvek gyakran lazán meghatározott és/vagy nem összeegyeztethető célokat (pl. kért szolgáltatások nyújtása, biztonságos használat, viselkedésértékelés, valamint üzleti tevékenységek működtetése és bővítése) kapcsolnak össze. [7] Például az eredetileg karbantartási vagy felhasználói élmény fokozásának céljával [8] gyűjtött adatokat az érintettek beleegyező nyilatkozata esetén a biztosítótársaságok felhasználhatják a járművezetői profilok gazdagítására, az egyéni árazás kialakítására, a vezetési magatartáson alapuló biztosítási kötvények kínálására vagy az autóbalesetekben fennálló felelősség kivizsgálására. [9] A főként az ipar 4.0 technológiákat érintő komplexitásból fakadó szabályozási problémákra a COVID-19 időszaka is rámutatott. [10] Megfelelő szabályozási környezetben a közlekedésbiztonsági hatóságok is felhasználhatják ezeket az adatokat a közlekedési szabályok betartatására, például a sebességkorlátozások ellenőrzésére. A személy autóhasználatára vonatkozó minden egyes adat, például a vezetési útvonalak és úti célok, az autóba épített kommunikáció vagy az infotainment-szolgáltatások érzékeny információkat tárhatnak fel az adott személy életéről. Az emberek vezetési rutinja és az érdeklődési körükbe tartozó helyek nemcsak az azonosításukat teszik lehetővé [11], hanem – például az általa látogatott helyszínek ismeretében – olyan érzékeny információkra is következtethet az adatfeldolgozó, mint a vallási és politikai kötődések, a szexuális irányultság és az egyéb emberi kapcsolatok. Ezért az összegyűjtött adatok hasznosak az egyének profilalkotásához és megfigyeléséhez, különösen akkor, ha a személyes adatok meglévő (magán- vagy kormányzati) adatbázisaihoz kapcsolódnak vagy például a mobiltelefonjaik által gyűjtött adatokkal kapcsolják össze azokat. [12] Az adatkezelőknek egyértelműen tájékoztatniuk kell az internetre vagy más hálózatra csatlakoztatott autók felhasználóit a helymeghatározási adatok feldolgozásának céljáról. A helymeghatározási adatok érzékeny jellege miatt ezen adatokra az adatvédelmi elvek alapos alkalmazása szükséges, különösen a célhoz kötöttség, az adatok minimalizálása és az adatok tárolása tekintetében. Bár a különböző autóiparban alkalmazott szabványok és jogszabályok ma már magukba foglalják az ellátási lánc védelmét is, amely sok esetben a beszállítóknak a gyártóval egyenértékű szintű szabványoknak

való megfelelését jelenti, [13] az információbiztonsági szabványok általában csak egy keretet határoznak meg és nem adnak konkrét utasításokat a végrehajtással kapcsolatban. Ez bizonyos mértékben szükséges is, hiszen a különböző speciális helyzetek miatt adott fokú rugalmasság kulcsfontosságú.

Széles körben elismert, hogy a mérőszámok fontosak az információbiztonság szempontjából, mivel ezek hiányában nem tudjuk mérni a biztonsági politika, mechanizmusok vagy megvalósítások sikerét. A különböző kockázatelemzési módszerek például hatékony eszközt jelenthetnek az információbiztonsági szakemberek számára, hogy mérjék rendszereik, termékeik, folyamataik biztonsági szintjét, valamint a biztonsági problémák kezelésére való felkészültségüket. A mérőszámok segíthetnek a rendszer sebezhetőségének azonosításában is, útmutatást nyújtva a korrekciós prioritások meghatározásához. Az autógyártóknak érdekük ezenfelül, hogy megfeleljenek a főbb információbiztonsági és IT biztonsági szabványoknak, megvédjék a termékeikben – személygépjárműben – tárolt adatokat és az autók IT infrastruktúráját.

A leggyakrabban használt általános szabvány, melyet különböző vállalatok világszerte széleskörben alkalmaznak, az ISO 27001[4]. Ez a szabvány a személygépjárműiparban is elterjedt és erős kereteket biztosít ugyan az információbiztonság megteremtéséhez, de nem ad iránymutatást arra vonatkozóan, hogyan kell megvalósítani a leírtakat. Amellett, hogy rendkívüli rugalmasságot biztosít ezzel a vállalatok számára, egyúttal a kerülőmegoldások előtt is kaput nyit. Ahogyan a másik népszerű általános szabvány, a NIST 800-53[5], az ISO 27001 is a folyamatok szemszögéből közelíti meg az információbiztonság problémáját. Bár mindkét szabvány alapján a beszállítók számára is kötelező ugyanazon audit elvégzése, ennek gyakorlati megvalósulása kérdéses lehet, hiszen egy olyan komplex terméken, mint a személygépjármű, számos beszállító és azok alvállalkozói dolgoznak, különböző területekről. Emiatt a betartatás nehézségekbe ütközhet például az átláthatatlanság miatt. Az általánosan használt információbiztonsági szabványok között termékorientált szemléletmódot képvisel a Common Criteria[6], mely így már jobban közelíti azt a célt, hogy a személygépjármű mint végtermék, illetve a vele szerves összeköttetésben álló hálózat és szerverek hardveres és szoftveres rendszerei biztonságos működését biztosítsa. A Common Criteria azonban az ISO 27001-hez és a NIST 800-53-hoz képest sokkal kevésbé elterjedt.

Az elmúlt évek jelentős előrelépésének tekinthető a TISAX és az ISO/SAE 21434[7] megjelenése, melyek már specifikusan a személygépjárműipar igényeire szabott információbiztonsági szabványok. Az ISO/SAE 21434 egy termékközpontú, autóipari kibervédelemmel foglalkozó specifikus szabvány, mely meghatározza a közúti járművek elektromos és elektronikus (E/E) rendszereinek - beleértve azok alkatrészeit és kapcsolódási pontjait - koncepciójára, termékfejlesztésére, gyártására, üzemeltetésére, karbantartására és leszerelésére vonatkozó kiberbiztonsági kockázatkezelés műszaki követelményeit. Meghatározásra kerül benne egy keretrendszer, amely a kiberbiztonsági folyamatokra vonatkozó követelményeket és a kiberbiztonsági kockázatok kommunikációjának és kezelésének közös nyelvezetét tartalmazza. A szabvány minden sorozatgyártású közúti jármű E/E-rendszereire alkalmazandó, beleértve azok alkatrészeit és kapcsolódási pontjait, amelyek fejlesztése

[4] https://www.iso.org/standard/27001
[5] https://www.nist.gov/privacy-framework/nist-sp-800-53
[6] https://www.commoncriteriaportal.org
[7] https://www.iso.org/standard/70918.html

vagy módosítása e dokumentum kiadása után kezdődött. Ez ígéretesen hangzik ugyan, azonban a többi szabványhoz hasonlóan, az ISO/SAE 21434 bevezetése sem kötelező, ráadásul mivel egy rendkívül fiatal, 2021-ben kiadott szabványról van szó, időbe telik az is, mire a piac befogadja és így kellő területet tud majd lefedni. A TISAX (Trusted Information Security Assessment Exchange)[8] egy olyan új biztonsági értékelési keretrendszer, amelyet az autóipar szereplői fejlesztettek ki a beszállítók biztonsági kockázatainak kezelése érdekében. Az értékelési rendszer célja, hogy a beszállítók biztonsági szintjét egységes és hatékony módon lehessen értékelni és ellenőrizni, valamint biztosítsa az autóipari vállalatok számára, hogy a beszállítóik biztonsági szintje megfelelő. A TISAX értékelési keretrendszer alapvetően az ISO/IEC 27001 információbiztonsági szabványra épül, de az autóipari beszállítók számára további biztonsági követelményeket is tartalmaz. Az értékelési folyamat során a beszállítók biztonsági szintjét egy harmadik fél értékeli és ellenőrzi, így biztosítva a független értékelést. A TISAX értékelési rendszer használata előnyös lehet a beszállítók számára, mert lehetővé teszi számukra, hogy bizonyítsák biztonsági szintjüket az autóipari partnereik számára. Emellett a TISAX értékelési keretrendszer segít a beszállítóknak abban is, hogy felmérjék saját biztonsági kockázataikat és javítsák információbiztonsági folyamataikat. [14]

A fenti szabványokon kívül érdemes még említést tenni az IEC 62443-ról[9], mely kifejezetten az ipari ellenőrzési rendszerekre vonatkozik, illetve a SAE J3061[10] szabványról, melynek lényege, hogy gyakorlati tapasztalatokat gyűjt egybe és ajánlásokat nyújt a gyártók számára az információbiztonsági folyamatok fejlesztéséhez. Az összegyűjtött jógyakorlatok legfőbb célja, hogy rugalmasak, pragmatikusak és adaptálhatók legyenek a járműiparban, valamint más területeken működő kiberfizikai járműrendszerekre nézve is (pl. kereskedelmi és katonai járművek, teherautók, buszok). Ez az ajánlott gyakorlat azonban szintén magas szintű irányadó elveket állapít meg, tehát a konkrét megvalósításra vonatkozóan nem rögzít elvárásokat.

Ezenkívül az autógyártók az általuk gyártott autókra vonatkozó specifikus szabványokat és irányelveket is alkalmazzák (például ISO/TS 16949, amely az általános, ISO 9001 minőségbiztosítási szabvány autóipari leképezése), amelyek lehetnek nemzetközi vagy helyi szintűek. Az Európai Unióban az autókra vonatkozó szabványokat az Európai Bizottság, míg az Egyesült Államokban a Nemzeti Autópálya-biztonsági Hivatal (NHTSA) határozza meg, így attól függően is eltérés tapasztalható a követelmények között, hogy a világ melyik pontját vizsgáljuk. Az Európai Uniót tekintve az elmúlt években egyre nagyobb hangsúlyt kapott a GDPR és ennek hatására más területek is nagyobb hangsúlyt kezdtek fektetni az adatvédelemre. Ennek köszönhetően a felsorolt szabványokban is egyre nagyobb súllyal jelent meg az adatvádelem kérdésköre. Ezzel együtt is elmondható azonban, hogy a szabályozások közül egyedül a GDPR fókuszál kifejezetten a fogyasztók adataira és az adatáramlás átláthatóságára. Jelen tanulmánynak nem célja teljeskörűen bemutatni a GDPR-al kapcsolatos problémákat, de információbiztonsági kontextusban is érdemes kiemelni, hogy a nemzetközi szakirodalom számos olyan példát szolgáltat, melyek alátámasztják, hogy a rendeletet szükséges fejleszteni. [15], [16], [17]

[8] https://www.tuvsud.com/en/services/auditing-and-system-certification/tisax
[9] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[10] https://www.sae.org/standards/content/j3061_201601

Szintén fontos megjegyezni, hogy a hálózati kommunikáció miatt a tanulmány témájához kapcsolódnak a különböző felhőszolgáltatásokra vonatkozó szabályozások, illetve egy sor ipari eszközökre vonatkozó szabályozás is, ám ezekre jelen kutatás terjedelmi okok miatt szintén nem tér ki.

A SZEMÉLYGÉPJÁRMŰ MINT IOT ESZKÖZ

A Dolgok Internete, azaz az "Internet of Things" (IoT) kifejezést Kevin Ashton alkotta meg 1999-ben, egy előadáson a Procter & Gamble-nél. Ashton az egyik alapítója a Massachusetts Institute of Technology Automatic Recognition Labjának. [18]

Az IoT eszközök fogalmára azóta többféle definíció is elterjedt, melyek közül néhány gyakran alkalmazottat az alábbi táblázatban szemléltetünk:

Forrás	Definíció
NIST SP 1800-16B-C	Eszközök hálózata, amely tartalmazza a hardvert, szoftvert, firmware-t és aktuátorokat, amelyek lehetővé teszik az eszközök kapcsolódását, kölcsönhatását és szabad adat- és információcsere lehetőségét.[11]
NIST SP 800-172	A kiadványban használt értelemben olyan felhasználói vagy ipari eszközök, amelyek csatlakoznak az internethez. Az IoT eszközök szenzorokat, vezérlőket és háztartási készülékeket is magukba foglalnak.[12]
Gartner	Az "Internet of Things" (IoT) a fizikai tárgyak hálózata, amelyek beépített technológiával rendelkeznek, hogy kommunikáljanak, érzékeljenek vagy kölcsönhatásba lépjenek a belső állapotukkal vagy a külső környezettel.[13]
Európai Parlament	Az „Internet of Things” (IoT) olyan elosztott hálózatot jelent, amely fizikai tárgyakat köt össze, képesek érzékelni vagy cselekedni a környezetükben, és kommunikálni egymással, más gépekkel vagy számítógépekkel.[14]

1. táblázat - IoT definíciók. (Saját szerkesztés)

A személygépjármű IoT eszközként való értelmezése az elemzett szakirodalmi anyagban nem szerepel ugyan, azonban ha arra gondolunk, hogy a napjainkban használt személygépjárművek szenzorokkal és internetkapcsolattal rendelkeznek, és a telekommunikációs hálózatokon keresztül a szenzorok által rögzített adatokat (vagy azok feldolgozásának eredményét) továbbítják a gyártó vagy harmadik felek szervei felé, akkor az 1. táblázatban felsorolt definícióknak megfelel.

Ez a megfigyelés azért tarthat számot érdeklődésre, mert az IoT eszközök sajátosságaikat tekintve sokkal közelebb állnak a jelenleg használt személygépjárművekhez, mint a 20-30 évekkel ezelőtti, külső hálózati kommunikációt egyáltalán nem használó régi személygépjárművekhez. Ennek okán a rájuk vonatkozó szabályozási környezet alkalmazása

[11] https://csrc.nist.gov/glossary/term/internet_of_things
[12] https://csrc.nist.gov/glossary/term/internet_of_things
[13] https://www.gartner.com/en/information-technology/glossary/internet-of-things
[14] https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

megoldást jelenthetne a személygépjárműivek biztonságának biztosítására. Az IoT eszközök standardizálása azonban mindmáig komoly kihívásokba ütközik, köszönhetően a technológia gyors fejlődésének, az eszközök rövid életciklusának és sokféleségének. [19] Ezek a kihívások szintén megfigyelhetőek a személygépjárművek esetén is.

MÓDSZERTAN

A kutatás módszertanaként a téma érzékeny mivoltát és összetettségét figyelembe véve a mélyinterjút választottuk. A mélyinterjú sajátossága, hogy a kutató nem megadott kérdéslista hanem előre definiált témakörök alapján folytat dialógust az interjúalanyokkal azzal a céllal, hogy lehetőséget kapjon olyan kontextuális információk megszerzésére is, melyek az előzetes kutatások alapján nem merültek fel. [20] A mélyinterjú nem alkalmas ugyan arra, hogy a kapott eredmények alapján általánosításokat fogalmazhassunk meg, de lehetőséget biztosít arra, hogy a tématerületet mélyen ismerő szakemberek tapasztalatait és javaslatait megismerjük és összefoglaljuk.

Jelen kutatás lefolytatásához ezért a terepkutatás kategóriájába tartozó féligstrukturált interjúztatás módszere került kiválasztásra, mint a témához illeszkedő technika. [22] Az empirikus kutatás célja egyrészt annak megismerése, hogy mi a magyar szakértők véleménye a szakirodalomban felvetett információbiztonsági szabályozásokkal kapcsolatos trendekről, érdemes-e IoT eszközként kezelni a személygépjárművet és milyen kihívásokkal szembesülnek az elméletek gyakorlati adaptálása során, másrészt pedig az, hogy a felmerült információbiztonsági problémákkal kapcsolatos megoldási javaslatok összegyűjtésre kerüljenek. Mivel ez a megközelítés mélyebb dialógust igényel és nem oldható meg például egyszerű kérdőíves módszertannal, ezért indokolt a mélyinterjúk alkalmazása. [23] Az interjú a kérdésfeltevésén és az arra adott válaszok megvitatásán kívül kötetlen formában zajlott, azaz interaktív beszélgetés keretében, ami megkönnyítette a többletinformációk megszerzését. [22] Az interjúk készítése közben fontos szempont volt olyan új információk feltárása, melyek a szakirodalmi elemzés során nem merültek fel, de újabb vizsgálatok alapját képezhetik.

A megfelelő kérdések megállapításához, először a dolgozatban körüljárt témákra alapozva négy dimenzió – személygépjármű mint IoT eszköz, információbiztonsági szabványok hatékonysága és alkalmazása, kihívások a szabványok és jogszabályok gyakorlati alkalmazásában, megoldási javaslatok – elkülönítése történt meg, amelyek sorbarendezésének szempontja az volt, hogy az általánosabb témakörtől tartsanak az egyre specifikusabb felé. Erre azért volt szükség, hogy meghatározható legyen, hogy a kiválasztott szakemberek milyen általános megközelítést alkalmaznak a munkájuk során és milyen specifikumokat fedeznek fel a személygépjárműipari információbiztonsággal kapcsolatban.

Mivel nem minden szakértő rendelkezik ugyanolyan mély tapasztalattal az autóipar kapcsán – de ettől függetlenül lehetnek releváns szakmai észrevételei, melyek az autóiparra is érvényesek – így fontos, hogy az iparágspecifikus kérdések csak kiegészítő információk gyűjtésére szolgáltak és csak akkor kérdeztünk rájuk, ha az adott interjúalany ténylegesen rendelkezett ilyen jellegű tapasztalattal is.

Narratív elemzés

Ahhoz, hogy az információbiztonsági szabványok alkalmazásának nehézségeit gyakorlati szempontból vizsgálhassuk, olyan technikával volt szükséges elemezni az interjúk

lefolytatása során keletkezett információkat, amely segítségével nem csak egy-egy tény állapítható meg [21] az auditori munkával és a szabványokkal kapcsolatban, hanem azonosíthatók az elmélet és gyakorlat közötti különbségek mélyebben meghúzódó okai, vagy például az eredményeket befolyásoló szubjektív tényezők.

Az interjúleiratok a Krippendorff-féle tartalomelemzési módszertannal kerültek elemzésre, melynek lényege, hogy a kontextus is szerves részét képezi a szövegelemzésnek, így illeszkedik a tanulmányban foglalt komplex témához azáltal, hogy lehetőséget nyújt arra, hogy a kutató induktív módon következtessen a tartalomra. [24]

Mintavétel

A kvalitatív, mélyinterjús kutatás központi alanyai az információbiztonsági szakértők, azaz auditorok, tanácsadók és kutatók. Ahhoz azonban, hogy az elemzés során releváns információkat fedhessünk fel, szükség volt az előzetes, 25 főből álló csoport szűkítésére. A kutatásban résztvevő 10 interjúalany kiválasztása során szűrőfeltétel volt az információbiztonsági szakmák valamelyikében eltöltött minimum 5 év munkatapasztalat, illetve a minimum 5 különböző iparágban vagy területen, iparágban szerzett jártasság. Ezek a kritériumok biztosítják, hogy a szakértők megfelelően széleskörű gyakorlati ismeretekkel rendelkezzenek a kutatott kérdéseket illetően. A személygépjárműiparban szerzett tapasztalat nem volt azonban követelmény, mivel jellegüknél fogva a kutatási kérdések megválaszolásához nem szükséges mély ágazati ismeret, ellenben a minél széleskörűbb rálátás a különböző iparágak szabályozási környezetéről hozzásegít a jó és rossz gyakorlatok felismeréséhez.

Ennek okán került a mintába például olyan szakember, aki főként magyar kis- és középvállalkozásokkal foglalkozik és olyan, aki jelenleg az állami szférában dolgozik, azonban korábbi ügyfelei és munkáltatói közé tartoznak pénzintézetek, gyógyszeripari gyárak és élelmiszeripari vállalatok is.

Eredmények

Az interjúalanyok válaszaiból kiderül, hogy három válaszadó dolgozott már valamilyen járműiparral kapcsolatatos információbiztonsági projekten, feladatkörben, míg hét személy nem rendelkezik ilyen tapasztalattal. Ennek okán csak az előbbi három személy számára tettünk fel iparágspecifikus, kifejezetten járműipari szabványokra vonatkozó kérdéseket.

1. A személygépjármű mint IoT eszköz

Ennek a kérdésnek a relevanciáját az adja, hogy a személygépjármű, illetve annak alkatrészei hasonlítanak az IoT-ként definiált eszközökre és az ezekre vonatkozó szabályozási környezet jelenleg még szintén igen hézagos – így van létjogosultsága az olyan javaslatoknak, mint például hogy az IoT eszközök esetében megjelenő új szabványokat a személygépjárművek esetében is alkalmazzák az auditorok.

A kutatás során megkérdezett szakértők mindegyike egyöntetűen IoT eszközként tekint a személygépjárműre információbiztonsági szempontból. Ezt javarészt azzal indokolták, hogy a jármű a szenzorok által adatokat rögzít és a külső hálózattal is képes a kommunikációra. Az egyik interjúalany megközelítése a többiekhez képest egyedi volt abban, hogy felvetése szerint nem maga a jármű tekinthető IoT eszköznek, hanem annak alkatrészei. Ezt a megközelítést támasztja alá a személygépjármű, mint kiberfizikai rendszer komplex összetétele és alkatrészeinek sokfélesége.

Azonban ha a személygépjárművet ilyen nézőpontból vizsgáljuk azzal azt kockáztatjuk, hogy egyes alkatrészek kimaradnak az ellenőrzésből. Az egyik interjúalany a korábban bemutatott ISO/SAE 21434 szabvánnyal kapcsolatban kiemelte, hogy bár az jelentős változással kecsegtet a személygépjárművek elektronikai biztonságát tekintve, mivel az egyes elemekre fókuszál a teljes rendszer helyett, ezért nem nyújt teljes megoldást. Amennyiben tehát az IoT eszközökre érvényes szabványokat kívánjuk alkalmazni a személygépjármű egyes részeire, akkor ezt a lefedettséggel összefüggő kockázatot figyelembe kell vennünk.

2. Kockázatelemzés, metrikák, adatbiztonság

A teljes mintából egy szakértő nyilatkozta csupán, hogy szerinte az ISO 27001 (és ISO 27005) alapján végzett kockázatelemzés képes biztosítani a végfelhasználó adatainak biztonságát. Véleményét azzal indokolta, hogy mivel a szabvány kimondja, hogy a szervezetnek a rá vonatkozó szabályoknak meg kell felelnie, így a GDPR-nak való megfelelési kötelezettség az Európai Unió területén biztosítva van. A másik kilenc interjúalany véleménye azonban ettől markánsan eltér, többnyire az elmélet és a gyakorlat között tátongó különbségekre hívják fel a figyelmet, illetve arra, hogy a szabványok betartásának kikényszerítésére nincsenek megfelelő eszközök.

Példaként említik, hogy a beszállítók kibújhatnak a megfelelés alól azzal, ha például azt nyilatkozzák, hogy a szabvány bevezetése már folyamatban van, míg végül a minősítő auditra évek múltán sem kerül sor. A szakértők olyan esetről is beszámoltak, amikor egy szabvány adatbiztonságra irányuló követelményeinek való megfelelést a tanúsítást kérő szereplő egyszerűen egy ügyvédi iroda által kiállított nyilatkozattal oldotta meg.

Akkor sincs biztosítva azonban a megfelelés, ha minden szereplő megfelelő hozzáállással rendelkezik, hiszen a legtöbb kockázatkezelési módszertan nem írja elő, hogy a maradványkockázatokat milyen időtartam alatt kell kiküszöbölni, hanem az erre vonatkozó szabályok és gyakorlatok pontos kidolgozását a szervezetre hagyja.

3. Kihívások és megoldási javaslatok

A kihívások kapcsán több interjúalany is kiemelte a jármű, mint végtermék komplexitását. Két interjúalany is rávilágított arra, hogy egyre nagyobb kihívást fog jelenteni a személygépjárművek szoftverkörnyezetének támogatása. Amennyiben a szoftvertámogatás lejár, akkor onnantól kezdve nem biztosított a megfelelő védelem sem. Az adatbiztonság szempontjából kihívásnak tekinthető az is, hogy a felhasználó nem kap rálátást arra, mi történik pontosan a személyautó informatikai rendszerével és adataival egy szerviz során. Ezt nem csak megfelelő tájékoztatással, de egyes interjúalanyok szerint kifejezetten erre a célra szolgáló archiválóeszközökkel kell biztosítani, azaz lényegében egy az aviatikában is ismert fekete doboz használatára lenne szükség.

Az egyik interjúalany arra világított rá, hogy a Common Criteria szabvány széleskörűbb alkalmazása megoldást jelenthetne a személygépjárművek információbiztonságának termékalapú megközelítésére, azonban ha a szabvány hivatalos weboldalán felsorolt biztosított eszközök listáját megnézzük[15], akkor látható, hogy világviszonylatban csak kevés számú eszköz rendelkezik ezzel a minősítéssel. Ezek nagyrésze pedig valamilyen általános informatikai eszköz például tűzfal.

[15] https://www.commoncriteriaportal.org/products

Az ISO/IEC 21434 szabvány esetében már valóban egy iparágspecifikus szabványról beszélhetünk, azonban nem maga a személygépjármű képezi a vizsgálat objektumát, hanem annak egyes elektronikai részei. Ilyenek lehetnek például a fékeket vezérlő elektronikai alkatrészek, de egy *infotaintment* rendszer *bluetooth* modulja is. A személygépjármű biztonságának szempontjából problémát jelent, hogy nem is minden alkatrésszel kapcsolatban várható el a tanúsítás, így viszont a gyártó igényeitől függően csak „foltszerűen" érvényesül annak hatása. Ez ráadásul nem csak a menedzsment szemléletéből, hanem a szűkös erőforrásokból is fakad, hiszen a szigorú előírásoknak való megfelelés magas költségekkel járhat.

Az átfogó megoldási javaslatok tekintetében szinte minden szakértő egyetértett abban, hogy szükséges lenne egy egységes európai szintű jogszabályra, mely pontosan előírja azoknak a kontrolloknak az alkalmazását a személygépjárműgyártók és beszállítói számára, amik jelenleg a szabványokban szerepelnek. Ehhez kapcsolódva szükségessé válik egy olyan hatóság létrehozása is, amely betartatja a szabályokat. Az egyik interjúalany kitért arra is, hogy amíg a gazdasági tényezők nem ösztönzik a gyártókat a nagyobb körültekintésre, addig a helyzet változatlan marad.

Végül a tíz interjúalanyból három is megoldási javaslatként hivatkozott a felhasználók tudatosságának növelésére. Az interjúalanyok általános vélekedése szerint ugyanis a felhasználót többnyire magát sem érdeklik az információbiztonsági problémák, csak akkor, ha egy eszköz meghibásodik vagy az adataik valóban veszélybe kerülnek, kiszivárognak. Ezzel kapcsolatban sokszínű megoldási javaslatok születtek az általános iskolai edukációtól (például információbiztonsági előadások az informatika órán) kezdve az átláthatóbb tájékoztatószövegek átadásáig.

Egy olyan vélemény is akadt, melynek lényege egyenesen az volt, hogy a fejlett kényelmi és szolgáltatási célú eszközök, gyakorlatok alkalmazását, mint például az ülésfűtés szolgáltatásként való nyújtását, be kéne tiltani a személygépjárművekkel kapcsolatosan. Ennek a gondolatnak a logikai hátterét az adja, hogy az informatika fejlődése ma már olyan méreteket ölt, hogy ennek köszönhetően a biztonsági szakemberek és a szabványok semmiképpen nem tudnak lépést tartani vele.

ÖSSZEGZÉS

Összességében elmondható, hogy a tanulmányban bemutatott szabványok és jogszabályi környezet elsősorban a gyártókat védi, folyamatközpontú és még az olyan célzott szabályok ellenére is, mint a GDPR, kevés hangsúly jut a végfelhasználó adatinak biztonságán. A szabványok nagy része folyamatalapú, a termékközpontú szabványokat pedig a jármű egyes részeire alkalmazzák csak.

A tanulmány első fejezetében bemutattuk a személygépjárművek információbiztonsági szabályozási környezetére vonatkozó szakirodalmi forrásokat, illetve röviden ismertettük a főbb általános és ágazati szabványokat és azok jellemzőit. A második fejezetben röviden vizsgáltuk, hogy az általánosan elterjedt definíciók alapján a személygépjármű tekinthető-e információbiztonsági szempontból IoT eszköznek, melyet a későbbi interjúelemzés során megerősítettünk. A harmadik fejezetben bemutattuk a kutatás módszertani sajátosságait.

A tanulmányban foglalt kvalitatív kutatás célja az volt, hogy a szakirodalomban fellelhető információk megismerése után hazai, tapasztalt szakemberek egy csoportjának véleményével összevetve azokat, megválaszoljuk a két kutatási kérdést:

1. A hazai információbiztonsági szakemberek szerint megfelelő-e a jelenlegi információbiztonsági szabályozási környezet hatékonysága a személygépjárműiparban?
2. Milyen változtatásokkal lehetne hatékonyabbá tenni a személygépjárműiparban alkalmazott információbiztonsági szabványokat és szabályozási környezetet, hogy azok megfelelően védjék ne csak a gyártó, de a felhasználó adatait is?

A 1 kérdés vizsgálata során azt tapasztalhattuk, hogy az interjúalanyok megerősítették és többféle különböző aspektusból is rávilágítottak arra, hogy a személygépjárművekben keletkezett vagy használt adatok biztonságának szabályzása és a folyamatok megfelelő biztosítása kihívást okoz a szakemberek számára. A szabályozási környezet az információbiztonság területén töredezett, sok esetben túlzottan megengedő és ennek megfelelően nem hatékony.

A 2 kérdés vizsgálata során az elemzést bemutató fejezetből kiderült, hogy a szakértők véleménye meglehetősen sokrétű, többen többféle oldalról közelítik a megoldást. Összességében elmondható azonban, hogy a vélemények többsége kettéoszlik: a szakértők a legnagyobb problémát egyrészt a szabványok gyakorlati betartatásában, a megfelelő erővel bíró hatóság hiányában látják, másrészt pedig a felhasználók attitűdjében, tudatosságuk hiányában.

Elmondható, hogy a javasolt megoldások túlmutatnak az információbiztonsági szabályozási intézkedések hatókörén, azonban ettől függetlenül is fontos alapot jelenthetnek mind a további felhasználói attitűdvizsgálatok, mind pedig a szabályok betartásának lehetséges megoldási módjait kereső kutatások számára.

FELHASZNÁLT IRODALOM

[1] Khan, Shah Khalid; Shiwakoti, Nirajan; Stasinopoulos, Peter; Chen, Yilun. „Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. , 148, 105837.," Accident Analysis & Prevention, 2020.

[2] Weimerskirch, A.; Gaynier, R. „An Overview of Automotive Cybersecurity: Challenges and Solution Approaches," 2015.

[3] Koubatis, Andrew; Schonberger, Jorge Yerena. „Risk management of complex critical systems," International Journal of Critical Infrastructures, %1. kötet1(2/3), 2005.

[4] D. Gardner. Risk: The Science and Politics of Fear, New York: Random House, 2009.

[5] Ellerby, Zack; McCulloch, Josie; Wilson, Melanie; Wagner, Christian. „Exploring How Component Factors and Their Uncertainty Affect Judgements of Risk in Cyber-Security," Critical Information Infrastructures Security. Lecture Notes in Computer Science, 1/11777, 2020.

[6] Ji, Zuzhen; Yang, Shuang-Hua; Cao, Yi; Wang, Yuchen; Zhou, Chenchen; Yue, Liang; Zhang, Yinqiao. „Harmonizing safety and security risk analysis and prevention in cyber-physical systems," Process Safety and Environmental Protection, %1. kötet148, 2021.

[7] Ogbuke, Nnamdi Johnson; Yusuf, Yahaya Y.; Dharma, Kovvuri; Mercangoz, Burcu A. „Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society, Production Planning & Control," 2020.
[8] Hofmann, Martin; Neukart, Florian; Bäck, Thomas. „Artificial Intelligence and Data Science in the Automotive Industry," 2017.
[9] M. Marabelli; S. Hansen, S. Newell; C. and Frigerio. „The Light and Dark Side of the Black Box: Sensor-based Technology in the Automotive Industry," Communications of the Association for Information Systems, 40/16, 2017.
[10] Ivanov, Dimitry; Dolgui, Alexandre. „A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0," Production Planning & Control, %1. kötet7287, 2020.
[11] Oliver, N.; Pentland, A. P. „Driver Behavior Recognition and Prediction in a Smart-Car," 2000.
[12] Peppes, Nikolaos; Alexakis, Theodoros; Adamopoulou, Evgenia; Demestichas, Konstantinos. „Driver Behavior Monitoring Based on Smartphone Sensor Data and Machine Learning Methods," in 2019 25th Conference of Open Innovations Association (FRUCT), 2019.
[13] Pereira, Teresa; Barreto, Luis; Amaral, António. „Network and information security challenges within Industry 4.0 paradigm," Procedia Manuf., 1/13, 2017.
[14] Haig, Zsolt, „TISAX, az autóipar új információbiztonsági követelményrendszere," Magyar Minőség, 1. /június, 2020.
[15] Machuletz, D.; Böhme, R. „Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR," Proceedings on Privacy Enhancing Technologies 2020.
[16] Stoica, L. A.; Savu, R. A. C. „RISKS AND EXPLOITS EXPOSED BY GDPR," Eurasian Journal of Social Sciences, 9(1), 2021.
[17] Gladis, A. ; Hartwich, N. J.; Salge, O. „Weaponizing the GDPR: How Flawed Implementations Turn the Gold Standard for Privacy Laws into Fool's Gold," in ICIS 2022, Koppenhága, 2022.
[18] Mouha, R. „ Internet of Things (IoT)," Journal of Data Analysis and Information Processing, 9., 2021.
[19] Szczepaniuk, H.; Szczepaniuk, E. K. Standardization of IoT Ecosystems Open Challenges, Current Solutions, and Future Directions, CRC Press, 2022.
[20] Kelemen-Erdős, Anikó; Mitev, Ariel, „Holisztikus szolgáltatásélmény-vendég-utazás és kölcsönös értékteremtés dimenziói az art-és romkocsmák példáján," Marketing & Menedzsment, 250(3-4), 2016.
[21] Babbie, Earl. A társadalomtudományi kutatás gyakorlata., Balassi Kiadó, 2020.
[22] Kelemen-Erdős, Anikó; Mitev, Ariel. „Tematikus szolgáltatásélmény art-és romkocsma környezetben," Turisztikai és Vidékfejlesztési Tanulmányok, %1. kötet2(3), 2017.
[23] Kelemen-Erdős, Anikó; Molnár, Adél. „Cooperation or conflict? The nature of the collaboration of Marketing and Sales organizational units," Economics and culture, %1. kötet16(1), 2019.
[24] Krippendorff, K. Content Analysis. An Introduction to Its Methodology, Thousand Oaks: SAGE, 2018.