HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 1. szám 109–124.
DOI: 10.32567/hm.2023.1.8

Koller Marco[1]

Okoseszközök mint a személyi hitelesítésre alkalmas interface-technológia biztonsági vetületei

Smart Devices as Security Aspects of Personal Authentication Interface Technology

A pandémia okozta lezárások az élet minden területén arra késztették az embereket, a munkáltatókat és az államokat, hogy a személyi jelenlétet nélkülöző megoldásokat találjanak, így a digitalizáció még inkább előtérbe került. Az elektronikus ügyintézés rendkívül gyors és hatékony megoldást kínálhat a különböző hatósági ügyek rendezésére az állampolgárok számára, azonban számos olyan ügymenet létezik, és nem csak a közigazgatásban, amelyhez személyes jelenlét szükséges a megfelelő hitelesítéshez. Ezt a jövőben kiválthatja egy elektronikus személyi hitelesítésre alkalmas applikáció. Jelen tanulmány során a személyi hitelesítésre alkalmas mobilapplikációk lehetséges magyarországi fejlődését és az abban rejlő kockázatokat mutatjuk be. Az új technológiák szükségképpen új típusú fenyegetéseket hordozhatnak magukban, és a jelen írás során vizsgált technológia jövőbeni nagyarányú elterjedése már nemzeti biztonsági szempontból is releváns tényező.

Kulcsszavak: okoseszközök, információs műveletek, e-közigazgatás, személyi hitelesítés, mobilapplikációk, információs biztonság

The pandemic shutdowns have forced people, businesses, and governments in all walks of life to find solutions that do not require a personal presence, and digitalization has become even more prominent. E-government can offer citizens a very fast and efficient solution to deal with various administrative issues, but there are many procedures, not only in public administration, that require personal presence for proper authentication. This could be replaced in the future by an application for electronic personal authentication. This paper will discuss the possible development of mobile authentication applications in Hungary and the potential of such applications. New technologies may

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: marcoakoller@gmail.com

inevitably bring with them new types of risks, and the future large-scale diffusion of the technology under study in this paper is already a relevant factor from a national security perspective.

Keywords: smart devices, information operations, e-government, personal authentication, mobile apps, information security

Bevezetés

A globalizációban és az egyre inkább digitalizálódó társadalmakban az okoseszközök és az egyes applikációk szerepe felértékelődőben van, és nem csupán a magán, hanem az állami szektorban is. Az egyes szolgáltatásokhoz való hozzáférés csak személyi hitelesítés után lehetséges, amelynek fontossága a különböző visszaélések visszaszorítása miatt kiemelt jelentőségű. Az e-közigazgatás és az elektronikus ügyintézés felhasználóbarát és rendkívül gyors és hatékony megoldást kínálhat a különböző hatósági ügyek rendezésében az állampolgárok számára, ami a jövőben alkalmas lehet a lakosság távoli azonosítással való ügyintézéseihez. Ezeket alapozza meg az e-aláírás, az Ügyfélkapu és az Azonosításra Visszavezetett Dokumentumhitelesítés (AVDH). A Covid okozta járványhelyzet is megmutatta a digitalizáció szükségességét a QR-kóddal[2] ellátott oltási igazolásokkal (EESZT), amelyek segítségével kizárólagosan számos szolgáltatás, köztük a nemzetközi utazás vált elérhetővé a pandémia időszakában.

A fentiek és a későbbiekben kifejtettek alapján nagy valószínűséggel a jövőben a személyi igazolványt és/vagy más személyi hitelesítésre alkalmas dokumentumot helyettesíteni – esetlegesen kiváltani – fog egy applikáció, ahogy a bankkártyák esetében is már megfigyelhető ez a tendencia. A továbbiakban bemutatjuk, hogy az alkalmazásalapú személyi hitelesítési metódus milyen főbb előnyökkel, illetve – információbiztonsági – kockázatokkal jár, mind a felhasználó, mind adott esetben az ország, illetve az eljáró hatóság szempontjából, kiemelt tekintettel az esetlegesen felmerülő információbiztonsági szempontokra és az információs műveletekre. A témakör relevanciáját erősítik az orosz–ukrán háború eddigi tapasztalatai, amelyek jól rávilágítottak arra, hogy az információs műveleteknek kiemelt jelentősége van a 21. század hadviselésében, így az okoseszközök evolúciója mint személyi hitelesítésre alkalmas technológia szükségképpen nemzeti biztonsági kockázatokat, kihívásokat hordoz magában.

Jelen tanulmány célja, hogy a rendelkezésre álló szakirodalom vizsgálatán, a Németországban alkalmazott jelenlegi elektronikus személyi igazolvány és a Horizont 2020 európai uniós finanszírozású SMILE projekt bemutatásán keresztül prezentálja a lehetséges jövőbeni alkalmazásalapú személyi hitelesítési eljárás lehetőségeit és a felmerülő kockázatokat az információs műveletek tükrében.

[2] A QR-kód egy kétdimenziós vonalkód (tulajdonképpen pontkód), amelyet a japán Denso-Wave cég fejlesztett ki 1994-ben. Nevét az angol quick response (gyors válasz) rövidítéséből kapta, egyszerre utalva a gyors visszafejtési sebességre és a felhasználó által igényelt gyors reakcióra. A QR-kód felhasználása könnyű használata miatt egyre jobban terjed az iparban, logisztikában, termelésben. Lásd Bártfai 2021.

Fogalmi háttér

A téma kifejtéséhez és adekvát értelmezéséhez elengedhetetlen a felmerülő fogalmi keret meghatározása, a fontosabb kifejezések definiálása. A tanulmány során így az alábbi fő fogalmak merültek fel: információs műveletek, okostelefonok, okoseszközök, e-közigazgatás és m-közigazgatás, amelyeket az alábbi alfejezetekben fejtünk ki.

Információs műveletek

Az információs műveletek nem más, mint az információért folyó küzdelem, olyan összehangolt tevékenységek, „amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire".[3] Az információs műveletek a szakirodalom alapján három dimenzióban folyhatnak:

- a fizikai dimenzióban;
- az információs dimenzióban;
- a kognitív (tudati) dimenzióban.

A fizikai dimenzió

Az információs infrastruktúrák és az infokommunikációs rendszerek egyes elemei ellen elkövetett fizikai (úgymond a valóságban megjelenő) támadásokat értjük, továbbá az előbbiek elleni védelmet is magában foglalja.[4]

Az információs dimenzió

Az elektronikus információs folyamatoknak elektronikai úton való, korlátozó hatású támadását jelenti fizikai ráhatás nélkül közvetlen befolyásolás érdekében. Ide tartozik a saját elektronikus információs folyamatokra irányuló támadások elleni védekezés is. Jelen tanulmány szempontjából álláspontom szerint az információs dimenzióban megvalósuló információs műveletek állnak kiemelt szerepkörben.[5]

A kognitív (tudati) dimenzió

Közvetlenül az emberi gondolkodást (észlelést, véleményt, vélekedést) veszik célba e dimenzióban, valós, csúsztatott vagy hamis információkkal.[6]

[3] Haig 2018: 15.
[4] Haig 2006.
[5] Haig 2006.
[6] Haig 2006.

Okostelefon, okoseszköz

„Az okostelefon egy olyan mobilkészülék, amelynek kijelzője érintőképernyős, a mindennapi használat folyamán a felhasználó elsődleges telefonkészülékeként működik. Lehetővé teszi a fejlett internetalapú szolgáltatásokhoz való hozzáférést, és számos tekintetben a számítógépekhez hasonló funkciókat képes ellátni. Olyan operációs rendszerrel rendelkezik, amely képes alkalmazások letöltésére és futtatására még akkor is, ha azok külső fejlesztőktől származnak."[7]

Természetesen a témában több fogalom is létezik, azonban bármelyiket is fogadjuk el, közös nevezőként merül fel az alkalmazások megléte.[8] A fentiek alapján megállapítható, hogy okoseszköznek nevezhető minden olyan készülék, amely az eredeti tárgyhoz képest (hűtő, tv stb.) olyan extra kényelmi funkciókkal rendelkezik, amelyek külön alkalmazás(ok)on keresztül valósulhatnak meg, illetve az internethez csatlakozik.

E-közigazgatás és m-közigazgatás

A közigazgatási szolgáltatások igénybevételének módja szerint három szolgáltatási rendszert különböztethetünk meg:

- „hagyományos" szolgáltatás (személyes ügyintézés);
- elektronikus közigazgatási szolgáltatások (e-közigazgatás);
- m-közigazgatás.[9]

Az elektronikus ügyintézés a közigazgatási ügyek elektronikus úton való elvégzését elsősorban az elektronizált, online szolgáltatásokat érthetjük (például Ügyfélkapu). Az m-közigazgatás az e-közigazgatás részeként is tekinthető, azonban sajátosságai miatt önálló szolgáltatási rendszert képez. Alapvetően három kategóriát különböztethetünk meg:

- SMS-alapú értesítések;
- mobiltelefonos fizetés; és
- mobilapplikációk.[10]

Jelen tanulmány szempontjából különösen relevánsak az applikációalapú m-közigazgatási szolgáltatások. Az alkalmazások a mobil eszköz beépített képességeit használják (például kamera, GPS, névjegyzék, NFC[11] stb.) A közigazgatási mobilapplikációknak alapvetően két nagy csoportja van: informatív alkalmazások és az ügyintézésre szolgáló programok.[12]

---

7 Eriksson 2017, Fordítva: Beláz 2020: 30–31.
8 Bányász 2014.
9 Beláz 2020: 34.
10 Beláz 2020: 37.
11 Near-field communication: rövid hatótávú kommunikációs szabványgyűjtemény okostelefonok és hasonló (általában mobil) eszközök között, egymáshoz érintéssel vagy egymáshoz nagyon közel helyezéssel (maximum pár centiméter) létrejövő rádiós kommunikációra.
12 Beláz 2020: 41.

Jelenlegi magyar eSzemélyi igazolvány

A magyar elektronikus személyi igazolványt (eSzemélyi igazolvány) 2016-ban vezették be, amely egy olyan kártyaalapú dokumentum, amely egy tárolóelemmel rendelkezik és elektronikus ügyintézési szolgáltatás használatára, illetve elektronikus aláírás alkalmazására is képes.[13] 2022. március végén bevezettek egy fejlesztést az eSzemélyi kapcsán, amely sokkal inkább azokat a perspektívákat tárja fel, amelyeket jelen írás is feszeget, ami nem más, mint a személyi igazolvány mobilapplikációként való megjelenése. A jelenlegi fejlesztés által, az újonnan létrejött eSzemélyi applikáción keresztül az NFC-képes mobiltelefon már kártyaolvasóként is használható, így az applikációval az eSzemélyihez kapcsolódó elektronikus funkciók és szolgáltatások válnak elérhetővé. (például megtekinthetők az okmány chipjén tárolt adatok, ellenőrizhető az elektronikus funkciók státusza, aktiválhatók és módosíthatók az okmányhoz kapcsolódó PIN-kódok).[14] Azonban a jelenlegi fejlesztés még nem teszi lehetővé, hogy az applikáción keresztüli személyes megjelenést igénylő ügyben tudjon kérelmezni az ügyfél, csupán az eddig alkalmazott kártyaolvasó készülék helyett merült fel egy könnyebben beszerezhető alternatíva. Ez egyelőre még nem az a személyi hitelesítésre alkalmas applikáció, amelynek jövőbeli alkalmazása számos lehetőséget és kockázatot hordoz magában, viszont felmerülhet már annak a lehetősége, hogy a jelenlegi alkalmazást új funkciókkal látják el, amit erősít az a hír, hogy Magyarország 2023-ban megteremti a magyar digitális állampolgárság kereteit, amelynek révén legkésőbb 2026-ig az állampolgárok minden olyan jogosultsággal és ügyintézési lehetőséggel rendelkeznek majd a digitális térben, mint a fizikai valóságban.[15] Ez pedig azt jelenti, hogy pár éven belül minden, ami a személyi azonosításhoz szükséges, az mobiltelefonon keresztül is elérhető lesz. Továbbá az applikációt fejlesztő IdomSoft Zrt. honlapján is az szerepel, hogy: „Az eSzemélyi igazolvány működése tehát egyfajta kapu, a kártya pedig egy hozzáférést biztosító eszköz, amely az elektronikus közigazgatási szolgáltatások folyamatosan bővülő körének elérését biztosítja. Sőt a jövőben ezek a lehetőségek piaci szolgáltatóknál is elérhetők lesznek, az erre irányuló fejlesztések már folynak."[16] A fentiek miatt kiemelten szükséges vizsgálni az okoseszközök mint személyi hitelesítésre alkalmas interface-technológia evolúcióját, kiemelten annak társadalmi elfogadottságára, illetve a benne rejlő kockázatokra és lehetőségekre.[17]

A személyi hitelesítésre alkalmas applikáció jövője Magyarországon

A következőkben az eSzemélyi, vagy más személyi hitelesítésre alkalmas applikáció közeli jövőjét, legvalószínűbb fejlődési trendjét fogom vizsgálni nemzetközi kitekintéssel.

[13] Ormai 2022b.
[14] Ormai 2022a.
[15] Schopp 2022.
[16] Lásd: https://idomsoft.hu/elektronikus-szemelyi-igazolvany
[17] Jelen témakör a szerző doktori kutatási témáját képezi, amellyel kapcsolatban készíti el a tárgykör lefedését célzó doktori disszertációját.

Németországban már alkalmazott applikáció

Németországban már megjelent az okostelefonok NFC-funkciója által, e-személyi igazolvánnyal való online személyazonosítás. Az azonosítás személyi igazolvánnyal és okostelefonnal történik, amely során az AusweisApp2 elnevezésű alkalmazás megerősíti az ügyfelek digitális személyazonosságát AusweisIDent rendszeren keresztül. A rendszert a D-Trust és a Governikus fejlesztette ki, amelyet a német Szövetségi Információbiztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik, BSI) is akkreditált.[18] A BSI a biztonságos digitalizáció fő tervezője Németországban, egyik alapvető feladata a kormányzati hálózatok és a szövetségi közigazgatás elleni kibertámadásokkal szembeni védelem.[19]

Jól látható, hogy Németországban már létezik olyan technológia, amely által online tudja magát azonosítani az adott személy egy kártyaalapú személyi igazolvány, illetve egy applikáció segítségével, amely az okostelefon NFC-funkcióját alkalmazza, mivel az NFC-képesség az, amely egy okoseszközt (okostelefont, okosórát) olyan szerkezetté alakíthat, amely alkalmas lehet különféle termékek, például tömegközlekedési jegyek/bérletek, belépő- és bankkártyák szimulálására.[20]

Figyelemre méltó körülményként értékelhető, hogy az újonnan létrejött magyar eSzemélyi applikáció már szintén a telefonok NFC-funkcióját használja, azonban a hazai alkalmazással még nem képes az állampolgár távolról hitelesíteni magát, azonban ennek elérése egyáltalán nem tűnik távolinak. A fentiek alapján vélelmezhető, hogy a Németországban már használt technológiát hazánkban is alkalmazni fogják a közeli jövőben.

Horizont 2020 – SMILE projekt

A témakör szempontjából figyelmet érdemlő kutatás a Horizont 2020 – SMILE projekt. A „SMILE" mozaikszó a „Smart mobility at the european land borders", azaz az *Európai szárazföldi határok okos mobilitásfejlesztése* cím betűiből tevődik össze.[21] A projekt hivatalosan 2017. július 1-jén indult el egy 14 tagot egybefogó konzorcium összehangolt tevékenységével. A projekt teljes költségvetése 4 999 276,25 euró, futamideje 36 hónap, a szerződés szerinti befejezés dátuma 2020. június hó vége. A SMILE projekt általános és részletes megvalósíthatósági, specifikációs célkitűzései rendkívül széles körűek, továbbá számos elem üzleti titok vagy minősített adat, amelynek nyilvánosságra kerülése veszélyeztetné a rendszer hatékony jövőbeli alkalmazását. Ennek okán a projekt alapvető elgondolását és fejlesztési célkitűzéseit ismertetem.[22]

A projekt a koncepció úgynevezett 6-os technológia érettségi szint (TRL 6) elérését tűzte ki célul. A TRL 6 szinten a technológiát már valós környezetben mutatták be, a technológia tesztelését reális, életszerű, de még szimulált szcenáriókban

[18] D-Trust, lásd: www.d-trust.net/en/solutions/ausweisident-online
[19] BSI, lásd: www.bsi.bund.de/EN/Das-BSI/Auftrag/BSI-Kurzprofil/kurzprofil_node.html
[20] Cavoukian 2011, Fordítva: Juhász-Nagy 2021.
[21] Európai Bizottság CORDIS, lásd: https://cordis.europa.eu/project/id/740931
[22] Zsákai 2019: 38.

végezték.[23] A projekt alapelgondolása a szárazföldi határforgalom-ellenőrzéshez[24] szükséges erők, eszközök és költségek csökkentését vette alapul, szem előtt tartva a schengeni térség biztonságát is természetesen.[25] A koncepció jelenleg alkalmazott fejlettségi szintet meghaladó minőségű és szintű infokommunikációs technológiák alkalmazását vette célul. A projekt egy prototípus-eszközkészletet valósított meg a gyorsabb és biztonságosabb szárazföldi határátlépés elősegítése céljából. A SMILE konzorciumi megállapodásban[26] is nevesített legfőbb célkitűzései közül az alábbiak, amelyek kiemelten relevánsak jelen tanulmány szempontjából:

- biometrikus adatok feltöltésének lehetőségével kialakított előregisztrációs rendszer létrehozása;
- hordozható személy- és okmányazonosító eszközök bevezetése és az elektronikus szolgáltatások kiterjesztése a közúti határátkelőhelyeken;
- biometrikus azonosítókon alapuló, hatékony személyazonosítási és adathitelesítési keretrendszer kifejlesztése;
- egy független, felhőalapú biztonsági infrastruktúra alapjainak kidolgozása, amely az utasok digitálisan tárolt adatainak biztonságos tárolására, megőrzésére irányul mind nemzeti, mind európai szinten.[27]

A kialakított rendszerben lehetőség nyílik a fentiekben már nevesített, a határátkelést megelőző, úgynevezett előregisztrációra is, amely biztosítani tudja az utasok számára az összes, utazással kapcsolatos kiemelt információt (például jogok és kötelezettségek, forgalom helyzete stb.). A SMILE segítségével a hatóságok hatékonyabban tudnak gazdálkodni az erőforrásaikkal, tekintettel arra, hogy a rendszer segítségével tudhatják a különböző időpontokban várható utazók számát, ennek megfelelően módosíthatják az alkalmazandó élőerőt. A fentieken túlmenően a SMILE-rendszer értesítheti az előre regisztrált személyeket, amennyiben sok utas várható az általuk megjelölt érkezési idősávban, így javasolhat egy tehermentesebb időpontot.[28]

A projekt számos felhasználói, illetve hatósági szempontból hasznos és kiemelkedő teljesítményt tudhat maga mögött, jól látható, hogy az alkalmazott applikáció a hagyományos úti okmányokat egészíti ki plusz funkciókkal, nem váltja ki egészében, hiszen az ügyfelek szempontjából egy kényelmi funkciót ellátó kvázi előregisztrációs rendszer.

[23] Lásd: www.h2020.gov.hu/hogyan-palyazzunk
[24] A Schengeni határ-ellenőrzési kódex értelmében a határforgalom-ellenőrzés a határátkelőhelyeken végzett ellenőrzés annak megállapítására, hogy a személyek, beleértve az azok birtokában lévő közlekedési eszközöket és tárgyakat, beléptethetők-e a tagállamok területére, illetve elhagyhatják-e azt.
[25] Balla 2017.
[26] Grant Agreement, number: 740931 – SMILE – H2020-SEC-2016-2017/H2020-SEC-2016-2017-1.
[27] Zsákai 2019: 39.
[28] Zsákai 2019.

A technológia alkalmazása során felmerülő kérdéskörök

Az okoseszközök mint személyi hitelesítésre alkalmas interface-technológia esetén kérdésként merülhet fel több tényező, amelyek során az alábbiakat emelném ki a feldolgozott szakirodalom alapján:

- Maga az eszköz (hardver) és a szoftver fejlesztőjének kiléte. Vagyis az alkalmazott okoseszköz, továbbá az applikáció fejlesztőjének, gyártójának és karbantartójának személye. Ugyanis az ilyen érzékenységű, adott esetben biometrikus adatokat kezelő, állampolgári jogosítványokat biztosító, azokat igazoló szolgáltatás esetén az államnak mindenképpen szerepet kell vállalnia, azonban ennek mélysége, miléntje lehet kérdéses.
- Közeli vagy távoli hitelesítést tesz lehetővé a technológia. Azaz kell-e személy jelenlét az egyes ügymeneteknél és csak a kártyát hitelesíti az eszköz, vagy pedig már személyes jelenlét sem kell, az applikáció (és az e-személyi) hitelesít bennünket.
- Adott esetben a hitelesítés során alkalmazott applikációnál minden esetben szükséges-e az elektronikus tárolóval ellátott személyi okmányt érintkeztetni, amennyiben az ember hitelesíteni szeretné magát, vagy elég egyszer „beregisztrálnia" magát a felhasználónak, onnan pedig az alkalmazás használta más metódussal azonosítani magát (PIN-kód, biometria stb.).

Jelen kérdéskör hosszabb elemzése, illetve az egyes eshetőségek modellezése terjedelmi korlátok miatt nem képzik jelen tanulmány részét. A továbbiakban a rendelkezésre álló szakirodalom és a német példa alapján végzett elemzés szerinti legvalószínűbb eshetőséget mutatjuk be.

A közeljövőben megvalósuló legvalószínűbb fejlődési irány

A fentiekben kifejtettek alapján álláspontom szerint a közeli jövőben (nagyjából 2 éven belül várhatóan) hazánkban a jelenlegi eSzemélyi applikáció olyan irányba fejlődhet, alakulhat át, hogy távoli hitelesítést lehetővé tevő alkalmazássá válik, amely a telefon NFC-funkcióját használja és leolvassa a személyi igazolvány tanúsítványát, és hitelesíti az adott állampolgárt a különböző ügymenetekben. Az applikáció jelen esetben maradna a jelenlegi fejlesztőé (az állami hátterű IdomSoft Zrt.),[29] illetve az alkalmazott eszköz is (azaz NFC-funkcióval rendelkező okoseszköz). Jól látható, hogy a legvalószínűbb fejlődési esetben szoftveres részről egy kvázi állami szolgáltató működne közre, hardveres részről viszont különböző hátterű magánvállalkozások, annak függvényében, hogy az adott felhasználó milyen gyártmányú okoseszközt (például Apple, Samsung, Huawei stb.) alkalmaz. Esetlegesen felmerülhet annak a lehetősége, hogy a hardverek kapcsán az állam iránymutatást adjon ki, hogy mely típusú és gyártmányú eszközök számítanak biztonságosnak. Ennek kapcsán valószínűsíthetően egy kormányhatározat születhetne, illetve az NBSZ Nemzeti Kibervédelmi Intézet és a magánszféra szakmai

[29] Lásd: https://idomsoft.hu/elektronikus-szemelyi-igazolvany

véleményének kormányzati döntéshozatalba való becsatornázására létrehozott[30] Kiberbiztonsági Fórum adhatna ki egy közös állásfoglalást. Egy ilyen ajánlás kifejezetten azokra a szereplőkre lehetne kötelező érvényű, akik az állam működésének szempontjából kiemelt létesítményekben dolgoznak (például minisztériumok, központi költségvetési szervek stb.), amíg az átlagos felhasználó számára csupán biztonságtudatossági iránymutatás lenne. Ennek szükségességét az adja, hogy az államigazgatás és más nemzeti biztonsági szempontból releváns kiemelt szereplők magasabb szintű kockázatnak vannak kitéve egy esetleges információs művelettel szemben, amely kockázat az adott esetben akár a nemzetbiztonságot is veszélyeztetheti.

Felmerülő jövőbeli lehetséges kockázatok és kihívások

Jelen tanulmány során a Bányász Péter által is alkalmazott felosztást fogom használni, amely a felmerülő kockázatokat kvázi azok „eredete/ helye" alapján kategorizálta az alábbiak szerint: adatátvitelből, alkalmazásokból (szoftver), a hardverből (magából az eszközből), az operációs rendszerből és a felhasználói szokásokból.[31]

Adatátvitel folyamatában rejlő biztonsági kockázatok

Adatátvitel alatt bármilyen információk egyik helyről egy másikra való továbbítását értjük, amely lehet vezetékes vagy vezeték nélküli. A vezeték nélküli adatátvitel történhet többek között Bluetooth, mobilinternet vagy wifihálózat segítségével. Ezek különböző kockázatot jelenthetnek. A Bluetooth sebezhetősége kapcsán a BlueBorne támadóvektort érdemes megemlíteni, amely távoli hozzáférést biztosít a készülékhez.[32] Jelen tanulmány szempontjából kifejezetten releváns az NFC-funkció sérülékenységét vizsgálni, amely kapcsán a rádiófrekvenciás átvitelből az alábbi kockázatok állapíthatók meg:

- „Könnyen lehallgathatók az üzenetek,
- zavarható a csomagok átvitele,
- esetleg részben vagy egészében meghamisíthatók a közlekedő adatcsomagok."[33]

A folyamatosan bekapcsolt NFC-vel fokozott biztonsági kockázatnak tesszük ki az okoseszközünket és saját magunkat.[34] Erre példaként szolgál a darmstadti egyetem kutatói által készített elemzés, amely megállapította, hogy az iPhone-ok (13-as széria) akkumulátorkímélő üzemmódja komoly biztonsági kockázatokat rejt magában, ugyanis esetében a Bluetooth és az NFC típusú kommunikációs rendszerek a készülék

[30] Lásd: https://nbsz.gov.hu/tevekenyseg-mukodes/nemzeti-kibervedelmi-intezet
[31] Bányász 2018a: 368.
[32] Bányász 2018a.
[33] Juhász-Nagy 2021.
[34] Juhász-Nagy 2021.

kikapcsolása után is aktívak maradnak, és rosszindulatú szoftverek futtatására is módot adhatnak a kikapcsolt készülékeken.[35]

Az alkalmazásokban (szoftverben) rejlő kockázatok

A készülékre telepített alkalmazások a kockázatok széles tárházát nyitják meg. A támadók gyakran másolnak le népszerű alkalmazásokat, amelyekben elrejtik a kártékony kódokat, vagy az eredeti alkalmazásokat fertőzik meg.[36] Az okostelefonok esetében is gyakoriak az úgynevezett zsarolóvírusok, amelyek a megfertőzött készülékek tartalmát titkosítják, a feloldásért cserébe pedig pénzt követelnek.[37] Egy olyan applikáció esetében, amely biometrikus azonosítóinkat tartalmazza, kvázi a közigazgatás bizonyos szegmenséhez való hozzáférésünket blokkolja, az esetleges zsarolások kifizetése iránti hajlam is megnőhet.

Tekintettel arra, hogy ezek az eszközeinkre telepített alkalmazások sokfélék, számos kockázatot rejtenek magukban. Ezeket többféle módon lehet kategorizálni.[38] A Haig Zsolt által összefoglalt az infokommunikációs rendszerek elleni fenyegetések közül az alábbiakat kell kiemelni a témakör szempontjából:

- „illetéktelen hozzáférés az információkhoz, vagy illetéktelen adatbevitel,
- rosszindulatú szoftverek bevitele a rendszerbe, ezáltal megváltoztatva, vagy lehetetlenné téve annak működését. Ezek a szoftverek különböző vírusok, »logikai bombák« és szoftverek lehetnek, melyek a védelmi programokat (tűzfalakat, víruskeresőket) kikerülve kerülnek a rendszerbe,
- rosszindulatú szoftverek útján az adatbázis lerontása, módosítása, felhasználhatatlanná tétele,
- elektronikai felderítés útján az infokommunikációs rendszer adatainak megszerzése."[39]

A fenti rendszerezés alapján egy olyan alkalmazás, amely használható személyünk azonosítására, járhat azzal a kockázattal, hogy valaki illetéktelenül fér hozzá adatainkhoz, azokat illetéktelenül használja fel. Azonban figyelemre méltóbb léptékű kockázat, ha egy elterjedt rendszer vírusos támadása esetén az alkalmazott ügymenet megbénul, esetlegesen a hatóság adatbázisaihoz való hozzáférés, amely esetén nem csupán illetéktelen személyek juthatnak adatainkhoz vagy módosíthatják őket, hanem hamis alteregókat is létrehozhatnak, így az okmányhamisítás új módja lépne életbe, sőt felmerülhet annak a lehetősége is, hogy egy ellenérdekű ország titkosszolgálata ezt kihasználva hozna létre fedést saját állománya részére.

[35] Nemzeti Kibervédelmi Intézet 2022a.
[36] Bányász 2018a: 372.
[37] Bányász 2019: 53.
[38] Bányász 2018a.
[39] Haig 2006.

A hardver kockázati elemei

A hardverben rejlő kockázatok kapcsán álláspontom szerint a legfőbb kategorizálási alap, hogy az adott hardveres hibát, amely miatt kompromittálódott a készülék, direkt építették be, vagy sem (például hátsókapu [backdoor]: olyan szoftverbe vagy hardverbe épített eljárás, amelynek segítségével ki lehet kerülni az adott entitás hitelesítési eljárásait).[40] A nem tudatos hardveres kockázatra kiváló példa, amikor 2018-ban kiderült, hogy az Intel, az ADM és ARM processzorok igen súlyos biztonsági rést tartalmaztak, amelyek kihasználásával hozzáférhettek az eszközök memóriájában tárolt adatokhoz.[41] Ezek a Spectre és Meltdown elnevezésű chipszintű sebezhetőségek voltak, amelyek lehetővé tették, hogy hozzáférjenek az adott telefon memóriájához, amely érzékeny információkat, például jelszavakat tartalmazott.[42]

A másik eshetőség, hogy a hardver szándékosan biztosít adatokat, hozzáféréseket a felhasználón kívüli entitásnak, akár nem állami vagy állami szereplőnek. Mint az már szinte köztudott ebben a tárgykörben, az állami szereplők esetén mindenképpen ki kell emelni Kínát. Greg Schaffer az amerikai Department of Homeland Security kiberbiztonsági igazgatóságának helyettes államtitkára már 2011-ben nyilvánosan arról beszélt, hogy egyre nagyobb kockázatot jelentenek a külföldről, például Kínából vásárolt hardverek.[43] A kockázatokat konkrétabban árnyaló 2021-es keletkezésű hír szerint, a német Szövetségi Információbiztonsági Hivatal (BSI) vizsgálatot indított kínai gyártmányú mobiltelefonok kiberbiztonságát illetően, mivel a litván kiberbiztonsági központ jelentése szerint a kínai gyártmányú Xiaomi és Huawei telefonokban beépített cenzúrafunkciók voltak találhatók, amelyekkel akár távoli hozzáféréssel lehetett cenzúrázni a kínai vezetésnek nem tetsző keresési kifejezéseket, de szakértők felhívták a figyelmet arra, hogy az igazi kockázatot az jelentheti, hogy ezen eszközök más rejtett funkciókat is tartalmazhatnak, akár a kommunikáció megfigyelésére is alkalmas képességet. Az eset kapcsán az is kiemelendő, hogy BSI szóvivője elmondta, hogy a német szövetségi hatóságok már jó ideje nem vásárolnak kínai készülékeket szolgálati célra.[44]

Az operációs rendszerekben rejlő kockázati elemek

Az operációs rendszer (speciális keretprogram, amely koordinálja és vezérli a hardver erőforrásait)[45] számos sebezhetőséget rejthet magában, amelyre a különböző gyártók frissítéseket bocsátanak ki, kiiktatva a felmerülő biztonsági réseket. Ezért nem szabad megfeledkezni az úgynevezett nulladik napi sebezhetőségről, amely olyan biztonsági fenyegetés, amelynek során a támadók egy számítógépes rendszernek még a fejlesztők

40 Muha–Krasznay 2018: 68.
41 Bányász 2018: 373.
42 Nemzeti Kibervédelmi Intézet 2022b.
43 Dajkó 2011.
44 Nemzeti Kibervédelmi Intézet 2021.
45 Fazekas 2003.

által sem ismert sebezhetőségét használják ki,[46] így egy személyi hitelesítésre alkalmas applikáció hozzáférhetővé tétele előtt számos tesztet kell végrehajtani, mint amilyen a SMILE projekt esetében meg is volt. Azonban a megfelelő mennyiségű tesztelés sem zárja ki egy esetleges hiba fennállását, főként nem a felhasználók biztonságtudatossági magatartásának hiányát.

A felhasználóban rejlő kockázati faktor

Már-már közhelynek számít, de igaz, hogy a világ legerősebb fizikai és logikai védelmével lehet ellátva egy adott alkalmazás, rendszer, vagy bármilyen technológia, a humán tényező mindig lehet gyenge pont.[47] A felhasználó mint biztonsági faktor két irányból is megközelíthető: egyrészt ha az adott eszköz vagy rendszer elleni támadás egy – vagy több – felhasználó által elkövetett figyelmetlenség, azaz az adott személy részéről indirekt károkozás miatt valósul meg. Másrészt megvalósulhat (kifejezetten több felhasználót is magában foglaló rendszerek esetén például egy multinacionális vállalat vagy egy önkormányzat hálózata) szándékos károkozás által is. Első esetre példa lehet egy kéretlen e-mail megnyitása és azzal egyidejűleg valamilyen káros kód letöltése, de az úgynevezett social engineering is ebbe a kategóriába esik, amikor a támadók az információbiztonságot nem, vagy csak nagyon kevéssé ismerő, jóhiszeműen együttműködő személyektől szereznek információt valamilyen pszichológiai manipulációval.[48]

A szándékosan elkövetett károkozás esetében az adott információs rendszer vagy annak tartalma ellen elkövetett cselekmény tudatos, a hátrányos következmény bekövetkezésével, vagy annak nagyfokú kockázatával a felhasználó tisztában van, azonban valamilyen oknál fogva a támadókat segíti. A legkönnyebben elképzelhető példa erre, ha anyagi támogatásért cserébe az információs rendszerhez hozzáférést biztosít egy jogosulatlan személy részére. Természetesen előfordulhat, hogy más indíttatásból segédkezik az adott személy (például zsarolás, jövőbeli előny reménye stb.), azonban a közös momentum a cselekmény természetének ismerete. A felhasználói attitűd kifejezetten releváns kockázat lehet egy személyi hitelesítésre alkalmas applikáció esetében, tekintettel arra, hogy az applikáció adatbázisához való hozzáférés vagy egy hamis alteregó létrehozása, esetlegesen egy magas beosztású személy profiljának ellopása vagy lemásolása több állami, vagy nem állami (például kiberbűnözők anyagi haszonszerzés érdekében) szereplő érdekében állhat. Egy adott állam megszerezheti a kiberfölényt egy másik állammal szemben, amennyiben hozzáfér annak hitelesítésre alkalmas technológiájához és a mögötte álló adatbázishoz. Haig Zsolt a kiberfölény kivívásának és megtartásának három egyenrangú és egymással szoros kapcsolatban lévő elemét különbözteti meg:

[46] Marsi 2018: 42.
[47] Bányász 2018b.
[48] Bányász–Bóta–Csaba 2019.

- „a különböző elektronikai és informatikai adatgyűjtő eszközökkel, szenzorokkal, valamint kommunikációs eszközökkel az információ biztosítása a másik fél képességeiről, a saját lehetőségekről és a környezetről;
- a másik fél hálózatos infokommunikációs rendszerei működésének akadályozása, az információ feldolgozásának, továbbításának korlátozása és megnehezítése, valamint a döntéshozók és a személyi állomány infokommunikációs hálózatokon keresztüli befolyásolása;
- a saját hálózatos információs képességek, valamint a saját döntéshozók és a személyi állomány védelme a másik fél hálózaton keresztül megvalósított különböző logikai és fizikai (elektronikai) támadásaival, valamint befolyásolási kísérleteivel szemben."[49]

A fentiek alapján is jól látható, hogy az állampolgári személyi hitelesítésre alkalmas technológia védelme kulcsfontosságú a 3. pont szerint, az első kettő pont szempontjából pedig a másik államnak az érdeke, hogy megszerezze, ezáltal akadályozza vagy befolyásolja a személyi hitelesítésre alkalmas rendszert. A fentieket továbbá súlyosbíthatja, ha a jövőben nem csupán a személyünk hitelesítésére lesz alkalmas ez a technológia, hanem az perszónák által betöltött szerepkörök, attribútumok igazolására is képes lesz (például ügyvéd, igazságügyi szakértő, bíró stb.).[50]

Az előbbieket jól szemlélteti és a témakör aktualitását is reprezentálja egy 2022 októberében napvilágot látott hír, miszerint a korábbiakban is már említett, a német BSI vezetője, Arne Schoenbohm esetében felmerült, hogy kapcsolatba került az orosz biztonsági szolgálatokkal.[51]

Összefoglalás és értékelés

Jól látható, hogy az m-közigazgatás korunk társadalmának nem csupán jövője, hanem már jelene is, ezért az egyes applikációk fejlődése elkerülhetetlen, feltételezhetően lesz személyi hitelesítésre alkalmas interface-technológia az okoseszközökben, ami megkönnyítheti az egyes ügyintézéseket, akár a határátkelést is. Az újfajta technológia újfajta kockázatokkal jár, így a biometrikus adatainkat, már-már a személyazonosságunkat tartalmazó alkalmazások kompromittálása komoly következményekkel járhat.

Az információbiztonság területén olyan megoldásokat kell keresni, amelyek az információs infrastruktúrák és rendszerek teljes spektrumát lefedik a biztonság oldaláról. Ezáltal biztosítható csak az információs sértetlenség, a fenyegetettség és sebezhetőség csökkentése. A fentiek mellett szükséges a felhasználók biztonságtudatosságának fejlesztése, mert, bármennyire is jól védett lehet egy adott alkalmazás és megfelelően lett fejlesztve, ha az adott személy gondatlansága okán lesz sebezhető a készülék.

A jelenleg alkalmazott technológiai megoldások és jogszabályi környezet között az eSzemélyi kizárólag természetes személyek azonosítására alkalmas, céges képviseletre

[49] Haig 2018: 234–235.
[50] Ormai 2022a.
[51] Reuters 2022.

nem használható. Habár jelentős nóvum lehetne, ha személyihez kapcsolhatók lennének a birtokos által betöltött különböző funkciók is (igazságügyi szakértő, ügyvéd, cégvezető stb.), ezek az úgynevezett attribútumtanúsítványok, az további biztonsági kockázatot hordozna magában.

A felhasználói biztonságon túlmenően kiemelt figyelmet érdemel maga a szolgáltató, ez esetben az állam érintettsége. Egy a fentiekben kifejtetett szoftver, illetve a hozzátartozó adatbázis ellen, az információs dimenzióban elkövetett információs művelet által akár a szervezett bűnözői hálózatok, vagy ellenérdekelt államok is hozzáférhetnek az adott nemzet állampolgárainak adataihoz, amelyeket különböző módokon tudnának felhasználni. A fentieken kívül kiemelendő a hamis adatok bevitele egy ilyen adatbázisba, amivel álszemélyiségek is létrehozhatók különböző célokkal.

Felhasznált irodalom

Balla József (2017): A schengeni elvek szerinti határforgalom-ellenőrzés tartalmi elemei Magyarországon 2016-ban. *Magyar Rendészet,* 17(3), 13–30. Online: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1903

Bányász Péter (2014): A közlekedést támogató alkalmazások biztonsági aspektusai. In Horváth Attila – Bányász Péter – Orbók Ákos (szerk.): *Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről.* Budapest: Nemzeti Közszolgálati Egyetem, 49–72.

Bányász Péter (2018a): Az okos mobil eszközök biztonsága. *Hadmérnök,* 13(2), 360–377.

Bányász, Péter (2018b): Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 6(1), 2–19. Online: https://doi.org/10.32561/nsz.2018.1.4

Bányász Péter (2019): Az okos mobil eszközök jelentette kiberbiztonsági kihívások. In Bányász Péter – Szabó András – Orbók Ákos (szerk.): *Okoseszközök – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában résztvevő személy számára 2016.* Budapest: Nemzeti Közszolgálati Egyetem, 49–69.

Bányász Péter – Bóta Bettina – Csaba Zágon (2019): A social engineering jelentette veszélyek napjainkban. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében*. Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Bártfai Endre (2021): A távolságtartás, mint marketing: a QR-kód sikerének okai. *Jogkövető,* 2021. június 23. Online: https://jogkoveto.hu/tudastar/qr-kod-sikere

Beláz Annamária (2020): Appok a közigazgatásban. In Sasvári Péter (szerk.): *Informatikai rendszerek a közszolgálatban II.* Budapest: Dialóg Campus, 29–50. Online: https://doi.org/10.36250/00733.00

Cavoukian, Ann (2011): Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private. Ontario: Information and Privacy Commissioner. Online: www.rfidjournal.com/wp-content/uploads/2019/07/386.pdf

Dajkó Pál (2011): Nemzetbiztonsági kockázat lehet az importált hardver. *ITcafé,* 2011. július 12. Online: https://itcafe.hu/hir/import_hardver_usa_virus_kockazat.html

Eriksson, Fredrik (2017): ITU Expert Group on Household Indicators (EGH). Background Document 3 Proposal for a Definition of Smartphone. Online: https://bit.ly/3JR4AhR

Európai Bizottság CORDIS: *SMart mobILity at the European land borders*. (2022. augusztus 17.). Online: https://doi.org/10.3030/740931

Fazekas Gábor (2003): *Operációs rendszerek (oktatási segédanyag)*. Debrecen: Debreceni Egyetem Informatikai Intézet, mobiDIÁK könyvtár. Online: https://arato.inf.unideb.hu/fazekas.gabor/oktatas/sajat/Op_rendszerek_Fazekas_Gabor.pdf

Grant Agreement, number: 740931 – SMILE – H2020-SEC-2016-2017/H2020-SEC-2016-2017-1.

Haig Zsolt (2006): Az információbiztonság komplex értelmezése. *Hadmérnök,* (különszám), 1–9. Online: www.hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.pdf

Haig Zsolt (2018): *Információs műveletek a kibertérben.* Budapest: Dialóg Campus.

Juhász-Nagy Attila (2021): Mobilfizetési megoldások biztonsági kockázatainak elemzése. In Varga Anikó – Virág Nándor (szerk.): *Eötvözet 9. Az Eötvös Loránd Kollégium 9. konferenciáján elhangzott előadások.* Szeged: SZTE Eötvös Loránd Kollégium, 160–168. Online: http://publicatio.bibl.u-szeged.hu/21553/1/9Eotvozet_kotet_PS.pdf

Marsi Tamás (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára.* Budapest: Nemzeti Közszolgálati Egyetem, 37–57.

Muha Lajos – Krasznay Csaba (2018): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

Nemzeti Kibervédelmi Intézet (2021): *A BSI is vizsgálja a kínai mobiltelefonok beépített cenzúra funkcióit.* 2021. szeptember 29. Online: https://nki.gov.hu/it-biztonsag/hirek/a-bsi-is-vizsgalja-a-kinai-mobiltelefonok-beepitett-cenzura-funkcioit/

Nemzeti Kibervédelmi Intézet (2022a): *Kikapcsolt iPhone-okat támadhatnak a hackerek.* 2022. május 19. Online: https://nki.gov.hu/it-biztonsag/hirek/kikapcsolt-iphone-okat-tamadhatnak-a-hackerek/

Nemzeti Kibervédelmi Intézet (2022b): *Mobil Security Threats – Mobilfenyegetettségek (CTI jelentés).* 2022. június 17. Online: https://nki.gov.hu/it-biztonsag/elemzesek/mobilfenyegetettsegek-mobil-security-threats/

Ormai László (2022a): e-Személyi – eSIGN: hogyan lehetne valódi áttörést elérni? *Arsboni,* 2022. szeptember 13. Online: https://arsboni.hu/e-szemelyi-esign-hogyan-lehetne-valodi-attorest-elerni/

Ormai László (2022b): eSzemélyi mobilapplikáció – áttörés a digitális szolgáltatások használatában? *Arsboni,* 2022. április 27. Online: https://arsboni.hu/eszemelyi-mobilapplikacio-attores-a-digitalis-szolgaltatasok-hasznalataban/

Reuters (2022): Germany's Cybersecurity Chief Faces Dismissal, Reports Say. 2022. október 10. Online: https:/www.reuters.com/world/europe/germanys-cybersecurity-chief-faces-dismissal-reports-2022-10-09

Schopp Attila (2022): Új világ jön az állami informatikában. *ITBUSINESS*, 2022. szeptember 10. Online: https://itbusiness.hu/technology/aktualis-lapszam/strategy/uj-vilag-jon-az-allami-informatikaban/

Zsákai Lénárd (2019): Az európai szárazföldi határok okos mobilitás fejlesztése – Magyarország Rendőrségének nemzetközi szerepvállalása a Horizont 2020 keretprogramban. *Határrendészeti Tanulmányok,* 16(3), 5–56. Online: https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Hatrend%20Tan_2019_3_sz%C3%A1m.pdf