HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 145–156.
DOI: 10.32567/hm.2021.4.11

Kerti András,[1] Koller Marco[2]

Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása[3]

Possible User-level Reduction of Misuse of Metadata Collected by Smart Device Applications at Risk Level

Az okoseszközök hétköznapivá válásával és a különböző funkciókat betöltő alkalmazások elterjedésével olyan információbiztonsági kockázatokkal néz szembe az átlagos felhasználó, amelynek talán nincs is tudatában. A különböző személyek és csoportok által fejlesztett applikációk, olyan (meta)adatokat is gyűjthetnek, amelyekkel adott felhasználó szokásai és kapcsolati hálózata könnyen beazonosíthatóvá, illetőleg felhasználhatóvá válhat az alkalmazás mögött rejlő személyek, csoportok számára. A nem kívánt adatgyűjtés elkerülése érdekében sokat segíthet a tudatos felhasználói magatartás. Ezen magatartás kialakításához hozzájárulhat, ha az applikációk alkalmazása előtt a vállalatok által is használt kockázatmenedzsment szemléletén keresztül közelítjük meg a különböző szoftvereket. Jelen kutatás célja a fentiek során kifejtett szemléletmód általi kockázatcsökkentés.

Kulcsszavak: **információbiztonság, kockázatmenedzsment, okoseszközök, metaadat, biztonságtudatosság**

As smart devices and applications with different functions become ubiquitous, the average user faces information security risks that he or she may not be aware

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi docens, e-mail: kerti.andras@uni-nke.hu
[2] Hadtudományi Doktori Iskola, doktori hallgató, e-mail: marcoakoller@gmail.com
[3] A tanulmány az Innovációs és Technológiai Minisztérium ÚNKP-20-3-I-NKE-94 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

of. Applications developed by different people and groups can also collect (meta) data with which a person's habits and network of contacts can be easily identified or used by the people and groups behind the application. Conscious user retention can help a lot to avoid unwanted data collection. Contributing to the development of this attitude can be achieved by approaching different software through the risk management approach used by companies before applying applications. The aim of the present research is to reduce the risk by the approach outlined above.

Keywords: **information security, risk management, smart devices, metadata, awareness**

1. Bevezetés

Az információs társadalom egyik ismérve a keletkezett adatok, információk mennyiségének és áramlásának nagymértékű növekedése. Ezen társadalom alkotórészévé vált a technológia, illetve a technológiai fejlődés, amely számos lehetőséget és kihívást rejt magában. Az ember és a gép kapcsolatát megvalósító eszközök a felhasználó és a berendezés kommunikációját teszik lehetővé, ez az ember-gép interfész technológia. E technológia legjellemzőbb példái a különböző okoseszközök.

Az okoseszközök térnyerésével, azok mindennapjaink szerves részévé válásával a különböző állami és nem állami szereplők olyan értékes információkhoz juthatnak az emberek mindennapi szokásairól, amelyekkel következtetni lehet adott személy kapcsolati hálózatára, baráti körére, tartózkodási helyeire, fogyasztási szokásaira, vagy akár káros szenvedélyeire is.[4] Kiemelt figyelmet érdemelnek az okoseszközök által betöltött különböző funkciók, azok evolúciója, mint például az okostelefonokon működő mobil banking applikációk, amelyekkel mindennapi banki ügyeinket már telefonon keresztül is végre tudjuk hajtani.[5] A fentiek alapján kijelenthető, hogy az okoseszközök és a hozzájuk köthető applikációk kockázatot hordoznak magukban.

1.1. A kutatás célja

A publikáció célja kockázati szemléletmód-alapú, a kockázatmenedzsment folyamatán keresztül tudományos igényességgel bemutatott, tudatos felhasználói magatartás megfogalmazása, amely alkalmas arra, hogy a felhasználó visszaszorítsa a nemkívánatos, személyével kapcsolatos (meta)adatgyűjtést. Ezzel járulva hozzá a személyes és társadalmi információbiztonsághoz egy humán aspektusú megközelítésen keresztül. Azért tartom fontosnak a humán aspektusú megközelítést, mert bár már közhelyes, azonban igaz, bármilyen erős fizikai és/vagy logikai védelemmel van ellátva adott technológia, maga a felhasználó (humán tényező) gyenge pont lehet, amelyen keresztül információt, adatot lehet kinyerni.[6]

[4] Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom,* 17. (2017), 1. 55–71.
[5] Vizi Pál: Okostelefonok biztonsági kihívásai. *Hadmérnök,* 6. (2011), 3. 131–141.
[6] Bányász Péter: Social Engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018b), 1. 4.

1.2. Kutatási módszertan

Jelen tanulmány elkészítése során a hazai és a nemzetközi szakirodalmat, illetve szabályozókat tekintettük át, illetve elemeztük a kockázatmenedzsment, a biztonságtudatosság, a metaadat, illetve az okoseszközök területén.

2. Alapfogalmak definiálása

A mobil applikációk által gyűjtött metadatokkal való visszaélések és abban rejlő kockázatok megértéséhez szükséges megteremteni az értelmezési keretet és a kellő kontextust, így fontos bemutatni a téma alapfogalmait. Az alábbiakban a kockázat és a metaadat fogalmi kereteit tisztázzuk.

2.1. A kockázat fogalmának bemutatása

A kockázat fogalmának több megközelítése is van. Resperger szerint a kockázat fogalma „az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek”.[7] A fenti besorolás a kockázatot mint biztonságpolitikai, hadtudományi, illetve nemzetbiztonsági fogalmat közelíti meg egy hármas rendszerezésben, ahol a kockázat középen, a kihívás legalul helyezkedik el, és a legnagyobb veszéllyel, úgymond hatással rendelkező lehetséges eseménynek a fenyegetést nevezi meg és helyezi legfölülre. Megállapítható, hogy ez a fogalmi keret hatásalapú megközelítést mutat be, azonban álláspontom szerint a hatás nagysága mellett a bekövetkezési valószínűség és a kettő elhárításának nehézsége is a fogalom részét kell képezze. „A kockázattal kapcsolatos fogalmakat a szakirodalom a szóban forgó tudományterülettől, a vizsgálati céloktól”[8] függően többféle szempont szerint tárgyalja.

Egy másik megközelítés szerint a kockázat: „A kockázati esemény esetleges bekövetkezésekor annak a szervezetre gyakorolt jelentősége, fontossága.”[9] A kockázati esemény pedig: „A szervezetre (a vezetők által meghatározott célok elérésre vagy a követelmények teljesítésére) várhatóan jelentős hatást gyakorló, de még be nem következett esemény. Egy eseményre vonatkozóan bejelentett gyanút nem lehet kockázati eseményként kezelni, mert ez utóbbi esetben egy, a feltételezés szerint már bekövetkezett eseménnyel kapcsolatban vagyunk bizonytalanok.”[10] A kockázatot – az ISO 31000 szabvány alapján – mint a bizonytalanság szervezeti célokra való hatását értelmezzük. A fentiek alapján megállapítható, hogy a kockázat valamilyen

[7] Resperger István: Biztonsági kihívások, kockázatok és fenyegetések 2030-ig. In Kobolka István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest, Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 31–33.
[8] Székely Csaba: Stratégiai kockázatmenedzsment. *Taylor,* 7. (2015), 1–2. 105.
[9] Horváth Péter – Németh Edit: *Integrált kockázatkezelési rendszer alapjai*. Budapest, Dialóg Campus, 2018. 9.
[10] Horváth–Németh (2018): i. m. 9.

bizonytalansági faktort jelöl, amelynek bekövetkezése esetén negatív hatása van valamilyen védendő értékre.

A kockázat fogalmából, amelyet a fentiek alapján értelmezünk, következik, hogy mi az a bizonytalanság, amely hatással lehet az adott célokra, a biztonság összetevőire. Információbiztonsági szempontból bizonytalanság annak a hiánya, hogy képesek vagyunk előre jelezni az aktuálisan végbe menő cselekmények jövőre történő hatását. „Kockázat esetén nem lehet pontosan előre jelezni az egyes kimenetelek bekövetkezését, illetőleg annak valószínűségeit."[11]

Amennyiben a bizonytalanság és a kockázat fenti definícióiból indulunk ki, arra a következtetésre juthatunk, hogy a kockázat negatív hatása bekövetkezésének megelőzése érdekében (proaktív gondolkodást elősegítve a reaktív ellenében) a bizonytalanságot kell csökkenteni, úgy, hogy a lehetséges hatás felmérése érdekében növeljük az informáltságunkat.[12]

A kockázat fogalma során felmerült összetevők közül a bizonytalanság tényezőjét tisztáztuk, az alábbiakban a hatás fogalmi kereteit kívánom körülírni. Tekintettel arra, hogy a kockázat minden egyes szervezet vagy személy számára mást-mást jelenthet, a különböző hatásokból is többféle létezik. Elmondható továbbá, hogy a hatások heterogenitásán túl annak nagysága alapján is érdemes differenciálni, ahogy ezt a különböző biztosítási társaságok teszik. Az átlag okostelefont használó személy esetében álláspontom szerint az is előrelépés, ha tisztában van, hogy egy applikáció telepítése, használata előtt szükséges felmérnie, hogy azzal kapcsolatban milyen mennyiségű és minőségű információkkal rendelkezik, így nehezebben érheti kellemetlen meglepetés.[13]

2.2. A metaadat fogalmának meghatározása

Minden informatikai eszköz vagy program használata során – így a különböző mobilapplikációk esetében is – keletkeznek metaadatok, mivel fontos szerepük van az automatizált adatfeldolgozás hátterének biztosításában, az adattárolási rendszerekben.[14]

A metaadat legegyszerűbb megfogalmazása álláspontom szerint: adat az adatról. Valójában a dokumentumok azonosítására szolgál, azáltal, hogy a leíró adatok struktúrája egységes szerkezetnek megfelelő struktúrában készül.[15] Azaz valamilyen adatról, információról nem tartalmi adat, hanem azzal kapcsolatos, kvázi külsőleges adat. Például egy levélnek a tartalma a fő információ, azonban az, hogy milyen szolgáltatón keresztül, kitől érkezett a levél és kinek, illetve mikor, az a levélről szóló adat, azaz a metaadat. Az ilyen jellegű információk birtokában az állami és nem állami szereplők különböző személyek szokásait, illetve kapcsolati hálóját képesek felderíteni.

[11] Székely (2015): i. m. 105.
[12] Székely (2015): i. m. 113–118.
[13] Székely (2015): i. m. 113–118.
[14] Kovács László – Bednarik László: Digitális dokumentumok formátumai és az XSLT-FO. In Berke József (szerk.): *Multimédia az oktatásban konferencia.* Nyíregyháza, MTESZ Neumann János Számítógép-tudományi Társaság, CD kiadvány, 2010.
[15] Lásd: https://openscience.hu/metaadat/

A metaadat fogalmát behelyezhetjük a személyes adatok halmazába, tekintettel arra, hogy a GDPR[16] szerint személyes adatnak minősül minden olyan adat, amely a természetes személy azonosítására akár részben is alkalmas. Ilyen lehet például a helymeghatározó adat, vagy az online azonosító. A fentiek alapján, amikor egy mobilapplikáció a különböző online azonosítónkat vagy a GPS-koordinátánkat kéri el, akkor a személyes adatainkat kezeli, így az alkalmazásért felelős cég adatkezelőként van jelen. A GDPR egyik nagy előnye, hogy tiltja azt a korábban bevett gyakorlatot, amely lehetővé tette a hallgatólagos beleegyezéssel történő adatgyűjtést, továbbá szankciókat is kilátásba helyez, amennyiben egy adatkezelő nem felel meg az előírtaknak.[17] A személyes adattal való visszaélés nem csupán a GDPR-ban megjelenő fogalom, a magyar büntetőjog is bünteti.[18]

A metaadatok, mint ahogy a fentiekben kifejtettem, adatok az adatról, általában egy dokumentum valamilyen strukturális, használati, formai, esetleg tartalmi kapcsolataira vonatkozó adat. Csoportosítása többféleképpen történhet, jelen tanulmányban két csoportra bontom a fogalmat, egyrészről leíró, másrészről forgalmi metaadatra.

- „A leíró metaadat a dokumentumok formai, tartalmi és strukturális jellemzőit biztosító, tipizált, másodrendű információ.
- A forgalmi metaadat a dokumentumok és a felhasználók közti használati, forgalmi kapcsolatokat (megtekintést, letöltést, meghallgatást, lájkolást, megvásárlást, kommentelést stb.) mint eseményeket leíró, másodrendű információ."[19]

A forgalmi metaadatok gyűjtése és elemzése által lehet felhasználói „profilokat", mintázatokat készíteni, amelyekkel vásárlási szokásokra, különböző kapcsolati hálókra lehet következtetni.

3. A kockázatmenedzsment folyamata

A kockázatmenedzsmentnek számos definíciója létezik, álláspontom alapján az alábbi az egyik legegyszerűbb és legérthetőbb. A kockázatmenedzsment „egy olyan vállalatvezetési alrendszer, ami a döntés szempontjából releváns kockázatokat rögzíti, méri és irányítja, valamint a vállalat összes kockázatát felügyeli és elemzi a kapcsolódó potenciális veszteségeket".[20] A kockázatmenedzsment mint folyamat magában foglalja a kockázatelemzést, kockázatkiértékelést, továbbá a kockázatszabályozással kapcsolatos irányítási elveket és gyakorlatokat. A folyamatos kockázatmenedzsment olyan széles

[16] 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.

[17] Erdős Gabriella: *Néhány gondolat az adatbiztonságról és az adatkezelésről az okos alkalmazások területén.* Budapest, Corvinus Egyetem, 2020.

[18] 2012. évi C. törvény a Büntetőtörvénykönyvről (Btk). 219. § – Személyes adattal visszaélés.

[19] Metainformáció, metaadat: www.fogalomtar.hte.hu/wiki/-/wiki/HTE+Infokommunikacios+Fogalomtar/Metainform%C3%A1ci%C3%B3+-+metaadat

[20] Halczmann Attila: Kockázatmenedzsment követelménye irányítási rendszerekben. *International Journal of Engineering and Management Sciences,* 3. (2018), 3. 315.

körben használt módszer, amely alkalmas a különböző kockázati elemeket is magában foglaló munka menedzsmentjére.[21] „A kockázatmenedzsment iteratív és adaptív folyamat, mely minden tevékenysége az előzőre épül, felhasználva a korábbi lépések során feltárt információkat, folyamatosan csökkentve a kockázatot."[22] A fogalmi meghatározásból jól látszik, hogy nem egyszeri cselekmény, hanem folyamat, amely több alkotóelemből áll, fontos az állandó visszacsatolás.

A kockázatmenedzsment folyamata alkotóelemeire bontva az alábbiak szerint néz ki:

1. környezetkialakítás;
2. kockázatfelmérés (kockázatazonosítás, kockázatelemzés, kockázatértékelés);
3. kockázatkezelés;
4. kockázatelfogadás;
5. kockázatok kommunikációja, konzultációja;
6. kockázat figyelemmel kísérése és átvizsgálása.[23]

Az elemekre bontott folyamat alapján kitűnik, hogy bizonyos kockázatokat el kell fogadni, azaz vannak olyan bizonytalansági tényezők, amelyek nem iktathatók ki teljesen, ezeket a minimumra kell redukálni. A későbbiekben jól láthatjuk, hogy egy adott személyre lebontva a folyamatot, mint szemléletmód is számolni kell maradványkockázatokkal, azonban a tudatos felhasználói viselkedés, akár a kockázatmenedzsment a vállalatoknál, a fennálló bizonytalanságot és annak hatását próbálja a minimálisra csökkenteni.

4. Mobilapplikációk által gyűjtött adatok és kockázatok

Bányász Péter az okosmobileszközök biztonságával kapcsolatban készített elemzésében is megállapította, hogy a legnagyobb számban előforduló fenyegetést ezek az alkalmazások, azaz az applikációk jelentik. Tekintettel arra, hogy az eszközeinkre telepített alkalmazások sokfélék, számos kockázatot rejtenek magukban. Bányász Péter is arra a következtetésre jutott, hogy a biztonságtudatos alkalmazás vagy használat csökkenti a nemkívánatos adatgyűjtés kockázatát, de az sem nyújt természetesen 100%-os védelmet, azaz mindig számolni kell maradványkockázattal. A különböző applikációkban rejlő kockázatokat többféle módon lehet kategorizálni. Megítélésem szerint két fő kategóriára osztható: egyrészről a kockázat fellépésnek időpontja, másrészről a felhasználó számára jelentkező negatív hatás alapján. A fellépés időpontja alapján jelentkezhet a kockázat az adott applikáció letöltése, telepítése vagy konkrétan annak futtatása során. Álláspontom szerint az első két fázisban lehet tudatosság által csökkenteni az esetlegesen fellépő negatív következményeket, illetve elhárítani azokat. A felmerülő negatív következmény alapján a nem kívánt adatgyűjtés eredményének felhasználóra való hatása alapján lehet kategorizálni, például telefon bothálózat

[21] Hanane Bahtit – Boubker Regragui: Risk Management for ISO 27005 Decision support. *International Journal of Innovative Research in Science,* Engineering and Technology, 2. (2013), 3. 530–538.
[22] Abonyi János – Fülep Tímea: *Biztonságkritikus rendszerek*. Pannon Egyetem, 2014.
[23] Székely (2015): i. m. 113–118.

tagjává tétel, banki adatok ellopása, identitás ellopása, vagy egyszerűen nem kívánt marketingcélú felhasználás.[24]

Véleményem szerint a legnagyobb kockázatot magukban hordozó applikációtípusok közé tartoznak a banki alkalmazások, amelyek egyre elterjedtebbek hazánkban is, tekintettel arra, hogy kényelmi funkciójuk megkérdőjelezhetetlen. Egy ilyen applikáció azonban olyan adatok birtokában van, amelyeket az átlagember a legjobban félt, azaz a pénzügyével, számlájával kapcsolatos információk, az azon található összeg feletti rendelkezés lehetősége. Az ImmuniWeb1 2019 közepén saját fejlesztésű mesterséges-intelligencia-alapú platformja által tesztelte a világ 100 legnagyobb bankjának alkalmazásait adatbiztonsági kritériumok alapján. Arra a megdöbbentő megállapításra jutottak, hogy csak három bank volt rendben adatbiztonsági szempontból. A kutatás a megvizsgált összes applikációban legalább alacsony kockázatú sebezhetőségeket talált, továbbá megállapította, hogy minden ötödik banki alkalmazás súlyos hibákkal működik. A kutatás alapján az alkalmazások 55%-a fér hozzá különösen érzékeny adatokhoz.[25]

A különböző mobilalkalmazásokban rejlő kockázatot legjobban szemlélteti a külföldön elterjedt Uber applikációval kapcsolatban megjelent 2017-es hír. Az Apple operációs rendszerét (iOS) használó telefonoknál detektálták, hogy az Uber applikáció képes volt arra, hogy megfigyelje a készülék kijelzőjén történteket, mindezt a felhasználó előtt rejtve. Ezzel olyan biztonsági rést generált az alkalmazás, amellyel személyek jelszavait, személyes adatait is rögzíthették volna, azonban a visszaélés megtörténtére nem keletkezett bejelentés. Az Uber az applikáció következő verziójában ezt a sérülékenységet kijavította.[26]

5. A metaadattal történő visszaélésben rejlő kockázatok

A fentiekben már említett okoseszközök térnyerésével, kiváltképp az okostelefonok elterjedésével a letölthető különböző kényelmi vagy szórakoztatási funkciót betöltő applikációk száma is nőtt. Számos applikáció kér hozzáférést bizonyos jellegű, a telefonon tárolt információkhoz (például telefonkönyv, helyadatok, képernyőidő stb.), amely által a szoftver fejlesztője fel tudja használni ezen információkat saját vállalkozása és terméke fejlesztése érdekében, vagy harmadik félnek is esetlegesen átadhatja bevételszerzés céljából. Az előbbiek megvalósulhatnak a felhasználó tudatos beleegyezésével (felhasználói nyilatkozat), illetve anélkül is. A második kategóriába már több esetben beletartoznak a különböző káros szoftverek (adathalász programok), amelyek nem csupán saját, hanem akár munkahelyünk adatbiztonságát is veszélyeztethetik rajtunk keresztül.[27]

[24] Bányász Péter: Az okos mobil eszközök biztonsága. *Hadmérnök,* 13. (2018a), 2. 360–377.
[25] Erdős (2020): i. m.
[26] Fehér-Polgár Pál – Michelberger Pál: A sajáttulajdonú mobil eszközök információbiztonsági kockázatai. *International Journal of Engineering and Management Sciences,* 3. (2018), 4. 176–185.
[27] Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatása. In Kállai Attila et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése (Tanulmánygyűjtemény I., e-book).* Nemzeti Közszolgálati Egyetem, 2016. 666.

Azonban az első kategória esetén a felhasználói attitűd és „érzékenység" kiváltképp meghatározó a nemkívánatos adatgyűjtés elkerülésének szempontjából, ugyanis, ha a felhasználó nem, vagy nem kellő alapossággal olvassa el a felhasználói nyilatkozatot vagy szerződést, akkor tevékenységéről, személyéről olyan adatok kerülnek egy adott céghez, amelyhez az adott szerződés teljes tudatában lehetséges, hogy nem járult volna hozzá.

A CRAMM[28] támadási modell alapján kifejezetten leegyszerűsítve így foglalható össze a metaadatokkal való visszaélésekben rejlő kockázat: a fenyegetés a felhasználó (meta)adataival történő nemkívánatos felhasználás, illetve visszaélés. A sebezhetőség, amelyen keresztül a fenyegetés kifejti a hatását, az adott applikáció, illetve a telepítéséhez szükséges szerződés elfogadása, illetve a nem kellően tudatos felhasználói attitűd. Amiben/amivel kárt lehet okozni, az az adott felhasználó adatai, adat- és információbiztonsága, illetve a felhasználói bizalom.[29]

Adott alkalmazás az általunk használt eszköz különböző szolgáltatásait veszi igénybe annak függvényében, hogy az applikáció milyen szolgáltatást nyújt a felhasználónak. Teljesen természetes, hogy egy fényképkészítő alkalmazás hozzáférést igényel a telefon kamerájához, galériájához. Azonban egyes esetekben jogosan merül fel a felhasználókban a kérdés, hogy például egy játékszoftver miért kér engedélyt telefonkönyvünkhöz, vagy egy zseblámpa-alkalmazás miért kér hozzáférést helyadatainkhoz.[30] A fentiekben felsoroltak kisarkított példák, amikor szinte egyértelmű, hogy az adott applikáció olyan adatokat gyűjt, amely nem szükséges az általa kínált funkciók használatához, csupán a fejlesztőnek vagy harmadik félnek gyűjt az eszköz használójáról szenzitív információkat. Nem ilyen egyszerű felfedezni a nem kívánt adatgyűjtést más esetekben. Hiszen egy futáshoz használt fitneszalkalmazás esetén életszerű, ha a valós idejű helyadatainkat akarja gyűjteni. Azonban pont egy ilyen alkalmazás fedte fel véletlenül egyes amerikai katonai központok titkos helyzetét, mivel az ott állomásozó katonák is használták, így a bázison és az a körül történt futóedzések alapján könnyen beazonosítható volt a „senki földjén" lévő objektumok helyzete.[31] Jól látható, hogy a metaadatok bár önmagukban nem tűnnek nagy jelentőségű adatállománynak, azonban megfelelő rendszerezéssel és értékeléssel olyan információk nyerhetők ki, amelyek nem csupán a marketingesek, hanem más nem törvényes célokat szolgáló személyek, csoportok részére is hatalmas értékűek lehetnek. Ezen adatok a big data-elemzéssel igen pontos előrejelzést is adhatnak a felhasználó szokásairól, jövőbeli cselekedeteiről.[32]

[28] Central Computer and Telecommunation Agency (Egyesült Királyság) által kidolgozott kockázatelemzési és -kezelési módszertan *(CCTA Risk Analysis and Management Method)*.

[29] Horváth Zsolt – Kocsis István: A CRAMM módszer alkalmazásának kiterjesztése. In *Proceedings of 8th International Engineering Symposium at Bánki.* 2016.

[30] Bányász (2018a): i. m.

[31] Fehér-Polgár – Michelberger (2018): i. m.

[32] Bányász (2018a): i. m.

6. Metaadattal történő visszaélések megelőzése kockázatmenedzsment-alapú szemléletmód által

Végezetül a kockázatmenedzsment folyamatán keresztül kívánom bemutatni, hogy a felhasználói szinten milyen módon kellene végbe mennie a tudatos okoseszköz-használatnak.

Környezetkialakítás: első lépésként a felhasználónak ki kell alakítania a környezetet, azaz meg kell állapítania az alapvető kritériumokat, milyen szempont alapján értékeli a kockázatokat, mi az a kockázati nagyság, az a hatás, amely még belefér adott applikáció letöltésébe, telepítésébe, illetve használatába. Le kell fektetnie azokat az alapokat, amelyek alapján a továbbiakban megközelíti az applikációkat, azaz meg kell határoznia, hogy egy alkalmazás telepítésekor milyen kockázatok várhatók, lebontva az applikáció készítőjének megbízhatóságára, illetve arra, hogy egyes jogosultságok (GPS-koordináták, névjegyzék) megadása, az azokkal való visszaélés milyen kockázatokat rejt magában. A környezet kialakításakor fontos az előzetes tájékozottság, egyfajta kutatómunka szükséges. Álláspontom alapján a kutatómunkát e pontnál általánosságban az applikációkra kell végezni, egyes konkrét alkalmazások esetén is szükséges külön kutatás végrehajtása.

6.1. Kockázatfelmérés (kockázatazonosítás, kockázatelemzés, kockázatértékelés)

Jelen pontnál a felhasználónak az egyes applikációkat szükséges vizsgálnia. Azonosítania kell az alkalmazás telepítése előtt, hogy annak letöltése, telepítése és alkalmazása során milyen specifikus fenyegetésekkel kell szembenéznie, fel kell mérnie, hogy mennyiben tudja kontroll alatt tartani az adott applikáció által gyűjtött adatokat. Lehetséges úgy használni a Facebook Messenger applikációját, hogy nem engedélyezzük a mikrofonhoz való hozzáférést, ez a jogosultság később is engedélyezhető, kikapcsolható. Azonosítani szükséges, hogy mik azok a vagyonelemek a felhasználó tekintetében, amelyekre az alkalmazás kockázatot jelenthet, például személyes adatok, a készülék vírusmentes állapota stb. Amennyiben ezek megtörténtek, elemeznie kell a felhasználónak, hogy milyen valószínűséggel következhet be egy biztonsági incidens, ennek milyen hatásai lehetnek, azaz a várható hatást és a bizonytalansági faktort kell szem előtt tartania. Érdemes az applikációinkat kategorizálni, szintekre bontani egy esetlegesen bekövetkezhető információbiztonsági incidens alapján. Végül a fentiek megtétele után értékelni szükséges, hogy a várható negatív hatás mértéke és bekövetkezésének valószínűsége alapján érdemes-e az applikációt letölteni, telepíteni, illetve használni.

6.2. Kockázatkezelés

Amennyiben egy alkalmazás kapcsán felmerül a felhasználóban, hogy értékelése szerint kockázat áll fenn, akkor a kockázatmenedzsment jelen szakaszát kell alkalmaznia. Alapvetően háromféle kockázatkezelési lehetőséggel tud élni. Módosítja a kockázatot,

amennyiben lehetséges, egyes jogosultságokat megvon az applikációtól. Vagy fenntartja a kockázatot, tekintettel arra, hogy az alkalmazás elengedhetetlen, vagy olyan kényelmi funkciót tölt be, hogy a kockázat vállalása megéri a felhasználó számára. Illetőleg elkerülheti a kockázatot, jelen esetben törli, vagy nem tölti le az applikációt, ezzel a lehetséges kockázatot elkerüli. Minden esetben mérlegelni kell, bármelyik stratégiát is választjuk, hogy milyen mértékű lesz a maradványkockázat, ez alapján az előzetes kritériumok, az elemzési módszertan módosítása is szükséges lehet.

6.3. Kockázatelfogadás

Fontos, mint ahogy a fentiekben is többször említettük, hogy a felhasználói tudatosság nem nyújt teljes védelmet, azonban a kockázatok szintjét meghatározhatjuk, ezáltal biztonságosabbá tehető az alkalmazások használata. Jelen stádiumnál a felhasználónak a fentiek alkalmazása után, amennyiben elfogadhatónak ítéli a fennmaradó kockázatokat, azokat el kell fogadnia, és tisztában kell lennie azok lehetséges hatásaival, illetve a bekövetkezési valószínűséggel.

6.4. A kockázatok kommunikációjának konzultációja

Felhasználói viselkedésre történő átvezetése jelen kategóriánál nehezen értelmezhető, tekintettel arra, hogy ez a vállalatok egyes projektjeinél alkalmazható metódus. Azonban felmerülhet a biztonságtudatos magatartás esetén is, amennyiben az adott személy felmér bizonyos kockázatot, akkor azt jelezheti az applikáció fejlesztőinél vagy az értékesítés felületén, ahol az alkalmazást vásárolta. Ezáltal káros vagy nem kívánt adatgyűjtéssel foglalkozó applikációkat akár ki is szűrhet az által, hogy a fejlesztő nem tudatosan végezte ezt, mint az Uber, vagy az értékesítési felületet birtokló cég távolíthatja el az alkalmazást az adott webshopból.

6.5. Kockázat figyelemmel kísérése és átvizsgálás

Végezetül kijelenthető, hogy a fentiek elvégzése nem egyszeri cselekvés, folyamatnak kell lennie; egyes applikációk frissítéseivel változhat kockázati besorolásuk, vagy a felhasználó igénye is megváltozhat a biztonság terén. Így a felhasználónak fontos mindig monitoroznia, figyelemmel kísérnie az okoseszközén telepített alkalmazásokat.

7. Összefoglalás

Általánosságban elmondható, hogy a digitális világ kiszélesedésével az adatbiztonság, személyes információink védelme egyre fontosabb és nehezebb lesz, illetve az okoseszközök és a különböző, azokra letölthető applikációk használata információbiztonsági kockázatot hordoz magában, amellyel kapcsolatban megállapítható, hogy a kockázat

minimalizálása érdekében a felhasználóknak a lehető legtudatosabb viselkedést kell fenntartania. A különböző szereplők az ilyen alkalmazások által olyan metaadatokhoz juthatnak hozzá, amellyel következtetni lehet a felhasználó fogyasztási szokásaira, kapcsolati körére, annak struktúrájára. A kutatás során feltártak szerint a felhasználói tudatosság egyik módszere lehet a kockázatmenedzsment folyamata, azonban le kell szögezni, hogy a biztonságtudatos felhasználói magatartás sem nyújt százszázalékos védelmet a nem kívánt adatgyűjtéssel szemben. A kockázatmenedzsment mint komplex folyamat rutinszerűvé tétele az ember életében nagyban hozzájárulhat a különböző mobilapplikációk által végrehajtott, nem kívánt adatgyűjtés visszaszorításában.

Felhasznált irodalom

Abonyi János – Fülep Tímea: *Biztonságkritikus rendszerek.* Pannon Egyetem, 2014. Online: http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/

Bahtit, Hanane – Boubker Regragui: Risk Management for ISO 27005 Decision support. *International Journal of Innovative Research in Science, Engineering and Technology,* 2. (2013), 3. 530–538. Online: www.ijirset.com/upload/march/1_Risk%20Management%20for%20ISO%2027005.pdf

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatása. In Kállai Attila – Krajnc Zoltán – Kristóf Zoltán – Szűcs Pál – Kalmár István – Csengeri János – Szabó Csaba – Horváth Tibor – Katona Zoltán – Varga Zsolt et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése (Tanulmánygyűjtemény I., e-book)*. Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673.

Bányász Péter: Az okos mobil eszközök biztonsága. *Hadmérnök,* 13. (2018a), 2. 360–377. Online: http://real.mtak.hu/94336/1/182_25_banyasz.pdf

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

Erdős Gabriella: *Néhány gondolat az adatbiztonságról és az adatkezelésről az okos alkalmazások területén.* Budapest, Corvinus Egyetem, 2020.

Fehér-Polgár Pál – Beerger Michel: A sajáttulajdonú mobil eszközök információbiztonsági kockázatai. *International Journal of Engineering and Management Sciences,* 3. (2018), 4. 176–185. Online: https://doi.org/10.21791/IJEMS.2018.4.16.

Halczmann Attila: Kockázatmenedzsment követelménye irányítási rendszerekben. *International Journal of Engineering and Management Sciences,* 3. (2018), 3. 314–323. Online: https://doi.org/10.21791/IJEMS.2018.3.26.

Horváth Péter – Németh Edit: *Integrált kockázatkezelési rendszer alapjai.* Budapest, Dialóg Campus, 2018. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12824/651_integralt_kockazatkezelesi_rendszer.pdf; jsessionid=BDD265F0BBC90AE65A614A8185A72E86?sequence=1

Horváth Zsolt – Kocsis István: A CRAMM módszer alkalmazásának kiterjesztése. In *Proceedings of 8th International Engineering Symposium at Bánki.* Budapest, Óbudai Egyetem, 2016. 1–6.

Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom,* 17. (2017), 1. 55–71. Online: https://doi.org/10.22503/inftars.XVII.2017.1.4

Kovács László – Bednarik László: Digitális dokumentumok formátumai és az XSLT-FO. In Berke József (szerk.): *Multimédia az oktatásban konferencia.* Nyíregyháza, MTESZ Neumann János Számítógép-tudományi Társaság, *CD kiadvány,* 2010.

Resperger István: Biztonsági kihívások, kockázatok és fenyegetések 2030-ig. In Kobolka István (szerk.): *Nemzetbiztonsági alapismeretek.* Budapest, Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 31–33.

Székely Csaba: Stratégiai kockázatmenedzsment. *Taylor,* 7. (2015), 1–2. 103–118. Online: http://acta.bibl.u-szeged.hu/36270/1/vikek_018_019_103-118.pdf

Vizi Pál: Okostelefonok biztonsági kihívásai. *Hadmérnök,* 6. (2011), 3. 131–141.

Jogi források

2012.évi C. törvény a Büntetőtörvénykönyvről

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