International Journal of Engineering and Management Sciences (IJEMS) Vol. 3. (2018). No. 4
DOI: 10.21791/IJEMS.2018.4.16.

A sajáttulajdonú mobil eszközök információbiztonsági kockázatai
The information security risks of the BYOD

P. FEHÉR-POLGÁR[1], P. MICHELBERGER[2]

[1]Óbudai Egyetem, Keleti Károly Gazdasági Kar, Szervezési és Vezetési Intézet, feherpolgar.pal@kgk.uni-obuda.hu
[2]Óbudai Egyetem, Keleti Károly Gazdasági Kar, Szervezési és Vezetési Intézet, michelberger.pal@kgk.uni-obuda.hu

Absztrakt. Ma már el sem tudjuk képzelni mindennapjainkat okoseszközeink nélkül. Úton-útfélen gyakran belebotlunk olyan emberekbe - akár szó szerint is - akik a nap 24 óráján keresztül végzik munkájukat hordozható eszközeiken. Ezen belül is széles körben elterjedtek az olyan vállalati megoldások, melyeknél a munkavállaló saját tulajdonú eszközét - leggyakrabban okostelefonját - nemcsak saját, személyes céljaira, de munkahelyi feladataira is használja, szinte hely- és időkorlát nélkül. Ebben a tanulmányban ennek a munkavégzési gyakorlatnak a vállalati adatok informatikai biztonsági kockázataira fogunk koncentrálni elméleti megközelítésben néhány esettanulmánnyal feltárva a problémakör lényegét. Megalapozzuk ezzel e kockázatok mérhetőségének és csökkenthetőségének kutatását.

Abstract. Today we cannot imagine our everyday lives without using our smart devices. While commuting we often get into people - even literally - who are doing their work on their portable devices 24 hours a day. This habit is widespread; there are many solutions that can be used by the corporation to have their employees work on their private devices, besides using it in their personal life. They can use these devices at their home, while commuting, or even while being at their own cubicle at the firm. In this article, we are concentrating on the IT risks of the firm with this work practice from a theoretical point of view. After this step, we will continue our research with investigating the problem of measuring and mitigating of these risks.

Bevezetés

A céges hálózatokban növekszik a mobil informatikai eszközök használata. [1] Kutatásaink során mobil informatikai eszközök alatt olyan hordozható készülékeket értünk, amelyeket a felhasználók nem teljesértékű számtógépnek tartanak. [2][3][4] Így tehát a különböző fajtájú okostelefonokat és tableteket. Az alkalmazottak által használt laptopok és egyéb számítógépeket tehát nem.

A legelterjedtebb használati eset a céges e-mailfiók elérése ezen eszközökről. Az elektronikus levélforgalom biztosítása azonban nem mindig elégséges a vállalati működés támogatására. A felhasználók egyre több szolgáltatást szeretnének elérni a rendelkezésre álló eszközeiken. Ilyenek lehetnek a közös könyvtárak elérése, vállalati intranet használata, belső vállalati alkalmazások elérése, az integrált vállalatirányítási rendszer elérése, videokonferenciák, és szinte minden olyan funkció, amit a dolgozók a

DOI: 10.21791/IJEMS.2018.4.16.

munkahelyi számítógépükön keresztül el tudnak végezni. Azonban e széles körű felhasználás, a növekvő rendelkezésre állási igény a biztonsági szint csökkenéséhez vezethet. [4][5]

A mobil eszközök méretüket és árukat tekintve egyre kisebbek, kapacitásuk és képességeik pedig egyre jobbak. A mobil távközlési hálózat teljesítménye, sávszélessége és lefedettsége folyamatosan javul. A mobil eszközök vállalati célra történő alkalmazása megkerülhetetlen. [6][7] Az információ védelmi lehetőségek azonban korlátozottak. Az erős titkosítás és a hitelesítés nem mindig jelent magasabb szintű védelmet. A mobil eszközök számos (meta)adatot küldenek el a kommunikáció során (például fizikai hely koordinátái, környezeti paraméterek, sebesség és gyorsulási adatok, hálózati partnerek elérhetősége). A mobil kommunikáció, ill. annak lehallgatása szinte ellenőrizhetetlen (rádióforgalmazás, például Bluetooth lehallgatása). A telefonbeszélgetés esetén pedig maga a hang is adatnak számít. [8][9][10]

A bizalmas vállalati adatok védelme új biztonságpolitikát kíván a szervezetektől. A magáncélú és vállalati használat szétválasztása alapvető fontosságú, de a vállalati alkalmazottaktól nem várható el, hogy a nap 24 órájában náluk levő okos telefont vagy bármilyen más mobil eszközt ne használják magán célra, különösen akkor, ha a készülék az ő tulajdonukban van (Bring Your Own Device - BYOD), vagy mobilszolgáltatás díját részben, vagy egészben ők fizetik. [4][5]

A védelmi tevékenység itt kettéválik. Egyrészt szükség~~es~~ van egy szervezeti működést, bizalmas vállalati adatok kommunikációját szabályozó – leírt és betartható – rend kialakítására. [5][7][10]

A másrészt az infokommunikációs eszközök védelmére. A dolgozók által használt mobilkészülékeken keresztüli adatlopás nem elhanyagolható kérdés. Ezt támasztja alá a Balabit által végzett széleskörű kutatás is, melyben 500 magasanképzett szakembert kérdeztek meg a vállalatokat leginkább veszélyeztető IT fenyegetettségekről. [11] Kiemelendő kérdés a megfelelő védelmi megoldásokat kínáló cégek (MDM - Mobile Device Management) ajánlatai közül történő választás. Ez utóbbi heterogén információtechnológia esetén igen nehéz feladat. [12][13]

1. A mobil eszközök vállalati alkalmazásának legfőbb kockázati tényezői

1. Abban az esetben, ha munkavállalótól elvárt a 24 órás, heti hétnapos készenlét fontos szempont a kapcsolattartás költségének minimalizálása. A munkavállalók általában nem szeretnek több eszközt is maguknál tartani ehhez. Szeretnék az általuk preferált, ismert felhasználói környezetet, telefontípust, operációs rendszert, szoftverkörnyezetet használni. Szélsőséges esetben ragaszkodhatnak egy konkrét mobil eszköz típushoz is. [14][15]
2. A vállalati tulajdonban lévő eszközök felett a vállalat szükség esetén teljes kontrollt gyakorolhat. Az ICT részleg tartja karban az eszközt. Megszabhatja és kikényszerítheti a munkavállalótól a szabályszerű használatot. A magánjellegű használat teljes tiltása azonban ellenállást válthat ki, szélsőséges esetben a munkavállaló kilépéséhez is vezethet. Ezzel szemben a saját tulajdonú eszköz vállalati célú használata magasabb kockázati szintet eredményezhet, magasabb fokú produktivitás mellett. Viszont, ha erre nincs megfelelően betartott szabályzat, vagy azt

DOI: 10.21791/IJEMS.2018.4.16.

nem tartják, nem tartatják be, akkor a munkavállaló a kifejezett tiltás ellenére is a vállalati adatokat saját eszközére továbbíthatja. (A leggyakoribb fegyelmezetlenség a vállalati levelek automatikus továbbítása a privát postafiókba.) [12][13][16]

3. A munkavállaló általában a „kényelmes" munkavégzést szereti. A hosszú jelszavak használata, azok rendszeres időközönkénti cseréje kontraproduktív. Ezen öncélú, más okból nem következő jelszócsere nem is növeli a biztonság szintjét. [17] A különböző hardver alapú biztonsági kulcsok használata sem könnyíti meg az eszközök kezelését. A biológiai alapú felhasználóazonosítás (ujjlenyomat, írisz, arc azonosítás) technikai és jogi kérdéseket vethet fel. A kiemelt pozíciókba kerülő – általában IT területen dolgozó - vezető beosztású munkavállalók (ún. power userek) sokszor szükségtelenül széleskörű jogosultságot is szerezhetnek. [4][18][19]
4. A magánhasználatú eszközök vállalati célú használata nem új gyakorlat. Példaként említhető saját gépkocsi használat. Ennek biztosítása, költségtérítése, adózása mára már megfelelőképpen szabályozott. BYOD eszközök esetében a cégek különböző gyakorlatokat folytatnak;
    a. legtöbb vállalatnál ezek az eszközök „megtűrtek" és szabályozás nincs, [20][21]
    b. használatuk szóbeli vezetői engedélyen alapul, itt már a technikai korlátozások is előfordulhatnak, [21]
    c. írott szabályzat van, amely esetenként kitér az információbiztonsági kérdésekre is. (A szabályzatban megadják a vállalati hálózathoz történő csatlakozás lehetséges protokolljait. A használható eszközök és alkalmazások felsorolását. Az elfogadott operációs rendszert, típust, verziót. A kötelezően alkalmazandó biztonsági szoftvereket. A mobil eszközről kezdeményezhető tranzakciókat (pl. lekérdezés és új adat felvétele igen; törlés nem). Az alkalmazott naplózási rendet és a magán- és céges adatok szétválasztásának szabályait) [4][5]
    d. a munkáltató kifejezetten ösztönzi a saját tulajdonú mobil eszközök vállalati célú alkalmazását. [5][21]
    e. A BYOD mobil eszközöknél a magánélet és a munkáltató által elvárt eredményesség konfliktusba kerülhet. Ebben az esetben a magánélet nem zárható ki, de arányosan korlátozható. Magyarországon a magánéletet a munkáltató nem ellenőrizheti, de a munkakörhöz méltó magatartás - munkaidőn kívül is – elvárható (2012. I. törvény, 8. §). [21]
5. Problémát jelenthetnek még az alábbi biztonsági kérdések;
    a. Milyen minőségű, megbízhatóságú és biztonságú a vállalati és vállalaton kívüli hálózathoz történhet kapcsolódás?
    b. Hová és milyen módon történnek a munkavállaló eszközén végzett adatmentések?
    c. 24 órás üzemidőt várunk el, vagy korlátozzuk az és szolgáltatási „időablakot" jelölünk ki, akár az eszközön, akár az eszköz által elért távoli erőforrásokon?
    d. Hány hibás bejelentkezés esetén blokkol a rendszer? Kizárható-e az adott eszköz és/vagy felhasználó a rendszerből?

DOI: 10.21791/IJEMS.2018.4.16.

e. Milyen az authentikációs sorrend (1. felhasználó, 2-3. eszköz, 2-3. sim kártya)?

f. Elérhet-e a felhasználó több „postaládát" (pl. főnök-titkár viszony esetén)? [21][22]

g. Csatlakoztathatóak-e adathordozók az adott eszközhöz, s ha igen akkor az azokon található adatok bejuttathatja-e a felhasználó a vállalati erőforrásokra? [23]

2. Esettanulmányok

Az eddigi elméleti megközelítés után, célszerű feltárnunk a vizsgálandó kutatási teret gyakorlati példákon keresztül is. Ahogyan azt a példákon keresztül is látni fogjuk a vizsgálandó kérdéskör igen széles. Éppen ezért érdemes kvalitatív kutatási módszerekkel feltárni a BYOD biztonság kérdéskörének értelmezési mezőjét, mielőtt kvantifikáló kutatásokba kezdhetünk. Ehhez a kvalitatív kutatási módszerek közül az esettanulmányos, exploratív kutatási módszert választottuk, mely abban segít, hogy a korábban megtörtént esetek alapján könnyebben megértsük a biztonsági kérdések komplexitását.

2.1. Eszközre telepített applikációk okozta adatszivárgás

Alig több mint 10 évvel az első iPhone és az első Android alapú okostelefonok megjelenése után [24], ma már el se tudjuk képzelni modern világunkat okostelefonok és tabletek nélkül. Használati szokásainkban a hangsúly egyre inkább áttolódik a klasszikus hanghívásokról és rövid szöveges üzenetekről a különböző applikációkon keresztül történő információ fogyasztásra és megosztásra. [25] Ehhez általában vagy a gyártó beépített applikációit, vagy harmadik fél által készített alkalmazásokat használunk. Rájuk bízva olykor igencsak érzékeny személyes és vállalati adatainkat is [26]. A következő példák jól mutatják, hogy adataink védelmében kiemeleten fontos szerepet játszik a mobil eszközeink tudatos használata.

2.1.1. Az eszközre előretelepített alkalmazások problémája

Amikor átvesszük eszközünket szolgáltatónktól, már rendelkezik előre telepített operációs rendszerrel, valamint a gyártó és a szolgáltató által telepített szoftvercsomaggal. 2017-ben a Check Point kutatói 36 olyan telefontípust találtak, melyekre előretelepített ártószándékú program (malware) volt az előretelepített szoftvercsomagban. 2018 elején a Dr. Web biztonsági cég 40 féle telefontípust talált, melyekre az Android.Triada.231 malware az előretelepítéskor a szoftvercsomaggal együtt telepítésre került. E program a különböző banki adatok lehallgatására volt képes. Ezen keresztül a támadók hozzáférhettek a felhasználó banki adataihoz, akár átutalásokat indíthattak, vásárlásokat bonyolíthattak le. [27][28][29][30][31]

2.1.2. A felhasználó által az eszközre telepített alkalmazások problémája

Azonban nem csak az előre telepített alkalmazások kémkedhetnek a felhasználók után. 2017 októberében jelent meg a hír, hogy a széleskörben használt Uber applikáció az iOS készülékeken titokban megfigyelheti a készülék kijelzőjét. A problémát feltáró Will Strafach szerint az applikáció egy interfészen keresztül fért hozzá az iOS akkor bevezetett képernyőrögzítő funkciójához. Ez letőséget adott arra, hogy akár biztonság kritikus adatokat is kijuttathassanak a készülékről, mint például jelszavakat,

DOI: 10.21791/IJEMS.2018.4.16.

használati szokásokat, banki adatokat, mindent, amit az eszköz a kijelzőjén megjelenített. S bár konkrét visszaélés nem ismert, ami kihasználta volna ezt a lehetőséget. A korlátozatlan megfigyelés lehetősége igen magas biztonsági kockázatot jelent. Az Uber az applikáció következő verziójában megszűntette ezt a sérülékenységet. De hasonló esetek tucatja történt már meg a mobileszközök világában, ami az adatok ellopását, vagy hozzájuk férését megakadályozta. Az ismert kártevők száma igen magas, számuk pedig igen gyorsan növekedik. [32][33][34][35][36][37][38][39]

2.2. Adatszivárgás a felhasználó „beleegyezésével”

Alkalmazásaink az eszközeink különböző szolgáltatásait használhatják. Teljesen egyértelmű például, hogy egy fényképeket készítő applikációnak működéséhez elkerülhetetlen, hogy az eszköz kameráját használhassa. Egy térkép program, ha használhatja az eszközbe épített navigációs lehetőségeket, sokkal szélesebb körű funkcionalitásra lehet képes, mint anélkül. Felmerülhet a kérdés azonban, hogy egy-egy applikáció az eszköz mely szolgáltatásához férhet hozzá. Tényleg szüksége van-e például egy üzenetküldő alkalmazásnak az eszközbe épített mikrofon használatára, vagy sem? Megvizsgálandó lenne, hogy a különböző alkalmazásaink, milyen szolgáltatásokat és milyen céllal vesznek igénybe. Teljesen érthető például, ha egy testmozgást naplózó applikáció engedélyt kér a helyadatok használatára. Sokan használnak olyan applikációkat, melyek segítségével mérhetővé válik a megtett út, a bejárt útvonal, az elégetett kalóriák száma… Azonban könnyen belátható, hogy e hozzáféréseken keresztül akár szenzitív adatok is rossz kezekbe kerülhetnek.

Ilyen adatszivárgásról adott hírt 2018. január 27-én Nathan Ruser az Institute for United Conflict Analysts alapítója. [40][41] A széleskörben elterjedt Strava fitnesz applikáció készítői a felhasználók eszközeiből gyűjtött adatokból egy igen részletes térképet készítettek és tettek közzé. Több mint 3 milliárd GPS koordinátát használtak fel. Jól mutatja a térkép részletességét és a felhasználók szokásait a következő ábra, melynek bal oldalán láthatjuk a Strava térképének Szilvásvárad és Fátyol-vízesés közti részletét, míg a jobb oldalán a turistautak.openstreetmap.hu közel azonos kivágását. Jól látszik, hogy a felhasználók milyen útvonalakat jártak be, hol követték a kijelölt turista útvonalat, hol vágtak át az erdőn. Azonban a felhasznált GPS pontok olyan helyekről is származtak, melyek Nathan Ruser szerint többek között az Egyesült Államok bázisait, és azon belül is a felhasználók mozgását is nyilvánosságra hozta.

DOI: 10.21791/IJEMS.2018.4.16.

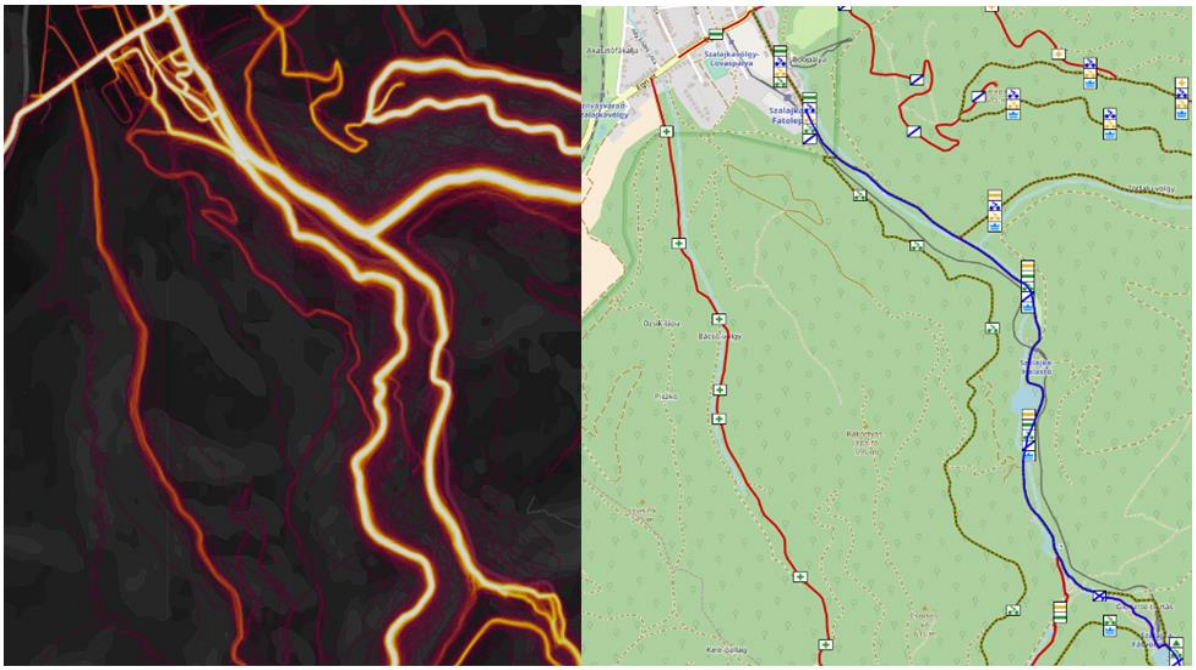

Figure 1. Strava felhasználói adatok vizualizációja és ugyanazon hely turista térképen.
(Saját szerkesztés a Strava térképének és a turistautak.openstreetmap.hu felhasználásával)

Bár az adatok lezárása 2017 novemberben történt, mégis érzékeny információkat tartalmazhattak a térkén publikálásakor. Az adatgyűjtés a felhasználók beleegyezésével történik. Az applikáció csak akkor küldi el a helyszíni adatokat a Strava szervereire, ha a felhasználó ezt nem kapcsolja ki. Itt tehát az érzékeny adatok a felhasználók tudtával, vagy tudatlansága miatt kerültek nyilvánosságra.

Hasonló eset történt 2014-ben, amikor egy orosz katona az Instagramra feltöltött fényképével megosztotta a kép készítésének helyét is. Ezzel feltárva, hogy ukrán területen végeznek tevékenységeket. [42]

A két esett közös vonása, hogy a felhasználó beállításai alapján, (elvileg) a felhasználók tudtával kerültek ki e biztonsági kockázatot jelentő adatok nyilvánosan elérhető oldalakra.

2.3. Az esettanulmányok alapján megfogalmazható következtetések

Bár az előző példák önmagukban nem konkrétan egy-egy vállalat biztonsági kérdéseit vetik fel, könnyen értelmezhetőek a vállalatokat fenyegető valós problémákra.

Az elméleti bevezetés és az esettanulmányok alapján is látható, hogy az embereknek és a vállalatoknak mobil eszközeik adatbiztonságával foglalkozniuk kell. Tudatosan kell tervezniük, hogy milyen adatok, milyen körülmények között kerülhetnek ezen eszközökre.

Az eszközök kiválasztását, védelmét és felhasználását körültekintően meg kell tervezni. A kiválasztásnál törekednünk kell olyan gyártó eszközét választani, amelyik az eszköz tervezett élettartama alatt biztosítja rendszereinek biztonsági frissítését. A kiválasztott eszközre az elérhető biztonsági megoldásokat alkalmazni kell. Amennyiben lehetséges, megbízható víruskeresőt kell telepíteni. A készülék beállításainál is az adatbiztonságot előtérbe kell helyezni. Ha más körülmény nem indokolja, csak megbízható forrásból telepítsünk, leellenőrzött alkalmazásokat. Ezen alkalmazásoknak a hozzáférését szű-

DOI: 10.21791/IJEMS.2018.4.16.

kítsük le, csak a használatukhoz szükséges jogosultságokat engedélyezzük. A használat során legyünk tisztában azzal, hogy milyen adatokat, kapunk, dolgozunk fel, továbbítunk, mely applikációkon keresztül.

Javasolt az IT- és információbiztonsági szabályozással foglalkozó szakemberek számára, hogy a vállalatnál ne csak a felhasználói profilokat határozzák meg, hanem a vállalati hálózatba bejelentkező különböző eszközökét is. Más legyen a hozzáférési jogosultsága ugyanannak a felhasználónak a belső hálózatra kötött munkaállomásra történő bejelentkezésénél, mint a nyilvános helyen használt saját tulajdonú mobil eszköz esetében.

A cégeknek a kifejezetten informatikai problémák mellett erőteljesen figyelembe kell venniük dolgozóik biztonságtudatosságát is. Ahogyan a két utolsó példában is látható volt, a vállalat alkalmazottai akár szándékosan, akár figyelmetlenségből, juttathatják ki az érzékeny vállalati adatokat mobileszközeik segítségével.

S bár ezen intézkedések következtében sem érhetjük el a 100%-os biztonság állapotát. De akár költségmentesen, vagy legalábbis a védekezési költség/kár arány alacsonyan tartásával is elérhetünk komoly biztonsági szintnövelést.

Hivatkozások

[1] M. Dhingra (2016) *Legal Issues in Secure Implementation of Bring Your Own Device (BYOD).* Procedia Computer Science, 78 pp 179-184. ISSN 1877-0509, https://doi.org/10.1016/j.procs.2016.02.030. http://sciencedirect.com/science/article/pii/S1877050916000326 (utolsó letöltés: 2018.2.12.)

[2] G. Disterer – C. Kleiner (2013) *BYOD Bring Your Own Device.* Procedia Technology, 9 pp. 43-53. ISSN 2212-0173, https://doi.org/10.1016/j.protcy.2013.12.005. http://www.sciencedirect.com/science/article/pii/S221201731300159X (u.l.: 2018.2.12.)

[3] C. Rose (2013) *BYOD: An examination of bring your own device in business.* The Review of Business Information Systems (Online), 17 (2) pp. 65-69. Retrieved from https://search.proquest.com/docview/1418721775?accountid=134728 (u.l.: 2018.2.12.)

[4] M. Olalere – M. T. Abdullah – R. Mahmod – A. Abdullah (2016) *Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication*. International Journal of Computer Networks and Communications Security. 4 (1) pp. 21-32.

[5] P. Baillette – Y. Barlette (2018) *BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: the identification of a twofold security paradox*. Journal of Organizational Change Management. 31.

[6] J. Lee – M. Warkentin – R. E. Crossler – R. F. Otondo (2017) *Implications of monitoring mechanisms on bring your own device adoption.* The Journal of Computer Information Systems, 57 (4) pp. 309-318. 2017 http://dx.doi.org/10.1080/08874417.2016.1184032

[7] A. Weeger – X. Wang – H. Gewald (2015) *It consumerization: byod-program acceptance and its impact on employer attractiveness.* The Journal of Computer Information Systems, 56 (1) pp. 1-10. https://search.proquest.com/docview/1729274646?accountid=134728 (u.l.: 2018.2.19.)

[8] C. Ke – Z. Lin (2015) *An approach for secure data exchange: Experiments on android-based mobile device.* Scientia Iranica.Transaction B, Mechanical Engineering. 22 (4) pp. 1586-93.

DOI: 10.21791/IJEMS.2018.4.16.

[9] Y. Wang – H. Li – T. Li (2017) *Participant selection for data collection through device-to-device communications in mobile sensing.* Personal and Ubiquitous Computing. 21 (1) pp. 31-41.

[10] W. B. Glisson – T. Storer – G. Mayall – I. Moug – G. Grispos (2011) *Electronic retention: what does your mobile phone reveal about you?* International Journal of Information Security. 10 (6) pp. 337-49.

[11] Balabit CSI Report 2015 https://pages.balabit.com/rs/855-UZV-853/images/Balabit-top-10-hacks.pdf (u.l.: 2018. 2. 24.)

[12] M. A. Harris – K. P. Patten (2014) *Mobile device security considerations for small- and medium-sized enterprise business mobility.* Information Management & Computer Security. 22 (1) pp. 97-114.

[13] K. E. Byol – O. Joohyung – I. Chaete (2014) *A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment. Lecture Notes in Engineering and Computer Science*. 2210. 2014 https://pdfs.semanticscholar.org/6a92/6e31903ee0f7fb684852c37dfeff27a76c44.pdf (u.l.: 2018.2.7.)

[14] M. K. Al Hassan (2017) *BYOD technological: Next generation business development programs for future accelerations, innovations and employee happiness.* International Journal of Computer Applications, 165 (10) 2017 http://dx.doi.org/10.5120/ijca2017913929 http://www.ijcaonline.org/archives/volume165/number10/hassan-2017-ijca-913929.pdf (u.l.: 2018.1.25.)

[15] B. Toperesu – J. P. Van Belle (2017) *Organisational capabilities required for enabling employee mobility through bring- your-own-device concept.* Business Systems Research, 8 (1) pp. 17-29. http://dx.doi.org/10.1515/bsrj-2017-0002

[16] A. Das – H. U. Khan (2016) *Security behaviors of smartphone users.* Information and Computer Security. 24 (1) pp. 116-34.

[17] A. Keszthelyi (2013) *About passwords*. Acta Polytechnica Hungarica 10 (6) pp. 99-118. (2013)

[18] A. Wójtowicz – K. Joachimiak (2016*) Model for adaptable context-based biometric authentication for mobile devices.* Personal and Ubiquitous Computing, 20 (2) pp. 195-207.

[19] P. Stapór – D. Laskowski (2016) *Bring Your Own Device - Providing Reliable Model of Data Access.* Journal of KONBiN, 39 (1) pp. 41-56.

[20] A. Leclercq – Vandelannoitte (2015) *Managing BYOD: how do organizations incorporate user-driven IT innovations?* Information Technology & People, 28 (1) pp. 2-33.

[21] D. Holló (2015) *Hol a határ? Hol a határ? Magánszféra Magánszféra kontra munkahely munkahely a digitális korban a digitális korban.* DETEKTOR Plusz, 3. 35 p.

[22] W. Fisher – C. Allen (2015) *Road warriors and information systems security: risks and recommendations.* Journal of Management Information and Decision Sciences. 18 (1) pp. 84-96.

[23] A. Keszthelyi (2013) *Netháborúk kora.* In: Gy. Juhász – K. Horváth – Z. Árki – J. Keserű –T. Török – A. Lévai – Z. Seben (szerk.): Új kihívások a tudományban és az oktatásban - Gazdaságtudományi szekció: Zborník medzinárodnej vedeckej konferencie Univerzity J. Selyeho – 2013 "Nové výzvy vo vede a vo vzdelávaní" Sekcia ekonomických vied. 437 p. (ISBN:978-80-8122-074-6)

[24] S. Gallotto – W. Chen (2014) *Security Management of Bring-Your-Own-Devices*. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp); 2014.

DOI: 10.21791/IJEMS.2018.4.16.

[25] S. R. Walli (2009) *Mobile internet and economics of open source*. The Open Source Business Resource, 01:13-9.

[26] K. Lazányi (2016) *Who do You Trust? – Safety Aspect of Interpersonal Trust among Young Adults with Work Experience.* In: A. Szakál (szerk.): Proceedings of the11th IEEE International Symposium on Applied Computational Intelligence and Informatics SACI 2016. 412 p. Konferencia helye, ideje: Timisoara, Románia, 2016.05.12-2016.05.14. Budapest: IEEE. pp. 349-354. (ISBN:978-1-5090-2379-0)

[27] C. Koo – N. Chung – H. Kim (2015) *Examining explorative and exploitative uses of smartphones: a user competence perspective*. Information Technology & People, 28 (1) pp. 133-62.

[28] Y. Jia et al. (2017) *Open Doors for Bob and Mallory: Open Port Usage in Android Apps and Security Implications.* 190-203. 10.1109/EuroSP.2017.44. 2017 https://eecs.umich.edu/eecs/about/articles/2017/open_euro17.pdf (u.l.: 2018.2.7)

[29] H. Elahi – G. Wang – X. Li (2017) *Smartphone Bloatware: An Overlooked Privacy Problem*. pp. 169-185. 2017 10.1007/978-3-319-72389-1_15.

[30] Doctor Web: over 40 models of Android devices delivered already infected from the manufacturers https://news.drweb.com/show/?i=11749&lng=en&c=9 (u.l.: 2018.2.12)

[31] J. Walls – K. K. R. Choo (2017) *Chapter 8 - A Study of the Effectiveness Abs Reliability of Android Free Anti-Mobile Malware Apps*. In: Mobile Security and Privacy. Syngress, Boston. pp. 167-203, ISBN 9780128046296, https://doi.org/10.1016/B978-0-12-804629-6.00008-0. https://www.sciencedirect.com/science/article/pii/B9780128046296000080 (u.l.: 2018.2.17.)

[32] O. Koriat (2017) *Preinstalled Malware Targeting Mobile Users Check Point Software Technologies Ltd.* https://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/ (u.l.: 2018.2.7.)

[33] M. F. Faiz – R. Rahman – S. T. Deepak (2017) *Scrutinizing permission based attack on android os platform devices*. International Journal of Advanced Research in Computer Science. 8 (7).

[34] A. S. Yuksel – A. H. Zaim – M. A. Aydin (2014) *A Comprehensive Analysis of Android Security and Proposed Solutions.* International Journal of Computer Network and Information Security. 6 (12) pp. 9-20.

[35] Kaspersky lab, Skygofree: highly advanced, powerful Android surveillance software active since 2014, 2018 http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Campaign/KESB_2013/Pdfs/Skygofree_-_Press_Release_.pdf (u.l.: 2018.2.7.)

[36] N. Buchka – A. Kivva – D. Galov (2017) *Jack of all trades.* https://securelist.com/jack-of-all-trades/83470/ (u.l.: 2018.1.25.)

[37] NS. Hackers Take Over HBO Social Accounts, Plant Spyware in App Store and Target Scottish Parliament. Nextgov.com (Online). 2017 Aug 21.

[38] K. Leswing (2017) *Apple gave Uber's app 'unprecedented' access to sensitive Apple features that can record iPhone screens, Business Insider* http://businessinsider.com/uber-iphone-app-secret-access-sensitive-apple-features-2017-10 (u.l.: 2018.1.25)

[39] A. Hern (2018) *Fitness tracking app Strava gives away location of secret US army bases,* The Guardian. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (u.l.: 2018.2.12.)

[40] F-Secure, Another Reason 99% of Mobile Malware Targets Androids https://safeandsavvy.f-secure.com/2017/02/15/another-reason-99-percent-of-mobile-malware-targets-androids/ (u.l.: 2018.4.25)

DOI: 10.21791/IJEMS.2018.4.16.

[41] L. Barron (2018) *U.S. Soldiers are Accidentally Revealing Sensitive Locations by Mapping Their Exercise Routes.* January 29, 2018 http://time.com/5122495/strava-heatmap-military-bases/ (u.l.: 2018. 2. 24.)

[42] P. Szoldra (2014) *A Russian Soldier's Instagram Posts May Be The Clearest Indication Of Moscow's Involvement In East Ukraine, Business Insider*, July 31, 2014. http://businessinsider.com/russian-soldier-ukraine-2014-7 (u.l.: 2018. 2. 24.)