FELSŐOKTATÁSBAN TANULÓ HALLGATÓK BIZTONSÁGTUDATOSSÁGA

SAFETY CONSCIOUSNESS OF THE STUDENTS IN HIGHER EDUCATION

FEHÉR-POLGÁR PÁL
Óbudai Egyetem Biztonságtudományi Doktori Iskola

Abstract

In the last few years the field of electronic devices had seen and dynamic spread of smart devices. Firstly smartphones and then tablets and nowadays smartwatches and other "smart" wearable devices. In security there is a common saying that the weakest link is the human part. This can be observed in the field of smartphones too. In order to measure the safety features of the human side, safety consciousness and its levels were introduced into the field of organisational safety; the improvement of which can only be achieved with education, the increase of the people's knowledge. In present article the relation of the students from Kodolányi University of Applied Sciences and the Óbuda University with their mobile phones is explored. The students' safety consciousness, perception of threats and conscious deeds against them is investigated. Research questions were: Is there a significant difference between the engineering manager students of the Óbuda Universiy and the business management students of the Kodolányi University of Applied Sciences? Are those students more safety conscious who store important data on their mobile phones? Is there a relevant common feature about those in the research that has significant correlation with the students perception of safety or their behaviour in connection with it?

1. Bevezetés

A mobilinformatikai eszközök (okostelefonok és tabletek) mára olyan széleskörűen elterjedtek, ami alapján kijelenthetjük: a mindennapjaink nélkülözhetetlen(nek hitt) részeivé váltak. Ezeken az eszközökön olvasunk, tanulunk, szórakozunk és dolgozunk, tartjuk a kapcsolatot az ismerősökkel és intézzük a hivatalos ügyeket. Ily módon mind a magán, mind a munkahelyi életünknek szerves részei, s ma már teljesen természetesnek vesszük használatukat. Felmerülnek azonban kétségek: Ennek a természetességnek, kényelemnek része-e a biztonságtudatos használat? Törődünk-e ezen eszközök, és az azokon elérhető, tárolható – akár magán, akár munkával összefüggő, munkahelyi – adatok, információk biztonságával? Jelen cikk egy, a felsőoktatási hallgatók körében végzett primer kutatással igyekszik az előző kérdésekre választ adni. E fiatal korosztály tagjai vagy már aktív munkavállalók vagy a közeljövőben válnak aktív munkavállalókká, tehát egyáltalán nem mellékes, hogy mennyire tudatosan kezelik az eszközeiket, amely magatartással – negatív avagy pozitív – hatással vannak a magán és munkahelyük biztonságára is.

2. Biztonságtudatosság

Mint tudjuk, 100%-os biztonság nem létezik, a biztonsági szint növelésére költött költség pedig exponenciálisan nő,[1] ezért meg kell határozni egy olyan biztonsági szintet, ami a megítélésünk szerint megfelelő biztonságot nyújt a megfelelő költségszinten.

A biztonsági szint eléréséhez szükség van szabályokra, mind a személyes biztonság, mind a vállalati biztonság esetén is. Azonban nem lehet mindent szabályozni. Szükség van egyfajta tudatosságra, mely Szabó Attila a T-Systems Magyarország szenior információvédelmi menedzsere szerint,[2] sokkal fontosabb, mint bármilyen szabályozás, bármilyen információvédelmi alapelv. Mint tudjuk, a technológiák önmagukban nem védenek meg bennünket. Közhelyszerű, de igaz, hogy minden biztonsági rendszer leggyöngébb láncszeme az ember.[3] Az embert pedig, mint biztonsági kockázatot pedig csak oktatással, a biztonságtudatosság növelésével lehet javítani, s elérni a biztonságtudatosság egy magasabb, érettebb szintjét.[4]

Schoop és Vasvári a következőképpen határozta meg a biztonságtudatosság érettségi modelljét:[5]

1. ábra. **A biztonságtudatosság érettségi modellje**

Figure 1. **The model of safety assurance mature**

Forrás: Saját szerkesztés Schoop Attila, Vasvári György (2012) Tudatos biztonság, alapján

0 (Nem létező): Teljesen hiányzik a jó gyakorlat.

1 (Kezdő): Ad hoc formában van néhány bizonyíték, hogy a szervezet felismerte a biztonságtudatosság fontosságát.

2 (Ismételhető, de intuitive): A felismerés növekvő, van törekvés e kérdés kezelésére, bár ezek az erőfeszítések nem megalapozottak, és nem dokumentáltak.

3 (Meghatározott folyamat): Egy mérsékelt szintű jó gyakorlat és folyamatok vannak jelen, és a munkatársak tudatában vannak a felelősségüknek.

4 (Menedzselt és mérhető): A jó gyakorlat egy szintje és a folyamatok jelen és dokumentálva vannak, valamint a munkatársak tudatában vannak felelősségüknek.

5 (Optimalizált): A folyamatok fejlettek, megfelelnek a követelményeknek, folyamatosan karban vannak tartva, egy önértékeléssel.

Összegzésként elmondható, hogy a biztonságtudat kialakítása mind a személyes biztonság, mind vállalati biztonság szférájában elengedhetetlenül szükséges. Ahhoz azonban, hogy ez a biztonságtudat megfelelő legyen folyamatos képzésre és/vagy önképzésre van szükség.

3. Az okostelefonok biztonsága

Az elmúlt években a mobilinformatikai eszközök robbanásszerű terjedését figyelhettük meg.

Az eNET 2012-ben végzett egy 1000 fős reprezentatív mintán felmérést, ami azt mutatta ki, hogy a válaszadók 29%-ka rendelkezik okostelefonnal.[6]

A Thinking insights with Google oldal felmérése alapján, ugyan ez a részarány 2012-ben 22%-os, míg 2013-ban 34,4%-os.[7]

Az NRC 2013-as nem reprezentatív piackutatásán a válaszadók 45%-a nyilatkozott úgy, hogy okostelefonnal rendelkezik, míg 51%-uk mondta azt, hogy okostelefonnal és/vagy tablettel rendelkezik.[8]

Ezek alapján megállapítható, hogy bár még az okostelefonok elterjedése ezekben az években nem érte el a 40%-ot, és elmaradt az 5 legnagyobb európai mobiltelefon piaccal rendelkező országtól utolsó helyezettjétől is. De akár csak azokban az országokban, Magyarországon is egy erőteljes növekedést figyelhettünk meg az okostelefonok piaci részesedésében.

Az okostelefonokkal kapcsolatos biztonsági aggályok kérdése nem új. Gareth James már 2004-ben a Network Security című szakfolyóiratban megjelent cikkében foglalkozott e témával. Az ő akkori felmérése azt mutatta, hogy ebben az időben nem léteztek még ártó szándékú szoftverek, melyek az okostelefonokat támadták volna. Azonban talált olyan sebezhetőségeket, amelyek lehetővé tették volna, hogy ilyen szoftverek kárt okozzanak. E cikk úgy jellemezte az akkori állapotokat, hogy bár az okostelefonok elterjedése alacsony, jellemzően olyan magas beosztású emberek rendelkeznek ilyen telefonokkal a politikai és üzleti élet területeiről, akik tevékenységi körükből fakadóan célpontjai lehetnének támadásoknak.[9]

Ezzel szemben, ahogy láthattuk ma már az okostelefonok elterjedési köre igen széles. Ma már nem csak magas beosztású emberek privilégiuma egy okostelefon, hanem szinte bárki megengedheti magának, hogy okostelefonja legyen. Azonban sajnos a biztonsági helyzet nem lett jobb, mint 2004-ben.

Szinte nem múlik el úgy hét, hogy ne olvashatnánk egy-egy felfedezett támadásról, vagy befoltozott eddig kihasználhatónak tekinthető biztonsági résről. Például a Kaspersky lab 2014 első negyedévében több mint 2500 ártó szándékú egyedi programot tartott nyilván, melyek a mobilbankolási folyamatot támadták Android platformon, s ezek közül több mint 1000 ebben a negyedévben került felfedezésre.[10]

Az apple iOS-e körül a nyáron nagy visszhangot keltett Jonathan Zdziarski publikációja, melyben az iOS-ben lévő backdoor-okat és támadási pontokat vizsgálta, s talán ennek hatására is szeptember 17-én az Apple 7 frissítésben 55 CVE-t (Common Vulnerabilities and Exposures) zárt le.[11]

Ez csak két példa, de jól mutatják, hogy mai mobiltelefonjaink platformjainak biztonsági kockázata igen magas.

Azonban a szoftveres oldal mellett kiemelten kell kezelni a mobiltelefonokkal kapcsolatban a rajtuk tárolt adatok adatbiztonságát is.

2012-ben az ENISA, az Európai Unió Információs és Hálózatbiztonsági Ügynöksége felmérte, hogy mik a legnagyobb kockázatok, amelyek az okostelefonokat fenyegetik. A három legfontosabb ezek közül:

1. Adatok kiszivárgása az eszközök elvesztése, vagy ellopása miatt.
2. Az adatok akaratlanul történő közzététele.
3. Azon eszközök támadása, melyek a használt telefonpiacra kerülnek vállalati használat után.[12]

Ez utóbbi kockázatokhoz kapcsolódik az ESET biztonsági cég londoni felmérése, melyben 300 taxisofőrt kérdeztek meg, arról, hogy mit hagytak az utasok a hátsó ülésen. A felmérés azt mutatta ki, hogy egy átlagos londoni taxisofőr évente 8 db mobiltelefont talál. S ha ezt az eredményt kivetítjük arra a 24 000 taxisra, akik Londonban dolgoznak, akkor az évi 190 000 db elhagyott mobiltelefont jelent.[13]

Mark James, az ESET egy biztonsági szakértője azt is kiemelte e felmérés kapcsán, hogy „mind annak ellenére, hogy mekkora publicitást kap a kiberbűnözés manapság, a felhasználók még mindig nem tekintik magukat valós célpontnak. E gyakorlat naiv és rossz. A bűnözők nagyon jól tudják, hogy a mobiltelefonjaink kapcsolódási pontok lehetnek a vállalati hálózatokhoz és akár érzékeny tartalmakat is tárolhatnak." S ennek ellenére az okostelefon tulajdonosok nem védik kellően a telefonjaikat és az azokon tárolt adatokat.[14]

Ezek alapján kijelenthető, hogy manapság a mobiltelefonjainkat több irányból is fenyegetik biztonsági kockázatok, amikre nem mindenki van felkészülve. Sokaknak nincs meg a kellő biztonságtudata, aminek hatására a mobiltelefonjaikat és a rajtuk tárolt adatokat kevesebb biztonsági kockázat fenyegetné.

4. Felsőoktatási hallgatókon végzett felmérés elemzése a biztonságtudatosság szempontjából

Kutatásomat a Kodolányi János Főiskola és az Óbudai Egyetem hallgatóinak körében végeztem. Azért választottam ezt a felmérésem számára ezt a mintát, mert a megkérdezett hallgatók vagy már dolgoznak vagy a közeljövőben fognak elhelyezkedni, így a biztonságtudatosságuk erőteljesen befolyásolja (illetve befolyásolni fogja) az adott szervezet informatikai biztonságát. Ezt azon keresztül vizsgáltam, hogy milyen a biztonságtudatosságuk az okostelefonjaikkal kapcsolatban. Ez megfelelő vizsgálati alapnak tekinthető, mert a mintát adó magasan iskolázott fiatal felnőttek alkotják azt a demográfiai csoportot, akik a leginkább használnak okostelefonokat.[15]

Kutatásmódszertan: A kvantitatív felmérés strukturált online kérdőív segítségével készült, az adatok feldolgozásához és értékeléséhez az alap leíró statisztikákon túlmenően az összefüggések feltárására T-próbát, továbbá Pearson-féle korrelációelemzést alkalmaztam IBM SPSS.22 program segítségével.

4.1. A minta jellemzése

A mintában részt vevő hallgatók átlagéletkora 22,7 év. A férfiak aránya 60%, míg a nőké 40% a mintában. 89%-uk rendelkezik okostelefonnal. Ez a részarány közel kétszerese az NRC által a 2013 év első negyedévére mért teljes piacra vonatkozó piackutatása által mért 45%-os részaránynak.[16]

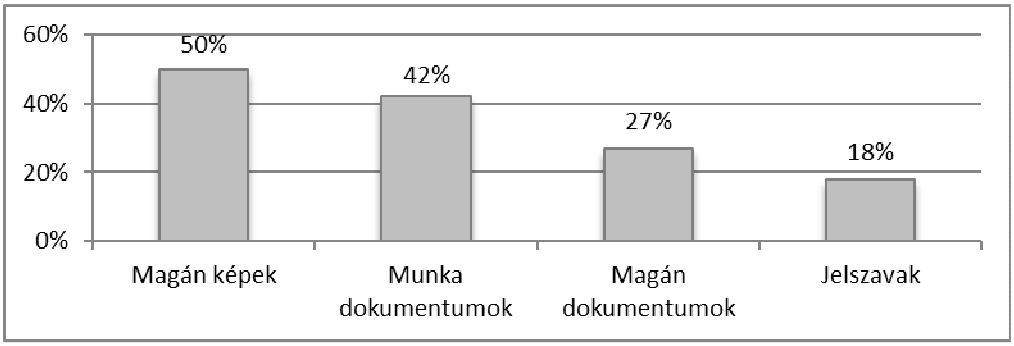
A foglalkoztatottság szempontjából a minta inhomogén; 43%-uk nem dolgozik jelenleg, míg 17%-uk munkaviszony mellett tanul, 24%-uk pedig diákmunkában dolgozik. Családi vállalkozásban dolgozik 6%-uk és 2%-uknak saját vállalkozásuk van.

Az ENISA által azonosított három fő biztonsági kockázati tényezőre tekintettel megkérdeztem a hallgatókat, hogy tárolnak-e adatokat a telefonjaikon, és ha igen, akkor milyen jellegű adatokat tárolnak.[17]

A válaszadók 64%-a tárol számára fontos adatokat a telefonján.

***2. ábra.* A telefonon tárolt legjellemzőbb adatok a kérdőív válaszai alapján**

***Figure 2.* The nature of the stored information on smartphones according to the questioner**



Forrás: Saját szerkesztés a kérdőíves felmérés alapján

4.2. A felmérés kutatási kérdései

1. A műszaki menedzser hallgatók különböznek-e a közgazdász hallgatóktól?

A vizsgálatot független mintás T próbával végeztem. A próba szignifikáns eltérést mutatott a telefonok használatának mértékében. A műszaki menedzser hallgatók kimutathatóan többet használják a telefonjaikat, mint a közgazdász hallgatók (F-érték 7,832, Szignifikanciaszint: 0,06).

Összefüggést lehet kimutatni a szak és a foglalkoztatás, a hírolvasási szokások, illetve a banki adatok telefonon történő tárolásában.

	Foglalkozás	Hírolvasási szokások	Banki adatok tárolása
Pearson-féle korreláció:	0,282	0,221	–0,309
Szignifikancia szint:	0,001	0,012	0,001

Vagyis a foglalkoztatás szempontjából inkább foglalkoztatottak a műszaki menedzserek Ők azok, akik banki adatokat is inkább tárolnak a telefonjukon Míg a közgazdász hallgatók tájékozódnak inkább a telefonjukon keresztül a hírekről.

2. Azok a hallgatók, akik fontos adatokat tárolnak a telefonjaikon különböznek-e a biztonsági kérdésekben társaiktól?

A tárolás kérdését tekintve nem volt kimutatható korreláció semelyik biztonsági kérdéssel, így megállapítható, hogy a mintában nincs kimutatható összefüggés a között, hogy valaki tárol-e a telefonján számára fontos adatot azzal, hogy hogyan viszonyul a telefonja biztonságához.

Azt viszont statisztikailag igazoltam, hogy aki többet használja a telefonját, az nagyobb valószínűséggel tárol is a telefonján biztonságilag fontos tartalmakat; dokumentumokat tárol (Pearson-féle korreláció: 0,226, Szignifikanciaszint: 0,011), határidőket tárol (Pearson-féle korreláció: 0,298, Szignifikancia szint: 0,001), jelszavakat tárol (Pearson-féle korreláció: 0,241, Szignifikancia szint: 0,006).

3. Azok a hallgatók, akik okostelefont használnak…

Feltártam, hogy azok akik okostelefont használnak, a telefonjukon valószínűbben tárolnak dokumentumokat, jelszavakat, személyes információkat; (Pearson-féle korreláció:

0,213, Szignifikancia szint: 0,016), (Pearson-féle korreláció: 0,283, Szignifikanciaszint: 0,001), (Pearson-féle korreláció: 0,213, Szignifikancia szint: 0,016).

Igazoltam, hogy azok, akiknek nincs okostelefonjuk, azok inkább tárolnak fontos információkat a telefonjaikon (Pearson-féle korreláció: 0,258, Szignifikancia szint: 0,003). Ez utóbbi biztonsági szempontból pozitívnak tekinthető, mert egy „buta telefon" távoli elérésének kockázata kisebb, mint egy okostelefoné.

5. Következtetések

Az elvégzett vizsgálatok alapján, a következő következtetéseket vonhatjuk le.

Egyfelől, nem mutatkozott lényeges különbség a biztonságtudatosság tekintetében a műszaki menedzser és a közgazdász hallgatók között, így kijelenthető, hogy a vizsgált mintában nem meghatározó a biztonságtudatosságban, hogy milyen szakra jár az adott hallgató.

Másodrészben, a minta alapján az is megállapítható, hogy azok, akik valamilyen fontos dokumentumot (magánjellegű képet, tanulmányokhoz vagy munkához kapcsolódó fájlokat, banki adatokat, jelszavakat stb.) tárolnak a telefonjaikon, nem mutatnak nagyobb biztonságtudatosságot, mint azok, akik nem. Pedig elvárt lehetne, hogy ha valamilyen számunkra fontos tartalmat tárolunk valahol, akkor annak a tárolónak a biztonságát kiemelten kezeljük.

Harmadrészt megállapítható volt a válaszok alapján, hogy azok, akik okostelefont használnak, biztonságtudatosabban gondolkodnak a telefonjukról és az azon tárolt adatokról.

Jegyzetek

1. Keszthelyi András (2013): Netháborúk kora, A SJE Nemzetközi Tudományos Konferenciája „Új kihívások a tudományban és az oktatásban" Komárom, 2013. szeptember 17–18.
2. Szabó Attila (2014): A biztonság szemüvegén keresztül. In: Jövőkép 2014/2, http://www.t-systems.hu/jovokep/201401/a_biztonsag_szemuvegen_keresztul, 2014. október 11.
3. Keszthelyi András (2014): Paradigmaváltás – Biztonság – Emberi Tényező, TAYLOR Gazdálkodás- és szervezéstudományi folyóirat, A Virtuális Intézet Közép-Európa Kutatására Közleményei, in press.
4. Kristóf Csaba (2013): A britek a biztonságtudatosság növelésére költenek, 2013. 6. 25. http://bitport.hu/biztonsag/a-britek-koeltenek-biztonsagtudatossag-noevelesere 2014. 10. 11.
5. Schopp Attila, Vasvári György (2012): Tudatos biztonság. 2012. 02. 25. http://www.itbusiness.hu/Fooldal/rss_3/Tudatos_biztonsag.html
6. eNET – Telekom, Már okostelefon-felhasználó a magyar lakosság több mint ¼-e http://www.enet.hu/hirek/mar-okostelefon-felhasznalo-a-magyar-lakossag-tobb-mint-%C2%BC-e/?lang=hu 2013, letöltve: 2014. 04. 30.
7. Think insights with Google http://think.withgoogle.com/ 2013 letöltve: 2014. 05. 29.
8. Molnár Judit (2013): Kütyükörkép 2013Q1: Lassan már több az okos, mint a nem okos http://nrc.hu/hirek/2013/05/15/Kutyukorkep_2013Q1, 2013, 2014. 05. 15.
9. Gareth James (2004) Malicious threats to Smartphones in Network Security Volume 2004, Issue 8, August 2004, 5–7. p.
10. Kaspersky Lab (2014): IT threat evolution Q1 2014 https://securelist.com/files/2014/07/q1-it-threats-en.pdf 2014. 10. 11.
11. Debra Littlejohn Shinder (2014): iOS 8 fixes 53 security flaws in iPhone and iPad, http://www.gfi.com/blog/ios-8-fixes-53-security-flaws-in-iphone-and-ipad/ 2014. 10. 11.

12. ENISA – European Union Agency for Network and Information Security Top Ten Smartphone Risks https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks 2014. 04. 30.
13. Dan Raywood (2014) 8 phones left in each London taxi each year, leads to security concerns http://itsecurityguru.org/8-phones-left-london-taxi-year-leads-security-concerns 2014. 10. 11.
14. Uo.
15. Hammill, Greg (2005), Mixing and Managing Four Generatons of Employees. In: EduMagazine Online, Winter/Spring 2005.
16. Molnár Judit (2013): i. m.
17. Lásd 12. jegyzetet.

Felhasznált irodalom

Keszthelyi András (2013): Netháborúk kora, A SJE Nemzetközi Tudományos Konferenciája „Új kihívások a tudományban és az oktatásban" Komárom, 2013. szeptember 17–18.

Szabó Attila (2014): A biztonság szemüvegén keresztül. In: Jövőkép 2014/2, http://www.t-systems.hu/jovokep/201401/a_biztonsag_szemuvegen_keresztul, 2014. október 11.

Keszthelyi András (2014): Paradigmaváltás – Biztonság – Emberi Tényező, TAYLOR Gazdálkodás- és szervezéstudományi folyóirat, A Virtuális Intézet Közép-Európa Kutatására Közleményei, in press.

Kristóf Csaba (2013): A britek a biztonságtudatosság növelésére költenek, 2013. 6. 25. http://bitport.hu/biztonsag/a-britek-koeltenek-biztonsagtudatossag-noevelesere 2014. 10. 11.

Schopp Attila, Vasvári György (2012): Tudatos biztonság. 2012. 02. 25. http://www.itbusiness.hu/Fooldal/rss_3/Tudatos_biztonsag.html

eNET – Telekom, Már okostelefon-felhasználó a magyar lakosság több mint ¼-e http://www.enet.hu/hirek/mar-okostelefon-felhasznalo-a-magyar-lakossag-tobb-mint-%C2%BC-e/?lang=hu 2013, letöltve: 2014. 04. 30.

Think insights with Google http://think.withgoogle.com/ 2013 letöltve: 2014. 05. 29.

Molnár Judit (2013): Kütyükörkép 2013Q1: Lassan már több az okos, mint a nem okos http://nrc.hu/hirek/2013/05/15/Kutyukorkep_2013Q1, 2013, 2014. 05. 15.

Gareth James (2004) Malicious threats to Smartphones in Network Security Volume 2004, Issue 8, August 2004, 5–7. p.

Kaspersky Lab (2014): IT threat evolution Q1 2014 https://securelist.com/files/2014/07/q1-it-threats-en.pdf 2014. 10. 11.

Debra Littlejohn Shinder (2014): iOS 8 fixes 53 security flaws in iPhone and iPad, http://www.gfi.com/blog/ios-8-fixes-53-security-flaws-in-iphone-and-ipad/ 2014. 10. 11.

ENISA – European Union Agency for Network and Information Security Top Ten Smartphone Risks https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks 2014. 04. 30.

Dan Raywood (2014) 8 phones left in each London taxi each year, leads to security concerns http://itsecurityguru.org/8-phones-left-london-taxi-year-leads-security-concerns 2014. 10. 11.

Hammill, Greg (2005), Mixing and Managing Four Generatons of Employees. In: EduMagazine Online, Winter/Spring 2005.