HADMÉRNÖK

XIII Évfolyam 2. szám – 2018. június

AZ OKOS MOBIL ESZKÖZÖK BIZTONSÁGA

SECURITY OF THE SMART MOBILE DEVICES

BÁNYÁSZ Péter

(ORCID: 0000-0002-7308-9304)

banyasz.peter@uni-nke.hu

Absztrakt

Az internet és az okos mobil eszközök elterjedése alapjaiban változtatta meg életünket. A legújabb okos mobil eszközök, amik majdnem mindenki zsebében megtalálhatóak, amellett, hogy nagyban megkönnyítik a kapcsolattartást, a munkavégzést, illetve szórakoztató funkciót is betöltenek, egyúttal új típusú kihívásokat is jelentenek.

A mű a KÖFOP-2.1.2-VEKOP- (tel:15201600001) azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *okos mobil eszköz, megfigyelés, adatbiztonság, vírusok*

Abstract

The availability of the internet and the smart mobile devices have changed our life. All the newest smart mobile devices, - which can be found in our pocket- make our work, to keep contact easier and they have also entertainment function.

„The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the Cyber Security Ludovika Workshop”

Keywords: *smart mobile devices, surveillance, data protection, viruses*

A kézirat benyújtásának dátuma (Date of the submission): 2018.01.25.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.02.06.

BEVEZETÉS

Az okos mobil eszközök biztonsága kiemelt jelentőségű kell, hogy legyen. Ennek oka rendkívül egyszerű, mindannyiunk zsebében -legalább egy- készülék megtalálható, amelyen keresztül az életünket éljük. Az okos mobil eszköz - legyen szó mobiltelefonról, tabletről- képességét tekintve egy számítógépnek feleltethető meg, és mint ilyen, ugyanazok a kockázatok fenyegetik, mint egy számítógépet. Ez a felismerés azonban sajnálatos módon nem tekinthető általánosnak az átlag felhasználó esetében, így hiába használja hasonló tevékenységek végzésére, mint egy számítógépet (pl. e-mailek küldésére, kapcsolattartásra, dokumentumok szerkesztésére, olvasására, internetezésre stb.), a védelemre nem fordít kellő időt, energiát és pénzt.

A tanulmány célja, hogy felhívja a figyelmet azokra a kockázatokra, amelyek az okos mobil eszköz használatából fakadnak, ily módon növelve a biztonságtudatos használatot. Bár a cím az okos mobil eszközöket fogalmazza meg, alapvetően az okos telefonok kockázatait vizsgálom, de azok tapasztalatai ugyanúgy érvényesek a táblagépekre is.

TRENDEK

Maga az okos telefon fogalom az angol smart phone tükörfordításából származik, maga a smartphone kifejezést először 1997-ben, az Ericsson a GS88 „Penelope” nevet viselő készülékre alkalmazták. Az okos mobil telefonok megalkotását a közvélemény az Apple iPhonejának 2007-es megjelenéséhez datálja, ez azonban csalóka. Annak függvényében, hogy mit értünk okos telefon alatt, különböző időpontokhoz köthetjük a megjelenését. Vitathatatlan, az iPhone számos olyan technológiai újítást tartalmazott, amelynek úttörő szerepe volt abban, hogy az okos telefonok elterjedjenek, de már a 90-es évek elején találkozhattunk „okosnak” nevezett mobil készülékkel- ez volt az IBM által 1994-ben piacra dobott, Simon fantázianevet viselő eszköz.

Az okos mobil telefonok fejlődését három nagy szakaszra bonthatjuk. Az első generációs eszközök megjelenését 1994 és 2002 közé datálhatjuk. Ezek az időszak inkább nevezhető egyfajta elő-elő okos telefon koraszknak, de ekkor még nem volt semmi komolyabbként nevezhető technológiai robbanás, ami segítette volna a tömeges elterjedésüket (a telefonok műszaki leírására bővebben lásd az 1. számú táblázatot).

Telefon	Processzor	Memória	Operációs Rendszer	Kamera	Kijelző	Egyéb
IBM Simon	16 MHz-s 16 bites, x86	1 MB	Dos	-	monokróm	Harmadik féltől származó alkalmazások futtatása
Nokia 9000 Communicator	Intel 24 MHz i386	8 MB	GEOS	-	monokróm 200*640	QWERTY billentyűzet
Nokia 9110	AMD 486	8 MB	GEOSTM	-	monokróm 200*640	bővíthető MMC-kártyával
Ericson R380	nincs adat	2 MB	EPOC 5.1	-	monokróm	
Nokia 9210	52 MHz ARM 9	14 MB	Symbian 6,0	-	200*640 (12 bit)	WAP, E-mail
Nokia 7650	104 MHz ARM 9	4 MB	Symbian 6,1	VGA	176*208 (12 bit)	WAP, E_mail, MMS, Bluetooth, Infra, JAVA alkalmazások

1. táblázat Okos telefonok 1994-2002. között
(saját szerkesztés, Forrás: Logout [1], TelefonGuru [2]))

2002-től végbement egy olyan innovációs folyamat, amelynek hatására megkezdődött az okos telefonok tömeges elterjedése. Ezt a 2007-ig tartó időszakot nevezzük a második generációs mobil eszközöknek (a készülékek műszaki leírását lásd a 2. számú táblázatban).

Telefon	Processzor	Memória	Operációs Rendszer	Kamera	Kijelző	Egyéb
Blackberry 5810	ARM 7EJ-S	8 MB	BlackBerry OS 3.6	-	monokróm 160*160	WAP, GPRS, POP3
HTC Wallaby	206 MHz-s StrongARM	32/64 MB	Microsoft Pocket PC	-	240 * 320	
Blackberry 6210	nincs adat	16 MB	BlackBerry OS	-	160 * 100	USB
Nokia N-Gage	104 MHz ARM 920T	-	Symbian 6,0	-	176*208 (12 bit)	GPRS, WAP, Bluetooth, E-mail
Blackberry 7210	nincs adat	16 MB	BlackBerry OS	-	240 * 160	USB, GPRS, WAP, 7270 WIFI képes
Nokia 6600	104 MHz ARM 9	6 MB	Symbian 7,0	VGA	176*208 (16 bit)	videó rögzítés, támák letöltése, GPRS, WAP, Bluetooth, E-mail, Infra
PalmOne Treo 600	Intel PXA270 312 MHz	23 MB	5,x Garnet Palm Os	VGA	320*320 (16 bit)	GPRS, EDGE, WAP, Bluetooth, E-mail, Infra
Nokia 6680	TI OMAP 1710, 220 MHz ARM926EJ-S	10 MB	Symbian 8,0	1,x Mpixel két kamera	176*208 (18 bit)	GPRS, EDGE, WAP, Bluetooth, E-mail,

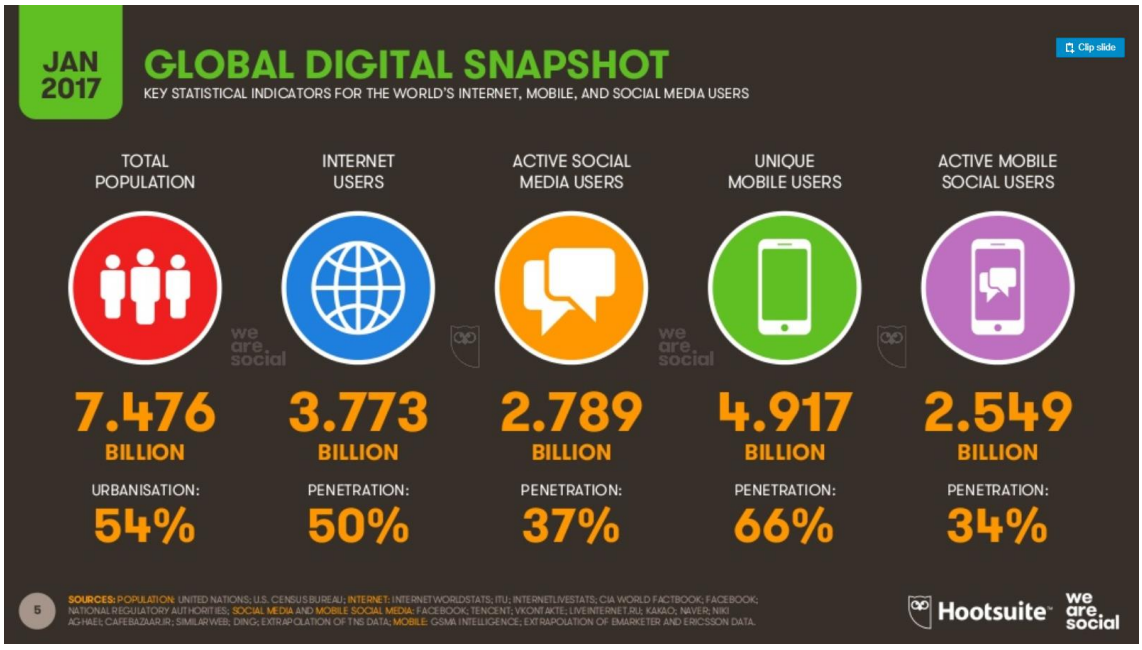
2. táblázat Okos telefonok 2002-2007. között
(saját szerkesztés, Forrás: Logout [1], TelefonGuru [2])

Az iPhone megjelenése alapjaiban változtatta meg az okos telefonok piacát. Letisztultsága, kezelhetősége paradigmaváltó volt, ugyanis oly módon egyszerűsítette le a készülék

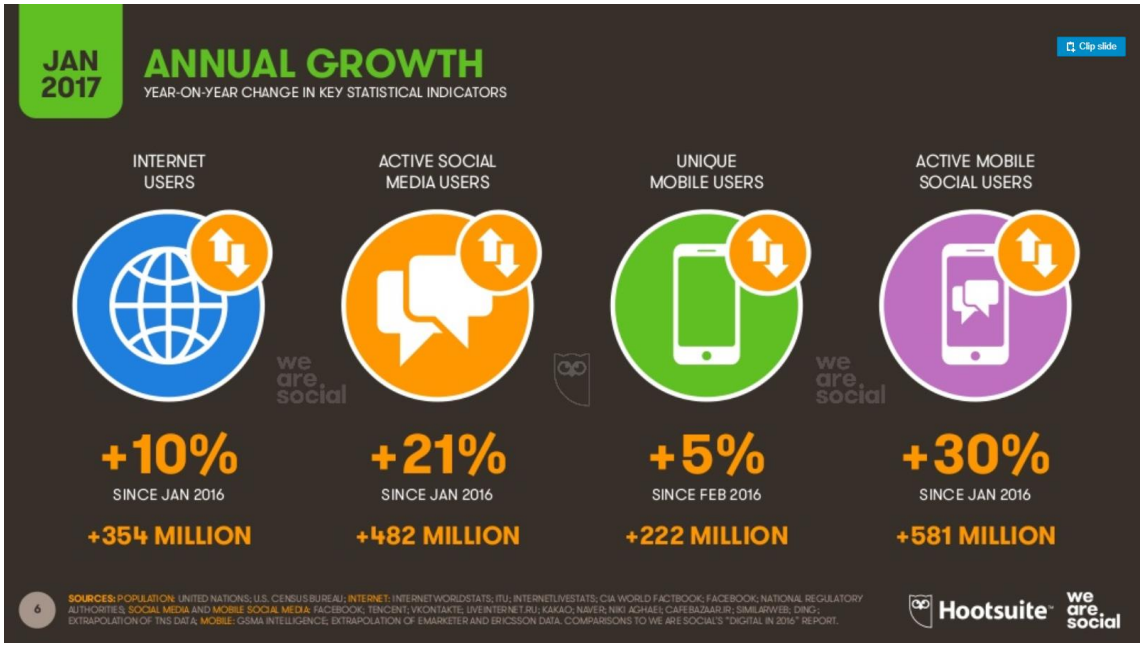
használatát, hogy azt bárki könnyen elsajátíthatta, nem kellett informatikusnak lennie. Természetesen az iPhone sem volt tökéletes, de olyan piaci versenyt generált, amely megteremtette az igényt a könnyen kezelhető okostelefonok iránt, és rákényszerítette a piaci versenytársait, hogy az innovációt az Apple által irányított keretek között folytassák- enélkül minden bizonnyal az Android is teljesen más fejlődési utat követett volna.

A táblagépek evolúciója az okos telefonokhoz analóg módon zajlott. Az első tablet megjelenése 1989-ben történt meg, a Grid Systems GRiDPAD-ja volt az, ami vizualitásában a mai tabletek elődjének feleltethető meg: a 10 hüvelykes monokróm kijelzős eszközt egy beépített toll segítségével lehetett irányítani. Képességei a kor színvonalán voltak, visszatekintve korlátozottnak tűnik, azonban mégis messze meghaladta korát. A következő nagy lépcsőfok a Microsoft által 2002-ben piacra dobott tabletje jelentette, azonban annak magas ára végül bukást eredményezett. Az áttörést, ahogy az okos mobil készülékek esetében, itt is az Apple hozta meg 2010-be piacra dobott iPadjével. Az iPad ötlete a riválisMicrosoft 2002-es készülékének megjelenésekor megfogalmazódott, de az iPhone fejlesztésével parkolópályára került, hogy a cég erőforrásait a telefon kifejlesztésére optimalizálják. Az iPhone sikerét követően döntöttek az iPad fejlesztésének folytatása mellett, ami a telefonhoz hasonlóan szintén átrendezte a piacot, kényszerpályára állítva a konkurens vállalatokat.

A We are social nevű online marketingre szakosodott reklámügynökség globális felméréseit alapul véve megállapíthatjuk, hogy 2017 januári felmérése alapján [3] 4,917 milliárd mobilelőfizetés él világszerte (lásd 1. számú ábra), ami az előző év adataihoz képest 5%-os növekedést, 222 millió új mobil előfizetést jelent (lásd 2. számú ábra). Ez a közel 5 milliárdos érték mintegy 66%-os penetrációt takar a Föld teljes népességéhez viszonyítva.



1. ábra Mobilelőfizetések száma 2017. január (Forrás: We are social [3])



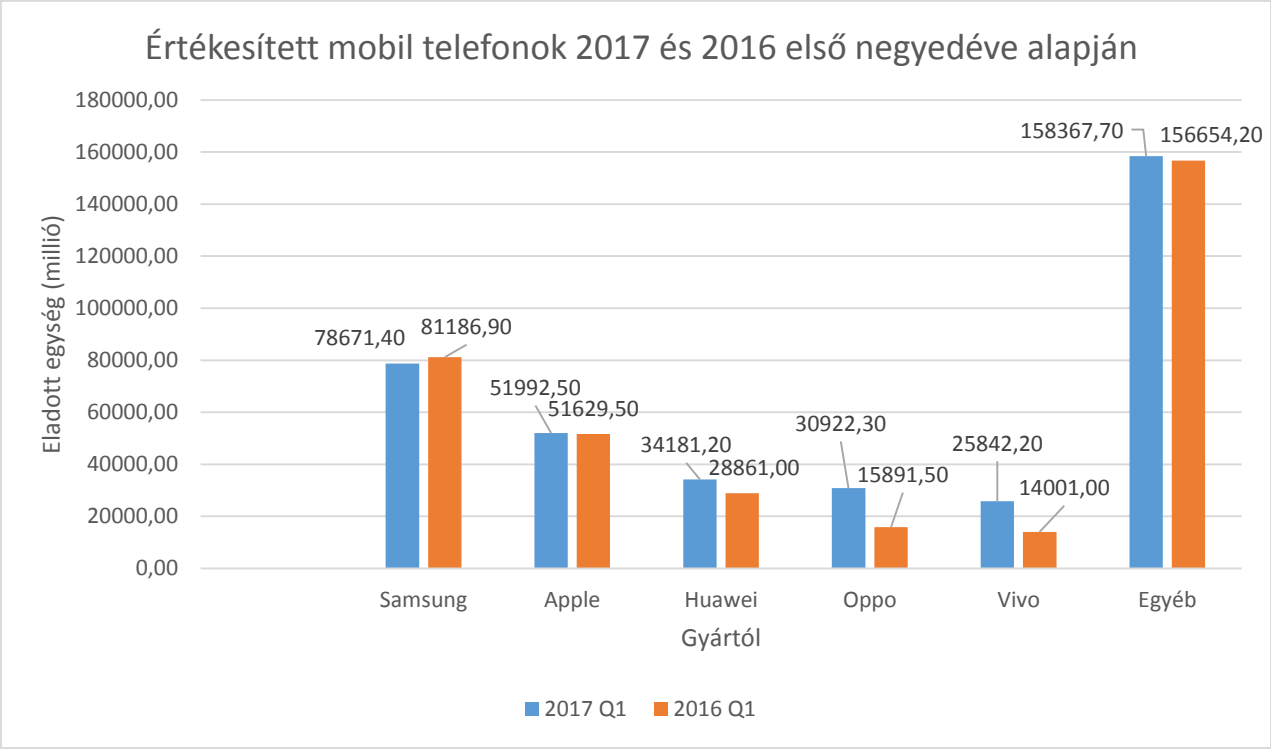
2. ábra Mobilelőfizetések számának éves növekedése 2017. január (Forrás: We are social [3])

Alapul véve a Gartner piaci elemző cég elemzését [4], a 3. számú táblázaton ábrázoltam 2016 és 2017 első negyedéveinek (Q1) mobil telefon eladásait, illetve a gyártók vonatkozó évek piaci részesedésének arányát.

Gyártó	2017 Q1 (millió eladott egység)	2017 Q1 Piaci részesedés (%)	2016 Q1 (millió eladott egység)	2016 Q1 Piaci részesedés (%)
Samsung	78671,40	20,70	81186,90	23,30
Apple	51992,50	13,70	51629,50	14,80
Huawei	34181,20	9,00	28861,00	8,30
Oppo	30922,30	8,10	15891,50	4,60
Vivo	25842,20	6,80	14001,00	4,00
Egyéb	158367,70	41,70	156654,20	45,00
Összesen	**379977,30**	**100,00**	**348224,10**	**100,00**

3. táblázat Mobiltelefon eladások száma 2016 és 2017 első negyedévében (saját szerkesztés, forrás: Gartner [4])

Látható, hogy a Samsung, bár közel 3%-al kevesebb mobiltelefont forgalmazott 2017 első negyedévében, mégis őrzi piacvezető szerepét, az öt nagy gyártó közül egyedül az Applenek sikerült növekedést realizálnia (3. számú ábra).



3. ábra Értékesített mobil telefonok 2017 és 2016 első negyedéve alapján

(saját szerkesztés, forrás: Gartner [4])

A mobil eszközök biztonsága esetében fontos szempont, hogy milyen operációs rendszert használ, hiszen eltérő azok biztonsági szintje. Az idézett Gartner jelentést figyelembe véve a 4. számú táblázatról leolvasható, hogy az Android növelte piaci részesedését 2017-re, közel 90%-a a készülékeknek Android operációs rendszert használ.

Operációs Rendszer	2017 Q1 (millió eladott egység)	2017 Q1 Piaci részesedés (%)	2016 Q1 (millió eladott egység)	2016 Q1 Piaci részesedés (%)
Android	327163,6	86,10	292746,9	84,10
iOS	51992,5	13,70	51629,5	14,80
Egyéb	821,2	0,20	3847,8	1,10
Összesen	**379977,3**	**100,00**	**348224,2**	**100,00**

4. táblázat Mobiltelefonok megoszlása operációs rendszer alapján 2016 és 2017 első negyedéve (saját szerkesztés, forrás: Gartner [4])

2017. első negyedévében az Android piaci részesedése 86,1%, a iOS-é 13,7%, míg az egyéb operációs rendszerek 0,2%-ra (4. számú ábra) tehető.

4. ábra Mobiltelefonok megoszlása operációs rendszer alapján 2017 első negyedéve

(saját szerkesztés, forrás: Gartner [4])

AZ OKOS MOBIL ESZKÖZÖK BIZTONSÁGI KOCKÁZATAI

Az okos mobil eszközök népszerűségét, ahogy a bevezetőben már volt szó róla, az iPhone által bevezetett könnyű kezelhetőség hozta meg. Az Apple ismerte fel, és gondolta újra az ezzel kapcsolatos technológiát, egy kis képernyőn teljesen más internetezni, csevegni vagy egyéb tevékenységeket végezni, ha nem optimalizálják a felhasználóbaráttá a folyamatokat. Az okos telefon használat kulcsává az alkalmazások váltak, amelyek könnyebb kezelhetőséget ígértek a felhasználóknak. Azonban az alkalmazások egyúttal rengeteg új típusú kockázatot is magukkal hoztak.

Az operációs rendszer, mint kockázat

A trendeket vizsgáló fejezetben volt szó az operációs rendszerek eltérő biztonsági szintjéről.

Az operációs rendszerek egy nagy csoportjának alapjául a Linux operációs rendszer szolgál. Bár maga a Linux is készített operációs rendszert mobil eszközökre, azonban inkább kiindulópontként nevesíthető a későbbi operációs rendszerek fejlesztésében. A Linux alapú operációs rendszerek legismertebbje a Google által megalkotott Android operációs rendszer. Az Android az elmúlt években számos verzióval jelent már meg, azonban ez is inkább alapként szolgál, az egyes gyártók eltérő Androidos operációs rendszert fejlesztenek a saját eszközükre optimalizálva. Az Android előnye, hogy rendkívül széles árkategóriában találkozhatunk vele, az alkalmazások telepítésére fájlból is nyílik lehetőségünk, illetve testre szabható. Hátránya természetesen a fragmentációból is fakad, mivel rengeteg eltérő verziójú Androidos operációs rendszer van, így nehéz optimalizálni az alkalmazásokat rá, pláne, hogy eltérő hardveres követelményeket támasztanak a különböző alkalmazások. Ahogy a 4. számú táblázatról

leolvashattuk, az Android a legelterjedtebb operációs rendszer, ezért előszeretettel támadják.[1] Az Androidra optimalizált alkalmazások esetében az is megkönnyíti a támadók dolgát, hogy a Google hivatalos alkalmazás boltjába, a Google Play Storeba felületes ellenőrzést követően tölthetnek fel a fejlesztők alkalmazásokat, amelyek így rengeteg biztonsági kockázatot hordoznak magukban.

Az Android után a második legnagyobb operációs rendszer az Apple által fejlesztett iOS. Kezdetekben csupán az Apple által fejlesztett alkalmazások futtatását engedélyezte a rendszer, azonban később megnyitották külső fejlesztők előtt is az utat, azonban szigorú biztonsági követelményeknek kell megfeleljenek ezek az alkalmazások. Az AppStorbe való feltöltés is több körös ellenőrzést követően lehetséges. Az iOS hátrányait az Apple termékek árszabásában szokták megjelölni, valamint a korlátozott testreszabhatóságban. Biztonsági szempontból azonban azt gondolom, a korlátozott testreszabhatóság védelmet is jelent, hiszen kevesebb olyan hibalehetőség jelentkezik, ami a nem feltétlenül tudatos használatból következik.

Egyszerű internetes kereséssel számtalan olyan oldalt találhatunk, amely az általunk használt operációs rendszer testreszabásának módját írja le. Ezek azonban számos esetben megkövetelik, hogy a felhasználó magasabb szintű informatikai tudással rendelkezzen, ezek hiányában, különösen egy Androidos eszköz esetében nem csak az eszközt teheti tönkre, de sebezhetőségek előtt is utat nyithat. A testreszabhatóság minősített esetét jelentik, amikor a felhasználók rendszergazdai jogosultságot szereznek a készülök fölött. IOS-es eszközök esetében ezt a folyamatot jailbreaknek, Androidos eszközök esetében rootolásnak nevezzük. Ezek során a felhasználó superuser-ré válik, vagyis egy olyan felhasználóvá, akinek teljes hozzáférése van minden utasításhoz és fájlhoz az operációs rendszerben.

Az operációs rendszerek egy másik típusát a Windows operációs rendszere jelentette, egészen 2017 októberéig, amikor is a Microsoft bejelentette, hogy a továbbiakban nem fejleszt mobil eszközre operációs rendszert [6], ahogy az eszköz fejlesztést is feladja [7]. Az operációs rendszer előnyét a többi Microsoft termékkel való integrációs adta, hátrányát pedig, hogy ugyanazok a sebezhetőségek voltak rá érvényesek, mint az alap Windows operációs rendszerre. A Microsoft lépése nem volt túlzottan meglepő, az elmúlt egy évben a vállalat eladta a Nokiát, több ezer alkalmazottat bocsájtott el a mobilfejlesztő részlegről. A döntés fő okául az a beismerés szolgált, hogy a Windows Phone és operációs rendszere nem tudta megtörni az Android egyeduralmát, a két nagy operációs rendszer együtt a piac 99,8%-át uralta. A Microsoft egyúttal bejelentette, hogy továbbra is támogatja a készülékeit frissítésekkel, hibajavításokkal.

Az operációs rendszerek frissítése egy rendkívül fontos sarokpontja a mobil eszközök biztonságának. Mint a fejezetből is kiderült, számos sebezhetőség jellemezheti az egyes operációs rendszereket, amelyekre a gyártók rendszeresen bocsájtanak a felhasználók rendelkezésére frissítéseket, hibajavításokat. Ezeket azonban a felhasználóknak kell telepíteni az eszközön, ezek hiányában a felfedezett sérülékenységek továbbra is megmaradnak a készüléken, amit a támadók ugyanúgy kihasználhatnak.

A sebezhetőségek esetében nem szabad megfelejtkezni az úgynevezett nulladik napi sérülékenységekről sem. Ez alatt olyan biztonsági fenyegetést értünk, amelynek során a támadók egy szoftvernek vagy hardvernek még a fejlesztők által sem ismert sebezhetőségét

[1] 2016 nyarán pl. 103 sérülékenységet javító frissítést adtak ki Androidra, ebből 47 kritikus, 42 súlyos, míg 14 darab mérsékelt veszélyességi besorolást kapott [5]. A sérülékenységek sokrétűek lehetnek. Az említett javítócsomagban többek között a Qualcomm nevű gyártó csipjeinek sebezhetőségét fedezték fel, amely az Android összes verzióját érintette, ily módon több mint 900 millió okos telefont és tabletet volt támadható. A sérülékenység kihasználásával a támadók észrevétlenül szerezhettek rendszergazdai jogosultságot, ily módon hozzáférve fényképeinkhez, e-mailjeinkhez, dokumentumainkhoz, de távolról bekapcsolhatták a mikrofont és kamerát is.

használják ki. Mivel a hiba senki által nem ismert, így értelemszerűen nem készült hozzá biztonsági javítás. Zero-day exploitnak nevezik azt a tényleges kódot, amit a támadók használnak a sérülékenység kiaknázására, mielőtt a fejlesztője tudna róla. A kifejezés az exploit keletkezésének időpontjából adódik. Amikor a fejlesztő tudomást szerez egy biztonsági résről, megkezdődik a verseny a támadók és a fejlesztők között; a felelősségteljes fejlesztő igyekszik befoltozni a hibát, mielőtt nyilvánosságra kerül. A „nulladik napi" támadás az első vagy „nulladik" napon történik, amikor a fejlesztő már tud a hibáról, de még nem volt lehetősége arra, hogy a biztonsági javítást eljuttassa a szoftver felhasználóihoz. Számos esetben azonban hiába derül ki egy szoftverről, hogy biztonsági rést tartalmaz, amely súlyos következménnyel járhat a felhasználó számára, a kiadott frissítőcsomagokat nagyon kevesen telepítik, így hiába van megoldás a lyuk befoltozására, ugyanolyan kockázatot jelentenek.

Adatátvitel, mint kockázat

Adatátvitel alatt bármilyen információk egyik helyről egy másikra való továbbítását értjük. Az adatátvitelnek megkülönböztetjük vezetékes és vezetéknélküli fajtáit.

Okos mobil eszközök esetében a vezetékes adatátvitel adatkábel segítségével történik. Az adatkábel nem csupán adatok átvitelére szolgál, hanem a telefon akkumulátorának töltését is kivitelezhetjük vele. Az okos mobil eszközök jelenlegi nagy korlátja, hogy a készülék üzemideje rendkívül alacsony. Ellenben a régi „buta" telefonokkal, amelyek akár egy hétig is üzemeltek egy feltöltéssel, az okos telefonok akkumulátora átlagosan egy napig bírja egy feltöltéssel. Az üzemidőt nagyban csökkenti, ha a mobilinternet vagy Wi-Fi folyamatosan üzemel, ha a felhasználó játszik, videót néz stb., így gyakran egy feltöltés egy fél napig elegendő. Tovább rontja a készülék üzemidejét, ha a felhasználó nem kímélte a készüléket akkumulátorát, nem megfelelő módon töltötte fel, összességében elmondható, minél régebb használja az eszközt, annál gyorsabban merül le. Egyes készülékek esetében az akkumulátor cseréjére sem nyílik lehetőség (pl. iPhoneok, számos táblagép).[2] Intenzív eszközhasználat esetében így rendszeres töltést igényelnek a készülékek. Az eszköz töltésére lehetőségünk van klasszikus úton, hálózatból- ez gyorsabb töltést is eredményez-, illetve USB porton keresztül adatkábel segítségével.[3] Ez utóbbi, az adatkábel funkciójából fakadóan igen komoly biztonsági kockázatot jelenthet, ugyanis, ha fertőzött eszközre csatlakoztatjuk a készüléket, utat nyithatunk a támadóknak, hogy megfertőzzék a mobil eszközt. Ez természetesen nem jelent automatikus kockázatot, hiszen ahogy a Stuxnet vírus ismertté válása után a Windows 7 esetében kiadott biztonsági frissítés következtében megszűntették az adathordozók csatlakozását követő automatikus futtatás lehetőségét a számítógépeken [9], úgy mobil eszközök esetében sem minden készülék indítja el az automatikus futtatás funkciót, egyes készülék típusok már védelmet nyújtanak ezzel kapcsolatban, egy felugró ablak segítségével kell engedélyt adnunk, hogy milyen tevékenységet szeretnénk a készülékünkkel végezni (pl. file átvitel). Az adatkábelen keresztül történő támadások következményeiről később lesz szó bővebben.

[2] 2017. év végén ismerte el az Apple, hogy a régebbi készülékek esetében a biztonsági frissítéssel szándékosan lassították a készülékeket, hivatalosan azzal magyarázva, hogy így védjék az akkumulátor üzemidejét, de ezzel nem kimondottan arra sarkalva a vásárlóit, hogy újabb modellre cseréljék le a teljesítményromlásnak kitett eszközüket. [8]

[3] Az iPhone 8 esetében jelent meg újításként vezeték nélküli töltés lehetősége, amelyre a tervek szerint köztereken is kihelyezett töltőpontokat rendszeresítenek, illetve gyorstöltő funkció, ami elvileg 30 perc alatt 50%-os töltöttséget fog eredményezni.

A vezetéknélküli adatátvitel egy okos mobil eszköz tekintetében történhet infravörös fény,[4] Bluetooth[5], mobilinternet vagy Wi-Fi[6] hálózat segítségével. Ezek különböző kockázatot jelenthet. A Bluetooth sebezhetősége 2017 őszén került a média figyelmének középpontjába, amikor az Armis Labs nevű biztonsági cég azonosított nyolc sérülékenységet[7], amik ezt a technológiát használják ki [11]. A BlueBorne néven keresztelt támadóvektor lehetővé teszi a támadóknak, hogy távolról férjenek hozzá a készülékhez. A sérülékenység a mobil eszközök mellett az asztali számítógépeket és operációs rendszereket. A BlueBorne segítségével, miután a támadók hozzáférést szereztek a Bluetooth technológiát használó eszközhöz, azon keresztül hozzáférést szerezhettek a készülékhez csatlakozó eszközökhöz is, valamint az érintett eszköz továbbadhatta a fertőzést a többi Bluetooth-t használó eszköznek is.

A Wi-Fi hálózatok sérülékenysége, legalábbis a nyílt hálózatok esetében kezd közismertté válni, azonban úgy vélem, ez egyben megtéveszti a laikusokat, és hamis biztonságérzetet ad a nyílt Wi-Fi hálózatok használatát illetően. Egy hálózat adatforgalmát a hálózat üzemeltetője képes monitorozni, ily' módon az üzemeltető a hálózaton keresztül lehallgathatja az általunk bonyolított adatforgalmat. Ezek lehetnek különösen érzékeny adatok is, legyen jó jelszavakról, bankkártya adatokról, szöveges üzenetekről, képekről stb. Bár azt mindenképpen pozitív fejleményként értékelem, hogy a szélesebb köztudatban is kezd kialakulni az immunitás a nyílt Wi-Fi hálózatokkal kapcsolatban, és az érzékeny adatokat, mint pl. bankkártya adatokat nem adnak meg ilyen hálózat használata közben. Ez azonban sokszor azzal jár együtt, hogy a laikusok a jelszóval védett Wi-Fi hálózatot biztonságosnak feltételezik, holott ugyanúgy a hálózat üzemeltetője megfigyelheti a hálózaton zajló adatforgalmat.[8] Egy jelszóval ellátott Wi-Fi hálózat esetében nem mindegy a jelszóválasztás. A gyártók a routerek jelszavának alapesetben az internetről is könnyen megtalálható jelszavakat állítanak be, amit, ha a felhasználó nem változtat meg, könnyű hozzáférést biztosít a támadóknak, akiknek a router típusát kell csupán ismerni. Az 5. számú táblázat 101 darab Cisco router adatait tartalmazó felsorolás egy kis részét mutatja be, amelyet egy egyszerű, „router password cisco" kulcsszavakat tartalmazó Google keresés eredményeként kaptam.

[4] Az IrDA (Infrared Data Association) egy ipari szabvány vezetéknélküli adatátvitelhez infravörös fény segítségével. A technológia segítségével csupán egyenes vonalban, illetve kis távolságon, 1 méteren belül használhatjuk adatátvielre. Amióta a bluetooth technológia elterjedt, az infra porton keresztüli adatátvitel kevésbé tekinthető relevánsnak, az újabb készülékek már nem is tartalmazzák. Ennek, valamint korlátozott használhatósága okán e tanulmány keretein belül bővebben nem foglalkozok, a technológia sérülékenysége kapcsán az érdeklődőknek ajánlom Iakovos Gurulian és szerzőtársai Preventing Relay Attacks in Mobile Transactions Using Infrared Light című tanulmányát [10].

[5] A Bluetooth rövid hatótávolságú, adatcseréhez használt, nyílt, vezetéknélküli szabvány.

[6] A Wi-Fi az Institute of Electrical and Electronics Engineers által kifejlesztett vezeték nélküli mikrohullámú kommunikációt (WLAN) megvalósító, széleskörűen elterjedt szabvány (IEEE 802.11) neve.

[7] Az érintett sérülékenységek: (1)Linux kernel RCE sebezhetőség– CVE-2017-1000251, (2) Linux Bluetooth (BlueZ) információ sebezhetőség – CVE-2017-1000250, (3) Android információ sebezhetőség – CVE-2017-0785, (4) Android RCE sebezhetőség #1 – CVE-2017-0781, (5)Android RCE sebezhetőség #2 – CVE-2017-0782, (6) The Bluetooth Pineapple in Android – Logical Flaw CVE-2017-0783, (7) The Bluetooth Pineapple in Windows – Logical Flaw CVE-2017-8628, (8) Apple Low Energy Audio Protocol RCE vulnerability – CVE-2017-14315

[8] Ezt a bizalmat kihasználandó semmibe nem kerül a támadóknak egy olyan hálózatot létrehozni, amit jelszóval látnak el, majd ezt a jelszót megosztják a csatlakozni kívánókkal.

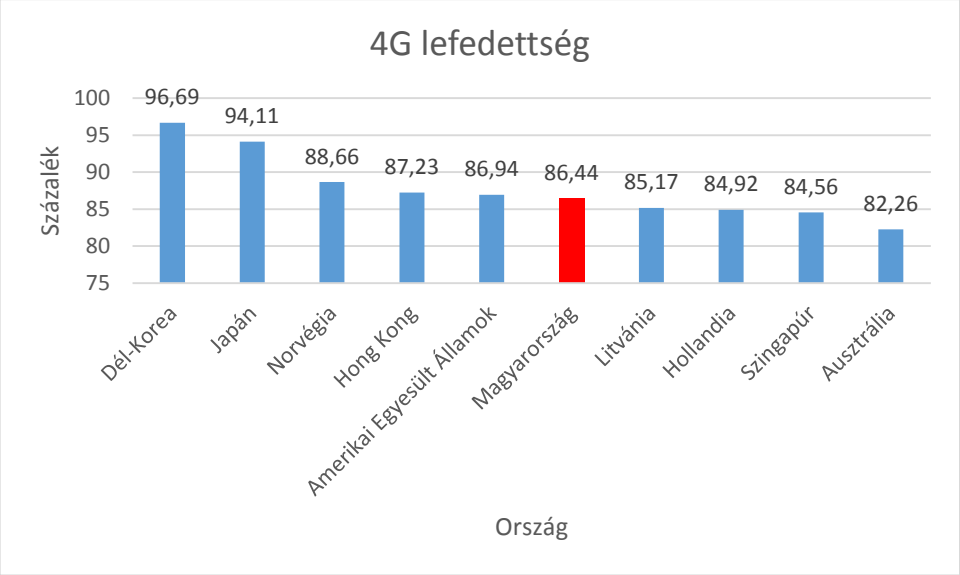
Cisco Model	Alapértelmezett felhasználó név	Alapértelmezett jelszó	Alapértelmezett IP cím
ESW-520-24-K9	cisco	cisco	192.168.10.2
ESW-520-24P-K9	cisco	cisco	192.168.10.2
ESW-520-48-K9	cisco	cisco	192.168.10.2
ESW-520-48P-K9	cisco	cisco	192.168.10.2
ESW-520-8P-K9	cisco	cisco	192.168.10.2
ESW-540-24-K9	cisco	cisco	192.168.10.2
ESW-540-24P-K9	cisco	cisco	192.168.10.2
ESW-540-48-K9	cisco	cisco	192.168.10.2
ESW-540-8P-K9	cisco	cisco	192.168.10.2
RV016	admin	admin	192.168.1.1
RV042	admin	admin	192.168.1.1
RV042G	admin	admin	192.168.1.1
RV082	admin	admin	192.168.1.1

5. táblázat Cisco routerek alapértelmezett jelszavai és felhasználó nevei (saját szerkesztés, forrás: LifeWire [12]

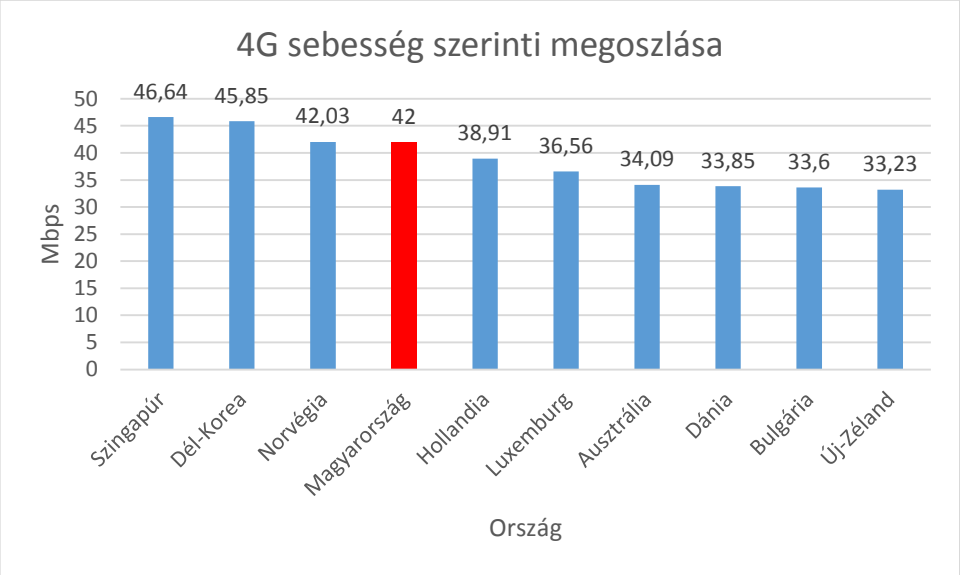
Ez egyben azt is jelenti, hogy a saját, otthoni hálózatunkhoz is könnyűszerrel férhetnek hozzá a támadók, amennyiben nem változtattuk meg a router jelszavát. 2015-ben a SearchLab nevű biztonsági cég a magyarországi UPC által telepített modemek biztonságát vizsgálva fedezte fel azok sérülékenységét, amely széles körben használt UBEE gyártmányú wifi routert érintette [13]. A kutatók visszafejtették az algoritmust, amivel a Wi-Fi hálózati azonosítójából (az SSID-ből) közvetlenül kitalálhatóvá vált a jelszó. A vizsgálatok során a Cisco routerjeit ilyen módon pár perc, míg Technicolor egyik modelljét 5 másodperc alatt fejtették vissza. Ehhez hasonló támadást, ismerve az eszközök biztonsági réseit, az utcán sétálva egy laptoppal, antenákkal és Wi-Fi adapterekkel könnyűszerrel végre tudnak hajtani a támadók. A Wi-Fi hálózat azonban nem csupán a routereken keresztül támadható, a Wi-Fi protokoll sebezhetőségét is tárták már fel biztonsági szakemberek [14]. A KRACK (Key Reinstallation AttaCK) nevű sérülékenység a Wi-Fi kliensük védett Wi-Fi hálózathoz való csatlakozásakor végrehajtott négylépéses hitelesítési folyamat harmadik lépés esetében felfedezett biztonsági rést használta ki. A harmadik lépésben a titkosító kulcs többször is újraküldésre kerül, amit a támadók megfelelő módon összegyűjtenek és újra lejátsszák ezeket az újraküldéseket, aminek következtében fel tudják törni a Wi-Fi titkosítást. Ehhez azonban a támadóknak fizikailag közel kell kerülniük a megtámadni kívánt hálózathoz, hogy lehallgathassák ezeket a Wi-fi hitelesítési kéréseket. Szakértők szerint a sérülékenység az Androidos készülékek 41%-át érintette. Segítségével többek között feltörhető a Wi-Fi titkosítás, valamint csomag újrajátszás, TCP kapcsolat eltérítés és HTTP tartalom beillesztés hajtható végre. Az utóbbi révén a támadók titokban programkódot szúrhatnak be az általunk meglátogatott weboldalakba, hogy rosszindulatú programokkal, zsarolóvírusokkal fertőzzék meg az eszközt. A biztonsági rést javító frissítés megérkezéséig a szakértők vezetékes ethernet kapcsolat vagy mobilinternet használatát javasolták. Az okos

mobil eszközök tekintetében csak a mobilinternet jelenthetett védelmet, azonban az előfizetés sok esetben drága, nem biztosít elégséges adatforgalmat.

Bár Magyarország globális összehasonlításban kiemelkedő helyen szerepel a 4G lefedettségét (86,44%) és sebességét (42 Mbps) illetően (bővebben lásd a 5. és 6. számú ábrákat) [15], azonban a 2017-es Digitális Gazdaság és Társadalom adatait figyelembe véve 2016-ban 100 magyar lakosból csak 43-nak volt hozzáférése a mobil szélessávhoz [16]. A relatíve drága magyar mobilinternet oka így abban mutatható ki, hogy a szolgáltatók kevés ügyféltől szedik be a hálózatépítés- és üzemeltetés költségét [17].



5. ábra Globális 4G lefedettség 2017. november (saját szerkesztés, forrás: Open Signal [15])



6. ábra Globális 4G sebesség 2017. november (saját szerkesztés, forrás: Open Signal [15])

A mobilinternet előfizetések számának alakulása így közvetetten jelent biztonsági kockázatot, különösen a fiatalok körében, akiknél az okos mobil eszköz használat sok esetben addiktívnak tekinthető- ennek okairól később bővebben lesz még szó. Azoknak, akik nem engedhetnek meg maguknak megfelelő mobilinternet előfizetést, azok számára a nyílt Wi-Fi

marad a megoldás az internetezésre az otthoni használaton kívül. Természetesen nem az ördögtől való a nyílt Wi-Fi hálózat használata sem, amennyiben betartunk néhány alapszabályt: kizárólag HTTPS titkosítást alkalmazó weboldalakat[9] keressünk fel, illetve célszerű virtuális magánhálózatot (VPN-t) használni, amelynek segítségével elrejthetjük a hálózati forgalmat.[10]

Alkalmazások, mint kockázat

Az okos mobil eszközök biztonságával kapcsolatban az egyik legnagyobb számban előforduló fenyegetést az alkalmazások jelentik. A készülékre telepített alkalmazások a kockázatok széles tárházát nyitják meg. A támadások sokfélék lehetnek, amelyeket kellő körültekintéssel minimalizálhatunk, de még a legnagyobb óvatosság sem jelenthet 100%-os védelmet. Az okos mobil eszközökre optimalizált alkalmazásokat alapesetben valamilyen hivatalos alkalmazás áruházból tölthetjük le pénzért cserébe vagy ingyen. Az ingyenesség azonban sokszor csupán látszat, az alkalmazások többsége cserébe hirdetéseket jelenít meg számunkra, rosszabb esetben az adatainkkal kereskedik [19]. Ahogy az operációs rendszerek kockázatait bemutató résznél volt szó róla, eltérő az egyes alkalmazás áruházak biztonsága, az Androidos alkalmazások jelentős része valamilyen kártevővel fertőzött. A fizetős tartalom sokszor olyan csábítást is jelent azonban, hogy azt valamilyen illegális úton, külső forrásból telepítsük készülékünkre. Ez alapesetben a készülékeknél le van tiltva, azonban bármikor engedélyezhetjük, hogy olyan alkalmazást is telepítsen az eszköz, amit nem hivatalos áruházból szereztünk be. Ez magában hordozza azt a kockázatot, hogy valamilyen rosszindulatú programmal fertőzött vagy adathalász alkalmazást telepítsünk. A támadók gyakran másolnak le népszerű alkalmazásokat, amelyekben elrejtik a céljuknak megfelelő kártékony kódokat vagy az eredeti alkalmazásokat fertőzik meg, és teszik illegális úton letölthetővé- sokszor az ingyenes hozzáférést ígérve a gyanútlan felhasználóknak. [11]

A letöltést követően a telepítés jelentheti a következő kockázatot. Minden alkalmazás a használatért cserébe különböző alkalmazás engedélyeket kér. Ezek az engedélyek széleskörűek lehetnek, de alapesetben olyan funkciókat, amelyek a használathoz szükségesek. Egy zseblámpa alkalmazáshoz természetesen elengedhetetlen a vakuhoz való hozzáférés, hiszen a használatkor a vaku fénye szolgál a világításhoz. A támadók tisztában vannak azzal, hogy a felhasználók nagyon kis százaléka olvassa el, mihez ad engedélyt egy alkalmazás telepítésekor, ezért rengeteg alkalmazást adathalászat céljából készítenek el. A Facebook alkalmazás közel 30 különböző engedélyt kér a használatért cserébe, többek között személyes adatok (névjegyadatok), tartózkodási hely (hálózatalapú és GPS alapú helymeghatározás), hálózati kommunikáció (teljes internet hozzáférés), fiókok adatai (üzenetek olvasása), tárhely (lehetőség az USB-tároló tartalmának módosítására vagy törlésére), telefonhívások, hardver vezérlők (fénykép és videókészítés, hangrögzítés), rendszereszközök (szinkronizálás). Egyes alkalmazások, kihasználva a gyártók piaci fölényüket, alapértelmezetten telepítve vannak bizonyos készülékeken, amit rendszergazda jogosultsággal nem rendelkező felhasználók nem tudnak törölni. Ily módon úgyis kiszolgáltatjuk az adatainkat, hogy nincs lehetőségünk nemet mondani az alkalmazások adatgyűjtésére. [12] Mivel egy alkalmazás, ha engedélyezzük, gyakorlatilag mindenhez hozzáférhet, ami a készüléken szerepel, a megfigyelés majdnem

[9] A HTTPS kapcsolat sem jelent automatikus védelmet, kifinomultabb adathalász oldalakat a támadók alapból HTTPS kapcsolattal hoznak létre, hogy ezzel növeljék az odatévedők bizalmát.
[10] A VPN-ek esetében nem feltétlenül célszerű ingyenes szolgáltatást igénybe venni, ugyanis azok is lehallgathatják az adatforgalmat.
[11] Az is előfordulhat, olyan hypeolt alkalmazásokat használnak ki, amelyek még nem érhetőek el globálisan mindenhol, csupán bizonyos országokban, ahogy tették például 2016 nyarán a Pokémon Go-val.
[12] Ilyenek például a Google alkalmazásai az Androidos készülékeken vagy a telefongyártók saját alkalmazásaik.

tökéletes eszközévé válhat. A probléma, hogy nem tudjuk, kik, illetve milyen célból kezelik az adatainkat. Számos alkalmazás esetében derült ki, hogy több százmilliós letöltött alkalmazások kértek olyan plusz engedélyeket, ami indokolatlan volt,[13] valamint adták el az így begyűjtött adatokat harmadik fél részére [18].[14] Hogy mit kezdenek az adatainkkal, a támadó motivációjának függvénye: a leggyakoribb a reklám célokra való felhasználása, de visszatérő lehet a social engineer támadásoknál, a kiberbűnözés és kiberkémkedés esetében egyaránt. Minél több időt töltünk az eszközünk, az alkalmazásaink használatával, annál több adat keletkezik rólunk. Ezek big data elemzéssel igen pontos előrejelzést is adhatnak a felhasználó szokásairól, jövőbeli cselekedeteiről.

Az alkalmazások jelentette kockázatok következő nagy kategóriája az alkalmazásokba ágyazott kártékony kódok. Ezek ismét szerteágazók lehetnek, irányulhatnak arra, hogy kémkedjenek a felhasználók után, titkosítsák a fájlokat, átvegyék az irányítást az eszköz fölött, botnet hálózat részévé váljon a készülék[15] stb.

Léteznek olyan alkalmazások is, amelyek a felhasználókkal elhitetik, emberekkel kommunikálnak, holott valójában botnet hálózatokkal, és ily módon igyekeznek pénzt kicsalni belőlük [21].

A védelmünk érdekében elengedhetetlen, hogy körültekintéssel töltsük fel az alkalmazásokat, amiket használni szándékozunk, és alaposan fontoljuk meg, hogy valóban telepítjük-e, mert úgy ítéljük meg, semmilyen vagy éppen elfogadható biztonsági kockázatot jelent számunkra. Az alkalmazások használata során azonban bármikor felfedezhetnek biztonsági réseket, amelyeket a frissítés megjelenését követően célszerű azonnal telepíteni. Tisztában kell azonban azzal lenni, hogy a frissítések is lehetnek a támadás eszközei. Ahogy a 2017 nyarán lezajlott NotPetya ransomware esetében a támadók egy könyvelő szoftver biztonsági frissítésébe ágyazták a kártékony kódot [22], és globális kampány során folytatták tevékenységüket, úgy több alkalmazásról derült ki korábban, hogy az eredetileg letöltött alkalmazás mentes volt a rosszindulatú programoktól, hogy az ellenőrzésen átmenjen, de a frissítések, amiket nem ellenőriztek az alkalmazás áruházban már tartalmazták a kártevőket [23].

Hardware, mint kockázat

2018 első napjaiban vált ismertté, hogy az Intel, az ADM és ARM processzorok igen súlyos biztonsági rést tartalmaznak, amelyek egyaránt érintik a számítógép mellett a telefongyártókat is [24]. A sérülékenységek kihasználásával hozzáférhetnek az eszközök memóriájában tárolt adatokhoz, akár a jelszavainkhoz is. A beszámolók először csupán az Intel sebezhetőségéről szóltak, ám hamar kiderült, az ADM és ARM processzorok is érintettek. A sérülékenység az ASLR (address space layout randomization) technikából fakadt, amit az 1990-es években fejlesztettek ki abból a célból, hogy megnehezítse a kernel oldali sebezhetőségek kihasználását. Azonban egy olyan hardveres hibát fedeztek fel az Intel processzoraiban van, ami lehetővé tesz bizonyos külső támadásokat, amelyek magát az implementációt érintő hardveres problémákat kihasználva hozzáférhetnek a memóriában tárolt adatokhoz, ezen belül is a kernelmemóriához.

[13] Például zseblámpa alkalmazás a vakun kívül az üzeneteink tartalma, ismerőseink stb.

[14] Külön kockázatot jelentenek azok az alkalmazások, amelyek valamilyen csatlakoztatott külső eszköz vezérlésért felelnek, és úgy is gyűjtenek adatokat, amik indokolatlanok. Több adatvédelmi incidens volt olyan okos mobil eszközökre csatlakoztatható szexuális segédeszközökről, amelyek egyrészt gyűjtötték a felhasználói szokásokat, másrészt rögzítették a használat közbeni hangokat, s ezeket továbbították [20]. Nem nehéz belátni, ezeknek az adatoknak a birtokosa milyen könnyen zsarolhatja adott esetben a felhasználót.

[15] Botnet hálózatokban mobil eszközöket ugyanúgy használnak túlterheléses támadásra, spamküldésre vagy kriptovaluta bányásására

A „Meltdown” és „Spectre” névre elkeresztelt sérülékenységekből három támadás típust nevesítettek, az bounds check bypass (CVE-2017-5753), branch target injection (CVE-2017-5715) a Spectre, a rogue data cache load (CVE-2017-5754) a Meltdown sérülékenységét használja ki.

Telefonhasználat, mint kockázat

Egyre többen adnak hangot annak a feltételezésnek, hogy a telefonhasználat ugyanolyan függőséget okoz, mint a drogok, ennek érdekében pedig a gyártók mindent megtesznek, hogy viselkedéspszichológusokkal közösen minél addiktívabbá alakítsák az alkalmazásokat, eszközöket. Az Apple két nagy részvénytulajdonosa, a Jana Partners és a California State Teachers' Retirement System nyílt levelet tett közzé 2018 év elején [25], amelyben arra kérte a gyártót, hogy fordítson nagyobb hangsúlyt a gyermekek védelmére, akik körében kutatások szerint egyre nagyobb mentális problémát okoz az okos mobil eszközök használata. Ezek alapján aggasztó mértékben növekszik a fiatalok körében a figyelemhiány, a depresszió, alváshiány és az ebből származó egészségügyi problémák, az öngyilkosság. A levél írói megoldásként szakértői tanács felállítását javasolják, aminek tagjai közé gyermekfejlődési szakértőket is delegálnának, valamint olyan szoftverek fejlesztését javasolják, amelyek segítségével a szülők hatékonyabban védhetnék meg a gyermekek egészségét.

Az, hogy lenne mi ellen védekezni, nem kérdés [26]. A fejlesztők igen komoly pszichológiai kutatásokat végeznek, és építenek be termékeikbe, hogy a felhasználók minél több időt töltsenek el az alkalmazásokat használva. Példaként gyakran a Facebook like gombját szokták felhozni, ami az agyunk dopamintermeléséért felelős részét ingerli oly módon, hogy az azonnali visszaigazolások hatására, mintegy pavlovi reflex alakul ki bennünk, a likeok hatására. Ha azt érezzük, másoknak tetszik, amit teszünk, akár csak a drogok esetében, dopamin szabadul fel, ami az örömérzetet okozza. Hogy ez növekedjen, egyre több ilyen ingerre van szükségünk, így többet posztolunk, olyan tartalmakat, amik szerintünk érdeklődésre tartanak számot, ezek elmaradása esetén pedig rossz közérzet válhat uralkodóvá. De ezen kívül számos technikát alkalmaznak a figyelmünk minél többszöri megragadása és a függőség növelésére. Ilyen például az úgynevezett váratlan jutalom elve, amelynek hatására az értesítések véletlenszerűen érkeznek, ezzel sarkalva a felhasználót, minél többször ellenőrizze az eszközét. Ennek oka a félelem, hogy lemaradunk valami fontosról. [27] A probléma, hogy ezeket a kihasználható emberi gyengeségeket tudatosan építik be a fejlesztők az alkalmazásaikba, amelyek igen komoly mentális problémákat okoznak. Ebből a függőségből aztán következményként megjelennek azok a közvetett fenyegetések, amelyeket e tanulmány során részletesen ismertettem. Amikor digitális immunerősítésről beszélünk, rendkívül nehéz dolgunk van, hogy növeljük a felhasználók biztonságtudatosságát, hiszen nem egyszerű pl. a nyílt Wi-Fi hálózatok veszélyeire felhívni a figyelmet valakinek, aki függősége miatt állandó késztetést érez, hogy ellenőrizze, kapott-e új értesítést valamilyen általa használt alkalmazástól.

ÖSSZEGZÉS

Tanulmányomban igyekeztem bemutatni az okos mobil eszközök jelentette biztonsági kockázatokat. A téma, mint látható, rendkívül széleskörű, az egyes területek önmagukban is önálló tanulmányokat érdemelnének. Megítélésem szerint az okos mobil eszközök kiberfenyegetettsége éppen azért ilyen sokrétű, mert rajtuk keresztül életünk minden perce kontrollálható, a szabadidőnk, munkavégzésünk jelentős részét ezeken az eszközökön keresztül hajtjuk végre, így igen komoly anyagi károkat is szenvedhetünk el a nem megfelelő használat során. Ezekből fakadóan a támadóknak továbbra is kiemelt célpontjai lesznek ezek az eszközök,

amik ellen jelentős részben védekezhetünk, ha tudatosan használjuk őket.[16] Reményeim szerint e tanulmány hozzájárul ehhez.

FELHASZNÁLT IRODALOM

[1] HuMarc: *Okostelefon-evolúció,* In. LogOut, 2013. május 15., https://logout.hu/cikk/okostelefon-evolucio/bevezeto.html (Letöltés dátuma: 2017. november 4.)

[2] TelefonGuru, http://www.telefonguru.hu/ (Letöltés dátuma: 2017. november 4.)

[3] KEMP, SIMON: *Digital in 2017- Global overview, We are social*, 2017. január 24., https://wearesocial.com/special-reports/digital-in-2017-global-overview (Letöltés dátuma: 2017. november 4.)

[4] *Gartner Says Worldwide Sales of Smartphones Grew 9 Percent in First Quarter of 2017,* In. Press Release, 2017. május 23., https://www.gartner.com/newsroom/id/3725117 (2017. november 4.)

[5] *Android Security Bulletin*—August 2016, In. Android.com, 2016. augusztus 1., https://source.android.com/security/bulletin/2016-08-01 (Letöltés dátuma 2017. november 6.)

[6] DÖMÖS ZS.: *Halálos ítéletet kapott a Microsoft mobilszoftvere*, In. 24.hu, 2017. október 9., http://24.hu/mobil/2017/10/09/halalos-iteletet-kapott-a-microsoft-mobilszoftvere/ (Letöltés dátuma: 2017. november 6.)

[7] DÖMÖS ZS.: *Hivatalosan is halott a Windows Phone,* In. 24.hu, 2017. szeptember 12., http://24.hu/mobil/2017/07/12/hivatalosan-is-halott-a-windows-phone/ (Letöltés dátuma: 2017. november 6.)

[8] *A Message to Our Customers about iPhone Batteries and Performance,* In. Apple, 2017. december 28., https://www.apple.com/iphone-battery-and-performance/ (Letöltés dátuma: 2017. december 30.)

[9] Kovács L.- Sipos M.: *A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala*, In. Hadmérnök, V. évfolyam, 4. szám, pp. 163-172., 2010.

[10] IAKOVOS G. ET. AL.: *Preventing Relay Attacks in Mobile Transactions Using Infrared Light,* In. Proceeding SAC '17 Proceedings of the Symposium on Applied Computing, pp. 1724-1731, https://pure.royalholloway.ac.uk/portal/files/27887119/main.pdf (Letöltés dátuma: 2018. január 10.)

[11] *The Attack Vector "BlueBorne" Exposes Almost Every Connected Device*, In. Armis, https://www.armis.com/blueborne/ (Letöltés dátuma: 2018. január 10.)

[12] FISHER, T.: *Cisco Default Password List- Updated List of Cisco Default Passwords, IP Addresses, and Usernames,* In. LifeWire, 2018. január 2., https://www.lifewire.com/cisco-default-password-list-2619151 (Letöltés dátuma: 2018. január 10.)

[16] A tudatosság mellett kiemelt szerep jut a kockázatelemzésre is természetesen, de a tanulmány keretei nem teszik lehetővé, hogy ezzel bővebben foglalkozzak, Szádeczky Tamás tanulmányait javaslom a téma iránt érdeklődőknek [28] [29].

[13] SearchLab: *Analysis of WiFi-enabled ISP modems*, In. SearchLab, https://www.search-lab.hu/advisories/secadv-20150720 (Letöltés dátuma: 2018. január 10.)

[14] VANHOEF, M.- PIESSENS, F.: *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*, In. ACM Conference on Computer and Communication Security (CCS 2017) USA, Dallas, 2017. október 30- november 3., https://papers.mathyvanhoef.com/ccs2017.pdf

[15] *The State of LTE* (November 2017), In. Open Signal, https://opensignal.com/reports/2017/11/state-of-lte (Letöltés dátuma: 2017. december 20.)

[16] *Europe's Digital Progress Report 2017*, In. European Comisson, https://ec.europa.eu/digital-single-market/en/scoreboard/hungary (Letöltés dátuma: 2017. december 20.)

[17] NAGY P. ET. AL.: *Az elveszett mobilinternet nyomában- A magyar mobil szélessáv penetrációs lemaradásának lehetséges okai, Verseny és Szabályozás, 2016*. (Szerk. Valentiny Pál et.al.), MTA KRTK Közgazdaság-tudományi Intézet, Budapest, 2016.

[18] SZABÓ A: *A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból I. rész* - Személyi számítógépek, In. Hadmérnök XII. Évfolyam KÖFOP különszám - 2017., pp. 163-180.

[19] *Adatokat eltulajdonító androidos zseblámpa alkalmazás,* In. GovCERT, 2013. december 6., http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (Letöltés dátuma: 2017. december 16.)

[20] HERN, A.: *Someone made a smart vibrator, so of course it got hacked*, In. The Guardian, 2016. augusztus 10., https://www.theguardian.com/technology/2016/aug/10/vibrator-phone-app-we-vibe-4-plus-bluetooth-hack (Letöltés dátuma: 2017. december 16.)

[21] ALLEN, K.: *Chinese dating apps closed after women revealed to be robots*, In. BBC, 2018. január 8., http://www.bbc.com/news/blogs-news-from-elsewhere-42609353 (Letöltés dátuma: 2018. január 8.)

[22] SZŰCS P: Ehhez képest a WannaCry felüdülés volt, In. IT Cafe, 2017. június 28., https://itcafe.hu/hir/petya_notpetya_zsarolovirus.html (Letöltés dátuma: 2017. december 28.)

[23] *Trojan targeted dozens of games on Google Play*, In. Dr. Web, 2016. január 28., https://news.drweb.com/show/?i=9803&lng=en (Letöltés dátuma: 2017. december 28.)

[24] STATT, N.: *Apple confirms all Mac and iOS devices are affected by Meltdown and Spectre bugs*, In. The Verge, 2018. január 4., https://www.theverge.com/2018/1/4/16852016/apple-confirms-mac-ios-affected-spectre-meltdown-chipocalypse (Letöltés dátuma: 2018. január 8.)

[25] *Open Letter From Jana Partners And Calstrs To Apple Inc*., In. Think Differently about Kids, 2018. január 6., https://thinkdifferentlyaboutkids.com/index.php?acc=1 (Letöltés dátuma: 2018. január 8.)

[26] KRASZNAY CS.- VARGA- PERKE B.: *Ifjúságvédelem a hacker szubkultúrában*, In: Ártalmas vagy hasznos internet?, A média hatása a gyermekekre és fiatalokra (szerk. In: Bíró A Zoltán, Gergely Orsolya), Csíkszereda: Státus Kiadó, pp. 179-202., 2013.

[27] HARRIS, T.: *How Technology Hijacks People's Minds*, In. Huffington Post, 2017. december 6., https://www.huffingtonpost.com/tristan-harris/how-technology-hijacks-peoples-minds_b_10155754.html (Letöltés dátuma: 2017. december 28.)

[28] SZÁDECZKY, T.: *The role of technology. Auditing and certification in the field of data security*. In.: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest 2012, ISBN 9789632581972, pp. 311-337.

[29] SZÁDECZKY T.: *Risk Management of New Technologies,* Academic and Applied Research in Military and Public Management Science 15:(3) pp. 279-290. 2016.