HADMÉRNÖK

XIII. Évfolyam „KÖFOP” szám – 2018. január

A FELHASZNÁLÓK DIGITÁLIS LÁBNYOMÁNAK, ANONIMITÁSÁNAK VIZSGÁLATA TECHNIKAI SZEMPONTBÓL II. RÉSZ MOBIL ESZKÖZÖK

DEMONSTRATING USER ANONYMITY AND DIGITAL FOOTPRINT WITH TECHNICAL TOOLS PART II. - MOBILE DEVICES

SZABÓ András

(ORCID: 0000-0002-8750-8557)

szabo.andras@uni-nke.hu

Absztrakt

Jelen cikksorozat a felhasználói kiberhigéniás szokások és gyakorlatok bemutatásával foglalkozik. A felhasználóra leselkedő fenyegetések bemutatása mellett javaslatokat tesz azok csökkentésére, a védelem fokozására. Ez napjainkban mindenki számára fontos, a közszolgálatban dolgozók pedig kiemelten érintettek lehetnek magánemberként, és a szervezetük informatikai rendszerének felhasználójaként is. Mindennap használjuk, mégis ritkán vizsgáljuk meg, hogyan is működnek az internetelérésre használt számítógépeink és okos eszközeink. Jelen cikksorozat a biztonságos számítógép használatra hívja fel a figyelmet, illetve a felhasználók személyes adatainak védelme érdekében az anonim internetezés lehetőségeit mutatja be. Az ajánlások a személetesség érdekében praktikus tanácsokat, és technikai jellegű példákat is tartalmaznak. Napjainkban a felhasználók internetelérésre jellemzően kétféle eszközt használnak: a klasszikus személyi számítógépeket (asztali és hordozható kivitelűeket), és a mobil eszközöket (okostelefonokat, tableteket és a viselhető okos eszközöket). Ez a két eszközcsoport eltérő megközelítést igényel, így a cikksorozat első része a „klasszikus” személyi számítógépekkel foglalkozik, majd a második rész a mobil eszközökre fókuszál.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *biztonságtudatosság, Informatikai biztonság, digitális lábnyom, anonimitás*

Abstract

This article deals with the Internet user's habits and practices. In addition to presenting threats to the users, I made some suggestion to reduce them and increase the security awareness of the reader. Today, this knowledge can be important for everyone who is using the Internet, but those who work in the public service need to be particularly concerned about privacy and security (as a home user, and also as a user of their department's IT system). We use our computers and smart devices every day, but we rarely look at how they really work. This article series focuses on to use of computers securely, and also how to access the Internet anonymously to protect personal information. Recommendations include practical advice and technical examples. Nowadays users are accessing the Internet using two main types of devices: computers (desktop and portable), and mobile devices (smartphones, tablets, and wearable devices). These two sets of devices require different approaches, so the first article in this series deal with "classical" personal computers, and the second focuses on the mobile devices.

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 Ludovika Workshop.

Keywords: *security awareness, IT security, digital footprint, anonymity*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.30.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.10.09.

BEVEZETÉS (MOBIL TECHNOLÓGIA FEJLŐDÉSE)

A mobil eszközök (okostelefon, okos óra, okos TV) védelmére azok elterjedésével, és az ellenük irányuló támadások számának, fejlettségének növekedésének következtében készülni kell. Sajnálatos módon ebben az új technológiai szegmensben még nem alakultak ki olyan iparági szabványok, útmutatók és "bevált gyakorlatok" (un. „best practice”-ek), melyek a klasszikus számítástechnikai architektúrák esetén már évek, esetenként évtizedek óta léteznek.

A hetvenes-nyolcvanas években a számítástechnikai eszközök elterjedése reformálta az irodai munkavégzést, a 90-es években az internet az online kereskedelem elterjedését tette lehetővé (ezzel pedig évtizedes hagyományokkal rendelkező kereskedelmi modelleket változtatott meg). A 2000-es években már az otthonokban is megjelentek a számítógépek. A 2010-es években megjelentek az okostelefonok – a mobil távközlés és számítástechnika integrációjának eredménye – melyek napjainkban nélkülözhetetlen eszközökké váltak.

A korosztályi olló, mely az újszerű technológiák elterjedését sokszor akadályozza, egyre szélesebbre nyílik a mobiltechnológia széleskörű elterjedésének köszönhetően. Szinte már nem található olyan hétköznapi-, vagy munkavégzésből fakadó feladat, mely nem függ össze számítógépes rendszerekkel. Ha utazást tervezünk, az időjárásra vagyunk kíváncsiak, a napi eseményekről informálódunk, hivatalos ügyeinket intézzük, vásárlunk, már nagy valószínűséggel elektronikus rendszereken keresztül tesszük mindezt.

A közigazgatásban is egyre nagyobb szerepet kapnak a feladatok automatizálása, az ügyintézés könnyítése, valamint a közérdekű információk megosztásának egyszerűsítése érdekében kialakított informatikai rendszerek, melyeket mind nagyobb számban mobil platformokról érnek el a felhasználók.

A vállalkozások is egyre nagyobb mértékben használják a számítástechnika és az internet adta lehetőségeket. Egyrészt a költséghatékonyságra való törekvés, a törvényi és jogszabályi kötelezettségeknek való megfelelés, de leginkább a felhasználói igények miatt kénytelenek váltani a piaci szereplők. A vállalatok, közigazgatási szervezetek a költséges IT infrastruktúra fejlesztését sokszor a munkavállalók saját eszközeinek felhasználásával kerülik ki. Egyre nagyobb divatja van, az un „home-office”-nak, melynél a munkavállaló otthonából, saját eszközein végzi a munkáját. A munkáltatónak csökkenek az infrastrukturális kiadásai, a munkavállaló pedig rugalmas munkaidejét jobban tudja a napi rutinjához illeszteni. A saját eszközökön végzett munka más szempontból is előnyös a munkáltatónak. Például, így a munkavállaló bármikor elérhető válik, szükség esetén bárhonnan meg tudja oldani a feladatát.

Minden innováció feloszthatő szakaszokra, ha az elterjedését és elfogadottságát vizsgáljuk. Az első szakaszban csak egy szűk kör kezdi használni, jellemzően valamilyen speciális célra. Amikor az adott technológia felhasználói köre elér egy kritikus felhasználószámot, akkor egy robbanásszerű terjedés következik be, ennek kezdetén csak az érdeklődök kezdik el használni, majd újabb és újabb alkalmazási területeket fedeznek fel. Végül kényszerből azok is kénytelenekké válnak használni, akik önszántukból nem akarták ugyan használni, de mivel a korábban használt megoldások, szolgáltatások vagy technológiák megszűntek így rákényszerültek.

Ez volt megfigyelhető az okostelefonok esetén is. Kezdetben néhány érdeklődő használta, majd a technológia kezdeti hiányosságait (kezdetleges operációs rendszerek, szoftveres és hardveres hibák, lassú processzorok, egyszálú folyamat végrehajtás, alacsony élettartalmú akkumulátorok stb.) követő innovációk hatására már széles tömegek is megszerették. Majd, mivel a mobil távközlési piac átrendeződött (a korábbi nagy gyártók beszüntették tevékenységüket, mint például a Sony-Ericsson[1], vagy váltottak mint a Blackberry[2]), már a

1 http://www.cellular-news.com/story/51529.php

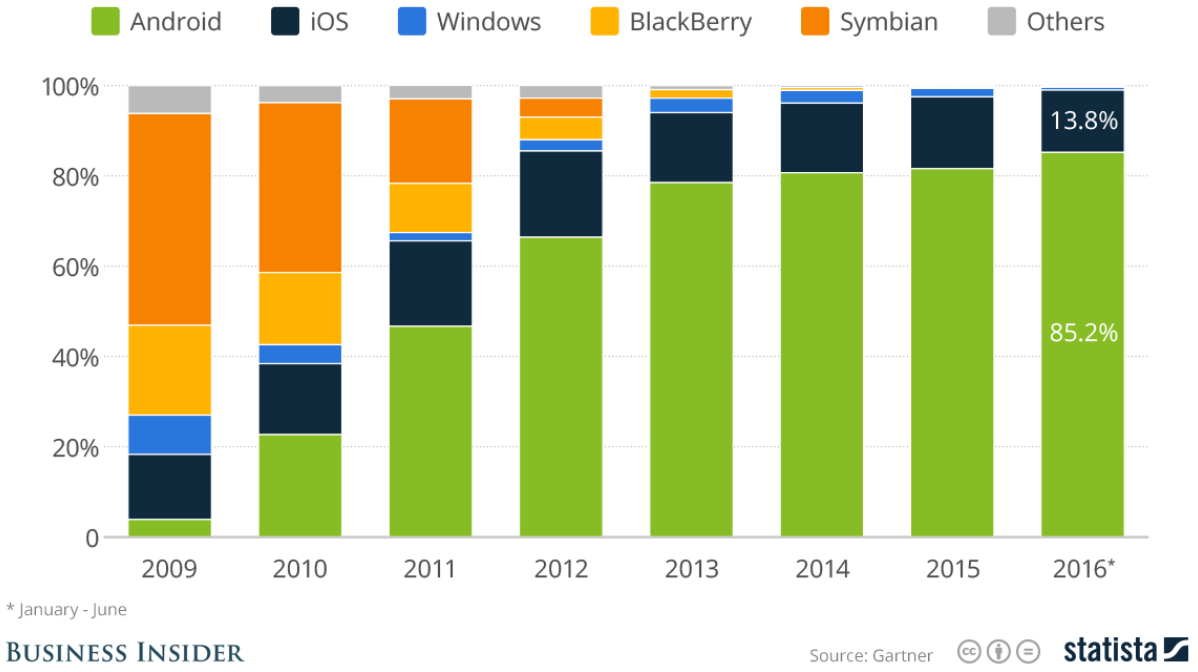
2 https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

"hagyományos", nyomógombos mobiltelefonok kedvelői is kénytelenekké váltak áttérni az „érintőkijelzőre”.

A kezdetben csak magánszemélyek által használt eszközök mellett megjelentek a vállalati eszközök, melyek felügyelete üzemeltetési- és biztonsági kihívások elé állította az addig csak a "klasszikus" asztali és mobil számítástechnikai eszközökkel (PC, laptop stb.) foglalkozó informatikai üzemeltetőket.

A "klasszikus" asztali számítógépes piacot három nagy szereplő osztja fel: a Microsoft, az Apple és a különböző Linux rendszerek (vannak még más szereplők is, de piaci részesedésük eltörpül az előző háromhoz képest)[3]. Az operációs rendszerek a hardver piacot is determinálják, a Apple cég saját hardvereket gyárt, a többi hardvergyártó pedig igyekszik a másik két piaci szereplővel kompatibilis hardvereket gyártani (a fő cél általában a Windows platformokkal való kompatibilitás).

Ezzel szemben a mobil hardver piac új, és így új hardver gyártók törtek fel a már meglévő óriáscégek mellé. Az Android élenjárása az operációs rendszer nyíltságának, fejleszthetőségének köszönhető. Az Apple cég a felső-kategóriás vásárlókat célozza, míg a Microsoft és a Blackberry elsősorban a vállalati felhasználókat.



1. ábra Mobil operációs rendszerek piaci részesedése [1]

ANDROID

Eredetileg a Google által kifejlesztett mobil operációs rendszer az, mely elsősorban az érintőképernyős alkalmazásokhoz lett kialakítva. Linux operációs rendszer képezi alapját, így forráskódja nyíltan elérhető. Ez vezetett a „közösség” által irányított fejlesztési módszertanhoz, mely során a rendszer továbbfejlesztését, az újításokat, a felhasználók igényeihez illesztik. Mivel a forráskódja nyíltan elérhető, ezért számtalan programozó-fejlesztő készít rá alkalmazást. A gyártók is hozzáférnek a forráskódhoz, könnyen módosítani is tudják azt elképzeléseik szerint, így a hardveres fejlesztéseik gyorsan megjelenhetnek a piacon (mivel azokat szoftver oldalról támogatják). A nyíltság és a popularitás azonban veszélyeket is rejt, így ez a platform napjainkban a fő célpontja a kiberbűnözőknek.

3 http://www.ecommercetimes.com/story/84085.html

IOS

Az iOS az Apple cég által gyártott okostelefonokra fejlesztett operációs rendszer. A cég törekszik a felhasználók igényei szerint fejleszteni az új operációs rendszereit, azonban annak forráskódjait nem osztja meg. A külső fejlesztők számára programfejlesztő környezetet (SDK) alakítottak ki, valamint lehetővé tették, hogy az online szoftverpiacukon, az Apple Store-on programjaikat a cég által kontrollált módon terjeszthessék. Fontos megjegyezni, hogy biztonsági szempontból az Apple alkalmazás piacának modellje jobb, mivel a szoftverek komoly ellenőrzésen esnek át, azonban a megnövekedő fejlesztési költségeket sokszor a fejlesztők azzal pótolják, hogy a felhasználói szokásokról készülő statisztikákat eladják. Ami *"privacy"* szempontból ez a felhasználókra nézve elég rossz hír.

MICROSOFT MOBILE

A Microsoft Mobile a Nokia cég Lumnia sorozatú készülékeire, majd azok továbbfejlesztéseire lett kialakítva. Előnye az asztali-, és felhő alapú Microsoft megoldásokkal való együttműködés. Ennek következtében a klasszikus nagyvállalati infrastruktúrával rendelkező szervezetek előszeretettel alkalmazzák a meglévő informatikai rendszerek mobil eszközökre való kiterjesztése érdekében.

BLACKBERRY OS

A BlackBerry a klasszikus nyomógombos készülékekkel – az érintőképernyős készülékeket kevésbé kedvelő felhasználókat – és a vállalati szolgáltatásaival az üzleti-kormányzati szektort célozza. Szintén zárt rendszer. A felhasználók az alkalmazásokat a BlackBerry World áruházon keresztül tölthetik le. 2016-ban a gyártó váltott, és kiszervezte a hardverkészítést, és az Android-on alapuló operációs rendszerével gyártja mobiltelefonjait.

MOBIL VÉDELMI MEGOLDÁSOK

Ahogy korábban említettük, a mobil eszközök mára szinte mindenkinél, szinte mindenhol ott vannak. Egyre több dologra használhatóak, azonban ennek következtében egyre jobban függünk is tőlük. A munkával kapcsolatos (üzleti), és a magáncélú felhasználás egyre nagyobb mértékben keveredik, mely komoly biztonsági kockázatot hordoz. Ezen kockázatok csökkentésére többféle megoldási lehetőség létezik:

A „Bring your own device" (BYOD) elv esetén a munkavállalók saját eszközeiket használják a munkával kapcsolatos feladataikhoz. Ebben az esetben háromféle módon lehet a biztonságot a munkáltató oldaláról biztosítani:

1. Mobil eszközmenedzsment megoldásokkal (MDM)[4] (jellemzően ekkor a tulajdonos átengedi a mobil eszköz feletti kontrollt a munkáltatónak);
2. Konténerizálással, mely során az operációs rendszer – a vállalati adatokat elkülönítetten, kriptográfiai módszerekkel támogatott módon – tárolja és lehetővé teszi a hozzáférést a hozzáférésre jogosultak számára;
3. Publikus-, vagy magán felhőmegoldásokkal[5] (melynél különböző távoli hozzáférési eljárással a felhasználók a vállalati erőforrásokat a saját eszközeikről érik el).

Vállalati tulajdonú eszközöknél (un. COPE[6]) is használhatóak az MDM, a konténerizációs technológiák, valamint a felhő alapú megoldások is, ráadásul a rendszerek felügyelete

4 Mobil Device management (MDM)
5 Cloud computing
6 Corporate Owned, Personally Enabled (COPE)

technológiai- és jogi szempontból is egyszerűsödik. Ennek egyetlen hátránya, hogy a felhasználónak egy plusz vállalati eszközt is kell magánál tartani a magáncélú eszköze mellett.

A SANS kiberbiztonsági oktatóközpont listája[7] segítséget nyújt a megfelelő vállalati modell kiválasztásában (annak eldöntésére, hogy a BYOD, vagy a COPE-e a hatékonyabb, a biztonság, és a költségek szempontjából).

Mobil technológia – paradigmaváltás az IT világban

Az első generációs mobil készülékek kizárólag hang alapú szolgáltatásokat biztosítottak. Az analóg elven működő cellás rádiórendszer mobil termináljai semmiféle védelemmel nem rendelkeztek, így lehallgatásuk viszonylag egyszerű volt. A digitális hang-, és adatszolgáltatásokat is biztosító GSM[8] már alkalmazott kriptográfiai eljárásokat a rádiófrekvenciás átviteli út védelmére (ennek védelmi foka országonként, szolgáltatónkként eltérő volt, ugyanis hol erősebb, hol gyengébb titkosítási algoritmussal implementálták). Azonban napjainkra már ez a védelem sem elegendő, mivel viszonylag alacsony költségen beszerezhetőek olyan eszközök melyek segítségével belátható időn belül visszafejthető egy-egy GSM hívás tartalma[9]. A biztonsági helyzetet tovább rontja, hogy az SMS küldésnél a GSM technológia azt nyílt szövegként, titkosítatlanul teszi. Így például SMS-t alkalmazni kétfaktoros hitelesítésre mára már nem javasolt [2] [3].

7 SANS SCORE Mobile Device Checklist:
https://www.sans.org/media/score/checklists/mobile-device-checklist.xls
8 Global System for Mobile Communications
9 Lásd részletesen Karsten Nohl "GSM Sniffing" című előadásanyagában
https://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf

rövidítés	Technológia		A letöltési sebesség elméleti maximum	A feltöltési sebesség elméleti maximum
2G	GSM	Global System for Mobile Communications	14.4 Kbits/s	14.4 Kbits/s
G	GPRS	General Packet Radio Service	53.6 Kbits/s	26.8 Kbits/s
E	EDGE	Enhanced Data rates for GSM Evolution	217.6 Kbits/s	108.8 Kbits/s
3G	UMTS	Universal Mobile Telecommunications System	384 Kbits/s	128 Kbits/s
H	HSPA	High-Speed Packet Access	7.2 Mbits/s	3.6 Mbits/s
H+	HSPA+	Evolved High-Speed Packet Access - Release 6	14.4 Mbits/s	5.76 Mbits/s
H+	HSPA+	Evolved High-Speed Packet Access - Release 7	21.1 Mbits/s or 28.0 Mbits/s	11.5 Mbits/s
H+	HSPA+	Evolved High-Speed Packet Access - Release 8	42.2 Mbits/s	11.5 Mbits/s
H+	HSPA+	Evolved High-Speed Packet Access - Release 9	84.4 Mbits/s	11.5 Mbits/s
H+	HSPA+	Evolved High-Speed Packet Access - Release 10	168.8 Mbits/s	23.0 Mbits/s
4G	LTE	Long Term Evolution	100 Mbits/s	50 Mbits/s
4G	LTE-A	Long Term Evolution - Advanced	1 Gbits/s	500 Mbits/s

2. ábra A különböző mobil szabványok elméleti sebességei [4]

A fenti ábra bemutatja a különböző mobil technológiák által biztosított elméleti adatátviteli sebességet. A GSM rendszerek korlátozott adatátviteli képességei (14.4kbps) egyszerű modemes összeköttetést biztosítanak. Érdekessége, hogy a beszédsávi modemes internetelérésre használható AT (Hayes) parancsok még szinte minden mobil eszköznél elérhető a soros, vagy USB interfészen keresztül. Az AT parancsok segítségével az mobilkészülékek alapsávi modeme vezérelhető, küldhető SMS, lekérhetők az IMSI[10], IMEI[11] és a SIM[12] kártyán tárolt egyéb adatok, valamint az aktuálisan használt hálózat cella információi[13].

A GPRS[14] megjelenésével a WAP[15] protokoll felhasználásával már böngészhetővé vált az internet. Az alacsony számú WAP-os előfizető nem jelentett értékes célpontot a támadóknak, így ez a technológia nem került a célkeresztjükbe. Mivel az internet elérést speciális protokoll segítségével biztosította, így a klasszikus támadások és sebezhetőségek is hatástalanok voltak a kor színvonalának megfelelő készülékek ellen. Tovább „fokozta” a biztonságot, hogy a mobil

10 International Mobile Subscriber Identity
11 International Mobile Station Equipment
12 Subscriber Identity module card
13 Christos Xenakis, Christoforos Ntantogian: Attacking the Baseband Modem of Mobile Phones to Breach the users' Privacy and network Security https://ccdcoe.org/cycon/2015/proceedings/16_xenakis_ntantogian.pdf
14 General Packet Radio Service
15 Wireless Application Protocol

készülékek korlátozott erőforrásaik révén egyszerre csak 1 folyamatot tudtak futtatni (az Android operációs rendszer tette először lehetővé a multitask működést). Az EDGE[16] majd az UMTS[17] egyre nagyobb adatátviteli sebessége révén már élvezhető minőségű internetes tartalomelérést tett lehetővé. A 4. generációs technológiák pedig megközelítették az asztali gépekkel elérhető adatátviteli sebességet és minőségét. Így már érdemes volt komolyabb számítási kapacitású készülékeket gyártani. Sajnos az erőforrások növekedésével, az elérhető szolgáltatások bővülésével és a készülékek széleskörű elterjedésével a technológiát fenyegető veszélyforrások is bővültek.

A különböző generációjú mobilhálózatok sok helyen még párhuzamosan üzemelnek, a felhasználón (és mobil eszközén) múlik, hogy melyik technológiát veszi igénybe. A fenti biztonsági okok miatt javasolt a GSM technológiát mellőzni (tiltani a készüléken). Figyelembe kell azonban venni, hogy a 3. és 4. generációs hálózatok lefedettsége csak a városokban teljes körű, vidéken, erdős-hegyes terepen még mindig a GSM technológia dominál (ha tehát ilyen területen szeretnénk szolgáltatást igénybe venni, akkor kénytelenek leszünk a GSM-re hagyatkozni, ellenkező esetben megbízhatatlan összeköttetésünk lesz, és a megnövekedett adóteljesítmény miatt hamarabb lemerül a telefonunk).

IT fenyegetések a mobil platformok ellen

Az ENISA[18] által készített összefoglaló alapján a mobil eszközök tekintetében az alábbi célpontjai lehetnek a különböző kibertámadásoknak[19]:

- személyes adatok;
- szervezeti/vállalati tulajdonú adatok;
- minősített adatok;
- pénzügyi információk;
- készülék és rendszerek funkcionalitása vagy rendelkezésre állása;
- magán-, vagy politikai reputáció[20].

Napjainkban a felhasználók egyre nagyobb mértékben tárolnak érzékeny adatokat a mobil eszközeiken. Többnyire nincsenek is tisztában ezek fontosságával és értékével (általában csak eg-egy incidens után döbbenek rá erre). Az alábbi táblázat ezekre a szenzitív adatokra hoz példákat (1. Táblázat).

16 Enhanced Data rates for GSM Evolution
17 Universal Mobile Telecommunications System
18 European Network and Information Security Agency
19 Enisa - "Smartphones: Information security risks, opportunities and recommendations for users" https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport
23 Erre az utóbbi időben több példát is láttunk, például az Egyesült Államok választási kampánya során http://www.businessinsider.com/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10, vagy FireEye kártékony kód elemzéssel foglalkozó IT cég alkalmazottja elleni un. #LeakTheAnalyst támadás Részletek: http://www.securityweek.com/hackers-compromise-accounts-fireeye-threat-intelligence-analyst

Személyes adatok	**Példák**
Különleges személyes adatok (magánélettel, vallási, politikai, szexuális beállítottsággal kapcsolatos adatok), személyes egészségügyi adat, természetes személyazonosító adatok	*jelszavak, látogatott oldalak, telefonszámok, kapcsolatok, okmányok, azonosítók*
Pénzügyi adatok	*banki, hitelintézeti ügyekkel kapcsolatos adatok*
Magántitkok	*levelezés, chat üzenetek, képek, videók, hangfájlok*
Vállalati adatok	**Példák**
Üzleti kapcsolatok, ügyféladatok	*Email címek, üzleti levelek telefonszámok, postacímek stb.*
Pénzügyi adatok	*banki, hitelintézeti ügyekkel kapcsolatos adatok*
Üzletpolitikával, módszerekkel, stratégiai tervekkel kapcsolatos információk	*Üzleti tervek, műszaki specifikációk, szabadalmak, vállalati módszerek, stb.*

1. táblázat Példák a mobil eszközökön tárolt saját / vállalati tulajdonú adatokra (saját szerkesztés)

A másik probléma napjainkban, hogy a felhasználók nem megfelelő „higéniával” kezelik készülékeiket. Szükségtelen, vagy kétes forrásból származó alkalmazásokat telepítenek, melyekkel egyrészt leterhelik a készülék erőforrásait, és növelik is ezzel az eszközök sérülékenységeinek lehetséges forrásait.

Jellemző felhasználói mentalitás, hogy az új készülékekre, a kézzelfogható „hardverekre” akár több százezer forintot is hajlandóak kiadni, azonban a néhány száz, esetleg ezer forintos költségű szoftverekre már nem áldoznak. Léteznek un. crack-elt szoftverek (melyekkel legitim, fizetős alkalmazásokat tudunk használni ingyenesen). Probléma ezekkel egyrészt, hogy illegálisak (révén, hogy sértik a gyártó szellemi tulajdonát, és anyagi kárt okoznak neki), továbbá jellemző, hogy a felhasználó a telepítésükkel rejtetten más alkalmazásokat is telepít (jobb esetben csak zavaró reklámokat megjelenítő adware-eket, de akár kémprogramokat, vagy rejtett hozzáférést biztosító backdoor-okat, esetleg egy botnet hálózathoz csatlakozó klienst).

Vannak továbbá olyan hamis (un. „fake”) programok, melyek egy populáris alkalmazáshoz hasonló névvel és logóval rendelkeznek, azonban más, gyakran kártékony tevékenységet folytatnak a telepítést követően. Ilyenre példa az un. „fake antivirusok”, melyek sajnos csak nevükben antivírus programok, működésük tekintetében kártékony kódok. De megfigyelhető még a népszerű alkalmazásoknak az „ingyenes” változatai, vagy a populáris alkalmazások vagy szolgáltatások kártékony kiegészítői (a kártékony böngésző kiegészítők és a mobil eszközökön futtatható játékok, azok kiegészítői jó példák ezekre a programokra[21]).

Ha a munkavégzésre használt mobil eszközöket vesszük szemügyre, akkor látjuk, hogy gyakori hiba, hogy nem rendszerben gondolkodnak azok tervezői (vagy felhasználói), hanem csak az egyes eszközök szintjén. Ha például egy szervezet felhasználói által használt

24 A népszerű pokémon-go játékhoz is készültek már kártékony kiegészítők
https://blog.kaspersky.com/pokemon-go-malware/12953/

készülékflotta beszerzését tervezzük, akkor célszerű ügyelni a homogenitásra, mely később egyszerűsíti az üzemeltetők és a támogatók munkáját, lehetővé teszi az egységes szabályzást, és a készülékek frissítésének követését. Ha inhomogén eszközparkot alakítunk ki, akkor lényegesen megnehezítjük a szervezet szintű védelem kialakítását, és az egységes felügyeletet.

A rendszerszemlélet fontosságára jó példa, a készülékek kártékony kód elleni védelmének kiválasztása. Az egyéni mobilkészülékek védelme, vagy a szervezeti hálózatba léptetett eszközök központi vírusvédelme jelentősen eltérő igényeket támaszt. Előbbinél a magáncélra ingyenesen használható megoldások is alkalmazhatóak, utóbbiaknál azonban már csak az un. „Enterprise" megoldásokkal lehet átlátható, egyenszilárd védelmet kialakítani.

MOBIL ESZKÖZÖK LOKÁLIS FENYEGETÉSEI

A fizikai biztonság szempontjából a mobil eszközök elvesztése, vagy eltulajdonítása (lopása) a legnagyobb fenyegetési forrás. Jellemzően napjaikra ezen fenyegetések kezelésére vannak már megoldások, azonban a kontrollokat a felhasználók csak ritkán alkalmazzák[22]. A lopás elleni védelem első eleme a biztonságtudatosság, és a megfelelő fizikai tárolás (pl.:nem hagyjuk felügyelet nélkül az eszközeinket). A védelem tovább fokozható a tárolt adatok védelmével, melyre a korszerű mobil készülékek fájlrendszer szintű titkosítást ajánlanak. Amennyiben ennél többre van szükségünk, akkor további titkosítást is alkalmazhatunk (alkalmazásokkal). További segítség lehet a távoli adattörlés, mellyel megakadályozzuk, hogy az adatokhoz jogosulatlanok férjenek hozzá (ha már az eszközhöz sajnos hozzá tudtak férni).

Az elvesztés ellen technikai módszerekkel az eszközlokációs szolgáltatásokkal és/vagy távtörléssel tudunk védekezni. Az előző megoldásokkal a legnagyobb biztonsági probléma, hogy felhő szolgáltatásokon keresztül tudjuk elérni. Amennyiben ezekhez a távtörlő, vagy lokációs szolgáltatásokhoz mások is hozzáférnek, akkor az katasztrófához vezethet, mint ahogy az *Mat Honan* újságíró esetében meg is történt[23].

A mobil eszközök vállalat szintű korlátozásánál azok pozíciója is figyelembe vehető (GPS koordináta, RFID szenzorok, cellainformációk, WiFi csatlakozási pont adatai). A GeoFencing segítségével meghatározható, hogy mely szolgáltatások (pl.: vállalati levelezés, belső alkalmazások, adatbázisok), honnan érhetőek el.

A MOBIL ESZKÖZÖK HÁLÓZATI FENYEGETÉSEI

A mobil eszközök hálózati fenyegetéseinél először a mobil cellás rendszerek használatából fakadó fenyegetéseket kell sorra venni. A GSM szabvány által biztosított védelem a hang és a szöveges üzenetküldés szempontjából sem tartható megbízhatónak. A másik probléma a GSM kapcsán az un. Baseband processzorok (melyek a készülék rádiófrekvenciás kommunikációjának vezérlésére szolgálnak) sebezhetősége[24]. Ugyan ilyen támadásokra egyenlőre még csak a biztonságot vizsgáló laborokban került sor, azonban ezek fényében célszerű olyan eszközöket választani, melyeket a gyártók komoly biztonsági teszteknek vetettek alá, és kiállták a próbákat. Az ilyen támadások azért sem voltak jellemzőek, mert a távközlés szolgáltatások (pl.:POTS[25], ISDN[26], VoIP[27]) még mindig jól visszakövethető, hogy ki volt egy

22 Az elvesztett készülékeket Android esetén a "Where is my droid" , iOS esetén az ICloud, „find device" szolgáltatásával találhatjuk meg

23 Mat Honan: How Apple and Amazon Security Flaws Led to My Epic Hacking, Wired https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

24 Andrew Davis CELLULAR BASEBAND SECURITY (Georgia Institute of Technology May 2012) https://smartech.gatech.edu/bitstream/handle/1853/43766/davis_andrew_t_201205_ro.pdf

25 Plain old telephone service

26 Integrated Services Digital Network

27 Voice over Internet Protocol

hívás, vagy üzenetküldés kezdeményezője (azonban előbb-utóbb jelentkeznek majd olyan kártevők, amelyek a fertőzést követően az áldozat készülékéről küldött speciális SMS, vagy MMS üzenetekkel bénítanak vállalati rendszereket).

A mobil eszközökre más vezetéknélküli fenyegetések is leselkednek. A régi, orosz gyártmányú katonai rádiók mindegyikén látható volt az alábbi szöveg:

"Az ellenség is hallja!"

A vezetéknélküli kommunikációra napjainkban is érvényes ez az figyelmeztetés. Azonban korunk rádióeszközein, az okostelefonokon ez sajnos nincs feltüntetve. A vezetéknélküli hálózatok (pl.:Wifi) elterjedésével számos helyen biztosított az ingyenes internet hozzáférés[28]. Ha utazunk, ha vásárlunk, kávézunk, hotelben szállunk meg, vagy épp egy reptéren várakozunk járatunkra, akkor jellemzően a védelem nélküli wifi hálózatot vesszük igénybe, hogy „spóroljunk" a mobilinternet előfizetésünkön. Sajnos ez komoly biztonsági problémákhoz vezethet, mivel ezeket könnyű lehallgatni, megszemélyesíteni a támadó eszközével, valamint az is előfordulhat, hogy maguk az üzemeltetők élnek vissza a rendszer nyíltságával.

VEZETÉKES ÉS VEZETÉK NÉLKÜLI INTERFÉSZEK

Az okos eszközökhöz vezetéknélkül illeszthető kiegészítők is hordozhatnak veszélyt, legyenek azok Bluetooth-on (pl.:headset, okosóra), ANT[29] szabvánnyal (pl. pulzusmérő pántok), vagy NFC[30]-n keresztül elérhetőek (pl.:érintés nélküli bankkártyák). Sok esetben speciális protokollokat használnak (pl.:okosTV-nél a Miracast[31]), melyeket kifejlesztésénél, vagy implementálásánál a gyártók nem törekedtek a biztonságra (általában a csak a költséghatékonyságra és a használhatóságra ltörekszenek).

A készülékekbe épített Wifi chip-ek firmware szinten is tartalmazhatnak hibákat, melyeket egy támadó kihasználhat, és távoli kódfuttatást idézhet elő felhasználói beavatkozás nélkül is (még ha az okostelefon operációs rendszere megerősített biztonsággal is bír, a hálózati kártya felől érkező alacsonyszintű támadásra nincs felkészítve) [5].

A vezetéknélküli interfészek mellett a vezetékes csatlakozásokra is figyelni kell. A töltésre és adatátvitelre is használható USB portok is veszélyt jelenthetnek, ha nem megbízható eszközre csatlakoztatjuk mobilkészülékünket[32]. Az USB csatlakozás kettős természetét kihasználó támadásokat „Juice Jacking"-nek hívják. Fizikai károkat is okozhat, ha ismeretlen töltőállomásokra csatlakozunk, erre jó példa a KillUSB nevű eszköz, melyet „Elektromágneses kompatibilitás" (lökőfeszültség elleni immunitás) vizsgálatához árulnak az interneten (legalábbis ez a hivatalos indok, de valójában arra, jó, hogy tönkre tegyünk egy USB interfésszel rendelkező eszközt)[33].

A klasszikus adatátviteli interfészek mellett minden ki-, és bemeneti portra, és szenzorra is oda kell figyelni, melyet az alábbi példák jól demonstrálnak.

28 Az alábbi weblapon ellenőrizni tudjuk, hogy környezetünkben milyen nyilvános wifi hálózat érhető el: https://wigle.net/

29 Elsősorban sport eszközökbe épített szenzorok adatkapcsolatára szolgáló szabvány

30 Near-field communication, két kis távolságra , két kis távolságra helyezkező elektronikus eszköz közti adatcserére szolgál

31 Ez a protokoll lehetővé teszi a mobil eszközök képernyőképének megosztását okostv-kkel, monitorokkal vagy projektorokkal

32 http://www.asd.gov.au/videos/cybersense1.htm

33 Az USB Killer nevű eszköz például kondenzátorokat tölt fel a USB tápcsatlakozón keresztül, majd süt ki az USB adatporton keresztül (további információ: https://www.usbkill.com/usb-killer/13-usb-killer-v3.html)

2015-ben az ANSSI[34], francia kormányzati ügynökség demonstrálta, hogy az okostelefonok hangvezérlését az audióinterfészen (az arra csatlakoztatott fülhallgatóval, mely antennaként funkciónál) keresztül távolról is használni tudták[35].

2017-ben amerikai kutatók kártékony, videótartalmakba rejtett parancsok alkalmazását demonstrálták a Google Assistant, az Apple Siri, és az Amazon cég Alexa beszédfelismerő rendszerei ellen[36].

A mobil eszközökbe GPS szenzorok RF vevőkészülékek, így zavarhatóak, megtéveszthetőek [6], sőt jelfeldolgozó egységeik közvetlenül is támadhatóak [7].

Ugyan ezek sem tekinthetőek a gyakorlatban könnyen kivitelezhető támadási formának, azonban rávilágítanak, hogy a technológiai innovációk újféle biztonsági szemléletet, és a biztonság alapos tesztelését igénylik. Így bármilyen interfészről is legyen szó, az támadási felületet képezhet, amennyiben ötletes és technológiailag felkészült támadóval állunk szemben.

MOBIL KÁRTÉKONY KÓDOK

Az operációs rendszerek szintjén a kártékony kódok képezik napjainkban a legnagyobb fenyegetést. Az alábbiakban ezeknek a biztonságra gyakorolt hatását mutatjuk be.

Bizalmasság és sértetlenség ellen irányuló támadások:

- felhasználói adatok elérése (lokációs információk, érdeklődési köre, kapcsolati háló stb.),
- hozzáférés a jelszavakhoz, tanúsítványokhoz, privát és publikus kulcsokhoz stb. ,
- az elküldött/fogadott üzenetekhez való hozzáférés (banki üzenetek, közösségi hálón folytatott kommunikáció, email SMS, MMS, bluetooth üzenetek stb.),
- a munkáltató bizalmas adataihoz és rendszereihez is hozzáférhetnek a támadók a kompromittált mobil eszközökön keresztül.

Rendelkezésre állás ellen irányuló támadások:

- akkumulátor gyors lemerítése[37],
- CPU, memória túlterhelése,
- hálózati forgalom generálása (pl.:DDoS támadásra felhasználva),
- túlterheléses támadások (SMS/MMS üzenetekkel, adatforgalommal, vagy hívásokkal túlterhelnek bizonyos telefonszámokat, telefonszámmezőket),
  adattörlése (privát adatok pl.: képek, zenék és videók), dokumentumok, vagy más jellegű kritikus információkat (pl.:telefonkönyv, SMS és hívásnapló, email-ek stb.),
- interfész fizikai pusztítása (pl.:USB Killer).

Sok támadás csak feltört, módosított operációs rendszereken (un. „jailbroken”, „rooted”) eszközök ellen alkalmazható, így célszerű kerülni ezeket a technikákat (még ha így fizetni is kell egyes alkalmazásokért).

A mobil eszközökön folytatott internet böngészés is komoly fenyegetésnek van kitéve, révén, hogy a mobil eszközökbe épített böngészők kevésbé vannak felkészítve a kártékony

34 L'autorité nationale en matière de sécurité et de défense des systèmes d'information
35 Lásd: Jose Lopes Esteves, Chaouki Kasmi:IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones
http://ieeexplore.ieee.org/document/7194754/?reload=true&arnumber=7194754
36 Lásd: http://www.darkreading.com/vulnerabilities---threats/covert-voice-commands-can-hack-a-smartphone/d/d-id/1326232
37 Frank Stajano és Ross Anderson az ilyen típusú támadást "Battery exhaustion" vagy "Sleep deprivation torture”-nak nevezte

tartalmakra, és az is megfigyelhető, hogy lényegesen kevesebb védelmi szoftvert telepítenek a mobil készülékekre a felhasználók, mint az asztali eszközökre (melyeknél már „megszokták", hogy szükség van az ilyen jellegű alkalmazásokra). A felhasználói élményt komolyan befolyásolják az erőforrásokat és az akkumulátoridőt is terhelő mobil antivírus-, tűzfal- és egyéb biztonsági szoftverek. Ilyenkor a felhasználóknak figyelembe kell venniük, hogy a kártékony kódok is negatívan befolyásolnák a „felhasználói élményt", például ha törlik, titkosítják adataikat, megfigyelik a kommunikációjukat, esetleg emelt díjas szolgáltatásokat vesznek igénybe készülékükről.

A MOBIL VÉDELEM TECHNOLÓGIAI ASPEKTUSAI

A fenyegetések figyelembevételével a mobil technológia biztonságos használatát a tárolt, és a továbbított adatok védelmével kell megalapozni. A tárolást megbízható kriptográfiai algoritmusokkal kell garantálni. A védelemnek az asztali operációs rendszerekhez hasonlóan az operációs rendszer fájljait tároló partíciókra, és a leválasztható adattárolókra (pl.:SD kártya) is ki kell terjednie. Sok esetben (elsősorban a régi készülékeken erőforrás okok miatt) sajnos a fájlrendszer szintű védelem nem lehetséges.

Hozzáférésvédelemi célból felhasználói azonosításra a klasszikus PIN, és jelszó alapú eljárások mellett a képernyőzár minta, és a különféle biometrikus azonosítási módok (pl.: ujjlenyomat, arcfelismerés vagy íriszazonosítás) is elérhetőek egyes készülékeknél. Ezeknek a technológiáknak hibája, hogy néhány próbálkozás után elérhetővé teszi a jelszavas/PIN alapú azonosítást, így a védelem visszaminősül (ennek oka szintén a könnyű kezelhetőségben keresendő). Központosított felügyelettel rendelkező készülékflotta esetén a hibás hozzáférési próbálkozások megjelennek a naplókban, és pl. telefonhívással ellenőrizni lehet, hogy a felhasználó felejtette el jelszavát, vagy egy támadó próbál hozzáférni a rendszerhez.

A szoftverek naprakészen tartása ugyancsak fontos, és az ismert fenyegetések elleni védelem egyik alappillére lehet. Sajnos a különböző platformok eltérő helyzetet mutatnak e téren. Sok eszköznél igen lassan jelennek meg frissítések, és az új, védettebb operációs rendszerek jellemzően eszközcserét követelnek, mivel a gyengébb képességű hardvereket már nem támogatják. Az operációs rendszer mellett az alkalmazások naprakészen tartása is fontos feladat, mely egyedi fejlesztések, vagy a fejlesztő támogatásának beszüntetését követően sajnos nehézkes.

A kártékony alkalmazások elleni védelem alapja, hogy csak megbízható forrásból töltsünk le alkalmazásokat, és csak amelyekre feltétlenül szükségünk van (és amennyiben már nem használjuk, akkor töröljük). Vállalati környezetben a megbízhatónak tartott forrásokból (alkalmazás áruházakból) letöltött alkalmazások is további ellenőrzésnek vethetőek alá, így fokozható a védelem. Jellemzően a szervezet számára fontos alkalmazásokat ekkor szakértők automatikus elemzőszoftverekkel, majd kézzel vizsgálják meg és keresnek bennük sérülékenységeket, vagy kártékony tartalmat.

A következő védelmi lépcső lehet, ha a telepített alkalmazásoknak csak a szükséges és elégséges jogosultságok engedélyezzük (így például ha egy naptár alkalmazás a kamerához, és a GPS-hez akar hozzáférni, esetleg híváskezdeményezési jogot kér, akkor azt ne engedélyezzük számára).

A mobil kártevőkre sajnos minden kommunikációs csatornán számítanunk kell (pl.: email, web böngészés, SMS, MMS, Bluetooth stb.), így kártékony kódokat detektáló, és a településüket, valamint a működésüket akadályozó védelmi megoldásokra mindenképpen szükségünk van.

A kártékony kódok okozta, vagy a nem szándékosan elkövetett adatvesztések hatásait megfelelő adatmentési és archiválási megoldásokkal tudjuk kivédeni. Célszerű a bizalmas adataink mellett a készülék által tárolt üzeneteket, kapcsolatokat (pl.:névjegyek, telefonszámok stb.) is menteni, valamint a visszaállíthatóságot időszakosan tesztelni.

A vállalati (vagy szervezeti) erőforrásokhoz való hozzáférést a klasszikus határvédelmi megoldásokkal (pl.:tűzfalak) már nem lehet megoldani, mivel a mobilitás következtében az eszközök különböző irányokból, különböző védettségű hálózatokból (pl.:vállalat belső hálózatából, nyílt internet felől mobilszolgáltatón vagy publikus WiFi kapcsolaton keresztül) csatlakoznak a vállalati erőforrásokhoz. Ennek következtében különböző szűrési és szeparációs szabályokat kell bevezetni, és ezeket dinamikusan alkalmazni a helyzet függvényében.

A Szeparáció és szűrés lehetőségei

- Szerepkör szerint (feladat, szervezeten belül betöltött munkakörök alapján);
- Eszköz szerint (máshoz férhet hozzá a felhasználó laptopról, máshoz okostelefonról);
- Hálózat jellege szerint (vállalati hálózat, otthoni, vezetékes/vezeték nélküli);
- Hely alapú (GPS koordináták, cellainformációk alapján).

A GSM hálózat okozta fenyegetésekre (lehallgatás, közbeékelődés, stb.) egyrészt az ilyen hálózatokra való csatlakozás tiltásával (a készülékekben beállítható, hogy mely mobilszabványokat használják, valamint kézzel állítható, hogy mely szolgáltató hálózatára csatlakozzanak csak fel). Vannak olyan alkalmazások[38], továbbá készülékek[39] is, melyek a GSM hálózat felől érkező fenyegetéseket jelzik, azonban ezek hatékonysága még nem általánosan bizonyított, így nem is terjedtek még el.

A WiFi hálózatok jelentette fenyegetéseket egyrészt a vezetéknélküli infrastruktúra védelmének fokozásával érhetjük el (az engedély nélkül üzemeltetett hozzáférési pontok keresésével[40], erős csatornavédelmi titkosítással, Radius alapú azonosítással, vezetéknélküli IDS rendszerek alkalmazásával, esetleg VPN megoldásokkal). A kliens oldalon a nem megbízható hálózatokra való csatlakozás tiltásával, az ismert és megbízhatónak vélt hálózatok paramétereinek rögzítésével, és a korábban csatlakoztatott hálózatra való automatikus csatlakozás kikapcsolásával fokozható a védelem. A nem használt szolgáltatások és protokollok kikapcsolása is fokozhatja a védelmet (pl.: ha a hálózat nem támogatja az IPv6-os címzést, akkor célszerű lenne azt az eszközön kikapcsolni[41], sajnos ilyen mély konfigurációt jelenleg a mobil operációs rendszerek nem tesznek lehetővé).

Amennyiben feltétlenül szükséges nyílt WiFi hálózatokat igénybe venni, akkor azokon VPN-en keresztül érjük el a védett rendszereinket. Így a forgalmunk megfigyelése, és a bizalmas adataink lehallgatása is nehezebbé válik.

A gyártók ajánlásainak és iránymutatásainak (un. „Hardening guide”-ok és „security checklist”-ek[42]) figyelembevétele fontos mind a magán, mind a vállalati eszközök biztonságának megőrzésében. A mobil technológia gyorsan fejlődik, így érdemes ezeket az ajánlásokat időszakosan újra szemügyre venni, és implementálni az újonnan jelentkező védelmi módszereket.

A készülékek részleges, vagy teljes törlése is fontos funkció lehet, érdemes megjegyezni, hogy egyes gyártók eltérő megbízhatósággal törlik a tárolt adatokat[43]. A szervezeti tulajdonú

38 Pl.:https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector
39 Pl.:https://cryptophoneaustralia.com/news/how-to-detect-stingray-imsi-catchers/
40 A rogue access point-ok (Kopé Ápék) felderítése és kikapcsolásával
41 Sajnos a legtöbb készüléken ez jelen pillanatban nem tehető meg
44 Például: The University of Texas at Austin:Google Android Hardening Checklist https://security.utexas.edu/handheld-hardening-checklists/android ; iOS Security https://www.apple.com/business/docs/iOS_Security_Guide.pdf ; Yuri Diogenes - Hardening mobile devices https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/mdm-hardening-mobile-devices
45 A különböző platformok gyári visszaállításairól, “reset”-eléséről részletesebben a National TechnicalAuthority Authority for Information Assurance (CESG), UK - Factory reset and reprovisioning guidance (https://www.gov.uk/government/publications/end-user-devices-security-guidance-factory-reset-and-reprovisioning/factory-reset-and-reprovisioning-guidance) leírásában olvashatunk

eszközök újra kiosztása, vagy az eszközök kivonása megfelelő előkészítést igényel, esetenként csak speciális szaktudással végezhető.

Mit sem érnek azonban ezek a védelmi kontrollok, ha azt nem tudatos, előrelátó felhasználók használják a mobil eszközöket. Így a biztonságtudatos magatartás a mobil eszközök esetén is kiemelt fontosságú[44]. Különösen, ha a fizikai tárolásra, használatra, vagy ha a különböző alkalmazások (~applikációk) telepítésére gondolunk. Célszerű átgondolni, hogy ha nem biztosítható a mobil eszközök folyamatos felügyelete, fizikai biztonsága (pl.: külföldi utazás, nyaralás, sport, egyéb tevékenység során), akkor érdemes-e magunkkal vinni ezen eszközöket. Amennyiben nélkülözhetetlen magunknál tartani, akkor pedig csak a feltétlenül szükséges adatokkal vigyük magunkkal, a megfelelő védelmi intézkedések betartása mellett.

Napjainkban a gyorsul életritmusnak köszönhetően hajlamosak vagyunk megfeledkezni, vagy kompromisszumokat kötni, ha a biztonságról van szó. Célszerű azonban az ilyen döntési helyzetekre készülni, és következetesen ragaszkodni a biztonsági elvárásainkhoz egyén szintjén, valamint követni a szervezetünk által előírt szabályokat.

A MOBIL VÉDELEM HUMÁN ASPEKTUSAI

Hiába van a legmodernebb technológiákat felvonultató rendszerünk, és világelső biztonsági kontrolljaink, ha azokat a felhasználóink, vagy az rendszer üzemeltetői nem képesek megfelelően használni.

Épp ezért a felhasználók figyelmének felhívása (veszélyfigyelmeztető levelekkel, vagy chat üzenetekkel), valamint oktatása (pl.: heti biztonsági körlevelekkel[45]) ugyancsak fontos, mivel ezzel is a biztonságtudatosságra neveljük őket. Azonban a reklámokhoz hasonlóan, ha ezek a levelek, felhívások, figyelmeztetések gyakoriak, és egyhangúak akkor ellentétes hatást váltanak ki (és az üzenetek olvasatlanul törlésre kerülnek). Érdemes interaktívvá tenni ezt a közlési módot, és például kérdőívekkel, rövid szituációs gyakorlatokkal ellenőrizni az ismeretek elsajátítását. A másik módja, ha teszteljük a felhasználók éberségét (pl.: gyanús email-ek, chatüzenetekkel, VoIP hívásokkal). Valósan kártékony hatást kiváltó tartalmat nem küldhetünk a felhasználóknak, de azt ellenőrizhetjük például, hogy egy csatolmányt, vagy linket megnyitnak-e ismeretlen forrásból. Célszerű ezen gyakorlati teszteket követően jutalmazni azokat akik helyes döntést hoztak, és oktatni a biztonsági szabályokat megszegő felhasználókat (a notórius vétők ellen retorziók is foganatosíthatóak). A változatosság és a valósághűség a fő elvárás ezeknek a teszteknek a kidolgozásánál. A vezetéknélküli hálózatok, a mobil platformok, és az azzal összefüggő felhő szolgáltatások esetén célszerű ezekre fókuszáló eseteket generálni (pl. nézni, hogy egy, nem a szervezet üzemeltetésében lévő, titkosítatlan vezetéknélküli hálózatra mely felhasználók csatlakoznak, azon milyen hálózati forgalmat generálnak, milyen információkat osztanak meg. A klasszikus email alapú "gyanús" üzenetek mellett a mobil platformokon terjedő azonnali üzenetküldő alkalmazások is kecsegtető célpontok lehetnek. A felhő alapú tárolás tesztelése esetén pl. megfigyelhetjük, hogy jelzik-e a felhasználók, ha az egyik kollégájuk azon oszt meg adatokat, vagy arra kér másokat, hogy ilyen tárolókra töltsenek fel adatot. Tekintettel arra, hogy ezek a tesztek magántulajdonú (BYOD elv), vagy külső rendszereket (felhőszolgáltató) is igénybe vehetnek, így jogi- és információvédelmi szempontból is körbe kell járni a tervezett biztonságtudatossági kampány megalapozottságát.

44 A mobil eszközök felhasználóit célszerű mobil fenyegetésekről tájékoztatni, időszakosan felkészítő foglalkozásokat tartani, és az újonnan megjelenő fenyegetésekről tájékoztatni levélben, esetleg oktatóvideókkal (pl.:A mobil eszközök felhasználóit célszerű mobil fenyegetésekről tájékoztatni, időszakosan felkészítő https://www.youtube.com/watch?v=3mIi_09CI9w https://www.youtube.com/watch?v=S8fuyJP_ZAA https://www.youtube.com/watch?v=X6wrm2hVXjo)

45 Mobile Apps: How To Use Them Safely, State of Illinois Central Management Services -Monthly CyberCyber Security Tips NEWSLETTER, Volume 7, Issue https://www2.illinois.gov/sites/doit/media/Documents/Security/2012/Cybertip_03.2012.pdf

Végül arról sem szabad megfeledkezni, hogy bármilyen körültekintő is a védelmi rendszerünk, vagy képzettek a felhasználóink és üzemeltetőink, biztonsági eseményekre akkor is készülni kell. A mobil eszközöknél a „klasszikus" számítógépes rendszerekben megszokottól eltérő jellegű fenyegetésre is számítani kell (pl.: SMS alapú támadások, Juice Jacking, stb.), továbbá a technikai háttér is speciális, így az asztali operációs rendszerek esetén alkalmazott módszerektől eltérőeket kell alkalmazni (pl.: a mobil igazságügyi szakértői vizsgálat, archiválás és helyreállítás, gyári beállítások visszaállítása, kártékony kódok analizálása, hálózati forgalomelemzés is eltérhet a „megszokottaktól"). Ezekre a rendszerekre így más procedúrákat és technikákat kell használni, melyeket kidolgozást követően integrálni kell a szervezetnél már meglévő incidenskezelési tervben (a mobil eszközök a szervezeti informatikai rendszereket bővítik ki, így célszerű egységes metodika szerint kezelni azokat, és nem elfelejtve, hogy pl. egy mobil felhasználónak asztali számítógépe is lehet, így a biztonsági eseményeket a mobil és a "klasszikus" rendszerek esetén is vizsgálni kell, valamint keresni az összefüggéseket a kettő között).

A felhasználó szempontjából talán a legfontosabb, hogy ismerje fel a biztonságot veszélyeztető tényezőket, a kompromittálódás jeleit, és tudja, hogy azt kinek kell jeleznie.

Mindenki tudja, hogy a tűzoltókat kell hívni ha meggyulladt valami, a rendőrséget ha betörést észlelt, a mentőket baleset esetén. A kérdés, hogy a felhasználók tudják-e, hogy kit kell hívniuk biztonsági események felfedezése esetén. Amennyiben a szervezetnek van központi informatikai üzemeltetése, 24 órás hálózatfelügyelete, akkor célszerű az ő telefonos, email, chat elérhetőségüket megadni. Amennyiben nincs, akkor a szakterületen illetékes CERT[46] szervezet elérhetőségét javasolt megadni (természetesen az adott szervezettel egyeztetni is kell ez ügyben).

NEMZETKÖZI AJÁNLÁSOK ÉS SZABVÁNYOK A MOBILVÉDELEM TERÜLETÉN

Az OWASP (Open Web Application Security Project) egy online közösség, melynek elsődleges célja a web alapú-, és az azzal kapcsolatos technológiák biztonságának fokozása a fejlesztők felkészítése, tesztelési metodikák és oktatási anyagok biztosítása révén. A mobil technológiában is egyre nagyobb mértékben alkalmazzák a web alapú technológiákat, így a közösség ezen technológiákat is szem előtt tartja. A 2016-os évben kiadott top 10 mobil fenyegetésnek[47] az alábbiakat értékelték:

- **M1** a mobil operáció rendszerek védelmi mechanizmusainak nem megfelelő használata (pl.:TouchID, Keychain);
- **M2** nem biztonságos adattárolási módszerek;
- **M3** nem biztonságos kommunikáció, adatátvitel (gyenge kriptográfiai algoritmusok, rossz implementációk);
- **M4** nem megfelelő autentikáció (rossz azonosítási eljárás, rossz hitelesített munkamenet ellenőrzés);
- **M5** nem elégséges kriptográfia támogatás;
- **M6** rossz jogosultság kezelés;
- **M7** kliens oldali szoftver minőségi hiányosságai;
- **M8** szoftver védelem hiánya (bináris fájl változtatásának lehetősége, hooking, dinamikus memória modifikálás);
- **M9** reverse engineering (futtatható állományok működésének visszafejtésének lehetősége, mely következtében kijátszhatóvá válnak a védelmi megoldások, vagy sérülékenységek fedezhetőek fel);

[46] Computer Emergency Response Team - számítástechnikai incidenskezelő csoport
47 Forrás: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

M10 rejtett funkciók (pl.: backdoor, vagy alapértelmezett jelszó az alkalmazásban).

Ezeknek és további fenyegetéseknek a kivédése érdekében a fejlesztőknek és a biztonsági tesztelőknek egy ellenőrzési listát[48] is összeállítottak. Továbbá olyan alkalmazásokat[49] is fejlesztenek, melyeken a fejlesztő gyakorolhatnak, vagy segítik fejlesztési munkájukat.

A *NIST 800-163*-as ajánlása[50] az alkalmazás fejlesztők, és a 3. fél által fejlesztett alkalmazásokat tesztelő szakemberek számára ad iránymutatást az ilyen folyamatok és képességek kifejlesztésének menetében. Bemutatja a lehetséges teszteket (megfelelőségi tesztek, forráskód-, bináris kód elemzések, statikus és dinamikus vizsgálatok, és az automatizálás lehetőségeit). A függelékekben felsorolják az ismert mobil operációs rendszerek főbb sérülékenységeit.

A *NIST 800-124-es* ajánlása[51] pedig a vállalati szintű mobil eszköz menedzsment követelményeit, és az életútját (követelménytámasztás, tervezés, implementáció, üzemeltetés és visszavonás) mutatja be.

Az ENISA készített egy összefoglalót a mobil eszközök (okostelefonok) fenyegetésének azonosíthatóságának érdekében[52]. Három különböző szintre sorolja be az okostelefonok használatát: magán, vállalati, és vezetői (VIP). Ezt követően pedig a fenyegetéseket a különböző felhasználási körök esetén azok bekövetkezési valószínűsége, gyakorisága, és hatása alapján értékeli. Érdemes egy szervezet mobil rendszerének fenyegetéseinek összegyűjtésekor, valamint a védelmi kontrolljainak tervezésénél ezt az összefoglalót, mint mintát felhasználni. Ugyancsak segítség lehet az „*Űrlap biztonsági osztályba soroláshoz és a védelmi intézkedések kiválasztásához, a 41/2015. (VII. 15.) BM rendelet alapján*” című táblázat[53], mely szerkeszthető formában összefoglalja a BM rendeletben előírt adminisztratív, fizikai és logikai védelmi intézkedéseket, valamint segít az osztályba sorolás folyamatában.

KÖVETKEZTETÉSEK

Jelen cikkben a mobil eszközök fenyegetései, és azok kezelésére alkalmazható kontrollok kerültek bemutatásra. A bemutatott fenyegetések közül egyesek egzotikusnak tűnhetnek, azonban céljuk felhívni a figyelmet, hogy az innovatív gondolkodású támadók kijátszhatják a konvencionális védelmi megoldásokat, így célszerű több fenyegetési modell szempontjából megvizsgálni, és többrétegű védelemmel biztonságban tudni adatainkat, valamint az általunk használt szolgáltatásokat.

A mobil eszközök munka célú használata miatt egyre nagyobb az igény a magán- és a szervezeti információk elkülönítésére, melyre a cikkemben részletesen kitértem.

Remélem a fenti példák felébresztették az olvasóban az igényt a biztonságos internetezéshez, és elindultak egy úton, hogy „tudatos” felhasználókká váljanak.

48 Lásd:https://drive.google.com/file/d/0BxOPagp1jPHWYmg3Y3BfLVhMcmc/view
49 További részletek:https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
50 Forrás:Steve Quirolgico, Jeffrey Voas, Tom Karygiannis, Christoph Michael, Karen Scarfone: Vetting the Security of Mobile Applications (NIST 800-163)
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf
51 Forrás: Murugiah Souppaya - Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST SpecialPu blication 800-124 Revision 1)
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
52 Forrás:Enisa - "Smartphones: Information security risks, opportunities and recommendations Fofor users"
https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport
53 Link: http://www.neih.gov.hu/sites/default/files/dlc/41_2015_BM_VHR_OVI_151102_0.xltm

FELHASZNÁLT IRODALOM

[1] http://static2.businessinsider.com/image/57bb2394ce38f2c0008b8111-1200/20160822_android_ios.png (Letöltve:2017.08.20)

[2] Yuwei ZHENG, Lin HUANG, Qing YANG, Haoqi SHAN, Jun LI, Ghost Telephonist Link Hijack Exploitations in 4G LTE CS Fallback - Blackhat 2017 konferencia https://www.blackhat.com/docs/us-17/thursday/us-17-Yuwei-Ghost-Telephonist-Link-Hijack-Exploitations-In-4G-LTE-CS-Fallback.pdf (Letöltve:2017.08.20)

[3] https://www.schneier.com/blog/archives/2016/08/nist_is_no_long.html (Letöltve:2017.08.20)

[4] http://techwelkin.com/wp-content/uploads/2014/11/2g-3g-4g-e-h-data-speed-comparison-techwelkin.png (Letöltve:2017.08.20)

[5] Nitay Artenstein - Broadpwn: Remotely Compromising Android and iOS via a Bug in Broadcom's Wi-Fi Chipsets https://blog.exodusintel.com/2017/07/26/broadpwn/ (Letöltve:2017.08.20)

[6] The University of Texas at Austin - UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea, Online https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea (Letöltve:2017.08.20)

[7] Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, David Brumley - GPS Software Attacks, Online https://users.ece.cmu.edu/~dbrumley/pdf/Nighswander%20et%20al._2012_GPS%20software%20attacks.pdf (Letöltve:2017.08.20)