Okoseszközök

Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára

BÁNYÁSZ PÉTER – SZABÓ ANDRÁS – ORBÓK ÁKOS

Nemzeti Közszolgálati Egyetem, Budapest

A Nemzeti Közszolgálati Egyetem kiadványa

Szerzők:
Bányász Péter
Orbók Ákos
Szabó András

Szakmai lektor:
Prof. Dr. Nemeslaki András

A hatályosítást 2022-ben végezte:
Mikula Fanni

A hatályosításért felelős szakmai szakértő:
Legárd Ildikó

A hatályosított kézirat lezásrásának dátuma:
2022. február 25.

Eredeti megjelenés éve:
2016

Kiadja:

Közigazgatási Továbbképzési Intézet

Felelős kiadó:
Prof. Dr. Kis Norbert
rektorhelyettes

TARTALOM

I. Bányász Péter – Orbók Ákos: Bevezető az okoseszközök világába 4

1. Az okos mobileszközök evolúciója 4
2. Az okos mobileszközök csoportosítása 8
   2.1. Hardver 8
   2.2 Szoftver 9
3. Az okos mobileszközök működési környezete 10
4. Az operációs rendszerek összehasonlítása 12
5. Malwarek és az okos mobileszközök 13
6. A jelentősebb gyártók gazdasági potenciálja 15
7. Az okos mobileszközök jövőképe 19
8. Felhasznált irodalom 19

II. Szabó András: Okoseszközökhöz kapcsolódó adatvédelmi kérdések 21

1. Információbiztonsági és adatvédelmi alapvetés 21
   1.1. Bevezető gondolatok 21
   1.2. Alapvetés az adatvédelemhez és az információbiztonsághoz 22
2. Rendszertani és szabályozási környezet 23
   2.1. Nemzeti szabályozás 23
   2.2. Európai uniós kapcsolódások 28
3. Adatvédelem és az Infotv. szabályozási környezete 32
   3.1. Az adatvédelmi szabályozás főbb mérföldkövei 33
   3.2. Az Infotv. releváns rendelkezései 35
4. Jövőbeni kihívások és lehetőségek 46
5. Felhasznált irodalom 47
6. Jogszabályok jegyzéke 47
7. Felhasznált internetes források jegyzéke 48

III. Bányász Péter: Az okos mobil eszközök jelentette kiberbiztonsági kihívások 49

1. Kiberfenyegetettségek osztályozása 50
2. Új típusú kihívások az okos mobil eszközök tekintetében 53
3. Az alkalmazások használatából fakadó biztonsági kockázatok 55
4. A közösségi média és az okos mobil eszközök 61
5. Social engineering és az okos mobil eszközök 66
6. Felhasznált irodalom 68

Fogalomtár 70

I. BÁNYÁSZ PÉTER – ORBÓK ÁKOS: BEVEZETŐ AZ OKOS-ESZKÖZÖK VILÁGÁBA

1. Az okos mobileszközök evolúciója

Az okos mobileszközök megjelenését a közvélemény általában az Apple által először piacra dobott iPhone-hoz kapcsolja, ez azonban nem helytálló. Bár az Apple számos olyan újítást vezetett be, aminek hatására elterjedtek az okostelefonok, később a tabletek, már a kilencvenes évek elején megjelentek olyan eszközök, amiket az „okos" jelzővel lehetett leírni. Az okos mobileszközök fejlődése így korántsem tekinthető irrelevánsnak abban a tekintetben, hogyan alakul ezen eszközök védelme. A fejezet azt a fejlődést mutatja be, amely napjainkig meghatározta az okos mobileszközök piacát, illetve bepillantást enged a jövőbe.

Az okostelefon az angol smartphone szó tükörfordításából ered. A smartphone kifejezést első ízben az Ericsson GS88 „Penelope" nevet viselő készülékre alkalmazták 1997-ben. Akkoriban a smartphone tehát egy leíró szó volt, ami jellemezte a GEOS operációs rendszerrel szerelt, e-mail, WAP[1] és IrDA[2]-képes telefont. Összehasonlítva a napjainkban elterjedt okostelefonokkal, rendkívül kezdetleges technológiának tűnik mindez, azonban abban az időben csúcstechnológiának számított, s csupán egy évtizedre volt szükség, hogy egy olyan rendkívül gyorsan fejlődő iparág alakuljon ki, amely a mai okos mobileszközöket takarja. A fejezetben a fontosabb mérföldköveket vesszük górcső alá, amelyek a napjainkban elterjedt okos mobileszközök megszületéséhez vezettek. Az okostelefonok fejlődéstörténetéről a LogOut nevű portál szerzője, HuMarc készített egy rendkívül széleskörű áttekintést, amelyből az általunk jelentősebbnek tartott mérföldköveket vesszük alapul.[3]

Az okostelefonok első generációja 1994 és 2002 közé datálható, amit inkább egy elő-elő okostelefon korszakként lehetne jellemezni, de ekkor még nem volt olyan komolyabb technológiai robbanás, ami segítette volna az elterjedésüket. A készülékek technikai leírását az 1. számú táblázat tartalmazza.

Az első telefon, ami már „okos"-ként nevezhető, az IBM által 1994-ben megalkotott Simon nevet viselő készülék. Az IBM Simon után a Nokia próbálkozott újra betörni az okostelefon piacra 1996-ban a 9000 Communicator nevű készülékével. A telefon újítását az jelentette, hogy kinyitható volt, így kétféleképpen is használhattuk.

Két évvel később ismét a Nokia újítása jelent meg, a Nokia 9110 legnagyobb újdonsága az MMC-kártyával való bővíthetőség.

2000-ben az Ericsson is piacra dobott egy okostelefont, az R380-at, ami a Symbianos mobilok ősének tekinthető, ugyanis az EPOC 6. verziója, ami közvetlen utódja az EPOC 5.1-nek, már Symbian Operating System néven jelent meg. Ez év novemberében a Nokia is új készüléket jelentetett meg, Nokia 9210 néven, ami a Nokia 9110 utódjaként tartható számon. Az elődhöz képest nagyon jelentős fejlődésen ment keresztül.

---

[1] A Wireless Application Protocol (WAP) a vezeték nélküli adatátvitel egy nyílt nemzetközi szabványa. Hordozható eszközökhöz (mobiltelefonok, PDA-k) fejlesztették ki. A protokollcsalád célja a webböngészés lehetővé tétele csökkentett funkciókkal és néhány mobilspecifikus kiegészítéssel. Ezt a protokollt használja a legtöbb mobiltelefonra írt internetes oldal (wap site).

[2] Infravörös port.

[3] HuMarc: Okostelefon-evolúció, In. LogOut, 2013. május 15., https://logout.hu/cikk/okostelefon-evolucio/bevezeto.html (2016. szeptember 15.)

2001 februárjában a Palm is megjelentetett egy telefonálásra alkalmas szoftvert a PalmOS-t futtató PDA-k számára.[4] A Palm már 2001-ben is (talán az egyetlen a HP mellett) nagy név volt a PDA-piacon, így kézenfekvő lehetett, hogy egy telefonálásra is alkalmas szoftvert adjanak ki. A szoftver adott volt, ám a Palm Inc. egyelőre nem adott ki hardvert is a szoftverhez, így az első PalmOS-szel hajtott okostelefon a Kyocera nevű cég 6035 nevű/kódszámú készüléke volt. Rendelkezett webböngészővel, így korlátozott módon ugyan, de képes volt fellépni a világhálóra. Tartalmazta a PalmOS-szel megtámogatott PDA-k (vagy éppen palmtopok) érdekességét, a Palm OS Graffiti technológiáját. A Kyocera 6035 volt az első, széles körben elterjedt okostelefon.

Az első Series 60-nal megjelent mobiltelefon/okostelefon a 2001 novemberében megjelent Nokia 7650 volt, ami bár egy régi Nokia telefonra emlékeztetett, ám belül egy okostelefon hardverét tartalmazta és számos változáson ment keresztül. A legnagyobb újítása mégis a beépített kamera volt. Bár eddig is voltak fényképezésre képes telefonok, hiszen az első kamerás mobil valójában a Kyocera VP-210 volt, ám ez nem terjedt el széles körben, mivel csak Japánban forgalmazták.

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 Okostelefonok 1994-2002. között
Forrás: Saját szerkesztés Logout, TelefonGuru alapján

Ahogy korábban megjegyeztük, az 1994–2002 közé datált időszak egyfajta elő-elő okostelefon korszak volt. 2002-ben azonban beindul egy olyan technológiai robbanás, egy gyorsabb fejlődés, aminek hatására nagyobb ütemben terjednek az okostelefonok, míg el nem érünk az Apple nevével fémjelzett korszakig. A 2001 után kezdődő időszakban az okostelefonok gyorsabb ütemben kezdtek el fejlődni, mint addig, de 2002-ben valószínűleg kevesen gondolták volna, hogy 2016-ban, 15 év múlva többmagos, 216 GB RAM-mal és Full HD kijelzővel szerelt telefonok kerülnek a piacra, hiszen akkoriban az ilyen hardver még asztali számítógépek szintjén sem tűnt általánosnak. Mindenesetre 2002-ben a Nokia elkezdi uralni az eddig igen kicsiny, ám egyre nagyobbá duzzadó okostelefon-piacot, és ez így marad talán egészen 2008-ig, amikor már mind az iOS, mind az Android tarol a piacon. A Blackberry

[4] Fontos megjegyezni, hogy a Kyocera 6035 nem a Handsprings – későbbi nevén Palm Inc. – terméke volt, hanem a Kyoceráé, tehát tulajdonképpen nem a Palm jelentette meg ezt a készüléket, ám mégis fontos lépés, hiszen a Palm végre beleteszi a szoftverébe a PalmOS-be a GSM-támogatást. A Palm csak 2002-ben jelent meg a piacon okostelefonnal. Ez volt a Palm Treo 180, ami azonban nem hordozott semmiféle technikai újdonságot, nem is terjedt el különösen nagymértékben.

is gyorsabb ütemű fejlődésbe kezd, és egyre több telefonálásra alkalmas Microsoft Pocket PC jelenik meg. A készülékek leírását a 2. számú táblázat tartalmazza.

2002. január 1-jén jelent meg a RIM első, Blackberry néven forgalmazott készüléke, amelynek érdekessége, hogy telefonálni csak headseten keresztül lehetett vele, ami annyit jelent, hogy nem volt beépített mikrofonja és hangszórója.

Az első Androidos operációs rendszerrel működő telefon a HTC G1 „Dream" (és G2 „Magic") volt. Amit sokan nem tudnak az az, hogy a HTC-t 1997-ben alapították, és eleinte az volt a cég fő profilja, hogy legyártott egy készüléket, amit aztán több cég vagy szolgáltató is brandelt. 2002-ben megjelenik az első HTC „okostelefon" Wallaby néven. Ezt a készüléket 6 cég is brandelte (Qtek, i-mate, Dopod, O2, T-mobile és Siemens), ami azt jelenti, hogy 2002-ben összesen 6 cég kínálatában jelent meg ugyanaz a telefon, más márkajelzéssel.

A következő években alapvetően különböző hibridekkel próbálkoztak a gyártók, amelyek mind alakjukban, mind funkciójukban jelentettek inkább újdonságot. 2003-ban megjelent az első „igazi" Blackberry, a 6210-es, amely bár hasonló volt az 5810-hez, ám ez már képes volt headset, vagy bármi egyéb kiegészítő nélkül hívást indítani és fogadni. Abban eltért viszont az 5810-től, hogy míg annak egy négyzet alakú, 160×160 pixeles kijelzője volt, ez egy 160×100 pixeles kijelzővel rendelkezett, teljesen más képarányú kijelzőt kapott.

2003-ban a Nokia egy nagyon merész ötlettel állt a világ elé, amikor bemutatta a Nokia N-Gage nevű okostelefon-marokkonzol hibridet. Kialakítását tekintve nem nevezhető éppen közönségesnek. A Nintendo Gameboy Advance ellenfelének szánták, azonban az eladások tekintetében messze alulmaradt riválisától. Okostelefon mivolta csak a rendszer szempontjából tűnik fel, ami egy Symbian Series 60. Az N-Gage inkább mint játékkonzol jelentős, hiszen ha maga az N-Gage brandként később meg is bukott, maga az első N-Gage akár sikeresnek is nevezhető, hisz 56 játék jelent meg rá. A készülékben már megtalálható az MMC-kártyával való bővítés lehetősége, ami tulajdonképpen megfelelhet a GameBoy cartridge-nek, vagy éppen az akkor még nem létező PSP-k UMD-jének, amiről beolvassa a játékot, viszont akár hagyományos módon, memóriakártyaként képek, zenék tárolására is alkalmas volt.

Ugyanebben az évben a Blackberry új telefonnal, a 72×× széria első darabjával, a 7210-zel lépett a piacra. Az újítás a 6210-hez képest, hogy ez színes kijelzővel, jóval nagyobb, 240×160 pixeles felbontással került piacra. További eltérés, hogy a RIM ugyanazzal a hardverrel többféle telefont gyártott (7210, 7220, 7230, 7250, 7270, 7280. 7290), azonban az eltérő típusszámok eltérő hálózatot kezeltek. Példának okáért a 7210 900 és 1900 MHz-s GSM-hálózatokra képes fellépni, míg a 7250 a 800 és az 1900 MHz-s CDMA2000-re. Ebből az okból egy-egy sorozatnak (58××, Quark, 72××) elég csak az első modelljét bemutatni. Mindazonáltal vannak típusok, amelyek mellett nem mehetünk el szó nélkül, mert nem csak a hálózati módban különböznek az alapverziótól. Ilyen például a 7270 is, ami az első WiFi-s Blackberry és egyike az első WiFi-s telefonoknak.

A 2003 4. negyedévében megjelent Nokia 6600 és a Symbian 7.0, azaz a Series 60 2nd Edition nem rendelkezett sok újdonsággal a 7650-hez képest, viszont egy népszerű modellről van szó, így meg kell említenünk. A telefon képes videót felvenni, illetve témákat is lehetett rá tölteni. Tojásdad formája nem nevezhető éppen megszokottnak, de ennek ellenére a maga korában sikeres és közkedvelt volt. A Nokia 6600-zal egy időben jelent meg a PalmOne Treo 600 is. Egy nagyon sikeres modellről beszélünk, ami a Blackberryk tényleges felvirágzása és elterjedése előtt kicsivel az egyik legsikeresebb üzleti mobil volt, hisz tökéletesen ötvözte a telefont, a PDA-t és a kamerát.

2005-ben jelent meg a Nokia 6680, ami az első 3G-s mobilok egyike volt, illetve két kamerával rendelkezett. Az elsődleges, hátoldali kamera egy 1,3 megapixeles egység LED-villanóval, a másodlagos, előlapi kamera pedig videóhívások lebonyolítására tette alkalmassá.

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 AR-M926EJ-S	10 MB	Symbian 8,0	1,x Mpixel két kamera	176*208 (18 bit)	GPRS, EDGE, WAP, Bluetooth, E-mail,

2. táblázat Okostelefonok 2002–2007. között
Forrás: Saját szerkesztés, Logout, TelefonGuru alapján

Az iPhone 2007 júniusában mindent megváltoztatott. Letisztultsága, kezelhetősége elért egy olyan szintre, amit azelőtt egyetlen más rendszer sem volt képes elérni. Forradalmasította az okostelefonokat, hiszen most már nemcsak informatikusok és hozzáértők kiváltsága volt az okostelefon, ugyanis egy iPhone-t bárki tud kezelni. Természetesen nem egyedül az iPhone-nak köszönhető az, hogy napjainkban ilyen okostelefonok vannak, ám ha az Apple 2007-ben inkább egy új iPodot ad ki, ma nem így néznének ki az okostelefonok. Az iPhone nélkül vélhetően az Android is teljesen más fejlődési utat jár be. Az iPhone-t közel sem lehet tökéletesnek nevezni, azonban egy olyan paradigmaváltást indított be, amely alapvetően alakította át az okos mobileszközökkel kapcsolatos viszonyunkat, megteremtette az igényt a könnyen kezelhető okostelefonok iránt.

A tabletek esetében hasonló folyamat írható le, mint a mobiltelefonok esetében. Az első kereskedelmi forgalomba kerülő készülékek közül az 1989-ben piacra dobott Grid Systems GRiDPAD-ja volt az, ami legjobban egyesítette mindazt formában, amit alapvetően a táblagépekben ma is meghatározónak tartunk, de a 10 hüvelykes kijelző itt még monokróm, és beépített toll segítségével volt lehetőség az adatbevitelre. Képességei korlátozottak voltak mai szemmel, és természetesen a technikai fejlettség azon időszakában még szó sem lehetett médiakezelésről, de jóval meghaladta korát. Az első mai értelemben vett táblagépet a Microsoft cég jelentette be 2001-ben. 2002-ben került forgalomba, de magas ára miatt nem lett hozta meg a várt sikert, gazdasági bukás volt. Az igazi áttörést itt is az Apple iPad megjelenése hozta 2010-ben. Az Apple már a Microsoft készülékének 2002 forgalomba hozása után fejleszteni kezdte a maga táblagépét, de a munkákat felfüggesztették, amikor az iPhone

ötlete felmerült, és az erőforrásokat és az addigi fejlesztéseket a telefongyártásnál használták fel. Az iPhone sikere után aztán újraindult az új termékszegmens fejlesztése, ami – köszönhetően a tudatos tervezésnek és marketingnek – páratlan áttörést hozott. A 2002 és 2010 közötti időszakban csak szórványosan jelent meg egy-egy új modell, de az iPad sikere után 2010-ben a főbb hardvergyártók piacra dobták a maguk modelljét. Többségük már az iPad felépítése alapján fejlesztett, ami több szabadalmi perhez is vezetett később. Az erős konkurencia hatására az árak esni kezdtek. A 2011-ben a korábban e-könyv olvasók piacán vezető szerepet betöltő Amazon is belépett a táblagépek piacára a Kindle Fire táblagépével. Az Amazon piacszerzési módszerének alapja a rendkívül nyomott alacsony ár tartása a hardvereladásoknál, így a Kindle Fire megjelenésével alámént a korábban lélektaninak számító 200 dollárnak, új irányt mutatva a piacnak.

2. Az okos mobileszközök csoportosítása

2.1. Hardver

A hardver szempontjából három nagy csoportot különíthetünk el. A legelterjedtebb az **okostelefon**, amellyel kezdődött a mobil távközlés forradalma. Ennek méretei általában egykezes kezelhetőséget tesznek lehetővé, tehát a képátlójuk nem nagyobb, mint 16 centiméter. Ennél nagyobb kivitelben már **tablet**nek nevezzük az okoseszközt. Ez a kategória általában csak a méretében és egyes funkcióiban különbözik a kisebb kivitelű telefontól. A telefonok mindegyike rendelkezik GSM kommunikációs funkcióval, a tableteknek csak egy részében elérhető ez a szolgáltatás. Egy gyártó általában csak egy operációs rendszerrel dolgozik a különböző konfigurációjú készülékein, de előfordul, hogy a telefonokra és tabletekre külön operációs rendszer fejlesztése szükséges az optimális működés érdekében.

A tabletek esetében is a méret nevezhető az igazi korlátnak, hiszen bizonyos méreten felül már használhatatlanná válik. Ez a határérték nagyjából a laptopok méretével egyezik meg, tehát 44 centiméter alatti képátlóval készülnek.

A **tablet-laptop hibrid** eszköz kategória nem is feltétlenül számítható külön kategóriaként, hiszen tulajdonképp a tablethez csatlakozó billentyűzetből áll, amelyen lehetnek kiegészítő számítógépes perifériák is. Annyiban elkülönül a tabletektől, hogy amikor a kiegészítő billentyűzettel összekapcsolódik, az operációs rendszere is átvált mobil operációs rendszerről a számítógépre optimalizált változatra (Windows 10), ezzel könnyítve például a szövegszerkesztést.

Az **okosóra**, amely képes lehet telefonként funkcionálni önmagában is, egy viszonylag új kiegészítő készüléke az okoseszközöknek. A szerkezet általában bluetooth kapcsolattal áll összeköttetésben az „anya" eszközzel. Az óra funkcióinak száma változó lehet, a legegyszerűbb kivitelek az idő mutatáson kívül csak egy kiterjesztett kijelzőként működnek és esetleg számlálják a felhasználó lépéseit. Ezek az egyszerűbb eszközök nem rendelkeznek olyan komplex operációs rendszerrel, mint az okostelefonok, elsősorban a telefonra telepített alkalmazás működteti a kiegészítő eszközt.

A kifinomultabb szerkezetek már saját operációs rendszert alkalmaznak (amely általában az anyaeszközön futó operációs rendszer egyszerűsített változata) és teljes értékű kijelzővel vannak felszerelve. Az alap funkciókon kívül a felhasználó egészségügyi adatait is képesek mérni. A funkciói közé tartozhat a lépésszámlálás, pulzusmérés, alvásciklus megfigyelés és ezek elemzése, összehasonlítása.

A legösszetettebb szerkezetek már saját SIM kártya befogadására is képesek és egy bluetooth fejhallgató segítségével teljes értékű telefonként is használhatóak. A fent már említett funkciókkal kiegészülve ezek a készülékek kielégíthetik azoknak a felhasználóknak az igényét, akiknek nincs szükségük egy teljes értékű okostelefonra

Az **okosszemüveg**et a Google alkotta meg, amely szintén egy kiterjesztett eszköz- kombináció. A szemüveg szárában kamera található, a lencse elé egy prizma segítségével egy kivetítő eszköz mutatja a felhasználónak a kért információkat az okoseszközéről. Egyes szemüvegekbe fülhallgatót is építettek, hogy a lehetséges igényeknek megfeleljenek.

Az okosszemüveget tulajdonságai miatt kitiltották olyan helyekről, ahol tilos fényképet készíteni. Biztonsági szempontból érthetőek ezek a döntések, hiszen az eszköz rejtve maradhat az átlagemberek számára, akikről a szemüveget alkalmazó hang és képfelvételt készíthet az engedélyük és tudtuk nélkül.

2.2 Szoftver

2.2.1. Operációs rendszerek

Az operációs rendszerek csoportosításánál több nagy csoportot különíthetünk el, a **Microsoft OS**-t, az iOS-t, a BlackBerry-t és a Firefox OS-t, amelyek az elsőn kívül mind a **Linux** mobil operációs rendszeren alapulnak. A Linux maga is készített operációs rendszert okostelefonokra, de a későbbiekben már csak mint kiindulópont volt a szoftverfejlesztés folyamatában. A Linuxon alapuló operációs rendszerek közül a legismertebb és elterjedtebb az **Android OS**, amelyet a Google fejlesztett ki és használ a saját márkás (régebben NEXUS, ma már PIXEL) okoseszközein. Az Android, ahogy a Linux is, kernelt használó mobil operációs rendszer,[5] elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve. Az Android 1.0 platform 2008. október 21-én került kiadásra Apache licenc alatt. Elég nagy számban készültek változatai, a különböző gyártók saját verziókat fejlesztettek a saját készülékükre optimalizálva azt. Ebből is kitűnik az Android rugalmassága programozási szempontból. A **Xiaomi- MIUI Palm WebOS** is Android alapú, de a felsorolást szinte minden gyártóra kiterjeszthetnénk.

A két legelterjedtebb operációs rendszer a Google (Android) és az Apple (OsX) rendszere. A két gyártó üzletfilozófiája merőben eltérő képet mutat. Az Google operációs rendszerét számtalan gyártó használja saját készülékükre optimalizálva, még korábbi konkurenciái is (Microsoft, Blackberry). Az Apple szoftverét csak az Apple által gyártott eszközökön használják. Ennek következményeként a két gyártó fő célközönsége is más.

Biztonsági szempontból is meghatározó az üzletfilozófia. Mindkét nagy gyártónak saját webáruházában árult alkalmazásai más biztonsági szinten kerülnek a felhasználókhoz. Az Apple biztonsági előírásai sokkal szigorúbbak a Google-énél. Ehhez társul az a tény is, hogy az Apple készülékeit és a rá készített alkalmazásokat a gyártó jobban kézben tudja tartani, mint a konkurenciái, ezért a támadásokban való érintettsége is alacsonyabb.

2.2.2. Alkalmazások

Minden operációs rendszerhez készülnek kiegészítő alkalmazások, amelyeknek a száma az operációs rendszer elterjedésétől függ. Általában az alkalmazásokat nem csak az operációs rendszerek gyártói készítik, hanem független fejlesztők is. Az alkalmazások mindig valamilyen kiegészítő lehetőséget vagy valamilyen céleszközt nyújtanak a felhasználóiknak. Léteznek ingyenes és fizetős változatok is, amelyek elérhetőek a nagy gyártók webáruházaiból. Ugyanazt az alkalmazást optimalizálják a különböző operációs rendszerekhez, így téve elérhetővé azt minél szélesebb körben.

Az alkalmazások biztonsági kockázatai pont azért nagyok, mert a bárki készítheti őket, csak a webáruházak biztonsági előírásai szabnak határokat egyes alkalmazások rosszindulatú tevékenységeinek. Ha valaki nem a hivatalos webáruházból tölti le az alkalmazást, akkor nincsenek meg azok a korlátok sem. A jogosulatlan hozzáféréseket kérő alkalmazásokat ellenőrizhetjük a http://privacy-grade.org/home oldalon, ahol az egyes alkalmazásokat rangsorolják A–D-ig osztályozva adatbiztonsági szempontokból.

[5] Lásd: http://www.openhandsetalliance.com/android_overview.html (utolsó letöltés: 2016. október 7.)

3. Az okos mobileszközök működési környezete

Az okos eszözök több szabvány szerint kommunikálhatnak. A legelterjedtebb kommunikációs szabványokat minden gyártó alkalmazza, azért hogy a készülékek ne csak a saját márkájú eszközökkel létesíthessenek kapcsolatot, hanem az összes okoseszközzel. A GSM az első szabvány, amely az alapját képezi a mobilkommunikációnak. Ha a legújabb készülékeket vizsgáljuk, a Google Pixel XL márkanevű terméke a következő szabványokat képes kezelelni: GSM / CDMA / HSPA / EVDO / LTE, 2G GSM, 3G, HSDPA, 4G LTE, GPRS, EDGE[6]

GSM:[7] A GSM Global System for Mobile Communications, az Európai Távközlési Szabványok Intézete (ETSI) által kifejlesztett szabvány a mobiltelefonok által használt második generációs digitális cellás hálózatok protokolljainak leírására. Valóban a mobil távközlés globális szabványa, több mint 90% a piaci részesedése, a világ több mint 219 országában vagy területén érhető el. A GSM szabványt az első generációs (1G) analóg cellás hálózatok helyettesítésére fejlesztették ki. Eredetileg egy teljesen kétirányú hangátvitelre szolgáló digitális, kapcsolat alapú hálózatot írt le. Később kiterjesztették adatkommunikációra, előbb kapcsolat alapú, azután csomagkapcsolt átvitelre a GPRS és EDGE szabványokban. A későbbiekben a 3GPP kifejlesztette a harmadik generációs (3G) UMTS, majd a negyedik generációs (4G) LTE szabványt, amelyek nem részei az ETSI GSM szabványnak.

A GSM legnagyobb biztonsági kockázata a lehallgathatósága. Bár a szabvány legújabb generációja számos titkosítást alkalmaz, ezeket célszoftverekkel hatékonyan lehet támadni.

WIFI:[8] A mobiltelefonok fejlődésével az okoseszközöknek szükségük van internetes kapcsolatra. A GSM szabvány fejlesztésével ez elérhetővé vált, de párhuzamosan fejlődött a Wifi az IEEE által kifejlesztett vezeték nélküli mikrohullámú kommunikációt (WLAN) megvalósító, széleskörűen elterjedt szabvány (IEEE 802.11). Ez a szabvány biztonságossá tehető, azonban a legtöbb esetben komoly biztonsági kockázat. Kifejezetten a nyilvános hálózatok jelentenek veszélyt. A nyilvános Wi-Fi-hálózatok egy részénél nem titkosítják a csatlakozó eszközök és a router közötti forgalmat, ezek azok az ingyenes szolgáltatások, amelyek igénybe vételénél nem kell semmilyen azonosítót vagy jelszót megadnunk. Az adathalászok man-in-the-middle támadást hajthatnak végre, melynek során beékelik magukat a számítógépünk és a Wi-Fi-router közé, így a hálózatra kapcsolódáskor nem közvetlenül a hotspottal kommunikálunk, hanem a hackereknek küldjük el az információkat. Jó megoldás lehet egy VPN-szolgáltatás, amely eltérítheti a támadót egy könnyebb célpont felé.

BLUETOOTH:[9] Az eddig tárgyalt szabványok egyaránt egy külső hálózathoz kötöttek, azaz anélkül nem működnek. Ezzel szemben két vagy több eszköz között rövid hatótávon belül létesített kapcsolathoz fejlesztették ki a Bluetooth nevű, rövid hatótávolságú, adatcseréhez használt, nyílt, vezetéknélküli szabványt. Alkalmazásával számítógépek, mobiltelefonok (telefonkihangosítók) és egyéb készülékek között automatikusan létesíthetünk kis hatótávolságú rádiós kapcsolatot. A wifi-hez hasonló biztonsági kockázatot rejt a szabvány működése. Különösen igaz ez, ha nem két okoseszköz, hanem egy telefonhoz kapcsolódó kiegészítő eszközt is alkalmaz a felhasználó. Ebben az esetben a kiegészítő eszközhöz férhetnek hozzá a támadók, és ezáltal az okoseszközünkhöz is. De már a kiegészítő eszköz által sugárzott adatok is értékesek lehetnek a támadóknak, hiszen egészségügyi vagy más személyes adatokat is tartalmazhatnak.

NFC: Az NFC **(Near field communication)**[10] egy rövid hatótávú kommunikációs szabványgyűjtemény okostelefonok és hasonló eszközök között, egymáshoz érintéssel vagy egymáshoz nagyon közel helyezéssel létrejövő rádiós kommunikációra. Alkalmazási területe a kommunikációs kapcsolatok létrehozásához szükséges adatcsere (például bonyolultabb, magasabb szintű kapcsolatok, WiFi,

[6] Lásd: http://www.gsmarena.com/google_pixel_xl-8345.php (utolsó letöltés: 2016. október 8.)
[7] Lásd: http://www.oldmobil.hu/cikkek/gsm-story (utolsó letöltés: 2016. október 8.)
[8] Lásd: http://www.inczedy.hu/~hupi/214a/wifi_alapok.pdf (utolsó letöltés: 2016. október 8.)
[9] Lásd: http://www.macmagazin.hu/igymukodikabluetooth/ (utolsó letöltés: 2016. október 8.)
[10] Lásd: http://www.hiradastechnika.hu/data/upload/file/2008/2008_8/HT8_4Takacs.pdf (utolsó letöltés: 2016. október 8.)

Bluetooth, beállítási adatai) gyorsítása, valamint az eszközök közötti azonosítási folyamat (például mobiltelefon – headset) gyorsítása, elvégzése. Az NFC nagyon alacsony sebességű adatátvitelt tesz lehetővé, de a kapcsolat extrém gyorsan jön létre két NFC kompatibilis eszköz között, ezért az NFC kiválóan alkalmas WiFi és Bluetooth eszközök gyors összekapcsolására, párosítására, kiváltva a lassú, nehézkes azonosítási folyamatot. Ebben az esetben az NFC kapcsolat csak a kapcsolat létrehozásában tölt be szerepet, a későbbiekben a kommunikáció, adatcsere már a gyorsabb adatátvitelt biztosító kapcsolaton (WiFi, Bluetooth) történik.

GPS: Az okostelefonok egyik kiemelkedő tulajdonsága a globális helyzetmeghatározó hálózat használata. Ez a funkció a legtöbb okos mobileszközben megtalálható. A műszergyártók készítenek GPS vevőket, illetve GPS+GLONASS vevőket, de egyetlen gyártó sem állít elő „csak GLONASS[11]" vevőt. Azt is tudjuk, hogy a geodéziában elvárt nagy pontosság eléréséhez (az RTK fix pozícióhoz) egy GPS+GLONASS vevőnek – gyártótól és vevőtípustól függően – minimum 3, 4 vagy 5 GPS műhold jeleit mindenképpen fel kell dolgoznia akkor is, ha emellett „lát" 6-8 GLONASS műholdat is. A magyarázat a GPS és a GLONASS rendszer működési módja közötti különbségben keresendő. A GLONASS frekvencia felosztású (FDMA), míg a GPS kód felosztású (CDMA) többszörös hozzáférésű rendszer. Leegyszerűsítve ez azt jelenti, hogy a GPS rendszer esetében mindegyik műhold azonos frekvencián sugároz holdanként más-más kódot (CDMA), míg a GLONASS esetében a kód azonos, viszont a frekvencia minden műhold esetében más (FDMA).

- A GPS kódfelosztású rendszer, mely azt jelenti, hogy azonos frekvencián ad mindegyik műhold, de más kódon
- GLONASS frekvencia felosztású, azaz a kódok azonosak műholdanként, de a frekvenciák mások.[12]

A helymegatározás kockázatai inkább közvetettek, mivel ezek az információk csak akkor válnak értékessé a támadók számára, ha valamilyen összefüggésben vannak más személyes vagy egyéb információval.

SATELITPHONE TECHNOLÓGIA:[13] Már a múlt században felmerült az igény a cellahálózattól függetlenül működő készülékre. A műholdas telefonok nem váltak annyira elterjedtté, mint hagyományos társaik, amelynek oka elsősorban a magas költségekkel indokolható. Ennek ellenére megvolt a saját piaca, hiszen a mobilhálózat nem terjedt ki a világ minden részére. A leginkább használt területe azok a civilizációtól távoli területek, ahol csak a műholdas kapcsolat volt elérhető. Ez a funkció ma is elérhető akár úgy is, hogy az okostelefonhoz egy műholdas kommmunikációra képes tokot[14] erősítünk, így nem csak a hálózaton belül használható, de a költségek ma is hasonlóan magasak a hagyományos okoseszközökhöz képest. De ennek a szabványnak is vannak hátrányai. Nem lehet fedett helyen használni, csak jelerősítővel illetve olyan árkokban, szakadékokban, ahonnan a földközeli műhold már nem érzékeli a jelet.

A műholdas rendszerek technológiáját tekintve két típusba sorolhatjuk a szolgáltatókat. Az első csoportba, a Low Earth Orbit (LEO) pályán keringő, nagyobb számú műholdat üzemeltető Iridium és Globalstart szolgáltatók sorolhatók, míg a másik csoportba a Geosynchronous Orbit (GEO), magasabb pályán keringő, kevesebb számú műholdat működtető Thuraya és Inmarsat szolgáltatók tartoznak.

LEO: A LEO rendszerek előnye, hogy az alacsonyabban keringő műholdak miatt a hálózati kapcsolódás általában gyorsabb, a hang késleltetése minimális (a jelnek kisebb utat kell megtennie), illetve az Iridiumnak köszönhetően megoldott a Föld teljes, 100%-os lefedettsége.

[11] Lásd: http://geomentor.hu/glonass_kalibralas (utolsó letöltés: 2016. október 8.)

[12] Lásd: http://www.zerge.info/GLONASS_es_GPS (utolsó letöltés: 2016. október 8.)

[13] Lázár János – Zautasvili Péter: Műholdas telefonok és mobil műholdas megoldások Kommunikáció 2010 o.243. Elérthetőség: http://193.224.76.4/download/hirado/kiadvanyok/konf2010.pdf (utolsó letöltés: 2016. október 10.)

[14] Műholdon is működik az iPhone. Elérhetőség: http://www.origo.hu/techbazis/20130322-egy-tok-segitsegevel-muholdas-telefonkent-mukodik-az-iphone.html (utolsó letöltés: 2016. október 8.)

GEO: A GEO rendszerek előnye a gyorsabb adatátviteli sebesség biztosítása, ami internetezésnél, TV közvetítésnél, egyéb típusú adatkommunikációnál előny, továbbá ha egyszer sikerült hálózati kapcsolatot létesítnünk, akkor sokkal kisebb az esélye a kapcsolat bontásnak, megszakadásnak.[15]

Ennek a kommunikációs szabványnak fontos tulajdonsága hogy nem kötődik egy ország szolgáltatóihoz, hanem külön globális szolgáltatók biztosítják a kommunikáció lehetőségét a felhasználóknak. A másik fontos tényező hogy a felhasználók viszonylag szűk köre miatt a támadás esélye is kisebb más szabványokhoz képest.

4. Az operációs rendszerek összehasonlítása

Az egyes operációs rendszerek eltérő biztonsági kockázatot rejtenek. A fejezet bemutatja a három legjobban elterjedt operációs rendszert, illetve ismerteti azokat a kockázatokat, amelyeket magukban hordoznak, továbbá javaslatot fogalmaz meg az ellenük történő védekezésre. Az operációs rendszerek egy nagy csoportjának Linux rendszer az alapja. Bár maga a Linux is készített operációs rendszert okos telefonokra, de a későbbiekben már csak mint kiindulópont volt a szoftverfejlesztés folyamatában. A Linuxon alapuló operációs rendszerek közül a legismertebb és elterjedtebb az **Android OS**,[16] amelyet a Google fejlesztett ki és használ a saját márkás (NEXUS) okoseszközein. A Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve Android 1.0 platform néven került kiadásra Apache licenc alatt. Elég nagy számban készültek változatai, a különböző gyártók saját verziókat fejlesztettek a saját készülékükre optimalizálva azt. Az Android előnye, hogy mindenféle árkategóriában vannak készülékek, fájlból is lehet telepíteni programokat, maximálisan testre szabható, rengeteg Google szolgáltatás létezik, melyet alapból ismer. A hátrányait tekintve meg kell említenünk a fragmentációt. A készülékek eltérő képességei miatt az Android sok modell-változata működik egy időben. Ezek összehangolása a különböző alkalmazásokkal nagyon nehezen megy, így előfordul, hogy egyes alkalmazások nem indulnak el bizonyos eszközökön. Egy másik hátránya, hogy bizonyos alkalmazások csak egy meghatározott konfiguráció esetén működnek. Hátrányként említhető még az, hogy nehezebb optimalizálni az operációs rendszert a sokfajta hardverre. Mivel az Android operációs rendszer a legelterjedtebb a világon, így a legnagyobb számban ezt támadják. Ehhez az is hozzájárul, hogy az alkalmazásokat csak felületesen elemzik biztonsági szempontból. Így a hivatalos Play webáruházból letöltött alkalmazás is lehet rosszindulatú.

Az **iOS** az iPhone és iPad operációs rendszere, amit az OS X-ből készítettek. Kezdetben csak saját alkalmazásai futottak rajta, később váltak elérhetővé más gyártók által készített alkalmazások iOS kompatibilis verziói. Ma már előnyei között említhetjük az alkalmazások nagy választékát. A biztonsági szempontot szintén az előnyökhöz sorolhatjuk, ugyanis minden App Store-ba kerülő alkalmazást ellenőriznek. További előnye, hogy a jól optimalizált szoftver hatására az eszközök nagy hatékonysággal képesek működni. A sok kiegészítő, amely elérhető hozzájuk, tovább növeli a használhatóságukat.

Azonban hátrányokkal is rendelkeznek az Apple termékek. Elsősorban a drága készülékek jelentik az első korlátot az eszközök terjedésében. Ehhez kapcsolódik a korlátozott testreszabhatóság is, amellyel szintén szűkül a felhasználó mozgástere. Szinte csak az iTunes szolgáltatásait lehet használni, a bluetooth használhatósága korlátozott. Meg kell említeni, hogy a biztonságos alkalmazások csak akkor azok, ha a hivatalos forrásból szerezzük be. Több gyártó is kínál olyan programokat, amellyel feloldhatjuk (jailbreak) az iOS korlátozásait és nem hivatalos helyről is letölthetjük az alkalmazásokat vagy hozzáférhetünk az operációs rendszerhez. Ezek az eljárások több kockázatot is magukkal vonnak.

[15] Lásd: http://www.satellitephone.hu/muholdas-telefon-muholdas-rendszerek (utolsó letöltés: 2016. október 10.)
[16] Lásd: http://www.openhandsetalliance.com/android_overview.html (utolsó letöltés: 2016. október 7.)

A Windows operációs rendszere nem csak okos mobileszközökre készült, ezt az előnyei közé sorolhatjuk. Az erős integráció Microsoft környezetben sok előnnyel jár úgy, mint a Microsoft szolgáltatások (Skydrive, Bing, Bingmaps, Web Office, Skype, OneDrive, e-mail), Microsoft fejlesztői eszközök (c#, .Net, Silverlight) és a szintén ellenőrzött alkalmazások, mindezt azzal fokozva, hogy az alkalmazások bármelyik készüléken működnek. Azonban itt is találkozunk a hátrányokkal. A drága készülékek mellett ugyan azt a felületet találjuk mindegyik telefonon és tableten, de ez korlátozottan testreszabható, a programok nem tudnak a rendszerbe beleépülni, valamint kevés program érhető el. Emellett a rosszindulatú programok ugyanúgy veszélyeztetik, mint az asztali gépeket, hiszen ugyanaz a Windows program fut rajtuk.

5. Malwarek és az okos mobileszközök

Az okos mobileszközök napjainkra komplett számítógépként funkcionálnak. Mint ilyenek, számos rosszindulatú program veszélyezteti szabályos működésüket, amelyek igen komoly következményekkel lehetnek életünkre. A vírusokat, malwareket, trójaikat a köznyelv sok esetben egymás szinonimájaként használja. Először is, tisztáznunk szükséges ezeket a fogalmakat; ennek alapjául Kovács Attila által összegyűjtött definíciókat vesszük alapul.[17]

Az angol malware kifejezés az angol malicious software (rosszindulatú szoftver, káros szoftver, kártékony szoftver) összevonásából kialakított mozaikszó. A malware-nek nevezzük a rosszindulatú szoftvereket, amelyeknek célja, hogy kárt okozzon a számítógépben (okos mobil eszközben), információkat gyűjtsön, amelynek során hozzáférhetnek kényes adatokhoz stb. A malware magába foglalja a vírusok, trójai programok, rootkit-ek, férgek, keylogger-ek, spyware-ek, adware-ek és minden más elképzelhető kártevő fogalmát. Azt hihetnénk, hogy a vírusok a legelterjedtebb malwarek, azonban a leggyakoribb kártevőnek a trójaik és a férgek számítanak.

Vírus alatt olyan rosszindulatú programot értünk, amely képes sokszorosítani és terjeszteni magát, az egyik gépről a másikra. Ugyanez a féregre is igaz, azzal a különbséggel, hogy a vírus általában „befúrja" magát egy futtatható fájlba, hogy teljesítse a célját. Ha a fertőzött futtatható fájl fut, akkor képes átterjedni egy másik futtatható fájlra. Tehát ahhoz, hogy egy vírus terjedni tudjon, általában szükség van valamilyen felhasználói beavatkozásra is. A vírusok manapság jellemzően pendrive vagy e-mail segítségével terjednek, az internetes böngészés mellett, valamint a megbízhatatlan oldalakról történő letöltések által. Bár a vírusok lehetnek kártékonyak (például adatokat semmisítenek meg), a vírusok bizonyos fajtái azonban csupán zavaróak. Némely vírus késleltetve fejti csak ki hatását, például csak egy bizonyos számú gazdaprogram megfertőzése után. A vírusok kártékony hatásának legenyhébbje az ellenőrizetlen reprodukciójuk, mely túlterhelheti az eszköz erőforrásait, lelassítja a gép működését, elfogyasztja a szabad helyet a merevlemezen. Súlyosabb, ha a vírus fontos fájlokat töröl a gépről, akár az operációs rendszert megbénítva, hasonlóképp törölhet célzottan dokumentumfájlokat, videofájlokat, programokat. A legsúlyosabb kár a merevlemez teljes tartalmának megsemmisítése vagy elérhetetlenné tétele vagy az eszköz valamelyik elektronikus alkatrészének szélsőséges túlterhelése révén műszaki meghibásodás, sérülés előidézése.

Ahogy az okos mobil eszközök esetében is végeztünk történeti áttekintést, úgy a mobileszközre írt vírusok esetében is célszerű ezt megtenni. Már a kétezres évek elején terjedtek rémhírek, amelyek a telefon tönkretételével és új mobil vásárlásával riogattak, ha egy „Ace" jelzésű bejövő hívást fogadunk, az első mobil vírus megjelenéséig azonban 2004-ig kellett várnunk. Az első bluetooth-os mobilvírus megjelenésével egy újabb, addig áthatolhatatlannak hitt falat döntöttek le a vírusírók. Az első valódi mobilvírus, a Cabir, mely a Symbian operációs rendszert használó telefonokra jelentett veszélyt. A Cabir ugyan csak egy úgynevezett proof-of-concept (kísérleti) kártevő volt, mégis

[17] Kovács Attila: Számítógépvírusok és kémprogramok, In. Kovacsattila.info, Elérhetőség: https://kovacsattila.info/szamitogepvirusok-es-kemprogramok.htm (utolsó letöltés: 2022. március 9.)

mindenkit megdöbbentett, hogy a gyakorlatban is működött a terjedési módszere: bluetooth vezeték nélküli hálózati technológia segítségével a fertőzött készülék pár méteres közelében lévő mobiltelefonokra küldte szét magát a féreg – hasonlóan egy náthához vagy más fertőzéshez, amely csak a közelben lévő embereket fertőzi meg. A Cabirból számos változat jelent meg néhány hónap alatt, sőt, 2004 decemberében a forráskódja is nyilvánosságra került, ezért nehéz felmérni, hogy hány újabb variáns, illetve az eredeti kódra épülő „új" kártevő látott napvilágot. Egy hónap elteltével egy újabb platform lett támadás célpontja: a Duts nevű vírus Microsoft Pocket PC operációs rendszerrel ellátott PDA-kat fertőzött meg – hozzáfűzte magát minden .exe kiterjesztésű fájlhoz. Ez szintén egy proof-of-concept kártevő volt, azonban csak néhány hétnek kellett eltelnie az első valódi, PDA-kat fertőző trójai és hátsóajtó megjelenésére: a Bradorral fertőzött kéziszámítógépek felett a támadó távolról is átvehette a teljes irányítást. Augusztusban mobiltelefonokra is megérkezett az első trójai: a Mos nevű kártevő egy Symbianos játéknak álcázta magát, valójában azonban emelt díjas SMS-eket küldözgetett. Novemberben pedig megjelent a szintén sok variánst megélt Skulls trójai, mely nevéhez híven koponyákat jelenített meg a képernyőn, és felülírta a telefonban található segédprogramokat, így a telefonálás kivételével gyakorlatilag teljesen használhatatlanná téve a készüléket. 2005 márciusa óta az MMS-képes okostelefonok tulajdonosai sincsenek biztonságban: a Commwarrior névre keresztelt vírus Symbian Series 60 operációs rendszert futtató Nokia készülékeket képes megfertőzni.

A rosszindulatú alkalmazások egy másik típusát az úgynevezett trójaik jelentik. A trójai egy olyan malware program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az úgynevezett hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a célseszközhöz. A trójai programnak – a megfelelő adminisztrátori jogokkal – korlátlan hozzáférést engedélyez az operációs rendszerhez, amivel a támadó számtalan dolgot végrehajthat, legyen szó rombolásról,[18] eszköz vagy identitás kihasználásáról,[19] pénzlopásról, váltságdíj szerzésről,[20] adatlopásról,[21] kémkedésről, megfigyelésről, tevékenységkövetésről.[22]

A számítógépes féreg (worm) egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. A férgek gyakran a számítógép-hálózatokat használják fel terjedésükhöz. Az önsokszorosításon kívül a féreg sokféle dologra beprogramozható, például a fájlok törlésére a gazdarendszeren, vagy önmaga elküldésére e-mailben. Az újabban megfigyelt férgek több végrehajtható állományt is visznek magukkal. Még valódi ártó szándékú kód nélkül is súlyos fennakadásokat okozhatnak, csupán azzal, hogy sokszorozódásuk kiugróan magas hálózati forgalmat generálhat.

Ahogy a mobiltelefonok egyre inkább a számítógépek funkcióját töltötték be, úgy készültek egyre újabb és újabb rosszindulatú programok. Az Android operációs rendszert használó okos mobil eszközöket fertőző kártékony programok egyre több trükköt vetnek be annak érdekében, hogy mind a detektálásuk, mind a kiirtásuk megnehezedjen. Az első, különösen nehezen irtható, nagyobb hír-

[18] A számítógép vagy eszköz tönkretétele; fájlok, adatok módosítása vagy törlése; további malware programok telepítése, futtatása; kémkedés a felhasználó tevékenysége és érzékeny adatai után.

[19] A megfertőzött célszemély internetkapcsolatának használata (mint átjáró vagy proxy) illegális célokra (például további gépek megtámadására), vagy akár a felhasználó adatainak, fájljainak megosztására; a célszemély hálózatát használó többi eszköz feltérképezése, megtámadása; a számítógép használata egy botnet részeként (például automatikus spamelések elvégzésére); aszámítógép erőforrásainak használata kriptovaluta bányászatra (például Bitcoin).

[20] Elektronikus úton történő pénzlopás; ransomware telepítése (például CryptoLocker).

[21] Felhasználó jelszavának, bankkártyaadatainak megszerzése, személyi adatok, privát fényképek eltulajdonítása; piaci titkok felderítése; személyi vagy ipari kémkedés.

[22] Gombleütések rögzítése (például felhasználó adatok, jelszavak lopásához); felhasználó képernyőjének megfigyelése; felhasználó webkameraképének megfigyelése, az informatikai eszköz távvezérlése.

verést kapott androidos károkozó a DKFBootKit volt, amelyet az NQ Mobile kutatói lepleztek le még 2012-ben. Ez a kártékony program azzal hívta fel magára figyelmet, hogy még azelőtt képes volt betöltődni a memóriába, mielőtt még az Android vagy akár a mobilbiztonsági szoftverek elindultak volna. Emellett számos rendszeralkalmazást is módosított, és ha ezeket sikerült is megszabadítani a fertőzéstől, attól még a károkozó életképes maradt. A DKFBootKit egy kernelszintű bootkit komponenssel rendelkezett, amivel jelentősen megnehezítette a teljes körű eltávolítását.

A mobilvírusok terjedése sok esetben rendkívül trükkös lehet. 2016 februárjában fedeztek fel biztonsági szakértők a Google Play áruházból letölthető alkalmazásokat, amelyek esetében a játék nem tartalmazott ártalmas kódokat, azonban egy programfrissítés során a felhasználó eszközére utólag töltött le képeket, amelyekben ott rejlett az ártalmas kód. A szakirodalom ezt az eljárás nevezi szteganográfiának. Az eljárás lényege, hogy olyan rejtett üzeneteket hoznak létre, amelyben az üzenet létezéséről csak a külső és a fogadó oldal tud, de bárki más számára az üzenet láthatatlan, az eredeti tartalom csak egy rejtjel segítségével válik újra láthatóvá. A fő eltérés a kriptográfiától, hogy ez esetben nem magát az üzenetet rejtjük el, hanem magának az üzenetnek a létét.[23] A támadók ezt az eljárást használták fel, annyi eltéréssel, hogy az elrejtett üzenet egy kártékony kódot tartalmazott, a felhasználó nem észlelte ebből, hogy nem az általa letölteni vélt képet kapta meg, legfeljebb „zajt" észlelhetett, de laikusként jó eséllyel hibás képpontnak értelmezne. Ezek a hibás képpontok azonban olyan kártékony kódok voltak, amit az alkalmazás kibontott és futtatott titokban, így szerezve hozzáférést például a telefon azonosítójához, IMEI számához, de akár a felhasználó személyes adataihoz is.[24]

A mobileszközöket fenyegető egyik legkomolyabb rosszindulatú programnak a ransomware tekinthető, ami fenyegetéssel próbál pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszi a számítógépet/mobil eszközt, vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, aminek a hatására visszaállítja az eredeti állapotot.

A ransomware-ekről, illetve a rosszindulatú programokkal szembeni védekezésről, a kártevők mobileszközökről való kiirtásával ebben a fejezetben bővebben nem foglalkozunk, ugyanis a mobileszközöket fenyegető, új típusú biztonsági kihívásokat bemutató tananyag részletesen vizsgálja ezeket a kérdéseket.

6. A jelentősebb gyártók gazdasági potenciálja

Az okos mobileszközök számának folyamatos bővülése óriási piaci harcot eredményez a gyártók között. A stratégia, amelyet az egyes gyártók a profitmaximalizálás érdekében választanak, nagyban befolyásolja az okos mobil eszközöknek a jövőjét, illetve azokat a kockázatokat, amelyeket jelentenek. A konkrét mobil eszközök gyártói itt csupán az egyik vizsgálandó szereplők, ugyanúgy jelentőséggel bírnak a szoftverek piacán érdekelt gyártók, amelyek között adott esetben akár átjárás is lehetséges.

2016. második negyedévében összesen 344 millió okostelefont értékesítettek világszerte (lásd 3. számú táblázat).[25]

[23] Bertók Zsófia: Szteganográfia, In. Elérhetőség: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2010/HF-reports/BertokZsofia.pdf (2016. szeptember 10.)

[24] Rátfai Gábor- Bátky Zoltán: Képekbe rejtett vírusok garázdálkodnak Androidon, In. 24.hu, 2016. február 2., Elérhetőség: http://24.hu/mobil/2016/02/03/kepekbe-rejtett-virusok-garazdalkodnak-androidon/ (2016. szeptember 10.)

[25] Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016, In. Press Release, 2016. augusztus 19., Elérhetőség: http://www.gartner.com/newsroom/id/3415117 (2016. szeptember 5.)

Gyártó	2016 Q2 (millió eladott telefon darab)	2016 Q2 (piaci részesdés %-ban)	2015 Q2 (millió eladott telefon darab)	2015 Q2 (piaci részesdés %-ban)
Samsung	76. 743,5	22,3	72. 072,5	21,8
Apple	44. 395,0	12,9	48. 085,5	14,6
Huawei	30. 670,7	8,9	26. 454,4	8,0
Oppo	18. 489,6	5,4	8. 073,8	2,4
Xiaomi	15. 530,7	4,5	15. 464,5	4,7
Egyéb	158. 530,3	46,0	160. 162,1	48,5
Összesen	**344. 359,7**	**100,0**	**330. 312,9**	**100,0**

3. táblázat: Okostelefonok eladási mutatója 2016. második negyedévében
Forrás: Saját szerkesztés, Gartner alapján

A táblázatból kiolvasható, hogy a Samsung egyértelműen uralja az eladásokat; 2015 hasonló időszakához képest 22,3%-kal volt képes növelni az eladott mobiltelefonok számát. A Samsung közel kétszer annyi telefont értékesített, mint a másodiknak tekinthető Apple. Szintén jelentős gyártónak mondhatók egyes kínai gyártók, mint a Huawei, az Oppo vagy a Xiaomi. Ez az öt vállalat a teljes piac több mint 50%-át lefedi. A listáról hiányoznak az egy évtizede olyan klasszikusnak számító nevek, mint a Nokia, a Motorola vagy az Ericson, annak ellenére, hogy – mint az okostelefonok evolúciójával foglalkozó fejezetben láthattuk – a Nokia élen járt azokban a fejlesztésekben, amelyek okoseszközök kialakulásához vezettek.

2006-ban a Nokia messze a legnagyobb gyártónak számított a maga 35 százalékos részesedésével, a nagy riválisnak pedig a Motorola volt tekinthető 20 százalékos piaci résszel. Úgy tűnt, semmi nem mozdíthatja ki a Nokiát vezető szerepéből, de jött az Apple és Steve Jobs, így a 2007 januárjában bemutatott iPhone alig fél évvel később a mobilpiac alapjait változtatta meg. A legszembetűnőbb változás, hogy megváltozott az elemzők és a kritikusok hozzáállása az okostelefonokhoz – szerették az iPhone-t. Nagyon sok tényező játszott közre ebben, de tagadhatatlan, hogy az egyik legfontosabb a marketing szerepe volt, amelyben a Nokia nem vehette fel a versenyt az Apple-lel. Nem arról volt szó, hogy az iPhone volt a legjobb telefon a piacon, hiszen az Apple azóta számtalan nagyon fontos vagy kritikus technikai fejlesztést hajtott végre az eredeti iPhone-hoz képest. A Nokia N95-nek számtalan olyan tulajdonsága volt, ami messze jobbnak számított, mint az iPhone, de ez senkit nem érdekelt. Az iPhone volt a legjobb okostelefon, mert Steve Jobs azt mondta, pedig az iPhone 2G még csak okostelefonnak sem volt mondható a szó szoros értelmében (elég csak a flash hiányára, multitaskingra és még néhány fájó hiányosságra emlékezni), valamint rendkívül drága is volt. De mindezek ellenére nagyon felhasználóbarát kezelőfelülettel és érintőkijelzővel rendelkezett. A Nokia visszaszorulását a mobilvilág megváltozása okozta, illetve az a tény, hogy a Nokia ehhez nem tudott alkalmazkodni. Az első hiba a kommunikáció volt. Az Apple tipikusan amerikai cégként hype-olta termékeit, nagyon ügyes marketing-gépezetet épített fel az évek során, és az iPhone-nál ezt ki is tudta használni, elhitette az emberekkel, hogy ez a legjobb telefon. A Nokia pedig tipikus finn cégként nyitott és őszinte vállalatként működött, ami nagyon jól működött az iPhone előtti korszakban, amikor a riválisok is hasonlóan gondolkodtak és ragaszkodtak a tényekhez. Az iPhone 4-ben például több olyan feature-t bemutattak, melyek a Nokia mobilokban már 2007-ben is megvoltak, ennek ellenére mindenki az Apple innovációiról beszélt. A másik fontos tényező, hogy a Nokia nem háborúzni akart a riválisokkal, mint az Apple tette mindenki ellen, hanem együttműködni velük – lásd a Symbianos együttműködést. De a következő időkben a *mindenki mindenki ellen* elv érvényesült. Ráadásul az Apple az összes addigi iparági standardot megváltoztatta, ezt sem értették a Nokiánál. Minden megváltozott, és a Nokia a mai napig nem tudott alkalmazkodni az új szabályokhoz. Ráadásul a két cég nem is igazán riválisa egymásnak, az Apple soha nem fogja magának tudni a piac harmadát, mindig is a prémium kategóriában marad. A Nokia igazi ellenfele így nem is az Apple volt, hanem a többi

gyártó (Samsung, LG, Sony Ericsson, HTC), akik mind előbb alkalmazkodtak és kezdtek el iPhone-riválisokat gyártani. Emellett alsóbb kategóriákban is olyan szereplők léptek színre, akik valóban riválisaik lettek a Nokiának. Ázsiában felbukkantak olyan gyártók, melyek sokkal olcsóbban állítanak elő hasonló minőségű mobilokat, mint a Nokia. Ezekkel a mobilokkal elárasztották a piacot, ha nem is Európában és Amerikában, de a világ többi részén a vásárlókat nem érdekli, hogy az olcsó mobilnak milyen a márkája, a lényeg, hogy megbízhatóan működjön.

Ebben a helyzetben lépett színre a Google operációs rendszere, az Android. A Google teljesen más stratégiát követett, mint az Apple, nem saját készüléket gyártott – bár arra vonatkozóan is volt több kísérlete –, hanem operációs rendszert. A modell lényege abban állt, hogy ők adják a rendszert, a gyártók a hardvert, és a kettőből kijön egy működő okostelefon. Az androidos mobilok is a prémium szegmensben kezdték, így eleinte még úgy tűnhetett a Nokiának, hogy még sokáig nem veszélyeztetik a középkategóriás piacukat. Ezzel szemben nagyon gyorsan megjelentek az olcsó androidos készülékek, az okostelefon-kategória már nem elérhetetlen a mobilra kevesebbet költők számára sem, nagyon széles rétegeknek elérhetővé vált. Az Androidnak köszönhetően sok olyan gyártó is jelentős piaci részt szerzett, melyek csak okostelefonokat gyártanak. A Nokia 2011-ben úgy döntött, hogy az elavult Symbiant leváltja és így megjelent az első Windowsos mobil, a Lumia 800. A Lumia sorozattal a Nokia jelentősége és piaci részesedése alaposan visszaesett, ami a Microsoft Nokia mobilos részlegének felvásárlásával zárult 2013-ban. Akkor egy rövid ideig úgy tűnt, hogy főleg Redmond járt jól az üzlettel, de jelenleg úgy tűnik, a Nokia az, amelyik sokkal jobb állapotban várja, hogy újra releváns szereplője legyen a mobilpiacnak. De nem a Nokia az egyetlen szereplő, amelyik hasonló utat járt be, a tanulmány írásának idején jelentette be a Blackberry is, hogy a mobiltelefon gyártást beszünteti.

Az alacsonyabb árkategóriát megcélzó gyártók esetében több olyan tényező is kimutatható, amelyek igen komolyan érinthetik mind a telefonunk, mind az adataink, adott esetben egészségünk védelmét. A biztonsági kockázatokról egy másik soron következő tananyag foglalkozik, itt csupán annyit szükséges megemlítenünk, hogy számos kínai gyártó esetében bizonytalan a mobil alkatrészek eredete, több esetben kiderült, a gyártás vagy a kereskedelmi forgalmazás során már kémprogramokat telepítenek az eszközökre. Erre szolgálhat példaként egy 2015-ös történet, amelyben a Lenovo laptopok[26] esetében fedezték fel, hogy a gyártó olyan hirdetéskezelő rendszert és gyökérszintű tanúsítványt telepített a számítógépeire, amely a webes forgalom monitorozására, de akár támadások lebonyolítására is alkalmas lehet.[27] A Superfish nevű programot felhasználói panaszok hatására eltávolították. Az eset során olyan képernyőmentések is készültek, amelyben egy tanúsítvány úgy tett, mintha a kibocsátója a Bank of America lenne. A Superfish gyárilag rajta volt a rendszereken, és alapvetően nem is ártó szándékú, csupán arra akarták használni, hogy a Google keresési eredményei közt másoktól származó hirdetések is megjelenjenek. A laptopgyártó azzal védte meg a szoftvert, hogy az képekkel segíti a termékek megtalálását. Emellett a vevők a laptop beüzemelése során elutasíthatják a használati feltételeket, hogy ne települjön a szoftver. Figyelembe véve, hogy az átlag felhasználó telepítéskor mindent elfogad anélkül, hogy elolvasná, nem nevezhető a legkorrektebb eljárásnak. A Superfish úgynevezett közbeékelődéses (man-in-the-middle) támadást használt, amivel belenyúlt a felhasználó webes adatforgalmába. Ilyenkor mindkét fél azt hiszi, hogy közvetlenül egymással kommunikálnak, pedig mindketten csak a csatornát irányító rejtett szereplővel állnak kapcsolatban. Nem véletlen, hogy a Superfish szoftverét a vírusirtók veszélyes alkalmazásként azonosítják, és az eltávolítását javasolják. A Lenovót képviselő PR-ügynökség reakciójában azt írta, hogy október és december között szállított notebookokon rajta volt a Superfish. Hozzátették, hogy alaposan megvizsgálták a technológiát, és nem találtak arra bizonyítékot, ami egyértelműen alátámasztaná a biztonsági problémát, de a felhasználói aggályok miatt léptek. Azóta teljes mértékben eltávolították

[26] Az eljárás természetesen érvényes lehet az okos mobil eszközökre is.

[27] Williams, Owen: Lenovo caught installing adware on new computers, In. The Next Web, 2015. február 19., Elérhetőség: http://thenextweb.com/insider/2015/02/19/lenovo-caught-installing-adware-new-computers/ ((utolsó letöltés: 2016. szeptember 7.)

a szerver-oldali interakciókat minden Lenovo termékről, így az minden terméken le van tiltva, illetve nem telepítik előre a szoftvert a notebookokon, és ezt a jövőben sem tervezik.

Szintén 2015-ben több mint húsz különböző típusú kínai okostelefonon találtak előre telepített kémprogramokat.[28] Ezek közé tartoztak többek között Lenovo, a Xiaomi és a Huawei készülékei, de kémprogramokat felfedező, G Data vírusvédelmi cég szakértői szerint nem a gyártók, hanem valószínűleg a kereskedők telepítették a kártevőket a Németországban forgalomba kerülő készülékekre. A kémprogramok jellemzően a Facebook vagy a Google Drive alkalmazások egyikébe voltak elrejtve. A manipulált alkalmazások teljesen úgy működnek, mint az eredetiek. A kártevőt tartalmazó Facebook alkalmazásnál például minden funkció elérhető, a felhasználó nem vesz észre semmit abból, hogy az alkalmazásban elrejtett kémprogram hátsó ajtót nyitott a mobilján a támadók számára, akik így hozzáférhetnek az összes adatához. Az alkalmazás pedig nem kér engedélyeket, mivel már minden szükséges engedélyt megkapott a telepítésekor. A felhasználó így kizárólag akkor veszi észre, hogy a telefonja fertőzött, ha telepít valamilyen biztonsági alkalmazást, amelynek során a biztonsági program jelzi a fertőzött állományt. A megtisztítás azonban gyakran nem lehetséges, mivel a kártevő bele van égetve a telefon gyári meghajtóprogramjába (firmware-jébe). Ilyen esetben a vásárlónak fel kell vennie a kapcsolatot a mobilkészülék gyártójával. A kártevőt tartalmazó hamis Facebook-alkalmazás rendkívül sok funkcióhoz szerezhet hozzáférést. A korábban ismertetett hozzáférési engedélyek mellett a támadók belehallgathatnak a telefonhívásokba és rögzíthetik azokat, vásárlásokat indíthatnak vagy emelt díjas számokat hívhatnak.

A Kínában gyártott informatikai eszközök, beleértve az okos mobil eszközöket is, komoly aggodalmakat szülnek a nemzetbiztonsági területen dolgozók számára. 2012-ben az Egyesült Államok két kínai telekommunikációs cég, a Huawei és a ZTE kitiltását tervezte az amerikai piacról, ugyanis megítélésük szerint nemzetbiztonsági kockázatot jelentenek az által, hogy az érintett cégeknél túlságosan nagy a kínai állam befolyása. Az amerikai Védelmi Minisztériumnak a kínai haderőről a Kongresszus számára készített éves jelentése szerint a Huawei technológiája olyan „hátsó kapukat” tartalmaz, amely a kínai hadsereg számára lehallgatási lehetőséget biztosít az amerikai telekommunikációs hálózaton belül.

A nem megbízható forrásból származó alkatrészek kockázatai többek között azt is magukban foglalják, hogy olyan anyagokat tartalmazhatnak, amelyek károsak az egészségére, a megengedettnél magasabb a károsanyag kibocsátásuk vagy a nem megfelelő technika miatt túlmelegszik, felrobban. Ez utóbbi a nagy gyártókat is fenyegeti, a Samsung csúcskat0egóriás Note 7 telefonja esetében alig két héttel a megjelenést követően jelentették be, hogy robbanásveszély miatt visszavonják és kicserélik az összes mobiltelefont.

Ahogy említettük, a hardver mellett igen fontos a szoftverek piaca is. A már idézett kutatás az Android egyértelmű dominanciáját mutatja (lásd 4. számú táblázat), a 2016 második negyedévben eladott eszközök 86,2%-án Androidos operációs rendszer található, ami egy év alatt 4%-os növekedést jelent.

Operációs rendszer	2016 Q2 (millió eladott telefon darab)	2016 Q2 (piaci részesdés %-ban)	2015 Q2 (millió eladott telefon darab)	2015 Q2 (piaci részesdés %-ban)
Android	296.912,8	86,2	271.647	82,2
iOs	44.395	12,9	48.085,5	14,6
Windows	1.971	0,6	8.198,2	2,5
Blackberry	400,4	0,1	1.153,2	0,3
Egyéb	680,6	0,2	1.229	0,4
Összesen	**344.359,7**	**100,0**	**330.312,9**	**100,0**

4. táblázat Forgalmazott okostelefonok operációs rendszere 2016. második negyedévében
Forrás: Saját szerkesztés, Gartner alapján

[28] Khandelwal, Swati: 26 Android Phone Models Shipped with Pre-Installed Spyware, In. The Hacker News, 2015. szeptember 3., Elérhetőség: http://thehackernews.com/2015/09/android-smartphone-malware.html (2016. szeptember 7.)

Az operációs rendszer különösen fontos egy mobileszköz biztonságát illetően, ugyanis eltérő többek között, hogy a ráoptimalizált alkalmazások milyen biztonsági szűrőt alkalmaznak, milyen mértékben vannak kitéve rosszindulatú alkalmazásoknak stb.

7. Az okos mobileszközök jövőképe

Előrejelzések szerint az okos mobileszközök száma pár éven belül meghaladja a 10 milliárd készüléket. Ez azonban egyúttal olyan evolúciós versenyt is eredményez, amely alapjaiban alakíthatja át az okos mobil eszközök funkcióját. Várhatóan a következő nagy újítás, ami mind a számítógépek, mind az okos mobil eszközök piacán bekövetkezik, a kiterjesztett[29] és/vagy virtuális[30] valóság egyre magasabb szintű integrálása az eszközökre, amelyek egy teljesen új felhasználói élményt jelentenek majd.

A mobil sávszélesség növekedése tovább fokozza a mobil eszközökkel kapcsolatos függőségünket. Az eszközök rendszeres használata egyre több és több adatot generál a felhasználókról, amelyek feldolgozása, releváns információvá történő átalakítása mesterséges intelligencia segítségével fog történni. A mesterséges intelligencia megalkotására történő kísérletek nem tekinthetőek újdonságnak, évek óta zajlanak olyan kutatások, amelyek például segítenek kiszűrni a közösségi médiában közzétett ironikus tartalmakat.[31] A mesterséges intelligencia megjelenése a big data feldolgozásában várhatóan paradigmaváltó jelenség lesz, hiszen megnyitja az utat nem csak az emberi viselkedés, de társadalmi folyamatok előrejelzésének.

8. Felhasznált irodalom

- Bertók Zsófia: Szteganográfia, In. http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2010/HF-reports/BertokZsofia.pdf (2016. szeptember 10.)
- Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016, In. Press Release, 2016. augusztus 19.,
- HuMarc: Okostelefon-evolúció, In. LogOut, 2013. május 15., https://logout.hu/cikk/okostelefon-evolucio/bevezeto.html (2016. szeptember 15.)

[29] A kiterjesztett valóság (angolul augmented reality, AR) a valóság egyfajta virtuális (látszólagos, nem valódi) kibővítése, amikor a mobil kamerájával szétnézve egy adott környéken megjelenik az éppen a kamerában látható boltok nyitvatartása vagy akár az adott irányban levő (éppen nem is látható) üzletek leírása és távolságuk.

[30] Virtuális valóságon (angolul virtual reality, VR) a digitális technikával létrehozott világot, és az általa felkeltett perceptuális élmény egészét értjük. A virtuális valóság úgy is meghatározható, mint olyan számítógéppel létrehozott környezet, amelyben a felhasználó is jelen van. Ezt a technológiát azért hozták létre, hogy az emberek könnyebben kezeljék az információt. A virtuális valóság lehetővé teszi az információ teljesen más szemléletét, melynek egyik jellemzője, a dinamikusság és közvetlenség. A VV szintén eszköz lehet a modellépítésre és a problémamegoldásra és potenciális eszköz a tapasztalva tanulásra. A VR-ben a program használója egy sisakot illeszt a fejére, melynek következtében jobb illetve a bal szem számára digitálisan előállított kép két, a szemhez közvetlen közel elhelyezett képernyőn jelenik meg. A látványon túl a Virtuális Valóságban a hallás, a tapintás, a hely- illetve a helyzetváltoztatás is fontos szerepet kap. A megjelenített tárgyak megközelíthetőek, megfoghatóak, a program felhasználója kölcsönhatásba léphet velük. A Virtuális Valóságra jellemző az immerzivitás (belemerülés), illetve az interaktivitás úgynevezett real time jellege, vagyis a számítógép késedelem nélkül, vagy nagyon kis késéssel "válaszol", ami az azonnali reagálás benyomását kelti a felhasználóban.

[31] Ezzel kapcsolatban például a német Alkotmányvédelmi Hivatal írt ki pályázatot 2013-ban. Bővebben lásd: Zezima, Katie: The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work., In. Washington Post, 2014. június 3., Elérhetőség: http://www.washingtonpost.com/blogs/the-fix/wp/2014/06/03/the-secret-service-wants-software-that-detects-social-media-sarcasm-yeah-sure-it-will-work/ ((utolsó letöltés: 2016. szeptember 7.)

- Khandelwal, Swati: 26 Android Phone Models Shipped with Pre-Installed Spyware, In. The Hacker News, 2015. szeptember 3., http://thehackernews.com/2015/09/android-smartphone-malware.html (2016. szeptember 7.)
- Kovács Attila: Számítógépvírusok és kémprogramok, In. Kovacsattila.info, https://kovacsattila.info/szamitogepvirusok-es-kemprogramok.htm (2022. március 9.)
- Lázár János – Zautasvili Péter: Műholdas telefonok és mobil műholdas megoldások Kommunikáció 2010 o.243. http://193.224.76.4/download/hirado/kiadvanyok/konf2010.pdf (2016. október 2.)
- Műholdon is működik az iPhone url: http://www.origo.hu/techbazis/20130322-egy-tok-segitsegevel-muholdas-telefonkent-mukodik-az-iphone.html (2016. október 27.)
- Rátfai Gábor – Bátky Zoltán: Képekbe rejtett vírusok garázdálkodnak Androidon, In. 24.hu, 2016. február 2., http://24.hu/mobil/2016/02/03/kepekbe-rejtett-virusok-garazdalkodnak-androidon/ (2016. szeptember 10.)
- Williams, Owen: Lenovo caught installing adware on new computers, In. The Next Web, 2015. február 19., http://thenextweb.com/insider/2015/02/19/lenovo-caught-installing-adware-new-computers/ (2016. szeptember 7.)
- Zezima, Katie: The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work., In. Washington Post, 2014. június 3., http://www.washingtonpost.com/blogs/the-fix/wp/2014/06/03/the-secret-service-wants-software-that-detects-social-media-sarcasm-yeah-sure-it-will-work/ (2016. szeptember 7.)

- http://www.gartner.com/newsroom/id/3415117 (2016. szeptember 5.)
- http://geomentor.hu/glonass_kalibralas (2016. október 30.)
- http://pcworld.hu/mobil/amit-az-nfc-rol-tudni-kell-130522.html (2016. október 30.)
- http://privacygrade.org/home (2016. október 27.)
- http://www.gsmarena.com/google_pixel_xl-8345.php (2016. október 27.)
- http://www.hiradastechnika.hu/data/upload/file/2008/2008_8/HT8_4Takacs.pdf (2016. október 27.)
- http://www.inczedy.hu/~hupi/214a/wifi_alapok.pdf (2016. október 27.)
- http://www.macmagazin.hu/igymukodikabluetooth/ (2016. október 28.)
- http://www.oldmobil.hu/cikkek/gsm-story (2016. október 21.)
- http://www.openhandsetalliance.com/android_overview.html (2016. október 27.)
- http://www.openhandsetalliance.com/android_overview.html (2016. október 27.)
- http://www.satellitephone.hu/muholdas-telefon-muholdas-rendszerek (2016. október 27.)
- http://www.zerge.info/GLONASS_es_GPS (2016. október 27.)

II. SZABÓ ANDRÁS: OKOSESZKÖZÖKHÖZ KAPCSOLÓDÓ ADATVÉDELMI KÉRDÉSEK

1. Információbiztonsági és adatvédelmi alapvetés

1.1. Bevezető gondolatok

Az ezredfordulót követően a mobil eszközök világban ugrásszerűen bekövetkező változások új kihívások elé állították a piac és az állam szereplőit. A rohamosan növekvő értékesítési mutatók, a sorozatban megjelenő fejlesztések és az azokat generáló felhasználói igények nemcsak technológia és biztonsági problémákat és azok megoldását, hanem számos szabályozási kérdést is felvetnek mind az állam, mind a szakmai szervezetek részéről. A mobil eszközök piacán az egyik legelterjedtebb és legkeresettebb termék az okostelefon, amely esetén a felmerülő kockázatokat számba véve több szempontot is szükséges figyelembe venni, így:

a) mely korcsoport (gyermek, felnőtt),
b) milyen célból (magán, üzleti),
c) milyen funkciók (alkalmazások)

tekintetében használja az eszközt, amely használat meghatározza a várható fenyegetettséget és az ezzel összefüggő kockázatokat. Emellett az okostelefonoknál eltérő igényekkel kell szembe nézni a készülék és annak hordozhatóságából adódóan az „útközben” felmerülő biztonsági kihívásokkal kapcsolatban.

A használati szokások kapcsán felmerülő és a mobilitásból adódó kockázatokhoz szükséges igazítani a biztonsági intézkedéseket, a lopás, eltulajdonítás elleni védelemtől kezdve a hálózati kapcsolatok és a kényelmi funkciók – részleges vagy átmeneti – tiltásán át, egészen az adatok titkosításáig. Mindemellett olyan alapvető felhasználói magatartásokat is szükséges megjegyezni és alkalmazni mint a PIN-kód rendszeres használata, az IMEI szám feljegyzése, webes felületen a mobilszám megadásának mellőzése, az alkalmazások telepítése előtt azok ellenőrzése, valamint a publikus WiFi hálózatok kerülése. A felelőtlen eszközhasználat komoly problémákat okozhat, amelyek megelőzése érdekében az eszközön meglévő biztonsági beállítások használatával minimális biztonsági intézkedéseket a felhasználó maga is megtehet. Fentiek magatartásokon túl ilyen a helymeghatározó és az adathálózat üzemmód (3G/4G) – átmeneti vagy teljes – kikapcsolása, a QR kódok linkjeinek előzetes ellenőrzése, amellett, hogy tanácsos vírusirtó szoftver feltelepítése okostelefonunkra. Fokozott védelem biztosítható a be- és kimenő adatforgalom szűrésével (WiFi-n és 3G-n) és rendszeres törléssel (mind az internet előzmények, mind az adatok tekintetében).

Ezzel azonban a felhasználó által megtehető – egyszerűbb – intézkedések köre bezárul, a megjelenő kihívások komplex kezelése azonban ezen túlmutat, ezért szükséges a piac és az állam szerepvállalása is. Utóbbi szereplőnek, mint a közhatalom birtokosának legerősebb és legszélesebb körre kiterjedő eszköze a szabályozás. Jelen tananyag célja, hogy mind a nemzeti, mind a nemzetközi jogi környezetet áttekintve kitekintést nyújtson a hatályos jogi normák rendszerére. Az áttekintés azonban nem lehet teljes körű néhány elméleti alapvetés és a fogalmi keretek számbavétele nélkül.

1.2. Alapvetés az adatvédelemhez és az információbiztonsághoz

Az áttekintés első lépése az adatvédelem és az információbiztonság fogalmi alapjainak felvázolása, amely jelentősége abban rejlik, hogy napról napra nő a társadalom tagjainak – legyen az magán- vagy jogi személy – irányába bekövetkezett biztonsági fenyegetések és események száma. Gondoljunk csak az elmúlt időszakban bekövetkezett adatlopások kiemelkedő számára, amely során mind személyes – esetenként különleges személyes –, mind üzleti adatok jogosulatlan megszerzésére került sor, úgy, hogy eközben az adatokat kezelő elektronikus információs rendszerek is sérültek. Ezen események nem csak az adatvédelem fontosságára, hanem az elektronikus információk sebezhetőségére, valamint az elektronikus információs rendszerek kitettségére is rávilágítottak. Az elektronikus információs rendszerekben akár csak átmenetileg bekövetkező működési zavarok, valamint az ezekben kezelt adatok, információk jogosulatlan megszerzése, időszakos kiesése, megsemmisülése, vagy bizalmasságának sérülése jelentős kihatással van a szervezet, a gazdaság, az állam működésére, a társadalom (minden tagjának) életére. Ennek hatására tehát az adatok védelme mellett az azokat tároló és kezelő elektronikus információs rendszerek védelmét is biztosítani kell. De mi a különbség, egyáltalán van-e különbség adat- és információ, adat- és információvédelem, illetve adatbiztonság és információbiztonság között?

E kérdések megválaszolására számtalan megközelítés létezik, megszámlálhatatlan azoknak a szakkönyveknek, szakcikkeknek, tudományos munkának vagy jegyzeteknek a száma, amelyek rávilágítanak e kettő közötti különbségre. Jelen fejezetnek a célja kizárólag gyakorlati szempontból történő rendszertani alapvetés rögzítése, a részletes kifejtés és ismertetés mind célját, témáját és terjedelmét tekintve túlmutat ezen jegyzeten. Anélkül, hogy a legegyszerűbb forrást választva a magyar értelmező kéziszótár meghatározásait számba vennénk általános megközelítés szempontjából vizsgálva alapvetésként rögzíthetjük, hogy az adat az információ hordozója.

Ezen alapvetést elfogadva különbség abban található, hogy az *adat* közlésre, megjelenítésre vagy további feldolgozásra alkalmas entitás, amely számos megjelenési formát vehet fel (például: alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása. Az *információ* valamilyen megfigyelés, tapasztalat vagy ismeret, amely által következtetések vonhatók le és döntések alapjául szolgálhat. Az információ, ha úgy tetszik nem más, mint a jelentéssel felruházott adat, azaz adatból akkor lesz információ, ha valamiről informál.[32]

Az adat és az információ tehát eltérő jelentéstartalommal felruházott fogalmak, amelyek tartalmukat tekintve eltérő védelem és biztonság fogalommal rendelkeznek különösen akkor, ha elfogadjuk azt az alapvetést, hogy védelem az a tevékenység, amely a biztonság állapotának elérésére szolgál. Ezen meghatározásból kiindulva az *adatvédelem* központi eleme az adatkezelés jogszerűségét biztosító – főként szabályozási – tevékenységek, elsősorban a védelmet biztosító szabályok és eljárások, valamint az adatkezelési eszközök és módszerek összessége. Az adatvédelemmel szemben az *adatbiztonság* meghatározása alatt alapvetően az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében.

Az *információvédelem* összetettsége miatt a definíciós meghatározás helyett, azokat a tevékenységeket rögzítjük, amelyekkel maga a védelmi tevékenyég leírható. Ide sorolható az információt hordozó entitások (személyek és eszközök) védelme, azaz az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az irat- és dokumentumvédelem, valamint a személyi védelem is. Az információvédelem célja – hasonlóan az adatvédelemhez – a jogosulatlan hozzáférés,

[32] Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz felhasználásával – Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016.

módosítás vagy megsemmisítés elleni védelem és az információk folyamatos rendelkezésre állásának biztosítása. Az *információbiztonság* – a hatályos nemzeti szabályozás alapvetéseiből kiindulva – olyan követelményrendszerként jellemezhető, amely középpontjában:

a) a bizalmasság (csak az arra jogosult és csak a jogosultság szintje szerint férhet az adathoz és használhatja fel),
b) a sértetlenség (az adat hitelessége és megváltoztatásának elkerülése), valamint
c) a rendelkezésre állás (az adatok elérhetőek és felhasználhatóak legyenek)

jelenik meg,[33] függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például: alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg.

Fenti elméleti alapvetést követően – igazodva a hatályos törvényi rendelkezésekhez – a továbbiakban az okostelefonokhoz kapcsolódó adatvédelemi és információbiztonsági szabályozásról (elektronikus információbiztonságról) lesz szó, mivel a védelmi és biztonsági szempontok meghatározásánál az adatok és információk megjelenési formája és hordozója eltérő szabályozást igényel.

Az okostelefonok esetében szabályozási szempontból az adatvédelmi szempontú megközelítés az eszközökön tárolt adatok hozzáférhetőségre és azok felhasználásra vonatkozik, míg az információbiztonsági szempontú megközelítés az okoseszközökkel végzett „műveletekre" és az eszközökön futtatott IT rendszerekre és alkalmazásokra mint elektronikus információs eszközökre vonatkozik.

2. Rendszertani és szabályozási környezet

Az adatvédelemre és az információbiztonságra vonatkozó szabályozási környezetre megfelelő szintű tagoltság jellemző. A szabályozás a jogforrási hierarchia mentén a törvényi rendelkezésekből és a törvényi felhatalmazás alapján megalkotott végrehajtási rendeletekből (akár kormányrendelet, akár miniszteri rendelet) kiindulva a közjogi szervezetszabályzó eszközök szintjéig (például: központi államigazgatási szerv vagy fővárosi és megyei kormányhivatal vezetője által kiadott Adatvédelmi Szabályzat, Informatikai Biztonsági Szabályzat) tart, figyelemmel Magyarország Alaptörvénye T) cikkének és a jogalkotásról szóló 2010. évi CXXX. törvény rendelkezéseire. Jelen fejezet célja a jogforrási hierarchia mentén a nemzeti főbb szabályzók számbavétele – amelyek részleteit a 3. és 4. fejezetek tartalmazzák – és az európai uniós kapcsolódások bemutatása – utóbbi esetében a gyakorlati adaptációt az 5. fejezet tartalmazza.

2.1. Nemzeti szabályozás

Magyarország Alaptörvénye mint a jogforrási hierarchia csúcsán álló jogszabály az információs alapjogokat – a személyes adatok védelmét és a közérdekű adatok nyilvánosságát – közös bekezdésben rögzíti. Az Alaptörvény VI. cikk (2) bekezdése szerint *„Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez."*[34] Az Alaptörvény szövegezése nem szakít a korábbi Alkotmány[35] elveivel, így bár az e tárgykörben hozott 15/1991. (IV. 13.) AB határozat az Alaptörvény 5. pontja alapján hatályát vesztette, a határozat által kifejtett joghatások mellett az értelmezési keretek véleményünk szerint napjainkban is helytállóak.

Az Alkotmánybíróság rögzíti: *„Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás*

[33] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján.
[34] Magyarország Alaptörvénye, VI. cikk (2) bekezdés.
[35] 1949. évi XX. törvény 59. § és 61. §-ai.

egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is. Az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel az Alkotmány 8. §-ában megkövetelt feltételeknek."[36] Az Alkotmánybíróság ezen határozatában az információs önrendelkezési jog gyakorlásának feltételeként és garanciális elemeként rögzítette a célhoz kötöttség, az adattovábbítás és az adatok nyilvánosságra hozása korlátozása elvét és részletesen kifejtette ezen elvek egymáshoz való viszonyát. A célhoz kötöttség elvéhez kapcsolódóan az Alkotmánybíróság azt is kimondta, hogy a meghatározott cél nélküli „készletre", azaz az előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és adattárolás, az úgynevezett „adatkészletezés" alkotmányellenes.[37] Ezen – máig érvényes elveket tartalmazó – döntésével az Alkotmánybíróság már az 1990-es évek elején rámutatott arra, hogy az alapjogok korlátozására alkotmányos keretek között, meghatározott elvek mentén kerülhet sor. Emellett elvi alapvetésként kell rögzíteni, hogy az alapjogok korlátozása nem lehet önkényes.

Az Alaptörvény kimondja, hogy *„Az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható."*[38] Az alapjogi konfliktusok feloldásának, az alapjogok korlátozásának alkotmányossági megítélésének módszere az alapjogi teszt, az úgynevezett szükségességi-arányossági teszt. A teszt lényege az a kétlépcsős eljárás, amely során először a jogkorlátozás céljának vizsgálatát, azaz a szükségességet kell elvégezni (például: más alapjogokkal való összeütközés), majd az alkalmazott jogkorlátozás mértékéről, azaz az arányosságról kell dönteni. A második lépcsőben külön szükséges vizsgálni, hogy észszerű (alkalmas), elengedhetetlen (szükséges) és arányos (cél és az okozott jogsérelem arányban áll-e egymással) az alkalmazott korlátozás vagy felfüggesztés. Ezen garanciális elvek érvényesítése érdekében az Alaptörvény rendelkezik arról, hogy fenti információs alapjogok érvényesülését sarkalatos törvénnyel létrehozott független hatóság – Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) – ellenőrzi.[39]

2012. január 1-jétől hatályos az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), amely – megtartva a korábbi szabályozás[40] főbb elveit – az információs alapjogok védelme céljából meghatározza az adatkezelés általános követelményeit és a védelem garanciális elemeit. Az Infotv. a hatálybalépését követően – az Alaptörvényben rögzített és fentebb említett hatóság létrehozása érdekében – újrafogalmazta és átrendezte az adatvédelem felügyeleti rendszerét és annak az államszervezetben elfoglalt helyét. A szabályozást áttekintve érzékelhető, hogy az adatvédelem komplex kérdésköre nem kezelhető egyetlen törvényben, az adatkezelés speciális, ágazati szabályait számos kapcsolódó jogszabály tartalmazza, amely az Infotv.-ben meghatározott általános szabályrendszert egészíti ki. (Az Infotv. kapcsolódó szabályainak ismertetésére a 3. fejezetben kerül sor.)

[36] 15/1991. (IV. 13.) AB határozat Indokolás II. fejezet.
[37] 15/1991. (IV. 13.) AB határozat Indokolás II. fejezet.
[38] Magyarország Alaptörvénye, I. cikk (3) bekezdés.
[39] Magyarország Alaptörvénye, VI. cikk (3) bekezdés.
[40] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

Az Alaptörvényben rögzített és az Infotv.-ben részletezett alapjogok kiemelt védelméből adódóan a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) XXI. fejezete az emberi méltóság és egyes alapvető jogok elleni bűncselekmények körébe emeli a személyes adattal való visszaélés cselekményét.[41] A törvényi tényállás szerint a személyes adattal való visszaélés vétségét követi el, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével:

a) haszonszerzési célból vagy jelentős érdeksérelmet okozva:
  aa) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
  ab) az adatok biztonságát szolgáló intézkedést elmulasztja,
b) az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

Az elkövető a vétség elkövetése miatt egy évig terjedő szabadságvesztéssel büntetendő. Ha a cselekményt különleges adatra vagy bűnügyi személyes adatra követik el, a büntetés két évig terjedő szabadságvesztés. Ha a visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el, a cselekmény bűntettnek minősül és három évig terjedő szabadságvesztéssel büntetendő.

A Btk. a XXI. fejezetben az Infotv. rendelkezéseivel összhangban a közérdekű adattal visszaélés cselekményét is bűntettnek minősíti. A közérdekű adattal visszaélés vétségét követi el és két évig terjedő szabadságvesztéssel büntetendő, aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével:

a) közérdekű adatot az adatigénylő elől eltitkol, vagy azt követően, hogy a bíróság jogerősen a közérdekű adat közlésére kötelezte, tájékoztatási kötelezettségének nem tesz eleget,
b) közérdekű adatot hozzáférhetetlenné tesz vagy meghamisít, illetve
c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz.

Ha a közérdekű adattal visszaélést jogtalan haszonszerzés céljából követik el, a cselekmény bűntettnek minősül és három évig terjedő szabadságvesztéssel büntetendő.[42]

Az Infotv. rögzíti, hogy ha a Nemzeti Adatvédelmi és Információszabadság Hatóság az eljárása során:

a) bűncselekmény elkövetésének alapos gyanúját észleli, büntetőeljárást kezdeményez,
b) ha szabálysértés vagy fegyelmi vétség elkövetésének alapos gyanúját észleli, szabálysértési, illetve fegyelmi eljárást kezdeményez

az eljárás lefolytatására jogosult szervnél.[43]

Az adatok védelme terén az Infotv. mellett – bár a társadalom tagjainak körében kevésbé ismert – kiemelt jelentőségű szabályozás a 2010 év végén kihirdetett, a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény[44], majd a nemzeti adatvagyonról szóló 2021. évi XCI. törvény (a továbbiakban: Adatvagyon tv.), amely nemzeti adatvagyonként a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összességét[45] határozza meg. Az állam felismerve annak jelentőségét, hogy az általa kezelt nemzeti adatvagyon körébe tartozó alapadatok az állam és a közigazgatás működéséhez elengedhetetlenek, kiemelt jelentőséget tulajdonított ezen adatok védelmének a szabályozás megalkotásával.

[41] Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 219. §.
[42] Btk. 220. §.
[43] Infotv. 70. § (1) bekezdés.
[44] Kihirdetve: 2010. december 22-én.
[45] A nemzeti adatvagyonról szóló 2021. évi XCI. törvény (a továbbiakban. Adatvagyon tv.) 2. § a) bekezdés.

Az Adatvagyon tv. kimondja,[46], hogy a nemzeti adatvagyon részét képező adatállomány tekintetében törvény az adatfeldolgozással megbízható személyek és szervezetek körét korlátozhatja, vagy az adatfeldolgozásnak az adatkezelőtől különböző személy vagy szervezet általi ellátását kizárhatja. Az adatok védelme érdekében az Adatvagyon tv. rendelkezik arról is, hogy nemzeti adatvagyon esetében adatfeldolgozást csak államigazgatási szerv vagy kizárólagos állami tulajdonú gazdálkodó szervezet láthat el. Kiegészítő szabályként rögzíti, hogy az adatkezelő kizárólag a Kormány rendeletében az adott nyilvántartás tekintetében meghatározott szervvel vagy szervezettel köthet adatfeldolgozási szerződést, és ha ez esetben meghatározott adatfeldolgozó igénybevétele kötelező, az adatkezelő ezen adatfeldolgozót bízhatja csak meg az adatfeldolgozással. Ezen szervek körét a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet melléklete tartalmazza.

Az Adatvagyon tv. kimondja továbbá, hogy ezen nyilvántartásokhoz kapcsolódó adatfeldolgozási műveletet az adatfeldolgozó kizárólag Magyarország területén végezhet.[47] Amennyiben a fent említett korlátozás valamely adatkezelő esetében a jogszabályban előírt feladatok határidőben történő teljesítését, vagy a rendelkezésre álló erőforrások szűkössége miatt a jogszabályban előírt feladatok teljesítéséhez szükséges fejlesztések határidőben történő megvalósítását veszélyezteti, az adatkezelő szakmai irányítására vagy felügyeletére kijelölt miniszter előterjesztésére a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter a korlátozás alól egyedi felmentést adjon.

Egyedi felmentés adható az időszakosan jelentkező adatfeldolgozási feladatok hatékony ellátásának biztosítása érdekében is, ha azok határidőben való ellátása a rendelkezésre álló erőforrások mellett más módon nem lehetséges. Az egyedi felmentés határozott időre adható meg.[48]

Az Adatvagyon tv. alkalmazásában a nemzeti adatvagyon a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.[49] Tartalmát tekintve ide sorolhatók az állami vagy helyi önkormányzati feladatot, továbbá jogszabályban meghatározott egyéb közfeladatot ellátó szervek vagy személyek kezelésében lévő hatósági nyilvántartási adatok, jogi normákkal és egyéb szervezeti normákkal összefüggő adatok, közművelődési és kulturális gyűjteményi adatok, illetőleg más (például levéltári) archívumok adatai, ezen felül statisztikai adatok, topográfiai és más téradatok, meteorológiai adatok, a közfeladat-ellátással és a közszolgáltatás-nyújtással összefüggő egyéb leíró adatok.[50]

Ilyen széles adatkör és kiemelt védelem tekintetében az Adatvagyon tv. célja a nemzeti adatvagyon körébe tartozó nyilvántartások biztonságának megteremtése, ezen nyilvántartások jogszerű felhasználását akadályozó cselekmények bűncselekménnyé nyilvánításával azok megelőzése. A Btk. XXV. fejezete nevesíti a nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekményt. A Btk. szerinti tényállás alapján[51] nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény esetén – ha más, súlyosabb bűncselekmény nem valósul meg – bűntett miatt három évig terjedő szabadságvesztéssel büntetendő, aki a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatot az adatkezelő részére hozzáférhetetlenné tesz, vagy a nemzeti adatvagyon körébe tartozó állami nyilvántartás működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza. Ha a bűncselekmény jelentős érdeksérelmet okoz, vagy a bűncselekményt haszonszerzés végett követik el, a büntetés egy évtől öt évig terjedő szabadságvesztés.

Az információbiztonság szabályozási környezetének kialakításával összefüggő első jogalkotási lépés az Országgyűlés 2013. április 15-ei ülésnapján elfogadott, az állami és önkormányzati szervek

[46] Adatvagyon tv. 12. § (1)-(2) bekezdések.

[47] Adatvagyon tv. 13. §.

[48] Adatvagyon tv. 12. § (5)-(6) bekezdések.

[49] Adatvagyon tv. 2. § a) pont

[50] Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz – Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016. április 19. oldal.

[51] Btk. 267. § (1) bekezdés.

elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.). Az Ibtv. elkészítésével párhuzamosan került 2013 márciusában elfogadásra Magyarország Nemzeti Kiberbiztonsági Stratégiája[52] (a továbbiakban: Kiberstratégia), amely elemezte Magyarország aktuális kiberbiztonsági helyzetét, jövőképét, továbbá megnevezte az aktuálisan elérendő célokat és az alkalmazandó eszközöket. Az Ibtv. az elektronikus információs rendszerekben tárolt, kezelt információk védelmét célozza és olyan szabályozási környezet alapjait teremti meg, amely a prevenciót, a fenyegetéseket számba vevő, az elektronikus információs rendszer minden elemére kiterjedő védelmet, illetve az elektronikus információbiztonság tudatosságnövelését tekinti alapvetésnek. A törvény végrehajtását számos végrehajtási rendelet segíti. Az Ibtv. és végrehajtási rendeleteinek ismertetésére – kitérve a Kiberstratégia főbb rendelkezéseire – a 4. fejezetben kerül sor.

Az eddigiekben leírtak alapján nem szükséges annak részletes kifejtése, hogy az állam – az információs alapjogok és a nemzeti adatvagyon védelme mellett – milyen védelem- és biztonságpolitikai célok érdekében határozta meg azokat az információs rendszerekkel összefüggő magatartásszabályokat, amelyeket büntetni rendel. Ez esetben is kiemelten fontos érdek, hogy az információs rendszerek, az abban kezelt adatok, a felhasználók és az üzemeltetők védelme biztosított legyen.

A Btk. önálló tényállásként szabályozza az információs rendszerekkel kapcsolatos bűncselekményeket, ezzel is kiemelve az információbiztonsághoz és az adatvédelemhez fűződő társadalmi érdek fontosságát. A Btk. alapján információs rendszer alatt az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezést, vagy az egymással kapcsolatban lévő ilyen berendezések összességét kell érteni[53].

A Btk. a vagyon elleni bűncselekmények között szabályozza *az információs rendszer felhasználásával elkövetett csalást*.[54] A bűntettet az valósítja meg, aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz. A kár bekövetkezésére az információs rendszer jogtalan befolyásolása miatt kerül sor. Alapesetben 3 év szabadságvesztéssel rendeli büntetni a jogalkotó a cselekményt, amely az okozott kár mértékétől függően akár 5 évtől 10 évig terjedő szabadságvesztés büntetéssel jár.

A *tiltott adatszerzés*[55] bűntett azáltal valósul meg, hogy az elkövető a személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot jogosulatlan módon akarja megismerni. Ezen adatok jogosulatlan megszerzése megvalósulhat:

- más lakásának, egyéb helyiségének vagy az azokhoz tartozó bekerített helynek a titokban való átkutatásával,
- az ott történtek technikai eszköz alkalmazásával való megfigyelésével, rögzítésével;
- más postai vagy egyéb zárt küldeményének felbontásával vagy megszerzésével, és tartalmának technikai eszközzel való rögzítésével;
- elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren másnak továbbított vagy azon tárolt adat kifürkészésével, és az észleltek technikai eszközzel való rögzítésével,
- információs rendszerben kezelt adatok titokban történő kifürkészésével, és az észleltek technikai eszközzel való rögzítésével.

A szabályozás szerint bűncselekménynek minősül az is, ha a fentiek szerinti információgyűjtésre a fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából kerül sor. Alapesetben 3 év szabadságvesztéssel rendeli büntetni a jogalkotó a cselekményt, minősített esetben (bűnszövetség, üzletszerűség, jelentős érdeksérelem okozása, hivatalos eljárás színlelése) a büntetési tétel 5 év is lehet.

[52] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
[53] Btk. 459. § (1) bekezdés 15. pont.
[54] Btk. 375. §.
[55] Btk 422. §.

Az *információs rendszer vagy adat megsértése*[56] bűncselekmény elkövetője olyan személy lehet, akinek a jogosultsága alapvetően kiterjed a szankcionált magatartásra (információs rendszerbe való belépés, adat megváltoztatása, törlése), azonban, ha e személy a jogosultsága kereteit túllépi, akkor már bűncselekményt követ el. Az információs rendszerbe való jogosulatlan adatbevitel önmagában nem szankcionálandó magatartás, csak abban az esetben, ha az további, nem kívánt következményekhez vezet, így ha a rendszer működését akadályozza. Az alaptényállás vétség, melyet a Btk. két évig terjedő szabadságvesztéssel rendel büntetni.

Az *információs rendszer védelmét biztosító technikai intézkedés kijátszása* bűncselekmény[57] tényállása akkor valósul meg, ha az elkövető az információs rendszer felhasználásával elkövetett csalás, illetve az információs rendszer vagy adat megsértése bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő:

- jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve
- jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja.

A tényállással összefüggően büntethetőséget megszüntető oknak minősíti a Btk. az eljáró hatósággal való együttműködést (tevékenység hatóság előtti felfedése, az elkészített dolognak a hatóság részére történő átadása, a készítésben részt vevő más személy kiléte megállapításának lehetővé tétele). Az alaptényállás vétség, melyet a Btk. két évig terjedő szabadságvesztéssel rendel büntetni.

Fentiekben azokat a főbb jogforrásokat vettük sorra, amelyek az adatvédelem és az információbiztonság szempontjából releváns szabályzók, és minden egyéb, a jogforrási hierarchia alsóbb szintjén álló jogszabály vagy szabályzó ezek rendelkezéseihez zsinórmértékként viszonyul. Az alapjogi szabályozás érvényesítésétől kezdve egészen azon közhatalom birtokában végezhető, állami kényszerrel kikényszeríthető szabályokig terjedt e kör, melyek végső soron, mint ultima ratio, egyes alapjogok korlátozásához is vezethetnek. Az adatvédelem és az információbiztonság témakörét érintően számos további szabályzó (ágazati törvények, végrehajtási rendeletek) tartalmaz speciális rendelkezéseket vagy részletszabályokat, ezek ismertetése azonban jelen jegyzet kereteit – azok egyedi és specifikus jellegét tekintve – meghaladja.

2.2. Európai uniós kapcsolódások

A következőkben az Európai Unió digitális világot érintő szabályozási keretrendszerét mutatjuk be. A bemutatás a 2010. évet követő dokumentumokra szorítkozik. Ennek oka az, hogy a pénzügyi és gazdasági világválság következményeinek kezelése új gondolkodásmódot követelt meg az Európai Unió vezetőitől. A fenntartható fejlődés és a jövő érdekében hosszú távú, tíz éves (jellemzően 2020-ig szóló) stratégiai tervdokumentumok születettek, melyeknek a jelenkor és az eljövendő időszak kihívásaira és dinamikus modernizációjára, valamint az erőteljes globalizációra válaszul szerves részét képezi a tudáson és innováción alapuló gazdaság kialakítása.

Elsőként az elkövetkezendő évek intézkedései alapdokumentumának számító *Európa 2020 foglalkoztatási és növekedési stratégiát ismertetjük*[58] (a továbbiakban: Európa 2020 stratégia).

Az Európai Unió 2010-ben azzal a céllal alkotta meg az Európa 2020 stratégiát, hogy megteremtse az *intelligens* (hatékonyabb oktatási, kutatási és innovációs beruházások, valamint a digitális társadalom fejlesztése), *fenntartható* (erőforrás-hatékonyabb, környezetbarátabb és versenyképesebb

[56] Btk. 423. §.
[57] Btk. 424. §.
[58] Lásd: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF (utolsó letöltés: 2016. október 10.)

gazdaság) és *inkluzív* (a gazdasági, szociális és területi kohéziót előmozdító, magas foglalkoztatási arányt biztosító gazdaság) növekedés feltételeit. Fontos, hogy az Európa 2020 stratégia az európai uniós intézmények, a tagállamok és a szociális partnerek közös stratégiája, azaz valamennyi címzettnek azonosulnia kell a stratégia célkitűzéseivel, és meg kell tennie az ezen célkitűzések végrehajtását szolgáló ütemezett intézkedéseket[59].

Az Intelligens növekedés prioritásban az Európa 2020 stratégia beavatkozási területként rögzítette a digitális társadalmat. Megállapítja ugyanis, hogy az információs és kommunikációs technológiák iránti globális kereslet 2 000 milliárd euró értékű piacot jelent, ennek azonban csak negyede származik európai vállalkozásoktól. Európában elmaradás tapasztalható továbbá a nagy sebességű internet használata terén is, ami – főként a vidéki területeken – hátrányos hatással van Európa innovációs képességére, a tudás online terjesztésére, valamint az áruk és szolgáltatások online forgalmazására.

Az Európa 2020 stratégia margóján 7 új kiemelt kezdeményezés indult, melyek esetében az Uniónak és a tagállami hatóságoknak össze kell hangolniuk intézkedéseiket. Az egyik ilyen kiemelt kezdeményezés – a digitális társadalom beavatkozási terület kapcsán felvázoltakra figyelemmel – az Intelligens növekedés célrendszerén belül az *Európai digitális menetrend*.

Az Európa 2020 stratégia célként fogalmazta meg az Európai digitális menetrend kapcsán, hogy:

a) a nagy sebességű és szupergyors internetre és az interoperábilis alkalmazásokra épülő egységes digitális piac révén fenntartható gazdasági és szociális előnyöket teremtsen,
b) 2013-ig mindenkinek szélessávú, 2020-ig pedig mindenki számára ennél is sokkal gyorsabb, legalább 30 Mbps sebességű internet-hozzáférést biztosítson,
c) az európai háztartások legalább fele a 100 Mbps-t meghaladó internetkapcsolatra szóló előfizetéssel rendelkezzen.

Az Európai digitális menetrend keretében tervezett intézkedések:

a) az egységes digitális piac megteremtése (az online tartalmakhoz való jogszerű hozzáférés, valamint az elektronikus fizetés és számlázás megkönnyítése),
b) az uniós adatvédelmi szabályozási keret felülvizsgálata,
c) távközlési szolgáltatások egységesítése,
d) fokozott interoperabilitás és szabványok,
e) készülékek, alkalmazások, adattárolók, szolgáltatások és hálózatok átjárhatóságának növelése,
f) bizalom és az internetes biztonság megerősítése,
g) nagy sebességű és szupergyors internet-hozzáférés mindenki számára,
h) befektetés a kutatásba és az innovációba,
i) digitális jártasság, a digitális készségek és a digitális integráció előmozdítása,
j) technológia intelligens használatából eredő előnyök kiaknázása a társadalom számára.

Jelen tananyag tematikáját érintően kiemelendő, hogy az Európai digitális menetrend problémaként rögzítette, hogy a számítógépes bűnözés terjedése miatt az emberek bizalmatlanok az online alkalmazásokkal és az internettel szemben, ezért nem szívesen használják azokat. Megoldási javaslatként a dokumentumban megfogalmazásra került, hogy meg kell erősíteni az infokommunikációs megoldások használatát számos olyan területen, ahol az uniós polgárok kézzelfoghatóan érzik ezen alkalmazások használatának előnyeit (például egészségügyi ellátás, méltóságteljes életvitellel, kultúra, e-közigazgatás fejlesztése, intelligens közlekedési rendszerek). További célkitűzés a nagy sebességű és szupergyors internet-hozzáférés biztosítása minél szélesebb körben, ennek keretében a szélessávú lefedettség és az új generációs, szupergyors hálózatok kiépítése, a nyílt és technológia-semleges szolgáltatások elterjesztése.

[59] Lásd: http://ec.europa.eu/europe2020/who-does-what/index_hu.htm (utolsó letöltés: 2016. október 10.)

Az Európai Digitális Menetrend hét beavatkozási területe közül a Bizalom és biztonság intézkedési területen célként kerültek meghatározásra az alábbiak:

a) javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;
b) számítógépes támadások elleni gyorsreagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok (CERT) hálózatának létrehozása, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepének megerősítése;
c) javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról;
d) tudatosságnövelés, így többek között az internetes védelem iskolai oktatása;
e) egyebek mellett a gyermekbántalmazással, a személyazonosság-lopással és számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása;
f) magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten és azon kívül egyaránt.

A hét beavatkozási terület minden eleme kapcsolódik valamilyen mértékben a hatályos szabályozáshoz. A 4. fejezet részletes betekintést nyújt a hazai információbiztonsági szabályokba, az 5. fejezetben pedig bemutatjuk annak hazai stratégiai megalapozását is. Erre figyelemmel nem szabad figyelmen kívül hagynunk az információbiztonságot érintő uniós szabályozókat sem.

A kiberbiztonság kérdéskörét az Európai Unió hosszú időn keresztül csupán büntetőjogi szempontból kezelte, annak széles spektrumú átfogó áttekintését először az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága végezte el *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* című uniós stratégiáról szóló, 2013-ban közzétett közös közleményében (továbbiakban: uniós stratégia). Az uniós stratégia az alábbi prioritásokat vázolja fel:

a) az információs rendszerek kibertámadásokkal szembeni ellenálló képességének megteremtése;
b) a számítástechnikai bűnözés drasztikus visszaszorítása;
c) kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát érintő képességek fejlesztése;
d) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
e) az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése;
f) a számítógépes bűnözéssel foglalkozó nemzeti kiválósági központok hálózatának kialakítása és finanszírozása.

Az uniós stratégiában foglaltak egyfajta intézkedési tervének tekinthető *a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvjavaslat* (továbbiakban: irányelvjavaslat).

Az irányelvjavaslat előírásai között szerepelnek az alábbiak:

a) a tagállamok a hálózat- és információbiztonság területén illetékes hatóságok létrehozásával, hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-ek) felállításával és nemzeti hálózat- és információbiztonsági stratégiák és együttműködési tervek elfogadásával nemzeti szinten biztosítsák a képességek minimális szintjét;
b) az illetékes nemzeti hatóságoknak hálózatot kell alkotniuk, amelyben együttműködnek az összehangolt információcsere, valamint az uniós szinten történő felderítés és reagálás biztosítása érdekében; a tagállamok e hálózaton keresztül az európai hálózat- és információbiztonsági

együttműködési terv alapján bonyolítják a hálózat- és információbiztonsági fenyegetések és események elleni küzdelemhez szükséges információcserét és együttműködést;

c) kialakuljon egy kockázatkezelési kultúra, és gyakorlattá váljon a magán- és a közszféra közötti információ-megosztás a hálózatokat és információs rendszereket komolyan veszélyeztető, valamint a kritikus szolgáltatások folyamatosságát és az áruellátást jelentősen befolyásolni képes biztonsági eseményekről;

d) a tagállamok nemzeti hálózat- és információbiztonsági stratégiát és együttműködési tervet készítsenek, hálózat- és információbiztonságért felelős nemzeti hatóságot jelöljenek ki, illetve úgynevezett számítógépes vészhelyzeteket elhárító csoportot állítsanak fel a biztonsági események és kockázatok kezelésére;

e) az érintett vállalkozások és a közszféra számára bizonyos biztonsági követelmények kerüljenek meghatározásra és ezen szereplők számára esemény bejelentési kötelezettség álljon fenn.

Az Európai Bizottság 2015. április 28-án közzétett, *Az európai biztonsági stratégia* című közleménye (a továbbiakban: biztonsági stratégia) az együttműködés fontosságát hangsúlyozza valamennyi szinten: együttműködés az Európai Unió egyes szervei között és a tagállamokkal, azok hatóságaival.[60] A biztonsági stratégia a terrorizmus leküzdése és a radikalizálódás megelőzése, valamint a szervezett bűnözés felszámolása mellett alappillérként rögzíti a számítástechnikai bűnözés elleni harcot és annak legfőbb eszközeként a kiberbiztonságot határozza meg.

A számítástechnikai bűnözés elleni harc területén szükséges fellépések a biztonsági stratégia szerint:

a) a kiberbiztonsággal kapcsolatos meglévő szakpolitikai eszközrendszer végrehajtásának megerősítése, az információs rendszerek elleni támadások és a gyermekek szexuális kizsákmányolása elleni küzdelem előtérbe helyezése (a tagállami jogszabályok közelítése egymáshoz, továbbá együttműködés a tagállamokkal az irányelvek megfelelő végrehajtása érdekében);

b) a készpénz-helyettesítő fizetési eszközökkel kapcsolatos csalás és hamisítás elleni küzdelemmel foglalkozó jogi aktusok felülvizsgálata és esetleges kiterjesztése a pénzügyi eszközöket érintő bűncselekmények és hamisítás újabb formáinak figyelembevétele érdekében, és az ezzel kapcsolatos javaslatok előterjesztése 2016-ban (a kerethatározat 2001. évi kiadása óta felmerült legújabb technikai kihívásokra reagáló szabályozás megalkotása);

c) a számítástechnikai bűncselekmények ügyében folytatott nyomozások útjában álló, nevezetesen az illetékes joghatósággal és a bizonyítékokhoz és információkhoz való hozzáféréssel kapcsolatos akadályok felszámolása (új technológiák alkalmazása, magánszektorral történő együttműködés, valós idejű elektronikus bizonyítékok beszerzése);

d) a kiberbiztonsági kapacitásépítést célzó fellépések előmozdítása a külső támogatási eszközök keretében (a nemzetközi együttműködés terén hozzáadott értékkel bíró kezdeményezések támogatása, például budapesti egyezmény[61]).

Fentiek alapján érzékelhető, hogy az Európai Unió szabályozásának középpontjában a keretjellegű elvek és intézkedési javaslatok, döntések meghatározása áll, azok végrehajtása és az ehhez szükséges szervezetrendszer kialakítása önálló feladatként jelentkezett minden tagállam számára.

[60] „Az Unió által az elmúlt években létrehozott eszközök sikere mindenekelőtt az összes résztvevő szereplő – az uniós intézmények és ügynökségek, a tagállamok és a nemzeti hatóságok – közötti felelősség-megosztásra, kölcsönös bizalomra és hatékony együttműködésre épül." – Az Európai Bizottságnak az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának szóló, „Az európai biztonsági stratégia" című közleménye.

[61] Az Európa Tanács egyezménye a számítógépes bűnözésről, Budapest, 2001. november 23.

A szakanyag lezárást követően a Tanács 2019. április 9-én elfogadta azt a kiberbiztonsági jogszabályként is ismert rendeletet, amely lehetővé teszi az EU számára, hogy célzott korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést jelentenek az EU vagy annak tagállamai számára.[62]

2020 decemberében az Európai Bizottság és az Európai Külügyi Szolgálat (EKSZ) új uniós kiberbiztonsági stratégiát terjesztett elő (Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér).[63] E stratégia célja, hogy:

- megerősödjön Európa kiberfenyegetésekkel szembeni rezilienciája,
- minden polgár és vállalkozás megbízható szolgáltatásokat és digitális eszközöket vehessen igénybe, és ezek előnyeit teljes mértékben ki tudja használni,
- megőrizze a globális és nyílt internetet, biztosítékot nyújtva ugyanakkor arra, hogy a biztonság mellett az európai értékek és a mindenkit megillető alapvető jogok is védelmet élvezzenek.

2021. november 26-án az Európai Unió Tanácsa elfogadta az EU egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekkel kapcsolatos álláspontját, amely intézkedések célja, hogy tovább javuljon mind az állami, mind a magánszektornak, illetve az Unió egészének kiberrezilienciája és a kiberbiztonsági eseményekre való reagálási képessége. Elfogadását követően az új, „NIS 2” elnevezésű irányelv a hálózati és információs rendszerek biztonságáról szóló jelenlegi irányelv (NIS-irányelv) helyébe lép.[64]

3. Adatvédelem és az Infotv. szabályozási környezete

Az adatvédelmi szabályozás történeti fejlődését bemutató szakirodalmak általánosan rögzítenek olyan szakaszokat, melyek a technológiai fejlődés kihívásaira és a társadalom szerkezeti változásaira is reflektálnak. A magyar szakirodalom egy része három fázist különböztet meg. Az első generációs szabályozás az 1970-es években fejlődött ki és az állami, automatizált nyilvántartásokkal szembeni védelmet alakította ki. A második generációs szabályok az 1980-as, 1990-es években jelentek meg, melyek már a papíralapú nyilvántartásokat is a szabályozás hatálya alá vonták. Az ezredfordulón előtérbe kerülő harmadik generációs szabályok főbb jellemzői közé az európai integráció sajátosságainak figyelembe vételét, és a szektorális szabályok megjelenését soroljuk.[65] Napjainkban egyre több szerző foglalkozik a szabályok kiegészítésével, vagy ha úgy tetszik, egy újabb generációs szabályozás szükségességével és megjelenésével, amely középpontjában az információs társadalom, az infokommunikáció térhódításából eredően az internet és az önszabályozás kérdése áll. Jelen fejezetnek nem célja az adatvédelmi szabályozás történeti áttekintése, az egyes főbb irányok melletti elköteleződés, azonban a főbb mérföldkövek rövid bemutatása szükséges ahhoz, hogy az Infotv. rendelkezéseivel összhangban az újabb – negyedik vagy harmadik (amely attól függ, hogy mely főáram tanait követjük[66]) – generációs szabályozás igényét felismerjük.

[62] AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”)

[63] Lásd: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001

[64] Bővebben ld.: https://www.consilium.europa.eu/hu/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/

[65] Majtényi László: Az információs jogok. in.: Halmai Gábor – Tóth Gábor Attila (szerkesztők): Emberi jogok. Osiris Kiadó, 2003. 582-583. oldal.

[66] A *Szerző* megjegyzése.

3.1. Az adatvédelmi szabályozás főbb mérföldkövei

Adatvédelmi szempontból főbb mérföldkövekről szabályozási szinten akkor érdemes beszélni, ha azok olyan átfogó változásokat hoztak vagy hoznak, melyek igazodnak valamely társadalmi, technológiai változáshoz és ezáltal új szabályok megalkotását igénylik.

A szakirodalom egységesen az 1970-es évekre vezeti vissza az úgynevezett *első generációs adatvédelmi szabályozás* kialakulását, amely középpontjában a számítástechnika fejlődéséből eredően az állami nyilvántartások adatainak elektronikus tárolásából, és ezen nyilvántartásokban való keresés lehetőségeiből adódó kérdések és azok jogi reflexiója állt. A technológiai fejlődés lehetővé tette a nagy tömegű automatizált adatfeldolgozást, amely a központi nyilvántartások kialakításának irányába mutatott. Az állam, mint nagy adatkezelő jelent meg, amely egy, egyedi azonosítószám alkalmazásával kívánta kezelni a nyilvántartásokat és az azokban tárol személyes adatokat. Ez vezetett odáig, hogy Európában – főként a jóléti államok körében – sorra jelentek meg az első szabályzók (Svédország, Német Szövetségi Köztársaság, Dánia, Norvégia, Ausztria, Franciaország). A szabályozás elsődleges célja a fentiekben említett nagy állami adatbázisok átláthatóságának megteremtése, amely alapvetően az automatizált adatkezelésekre terjedt ki, és hangsúlyos szerepet kapott benne a konkrét technológia szabályozása. Mindemellett ezen szabályzók az egyén részére nem garantálták az általános rendelkezési jogot a személyes adataik felett. A szabályozás már ekkor is tartalmazta az adatvédelemi rendelkezések felett őrködő felügyeleti szervek feladat- és hatásköreit. [67]

Az 1980-as években a számítástechnika ugrásszerű fejlődése eredményeképpen teret hódított a személyi számítógép (a továbbiakban: PC – Personal Computer) amely mind a gazdasági és üzleti szektorban, mind a lakosság körében is széles körben elterjedt. Ezeket a PC-ket az 1990-es években megjelenő Internet hálózatba kötötte, ahol minden eddiginél gyorsabban és nagyobb mennyiségben, ámde különösebb kontrol nélkül lehetett az adatokat (például: e-mailen) továbbítani. Az üzleti szektor adatbázisai az ügyfelekről számos – esetenként különleges – adatot is kezeltek.[68] Az információ oly mértékben felértékelődött, amely elvezetett az úgynevezett *második generációs adatvédelmi szabályozás* megjelenéséhez. A szabályozás kialakítását sürgette azon álláspont Európai Unión belüli térnyerése, amely szerint az adatok szabad áramlását úgy kell biztosítani, hogy a magánszféra és a személyes adatok védelme garantált legyen. A második generációs szabályozás fő eleme, hogy a technológiai megközelítés helyett az adatkezeléssel érintett személyt – az adatgazdát – széleskörű rendelkezési joggal ruházta fel.[69] A szabályozás az elektronikus adatkezelésekre és a manuális, papír alapú adatkezelésekre egyaránt kiterjedt.

A szabályozásban megjelentek a nemzetközi dokumentumok, melyek közül egy, ugyan nem kötelező érvényű, de számos máig is fontos alapelvet tartalmazó szabályt külön ki kell emelni.

A magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló OECD irányelveket 1980-ban fogadták el,[70] amely az adatvédelem alapelveinek az alábbiakat tekinti:

1. Adatgyűjtés korlátozásának elve: személyes adatok gyűjtésére csak törvényes és tisztességes eszközökkel, az adatalany tudtával és beleegyezésével kerülhet sor.
2. Az adatminőség elve: a gyűjtött adatoknak az adatkezelés céljával összhangban pontosnak, teljesnek és aktuálisnak kell lenniük.
3. A célhoz kötöttség elve: személyes adatokat csak előre meghatározott célból, csak a cél megvalósulásához szükséges mértékben és ideig lehet kezelni.
4. A korlátozott felhasználás elve: az adatokat csak az adatalany hozzájárulásával vagy törvényi felhatalmazással lehet felhasználni.

[67] Jóri András: Adatvédelmi kézikönyv Osiris Kiadó, Budapest, 2005. 24–25. oldal.

[68] Majtényi László: Az információs szabadságok, in.: Halmai Gábor – Tóth Gábor Attila (szerkesztők): Emberi jogok. Osiris Kiadó, 2003. 36. oldal.

[69] Jóri András: Adatvédelmi kézikönyv Osiris Kiadó, Budapest, 2005. 27. oldal.

[70] Jóri András: Adatvédelmi kézikönyv Osiris Kiadó, Budapest, 2005. 28–29. oldal és Majtényi László: Az információs szabadságok, in.: Halmai Gábor – Tóth Gábor Attila (szerkesztők): Emberi jogok. Osiris Kiadó, 2003. 95–96. oldal.

5. A biztonság elve: az adatokat a technológia mindenkori állásának megfelelő ésszerű intézkedésekkel és eszközökkel kell védeni a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás, sérülés és megsemmisülés ellen.
6. A nyíltság elve: az adatkezelés tényének, helyének és céljának, az adatkezelő személyének, valamint az adatkezelési politikának nyilvánosnak kell lennie.
7. A személyes részvétel elve: az adatalany megismerheti a rá vonatkozó adatokat, azokat szükség esetén helyesbítheti, kiegészítheti vagy töröltetheti.
8. A felelősség elve: az adatkezelő a felelős a fentebb felsorolt elvek betartásáért, s bizonyítani kell tudnia az adatkezelés jogszerűségét.

Ezen OECD elvek már a második generációs szabályozásban is megjelennek, mindemellett fontos szerepet töltöttek be abban a harmonizációs folyamatban, melyek az Európai Unió 1995-ben elfogadott adatvédelmi irányelvéhez,[71] majd a harmadik generációs egységes adatvédelmi szabályrendszer kialakításához vezettek.

Az infokommunikációs szolgáltatások térhódítása és az Internet világméretű elterjedése, a fokozódó felhasználó igények (közösségi oldalak elterjedése) miatt vált szükségessé a harmadik generációs adatvédelmi szabályozás kialakítása, amely jelenleg is tart (és vagy kiegészítése, vagy új generációs szabályozás szükséges a kihívások kezelésére). A tartalomszolgáltatás megváltozása mellett ez a térhódítás óriási méretű adatbázisok kialakulását is jelentette, amely együtt jár az adatbányászati tevékenységgel. Komoly kockázat a mobileszközök elterjedése, és ezzel összefüggésben a helymeghatározáson alapuló szolgáltatások elterjedése, amely nem más, mint a személy valós idejű tartózkodási helyének közvetítése „ismeretlen" számú adatkezelő irányába. Ugyanakkor egyre nagyobb igény mutatkozik a felhőalapú szolgáltatások igénybevételére, amely alapjaiban rendezi át az adatok tárolásának módját.

Ezen szabályozási elvek már megjelennek a 2016. május 25-én hatályba lépett, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679 Rendeletében (a továbbiakban: általános adatvédelmi rendelet). Az általános adatvédelmi rendeletet 2018. május 25-től kell kötelezően alkalmazni, amely az elmúlt időszakban számos jogharmonizációs feladatot keletkeztetett (többek között az Infotv. módosítását is). A szabályozás – a teljesség igénye nélkül – főbb jellemzője, hogy alapvetően az adatkezelők kötelezettségeit és felelősségét helyezi előtérbe, ezáltal az információs önrendelkezési jog egyéni érvényesítését mellérendelt pozícióba helyezi. Kötelezettségként rögzíti a megfelelő eljárásrendek, szabályzatok elfogadását, adatkezelési dokumentáció vezetését, adatbiztonsági intézkedések megtételét, belső adatvédelmi felelős kijelölését. A szabályozásban megjelenik a technológia szabályozás problematikája, hiszen az közvetlen hatással van az adatvédelemre és az információbiztonságra.[72]

2018. július 26-án hatályba lépett az Infotv. átfogó módosítása, így ennek következtében a törvény összhangba került az általános adatvédelmi rendelettel. Az Infotv. tartalma, főbb szabályai bemutatásra kerülnek akövetkezőkben, ezért a GDPR közvetlen ismertetése nem képezi jelen tanulmány részét.

[71] A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelve.

[72] A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679 Rendelet alapján.

3.2. Az Infotv. releváns rendelkezései

3.2.1. A törvény hatálya[73]

Az Infotv. hatálya kiterjed minden olyan adatkezelésre, amely személyes adatra, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik. A törvény területi hatálya Magyarországra terjed ki.

Nem kell alkalmazni az adatvédelmi szabályokra vonatkozó Infotv. rendelkezéseket a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezelései esetében (például: magánszemély okostelefonjában szereplő címjegyzék, ha magáncélra használják).

3.2.2. Az értelmezendő rendelkezések köre[74]

Az egységes jogértelmezés biztosítása érdekében az Infotv. közel harminc pontban rögzíti az értelmező rendelkezéseket, többek között meghatározza:

a) az adatok milyenségére vonatkozó (személyes adat, különleges adat, bűnügyi személyes adat, közérdekű adat, közérdekből nyilvános adat stb.),
b) az adatkezelési tevékenységgel összefüggő (hozzájárulás, adatkezelés, adattovábbítás, nyilvánosságra hozatal, adattörlés, adatmegsemmisítés, adatfeldolgozás stb.), és
c) az adatkezelésben érintett szereplőkre vonatkozó (érintett, adatkezelő, adatfeldolgozó, adatfelelős, adatközlő, harmadik személy stb.)

alapfogalmakat. Az alapfogalmak teljes körű részletes ismertetése jelen jegyzet tárgykörét tekintve nem releváns, ezért a következőkben az adatvédelmi szempontból fontos fogalmakat vesszük sorra.

A *személyes adat* fogalmának meghatározása tág keretek között mozog, személyes adat az érintettre vonatkozó bármely információ. E széles körű megfogalmazásba a személy azonosítására vonatkozó adatok – természetes (például: név, születési és lakcím adatok) és mesterséges azonosítók (például: TAJ szám, adóazonosító jel, útlevélszám) – is beletartoznak. A személyes adat fogalma együtt értelmezhető az *érintett* fogalmával, amely bármely információ alapján azonosított vagy azonosítható természetes személy.

Kiemelt jelentőséget tulajdonít a jogszabály a személyes adatok speciális körének, a különleges adatoknak, mivel ezek olyan szenzitív jelleggel bírnak, amely adatokkal való visszaélés súlyosabb sérelemmel, jogkövetkezményekkel jár. Az Infotv. szerint *különleges adat* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.[75]

Annak érdekében, hogy a személyes adatokkal végzett tevékenységek, műveletek jól körbehatárolhatóak legyenek, az Infotv. mintegy gyűjtő fogalomként meghatározza mi minősül:[76]

a) *adatkezelés*nek (az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése,

[73] Infotv. 2. §.
[74] Infotv. 3. §.
[75] Infotv. 3. § 3. pont.
[76] Infotv. 3. § 10. és 17. pontok.

valamint a személy azonosítására alkalmas fizikai jellemzők; például ujj- vagy tenyérnyomat, DNS-minta, íriszkép rögzítése), valamint

b) *adatfeldolgozás*nak (az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége).

Fentiekhez igazodóan az Infotv. rögzíti az *adatkezelő* (az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre – beleértve a felhasznált eszközt – vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja) és az *adatfeldolgozó* (az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel).[77]

Az *adatvédelmi incidens* fogalma szerint adatvédelmi incidensnek kell tekinteni az adatbiztonság olyan sérelmét, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.[78] Ez a fogalom meghatározás összhangban áll az Ibtv. által alkalmazott biztonsági esemény fogalmával (bővebben a 4. fejezetben), melyek együttes értelmezésével az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosítása – jogi szempontból – könnyebben elvégezhető.

3.2.3. Az adatkezelés elvei és jogalapja

Az Infotv. az előzőekben már említett OECD adatvédelmi alapelvek figyelembevételével főbb garanciális elemként a célhoz kötöttség elvét alkalmazza és rögzíti, hogy:

a) személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető,

b) az adatkezelés minden szakaszában meg kell felelni az adatkezelési célnak,

c) az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie,

d) csak az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas személyes adat kezelésére kerülhet sor,

e) a személyes adat kezelése nem haladhatja meg a cél megvalósulásához szükséges mértéket és időtartamot, azaz, ha az adatkezelés célja megszűnt, akkor a személyes adatot törölni kell.[79]

Az Infotv. a személyes adat adatkezelésre vonatkozó minőségi követelményeket is meghatározza, és rögzíti, hogy az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. E követelmény alapján az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. A törvény kimondja, hogy a személyes adat az adatkezelés során mindaddig megőrzi az adatok felvételével és kezelésével szemben támasztott tisztesség és törvényesség követelményét, amíg kapcsolata az érintettel helyreállítható, azaz ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

[77] Infotv. 3. § 9. és 18. pontok.

[78] Infotv. 3. § 26. pont.

[79] Infotv. 4. § (1)-(2) bekezdések.

Már a második generációs szabályozástól kezdve az adatvédelmi szabályok megalkotása során alapvetésként volt kezelve, hogy személyes adatok kezelésére kizárólag jogszabályban felsorolt jogalap alapján kerülhet sor, ezen jogalapok az Infotv.-ben természetszerűen megjelennek, melyek a következők:

a) *Az érintett hozzájárulása*. Az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez. Személyes adat akkor kezelhető, ha azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli, ennek hiányában hiányában az az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult, vagy az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.[80] Az előzetes tájékozódáshoz való jog érvényesülése érdekében az adatkezelő az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek megkezdését megelőzően vagy legkésőbb az első adatkezelési művelet megkezdését követően haladéktalanul az érintett rendelkezésére bocsátja az adatkezelő és - ha valamely adatkezelési műveletet adatfeldolgozó végez, az adatfeldolgozó - megnevezését és elérhetőségeit, az adatvédelmi tisztviselő nevét és elérhetőségeit, a tervezett adatkezelés célját és az érintettet e törvény alapján megillető jogok, valamint azok érvényesítése módjának ismertetését. Ezekkel egyidejűleg, azzal azonos módon vagy az érintettnek címzetten az adatkezelő az érintett számára tájékoztatást nyújt az adatkezelés jogalapjáról, a kezelt személyes adatok megőrzésének időtartamáról, ezen időtartam meghatározásának szempontjairól, a kezelt személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek - ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket - köréről, a kezelt személyes adatok gyűjtésének forrásáról és az adatkezelés körülményeivel összefüggő minden további érdemi tényről.[81] A különleges adatok kezelésének feltételeire vonatkozó szabályokat a GDPR 5., 6. és 9. cikke tartalmazza.

b) *Jogszabályon alapuló adatkezelés*. Személyes adat kezelését közérdekből törvény, valamint törvény felhatalmazása alapján kiadott helyi önkormányzati rendelet is előírhatja (kötelező adatkezelés).[82] A kötelező adatkezelés célját és egyéb feltételeit az adatkezelést elrendelő jogszabály határozza meg, de ez esetben is az adatkezelés csak a jogszabályban meghatározott célra, adatkörre és időtartamra terjedhet ki.

c) *Jogi kötelezettség teljesítésén, érdekérvényesítésen vagy nyilvánosságra hozatalon alapuló adatkezelés.* Személyes adat kezelhető akkor is, ha az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult. Továbbá, ha az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához, illetve megelőzéséhez szükséges és azzal arányos. Ezen kívül személyes adat kezelhető akkor, ha a személyes adatot az érintett kifejezetten nyilvánosságra hozta, valamint az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.[83]

[80] Infotv. 3. § 7. pont és 5. § (1) bekezdés b) pont.
[81] Infotv. 16.§ (1) és (2)
[82] Infotv. 5. § (1) bekezdés a) pont.
[83] Infotv. 5. § (1) bekezdés b)–d) pontok.

3.2.4. Az adattovábbítás feltételei[84]

Személyes adatot adatkezelő vagy adatfeldolgozó harmadik országban[85], továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő részére akkor továbbíthat, vagy harmadik országban adatfeldolgozást végző adatfeldolgozó részére akkor adhat át, ha:

a) ahhoz az érintett kifejezetten hozzájárult, vagy
b) az adattovábbítás az adatkezelés céljának eléréséhez szükséges, továbbá
c) más jogalapon alapuló adatkezelések esetén a harmadik országban az átadott adatok kezelése, valamint feldolgozása során biztosított a személyes adatok megfelelő szintű védelme.

A személyes adatok megfelelő szintű védelme akkor biztosított, ha:

a) az Európai Unió kötelező jogi aktusa azt megállapítja,
b) az érintetteknek jogai érvényesítésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés alkalmazandó Magyarország és azon harmadik ország, illetve nemzetközi szervezet között, amelynek joghatósága kiterjed a nemzetközi adattovábbítás címzettjére, vagy
c) a nemzetközi adattovábbítást megelőzően az adatkezelő a személyes adatok továbbításának valamennyi körülményét megvizsgálta és megállapította, hogy a személyes adatok megfelelő szintű védelme tekintetében megfelelő garanciák állnak fenn.[86]

Kiegészítő szabály, hogy az EGT-államba[87], valamint az Európai Unió működéséről szóló szerződés V. címének 4. és 5. fejezete szerint létrehozott ügynökségek, hivatalok és szervek részére irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor, azaz a fentiekben részletezett harmadik országba irányuló szabályok az Európai Unión belüli adattovábbításra, továbbá az EGT tagság miatt Izlandra, Lichtensteinre és Norvégiára nem vonatkoznak.

3.2.5. Az érintett jogai az adatkezeléssel kapcsolatban és azok érvényesítése

Az érintett részére a személyes adataik kezelésével összefüggésben biztosított jogok az adatkezelési folyamat összes elemére kiterjednek, melyek szabályai az alábbiak szerint összegezhetők. Az érintett jogosult arra, hogy:

a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (előzetes tájékozódáshoz való jog),
b) kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa (hozzáféréshez való jog),
c) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő helyesbítse, illetve kiegészítse (helyesbítéshez való jog),
d) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatai kezelését az adatkezelő korlátozza (az adatkezelés korlátozásához való jog),
e) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő törölje (törléshez való jog).[88]

---

[84] Infotv. 8. §.
[85] harmadik ország: minden olyan állam, amely nem EGT-állam (Infotv. 3. § 24. pont).
[86] Infotv. 10. § (4).
[87] *EGT-állam:* az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez. (Infotv. 3. § 23. pont).
[88] Infotv. 14. §.

Az adatkezelő az érintett jogai érvényesülésének elősegítése érdekében megfelelő műszaki és szervezési intézkedéseket tesz. Így különösen az érintett részére az Infotv.-ben nevesített esetekben nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti. Ezen kívül az érintett által benyújtott, az őt megillető jogosultságok érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb idő alatt, de legfeljebb 25 napon belül elbírálja és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.[89]

3.2.6. Az adatkezelés korlátai[90]

Az Infotv. rögzíti, hogy törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az adatkezelő személyes adatot úgy vehet át, hogy az adattovábbító adatkezelő vagy adatfeldolgozó az adattovábbítással egyidejűleg jelzi a személyes adat:

a) kezelésének lehetséges célját,
b) kezelésének lehetséges időtartamát,
c) továbbításának lehetséges címzettjeit,
d) érintettje e törvényben biztosított jogainak korlátozását, vagy
e) kezelésének egyéb feltételeit.

A személyes adatokat átvevő adatkezelő fenti adatkezelési korlátozásoknak megfelelő terjedelemben és módon köteles a személyes adatot kezelni és az érintett jogait megfelelően biztosítani. A fentiekben felsorolt adatkezelési korlátozásoktól eltérni csak az adatot továbbító adatkezelő előzetes hozzájárulásával lehet, ha az nem ütközik a Magyarország joghatósága alatt álló jogalanyok tekintetében alkalmazandó jogi rendelkezésbe. Az adatkezelőnek a személyes adat továbbításával egyidejűleg a címzettet kötelessége tájékoztatni az alkalmazandó adatkezelési korlátozásról.

3.2.7. Adatkezelő kötelezettségei

Az adatkezelő általános feladatairól az Infotv. külön alpontban rendelkezik. Az adatkezelő az adatkezelés által fenyegető kockázatokhoz igazodó műszaki és szervezési intézkedésekkel biztosítja az adatkezelés jogszerűségét, az érintettek alapvető jogainak érvényesülése érdekében. Ezen intézkedéseket az adatkezelő folyamatosan felülvizsgálja, és szükség esetén módosítja is.[91] Az intézkedéseket úgy kell kialakítani, hogy azok:

a) a tudomány és technológia mindenkori állásának és az intézkedések megvalósítása költségeinek figyelembevételével észszerűen elérhető módon a személyes adatok kezelésére vonatkozó követelmények, így különösen az adatkezelés alapelvei és az érintettek jogai hatékony érvényesülését szolgálják, valamint
b) alkalmasak és megfelelőek legyenek annak biztosítására, hogy alapértelmezés szerint
  ba) kizárólag olyan és annyi személyes adat kezelésére kerüljön sor, olyan mértékben és időtartamban, amely az adatkezelés célja szempontjából szükséges, és
  bb) az adatkezelő által kezelt személyes adatok az érintett erre irányuló kifejezett akarata hiányában ne válhassanak nyilvánosan hozzáférhetővé.[92]

[89] Infotv. 15. § (1) bekezdés.
[90] Infotv. 9. §.
[91] Infotv. 25/A. § (1) bekezdés.
[92] Infotv. 25/A. § (2) bekezdés.

3.2.8. Az adatok feldolgozására vonatkozó szabályok, az adatfeldolgozó

Az adatfeldolgozóra vonatkozó jogokat és kötelezettségeket az Infotv. önálló alcím alatt, generális jelleggel tartalmazza, kiegészítő szabályként felhívva a külön ágazati törvényeket, azzal, hogy főszabályként rögzíti, az adatkezelő az általa adott utasítások jogszerűségéért és az érintettek jogai védelmének biztosítására alkalmas műszaki és szervezési intézkedések végrehajtásáért felel.

Az adatfeldolgozó további adatfeldolgozót kizárólag akkor vehet igénybe, ha azt jogszabály nem zárja ki, illetve, ha az adatkezelő ehhez előzetesen közokiratban vagy teljes bizonyító erejű magánokiratban eseti vagy általános felhatalmazást adott. Az adatkezelő és az adatfeldolgozó közötti jogviszony részletes tartalmát az Infotv.-ben, valamint az Európai Unió kötelező jogi aktusában meghatározott keretek között jogszabály vagy az adatkezelő és az adatfeldolgozó között írásban létrehozott szerződés határozza meg. Ezen szerződésben rendelkezni kell különösen az adatkezelő azon kötelezettségéről, hogy:

a) tevékenysége során kizárólag az adatkezelő írásbeli utasítása alapján jár el,
b) tevékenysége során biztosítja azt, hogy az érintett személyes adatokhoz való hozzáférésre feljogosított személyek az általuk megismert személyes adatok vonatkozásában titoktartási kötelezettséget vállaljanak,
c) tevékenysége során minden megfelelő eszközzel segíti az adatkezelőt az érintettek jogai érvényesítésének elősegítése, ezzel kapcsolatos kötelezettségei teljesítése érdekében,
d) az adatkezelő választása szerint az általa végzett adatkezelési műveletek befejezését követően – ha törvény másként nem rendelkezik – vagy haladéktalanul törli a tevékenysége során megismert személyes adatokat, vagy továbbítja azokat az adatkezelőnek és azt követően törli a meglévő másolatokat,
e) az adatkezelő rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozó igénybevételére vonatkozó jogi rendelkezéseknek való megfelelés igazolásához szükséges, valamint
f) további adatfeldolgozót csak az e törvényben meghatározott feltételek teljesítése mellett vesz igénybe.[93]

3.2.9. Az adatkezelői, adatfeldolgozói nyilvántartás és az elektronikus napló

Az adatkezelő a kezelésében lévő személyes adatokkal kapcsolatos adatkezeléseiről, az adatvédelmi incidensekről és az érintett hozzáférési jogával kapcsolatos intézkedésekről nyilvántartást vezet. Ebben az adatkezelőnek rögzítenie kell:

a) az adatkezelő(k), valamint az adatvédelmi tisztviselő nevét és elérhetőségeit,
b) az adatkezelés célját vagy céljait,
c) személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek körét,
d) az érintettek, valamint a kezelt adatok körét,
e) profilalkotás alkalmazása esetén annak tényét,
f) nemzetközi adattovábbítás esetén a továbbított adatok körét,
g) az adatkezelési műveletek jogalapjait,
h) ha az ismert, a kezelt személyes adatok törlésének időpontját,
i) a végrehajtott műszaki és szervezési biztonsági intézkedések általános leírását,
j) az általa kezelt adatokkal összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és a kezelésükre tett intézkedéseket,
k) az érintett hozzáférési jogának érvényesítését e törvény szerint korlátozó vagy megtagadó intézkedésének jogi és ténybeli indokait.[94]

[93] Infotv. 25/D. § (3) bekezdés.
[94] Infotv. 25/E. § (1) bekezdés.

Az adatfeldolgozó az általa végzett adatkezelésekről nyilvántartást vezet (a továbbiakban: adatfeldolgozói nyilvántartás). Az adatfeldolgozói nyilvántartásban az adatfeldolgozó rögzíti:

a) az adatkezelő, az adatfeldolgozó, a további adatfeldolgozók, valamint az adatfeldolgozó adatvédelmi tisztviselőjének nevét és elérhetőségeit;
b) az adatkezelő megbízásából vagy rendelkezése szerint végzett adatkezelések típusait;
c) az adatkezelő kifejezett utasítására történő nemzetközi adattovábbítás esetén a nemzetközi adattovábbítás tényét, valamint a címzett harmadik ország vagy nemzetközi szervezet megjelölését;
d) az Infotv. szerint végrehajtott műszaki és szervezési biztonsági intézkedések általános leírását.[95]

Az adatkezelői és az adatfeldolgozói nyilvántartást írásban vagy elektronikus úton rögzített formában kell vezetni és azt – kérésére – a Nemzeti Adatvédelmi és Információszabadság Hatóság rendelkezésére kell bocsátani.[96]

A személyes adatokkal elektronikus úton végzett adatkezelési műveletek jogszerűségének ellenőrizhetősége céljából az adatkezelő és az adatfeldolgozó automatizált adatkezelési rendszerben (a továbbiakban: elektronikus napló) rögzíti az adatkezelési művelettel érintett személyes adatok körének meghatározását, az adatkezelési művelet célját és indokát, az adatkezelési művelet elvégzésének pontos időpontját, az adatkezelési műveletet végrehajtó személy megjelölését, valamint a személyes adatok továbbítása esetén az adattovábbítás címzettjét.

Az elektronikus naplóban rögzített adatok kizárólag az adatkezelés jogszerűségének ellenőrzése, az adatbiztonsági követelmények érvényesítése, továbbá büntetőeljárás lefolytatása céljából ismerhetőek meg és használhatóak fel.[97]

3.2.10. Az adatvédelmi hatásvizsgálat

Az adatkezelő a tervezett adatkezelés megkezdése előtt felméri, hogy az adatkezelés annak körülményeire várhatóan milyen hatásokat fog gyakorolni. Ha a kockázatbecslés eredményeként valószínűsíthető, hogy az adatkezelés az érintetteket megillető, valamely alapvető jog érvényesülését lényegesen befolyásolja, akkor írásbeli elemzést kell készíteni a várható hatásokról. Abban az esetben, ha a tervezett adatkezelés vonatkozásában lefolytatott adatvédelmi hatásvizsgálat eredménye alapján az adatkezelés magas kockázatú lenne, vagy vélelmezni kell, hogy magas kockázatú lenne, akkor az adatkezelőnek vagy az adatfeldolgozónak az adatkezelés megkezdését követően konzultációt kell kezdeményeznie a Hatósággal. A Hatóság az előzetes konzultáció kezdeményezésétől számított hat héten belül, írásban reagál.[98]

3.2.11. Az adatbiztonságra vonatkozó szabályok[99]

Az adatbiztonság követelményeinek törvényi feltételei garantálják az adatkezelés teljesítése során felmerült kockázatok kezelését. Az Infotv. önálló alcímben szabályozza az adatbiztonság követelményét, rögzíti az adatkezelő és az adatfeldolgozó azon kötelezettségét, amely az adatkezelési műveletek olyan formában történő megtervezésére és végrehajtására vonatkozik, amely az Infotv. és az

[95] Infotv. 25/E. § (2) bekezdés.
[96] Infotv. 25/E. § (3) bekezdés.
[97] Infotv. 25/F. § (1)–(2) bekezdés.
[98] Infotv. 25/G. § (1)–(5) bekezdések.
[99] Infotv. 25/I. §.

adatkezelésre vonatkozó más szabályok alkalmazása során biztosítja az érintett magánszférájának védelmét. Az adatok biztonságáról az adatkezelő és az adatfeldolgozó is köteles gondoskodni, illetve köteles megtenni azokat a technikai és szervezési intézkedéseket, továbbá kialakítani azokat az eljárási szabályokat, amelyek az Infotv., valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az Infotv. rögzíti, hogy az adatkezelő és tevékenységi körében az adatfeldolgozó szervezési és műszaki intézkedésekkel biztosítja:

a) az adatkezeléshez használt eszközök (a továbbiakban: adatkezelő rendszer) jogosulatlan személyek általi hozzáférésének megtagadását,
b) az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását,
c) az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását,
d) az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását,
e) azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá,
f) azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére,
g) azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban, ki vitt be az adatkezelő rendszerbe,
h) a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását,
i) azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen, valamint
j) azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.[100]

A védelmet erősíti az a követelmény is, amely a különböző nyilvántartásokban elektronikusan kezelt adatállományokra vonatkozóan rögzíti, hogy a nyilvántartásokban tárolt adatok esetében megfelelő technikai megoldással biztosítani kell, hogy azok közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők. Az összekapcsolás és összerendelést kizárólag törvényi előírás teheti lehetővé.

Elvi jelleggel került megállapításra, hogy mind az adatkezelőnek, mind az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére és több lehetséges adatkezelési megoldás közül azt kell választaniuk, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséggel járna. Ez a szabály a technológiasemlegesség követelményének érvényre juttatását célozza.

3.2.12. Az adatvédelmi incidens

Az adatkezelő és az adatfeldolgozó által kezelt adatokkal összefüggésben felmerült adatvédelmi incidens kapcsán rögzíti a kapcsolódó információkat, valamint az adatvédelmi incidenst haladéktalanul,

[100] Infotv. 25/I. § (3) bekezdés.

de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő hetvenkét órán belül bejelenti a Hatóságnak. Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére. A bejelentési kötelezettség magában foglalja, hogy az adatkezelő:

a) ismerteti az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és hozzávetőleges számát, valamint az incidenssel érintett adatok körét és hozzávetőleges mennyiségét,
b) tájékoztatást nyújt az adatvédelmi tisztviselő vagy a további tájékoztatás nyújtására kijelölt más kapcsolattartó nevéről és elérhetőségi adatairól,
c) ismerteti az adatvédelmi incidensből eredő, valószínűsíthető következményeket, valamint
d) ismerteti az adatkezelő által az adatvédelmi incidens kezelésére tett vagy tervezett intézkedéseket.[101]

3.2.13. Az adatvédelmi tisztviselő

Az adatkezelőnek és az adatfeldolgozónak az adatkezelés jogszerűsége és az érintettek jogai érvényesülésének elősegítése céljából adatvédelmi tisztviselőt kell alkalmaznia, ha az adatkezelő, illetve az adatfeldolgozó állami feladatot vagy jogszabályban meghatározott egyéb közfeladatot lát el – kivéve a bíróságokat –, vagy ha törvény vagy az Európai Unió jogi aktusa azt előírja.[102]

Adatvédelmi tisztviselőnek az jelölhető ki, aki a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik és alkalmas az Infotv.-ben nevesített feladatainak ellátására.[103]

Az adatvédelmi tisztviselő feladata sokrétű. Elősegíti az adatkezelő, illetve az adatfeldolgozó kötelezettségeinek teljesítését, így különösen:

a) a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és azok érvényesítésének módjaival kapcsolatban tanácsot ad az adatkezelési műveleteket végző személyek részére;
b) folyamatosan figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogi előírások érvényesülését;
c) elősegíti az érintettet megillető jogok gyakorlását;
d) szakmai tanácsadással elősegíti és figyelemmel kíséri az adatvédelmi hatásvizsgálat lefolytatását,
e) együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel;
f) közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában.[104]

3.2.14. A Nemzeti Adatvédelmi és Információszabadság Hatóság feladat- és hatásköre

A Nemzeti Adatvédelmi és Információszabadság Hatóság autonóm államigazgatási szerv, melynek feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése, továbbá a személyes adatok Európai Unión belüli szabad áramlásának biztosítása.[105]

[101] Infotv. 25/J. § (5) bekezdés.
[102] Infotv. 25/L. § (1) bekezdés.
[103] Infotv. 25/L. § (4) bekezdés.
[104] Infotv. 25/M. § (1) bekezdés.
[105] Infotv. 38. § (1) bekezdés.

A Hatóság független, csak a törvénynek van alárendelve, feladatkörében nem utasítható, a feladatát más szervektől elkülönülten, befolyásolástól mentesen látja el. A Hatóság számára feladatot csak törvény állapíthat meg.[106]

A Hatóság feladatkörében:

a) bejelentés alapján és hivatalból vizsgálatot folytat;
b) az érintett kérelmére és hivatalból adatvédelmi hatósági eljárást folytat;
c) hivatalból titokfelügyeleti hatósági eljárást folytat;
d) a közérdekű adatokkal és a közérdekből nyilvános adatokkal kapcsolatos jogsértéssel összefüggésben bírósághoz fordulhat;
e) a más által indított perbe beavatkozhat;
f) kérelemre adatkezelési engedélyezési eljárást folytat;
g) ellátja az Európai Unió kötelező jogi aktusában, így különösen az általános adatvédelmi rendeletben és a 2016/680 (EU) irányelvben a tagállami felügyeleti hatóság részére megállapított, továbbá a törvényben meghatározott egyéb feladatokat.
h) javaslatot tehet a személyes adatok kezelését, valamint a közérdekű adatok és a közérdekből nyilvános adatok megismerését érintő jogszabályok megalkotására, illetve módosítására, véleményezi a feladatkörét érintő jogszabályok tervezetét;
i) tevékenységéről minden évben március 31-éig beszámolót hoz nyilvánosságra és a beszámolót benyújtja az Országgyűlésnek;
j) általános jelleggel vagy meghatározott adatkezelő részére ajánlást bocsát ki;
k) véleményezi a közfeladatot ellátó szerv tevékenységével kapcsolatosan a különös, illetve egyedi közzétételi listákat;
l) törvényben meghatározott szervekkel vagy személyekkel együttműködve képviseli Magyarországot az Európai Unió közös adatvédelmi felügyelő testületeiben;
m) megszervezi az adatvédelmi tisztviselők konferenciáját.[107]

A Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll. A bejelentés miatt senkit sem érhet hátrány, a bejelentő kilétét a Hatóság csak akkor fedheti fel, ha ennek hiányában a vizsgálat nem lenne lefolytatható. Ha a bejelentő kéri, kilétét a Hatóság akkor sem fedheti fel, ha ennek hiányában a vizsgálat nem folytatható le – erről a következményről a Hatóság a bejelentőt köteles tájékoztatni.[108] A Hatóság a bejelentést köteles érdemben megvizsgálni, kivéve az Infotv.-ben előírt eseteket.[109]

---

[106] Infotv. 38. § (5) bekezdés.
[107] Infotv. 38. § (4) bekezdés.
[108] Infotv. 52. §.
[109] Infotv. 53. § (2) – (3) bekezdések.
A Hatóság a bejelentést érdemi vizsgálat nélkül elutasíthatja, ha
a) a bejelentésben megjelölt jogsérelem csekély jelentőségű, vagy
b) a bejelentés névtelen.
A Hatóság a bejelentést érdemi vizsgálat nélkül elutasítja, ha
a) az adott ügyben bírósági eljárás van folyamatban, vagy az ügyben korábban jogerős bírósági határozat született,
b) ha a Hatóság vizsgálat le nem folytathatóságára vonatkozó tájékoztatás ellenére a bejelentő továbbra is kéri, hogy a kilétét ne fedjék fel,
c) a bejelentés nyilvánvalóan alaptalan,
d) az ismételten előterjesztett bejelentés érdemben új tényt, adatot nem tartalmaz,
e) a bejelentést határidőn túl nyújtották be.

A Hatóság a vizsgálat során:

a) a vizsgált adatkezelő kezelésében levő, a vizsgált üggyel összefüggésbe hozható összes iratba betekinthet, illetve azokról másolatot kérhet,
b) a vizsgált üggyel összefüggésbe hozható adatkezelést megismerheti, az adatkezelés helyszínéül szolgáló helyiségbe beléphet,
c) a vizsgált adatkezelőtől, illetve az adatkezelő bármely munkatársától írásbeli és szóbeli felvilágosítást kérhet,
d) a vizsgált üggyel összefüggésbe hozható bármely szervezettől vagy személytől írásbeli felvilágosítást, illetve a vizsgált üggyel összefüggésbe hozható iratról másolatot kérhet, és
e) az adatkezelő hatóság felügyeleti szervének vezetőjét vizsgálat lefolytatására kérheti fel.[110]

A vizsgálat végeztével – a bejelentés érkezésétől számított 2 hónapon belül – a Hatóság:

a) ha a bejelentést megalapozottnak tartja:
   a. felszólítja az adatkezelőt a jogsérelem orvoslására, illetve annak közvetlen veszélye megszüntetésére, amelynek megtételéről, vagy arról, hogy az abban foglaltakkal nem ért egyet, az adatkezelő 30 napon belül köteles a Hatóságot tájékoztatni, és ha a felszólítás nem jár eredménnyel a Hatóság ajánlást tehet a szerv felügyeleti szervének;
   b. nyilvános jelentést készíthet az ügyről;
   c. adatvédelmi hatósági eljárást, vagy
   d. titokfelügyeleti hatósági eljárást indít.
b) ha a bejelentésben foglaltakat nem tartja megalapozottnak, a vizsgálatot lezárja.[111]

A Hatóság a vizsgálat eredményeként ajánlást tehet jogszabályalkotásra, illetve a közjogi szervezetszabályozó eszköz kiadására jogosult szervnek, illetve a jogszabály előkészítőjének a jogszabály, illetve a közjogi szervezetszabályozó eszköz módosítására, hatályon kívül helyezésére vagy megalkotására, ha a jogsérelem, illetve annak közvetlen veszélye valamely jogszabály vagy közjogi szervezetszabályozó eszköz fölösleges, nem egyértelmű vagy nem megfelelő rendelkezésére, illetve az adatkezeléssel összefüggő kérdések jogi szabályozásának hiányára vagy hiányosságára vezethető vissza.[112]

Az adatvédelmi hatósági eljárás megindításának feltétele, hogy valószínűsíthető az, hogy a személyes adatok jogellenes kezelése, és a jogellenes adatkezelés személyek széles körét érinti vagy nagy érdeksérelmet vagy kárveszélyt idézhet elő.[113]

A NAIH az általános adatvédelmi rendeletben meghatározott jogkövetkezményeket alkalmazhatja. Az adatvédelmi hatósági eljárás jogkövetkezménye lehet:[114]

a) a személyes adatok jogellenes kezelésének megállapítása,
b) a valóságnak nem megfelelő személyes adat helyesbítésének elrendelése,
c) a jogellenesen kezelt vagy feldolgozott személyes adatok zárolásának, törlésének vagy megsemmisítésének elrendelése,
d) a személyes adatok jogellenes kezelésének vagy feldolgozásának megtiltása,
e) a személyes adatok külföldre történő továbbításának vagy átadásának megtiltása,
f) az érintett tájékoztatásának elrendelése, ha azt az adatkezelő jogellenesen mellőzte vagy tagadta meg,
g) bírság kiszabása, valamint
h) határozat – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalának elrendelése, ha azt az adatvédelem érdekeinek, illetve nagyobb számú érintett jogainak védelme ezt megköveteli.

[110] Infotv. 54. § (1) bekezdés.
[111] Infotv. 55. §, 56. §, 58. §.
[112] Infotv. 57. §.
[113] Infotv. 60. §.
[114] Infotv. 61. § (1)-(3) bekezdések.

Az Infotv. rövid bemutatását követően is jól látható, hogy az adatvédelmi célkitűzésekhez általános jogi kereteket ad, a védelem formáját és ezzel összefüggésben a technológia kiválasztását az adatkezelőre bízza, még akkor is, ha a személyes adatok vonatkozásában az adatkezelő által teljesítendő egyes biztonsági elvárásokat rögzíti. Az adatkezelő ebből adódóan köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az az Infotv. és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Az elektronikus információbiztonság szabályozása az általános kereteken túlmutat, ezen esetekben a speciális szabályokat az elektronikus információs rendszer biztonságára és ezekben a rendszerekben kezelt adatok védelmére vonatkozóan az Ibtv. és végrehajtási rendeletei tartalmazzák, melyek hozzájárulnak az adatbiztonság szintjének növeléséhez, különös tekintettel az elektronikus információs rendszerekben tárolt személyes adatok kezelése esetén.

4. Jövőbeni kihívások és lehetőségek

Az okostelefonok (mobileszközök) adatvédelmi és információbiztonsági kockázata – ahogy azt a bevezetőben már említettük – alapvetően két tényezőre vezethető vissza: az egyik hogy hogyan és mire használjuk az eszközt, a másik, hogy milyen szolgáltatásokat szeretnénk elérni azzal. A hogyan és mire használjuk az eszközt, alapvetően felhasználói magatartásra és biztonságtudatosságra vezethető vissza, amely elsődlegesen nem a szabályozás oldaláról, hanem a tudatosítás és a képzés oldaláról igényel törekvéseket (bár kétségtelen, hogy szabályozási alapok nélkül nem megy). Alapvető probléma, hogy a felhasználók nincsenek felkészítve a technológiai fejlődésből eredő biztonsági kockázatokra. Már egy 2011-es felmérés során is kimutatták, hogy bár a felhasználók aggódnak az okostelefonon tárolt adataik biztonságáért, a védelmi intézkedések körével és a lehetőségekkel azonban nincsenek tisztában.[115] A szolgáltatások igénybevételével járó veszélyek túlmutatnak a biztonságtudatosságon, a külső és belső intézményi információk, továbbá az új és újabb alkalmazások igénye a véletlen adatvesztéstől kezdve egészen a szándékos adatszivárgásig biztonsági kockázatot jelent. A mobil alkalmazások fejlesztésénél ezért előtérbe kell helyezni a felhasználók azonosítását és a jogosultságkezelését. Meg kell valósítani a magán és üzleti adatok elkülönítését és védelmét, az eszközök, alkalmazások, felhasználók központi adminisztrációját és támogatását, az intraneten futó alkalmazások biztonságos elérését és használatát. Mindezt hogyan támogatja a – fentiekben bemutatott – szabályozási környezet?

A szabályozási környezetből jól érzékelhető, hogy a stratégiai szintű, hosszú távú tervezés mind a nemzeti, mind a nemzetközi szinten kiemelkedő eredményeket mutat. Ez a hosszú távú tervezés a 2014-2020 közötti fejlesztési időszakban megjelenő források lehívásával váltható „aprópénzre”. A „beváltás” feltétele a törvényi szintű szabályozás jelenleg meglévő keretszabályainak specializálása, az ágazati szabályzók kiegészítése. Mindezt úgy szükséges kodifikálni, hogy a jelenlegi szabályozással elért eredmények mind az adatvédelem – különös tekintettel a nemzeti adatvagyon védelmére – mind az információbiztonság tekintetében továbbra is érvénybe maradjanak, és az újonnan megjelenő technológiai kihívásokhoz, valamint a biztonsági kockázatokhoz igazodjanak.

Fontos, hogy:

a) az okostelefonunkon tárolt és felhasznált adatokat minősítsük és szűrjük,
b) személyes és különleges adatot csak az Infotv. szabályrendszere alapján, megfelelő, az Ibtv. által biztonsági osztályba sorolt elektronikus információs rendszeren kezeljük,
c) a meglévő és védett adatvagyon tekintetében ne használjunk olyan alkalmazásokat, amelyek sérülékenyek.

[115] www.fudzilla.com Smartphone users fear data loss – 2011.06.09.

Releváns változást az általános adatvédelmi rendelet 2018. május 25-től kötelező alkalmazása hozhat, amely az adatkezelők kötelezettségeként írja elő és felelősségi körükbe helyezi a megfelelő eljárásrendek, szabályzatok elfogadását és a biztonság garantáláshoz szükséges adatbiztonsági intézkedések megtételét. Emellett szükséges továbbá a technológiai szabályok ismételt megjelenése is (vö. 3. fejezet az első generációs adatvédelmi szabályozásnál leírtak), mivel a biztonsági kockázatok csökkenthetők azáltal, ha megfelelően van szabályozva – mind jogi, mind műszaki megvalósítás szempontjából – az, hogy a mobil alkalmazás:

a) csak a szükséges és engedélyezett adatot tölti (töltheti) le – vö. célhoz kötöttség elve és információbiztonsági szempontok,
b) minimalizálja az adatforgalmat, ezáltal csökkenti a várakozási időt,
c) minél nagyobb mennyiségű személyes adatot kezel és magasabb a biztonsági osztályba sorolt értéke jelszó alapú hitelesítést követeljen meg.

Nem szabad figyelmen kívül hagyni, hogy személyes adatot felvenni és felhasználni alapesetben csak az érintett beleegyezésével szabad, úgy, hogy az adatfeldolgozás útját az érintett részére követhetővé és ellenőrizhetővé kell tenni. Alapvetés, hogy mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel a személyes adatát. Ezen elvek a mobileszközök, különös tekintettel az okostelefonok világában fokozottan kell, hogy érvényesüljenek, hiszen az okostelefonokon rengeteg személyes adatot és információt tárolunk. Gondoljunk csak arra, hogy hogyan és mennyire biztosítható a magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten. Hogyan tud érvényesülni a szolgáltatóknál az, hogy az érintett jogai védelme érdekében a személyes adatainak helyesbítését, azok törlését vagy zárolását kérje, feltételezve, hogy a személyes adat kezelésének jogalapja biztosított. Ha a felhasználók tudatosítása nem kap kiemelt figyelmet, nem biztosít megfelelő sikereket.

A jogi keretek adottak, azonban a jelenlegi szabályozások mentén sok tényező határozza meg azt, hogy a jogérvényesítésre mikor és mely személy vagy szerv által, és szükség esetén a megfelelő szankciók alkalmazásával kerülhet sor.

5. Felhasznált irodalom

- Halmai Gábor – Tóth Gábor Attila (szerk.) (2003): Emberi jogok. Osiris Kiadó, Budapest.
- Jóri András (2005): Adatvédelmi kézikönyv. Osiris Kiadó, Budapest.
- Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz (2016). Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest.

6. Jogszabályok jegyzéke

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- A nemzeti adatvagyonról szóló 2021. évi XCI. törvény
- A Büntető Törvénykönyvről szóló 2012. évi C. törvény
- Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat
- Az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér” című közös közleménye

7. Felhasznált internetes források jegyzéke

- http://eur-lex.Európa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF
- http://ec.Európa.eu/europe2020/who-does-what/index_hu.htm

III. BÁNYÁSZ PÉTER: AZ OKOS MOBIL ESZKÖZÖK JELENTETTE KIBERBIZTONSÁGI KIHÍVÁSOK

Napjainkban az okos mobil eszközök használata majdhogynem evidensnek tekinthető. A *Bevezető az okos mobil eszközök világába* címet viselő tananyagban ismertetett Gartner jelentés, ami az okostelefonok eladást és piaci részesedést vizsgálta, kiderült, hogy 2016. második negyedévében összesen 344 millió okostelefont értékesítettek globálisan, ami 4,3 százalékos növekedést jelent a 2015-ös év azonos időszakához képest.[116] Az okostelefon piac meghatározó szereplője az Android, amely 86,2 százalékos piaci részesedést tudhat magának. Az Android mögött messze lemaradva található az iOS, amely a piac 12,9 százalékát adja.

A fenti számok kizárólag okostelefonokra vonatkoznak, nem tartalmazzák a tabletek és más okoseszközök eladási mutatóit. Az okostelefonok ilyen fokú elterjedéséhez nagyban hozzájárult – az új technológiák térhódítása mellett – az alkalmazások használatában levő kényelem, egyszerű kezelhetőség. Az okos mobil eszközökre írt alkalmazások számos olyan funkcióval rendelkeznek, amelyek nagyban megkönnyítik mindennapjainkat, hatékonyabb életvezetést biztosítanak számunkra. Az Ericsson 2013 októberében publikált[117] egy közvélemény kutatást, amely 7500 nagyvárosi okostelefon használót, 15-69 év közti személyt szólított meg. A kutatás egyik jelentős megállapítása, hogy a felhasználók a felmerülő problémák megoldását a technikától várják, egy okostelefonra készített alkalmazás segítségével. Legyen szó idősgondozásról, vásárlásról, közösségi közlekedésről, hivatali ügyintézésről, a megkérdezettek többsége ezeket az ügyeket egy direkt ilyen célra optimalizált alkalmazással kívánja elvégezni.

Az új technológia azonban egyúttal számos új típusú kihívást is magával hozott, amelyekre a felhasználók jelentős része nem készült fel, így igen komoly veszélyeknek teszi ki magát. Az által, hogy az okostelefonjaink szinte eggyé váltak velünk, a használókkal, az eszközök fenyegetettsége egyúttal a mi veszélyezettségünket is fokozatosan növeli.

Jelen tananyag célja, hogy növelje a felhasználók okos mobil eszközökre vonatkozó adat- és információ érzékenységét, segítsen abban, hogy tudatosabbak legyenek, hiszen ahogy a későbbiekben látni fogjuk, igen komoly kockázatai lehetnek az óvatlan eszközhasználatnak. Az egyszerűség miatt okos mobil eszköz alatt e tanulmány alapvetően az okostelefonok és tableteket érti, mivel a közigazgatásban ezek jelentősek, de számos téren kiterjeszthetőek a bemutatott koncepciók egyéb okoseszközökre is, mint például az órák, okosmérők vagy háztartási eszközök.

---

[116] Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016, In Press Release, 2016. augusztus 19., http://www.gartner.com/newsroom/id/3415117 (2016. szeptember 5.)

[117] Ericsson Consumerlab: Smarthphones Change Citys, Ericsson Consumer Insight Summary Report, 2013. október, http://www.ericsson.com/res/docs/2013/consumerlab/smartphones-change-cities.pdf (utolsó letöltés: 2016. szeptember 5.)

1. Kiberfenyegetettségek osztályozása

A *Bevezető az okos mobil eszközök világába* címet viselő tananyagban az Olvasó már szembesült az okostelefon definíciós nehézségeivel, ebben a fejezetben egy közös jellemzőt azonban ki kell ragadnunk. Nevezetesen, bár internetkapcsolat nélkül is használhatóak az okos mobil eszközök, akárcsak elődjeik, de az igazán hatékony működés megköveteli mobil- vagy vezeték nélküli internet használatát. Azáltal, hogy csatlakozunk a kibertérhez, számos támadási felületet nyújtunk.

A kibertér kifejezést William Gibson sci-fi író használta először az 1982-ben megjelent Izzó króm című novellájában, majd az 1984-es Neurománc című regényében, és innen szivárgott át a köztudatba. Gibson a kibertér fogalma alatt hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális teret értett.[118] A kibertér kifejezés a görög kyber (hajózni) szóból származik, és hajózásra alkalmas teret jelent. A Neurománc óta különböző fogalmi meghatározások születtek a kibertérre, de földrajzi értelemben az infokommunikációs technológiákban megnyilvánuló térfogalmat jelent, nem pedig a technológiára utal.

A kibertér térszerkezetének leírására számos kísérlet született geometriai, formai, szerkezeti jellemzőinek meghatározásával. A térgeometriai jellemzők feltárása azonban nem egyszerű, hiszen a kibertér számos különböző, eltérő funkciójú tartományból tevődik össze, illetve mindegyike mesterségesen konstruált. A különböző térfelfogásokat az alapján alkották meg, hogy a fogalom használói a kibertér mely csoportjával foglalkoztak.[119] Ez alapján beszélünk:

- Koncepcionális térfelfogásról: ez esetben az IKT önálló belső terét értjük, az internetet és annak alkotó térrészeit, például e-mailek tere, a fájl átvitel tere. Ebben az értelmezésben az internet az abszolút kibertér.
- Infrastrukturális térfelfogásról: e felfogás alapján a kibertér leginkább fizikai megközelítése áll, azokat a háttérben meghúzódó infrastrukturális elemeket értik, amelyeken a virtuális interakciók lezajlanak- szerverek, gerincvezetékek, optikai kábelek stb.
- Oldaltérképek terei: nagyban hasonlatos a könyvekben található tartalomjegyzékekhez. Az oldal térképek egyfajta modellezési eljárások, a honlapokon elhelyezett útmutatók, amelyek a honlap tartalmában segítenek eligazodni a felhasználóknak. Ez esetben már nem beszélhetünk semmiféle fizikai leképzésről, földrajzi lokalizációról, kizárólag a virtuális térben értelmezhető.
- A sajátos „páva" modellek terei: az egyik legelvontabb térfelfogás, amelynek a lényege, hogy egy nyomkövető eljárással az információs csomagok útvonalát követik a hálózatban (kiindulási ponttól a célig), majd ezeket vizuális módon faszerkezethez vagy pávatollhoz hasonló ábrán jelenítik meg. Az eljárás célja, hogy az internet belső szerkezetét térképezze fel. Maga a páva térkép az internethez hasonlóan folyamatosan változik, hol bővül, hol szűkül, így a teljes feltérképezés megoldhatatlan feladatnak bizonyul. A páva modell térszerkezet már önálló belső teret alkot, híján minden fizikai kapcsolatnak.
- Virtuális világok: maga a fogalom egy erőteljes szűkítés az internethez képest, digitális technológiával létrehozott világot jelent, az általa képzett perceptualitást értjük alatta. Megalkotása mögött az az egyszerű igény húzódik meg, hogy az információ könnyebben kezelhetővé váljon. Sajátosságának tekinthető, hogy a digitális környezetben a felhasználó is jelen van. A virtuális valóság eszköze lehet például az okosszemüveg.

[118] Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése, In Magyar Tudomány, 2001/7., pp. 769–779., 2001.

[119] Jakobi Ákos: A virtuális világ terei – Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése" című tanulmányához, In *Magyar Tudomány*, 2002/11., pp. 1482–1491., 2002.

Bár a kibertér szakít a klasszikus térfelfogással, mivel számos fizikai alapvonást nem képes értelmezni, amelyek hatására a tér halmazt alkot, mégis felfedezhetőek bizonyos térszerkezeti elemek, de teljesen új interpretációt jelentve a virtuális térben. Ilyen kategóriaként értelmezhető a külső és belső tér, a hely, a helyzet, a távolság, az irány, a határ, illetve a különböző szintek. A kibertér definiálására a magyar stratégiai gondolkodásban is születtek kísérletek. A Magyarország Nemzeti Kiberbiztonsági Stratégiája a következő megfogalmazást tartalmazza: „*A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.*”[120]

Resperger István megfogalmazása szerint „*A biztonsági kockázatot az általános meghatározásból következően, a biztonsági dimenziók vonatkozásában értelmezhetjük. A fenyegetés a veszély konkrét, cselekvési szándékot is megjelenítő formája.*”[121] A fenyegetések az általánosan értelmezett biztonság egyes összetevőire ható helyzetek és állapotok összessége a lehetséges veszélyek legmagasabb megnyilvánulási szintjét tekintve.

A szakirodalom napjainkban a kiberfenyegetettségek négy típusát különbözteti meg, amelyek nem csak az elkövetés módja, de motivációja szerint is eltérnek.

Az első kategóriába a kiberbűnözés, amelynek a célja, hogy informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket. Az EUROPOL minden évben közzéteszi jelentését az internetes szervezett bűnözés általi fenyegetettségről. Ez alapján 2015-ben az alábbi területeket azonosították:[122]

1. Malwarekkel[123] (például CryptoLocker, CTB-LOCKER stb.) való visszaélés.[124]
2. Gyerekek szexuális kizsákmányolása;[125]
3. Fizetőeszközzel elkövetett csalás;[126]
4. Social engineering;
5. Adatok megszerzése, hálózatok támadása;[127]
6. Létfontosságú rendszerelemek ellen elkövetett támadások;
7. Különböző pénzügyi tevékenységek (criminal-to-criminal payments, payment for legitimate services, victim payments);
8. Online kommunikáció;

[120] 1139/2013, (III. 21.) Korm. határozat Magyarország Nemzet Kiberbiztonsági stratégiájáról, In *Magyar Közlöny*, 2013/47.

[121] RESPERGER István: Kockázatok, kihívások, fenyegetések a XXI. században. Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest, 2002.

[122] The 2015 Internet Organised Crime Threat Assessment (IOCTA), Europol, Hága, 2015., https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (2016. szeptember 20.)

[123] Az angol malware kifejezés az angol malicious software (rosszindulatú szoftver, káros szoftver, kártékony szoftver) összevonásából kialakított mozaikszó. Ide tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit). Az informatikai eszközökre írt kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el.

[124] Az idézett jelentés szerint az egyik legnagyobb kockázat a rosszindulatú programok esetében a zsarolóvírusok elterjedése, amelyek titkosítják a megfertőzött eszköz filejait, és a feloldásért cserében pénzt követelnek.

[125] Ez esetben alapvetően a Darkneten zajló illegális kereskedelmet kell érteni, amely a gyermekprostítúciótól kezdve a gyermekporográfia tartalmakon át a gyermekek szexrabszolga-kereskedelmét foglalja magában.

[126] Alapvetően az ATM-ekkel kapcsolatos csalások tartoznak ide.

[127] Piaci, állami szereplők adatbázisaiba történő behatolás, szolgáltatók elleni DoS,DDoS támadások.

9. Darknet;[128]
10. Internet of Things,[129] Big Data,[130] Clouds.[131]

A kiberbűnözés esetében évek óta megjelent a Crime as a Service, vagyis a szolgáltatásszerű bűnözés, ami összekapcsolta a szervezett bűnözői köröket a feketekalapos hackerekkel.[132] Ezesetben a megrendelő számos szolgáltatást vehet igénybe, legyen szó betörést elősegítő eszköz vásárlásáról, egy adott informatikai bűncselekmény végrehajtásáról, vagy mindezek technológiai támogatásáról az üzleti szférából jól ismert „tech support" mintájára.

A kiberfenyegetettségek második típusa alatt a hacktivizmust és a kiberterrorizmust értjük, amelyek bár fogalmilag eltérőek ugyan, mégis több közös pont határozható meg esetükben. Ilyen közös pont, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport.

A harmadik típust a kiberkémkedés jelenti, amely alatt az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést értünk. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület.

A kiberfenyegetettségek negyedik csoportjába a kiberhadviselés sorolható. A kiberhadviselés az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására (ahogy történt a 2008-as orosz-grúz háború esetében), azonban ahogy a 2007-es észtországi

---

128 a Deep Web része, ahol alapvetően illegális cselekmények folynak.

129 A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra, és azok internet-szerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először.Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, "mérni", és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő, vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek.

130 A cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára.

131 A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (például: Gmail), vagy az online tárhelyek (például: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni.

132 Feketekalapos (black-hat) hackernek nevezzük azokat a hackereket, akik tudásukkal visszaélve, jogosulatlanul számítógépbe illetve számítógép-hálózatokba törnek be haszonszerzés vagy károkozás céljából.
Black-hat hackerek csoportjába tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba. Sok black-hat válik később white-hat hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon white-hat hackerként, hogy előtte soha nem próbált betörni egy számítógépbe sem. Így a határ inkább etikus és etikátlan hackerre osztható.

események is igazolták, önmagában is képes egy államot térdre kényszeríteni.[133] Amellett, hogy igen komoly károkozást lehet véghez vinni kibertámadással, bonyolítja a problémát, hogy szinte lehetetlen bizonyítani, ki is áll valójában a támadás mögött. Nemzetközi jogi megközelítésben egyre többen hangoztatják, hogy a kibertámadások háborús cselekmények, amelyek kiváltják az önvédelemhez való jogot. Ezek közé tartozik többek között Harold Koh, az amerikai Külügyminisztérium jogtanácsosa vagy Tony Blair korábbi nemzetbiztonsági főtanácsadója, Sir Richard Mottram is. Ezt erősíti meg az úgynevezett tallinni jegyzőkönyv, ami a NATO kérésére nemzetközi szakértők által összeállított ajánlás arra nézve, hogy a kiberhadviselés milyen nemzetközi jogi elvek szerint legyen szabályozva. A kézikönyv az online háborút próbálja értelmezni a klasszikus hadviselés elvei alapján, követve a genfi és hágai konvenciókat, deklaráltan a civilek védelmére. Ebből adódóan tiltja a kórházak, vízi- és nukleáris erőművek ellen intézett támadásokat. A halálos áldozatokkal, illetve különösen nagy anyagi kárral járó támadásokat háborús cselekménynek minősíti, ami kiváltja a konvencionális eszközökkel való válaszcsapás jogát is, valamint a támadást végrehajtó hackereket nem civilekként, hanem katonákként értelmezi. Fontos azonban azt látnunk, hogy elképesztően nehéz bizonyítani, hogy ki állt a támadások mögött. Ahogy az említett Észtországot ért kibertámadás is mutatta, hiába lehetett tudni, hogy kikhez köthető a támadás, nem lehetett egyértelmű bizonyítékokkal alátámasztani az orosz fél érintettségét. Márpedig, ha a tallinni jegyzőkönyv háborús cselekményként aposztrofált kitételeit nézzük, különösen nagy anyagi kárral járó támadás kiváltja az önvédelemhez való jogot.

Napóleontól származtatják a „legjobb védekezés a támadás" elvét, természetesen ez a kibertámadásokra is megfeleltethető. Egyre több állam ismeri fel ennek szükségességét, és alakít ki olyan képességet, amelyet kibertámadásra és a kibertámadások elleni védekezésre egyaránt alkalmazhat. Ebbe a körbe tartozik az Egyesül Államok, Kínához, Oroszország, Izrael, Irán, de nem lebecsülendő Észak-Korea 3000 főre tehető kiberserege sem, amely egy kiszámíthatatlan, irracionális döntések meghozatalára hajlamos rezsim kezében növeli a veszély mértékét.

Ahogy látni fogjuk, az okos mobil eszközök közvetetten vagy közvetlenül mind a négy kiberfenyegetettség esetében kockázatosak lehetnek.

2. Új típusú kihívások az okos mobil eszközök tekintetében

Függőségünk az infokommunikációs eszközöktől, beleértve az okos mobil eszközöket is, nem elhanyagolható. Mielőtt minden infokommunikációs eszközünket az internetre kötöttük volna, a kockázatok megmaradtak bizonyos fizikai korlátok között. A klasszikus mobiltelefonok esetében korábban a legnagyobb kockázatot az jelentette, ha megtámadták a használóját, ami természetesen a támadástól függően komolyabb sérüléssel is járhatott. Az okos mobil eszközök, az által, hogy az internetre csatlakoznak, új típusú kihívások elé állítottak. Ezek az új típusú kihívások egyáltalán nem követelik meg, hogy a támadó és a megtámadott fizikailag egy helyen legyenek egy időben, egy támadás adott esetben több ezer kilométeres távolságból is elkövethető.

Értelemszerűen nem szűnt meg a klasszikus kockázat, amely az okos mobil eszközök eltulajdonításából fakad, hiszen egy-egy készülék több százezer forintos értéket is képviselhet. Fontos azonban látni, olyan mértékű fenyegetéseket okozhatnak ezek az eszközök, amelyek mellett már nem tűnhet olyan jelentősnek, ha ellopják a telefonunkat.

Figyelembe véve a kiberfenyegetettségek négy típusát, mielőtt konkrét példákon keresztül mutatnánk be az okos mobil eszközök használatából fakadó kockázatokat, vizsgáljuk meg általánosan, milyen területeken vagyunk veszélynek kitéve.

[133] 2007-ben, miután a kormányzat megpróbált eltávolítani egy szovjet köztéri emlékművet, Észtország kormányzati és pénzügyi rendszereit közel egy hónapon keresztül érte kibertámadás, amely óriási anyagi károkat szenvedett el. Ahogy az egyik észt politikus fogalmazta, országukat „a digitális kőkorszakba bombázták vissza".

Az előző fejezetben említett Europol jelentésből kitűnik, hogy a legnépszerűbb bűnelkövetési forma a malwarekkel való visszaélés. Az okos mobil eszközök esetében is igen gyakoriak az úgynevezett zsaroló vírusok, amelyek a megfertőzött telefonok/tabletek tartalmát titkosítják, a feloldásért cserébe pedig pénzt – többnyire bitcoinban[134] – követelnek. Az esetek nagy részében természetesen a követelés teljesítése után sem kapjuk vissza filejainkat, így nem érdemes fizetni a zsarolóknak. Az okos mobil eszközök vírusfenyegettségével a *Bevezető az okos mobil eszközök világába* címet viselő tananyag részletesen foglalkozik, így itt külön nem ismételnénk meg, azonban szükséges minden esetben hangsúlyozni, hogy a nem biztonságtudatos eszközhasználat nagymértékben növeli kitettségünket a rosszindulatú támadással szemben.

Megítélésünk szerint rendkívül fontos, hogy odafigyeljünk a fiatalok, gyermekek sérelmére elkövetett bűncselekményekre, illetve ezek lehetőség szerinti megelőzésére, ezek közül is kiemelten a gyermekek szexuális zaklatására, kizsákmányolására. A közösségi oldalak és az okos mobileszközök elterjedésével egyfajta paradigmaváltás figyelhető meg az internethasználat tekintetében, amelynek egy sarkalatos pontja a magánszféra egyre nagyobb mértékben történő visszaszorulása. Minden cselekedetünket, életünk minden apró mozzanatát megosztjuk ismerőseinkkel és ismeretlenekkel egyaránt. Az okos mobil eszközök technikai fejlődése egyre jobb és jobb minőségű képek, videók elkészítését teszi lehetővé, az állandó internetkapcsolat pedig nem csupán az azonnali megosztásukat segíti elő, de élőben sugározhatjuk a nagyvilágnak, hogy éppen milyen tevékenységet végzünk. A fiatalok körében különösen népszerűek a képmegosztó és képküldő alkalmazások, mint az Instagram vagy a Snapchat. Ezeken kívül számos üzenetküldő alkalmazás biztosít névtelenséget és titkosított üzenetküldést is, ami megkönnyíti például a pedofil tevékenységek végzését. Az interneten számos olyan fórum fellelhető, ahol nem csak pedofilok, de a kiskorúak is cserélgetik egymás között a magukról, társaikról készített erotikus képeket, videókat. Nem szabad elfelejteni, hogy míg ezek megragadnak „amatőr" szinten, elképesztően nagy üzletet jelent egyes köröknek a képek, videók terjesztése, de különböző szexuális tevékenységeket élőben közvetítő stream-szolgáltatások üzemeltetése. De nem szükséges, hogy valaki szándékosan, üzleti céllal tegye nyilvánossá privát képeinket, videóinkat. Óriási károkat okozhat az embernek, ha akarata ellenére akár pár ember, akár szélesebb tömegek ismerik meg ezeket a tartalmakat róluk. A tananyag készítésének idején foglalkoztak a hírek a 31 éves olasz nő, Tiziana Cantone esetével, aki öngyilkos lett a róla kikerült házi pornó miatt. A videóból mém lett, pólókat nyomtattak belőle és azokat forgalmazták. Cantone otthagyta a munkáját, Toszkánába költözött, még a nevét is megpróbálta megváltoztatni. Végül hosszú pereskedés után sikerült elérnie, hogy levegyék a róla készült videót az internetről, még a Facebooknak is törölnie kellett. A bíróság végül Cantonet kötelezte arra, hogy fizesse meg a 20 ezer eurós jogi költséget. Korábban kétszer próbált meg öngyilkosságot elkövetni.[135]

Az okos mobileszközök elterjedése utat nyitott a fizetési eljárások kiszélesítésének is. Számos alkalmazás használatáért cserébe fizetnünk szükséges, amiért a telefonunk egyben pénztárcaként is szolgálhat. De nem csak alkalmazásokért fizethetünk mobilunkon keresztül, szolgáltatásokat is vehetünk így igénybe, gondoljunk csak a parkolásra vagy az autópálya matrica vásárlására. Ezek mellett ugyanúgy intézhetjük az online bankolást is mobil eszközökről. Mivel pénzügyi tranzakciók végzéséről van szó, kiemelten fontos, hogy az eszköz, amiről fizetünk, illetve az eljárás, amit követünk, biztonságos legyen. Sajnálatos módon a felhasználók jelentős része igen csak óvatlan az eszközei védelmét illetően. A mobilitás együtt jár azzal, hogy pénzügyi tranzakciót bárhonnan indíthatunk. A bárhonnan egyben azt is jelenti, hogy nem biztonságos kapcsolaton keresztül használjuk telefonunkat. Ha nem otthonról, saját, védett Wi-Fi hálózatról kapcsolódunk az internethez, a legbiztonságosabb,

[134] A bitcoin egy virtuális fizető eszköz, amely titkosított csatornán keresztül teszi lehetővé a fizetést. Ennél fogva különösen népszerű az illegális cselekmények finanszírozásában, legyen szó kábítószer-, fegyverkereskedelemről vagy akár terrorizmus finanszírozásról.

[135] Index: Öngyilkos lett egy nő, mert kikerült a netre a szexvideója, In. Index, 2016. szeptember 15., http://index.hu/kulfold/2016/09/15/ongyilkos_lett_egy_no_mert_nem_nem_toroltek_le_a_szexvideojat/ (utolsó letöltés: 2016. szeptember 15.)

ha saját mobil internetünket használjuk. Ennek természetesen anyagi vonzata van, egy olcsóbb előfizetés kisebb adatforgalommal, lassabb letöltési sebességgel jár, ezért sokan igyekeznek valamilyen nyilvános Wi-Fi hálózatra csatlakozni. Ez azonban igen komoly biztonsági kockázatot jelent, hiszen az adatforgalmunkat a hálózat üzemeltetője is látja, és megfelelő eszközök segítségével képes lehet hozzáférni jelszavainkhoz, beszélgetéseinkhez.

Az okos mobileszközök elterjedése sok esetben összemossa a munkaidőt a szabadidővel. Utazás közben a telefonunkról elérjük a munkahelyi e-mailjeinket, munka közben tudunk ismerőseinkkel csetelni, képeket megosztani stb. Mindez megnöveli a támadások lehetőségét, hiszen ha mobiltelefonunkról egy kevésbé vagy egyáltalán nem biztonságos kapcsolatról jelentkezünk be munkahelyi levelezésünkhöz, hiába van egyébként a munkahelyünkön jól védett, biztonságos rendszer, a támadók megkerülhetik rajtunk keresztül azt, és könnyedén hozzáférhetnek védett adatokhoz, hálózatokhoz.

2013 óta, amikor Edward Snowden a nyilvánosságra hozta az amerikai Nemzetbiztonsági Ügynökség megfigyeléssel kapcsolatos eljárásait, a laikusok számára is világossá vált, mennyire könnyen hozzáférhető „kíváncsi fülek" számára a mindennapos kommunikációnk. Természetesen ez nem csak egyes nemzetbiztonsági szolgálatok kiváltsága, rosszindulatú támadók ugyanúgy megfigyelhetik online kommunikációnkat. A Snowden iratok egyik következménye, hogy megnőtt az igény a titkosított online kommunikációra. Ezzel egy időben a valóban illegális tevékenységet elkövetni szándékozók óvatosabbak lettek az online kommunikációjukat illetően – gondoljunk csak 2015-ben, az év végén elkövetett párizsi merényletek elkövetőire, akik a lebukás elkerülése érdekében tudatosan régi, eldobható mobil eszközöket használtak. Másrészt egyre több olyan alkalmazás került piacra, ami titkosítást ígér a felhasználóknak.[136] Az egyik ilyen alkalmazás a Telegram Messenger nevű alkalmazás, amelyet nemzetbiztonsági jelentések szerint újabban az Iszlám Állam nevű terrorszervezet is előszeretettel használ kapcsolattartásra, propagandaterjesztésre.

Az Europol jelentése is kiemeli a social engineeringet, ami alatt egy olyan eljárást értünk, amelynek során az emberi hiszékenységet kihasználva próbálnak meg a támadók hozzáférést szerezni egy védett rendszerhez. Maga a social engineering megítélésünk szerint mind a négy kiberfenyegetettség esetében alkalmazható eljárás, éppen ezért e tanulmányban, utolsó pontként, külön fejezetet szenteltünk a bemutatására. Ehhez kapcsolódik a hacktivizmus, vagy kiberterrorizmus, amin az adatokhoz, védett rendszerekhez hozzáférést kell értenünk, ami értelemszerűen a kiberkémkedésre is vonatkozik.

Az okos mobil eszközök jelentette új típusú kihívások a korábbiak esetében elsősorban közvetlenül jelentkeztek, a kibertámadás esetében azonban inkább közvetett hatásról beszélhetünk, amely alapvetően az okos mobil eszközök rosszindulatú programok elterjesztésében írhatóak le.

3. Az alkalmazások használatából fakadó biztonsági kockázatok

Az előző fejezetben általános mutattuk be azokat új típusú kihívásokat, amelyek az okos mobil eszközök használatából erednek. A továbbiakban, kapcsolódva a tananyag mellett elkészített esettanulmányokhoz, részletesebben is megvizsgáljuk a ránk leselkedő fenyegetéseket egy-egy kockázati elemet kiemelve.

Az okos mobil eszközök kockázatait alapvetően az alkalmazások biztonságán keresztül foghatjuk meg. Az alkalmazások a mobil eszközök esetében az operációs rendszer szolgáltatásain keresztül valamilyen feladatra felhasználó programok. A felhasználó ezeket a programokat használja általában, hogy egy alkalmazást használhassunk, valahonnan le kell töltenünk. Ez történhet biztonságos, illetve nem biztonságos forrásból. Ez természetesen nem jelenti azt, hogy biztonságos forrásból letöltött alkalmazás biztonságos, csupán nagyobb esélyünk van arra, hogy megvédjük

[136] Ezt azonban érdemes fenntartásokkal kezelnünk.

adataink, eszközünk biztonságát. A telefonok, tabletek alapbeállítása általában tiltja, hogy nem biztonságos forrásból tölthessünk le alkalmazásokat, ezt azonban a beállítások között a felhasználható kikapcsolhatja. Létezhetnek alkalmak, amikor indokolt lehet nem biztonságos forrásból letölteni egy-egy alkalmazást, de alapesetben célszerű csak megbízható forrásból származó alkalmazásokat telepíteni. A megbízható forrás esetünkben az okos mobil eszköz (például Samsung készülékek esetében Galaxy App) vagy az általa használt operációs rendszerének hivatalos alkalmazás áruháza (Android esetében Google Play Áruház, iOS esetében Apple Store, Windows Phone esetében Microsoft Áruház stb.). Az egyes áruházak eltérő biztonsági előírásokat fogalmaznak meg az alkalmazások gyártóival kapcsolatban, így androidos alkalmazások esetében jelentősen nagyobb számban találkozhatunk rosszindulatú kódokat is tartalmazó vagy adathalász alkalmazásokkal.[137] Egyes népszerű alkalmazások nem érhetőek el globálisan mindenhol. A 2016 nyarán megjelent Pokémon Go alkalmazás szinte egyből óriási érdeklődésre tett szert, azonban a világ sok országában később vált letölthetővé, és akkor sem minden platformra. A játékra kíváncsi tömegek mindent megpróbáltak, hogy idő előtt hozzájussanak a várva várt alkalmazáshoz, így nagyon sokan nem megbízható forrásból töltötték le. Ezt az eljárást követve azonban nem lehetett tudni, kiknek szolgáltatják ki adataikat. A lehetőségek tárháza széles.

Ha letöltünk és telepítünk egy alkalmazást, a használatáért cserébe különböző engedélyeztetéseket kér tőlünk. Például egy alkalmazás letöltése lehet ingyenes, de a használatért cserébe az adatainkat kéri. Alkalmazástól függ, hogy pontosan mikhez kíván hozzáférni (például a telefonkönyvünk, helyi koordinátáink, vagy fényképalbumunk esetleg a kameránk), a lényeg, hogy ne legyenek illúzióink, ha valami ingyenes, ott minden esetben mi vagyunk a termék. Minden esetben, mielőtt egy alkalmazás telepítése mellett döntenénk, olvassuk el figyelmesen, milyen engedélyeket kér a használatért cserébe, és ha túlzónak ítéljük meg, szakítsuk meg a telepítési folyamatot. Célszerű telepítés előtt ellenőrizni az egyes alkalmazásokat különböző adatbiztonsággal foglalkozó honlapokon. Ilyen weboldal például a Privacy Grade (http://privacygrade.org/home), ami biztonsági kategóriába sorolja az alkalmazásokat annak függvényében, hogy milyen engedélyeket kér a használatáért cserébe, és ez mennyire reális az alkalmazás alapvető funkciójához képest. Egy „zseblámpa” alkalmazás esetében például több mint indokolatlan az üzenetek tartalmához, geolokációs adatainkhoz való hozzáférés kérdése. Amennyiben ilyennel találkozunk, ne telepítsük az alkalmazást, mert vélhetően adathalász programmal van dolgunk. Egy alkalmazás adatkezelési gyakorlatánál mindig komoly kockázatot jelent, hogy nem tudjuk, a rólunk gyűjtött adatokat ki és milyen módon kezeli. Nem egy esetben volt már rá precedens, hogy az alkalmazásfejlesztők harmadik félnek adták el az adatokat. Rendkívül jól jövedelmező üzletág az adatok forgalmazása.

Egy alkalmazás a legkülönfélébb adatainkhoz kérhet hozzáférést. A legnépszerűbb alkalmazások, mint a Facebook vagy a Google alkalmazásai többek között az alábbi adatokhoz férnek hozzá: 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). A Facebook közel 30 hozzáférés engedélyt kér az egyszerű használatért cserébe. Nem nehéz belátni, rossz kezekben milyen hatalmat jelenthetnek azok az adatok, amiket kiárusítunk magunkról. Az okos mobil eszközökhöz való függőségünk azzal is jár, hogy mindenhová magunkkal visszük őket. Amennyiben feltelepítettünk egy olyan nem megbízható alkalmazást, amelynek a kamerához is hozzáférést biztosítottunk, a fejlesztők adott esetben bármikor átvehetik az irányítást a kameránk fölött, kompromittáló képeket is megszerezve az által. Elég, ha arra gondolunk, milyen sokan viszik magukkal a telefonjukat a mosdóba, hogy gyorsabban teljen az idő a használatával. Az egyes hozzáférési engedélyekből fakadó kockázatokkal az utolsó fejezetben bővebben foglalkozunk.

[137] Fontos látni, készülékünkre csak a saját operációs rendszerére megírt alkalmazást telepíthetünk, eltérő platformét nem. Ha például csak iOS-ra írt alkalmazást kínálnak számunkra Android rendszerre, ne foglalkozzunk vele, ugyanis egyértelműen csalásról van szó.

A Pokémon Go megjelenése után pár nappal elterjedt, hogy az alkalmazás valójában a CIA kémprogramja. Emögött az állt, hogy az alkalmazás a használatért cserébe a teljes Google fiókhoz hozzáférést kért. A felhasználói felháborodás hatására a fejlesztők kiadtak egy frissítést, ami korlátozta a hozzáférést, arra hivatkozva, hogy tévedésből kértek teljes hozzáférést, természetesen nem az amerikai nemzetbiztonsági szolgálatok állnak a játék mögött.

Vannak esetek, amikor azonban nem dönthetünk egyes alkalmazások telepítéséről, ugyanis a szolgáltató előre telepítette őket, és törölni sem tudjuk. A Google-t ezen gyakorlata miatt számos támadás éri, ugyanis emiatt aránytalan előnyt élvez más, hasonló szolgáltatást nyújtó alkalmazásokkal szemben. Az sem mellékes, hogy a telefon memóriájának bizonyos százalékát is leköti, ami olcsóbb eszközök esetében igen csak komoly erőforrás pazarlást jelenthet. A nagy informatikai cégek és az amerikai Nemzetbiztonsági Ügynökség közti kapcsolatot a már említett Snowden iratokból ismerjük, ez alapján tudjuk, hogy az NSA elérte, hogy ezeknek a cégeknek a felhasználókról gyűjtött adatbázisához hozzáférjenek (amiket aztán továbbadhattak a partnerszolgálataiknak), vagyis alapesetben nem tehetünk az ellen semmit, hogy ezek az alkalmazások ne továbbítsák igény esetében az adatainkat az NSA-nek. Természetesen van rá mód, hogy töröljük ezeket az előre telepített alkalmazásokat, ehhez azonban rendszergazda hozzáférésre van szüksége a telefon tulajdonosának, ami alapesetben nem jár a telefonhoz. Ennek megszerzése különböző eljárásokkal elérhető, ezek azonban olyan informatikai tudást követelnek meg, ami az átlag felhasználó számára nem ismertek. Persze felismerték ezt többen, így szolgáltatásszerűen megvásárolható nem hivatalos úton, hogy a telefonhoz rendszergazda hozzáférést biztosítsanak. Ezzel az eljárással azonban nem csak a készülék garanciáját kockáztatjuk, hanem szabadutat engedünk a rosszindulatú programok elharapódzásának.

Az előre telepített programoknak van egy másik aspektusa, amelyről a felhasználó nem tud. Több esetben bebizonyosodott, egyes kínai telefonok gyártók már a gyártósoron vagy a forgalmazás során olyan kémprogramokat telepítenek az eszközre, amelyeknél nem lehet tudni, kihez kerülnek a rólunk gyűjtött adatok. 2015-ben a Lenovo laptopok[138] esetében fedezték fel, hogy olyan hirdetéskezelő rendszert és gyökérszintű tanúsítványt telepítettek a számítógépeikre, amelyek akár a webes forgalom monitorozására, de akár támadások lebonyolítására is alkalmasak voltak.[139] Az érintett program a Superfish nevet viselő alkalmazás volt, amelyet végül felhasználói panaszok hatására eltávolították. Az eset során olyan képernyőmentések is készültek, amelyben egy tanúsítvány úgy tett, mintha a kibocsátója a Bank of America lenne. A Superfish gyárilag rajta volt a rendszereken, és alapvetően nem is ártó szándékú, csupán arra akarták használni, hogy a Google keresési eredményei közt másoktól származó hirdetések is megjelenjenek. A laptopgyártó azzal védte meg a szoftvert, hogy az képekkel segíti a termékek megtalálását. Emellett a vevők a laptop beüzemelése során elutasíthatják a használati feltételeket, hogy ne települjön a szoftver. Figyelembe véve, hogy az átlag felhasználó telepítéskor mindent elfogad anélkül, hogy elolvasná, nem nevezhető a legkorrektebb eljárásnak. A Superfish úgynevezett közbeékelődéses (man-in-the-middle) támadást használt, amivel belenyúlt a felhasználó webes adatforgalmába. Ilyenkor mindkét fél azt hiszi, hogy közvetlenül egymással kommunikálnak, pedig mindketten csak a csatornát irányító rejtett szereplővel állnak kapcsolatban. Nem véletlen, hogy a Superfish szoftverét a vírusirtók veszélyes alkalmazásként azonosítják, és az eltávolítását javasolják. A Lenovót képviselő PR-ügynökség reakciójában azt írta, hogy október és december között szállított notebookokon rajta volt a Superfish. Hozzátették, hogy alaposan megvizsgálták a technológiát, és nem találtak arra bizonyítékot, ami egyértelműen alátámasztaná a biztonsági problémát, de a felhasználói aggályok miatt léptek az ügyben. Azóta teljes mértékben eltávolították a szerver-oldali interakciókról minden Lenovo termékről, így az minden terméken le van tiltva, illetve nem telepítik előre a szoftvert a notebookokon, és ezt a jövőben sem tervezik.

---

138 Az eljárás természetesen érvényes lehet az okos mobil eszközökre is.

139 Williams, Owen: Lenovo caught installing adware on new computers, In. The Next Web, 2015. február 19., http://thenextweb.com/insider/2015/02/19/lenovo-caught-installing-adware-new-computers/ (utolsó letöltés: 2016. szeptember 7.)

Szintén 2015-ben több mint húsz különböző típusú kínai okostelefonon találtak előre telepített kémprogramokat.[140] Ezek közé tartoztak többek között Lenovo, a Xiaomi és a Huawei készülékei, de a kémprogramokat felfedező, G Data vírusvédelmi cég szakértői szerint nem a gyártók, hanem valószínűleg a kereskedők telepítették a kártevőket a Németországban forgalomba kerülő készülékekre. A kémprogramok jellemzően a Facebook vagy a Google Drive alkalmazások egyikébe voltak elrejtve. A manipulált alkalmazások teljesen úgy működnek, mint az eredetiek. A kártevőt tartalmazó Facebook alkalmazásnál például minden funkció elérhető, a felhasználó nem vesz észre semmit abból, hogy az alkalmazásban elrejtett kémprogram hátsó ajtót nyitott a mobilján a támadók számára, akik így hozzáférhetnek az összes adatához. Az alkalmazás pedig nem kér engedélyeket, mivel már minden szükséges engedélyt megkapott a telepítésekor. A felhasználó így kizárólag akkor veszi észre, hogy a telefonja fertőzött, ha telepít valamilyen biztonsági alkalmazást, amelynek során a biztonsági program jelzi a fertőzött állományt. A megtisztítás azonban gyakran nem lehetséges, mivel a kártevő bele van égetve a telefon gyári meghajtó programjába (firmware-jébe). Ilyen esetben a vásárlónak fel kell vennie a kapcsolatot a mobilkészülék gyártójával. A kártevőt tartalmazó hamis Facebook alkalmazás rendkívül sok funkcióhoz szerezhet hozzáférést. A korábban ismertetett hozzáférési engedélyek mellett a támadók belehallgathatnak a telefonhívásokba és rögzíthetik azokat, vásárlásokat indíthatnak vagy emelt díjas számokat hívhatnak.

A Kínában gyártott informatikai eszközök, beleértve az okos mobil eszközöket is, komoly aggodalmakat szülnek a nemzetbiztonsági területen dolgozók számára. 2012-ben az Egyesült Államok két kínai telekommunikációs cég, a Huawei és a ZTE kitiltását tervezte az amerikai piacról, ugyanis megítélésük szerint nemzetbiztonsági kockázatot jelentenek az által, hogy az érintett cégeknél túlságosan nagy a kínai állam befolyása. Az amerikai Védelmi Minisztériumnak a kínai haderőről a Kongresszus számára készített éves jelentése szerint a Huawei technológiája olyan „hátsó kapukat” tartalmaz, amely a kínai hadsereg számára lehallgatási lehetőséget biztosít az amerikai telekommunikációs hálózaton belül.

Részben kapcsolódik a megbízhatatlan gyártókhoz a soron következő kockázat, ami a telefonok üzemidejéből ered. Az okos mobil eszközök akkumulátorának az üzemideje nagyban függ a használattól. Az okostelefonok jelenleg nagyon ritkán bírják egy feltöltéssel akár több napig is, mint a „butatelefonok”. Eltérő módon terheli az akkumulátort, ha mobil internetet vagy wifit használunk. Egyes alkalmazások olyan mértékben veszik igénybe az akkumulátort, hogy akár órák alatt is lemerülhet a telefonunk. Ilyen alkalmazás a már említett Pokémon Go is, aminek az a célja, hogy kiterjesztett valóságot felhasználva a városban mászkálva Pokémonokat gyűjtsünk a telefonunkkal. Az okos mobil eszközöket nem csak hálózatról, de USB portról is feltölthetjük. Léteznek városszerte olyan USB portok, amikről a lemerült vagy éppen a teljes lemerülés szélén álló eszközeinket feltölthetjük, ezek azonban igen komoly kockázatot jelentenek, ugyanis az ismeretlen forráshoz való csatlakozás megteremti annak a lehetőségét, hogy rosszindulatú programmal fertőzzük meg az eszközeinket. Ennél fogva kerüljük az ismeretlen forrásból történő töltés lehetőségeit USB portról, igyekezzünk csak hálózatról tölteni telefonunkat.

A gyenge üzemidő egyúttal újabb támadási felületeket is jelent. Rengeteg olyan alkalmazást készítenek, amelyek azt ígérik, megnövelik a készülék üzemidejét, optimalizálják az alkalmazások energiafogyasztását. Egyes alkalmazások a klasszikus árukapcsolás elvét követve folyamatosan ajánlják a jobbnál jobb alkalmazások további letöltését, nem egy esetben eltúlozva a telefonra leselkedő veszélyeket. Természetesen ez nem azt jelenti, hogy minden alkalmazás, ami hasonló módon jár el, veszélyt jelent, de a felhasználónak rendkívül óvatosnak kell lennie. Mindig értelmezzük, amit az alkalmazás kiír, ugyanis gyakran az emberi hiszékenységre alapoznak, kétértelmű megfogalmazással. Például „Telefonja veszélynek van kitéve, akár 17 vírusos alkalmazás is lehet rajta”. Nem állítja,

[140] Khandelwal, Swati: 26 Android Phone Models Shipped with Pre-Installed Spyware, In. The Hacker News, 2015. szeptember 3., http://thehackernews.com/2015/09/android-smartphone-malware.html (utolsó letöltés: 2016. szeptember 7.)

hogy a telefon fertőzött lenne, az az állítás, pedig hogy veszélynek van kitéve, a tananyag ezen pontján pedig egyértelműen igaz. Az a felhasználó pedig, aki kevésbé jártas az informatikában vagy nem igazán jellemezhető biztonságtudatosnak, nagyobb eséllyel tölti le a rosszindulatú alkalmazást.

Nem csak alkalmazások letöltésével fertőzhetjük meg telefonunkat, tabletünket, ugyanúgy kattinthatunk egy fertőzött honlapra böngészés közben, mint ahogy számítógépen lehetséges. De mit tehetünk akkor, ha akár óvatlanságból, akár egyéb okból kifolyólag megfertőződött az általunk használt eszköz? Először is, nem mindegy, milyen platformot használ a telefonunk, ugyanis iOS esetében nagyon ritkán beszélhetünk vírusokról, a rosszindulatú alkalmazások elsősorban az adathalászat tekintetében jelentkeznek. Az Apple sokáig kifejezetten büszkén hirdethette, hogy alkalmazásboltjába nem kerülhetnek károkozó kódokat tartalmazó alkalmazások, mivel mindegyiket heteken, akár hónapokon keresztül vizsgálják, mielőtt engedélyezik őket. Most azonban egy trükkös megoldással kerülték meg ezt a folyamatot, valószínűleg kínai hackerek. A vírust ugyanis nem az alkalmazásokba próbálták utólag beerőszakolni, hanem már az Xcode nevű fejlesztőkörnyezetet támadták meg. Ez az a programozási környezet, amelyet az alkalmazások készítői használnak az alkalmazások megírása során. A károkozók azt használták ki, hogy számos fejlesztő nem az Xcode hivatalos verzióját használta (ugyanúgy, ahogy mezei felhasználók tört Windows-t futtatnak a gépükön, vagy filmeket torrenteznek). A hackerek az Xcode egyik kalózváltozatába rejtették a kártevő kódokat, majd feltöltötték a fejlesztőcsomagokat kínai warez szerverekre. Így a fejlesztők észre sem vették, hogy vírus kerül az általuk készített mobilos alkalmazásokba a már eleve fertőzött eszközből. Amennyiben olyan alkalmazást töltöttünk le, amit hasonló eljárással megfertőztek, azonnal töröljük, vagy frissítsük még újabb verzióra. Ezen felül pedig érdemes egy másik eszközről megváltoztatni a jelszavainkat a webes szolgáltatásokhoz (például levelezéshez), de akár a netbankhoz és egyéb fontos helyekhez is érdemes új belépési adatokat megadni.

Az Androidot használó készülékek tulajdonosai nagyobb számban vannak veszélynek kitéve, ugyanis nincs olyan szigorú ellenőrzés az alkalmazásboltba való bekerüléshez. A biztonsági szakértők információi szerint a legtöbb vírus fizetés alapú, ami azt jelenti, hogy megpróbálnak hozzájutni a bankkártya-adatokhoz, a felhasználónevekhez, a jelszavakhoz és más személyes beazonosításra is alkalmas adatokhoz. Emellett persze több száz olyan mobilvírus is létezik, amelyek „kevésbé ártalmas" célokra készültek. Ezek közé tartozik például a névjegyzék, az e-mail címek és más adatok harmadik feleknek való továbbítása, „prémium" szolgáltatások megjelenítése, a beszélgetések rögzítése, további malware-ek letöltése, felugró ablakok megjelenítése és kétes weboldalakat célzó átirányítások indítása. A szokásos vírusokhoz hasonlóan először az androidos fertőzések esetében is nehéz észrevenni a problémát, mert a fájlok a rendszer mélyében rejtőznek. A rendszer lassulása, a gyanús értesítések, az átirányítások és a valamivel magasabb telefonszámla azonban mind gyanúra ad okot. Ilyen esetekben mindig ellenőrizze a készüléket egy elismert antivírus programmal. Az esetek többségében a felhasználók valamilyen nemhivatalos forrásból származó alkalmazás mellékleteként töltik le a fertőzést.

Miből ismerhetjük fel, ha az eszközünk megfertőződött? Ha az alábbi problémák jelentkezhetnek, akkor vírusos a telefonunk:

- *Érzékeny adatok elvesztése*. A rosszindulatú alkalmazások számos információhoz férhetnek hozzá, például a névjegyzékhez, a bejelentkezési adatokhoz és az e-mail címekhez.
- *Anyagi kár.* Az androidos malware-ek akár emeltdíjas számokra is küldhetnek üzeneteket, és feliratkozhatnak fizetős szolgáltatásokra. Mindezt természetesen az áldozat fizeti.
- *További malware-ek bejutása.* Az Android vírus további fertőzéseket juttathat a rendszerbe. Emellett hirdetéseket, felugró ablakokat és megtévesztő értesítéseket is megjeleníthet.
- *A teljesítmény romlása.* A fertőzött rendszer lassabbá, instabilabbá válik.

Ha úgy sejti, hogy készülékébe bejutott az Android vírus, mielőbb vizsgálja át a rendszert a valamilyen antivírusprogrammal, amely képes észlelni a kártékony fájlokat és más víruskomponenseket. Előfordul, hogy a vírus letiltja a biztonsági szoftvereket. Ebben az esetben indítsa a készüléket csökkentett módban, és úgy futtassa az antivírus-alkalmazást.

Csökkentet mód indítása kétféleképpen lehetséges. Az egyik, hogy kikapcsoláskor választhatjuk azt a lehetőséget, hogy a készülék csökkentet módban induljon újra. Ha ezt nem ajánlja fel a rendszer, akkor kapcsoljuk ki a telefont, majd indítsuk újra. Amint a készülék bekapcsol, tartsuk lenyomva a Menü, Hangerő le vagy Hangerő fel gombokat, esetleg a Hangerő le és Hangerő fel gombokat egyszerre, így csökkentett módban indíthatja a rendszert. Megpróbálhatunk kézzel is megszabadulni az Android vírustól, az alkalmazás szokásos módú eltávolításával. Legyünk óvatosak ezzel a módszerrel, véletlenül akár hasznos alkalmazásokat is törölhetünk. A kézi eltávolítás lépései a következők:

(1) A fenti lépések segítségével indítsuk a készüléket csökkentett módban.
(2) Csökkentett módban nyissuk meg a *Beállítások* menüt. Válasszuk ki az *Alkalmazások* vagy *Alkalmazáskezelő* menüpontot (a pontos név készülékenként eltérő lehet).
(3) Keressük ki a kártékony alkalmazást és távolítsuk el.

Megjelentek azonban olyan trójai vírusként működő hirdetőprogramok, amelyek népszerű alkalmazásként álcázzák magukat (Candy Crush, Facebook, GoogleNow, Twitter, SnapChat, WhatsApp stb.), és telepítésükkor automatikusan, a felhasználó tudta nélkül rootolják[141] a mobil eszközt, rendszeralkalmazásként ágyazva be magukat, amelyet aztán szinte lehetetlen eltávolítani. Ugyanis az egyszerű eltávoltás (uninstall) esetükben nem használható, így a pórul járt felhasználónak nincs más választása, mint a telefon gyártójával töröltetni a tárolót (a mobil alaphelyzetbe állítása nem segít a gondon) vagy egy új okostelefont vásárolni. A dolog érdekessége, hogy az álcázásként használt alkalmazások jó része rendeltetésszerűen működik, miközben rosszindulatú tevékenységet is végez.

Korábban volt szó a zsarolóvírusokról, más néven ransomwarekről, amik olyan rosszindulatú programok, amelyek valamilyen fenyegetéssel próbálnak meg pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszik az eszközt vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, aminek a hatására visszaállítják az eredeti állapotot. Ha a felhasználó kártékony alkalmazást telepít és futtat, értesítést kap a képernyőn, amely szokványos rendszerüzenetnek tűnik, és arról tájékoztat, hogy bizonyos beállításokat módosítania kell, vagy további alkalmazást kell (vagy ajánlott) telepítenie. Ha a felhasználó rákattint az ablakra vagy máshogy beleegyezik a folytatásba, rendszergazdai hozzáférést ad a vírusnak. Pontosan erre van szüksége a ransomware-nek. A felhasználó beleegyezésének ezt a közvetett megszerzését clickjacking néven szokás említeni – ezzel az áldozat rákényszerül, hogy olyan dolgot telepítsen, amit nem is szeretett volna. Amikor a fenyegetés (amely az Android vírushoz kapcsolódik) adminisztrátorként fér a telefonhoz, minden tárolt fájlt megkeres, majd titkosítja őket. Az eredmény, hogy ezek a fájlok hozzáférhetetlenné válnak. Ezt követően a mobilvírus fenyegető üzenetet jelenít meg, azt állítva, hogy az áldozat illegális tartalmakhoz fért hozzá. Figyelmeztet továbbá, hogy a személyes adatokat – beleértve a böngészési előzményeket is – minden névjegynek elküldte. A vírus mindemellett képes megváltoztatni a telefon feloldókódját és PIN-kódját is. A fenyegető üzenet váltságdíjat követel a személyes adatok visszaállításáért cserébe. Ne fizessen! A vírus titkosítja a fájlokat, de állítólag végleg törölni is képes őket. Nincs tehát értelme fizetni. Rendkívül valószínűtlen, hogy visszakapja a fájlokat, az egyetlen dolog, amit tehet, hogy eltávolítja az Android ransomware-t és megvédi a készüléket a hasonló vírustámadásoktól. Bár a vírus eltávolítását a felhasználó is elvégezheti, de ha csupán felhasználói szintű kompetenciával rendelkezik, célszerű szakemberhez fordulni vele.

Egy alkalmazás nem csak akkor jelenthet veszélyt ránk nézve, ha valamilyen rosszindulatú programmal fertőzött. A már többször említett Pokémon Go nem egy esetben emberéletet követelt, ugyanis a játékos nem figyelt a környezetére, és magánterületre tévedt, ahol lelőtték.[142] A szarajevói magyar

[141] A rootolás folyamán a felhaszáló root user-ré/superuser-ré válik, vagyis egy olyan felhasználóvá, akinek teljes hozzáférése van minden utasításhoz és filehoz az operációs rendszerben.

[142] Az első eset Guatemalában történt, két héttel az alkalmazás megjelenését követően. Bővebben lásd: Origo: Meghalt egy tinédzser pokémonozás közben, In. Origo, 2016. július 20., http://www.origo.hu/techbazis/20160720-pokemon-go-halal-baleset.html (2016. szeptember 16.)

nagykövetség közleményt adott ki,[143] amelyben arra figyelmeztetik a Bosznia-Hercegovinába látogató magyar állampolgárokat, hogy *„a Pokémon Go játék nem veszi figyelembe az aknamezőket”*, és kéri az embereket, hogy figyeljenek oda az aknamezőket jelző táblákra, emellett arra is figyelmeztetnek, hogy a gyakori esőzések miatt a jelzőtáblák és szalagok mozoghatnak, így egyáltalán nem javasolják, hogy lakatlan területen játsszák a játékot. Ha nem is mindennapi, hogy aknamezőre tévedjünk, de figyelmetlenségünkből kifolyólag bármikor nagyon könnyen szenvedhetünk balesetet, akár úgy, hogy a telefonunkat nyomkodva nekimegyünk valaminek, valakinek, lelépünk az útról és úgy szenvedünk balesetet. Ezek elkerülése érdekében lehetőleg ne használjuk a telefonunkat gyaloglás, különösen autóvezetés közben. Amennyiben mégis rákényszerülünk, legyünk tekintettel környezetünkre.

Maradva a Pokémon Go-nál, a játék lehetőséget biztosít úgynevezett PokéStopokat is, amelyek előfizetés eredményeképpen egy adott pontra lokalizál különböző gyűjthető dolgokat. Amellett, hogy ennek akár bizonyos gazdaságélénkítő hatása is lehet,[144] komoly biztonsági kockázata is van egyben. Nem sokkal az alkalmazás megjelenését követően a New York-i Central Parkban okozott kisebb csődületet egy ritka Pokémon feltűnése,[145] amit megpróbáltak sokan befogni egyszerre. Tekintsünk most el attól, hogy megfelelő körülmények között akár egy ilyen eset is elmérgesedhet, sokkal fontosabb számunkra az, hogy bárki szándékosan előállíthat egy ilyen helyzetet, amit saját céljaira használhat ki. Történhet ez véletlenszerűen kiválasztott célpontokkal, de akár célzottan is, hogy egy adott időben adott helyre csaljunk valakit. Nem csak rablók, pedofilok, de akár terroristák is könnyű szerrel hozhatnak létre ilyen pontokat, hogy aztán az odatévedő tömeg ellen merényletet hajtsanak végre. A terrorizmus lételeme a médiafelhajtás, egy ilyen óriási hype-pal járó alkalmazás esetében, mint a Pokémon Go is, minden bizonnyal, ha sikertelen merényletet is követnének el, garantáltan hosszú ideig vezető hír lenne.

Fontos leszögezni, hogy a Pokémon Go-val kapcsolatban leírt kockázatok, példák nem magából az alkalmazásból fakadnak, ellenkezőleg! Az alkalmazás népszerűsége újszerűségéből, eredetiségéből ered, amit kihasználhatnak rosszindulatú támadók. Minél népszerűbb, minél elterjedtebb egy alkalmazás, szolgáltatás, annál nagyobb eséllyel fogják valakik megtalálni a módját, hogy saját céljukra használják fel. A következő fejezet a közösségi média és az okos mobil eszközök kapcsolatában alaposabban körbejárja ezt az állítást.

4. A közösségi média és az okos mobil eszközök

A közösségi média napjainkban tapasztalt népszerűsége nem választható el az okos mobil eszközöktől, hiszen például a Facebookot naponta közel 1,2 milliárd ember használja, amiből 1 milliárdra tehető azok száma, akik mobiltelefonról érik el a közösségi oldalt. A közösségi média használatából fakadó kockázatok nagyban függenek a felhasználó biztonságtudatosságából. A közösségi média, ahogy lehet a kapcsolattartás, a szórakozás eszköze, úgy megfelelő körülmények együtt állása esetén rendkívül veszélyes lehet.

---

143 Konzuli tájékoztatás, In. Konzuli Szolgálat, http://konzuliszolgalat.kormany.hu/europa-utazasi-tanacsok?bosznia-hercegovina (utolsó letöltés: 2016. szeptember 16.).

144 Gondoljunk csak arra az esetre, amikor egy pizzázó tulajdonosa az üzletébe csábította így a játékosokat, akiknek jó része végül vásárolt is egy-egy szelet pizzát. Bővebben lásd: Mosendz, Polly- Kawa, Luke: Pokémon Go Brings Real Money to Random Bars and Pizzerias- Brick-and-mortar shops find themselves in the middle of an invisible game craze, In. Bloomberg, 2016. július 12., http://www.bloomberg.com/news/articles/2016-07-11/pok-mon-go-brings-real-money-to-random-bars-and-pizzerias (2016. szeptember 16.)

145 Hooton, Christopher: This video of Pokémon GO players in Central Park is proof that The Matrix is coming, In. Independent, 2016. július 12., http://www.independent.co.uk/arts-entertainment/pokemon-go-central-park-pokestop-gym-nyc-new-york-the-matrix-is-coming-a7132391.html (2016. szeptember 16.)

De mit is értünk közösségi média alatt?

A közösségi média fogalmát számos (elsősorban marketinggel foglalkozó) szerző[146] próbálta meghatározni, ebből következően alapvetően marketinghez kapcsolódó fogalmakkal tarkítva. Az Oxford Dictionaries[147] a közösségi médiát weboldalak és alkalmazások összességeként írja le, amelynek során a felhasználók tartalmat készíthetnek és megoszthatnak a közösségi hálózatokon. Ehhez a definícióhoz köthető Andreas Kaplan és Michael Haenlein által megfogalmazottak, mi szerint a közösségi média *„internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom."*[148]

Jelen tananyag szerzője elfogadva, de mégis kiegészítve a meghatározást, a közösségi média alatt *„olyan internetes oldalak és alkalmazások összességét érti, amelyeknél a szolgáltató csupán a keretet biztosítja, a tartalmat a felhasználók állítják elő. Ebből következik, hogy a közösségi média elsősorban a felhasználók interakciójából alakul ki, amely a többi felhasználó megosztásából, kiegészítéséből akár részben/teljesen új tartalom előállítását jelentheti. Elméletileg ez a tartalom folyamatosan változhat, kiegészülhet, akár új információk hatására bővülhet."*[149] Látni kell, a közösségi média ideológiája mögött nem egy új attitűd áll, az emberi történelem során mindig is igény volt a közösség szerveződésre,[150] csupán a technológiai fejlődés egy új csatornát biztosít ennek az igénynek a kielégítésére.

Látszólag nincs minőségi változás a két megfogalmazás között, azonban ha elfogadjuk ezt az új kitételt, kibővül a közösségi eszközök köre. Ez alapján a közösségi médiához sorolhatjuk a különböző okostelefonokra írt alkalmazásokat is, hiszen egyrészt ezek is a felhasználók közti interakcióra épülnek, másrészt integratív szerepet töltenek be a különböző közösségi eszközök közt. Mi sem igazolja jobban az állítást, mint a Google példája. A kezdetben keresőszolgáltatóként működő cég mára egy személyben integrálja a különböző közösségi eszközöket (blogszolgáltató, fénykép- és videómegosztó, közösségi hálózat, okostelefon platform stb.), miközben a nyílt forrású hírszerzés széles spektrumát is magába foglalja.[151] Ez alapján a közösségi média eszközeinek tekintjük a blogokat[152] (például Blog.hu, Blogspot.com) és mikroblogokat[153] (például Twitter, Tumblr), a közösségi hálózatokat (például Facebook, Google+), videó- és fényképmegosztó oldalak (YouTube, Indavideó, Picasa, Instragram), hírmegosztó oldalak (például Reddit, Google News), közösségi szerkesztésű tudásbázisok (például Wikipedia), közösségi játékok (például Second Life, World of Warcraft). Ez csupán egy rövid felsorolása az egyes eszközöknek, mert egyre több oldal jön létre a közösségi média alapján (közösségi vásárlás, közösségi akció, információ aggregációs oldalak, szolgáltatás- és termékvéleményező oldalak stb.), itt csupán a legjelentősebbek közül válogattunk.

---

146 Heidi Cohen, marketing szakértő gyűjtött össze 30 közösségi média fogalmat, amelyről bővebben lásd: http://heidicohen.com/social-media-definition/ (utolsó letöltés: 2016. szeptember 16.)

147 Lásd: http://www.oxforddictionaries.com/definition/english/social-media (utolsó letöltés: 2016. szeptember 16.)

148 Kaplan, Andreas- Haenlein, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010.

149 Bányász, Péter: A közösségi média használat biztonsági kérdései a védelmi iparban, In. Hadtudomány Online, 24:(1) pp. 49-67., 2014.

150 Keith Loell játszadozott el 2013 áprilisában a Forbes magazin hasábjain a gondolattal, hogy a közösségi média alapjai Sir Isaac Newtonhoz vezethetőek vissza, ugyanis a gravitációs elméletének publikálást követően a tudósok akár hónapokat is hajlandóak voltak utazni Londonba, hogy bekapcsolódjanak a tudományos diskurzusba, kiegészítve, megosztva a megfogalmazott „tartalmat", tételeket. Lásd: Loell, Keith: Did Sir Isaac Newton Invent Social Media? In. Forbes, 2013. április 18., http://www.forbes.com/sites/gyro/2013/04/18/did-sir-isaac-newton-invent-social-media/ (utolsó letöltés: 2016. szeptember 16.).

151 Elég, ha a különböző szolgáltatásaira gondolunk, az Earthre, Mapsre, Street Viewra, amelyek a Google szolgáltatásihoz hasonlóan ingyen biztosít hozzáférést a Föld műholdas képeihez, a világ teljes térképes adatbázisához, akár utcaszintű 360 fokos panorámakép formájában.

152 A blog internetes napló, amely a kezdeti személyes naplóból tematikus, szakmai tartalommá nőtte ki magát.

153 Jellemzően korlátozott tartalom előállítására biztosítanak lehetőséget, például 140 karakterben maximalizálják a közzétehető tartalmat.

A közösségi média az állandó változás terepe. E változás mögött gazdasági racionalitás áll, hiszen óriási profitot maximalizálhatnak a vállalatok. 2015-ben a Google csak az Egyesült Államokban az online reklámpiac közel 60 milliárd dollárjából 30 milliárd dollárt tudhatott magáénak.[154] A Facebook esetében ez körülbelül 8 milliárd dolláros bevételt jelentett. Ahhoz, hogy növelni tudják a bevételeket, két dologra van szükségük a cégeknek. Egyrészt, minél több, minél pontosabb adatot gyűjtsenek a felhasználókról, másrészt továbbra is maradjanak meg a felhasználók, ne kezdjék el a riválisokat használni. A megújulásnak nem csak az az eszköze, hogy folyamatosan új szolgáltatásokat vezetnek be, sok esetben a riválisok jobb termékét integrálják, azt követően, hogy felvásárolták őket. Miután a fiatalok egyre nagyobb számban kezdték el használni fényképmegosztásra a Facebook helyett az Instagramot, a Facebook felvásárolta az Instragramot, hogy így akadályozza meg, hogy mást használjanak helyette. Oly jellemző ez a piaci stratégia, hogy számos internetes start-up cég célja egy olyan alkalmazás alkotása, amit aztán a nagy cégek, félve attól, hogy a fejükre nőnek, még időben irreális összegekért felvásárolnak.

Az adatgyűjtésről korábban már volt szó a hozzáférési engedélyekkel kapcsolatban, de az csak egy kis részét jelenti a felhasználók személyre szabott adatbázisából. Több ezer szempont alapján elemzik a felhasználókat, de ezek nagy része nem ismert a felhasználók, a nyilvánosság számára. A Facebook például figyelembe veszi, kiknek a bejegyzéseire kattintunk, kiket követünk, kiket lájkolunk, kiknek a bejegyzéseit szoktuk kommentelni, kik csinálják velünk ugyanezeket stb. Azt is figyelemmel kísérik, ha számítógépen használjuk az oldalt, éppen hol tartózkodik az egérmutató.

Ezt az óriási mennyiségű adatot valamilyen eljárással elemezni szükséges, hogy minél pontosabb, személyre szabottabb hirdetést jeleníthessen meg az oldal számunkra. Ennek az algoritmusnak a feladata a Facebook esetében az is, hogy a hírfolyamunkat átláthatóvá tegye. Egy átlag felhasználónak több száz ismerőse van a Facebookon, aminek az a következménye, hogy olyan mértékű tartalom keletkezik, hogy a számunkra érdekes megosztások könnyen elveszhetnek. Persze lehetősége van a felhasználónak, hogy tiltson bizonyos tartalomtípusokat (például a mindenegyben.blog megosztásait), alkalmazásokat (játékok, kvízek) vagy felhasználókat, de még így is kezelhetetlen lehet a hírfolyam. Viszont így a felhasználó unatkozik, inkább más oldalakat látogat meg, így az algoritmus megpróbálja meghatározni azt, hogy a felhasználó milyen tartalmakat preferál, kiktől olvas szívesen bejegyzéseket, és milyen tartalomban. Ha például egy adott politikai oldalhoz köthető híreket keresünk fel gyakran, rendszeresen hozzászólunk ismerőseink ilyen témájú megosztásaihoz, akkor nagyobb számban fognak megjelenni az ilyen jellegű tartalmak.

Nagy port kavart egy volt Facebook-dolgozó közlése, aki azt állította, hogy a közösségi oldalon megjelenő hírfolyamot a cég szerkesztői alakítják, és nem a felhasználók érdeklődése.[155] Az oldalon tehát nem feltétlenül az az anyag kerül előtérbe, amelyre a legtöbben kattintottak – ahogy azt egyébként a Facebook mondja. A manipuláció során bizonyos tartalmakat eltüntetnek – állítja a Facebook egykori munkatársa. A Facebook Trending szekciója – amely Magyarországon még nem működik – a fontos híreket listázó sáv. A vád szerint a Facebook szerkesztőcsapata ennek tartalmát manipulálta. Az egykori alkalmazott szerint a cég egyenesen felszólította a szerkesztőit, hogy cenzúrázzák a konzervatív értékeket képviselő tartalmakat. A Facebook hírfolyamát kétféleképpen böngészhetjük: kiválaszthatjuk, hogy a „legfrissebb eseményeket" mutassa-e az oldal vagy az úgynevezett „legfontosabb híreket". Maga a Facebook sem titkolja, hogy rendszeresen kísérletezget a hírfolyamon megjelenő tartalmakkal, ennek nagyon egyszerű oka van: a hirdetési bevételek. Legutóbb azt jelentette be a Facebook, hogy blokkolni fogja azokat az oldalakat, amelyek szándékosan kattintás vadász címeket adnak a híreknek, hogy minél többen az oldalukra lépjenek. Korábban bejelentették, nagyobb teret

[154] Meeker, Mary: Internet Trends 2015, Kleiner Perkins Caufield & Byers, 2016. június 1., http://www.kpcb.com/internet-trends (utolsó letöltés: 2016. szeptember 16.)

[155] Nunez, Michael: Former Facebook Workers: We Routinely Suppressed Conservative News, In. Gizmodo, 2016. május 9., http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006 (utolsó letöltés: 2016. szeptember 16.)

adnak azoknak a bejegyzéseknek, amelyek barátaink képeit, írásait tartalmazzák, és ezzel egyúttal inkább háttérbe szorítják a híreket, cicás képeket. Előtte a videókat kezdték el preferálni és így tovább. A hírfolyam ilyen irányú befolyásolására nem csak ily módon van lehetőség. 2016 májusában a Wikileaks megvádolta a Facebookot, hogy blokkolja azoknak a híreknek a megosztását, amik Hillary Clinton demokrata elnökjelölt kiszivárgott e-mailjeire vonatkoznak. A Facebook a botrány hatására kijelentette, hogy csak átmeneti hiba volt, amit javítottak, majd ezt követően ismét meg lehetett osztani az erre vonatkozó híreket. Amennyiben nem hiba volt, hanem szándékos befolyásolás, úgy igen komoly állásfoglalást jelent a demokrata jelölt mellett.

2015 novemberében novemberben jelentette be a Facebook, hogy az elnökválasztás miatt azonosítanák a politikailag leginkább aktív felhasználókat. Ez a kampánystáboknak azért lenne nagyon jó, mert így irányított reklámokat lehet megjeleníteni a legmegfelelőbb embereknek, és irányítani az egyes posztok megjelenését is, hogy bizonyos emberek biztosan lássák őket. E mögött az a felismerés áll, ha megfelelő emberek osztanak tovább valamilyen politikai üzeneteket, akkor az ismerőseik felmérések szerint sokkal jobban megbíznak egy olyan politikai üzenetben, amit egy ismerősük oszt meg, mintha az közvetlenül egy párttól vagy egy politikustól származna. Vagyis a Facebook segítségével az amerikai pártok úgy reklámozhatnak, hogy a legtöbb felhasználó észre se fogja venni, hogy tényleg reklámot olvasnak. Ez az algoritmus persze nem a Facebook első politikai terméke, a cég régóta segít demográfiai adatok alapján célozni a felhasználóknak a politikai hirdetéseket. Viszont az új algoritmus ennek ellenére is sok vitát szülhet, hiszen fontos, hogy mi hogyan befolyásolja a politikai kampányokat. Míg a tévés politikai hirdetéseket nagyon szigorúan szabályozzák, a Facebook szinte szabályozatlan terület, hiszen nagyon nehéz lekövetni az ottani hirdetések forrását, nehéz megmondani azt is, hogy egyáltalán mi minősül hirdetésnek és mi nem.

A Facebook végzett egy kísérletet 2010-ben, azt vizsgálva, hogyan tudja befolyásolni a szavazási hajlandóságot, bevezettek egy „szavaztam" gombot. Ha ezt megnyomta valaki, az ismerősei körében megjelent, hogy ő szavazott, a profilképével, és több más, a gombot szintén megnyomó ismerős képével együtt. Aki pedig ezt látja a saját Facebook falán, de még nem volt szavazni, az elgondolás szerint érezni fog egy kis közösségi nyomást, hogy neki is el kellene mennie. A kísérletből az is pontosan kiderült, mekkora ez a nyomás. Az University of California adatai szerint azok, akiknek a hírfolyamában megjelent, hogy ismerőseik szavaztak, 0,39 százalékkal nagyobb valószínűséggel mentek el maguk is szavazni. Ami elsőre nem tűnik nagy dolognak, csakhogy ez összességében 340 ezer plusz szavazót jelentett. A példa kedvéért: 2000-ben 537 szavazaton múlt George W. Bush győzelme Floridában, így az elnöksége is. Ehhez képest már egyáltalán nem tűnik olyan kevésnek. A 2010-es kísérlet a választás eredményét nem változtatta meg, legalábbis célzottan semmiképp. Akkor véletlenszerűen választották ki a felhasználókat, akik falán megjelent/nem jelent meg a szavaztam-gomb. Ez alapján viszont elég könnyű továbbgondolni, hogy lehet ezzel a módszerrel célzottabban belenyúlni egy választás eredményébe. A felhasználók lájkjai és interakciói alapján meglehetősen pontosan belőhető, kire fognak szavazni. Ehhez pedig hozzá lehet igazítani, milyen hírek/funkciók jussanak, vagy épp ne jussanak el hozzájuk. A konkrét Trump-esetben pedig azt is tudni lehet, hogy szavazói jellemzően kevésbé képzettek, és nem városokban élnek. A Facebook ezeket az adatokat pontosan tudja a felhasználóiról, így ez alapján is be lehet lőni a mozgósítást. Ezt hívják digitális gerrymanderingnek – a körzethatár-átrajzolás virtuális változata.

A felhasználókon végzett kísérlet nem újdonság a Facebook esetében, 2014-ben került napvilágra ki, hogy 700 ezer felhasználót vontak be egy pszichológiai kísérletbe. Az embereket két csoportra osztották. Az egyik csoport feedjéből a negatív, a másikéból a pozitív posztokat vették ki különböző arányban. Tehát volt, akinek egyáltalán nem jelent meg pozitív/negatív tartalom, és volt, akinek csak kevesebb, mint máskor. Azt mérték, hogy ez változtatás hogyan befolyásolja azt, amit ez a 700 ezer kísérleti alany maga kitesz a Facebookra. Kiderült, hogy ha az emberek nem találkoznak pozitív bejegyzésekkel, akkor sokkal valószínűbb, hogy ők sem tesznek ki vidám tartalmat, sőt inkább negatív dolgokat posztolnak. Fordítva is igaz: ha valakinek a negatív dolgokat tüntették el a szeme elől, akkor ő is vidám dolgokat rakott ki. Ennek azért van jelentősége, mert korábban még nem bizonyították

ennyire egyértelműen, hogy a Facebook képes befolyásolni a használók érzelmeit, illetve hogy érzelmek átadhatóak személyes találkozás és testbeszéd nélkül. A Facebook és a kísérlet vezetője is igyekeztek kisebbíteni a dolog jelentőségét. Egyrészt azzal érvelnek, hogy valójában nem manipuláltak, csak bizonyos posztok nem jelentek meg, másrészt azzal, hogy az egésznek csak marginális hatása volt. A konkrét eredmény mindössze egy ezrelék körüli változás volt, vagyis ennyivel nőtt például a negatív hangvételű posztok aránya a negatív bejegyzésekkel bombázott csoportban. Illetve, hogy a kísérlet célja a felhasználói élmény javítása volt.

A gyanútlan felhasználót a hírfolyam befolyásolásán egyéb kockázatok is fenyegetik. Az előző fejezetben már volt szó vírusokról, és ahogy megjegyeztük, minél népszerűbb egy alkalmazás, annál nagyobb eséllyel írnak rá valamilyen kártevőt, hogy kihasználják a népszerűségét. Nincs ez másképp a Facebookkal sem. A Facebookra optimalizált rosszindulatú alkalmazások is eltérő célokat szolgálhatnak. Léteznek adathalászatra írt alkalmazások, de szép számmal találhatóak olyan alkalmazások, amelyek megfertőzik a felhasználó eszközét.

A clickfraud-ot támogató vírus az úgynevezett PPC alapú hirdetést, azaz pay per click-t használja ki. Ennek lényege, hogy a hirdető nem egy adott időszakra fizet, hanem a hirdetésre érkezett kattintás után. Ilyen hirdetéseket ajánl többek között a Google AdWords vagy a Facebook is. A clickfraud ezt használja ki: olyan kattintásokat generál az adott hirdetésre, ami mögött nem valós érdeklődők vannak, hanem robotok. E mögött gyakran a hirdető vetélytársai állnak, akik így akarnak anyagi kárt okozni.

Rendkívül népszerűek a különböző játékos-vicces alkalmazások Facebookon. Ezek az alkalmazások pár perces kikapcsolódást jelenthetnek a felhasználóknak, és amíg végigkattint a kérdéseken, „megtudja", mi volt az előző életében, melyik amerikai elnök volt stb. Ezek, amellett hogy sok esetben egyébként valamilyen adatgyűjtő alkalmazások, sokkal súlyosabb fenyegetéseket jelentenek. 2011-ben a „Mi az indián neved?" alkalmazást néhány nap alatt 800.000 ember töltötte ki, s utólag derült ki, hogy egy ékszer webáruház marketingkampánya az egész, s így fillérekért fért hozzá ennyi ember adatához, illetve tette rendkívül ismerté magát. Ezek a kisebb veszélyek csupán, de az adathalászat igencsak nagy károkat okozhat a felhasználóknak. Ha egy olyan fertőzött alkalmazást használ, ami kémprogramokat telepít a számítógépére, amik harmadik félnek enged hozzáférést a hálózathoz, igen komoly következményekkel járhat. 2013-ban a Kaspersky Lab és a Budapesti Műszaki Egyetemen működő Laboratory of Cryptography and System Security (CrySyS Lab) azonosított egy MiniDuke nevű vírust, amellyel valaki körbetámadta fél Európa kormányzatát, főleg a külügyet. Magyarországon négy megtámadott célpontról tudnak, összesen pedig 59-ről, 23 országból. Akkor a számítógép felett az Adobe Reader sebezhetőségét kihasználva vették át az irányítást, a Miniduke-ot célba juttató fájlt egy valódinak látszó PDF-dokumentumba csomagolták. A magyar támadásokhoz használt verzió egy Ukrajna NATO-csatlakozásához szükséges emberi jogi szeminárium megtartásáról szól. A Duke kiberfegyver-család mögött a későbbi szakértői vélemények szerint az orosz állam állt. És ha valaki szándékosan kormányzati számítógépeket használ, akkor vélelmezhetően valamilyen állami szereplő áll a háttérben, és teljesen mindegy, hogy melyik ország: komoly fenyegetést jelent. Márpedig adott esetben egy Facebookos alkalmazás is eszköze lehet annak, hogy megfertőzzék a számítógépeket.

Ransomwarekről korábban is volt szó, a Facebookon terjedő vírusok között is jó eséllyel bukkanhatunk ilyenre, így mindig legyünk körültekintőek, mielőtt megnyitnánk egy nem megbízható alkalmazást, honlapot. Csak a saját elővigyázatosságunk véd meg biztosan: mérlegeljünk a könnyelmű kattintgatás előtt. Ha a barátaink valamilyen idegen nyelvű linket lájkoltak, ilyenen bejelöltek, az egyből gyanús. Különösen igaz ez olyan oldalakra, amelyek valamilyen szenzációs leleplezést, erotikus tartalmat, hírességekkel kapcsolatos botrányokat ígér. Ha pedig lekattintottuk, és valamilyen Facebook- vagy YouTube-hasonmás oldalra, vagy ismeretlen videomegosztóra keveredtünk, ne kattintgassunk ott tovább, és semmilyen feltáruló adatmezőben, felugró ablakban ne adjunk meg adatokat. Célszerű olyan kiegészítőket telepíteni a böngészőnkbe, amelyek figyelmeztetnek a fertőzött oldalakra, s nem engedi megnyitni őket, ha csak mi jóvá nem hagyjuk (itt kimerevedik a képernyő, ahol példaként megjelennek a NoScript Security, illetve a Web of Trust nevű kiegészítők). Emellett

célszerű minden olyan alkalmazást mellőzni Facebookon, amelyek valamilyen „vicces” választ adnak, legyen szó indián nevünkről vagy kik a legközelebbi barátaink Facebookon stb.

Mi a teendő, ha egy Facebookos vírus megtámadta az eszközünket? Első lépésként nyissuk meg a Facebookot, majd válasszuk a Beállítások részt. A bal oldali listában az Alkalmazások fülre kattintsunk, majd az összes olyan alkalmazást, amelyet látunk a listában, az X-re kattintva távolítsunk el. Ha ezzel megvagyunk, lépjünk ki a böngészőből, majd válasszuk ki a Windows Vezérlőpultot (verziótól függően a Start menüben található, vagy újabb verzióknál a keresőben, ha beírjuk a Vezérlőpult, vagy Control Panel szavakat, egyből kiadja). Ezen belül keressük meg a Programok és szolgáltatások almenüt. Ezt követően válasszuk ki a böngészőt a listában, jelöljük ki kattintással, majd nyomjuk meg az Eltávolítás gombot. Célszerű minden böngészőt eltávolítani, amivel korábban beléptünk a Facebookra.[156] Ezt követően nyissunk meg valamilyen fájlkezelőt (akár a Windows sajátját), és keressük meg a böngészőnek megfelelő mappát a Felhasználók (angol Windows esetén Users) mappában. Ennek leggyakoribb útvonala a C:\Users\azönfiókjánakneve\AppData\Local. Itt kell letörölni a böngészőnek megfelelő mappát, hogy a maradék letöltött és konfigurációs fájlok is törlődjenek. Ha Firefoxot használunk, a Mozilla mappát keressük, Chrome esetén a Google-t és így tovább. Ha mindezzel végeztünk, indítsuk újra a számítógépet, és telepítsük újra a böngészőt. Az esetek 99 százalékában a Facebook-vírusnak már nyoma sincs. A Facebookkal összekapcsolt szolgáltatásokat ezt követően újra össze lehet kötni. Amíg a számítógép újraindul vagy a törlési-újratelepítési folyamatok zajlanak, az okos mobil eszközre telepített Facebook alkalmazást is töröljük le, majd telepítsük újra.

5. Social engineering és az okos mobil eszközök

Az internet oly sok tevékenység átformálása után a bűnözésben, hírszerzésben is rengeteg nóvumot hozott. Bár maga az internethasználat nagy mértékben elterjedt, a felhasználók nincsenek tisztában azokkal a veszélyekkel, amelyek rájuk leselkednek. Ennek egyik oka, hogy konstans technikai és technológiai innováció jellemzi az infokommunikációs szektort, amivel az átlag felhasználó nem képes lépést tartani, a bűnözők vagy a nemzetbiztonsági szolgálatok azonban rendkívül gyorsan adaptálják a megváltozott környezet eszközeit, eljárásait. A kibertérben napjainkban több területen és dimenzióban folyik háború, amelyben a támadók mindig előnyben vannak a védekezőkkel szemben. Abban a pillanatban, ahogy egy korábban sikeres támadási módszert sikerült kivédeni, rögtön új eljárásokat keresnek a sikeres támadás érdekében. Egy-egy igazán védett rendszer megtámadása adott esetben rendkívül költséges lehet, ami nem feltétlenül arányos a megszerezhető információ értékével. Hogy ezt megkerüljék, a támadók sok esetben a humán faktor gyengeségének kihasználásával kísérleteznek. Ahogy azonban a fizikai, logikai védelem esetében igaz, úgy a humán faktor szempontjából igaznak kell elfogadnunk: ahogy egyre tudatosabbak a felhasználók, egyre érzékenyebbek az információ- és adatbiztonságra, úgy a támadók egy szinttel mindig lentebb próbálkoznak, akiknél kevésbé alakult ki ez a fajta biztonságtudatos aspektus. Ebből egyenesen következik, hogy egy szervezet esetében mindenki lehet potenciális célpont, annak ellenére, hogy az emberek nagy része nem gondolja magát annyira érdekesnek, jelentősnek, hogy ő váljék egy támadás célpontjává.

Az ilyen jellegű támadások nagy részét az úgynevezett social engineering támadással hajtják végre. A fogalomnak napjainkban nincs igazán jó magyar megfelelője, így viszonylag nehéz egy pontos definíciót alkalmazni rá. Kevin D. Mitnick, a „legendás hacker” az alábbiak szerint fogalmazott: *„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”*[157] Douglas P. Twitchell megfogalmazásában *„a social engineering a*

[156] Mielőtt ezt megtennénk, javasolt előbb letölteni újra a böngészők telepítőfájlját, hogy könnyen újra tudjuk telepíteni.

[157] Mitnick, Kevin D.: A legendás hacker a megtévesztés művésze, Budapest, 2003., Perfact-Pro KFT., p. 348.

csalásnak vagy rábeszélésnek a gyakorlati alkalmazása információ – vagy ingóságok szerzése érdekében. A kifejezést gyakran használják számítógépes rendszer, vagy annak információ tartalmával kapcsolatban."[158] Christopher Hadnagy, a terület elismert szakértője szerint *„social engineering a művészete, még inkább a tudománya annak, hogy gyakorlatias műveletekkel befolyásoljuk az emberi lényeket, azért hogy a célunk érdekében cselekedjenek az életük néhány helyzetében."*[159]

Social enginering esetében megkülönböztetünk humán (például identitás lopás) és IT alapú (például előzetes információszerzés) technikákat.

Az okos mobil eszközök nem megfelelő használata a social engineering alkalmazásának széles tárházát biztosítja. Elég, ha arra gondolunk, hogy egy nem megbízható alkalmazás feltelepítésével számos információt szolgáltatunk ki magunkról. Természetesen ez esetben célzott támadásról van szó, de egy hiszékeny felhasználót könnyű megfelelő irányba terelni, hogy egy adott alkalmazást telepítsen- igaz, ehhez előzetesen fel kell mérni az érdeklődési körét, személyiségének jellemzőit. Ez ismét csak nem jelenthet problémát egy adat- és információbiztonságra kevésbé érzékeny személy esetében, hiszen ha rendszeresen publikál a nyilvánosság számára képeket, rendszeresen bejelentkezik különböző helyszínekről stb., nagyban megkönnyíti a nyílt forrású információgyűjtést. Az információgyűjtés, legyen szó nyílt forrásúról (OSINT), emberi erőn alapulón (HUMINT) vagy akár rádióelektronikai felderítésről[160] (SIGINT), elengedhetetlen, hogy olyan információkról rendelkezzünk a célszemélyről, ami alapján megfelelő módon tudjuk social engineering támadást végrehajtani.

Képzeljünk el egy személyt, aki rendszeresen csalja a házastársát, szeretőjével pedig valamilyen közösségi oldalon szervezi a találkozóit, míg a házastársának közben azt írja, túlóráznia kell. Ha egy nem biztonságos alkalmazás, egy előre feltelepített rosszindulatú programmal hozzáférnek a telefonja tartalmához a fentebb ismertetett eljárásokkal, akkor a célszemély könnyen zsarolhatóvá válik, hogy megtegye azt, amire a támadóknak szüksége van, például hozzáférni egy védett rendszerhez. Az IT alapú támadásokon kívül az okos mobil eszközök esetében beszélhetünk humán alapú támadásokról is. Ha például mellettünk ül a célszemély egy közösségi közlekedési eszközön, ugyanúgy olvashatjuk mi is az üzeneteinket, vagy ha pont akkor jelentkezik be egy olyan szolgáltatásba, ahová jelszót kell beírnia. De ha már kialakult valamilyen bizalmi kapcsolat vele, adott esetben a telefonját is kölcsönkérhetjük, mondván, lemerült a sajátunk, engedje meg, hogy egy hívást kezdeményezzünk róla, amit felhasználhatunk például egy vírusos oldal felkeresésére, amivel megfertőzhetjük az eszközt. Számos technika áll a támadók rendelkezésére, amelyek esetében csak a kreativitás szabhat határt.

***

Le kell számolni a biztonság illúziójával, hogy mi, felhasználók nem vagyunk érdekesek, eléggé fontosak, hogy ilyen támadások áldozataivá váljunk. Ahhoz, hogy minimalizáljuk a veszélyeket, elengedhetetlen, hogy nagyfokú érzékenységet tulajdonítsunk adataink védelméhez. Ez persze nem azt jelenti, hogy ha például csaljuk a párunkat, akkor elővigyázatosabban járjunk el, hogy ne válhassunk támadás célpontjává; törekedni kell olyan életvitelre, ami nem tesz minket zsarolhatóvá, ugyanis ha egy célpont különösen értékes, akkor bizony valakinek meg fogja érni az erőforrások megfelelő allokációja, hogy felfedje titkainkat. A közszférában dolgozók számára ez különösen érvényes. A biztonságtudatosság megteremtésében fontos szerep jut a Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet által kínált továbbképzéseknek, amelynek keretében ez a tananyag is elkészült; de ezek mellett a munkahelyeknek önálló biztonságtudatossági tréningeket célszerű szervezni, figyelmet fordítva az integritás programokra egyaránt.

---

158 Twitchell, Douglas P.: Social engineering in information assurance curricula, InfoSecCD 2006: Kennesaw, Georgia, US.

159 Hadnagy, Christopher: Social Engineering: The Art of Human Hacking, 2011., Indianapolis, USA, Wiley Publishing Inc.

160 A SIGINT részét képezi az ELINT, azaz az elektronikus hírszerzés, amelynek során a számítógépeken tárolt adatokhoz férnek hozzá.

6. Felhasznált irodalom

- 1139/2013, (III. 21.) Korm. határozat Magyarország Nemzet Kiberbiztonsági stratégiájáról, In. *Magyar Közlöny*, 2013/47.
- Bányász, Péter: A közösségi média használat biztonsági kérdései a védelmi iparban, In. *Hadtudomány Online*, 24:(1) pp. 49-67., 2014.
- Cohen, Heidi: 30 Social Media Definitions, In. HeidiCohen.com, 2011. május 9. http://heidicohen.com/social-media-definition/ (2016. szeptember 16.)
- Definition of social media in English, In. Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/social-media (2016. szeptember 16.)
- Ericsson Consumerlab: Smarthphones Change Citys, Ericsson Consumer Insight Summary Report, 2013. október, http://www.ericsson.com/res/docs/2013/consumerlab/smartphones-change-cities.pdf (2016. szeptember 5.)
- Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016, In. Press Release, 2016. augusztus 19., http://www.gartner.com/newsroom/id/3415117 (2016. szeptember 5.)
- Hadnagy, Christopher: Social Engineering: The Art of Human Hacking, 2011., Indianapolis, USA, Wiley Publishing Inc.
- Hooton, Christopher: This video of Pokémon GO players in Central Park is proof that The Matrix is coming, In. Independent, 2016. július 12., http://www.independent.co.uk/arts-entertainment/pokemon-go-central-park-pokestop-gym-nyc-new-york-the-matrix-is-coming-a7132391.html (2016. szeptember 16.)
- Index: Öngyilkos lett egy nő, mert kikerült a netre a szexvideója, In. Index, 2016. szeptember 15., http://index.hu/kulfold/2016/09/15/ongyilkos_lett_egy_no_mert_nem_nem_toroltek_le_a_szexvideojat/ (2016. szeptember 15.)
- Jakobi Ákos: A virtuális világ terei – Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése" című tanulmányához, In. *Magyar Tudomány*, 2002/11., pp. 1482–1491., 2002.
- Kaplan, Andreas – Haenlein, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010.
- Khandelwal, Swati: 26 Android Phone Models Shipped with Pre-Installed Spyware, In. The Hacker News, 2015. szeptember 3., http://thehackernews.com/2015/09/android-smartphone-malware.html (2016. szeptember 7.)
- Konzuli tájékoztatás, In. *Konzuli Szolgálat*, http://konzuliszolgalat.kormany.hu/Európa-utazasi-tanacsok?bosznia-hercegovina (2016. szeptember 16.).
- Loell, Keith: Did Sir Isaac Newton Invent Social Media? In. Forbes, 2013. április 18., http://www.forbes.com/sites/gyro/2013/04/18/did-sir-isaac-newton-invent-social-media/ (2016. szeptember 16.).
- Meeker, Mary: Internet Trends 2015, Kleiner Perkins Caufield & Byers, 2016. június 1., http://www.kpcb.com/internet-trends (2016. szeptember 16.).
- Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése, In. *Magyar Tudomány*, 2001/7., pp. 769-779., 2001.
- Mitnick, Kevin D.: *A legendás hacker a megtévesztés művésze*, Budapest, 2003., Perfact-Pro KFT., p. 348.
- Mosendz, Polly- Kawa, Luke: Pokémon Go Brings Real Money to Random Bars and Pizzerias- Brick-and-mortar shops find themselves in the middle of an invisible game craze, In. Bloomberg, 2016. július 12., http://www.bloomberg.com/news/articles/2016-07-11/pokmon-go-brings-real-money-to-random-bars-and-pizzerias (2016. szeptember 16.)

- Nunez, Michael: Former Facebook Workers: We Routinely Suppressed Conservative News, In. Gizmodo, 2016. május 9., http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006 (2016. szeptember 17.)
- Origo: Meghalt egy tinédzser pokémonozás közben, In. Origo, 2016. július 20., http://www.origo.hu/techbazis/20160720-pokemon-go-halal-baleset.html (2016. szeptember 16.)
- The 2015 Internet Organised Crime Threat Assessment (IOCTA), Europol, Hága, 2015., https://www.europol.Európa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (2016. szeptember 20.)
- Twitchell, Douglas P.: Social engineering in information assurance curricula, InfoSecCD 2006: Kennesaw, Georgia, US
- Williams, Owen: Lenovo caught installing adware on new computers, In. The Next Web, 2015. február 19., http://thenextweb.com/insider/2015/02/19/lenovo-caught-installing-adware-new-computers/ (2016. szeptember 7.)

FOGALOMTÁR

- *29-es Munkacsoport:* a 95/46/EK irányelv 29. cikkében meghatározott, a tagállamok adatvédelmi biztosaiból, illetve adatvédelmi hatóságainak képviselőiből álló független tanácsadó, véleményező és konzultatív fórum. Állásfoglalásaival és javaslataival segíti az Európai Bizottság munkáját az európai polgárok információs önrendelkezési jogának védelme érdekében.
- *Adaptív jelzőlámpa:* a forgalmi viszonyoknak megfelelően szabályozza a szabad jelzések ciklusait.
- *Adat:* közlésre, megjelenítésre vagy további feldolgozásra alkalmas entitás, amely számos megjelenési formát vehet fel (pl.: alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása.
- *Adatalany:* bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.
- *Adatbiztonság:* az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében.
- *Adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).
- *Adatintegráció:* az elmúlt időszak trendjeit figyelve látható, hogy az okoseszközökön (és nem csak ott) futó alkalmazások mind nagyobb integrációra törekednek egymással, a kapcsolódó felhőszolgáltatásokkal, az eszközök más funkcióival, de akár a közösségi médiával is. Ezek az integrációs törekvések mára odáig jutottak, hogy egyes appok telepítése során alapértelmezetten kérik le az adatokat az eszköz kontaktlistájából, az elérhető közösségi médiából vagy más, kommunikációra (is) használt alkalmazásból. Ezek a kapcsolódások és adatintegrációk ma még sok esetben kellően tudatos felhasználói magatartással csökkenthetők, de sokszor az ilyen korlátozások az alkalmazások funkcionalitásának a korlátait is jelentik. Céges környezetben használt okoseszközök esetén persze elvárás lenne az ilyen összekapcsolások korlátozása, illetve megtiltása, de az imént említett funkcióvesztés ennek az egyik legfőbb akadályozó tényezője. Azt is meg kell említeni, hogy lehetnek olyan esetek, amikor az adatok átadása és szinkronizálása – ha ellenőrzött körülmények között zajlik – a biztonság fokozását szolgálhatja. Ilyen eset lehet például az, ha egy lokális címjegyzék nem csak lokálisan, hanem – egy megfelelően védett környezetben – máshol letárolódik.
- *Adatfeldolgozó:* az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.
- *Adathordozó:* sok esetben elég nehéz elválasztani az adathordozókat a hardver elemektől. Ami a fő különbséget jelenti az az, hogy ezeket az elemeket arra tervezték, hogy hosszabb-rövidebb ideig megőrizzék és tárolják az információt. Ilyen módon az adatok jelentősen koncentrálódnak az információs rendszernek ezeken az elemein. A koncentrálódás pedig érzékennyé teheti ezeket az elemeket az információ sértetlensége és bizalmassága szempontjából egyaránt. Az „okos” eszközök többnyire beépítetten és csatlakoztatható módon is tartal-

maznak adathordozókat, amelyeknek a kontrolja egyértelmű elvárás az információbiztonság szemszögéből.

- *Adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése.
- *Adatkezelés jogalapja:* főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés.
- *Adatkezelés elvei:* a célhoz kötött adatkezelés követelménye, valamint az adatminőség követelménye. Ez utóbbi magában foglalja a pontos, teljes és naprakész adatok igényét, valamint az adatfelvétel és az adatkezelés tisztességes és törvényes mivoltát.
- *Adatkezelő:* az a személy vagy szervezet, aki az adatok kezelésének a célját meghatározza, és az adatkezelésre vonatkozó (beleértve a felhasznált eszközt) döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.
- *Adattovábbítás külföldre:* személyes adatok továbbítása az EGT-n (*Európai Gazdasági Térség,* vagyis az Európai Unió országai, továbbá Izland, Norvégia és Liechtenstein) kívül, harmadik országban adatkezelési tevékenységet folytató adatkezelőhöz.
- *Adatvagyontv.:* a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény.
- *Adatvédelem:* az adatkezelés jogszerűségét biztosító, főként szabályozási tevékenységek – elsősorban a védelmet biztosító szabályok és eljárások –, valamint az adatkezelési eszközök és módszerek összessége.
- *Adatvédelmi incidens:* személyes adat jogellenes kezelésének vagy feldolgozásának, így különösen a jogosulatlan hozzáférésnek, megváltoztatásnak, továbbításnak, nyilvánosságra hozatalnak, törlésnek vagy megsemmisítésnek, valamint a véletlen megsemmisülésnek és sérülésnek az esetei. Ez a fogalom-meghatározás összhangban van az Ibtv. által alkalmazott biztonsági esemény fogalmával, ezek együttes értelmezésével az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosítása – jogi szempontból – könnyebben elvégezhető.
- *Android:* egy *Linux* kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobileszközökre (okostelefon, táblagép) tervezve.
- *Automatizált adatfeldolgozással hozott döntés:* az érintett – kérelemre történő – tájékoztatásának a kötelezettségét írja elő az alkalmazott módszerről és annak lényegéről, azzal a kitétellel, hogy ez esetben az érintett részére lehetőséget kell biztosítani az álláspontjának a kifejtésére. További szabály, hogy az érintett személyes jellemzőinek az értékelésén alapuló döntés meghozatalára csak akkor kerülhet sor, ha a döntést az érintett kezdeményezésére valamely szerződés megkötése vagy teljesítése során hozták, vagy ezt olyan törvény teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja (pl. személyiség alapú online tesztek).
- *Autonóm jármű:* A jármű önmagát képes irányítani (vezet és navigál is)
- *Avtv.:* Az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. Ez a rendszerváltás utáni első adatvédelmi törvény, amely 2011. december 31-ig volt hatályban. 2012. január 1-től hatályon kívül helyezte az Infotv.
- *Belső adatvédelmi felelős:* az adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki a szervezet nevében felelős az adatvédelmi szabályok betartásáért és a személyes adatok védelméért.
- *Bécsi Közlekedési Egyezmény:* A közlekedési szabályok, jelzéseket és szimbólumok egységesítésének az egyezménye.

- *Big Data:* a cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és az ügyfelek számára.
- *Bitcoin:* egy virtuális fizetőeszköz, amely titkosított csatornán keresztül teszi lehetővé a fizetést. Ennél fogva különösen népszerű az illegális cselekmények finanszírozásában, legyen szó kábítószer- és fegyverkereskedelemről vagy akár a terrorizmus finanszírozásáról.
- *Bizalmasság elve:* az elektronikus információs rendszernek az a tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot és információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.
- *Biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
- *Biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek a felszámolása, a bekövetkezés okainak és felelőseinek a megállapítása, valamint a hasonló biztonsági események jövőbeni előfordulásának a megakadályozása érdekében végzett tervszerű tevékenység.
- *Biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége.
- *Biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének a meghatározása.
- *Biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.
- *Biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.
- *CERT (Computer emergency response teams):* számítógépes szükséghelyzeteket kezelő csoportok.
- *Célhoz kötött adatkezelés:* személyes adat kizárólag előre meghatározott célból kezelhető, valamely jog gyakorlása vagy kötelezettség teljesítése érdekében. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének pedig tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és – ha az adatkezelés céljára tekintettel szükséges – naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.
- *Clickjacking:* a felhasználó beleegyezésének megszerzése, amivel az áldozat rákényszerül, hogy olyan dolgot telepítsen, amit nem is szeretett volna.
- *Cloud computing* („számítástechnikai felhő” vagy „felhő alapú informatika”): a számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe vagy vállalati számítóközpontja, hanem egy távoli szerver vagy a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek és virtuális munkaállomások. Felhő alapú informatikai alapon működnek például a milliók által használt internetes levelező rendszerek (pl. *Gmail*) és az online tárhelyek (pl. *Dropbox*). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy költenie kellene az ehhez szükséges drága beruházásokra és személyzetet alkalmaznia a rendszerek fenntartásához szükséges kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok

ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját – főleg marketing – céljára is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni.

- *Cookie-k („sütik”):* rövid adatfájlok, amelyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse és kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl. egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl. egy honlap nyelvi beállítása), amely addig marad a számítógépen, amíg a felhasználó azt le nem törli. Az Európai Bizottság irányelvei alapján cookie-kat (kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek) csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetők a felhasználó böngészési szokásai.
- *Crime as a Service:* szolgáltatásszerű bűnözés.
- *Dark Web (Dark Net):* a *Deep Web* része, ahol alapvetően illegális cselekmények folynak.
- *DDoS (Distributed Denial of Service) támadás:* lásd elosztott szolgáltatásmegtagadással járó támadás.
- *Deep Web (Deep Net):* az internetnek az a része, amit nem indexelnek a különböző keresőmotorok.
- *DGYS:* Magyarország Digitális Gyermekvédelmi Stratégiája.
- *DJP:* Digitális Jólét Program.
- *DOS:* Magyarország Digitális Oktatási Stratégiája.
- *DoS (Denial of Service vagy DoS) támadás:* lásd szolgáltatás-megtagadással járó támadás.
- *Dokumentumok, dokumentáció:* az adattárolás és megőrzés hagyományos formája a (papíralapú) dokumentumok létrehozatala. Ha ezt a rendszerelemet ilyenformán értelmezzük, akkor az információbiztonsági vonatkozások – elvárás szintjén – nagyban megegyeznek az adathordozókéval. Ha azonban ezt a rendszerelemet úgy értjük, mint a dokumentumokban megjelenő információt, akkor valójában magával a védelem tárgyával állunk szembe, azaz ezeket kell megvédenünk. Az okoseszközök kapcsán általában nem igazán jelenik meg a papíralapú dokumentumok kérdésköre, a tárolt és feldolgozott adatok annál inkább. Ilyen módon fontos felmérnünk, hogy mihez férhet hozzá az eszköz, illetve mit lehet rajta tárolni.
- *DNFP:* Digitális Nemzet Fejlesztési Program.
- *eIDAS rendelet:* az uniós szintű elektronikus tranzakciókkal kapcsolatos bizalom, amely az online köz- és magánszolgáltatások, valamint az e-kereskedelem hatékonyságának növelése érdekében közvetlenül alkalmazandó általános hatállyal bíró rendelkezéseket tartalmaz a tagállamok számára.
- *Elektronikus információs rendszer:* az adatok és információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.
- *Elektronikus információs rendszer biztonsága:* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.
- *Elosztott szolgáltatás-megtagadásos támadás:* az informatikai szolgáltatás teljes vagy részleges megbénítása vagy a helyes működési módjától való eltérítése. Egy meghatározott al-

kalmazás vagy operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A támadás lényege, hogy lehetőség szerint megakadályozza a célgép elérését.

- *Első generációs adatvédelmi szabályozás:* a szabályozás középpontjában a számítástechnika fejlődéséből eredően az állami nyilvántartások adatai elektronikus tárolásából, és az adatoknak a nyilvántartásokban való keresésének a lehetőségeiből adódó kérdések és azok jogi reflexiója állt. A technológiai fejlődés lehetővé tette a nagytömegű automatizált adatfeldolgozást, amely a központi nyilvántartások kialakításának irányába mutatott. Az állam, mint nagy adatkezelő jelent meg, amely egy egyedi azonosítószám alkalmazásával kívánta kezelni a nyilvántartásokat és az azokban tárolt személyes adatokat. Ez vezetett odáig, hogy Európában – főként a jóléti államok körében – sorra jelentek meg az első szabályzók. A szabályozás elsődleges célja a fentiekben említett nagy állami adatbázisok átláthatóságának a megteremtése volt, amely alapvetően az automatizált adatkezelésekre terjedt ki, és hangsúlyos szerepet kapott benne a konkrét technológia szabályozása. Mindemellett ezek a szabályzók az egyén részére nem garantálták az általános rendelkezési jogot a személyes adataik felett. A szabályozás már ekkor is tartalmazta az adatvédelemi rendelkezések felett őrködő felügyeleti szervek feladat- és hatásköreit.
- *ENISA:* Európai Hálózat- és Információbiztonsági Ügynökség.
- *EUROCITIES:* olyan program, amely a stratégiaalkotás és a kutatás-fejlesztés területén hat tematikus témakörben (kultúra, gazdaság, környezet, tudásalapú társadalom, mobilitás, társadalmi ügyek, együttműködés) történő információ átadással segíti a partnervárosokat. Budapest is a program tagja.
- *Európa Tanács Adatvédelmi Egyezménye:* az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény (az Európa Tanács ún. 108-as Egyezménye). Az első jelentős, az aláíró államokra nézve kötelező erejű nemzetközi jogi dokumentum az adatvédelem terén. Magyarországon az 1998. évi VI. törvény hirdette ki, 1998. február 27-én.
- *Érintett:* lásd *adatalany*.
- *Érintett jogai:* az adatalanyt még az adatkezelés megkezdése előtt, de ezen felül kérésére bármikor egyértelműen tájékoztatni kell az adatkezelés minden részletéről. Az érintett kérheti az adatai helyesbítését, bizonyos esetben a törlését is, valamint törvényben meghatározott esetekben tiltakozhat a személyes adatainak a kezelése ellen.
- *Észlelés:* a biztonsági esemény bekövetkezésének a felismerése.
- *Felhasználó:* egy adott elektronikus információs rendszert igénybe vevők köre.
- *Fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszernek vagy az elektronikus információs rendszer elemeinek a védettségét és biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét és biztonságát.
- *Feketekalapos (black-hat) hacker:* azok a hackerek, akik tudásukkal visszaélve, haszonszerzés vagy károkozás céljából jogosulatlanul betörnek számítógépekbe vagy számítógép-hálózatokba. Sok *black-hat* válik később *white-hat* hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon *white-hat* hackerként, hogy előtte sohasem próbált betörni egy számítógépbe sem. Így a határ inkább az etikus és az etikátlan hackerekre osztható. A *black-hat* hackerek csoportjába tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba.
- *Fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelző-

rendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás védelme, a sugárzott és vezetett zavarvédelem, a klimatizálás és a tűzvédelem.

- *Folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.
- *Globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezeken a rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese.
- *Hacktivizmus:* olyan cselekedet, amelyben a támadók számítógép-hálózatokba hatolnak be, és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag bár nem azonos, mégis számos közös pont van a kiberterrorizmussal. Mindkettőre jellemző, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat a támadásokat, amelyeknek az a célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Bár a hatásuk elenyésző, mert nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport.
- *Harmadik generációs adatvédelmi szabályozás:* az infokommunikációs szolgáltatások térhódítása, az internet világméretű elterjedése és a fokozódó felhasználó igények (a közösségi oldalak elterjedése) miatt vált szükségessé a harmadik generációs adatvédelmi szabályozás kialakítása, amely jelenleg is tart (és szükség van a kiegészítésére vagy új generációs szabályozásra a kihívások kezeléséhez). A tartalomszolgáltatás megváltozása mellett ez a térhódítás óriási méretű adatbázisok kialakulását is jelentette, amely együtt jár az adatbányászati tevékenységgel. Komoly kockázatot jelent a mobileszközök elterjedése és ezzel összefüggésben a helymeghatározáson alapuló szolgáltatások elterjedése, ami nem más, mint a személy valósidejű tartózkodási helyének a közvetítése ismeretlen számú adatkezelő irányába. Ugyanakkor egyre nagyobb igény mutatkozik a felhő alapú szolgáltatások igénybevételére, amely alapjaiban rendezi át az adatok tárolásának a módját.
- *Hashtag:* a hashtaget először a Twitter vezette be és terjesztette el más platformokra. Ez egy olyan egyszerű címkerendszert takar, amin keresztül az eltérő forrásokat szűrni és kategorizálni lehet, és ami könnyed átjárást jelent egy téma mentén a különböző bejegyzésekben. Hashtaget a # szimbólummal kezdődően lehet elhelyezni.
- *Hardver:* az információs rendszerek (talán) legegyértelműbb eleme, amely magában foglal minden olyan eszközt vagy részelemet, amely az információ feldolgozásában, továbbításában és tárolásában részt vesz. Az „okos” eszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, amelyek ideiglenesen vagy állandó módon csatlakoztathatok az eszközhöz.
- *Hozzájárulás:* az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Különleges adatok esetében csak írásos formában adható meg.
- *HUMINT (Human intelligence):* emberi erővel folytatott hírszerzés.
- *Ibtv.:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.
- *Infotv.:* az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.
- *Információ:* valamilyen megfigyelés, tapasztalat vagy ismeret, amelyből következtetéseket lehet levonni és döntések alapjául szolgálhat. Az információ, ha úgy tetszik, nem más, mint jelentéssel felruházott adat, azaz az adatból akkor lesz információ, ha valamiről informál.
- *Információbiztonság:* olyan követelményrendszer, amelynek a középpontjában a bizalmasság, a sértetlenség és a rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt

hordozó adat milyen megjelenési formát vesz fel (pl. alfabetikus, numerikus, grafikus vagy képi forma) és milyen adathordozón jelenik meg.

- *Információszabadság:* a közérdekű, valamint a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog, amely elősegíti a közhatalom gyakorlásának demokratikus kontrollját és a közintézmények átláthatóságát (transzparencia).
- *Információs rendszer felhasználásával elkövetett csalás:* ha valaki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz.
- *Információs rendszer vagy adat megsértésének bűncselekménye:* ha olyan személy, akinek amúgy megvan a jogosultsága a szankcionált magatartásra (információs rendszerbe való belépésre, adat megváltoztatására és törlésére), túllépi a jogosultságának a kereteit, akkor már bűncselekményt követ el. Az információs rendszerbe való jogosulatlan adatbevitel önmagában nem szankcionálandó magatartás, csak abban az esetben, ha az további nem kívánt következményekhez vezet, így a rendszer működését akadályozza. Az alaptényállás vétség, amelyet a Btk. kétévi szabadságvesztéssel rendel büntetni.
- *Információs rendszer védelmét biztosító technikai intézkedés kijátszásának bűncselekménye:* akkor valósul meg, ha az elkövető az információs rendszer felhasználásával elkövetett csalás, illetve az *információs rendszer vagy adat megsértésének bűncselekménye* elkövetése céljából ehhez szükséges vagy ezt megkönnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz, illetve jelszó vagy ilyen számítástechnikai program készítésére vonatkozó gazdasági, műszaki vagy szervezési ismereteit más rendelkezésére bocsátja.
- *Információvédelem:* összetettsége miatt a definíciós meghatározás helyett azokat a tevékenységeket rögzítjük, amelyekkel maga a védelmi tevékenyég leírható. Ide sorolható az információt hordozó entitások (személyek és eszközök) védelme, azaz az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az iratés dokumentumvédelem, valamint a személyi védelem is. Az információvédelem célja – hasonlóan az adatvédelemhez – a jogosulatlan hozzáférés, módosítás vagy megsemmisítés elleni védelem és az információk folyamatos rendelkezésre állásának a biztosítása.
- *Internet of Things (Iot):* a *dolgok internete* kifejezés különböző, egyértelműen azonosítható objektumokra és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg *Kevin Ashton*, de a koncepció ötlete először 1991-ben vetődött fel. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, mérni és ezt egy másik eszköz felé kommunikálni is. Lehet ez egy okostelefon, egy vérnyomásmérő vagy az autónk fedélzeti számítógépe (ECU). Ezeknek az eszközöknek nincsenek sem méretbeli, sem pedig felhasználási megkötései.
- *iOS:* az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- *IS (Islamic State):* önmagát Iszlám Államnak nevező terroristacsoport.
- *ISO 2700x szabványcsalád:* az információbiztonsági menedzsment rendszerek mára alapvetővé vált szabványcsaládja. Története (az elődszabványaival együtt) a 90-es évek közepéig nyúlik vissza, és mára meghatározó szerepet tölt be a szervezetek információbiztonsági rendszereinek kialakításában és tanúsításában. A jelenlegi törekvések szerint ebbe a szabványcsaládba rendezi az ISO minden olyan szabványát, mely többé-kevésbé szorosan kapcsolódik az információbiztonsághoz. Ennek megfelelően igen népes a 2700x szabványcsalád, több tíz szabványból áll. Alapja az ISO/IEC 27001, amely alapvetően nem technikai, hanem egy menedzsment szabvány, még akkor is, ha tartalmaz technikai vonatkozású elvárásokat is. A felépítését tekintve két részből áll. A szabvány törzse tartalmazza a menedzsment rendszerekre vonatkozó elvárásokat, az A melléklet pedig az információbiztonsági

kontrollkövetelményeket. Ez utóbbiak kiterjedésükben és jellegükben hasonlóak a 41/2015. (VII. 15.) BM rendelet mellékleteiben megtalálható követelményekhez. Kockázatmenedzsment szempontból érdemes kiemelni ebből a családból az ISO/IEC 27005 szabványt, amely az információbiztonsági kockázatmenedzsmenttel foglalkozik. Logikája és felépítése hasonló a már korábban említett ISO 31000-hez, ugyanakkor több a kifejezetten információbiztonsági vonatkozása, és a mellékletei sok segítséget jelentenek egy kockázatkezelési eljárás kialakításához, illetve tartalommal való feltöltéséhez.

- *ISO 31000-es szabványok:* A kockázatelemzés elvégzéséhez az egyik legelterjedtebb módszertani segítséget nyújtó szabvány(család) az ISO 31000-es. Történetét tekintve nem egy réges-régen kialakult családtól beszélünk. Kiadásában és sikerében a különböző ISO szabványokon alapuló irányítási és menedzsment rendszerek (minőségirányítás, környezetközpontú irányítás és információbiztonsági irányítás), elterjedése, és kockázati alapokra helyezése játszotta a legnagyobb szerepet Mint általában az ilyen menedzsment jellegű szabványok, ez sem konkrét megoldást vagy egyszerűen, lépésről lépésre alkalmazandó technikát definiál, hanem azt a folyamatot, amit egy kockázatelemzés során végig kell vinni. Megadja, hogy milyen szempontokat kell figyelembe venni, amikor kiválasztjuk, illetve kialakítjuk a saját működésünknek leginkább megfelelő kockázatelemzést. Definiálja a kockázatelemzés-értékelés folyamatát, és a 31010-es szabvány különböző eszközöket mutat be, értékelve azokat abból a szempontból, hogy melyiket mikor érdemes használni a kockázatfelmérés során. Ezt a szabványt haszonnal forgathatja mindenki, aki segítséget szeretne kapni a saját eljárásainak kialakításában.
- *Jailbreaking:* olyan eljárás, amelynek folyamán az *Apple* telefonon keresztül a felhasználó *superuser*évé válik, vagyis egy olyan felhasználóvá, akinek teljes hozzáférése van minden utasításhoz és fájlhoz az operációs rendszerben.
- *Kiberbiztonság:* a kibertérben meglévő kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatokat elfogadható szinten tartják, és a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.
- *Kiberbűnözés:* célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, akiknek a tagjai rendkívüli adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ebben a területben rejlő lehetőségeket.
- *Kiberhadviselés:* az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még leginkább a konvencionális hadviselés támogatására.
- *Kiberkémkedés:* az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzés. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület.
- *Kibervédelem:* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését.
- *Kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az általa okozott kár nagyságának a függvénye
- *Kockázatazonosítás:* célja azoknak a helyzeteknek, lehetőségeknek és eseményeknek a felismerése, amelyek a kitűzött céloknak való megfelelést befolyásolhatják. Az azonosításnak a lehetőségek felmérésén túl magában kell foglalnia mindazokat a tényezőket, amelyek a kockázat kialakulásának a környezetét jelentik. Ebben ki kell térni azokra a folyamatokra, szabályozókra, technikai eszközökre, emberekre, rendszerekre, hardver és szoftver tényezőkre stb., amelyek relevánsak a kockázat és a környezet megértésének a szempontjából.

- *Kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.
- *Kockázatértékelés:* választ kaphatunk olyan kérdésekre, mint hogy kell-e kezelni egy kockázatot; ha igen, milyen sorrendben; megkezdhető-e egy adott beruházás vagy folyamat a jelenlegi paraméterekkel; a különböző lehetséges megoldások közül melyiket kell választani. A különböző besorolások és értékelése értelmezésére a legtöbb esetben nem két (elfogadható és nem elfogadható) hanem három (elfogadható, feltételekkel elfogadható és nem elfogadható) kategóriát célszerű létrehozni.
- *Kockázatfelmérés:* a kockázatoknak egy olyan növelt megértését nyújtja a döntéshozóknak és felelős résztvevőknek, amely befolyásolhatja a célok elérését és az irányítás megfelelőségét és hatékonyságát a szóban forgó helyen. Ez alapot ad a döntéshez, hogy a leginkább megfelelő megközelítést használják a kockázatok kezeléséhez.
- *Kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása. A kockázatokkal arányos védelem azt jelenti, hogy a védelmi intézkedésekre fordított költségeknek arányosnak kell lenniük a fenyegetések által okozott lehetséges károk értékével.
- *Kockázatkezelési terv:* összefoglalja mindazokat az intézkedéseket, amelyeket a szervezetnek el kell végeznie a különböző kockázatok megszüntetésére, átruházására és csökkentésére. A kockázatkezelési terv tartalmazza az intézkedéseket azok részletes bemutatásával együtt, az összerendeléseket, hogy egy intézkedés melyik azonosított kockázatra van hatással, a kockázatcsökkenés mértékét, illetve ebből következően a maradványkockázat értékelését, valamint az egyes maradványkockázatok elfogadását.
- *Korai figyelmeztetés:* olyan aktív szervezeti cselekvés, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni.
- *Közérdekű adat:* az állami/önkormányzati feladatot, illetve egyéb közfeladatot ellátó szerv kezelésében lévő és a tevékenységére vonatkozó vagy a közfeladatának az ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül a kezelésének a módjától, önálló vagy gyűjteményes jellegétől (így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre és annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat).
- *Kritikus adat:* az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;
- *Különleges adat:* a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallási vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, illetve a kóros szenvedélyre vonatkozó adat, valamint a bűnügyi személyes adat.
- *Létfontosságú információs rendszerelem:* a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azok az elektronikus információs létesítmények, eszközök vagy szolgáltatások, amelyeknek a működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné a vagy működőképességüket jelentősen csökkentené.
- *Linux:* egy operációs rendszer, a szabad szoftverek és a nyílt forráskódú programok egyik legismertebb példája.
- *Logikai védelem:* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.

- *Magyar kibertér:* a globális kibertér elektronikus információs rendszereinek az a része, amelyek Magyarországon találhatóak, továbbá a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.
- *Malware:* az angol *malicious software* (kártékony szoftver, káros szoftver vagy rosszindulatú szoftver) összevonásából kialakított mozaikszó, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (*worm*), kémprogramok (*spyware*), agresszív reklámprogramok (*adware*), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (*rootkit*).
- *Man-in-the-middle:* közbeékelődéses támadás, amely során mindkét fél azt hiszi, hogy közvetlenül egymással kommunikálnak, pedig mindketten csak a csatornát irányító rejtett szereplővel állnak kapcsolatban.
- *Mavtv.:* a minősített adat védelméről szóló 2009. évi CLV. törvény.
- *Második generációs adatvédelmi szabályozás:* a szabályozás kialakítását sürgette annak az álláspontnak az Európai Unión belüli térnyerése, amely szerint az adatok szabad áramlását úgy kell biztosítani, hogy a magánszféra és a személyes adatok védelme garantálva legyen. A második generációs szabályozás fő eleme, hogy a technológiai megközelítés helyett az adatkezeléssel érintett személyt – az adatgazdát – széleskörű rendelkezési joggal ruházta fel. A szabályozás egyaránt kiterjed az elektronikus adatkezelésekre és a manuális, tehát papíralapú adatkezelésekre. A szabályozásban megjelentek a nemzetközi dokumentumok, amelyek közül az egyik, ugyan nem kötelező érvényű, de számos máig is fontos alapelvet tartalmazó szabályt külön ki kell emelni.
- *MDM rendszerek:* a legelterjedtebb okoseszközök – az okostelefonok – már évek óta jelen vannak a szervezetek életében, és okoznak fejtörést az információbiztonsággal foglalkozó szakemberek számára. Éppen ezért a piacon egyre több eszköz és megoldás jelenik meg az okostelefonok technikai oldalról működtetett kontrolljának a megvalósítására. Ezeket összefoglaló néven MDM, azaz *mobile device management* rendszereknek nevezik. A különböző gyártók különböző megoldásokat kínálnak a szervezet méretének, céljainak és eszközparkjának a függvényében. Mivel ezek a megoldások is folyamatosan fejlődnek és változnak, a következőkben csak néhány jellemző gondolatot összegzünk, hogy mire is alkalmasak ezek a rendszerek. Egy szervezet saját megoldásának keresése során mindenképpen célszerű, ha tájékozódik a piacon aktuálisan fellehető megoldásokról, hiszen ezekben jelentős eltérések lehetnek, mind a technikai megoldást, mind pedig az árakat illetően. Az MDM rendszerek általában alkalmasak a mobileszközök és a rajtuk tárolt információk és alkalmazások, illetve a rajtuk folyó kommunikációs folyamatok központi, távoli védelmére és flottában történő menedzselésére, amely így nem csak egységesen, de viszonylag könnyen meg is valósítható. Az MDM fő funkciói között megtalálható az üzembe helyezés, amely alkalmassá teszi a készüléket a beszerzését követően annak üzembe helyezésére, cégprofil kialakítására és a device management rendszerhez való távoli csatlakoztatására.
- *Megelőzés:* olyan hatás bekövetkezésének az elkerülése, amelyet egy fenyegetés okozhat.
- *Megfelelő tájékoztatás:* az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

- *Minősített adat* (korábbi elnevezése államtitok vagy szolgálati titok): olyan, minősítéssel védhető közérdek körébe tartozó információ, amelyről a minősítésre jogszabályban felhatalmazott személy megfelelő eljárásban megállapította, hogy az adat érvényességi időn belüli nyilvánosságra hozatala vagy illetéktelen személy részére hozzáférhetővé tétele veszélyeztetné Magyarország biztonságát. A Szigorúan titkos, a Titkos, a Bizalmas és a Korlátozott terjesztésű jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása vagy nyilvánosságra hozatala bűncselekmény. A minősítéssel védeni kívánt közérdek lehet Magyarország szuverenitása és alkotmányos rendje; honvédelmi, nemzetbiztonsági, bűnüldözési és bűnmegelőzési tevékenysége; igazságszolgáltatási, központi pénzügyi és gazdasági tevékenysége; külügyi és nemzetközi kapcsolatai; valamint az állami szervei illetéktelen külső befolyástól mentes működésének a biztosítása.
- *OECD irányelvek:* a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Tanácsa által elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvek, amelyek 1980. szeptember 23-án léptek életbe.
- *Okostelefon (smartphone):* fejlett, gyakran PC-szerű funkcionalitást nyújtó mobiltelefon.
- *„Okos város" (smart city):* egy komplex stratégia, a benne foglalt célkitűzések és a meglévő eszközök, fejlesztések és infrastruktúrák összehangolását és egymást szolgáló tervezését jelenti a fenntarthatóság és hatékonyság jegyében.
- *OSINT (Open Source Intelligence):* nyílt forrású információgyűjtés a hírszerzés. Ez a katonai felderítés egyik információ- és adatszerző tevékenysége, amely során az információt nyílt adatokból gyűjtik.
- *NAIH – Nemzeti Adatvédelmi és Információszabadság Hatóság:* az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, amelynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének a felügyelete.
- *Nemzeti adatvagyon:* a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.
- *NMHH:* Nemzeti Média és Hírközlési Hatóság.
- *NTG:* Nemzeti Távközlési Gerinchálózat
- *PreDeCo (Preventive-Detective-Corrective) elve:* a védelmi feladatok közé sorolja a megelőzést, a korai figyelmeztetést, az észlelést, a reagálást és az eseménykezelést.
- *Ransomware:* olyan *malware*, amely valamilyen fenyegetéssel megpróbál pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszi a számítógépet vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, amelynek a hatására visszaállítja az eredeti állapotot.
- *Reagálás:* a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére és a további károk mérséklésére tett intézkedés.
- *Rendelkezésre állás elve:* annak a biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
- *Rootolás:* olyan eljárás, amelynek folyamán az androidos telefonon a felhaszáló root userré/superuserré válik, vagyis egy olyan felhasználóvá, akinek teljes hozzáférése van minden utasításhoz és fájlhoz az operációs rendszerben.
- *Rövidülő életciklus:* a legtöbb használati cikkünkre igaz, hogy a tervezett felhasználási idejük egyre rövidül, mind technikailag, mind erkölcsileg sokkal hamarabb elavulnak. Terméktípustól függően 1-3 évente a gyártók újabb típusokkal és fejlettebb tudású eszközökkel rukkolnak elő, ezzel teszik elavulttá az egy, esetleg két generációval korábban kiadott készülékeiket. A rövidülő életciklus és a folyamatos újítási kényszer azonban nem csak az eszközök gyártóit terheli, hanem a szoftverek készítőit is.
- *Sértetlenség elve:* az adat tartalma és tulajdonságai megegyezik az adattal szemben felállított

követelményekkel, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz az eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek az a tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme a rendeltetésének megfelelően használható.

- *Sérülékenység:* az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.
- *Sérülékenységvizsgálat:* az elektronikus információs rendszerek gyenge pontjainak (biztonsági réseknek) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.
- *SIGINT (Signals Intelligence):* rádióelektronikai felderítés – a hírszerzésnek egy fajtája, amely az ellenséges rádióforgalmazás (radar, távközlés, telemetria, IT) elfogása és elemzése alapján jut információhoz.
- *Social engineering:* az emberi tényező kihasználható tulajdonságaira és az emberi hiszékenységre építő támadási forma – olyan technikák és módszerek összessége, amely az emberek befolyásolására és manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését.
- *Súlyos biztonsági esemény:* olyan informatikai esemény, amelynek a bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek közvetlen veszélybe kerülhetnek, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, illetve alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.
- *Számítógépes eseménykezelő központ:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik (európai használatban: CSIRT [Computer Security Incident Response Team], amerikai használatban: CERT)
- *Számítógépes féreg:* egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá, illetve válnak a részeivé, addig a férgeknek nincs szükségük gazdaprogramra, hanem önállóan fejtik ki működésüket.
- *Személyes adat:* bármely meghatározott, azonosított vagy azonosítható természetes személlyel *(érintett)* kapcsolatba hozható adat és az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi ezt a minőségét, amíg a kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
- *Személyes adattal való visszaélés vétsége:* az követi el, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével, haszonszerzési célból vagy jelentős érdeksérelmet okozva, jogosulatlanul vagy a céltól eltérően személyes adatot kezel vagy az adatok biztonságát szolgáló intézkedést elmulasztja, vagy az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget és ezzel más vagy mások érdekeit jelentősen sérti.
- *Személyes adatok statisztikai célra történő felhasználása:* ebben az esetben érvényesül a célhoz kötöttség elve. A normaszöveg ilyenkor azt is rögzíti, hogy a statisztikai célra felvett, átvett vagy feldolgozott személyes adatok – eltérő törvényi rendelkezésnek hiányában – csak statisztikai célra kezelhetők, azzal, hogy a Központi Statisztikai Hivatal egyedi azonosításra alkalmas módon a kötelező adatkezelés keretében kezelt személyes adatokat átveheti és a törvényben meghatározottak szerint kezelheti.
- *Személyes adatok tudományos kutatás során történő kezelése:* ebben az esetben fokozottan érvényesül a célhoz kötöttség elve. A normaszöveg rögzíti, hogy a tudományos kutatás cél-

jára felvett személyes adat csak tudományos kutatás céljára használható fel. A tudományos kutatást végző szerv vagy személy személyes adatot csak akkor hozhat nyilvánosságra, ha ahhoz az érintett hozzájárult, vagy az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges. Ez esetben a személyes adat érintettel való kapcsolata megállapításának a lehetőségét ki kell zárni azzal, hogy a végleges kizárásig (lehetetlenné tételig) külön kell tárolni azokat az adatokat, amelyek a meghatározott vagy meghatározható természetes személy azonosítására alkalmasak.

- *Szervezet:* az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető.
- *Szoftver:* az információs rendszerek másik egyértelmű eleme (a *hardver* mellett), amely alatt a legszűkebb értelemben az információtechnológiai berendezéseket működtető programokat értjük. A jelen technikai szinten, amikor hétköznapi körülmények között az azonos hardverkiépítésű eszközök a legtöbb esetben a szoftvereknek köszönhetően a legkülönbözőbb feladatokra válnak alkalmassá, kijelenthető, hogy a szoftverek sokfélesége biztosítja az eszközeink sokféle feladatra való alkalmasságát. Az „okos” eszközök esetén szintén ilyen módon működnek, vagyis a különféle szoftverek a legkülönbözőbb tulajdonságokat biztosítanak nekik. Ebből adódóan fontos, hogy kellő alapossággal mérjük fel mind a szoftvereket, mind azok verzióit.
- *Szolgáltatás-megtagadásos támadás:* az informatikai szolgáltatás teljes vagy részleges megbénítása vagy a helyes működési módjától való eltérítése. Egy meghatározott alkalmazás vagy operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassulhat, elérhetetlenné válhat, esetleg össze is omolhat. A támadás lényege, hogy lehetőség szerint megakadályozza a célgép elérését.
- *Tablet:* hordozható számítógép, amelyet leginkább tartalomfogyasztásra fejlesztettek ki.
- *Teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.
- *Tiltakozás:* az érintett nyilatkozata, amelyben személyes adatainak kezelését kifogásolja és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.
- *Tiltott adatszerzés bűntette:* az elkövető a személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot jogosulatlan módon akarja megismerni. Ezeknek az adatoknak a jogosulatlan megszerzése megvalósulhat más lakásának, egyéb helyiségének vagy az azokhoz tartozó bekerített helynek a titokban való átkutatásával; az ott történteknek technikai eszköz alkalmazásával való megfigyelésével, rögzítésével; más közlést tartalmazó zárt küldeményének felbontásával vagy megszerzésével és tartalmának technikai eszközzel való rögzítésével; illetve elektronikus hírközlő hálózat útján másnak továbbított vagy azon tárolt adat kifürkészésével és az észleltek technikai eszközzel való rögzítésével.
- *Trójai progam:* egy olyan *malware*-program, amely nem magát próbálja lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az ún. hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz.
- *Uniós adatvédelmi irányelv:* az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Ez az Európai Unió 1995. október 24-én született általános adatvédelmi irányelve, amely – többek között – létrehozta az ún. 29-es Adatvédelmi Munkacsoportot.
- *URBACT:* olyan, tapasztalatcserét és tanulást támogató program, amely segíti az európai

fenntartható városfejlesztést. A program képessé teszi a városokat arra, hogy a főbb városi kihívásokra közösen megoldásokat dolgozzanak ki és az egyre komplexebb társadalmi változásokkal szembesülve a központi szerepüket megerősítsék. Az új, fenntartható gyakorlati megoldások integrált megközelítéssel adnak válaszokat a társadalmi, gazdasági és környezeti folyamatokra. A legjobb gyakorlati példákat és tapasztalatokat a programban résztvevő partnervárosok Európa-szerte megosztják egymással, a várospolitikában, várostervezésben érintett szakemberekkel és minden olyan érdeklődővel, aki elkötelezett a szűkebb vagy tágabb városi lakó- és munkakörnyezete felé.

- *Üzemeltető:* az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszernek vagy annak a részeinek a működtetését végzi és a működésért felelős.
- *Vírus:* olyan rosszindulatú program, amely képes sokszorosítani és terjeszteni magát, az egyik gépről a másikra. Ugyanez a féregre is igaz, azzal a különbséggel, hogy a vírus általában „befúrja" magát egy futtatható fájlba, hogy teljesítse a célját.
- *Zártcélú elektronikus információs rendszer:* a nemzetbiztonsági, honvédelmi, rendészeti és diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az erre a célra létrehozott szervezet és technika működését szolgálja.
- *Zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Császár-Biró Anna

Tördelőszerkesztő:
Vörösss Ferenc

ISBN 978-963-498-491-7 (elektronikus)

Az eredeti kiadvány
a **KÖFOP-2.1.1-VEKOP-15-2016-00001**
„A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése”
című projekt keretében készült el és jelent meg.