HADMÉRNÖK

IX. Évfolyam 2. szám - 2014. június

KOVÁCS Zoltán
zkovacs@nbsz.gov.hu

HORDOZHATÓ INFOKOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATÁNAK VESZÉLYEI A VÉDETT VEZETŐK BIZTONSÁGTUDATOSSÁGI KÉPZÉSÉNEK SZEMPONTJÁBÓL II.

Absztrakt

A védett vezetők mindennapi tevékenységéhez szorosan hozzátartozik a kommunikáció, és az ezekhez szükséges hordozható infokommunikációs eszközök (pl. okostelefon) használata. Védelmüket ezen a területen is biztosítani kell, hiszen ők mindig is kiemelt célpontjai voltak az információszerző támadásoknak. A védelem egyik legolcsóbb és leghatásosabb módja a biztonságtudatos használat, amelyre a védett vezetőket fel lehet készíteni. A cikksorozat első része áttekinti a védett vezetők információbiztonsági védelmének főbb kérdéseit, körülhatárolja a veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat, majd számba veszi az elemezendő biztonsági kategóriákat. A második rész az elsőben megadott kritériumok alapján összefoglalja az említett eszközök és szolgáltatások használata során jelentkező veszélyeket.

The communication and the use of portable infocommunication devices (e.g. smart phone) form an inherent part of the everyday activities of protected leaders. Their protection has to be provided in that field as well, because they have always been emphasised targets of attacks of unauthorized access for information. One of the most cost efficient and effective means of protection is the security awareness, which the protected leaders can be trained for. The first part of this article series reviews the main issues of the protection of data security of protected leaders, determines the Internet based services and portable infocommunication devices which should be analysed in terms of the threats, and describes the security categories which must also be analysed. By the criteria given in the first article the second part of this article series summarizes the threats appearing while using the above mentioned devices and services.

Kulcsszavak: *védett vezető, hordozható infokommunikációs eszközök, internet-technológián alapuló szolgáltatások ~ protected leader, portable infocommunication device, internet based services*

BEVEZETÉS

A védett vezetők információbiztonsági védelme összetett feladat. Ebbe ma már szorosan beletartozik az általuk használt hordozható infokommunikációs eszközök, valamint az azokkal folytatott kommunikáció védelme is. Ahhoz, hogy az információbiztonságot ebben a szegmensben is teljes körűen ki lehessen alakítani, több szervezet, sőt, a védett vezető aktív közreműködése is szükséges.

A cikksorozat első része rámutatott, hogy a védett vezetők információbiztonságának garantálásához az információbiztonság komplex megközelítése szükséges. Ennek érdekében a technikai elhárítást ki kell terjeszteni a védett vezetők által használt kibertérre is, azon belül pedig kiemelten kell kezelni az elterjedt személyi használatú hordozható infokommunikációs eszközöket és az internet-technológiára épülő szolgáltatásokra. Ugyanakkor azt is megállapította, hogy egyrészt a védelemnek ez csak az egyik része, másrészt a teljes körű védelem csupán technikai eszközökkel nem, vagy csak irreálisan magas költségekkel valósítható meg.

A védekezés egyik leghatékonyabb módszere a biztonságtudatos használat, amelyre a védett vezetőket is fel lehet, fel kell készíteni. Ehhez viszont személyre szabott oktatási tematikát célszerű kialakítani, amelyhez a kellő alapot a lehetséges veszélyek áttekintése adhatja meg. Ez a cikksorozat második része – az első részben leírt csoportosítás alapján – ezeket a veszélyeket tekinti át.

SZEMÉLYI HASZNÁLATÚ HORDOZHATÓ INFOKOMMUNIKÁCIÓS ESZKÖZÖK, ÉS AZOK HASZNÁLATÁVAL IGÉNYBE VETT INTERNET-TECHNOLÓGIÁRA ÉPÜLŐ SZOLGÁLTATÁSOK VESZÉLYEI

A biztonsági kategóriák csoportosítását követően már célirányosan meg lehet vizsgálni, hogy az egyes kategóriákban milyen veszélyekkel találkozhat a felhasználó, és ezek közül melyek azok, amelyek biztonságtudatos felhasználással elkerülhetők, vagy legalábbis a kockázat mértéke csökkenthető. Ez azért lényeges, mert azokra, amelyekre a nincs ráhatása a felhasználónak, azokat tudomásul kell venni és arról kell döntenie, hogy használja-e vagy sem az adott eszközt, szolgáltatást, míg azoknál, amelyeknél van ráhatása, ott ismertetni kell a veszélyeket és oktatni a kockázatok csökkentésének módjait. Egyszerűbben szólva ezek alapján lehet majd – természetesen a védett vezetőkre vonatkozó egyéb speciális keretfeltételek figyelembevételével – kidolgozni egy hatékony biztonságtudatos felhasználói képzés tematikáját.

Üzembiztonsági veszélyek

Az üzembiztonsági veszélyek gyakorlatilag két részre oszthatók: a felhasználó, mint üzemeltető által kontrollálható tényezőkre és a szolgáltatók által biztosított üzembiztonsági kérdésekre.

Az első csoportba tehát a felhasználó, mint üzemeltető által kontrollálható tényezők tartoznak. Az üzemeltető meghatározás ebben az esetben nem elírás. A felhasználónak ugyanis a hordozható infokommunikációs eszközök használatával vannak „üzemeltetői” feladatai, és felelősségei is. Ilyenek lehetnek például az eszközei rendelkezésre állásának biztosítása (pl. akkumulátor feltöltése, kímélő használat stb.), a készülékein tárolt adatok biztonsági mentése, vagy azok redundáns tárolása. Ezek azonban ismertnek tekinthetőek, hiszen egyrészt egyértelműek (pl. akkumulátor feltöltése), másrészt jelentős részük (pl. biztonsági mentés) az asztali számítógépek kapcsán már minden felhasználó számára nyilvánvalónak feltételezhetők.

A második csoport a szolgáltatók által biztosított üzembiztonság kérdése szintén egyszerűen rendezhető. A hordozható infokommunikációs eszközök esetében ez a gyártó által kínált garanciális és szervizelési feltételeket jelenti, amelyet a készülék vásárlásával a felhasználó elfogad. Mivel a védett vezetők esetében hivatali hordozható infokommunikációs készülékeiket kapják, ezért ebben az esetben számukra ez már adott tényként kezelhető, erre ráhatásuk nincs. A készülékekkel elért legnépszerűbb – és így a védett vezetők által is leggyakrabban használt – internet-alapú szolgáltatások (pl. közösségi oldalak, levelező rendszerek, tárhelyek stb.) igénybevételekor a szolgáltató által megírt, és minden felhasználó számára egyforma felhasználási feltételek – beleértve az üzembiztonsági (pl. rendelkezésre állás, redundáns tárolás stb.) kérdéseket – elfogadásáról, vagy adott esetben elutasításáról dönthet a felhasználó. Itt egyedi szerződések megkötésére, egyedi feltételek kialakítására nincs lehetőség.

Összességében tehát megállapítható, hogy a fent leírtak okán, az üzembiztonsági kérdésekkel a védett vezetőknek szóló biztonságtudatossági képzés során nem célszerű foglalkozni.

Adatbiztonsági veszélyek

Az adatbiztonság témaköre az adatokhoz való biztonságos hozzáférés (kezelés, használat stb.), valamint az illetéktelen hozzáférések megakadályozása kapcsán felmerülő problémákat tartalmazza. A három kategóriát összehasonlítva ez az, amelyre a felhasználónak a legnagyobb ráhatása van, függetlenül a felhasznált eszköz vagy szolgáltatás típusától, valamint az elfogadott felhasználói szerződés tartalmától. Ennek okán érdemes áttekinteni, hogy a védett vezetők adatai milyen veszélyeknek vannak kitéve hordozható infokommunikációs eszközök és internet-alapú szolgáltatások igénybevétele során. Alapvetően négy kategóriába sorolhatjuk ezeket a veszélyeket:

- illegális adatszerzés,
- nem valós adatok feltöltése,
- nyílt forrású információgyűjtés,
- egyéb veszélyek.

Az illegális adatszerzés talán a legismertebb kategória, ez az, amire általában mindenki gondol. Ma a kibertérben az illegális információgyűjtésére, azok kereskedelmére komplett iparág alakult. Például egy ügyfél adatait tartalmazó, ellopott banki adatcsomagot 50 Fontért lehet értékesíteni. [34] De nem csak a bűnözőktől, hanem az idegen titkosszolgálatoktól, ellenérdekelt felektől is tartani kell. Snowden által közzétett anyagok [35] megmutatták, hogy bizonyos titkosszolgálatok számára, ma már gyakorlatilag bármely „átlagfelhasználó" levelezése, tárolt adatai is megszerezhetőek, ha használja az internetet, és az arra épülő népszerű szolgáltatásokat.

A nem valós adatok feltöltésének veszélye már nem mindenki számára ennyire nyílván való, pedig ez egy egyre jobban megfigyelhető jelenség. Ebben az esetben egy megszerzett azonosítót, egy feltört honlapot, Facebook fiókot stb. nem információszerzésre használnak a támadók, hanem épp ellenkezőleg, hamis információk közlésére. Egy saját honlapot ért „deface[1]" támadás inkább csak kellemetlen, de egy saját blogban, vagy Facebook fiókban történt bejegyzés már akár magyarázkodásra késztetheti a politikust [36], adott esetben egy védett vezetőt. Ráadásul az incidens végén mindenkiben ott marad a kétely, hiszen a bejegyzés valódi feltöltőjének kiléte – főleg hosszabb idő elteltével – nagyon ritkán határozható meg egyértelműen.

[1] Deface (vagy defacement): általában weboldalak feltörését és tartalmának, kinézetének megváltoztatását jelenti. (További információ pl.: http://www.techopedia.com/definition/4870/defacement)

A nyílt forrású információgyűjtés veszélyei talán a legkevésbé ismertek. Ezt a technikát fel lehet használni az adott személyről elérhető információk összegyűjtéséhez (pl. profil elkészítéséhez), kapcsolati rendszerének feltérképezéséhez, vagy egy esetleges későbbi, akár kibertámadás előkészítéshez szükséges információk megszerzéséhez. A nyílt forrású információk között a támadóknak talán azok a leghasznosabbak, amelyeket a felhasználó saját maga tölt fel (ráadásul önként!) a különböző közösségi oldalakra, blogokra.

Az egyéb veszélyekbe tartozó problémák ugyan kapcsolódnak az előzőekhez, de mégis kilógnak a fenti három kategóriából. Ilyen például az adatok törlése az internetről. Egy korábban feltöltött információt ugyan eltávolíthat a gazdája, de – főleg a mindenki által hozzáférhető, pl. közösségi oldalak esetén – semmi sem garantálja, hogy azt másvalaki már nem mentette le, és töltötte fel máshová. Erre szokták mondani, hogy „az Internet nem felejt!" Ugyancsak az egyéb veszélyek közé tartozik a blogok, közösségi oldalak kommentjeinek témája, ahol a látogatók, követők le tudják írni a véleményüket a bejegyzésekről (is). Egy politikus, védett vezető esetén itt célzott kommentekkel egyszerűen indíthatók lejáratókampányok, vagy félrevihetők az eredeti kommentek irányai ellehetetlenítve az eredeti témáról a vélemények kifejtését, vagy akár el is riasztva a szimpatizánsok egy részét azok olvasásától.

Az említett veszélyek az „átlagfelhasználó" esetén is fennállnak, de a védett vezetők esetén – akik mindig is kiemelt célpontot jelentettek az ellenérdekelt felek számára – még fokozottabban igazak. A veszélyek általános áttekintése után célszerű megkeresni azokat a pontokat, amelyekre a felhasználónak, így adott esetben a védett vezetőnek is van, lehet ráhatása.

Az adatok elérésének egyik sarkalatos pontja az azonosítás. A leggyakrabban használt internet-alapú szolgáltatások esetében ez a bejelentkezési névre és a jelszóra korlátozódik. Veszélyt jelent az azonosítók mások általi megszerzése, vagy kitalálása, hiszen így a támadók teljes jogosultsággal hozzáférhetnek a felhasználói fiókhoz, annak adataihoz. Ez ellen a felhasználó tehet bizonyos lépéseket. A már bejelentkezéskor biztonságos kapcsolatot használó (pl. HTTPS) szolgáltatások használatával jelentősen csökkenthető az azonosítók lehallgatás útján történő megszerzése, így amennyiben lehetséges, célszerű ilyet választani. A jelszó feltörése (pl. brute force[2] módszerrel) ellen is védekezhet a felhasználó, ha a jelszógenerálás alapvető szabályait (legalább 8 karakter, kisbetű, nagybetű, szám, esetleg speciális karakterek vegyesen) betartja, és annak megfelelően gyakori cseréjét elvégzi. Fontos megjegyezni, hogy a szolgáltató hálózatára a felhasználónak nincs ráhatása, így például az ellen nem tehet óvintézkedéseket, hogy ha szolgáltató rendszeréből szerzik meg az támadók az azonosító adatokat. A hordozható eszközök esetében már több lehetősége van a felhasználónak. Itt gyakoriak és elterjedtek a különböző gyárilag beépített azonosító eljárások (pl. PIN kódok, képernyő-feloldó, ujjlenyomat azonosító). Ehhez plusz védelmet adhat a felhasználó, például a teljes háttértárat titkosító alkalmazás használatával, amelynél szintén a megfelelő jelszó beírása szükséges az adatok eléréséhez, az eszköz rendeltetésszerű használatához.

A jogosultságkezeléssel – ráhatás híján – a leggyakrabban használt internet-alapú szolgáltatások esetében nem kell foglalkozni. Ennek ugyanakkor már van jelentősége a hordozható infokommunikációs eszközök esetében. Bizonyos rendszerek esetében (pl. Windows) a jogosultságok beállíthatók, így korlátozhatók bizonyos adatokhoz, szoftverekhez való hozzáférések, vagy szoftvertelepítési jogosultságok. Ez pedig segíthet megelőzni rosszindulatú szoftverek telepítését (települését), vagy az adatokhoz való hozzáférést, esetleg azok módosítását.

[2] Brute force vagy nyers erő módszere, ahol a támadó az összes lehetséges jelszót végigpróbálgatva keresi meg a valódit. (További információ pl.: Biztonságos jelszavak és a gyenge jelszavak feltörése http://iesb.hu/logikai-biztonsag/biztonsagos-jelszavak-es-a-gyenge-jelszavak-feltorese/

Internet-alapú szolgáltatásnál adataink a „felhőben” utaznak, ott tárolódnak, így elemi kérdés, hogy azokat lehallgatás és akár szolgáltatói hozzáférés elleni védelem érdekében tikosítsuk Eszközök esetében kicsit másképp, de szintén értelmezhető kérdés. Ott például az azonosítás kapcsán már említett, teljes háttértárat titkosító megoldások alkalmazásával védhetőek adataink. Ez a védelem akkor is hatásos lehet, ha például az eszközt ellopják.

Hordozható eszközök tekintetében a fentieken túl, további lehetőségek is a felhasználó rendelkezésére állnak arra, hogy az elektronikus úton történő illetéktelen adathozzáférés veszélyét csökkentse. Ezek között vannak olyanok, amelyek már mindenki számára ismertnek tekinthetőek, ilyenek például a biztonsági szoftverek használata (pl. vírusirtók, internet-biztonsági programcsomagok). Fontos ezek naprakészen tartása és az ellenőrzések rendszeres elvégzése. Szintén ilyen a felhasználói szoftverek napra készen tartása, folyamatos frissítése. Ezzel ugyanis legalább a már ismert és javított sérülékenységek befoltozhatók. Vannak azonban olyanok, amelyek már nem ennyire értelemszerűek minden felhasználó számára.

Az egyik, hogy csak a feltétlenül szükséges szoftvereket telepítsük. Ennek több oka is van. Egyrészt minden szoftver tartalmaz(hat) olyan – publikusan még nem ismert –sérülékenységet, amelyet kihasználva a támadók hozzáférhetnek az eszközön tárolt adatokhoz, vagy telepíthetnek más rosszindulatú programokat. Másrészt vannak olyanok, amelyek telepítésével a felhasználó elfogadja és önként veti alá magát annak, hogy adatihoz a készítők hozzáférjenek. (Ma a legtöbb – főleg ingyenesen – android és iOS alkalmazás szerződési feltételei tartalmazzák, hogy ezt.) Harmadrészt pedig vannak olyanok, amelyekbe kifejezetten adatszerzési szándékkal írtak bele bizonyos kódrészleteket. [37]

A másik kevésbé ismert veszélyforrás a hardver sérülékenységek kihasználhatósága. Egyfelől bizonyos hardver elemek támadhatóak, így akár a velük kommunikáció lehallgatható (pl. Bluetooth, WiFi), akár rajtuk keresztül az eszköz felett az ellenőrzés átvehető. Ezek elkerülése érdekében egyrészt kerülni lehet bizonyos eszközök használatát (pl. Bluetooth billentyű), másrészt bizonyos beállítások használatával fokozni lehet a biztonságot. Ez utóbbira egy példa lehet a WiFi csatoló letiltása és csak szükség esetén történő használata. Ekkor ugyanis csökkenthető egyrészt az ezen keresztüli támadás, másrészt az általa bekapcsolásakor szórt információk (ugyanis azonnal keresni kezdi azokat a hálózatokat, amelyekre korábban már felkapcsolódott és ezek azonosítóit sugározza) lehallgatásának kockázata.

Összességében tehát megállapítható, hogy – bár a fenti felsorolás korántsem teljes, már így is bizonyítja – az adatbiztonsági kérdésekkel a védett vezetőknek szóló biztonságtudatossági képzés során kiemelten célszerű foglalkozni. Ez az a terület, ahol a felhasználó – ebben az esetben a védett vezető – a legtöbbet tehet elektronikus információinak biztonsága érdekében. Ezek egy részét (pl. WiFi csatoló kikapcsolása) ő maga képes elvégezni, míg más részében szakemberek (pl. egyéb biztonsági beállítások, biztonsági szoftverek telepítését az üzemeltető rendszergazdája, a hordozható eszközök átvizsgálását lehallgató eszközök, kémszoftverek megtalálása érdekében nemzetbiztonsági szakemberek) lehetnek, lesznek a segítségére. Ezen lehetőségek oktatása és fontosságuk tudatosítása a védett vezetők számára megkerülhetetlen.

Egyéb (jogi, fizikai stb.) biztonsági veszélyek

Az egyéb biztonsági kategóriába tartozó tényezőket a veszélyek szempontjából szintén a szerint érdemes áttekinteni, hogy azok elkerülésére, csökkentésére a felhasználóknak van-e bármilyen ráhatása.

A fizikai biztonságot kivéve, az ebbe a kategóriába eső biztonsági tényezőkre a felhasználónak nincs ráhatása. A hordozható infokommunikációs eszközök esetében nincsenek olyan jogi garanciák, amelyek az üzembiztonságon túlmutatnának, auditról, vagy esetleg más harmadik fél bevonását illető, nem technikai úton rendezendő kérdésről pedig nem beszélhetünk az említett készülékeknél. Az említett eszközökkel elérhető internet-alapú

szolgáltatásoknál már kicsit összetettebb, ám végeredmény szempontjából mégis hasonló a helyzet. A cikkben használt szűkített értelemben vett szolgáltatások esetén a felhasználónak – így a védett vezetőknek – is csupán a szolgáltató által kínált szerződés elfogadására, az abban megfogalmazott jogi lehetőségek igénybevételére van módjuk. Ráadásul, mivel a szolgáltatók a leggyakrabban külföldi telephellyel rendelkeznek és Magyarországon sem bejelentési, sem engedélyeztetési, sem egyéb (pl. hatósági felügyelet elfogadási, adófizetési stb.) kötelezettségük nincs, így probléma esetén még az országban hatályos jogi garanciák kikényszerítése is szinte lehetetlen. Auditról, vagy bármilyen más harmadik fél bevonását igénylő, nem technikai úton rendezendő kérdésről pedig itt sem beszélhetünk.

A fizikai biztonság esetében azonban már más, kettős képet kapunk. Egyfelől az internet-alapú szolgáltatásoknál a fizikai biztonságra, – hasonlóan a jogi kérdésekhez – a felhasználónak nincs ráhatása, nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogyan és hány emberrel, milyen technikai berendezésekkel, vasráccsal stb. őrzi az adatközpontjait.

Másfelől a hordozható infokommunikációs eszközök esetében a fizikai védelem teljes egészében a felhasználó feladata, így arra teljes mértékű ráhatása van. Ráadásul több veszélyt is megelőzhet, vagy azok kockázatát csökkentheti, ha felelősen végzi ezt a tevékenységet. Megakadályozhatja a készülék eltulajdonítását, így egyrészt elkerülhet egyfajta információvesztést, másrészt azt, hogy illetéktelenek hozzáférjenek az adataihoz. A fizikai felügyeletnek azonban nem csak a készülék elvesztése, eltulajdonítása és az ezzel járó anyagi-, és információveszteség miatt van jelentősége. A néhány percre, órára magára hagyott eszköz lehetőséget biztosíthat illetéktelenek számára az eszközön lévő adatokhoz való hozzáférésre, azok lemásolására, vagy valamilyen rosszindulatú szoftver telepítésére is. Ez utóbbival pedig nem csak a készüléken éppen fent lévő adatokhoz, hanem a felhasználó – ez esetben a védett vezető – későbbiekben folytatott kommunikációjához, felvitt adataihoz, mozgási (hely) adataihoz stb. is hozzáférhetnek a támadók. [38] [39]

Problémát jelenthet családtagok (pl. gyerek) hozzáférése is a védett vezető hordozható infokommunikációs eszközeihez. Egyrészt, akár véletlenül is feltölthet valamilyen oldalra olyan adatokat, amelyeknek nem lenne szabad kikerülniük (gondoljunk itt például egy véleményezés alatt lévő törvényjavaslatra, vagy beruházási tervre), másrészt pedig – a védett vezető tudta nélkül – telepíthet olyan programot, amely kártékony kódokat is tartalmazhat. [37] (Ezek veszélyeiről az adatbiztonság rész bővebben szól.)

Összességében tehát megállapítható, hogy az egyéb biztonsági kérdések közül a védett vezetőknek szóló biztonságtudatossági képzés során csupán a hordozható infokommunikációs eszközök fizikai biztonságának kérdéseivel célszerű foglalkozni, azzal viszont feltétlenül szükséges.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A cikksorozat rámutatott, hogy a védett vezetők információbiztonságának garantálásához az információbiztonság komplex megközelítése szükséges. Ennek érdekében a technikai elhárítást ki kell terjeszteni a védett vezetők által használt kibertérre is, azon belül pedig kiemelten kell kezelni az elterjedt személyi használatú hordozható infokommunikációs eszközöket és az internet-technológiára épülő szolgáltatásokra. Ezen eszközök és szolgáltatások tekintetében az információk megvédésének egyik leghatékonyabb – és nem utolsó sorban legolcsóbb – módja a biztonságtudatos használat Ennek kialakításához viszont személyre szabott oktatási tematikát célszerű kialakítani. A feltárt veszélyek és az oktatási tematika azonban – megfelelő adaptációval – más területeken (gazdasági, magán) is felhasználhatók, így több szempont miatt is célszerű körbejárni a témát.

A cikksorozat bemutatta azokat a veszélyeket, amelyek az elterjedt személyi használatú hordozható infokommunikációs eszközöket és az internet-technológiára épülő szolgáltatások használata során felmerülnek. Ezt követően már kidolgozhatóak azok a módszerek, amelyekkel az információk megvédhetők egy esetleges támadással szemben, vagy legalábbis a kockázatokat az elfogadható mértékűre csökkenthetőek. Másfelől feltárhatók azok a pontok, amelyeknél nem célszerű (hatékonysági, technikai vagy akár gazdasági szempontból) technikai eszközökkel védekezni, hanem biztonságtudatossági oktatással, képzéssel, a felhasználói szokásokat célszerű olyan irányba terelni, hogy a védett vezetők normál kommunikációs és egyéb felhasználói szokásaikkal ne okozzanak nemzetbiztonsági kockázatot.

Felhasznált irodalom

[1] Ügyfelek tízezreinek adatait lopták el egy brit nagybanktól http://sg.hu/cikkek/103209/ugyfelek-tizezreinek-adatait-loptak-el-egy-brit-nagybanktol (2014. 03. 24.)

[2] NSA Files: Decoded http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (2014. 03. 24.)

[3] Balogh Artúrt Gavráék sem tolerálták http://mno.hu/magyar_nemzet_belfoldi_hirei/balogh-arturt-gavraek-sem-toleraltak-1210883 (2014. 03. 24.)

[4] James Ball: Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data (2014. 01. 28.) http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data (2014. 03. 08.)

[5] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. problémái. Hadmérnök, VIII. Évfolyam 3. szám - 2013. szeptember pp. 184 – 197 - ISSN 1788-1919

[6] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. problémái. Hadmérnök, VIII. Évfolyam 3. szám - 2013. szeptember pp. 198 – 210 - ISSN 1788-1919