HADMÉRNÖK

IX. Évfolyam 2. szám - 2014. június

KOVÁCS Zoltán
zkovacs@nbsz.gov.hu

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

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

Napjainkban az információ védelme egyre nagyobb hangsúlyt kap, és különösen igaz ez a kibertérre. Katonai, állami szempontból értékes adatokat az érintettek mindig is megpróbálták a kor technikai színvonalának és az anyagi lehetőségeknek megfelelően, a lehető legjobban megvédeni. Az üzleti információkat is folyamatosan védték, védik tulajdonosaik, hiszen ehhez alapvető anyagi érdekük fűződik. Ám ezekben a szegmensekben az elektronikus úton folytatott kommunikációs és adattovábbítási lehetőségek, az internet-technológiára épülő szolgáltatások rohamos fejlődése új, korábban nem ismert kihívások elé állította/állítja az illetékeseket, döntéshozókat és a szakembereket. Azonban éppen ennek a technikai fejlődésnek köszönhetően adataink védelme a privát szférában is alaposan felértékelődött.

Az, hogy az élet szinte minden területén kiemelt szerepet kapott az információbiztonság, több tényezőnek köszönhető. Az egyik, a kibertér veszélyeinek ugrásszerű, minden felhasználót érintő növekedése, a másik az elektronikus kommunikációs és adattovábbítási lehetőségek, az internet-technológiára épülő szolgáltatások, valamint a személyi használatú hordozható infokommunikációs eszközök rohamos fejlődése, elterjedése.

A technológiák fejlődése és a felhasználási szokások nem választhatók szét egymástól. Egyfajta összefonódó spirált képezve, egymást is erősítve, gerjesztve hozták létre a mai népszerű kommunikációs formákat, adattárolási-, továbbítási lehetőségeket és egyéb internet-technológián alapuló szolgáltatásokat. A szélessávú és mobil internet elérések elterjedése, a hordozható eszközök (pl. ultrabookok, tabletek, okostelefonok stb.) hihetetlen mértékű fejlődése, a közösségi oldalak népszerűségének ugrásszerű növekedése, a különböző kommunikációs lehetőségeket biztosító internet-technológián alapuló szolgáltatások, felhő alapú rendszerek (mint pl. Facebook, Gmail, Dropbox, Twitter, Skype stb.), valamint az ezek használatát biztosító alkalmazások megjelenése minden nagyobb platformra (Windows, iOS, Andoid), mind-mind növelték a felhasználás mértékét, egyre több emberben erősítették az igényt a csatlakozásra, a használatra. [1] Ez a megállapítás a védett vezetőkre is igaz, hiszen ők is használják ezeket az eszközöket, technológiákat. [2] [3] [4] [5] [6]

A kibertérben ma minden felhasználót veszélyek egész sora fenyegeti, a kiberbűnözéstől (pl. banki adatok megszerzése után pénz leemelése a bankszámláról) [7] [8] [9], az idegen titkosszolgálatok adatszerző tevékenységéig (pl. Prism ügy [10]). Fokozottan igaz ez a védett vezetőkre, akik mindig is kiemelt célpontjai voltak az információszerző támadásoknak. [11] Éppen ezért fontos megvizsgálni, hogy mit is tehetünk a védett vezetők információinak – azon belül is legfőképpen elektronikus információinak – megvédése, biztonságának garantálása érdekében. A védekezés egyik leghatékonyabb módszere az internet-technológiára épülő szolgáltatások, és a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használata. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne kialakítható a megfelelő szinten. [12]

A biztonságtudatos felhasználásért azonban tennünk kell, hiszen a védett vezetők sokszor tudatában sincsenek a veszélyeknek, így azt sem tudják, hogyan kellene használniuk eszközeiket és az igénybevett szolgáltatásokat, hogy a használat már önmagában ne okozzon nemzetbiztonsági kockázatot. Ennek tudatosításában a leggyorsabb út az oktatás.

A cikksorozat célja, hogy a védett vezetők információbiztonsági védelmének tükrében rendszerezze személyi használatú hordozható infokommunikációs eszközök, valamint az ezekkel elérhető internet-technológiára épülő szolgáltatások használata során jelentkező veszélyeket. Ez megalapozza egy olyan oktatási tematika kidolgozását, amely a védett vezetők sajátosságaihoz igazodva, biztonságtudatos felhasználói szemléletet adhat számukra. A kitűzött végcél, egy kifejezetten védett vezetőknek szóló, az ő sajátosságaikat figyelembe vevő

biztonságtudatossági oktatási tematika kidolgozása azonban már nem a jelen, hanem egy következő cikk feladata.

Az elérendő eredmények ugyanakkor megfelelő adaptációval mások – akár magánemberek – számára is segítséget adhatnak az internet-technológiára épülő szolgáltatások és az azokat elérő személyi használatú eszközök kockázatmentesebb használatához.

Jelen cikk, céljának elérése érdekében, áttekinti a védett vezetők információbiztonsági védelmének főbb kérdéseit, majd körülhatárolja a veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat. Ezt követően számba veszi az elemezendő biztonsági kategóriákat, majd a következő cikk, az itt megadott kritériumok alapján összefoglalja az említett eszközök és szolgáltatások használata során jelentkező veszélyeket.

VÉDETT VEZETŐK INFORMÁCIÓBIZTONSÁGI VÉDELME

Az alap célkitűzés tehát az, hogy kidolgozásra kerüljön a védett vezetők számára egy testreszabott, különleges helyzetüket, időbeosztásukat, stb. figyelembe vevő biztonságtudatossági képzési tematika. Egyrészt azért, mert a Snowden ügy kapcsán megjelent hírek [10], a 2013-ban elfogadott kiberbiztonsági stratégia [13], valamint a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról törvény [14] mind az információk fokozottabb védelme irányába mutatnak. Másrészt azért, mert védett vezetőknél hagyományosnak tekinthető információvédelmi módszert, azaz a technikai elhárítást ki kell terjeszteni a kibertér általa használt régióira is.

A védett vezetők teljes körű, ezen belül az információbiztonsági védelmük meglehetősen összetett feladat. Ennek az egyik speciális részét képezi technikai elhárítás, mint a védett vezetők információbiztonsági védelmének egy jól körülhatárolható, és önállóan is működtethető része. A cikk ez utóbbinak a szempontjából közelíti meg a biztonságtudatossági képzés kérdését, és nem foglalkozik a védett vezetők egyéb védelmi kérdéseivel.

A biztonságtudatossági képzési tematika kidolgozáshoz szükséges vizsgálat és annak eredményéül előálló oktatási tematika azonban megfelelő adaptációval máshol, a gazdasági vagy akár a magán szférában is felhasználható. A probléma megoldásával így több – fontos és indokoltan megoldandó – célt is elérhetünk.

Ráadásul az internet-technológiára épülő szolgáltatások, valamint a személyi használatú hordozható infokommunikációs eszközök használatánál az információvédelem kapcsán hasonló problémákkal, veszélyekkel és jelenségekkel találkozunk akár a védett állami vezetőket, akár a nagyvállalatok vezetőit, akár a magánembereket tekintjük.

Erre egy tipikus példa, hogy a védett vezetők személyi használatú hordozható infokommunikációs eszközei esetében is vegyes (hivatali és magán) használatra kerül sor. Az ennek kapcsán felmerülő problémák és veszélyek nagyban hasonlítanak a saját használatú eszközök (BYOD (Bring Your Own Device, azaz Hozd a saját eszközöd)) esetében felmerülő problémákhoz, veszélyekhez [15] [16] [17] [18], azzal a különbséggel, hogy míg ott a dolgozó saját eszközét viszi munkába, addig itt (javarészt) hivatalból biztosított eszközöket használják fel magáncélra is. Az eredmény azonban hasonló, mindkét esetben a vegyes felhasználás miatt információbiztonsági problémákba ütközünk, még akkor is, ha a nem felhasználói tulajdonú eszközök talán kissé jobban védhetők, pl. rezsimszabályokkal.

A legszigorúbb, mindenre kiterjedő védelmet a védett vezetőknek kell megkapniuk, így a számukra kidolgozott biztonságtudatos felhasználói oktatási tematika (például a szükségtelen részek elhagyásával) könnyebben átültethető az élet többi területére, mint fordítva.

Technikai elhárítás változása, kiterjesztett értelmezése

Annak érdekében, hogy az állami szempontból fontos információkat a lehető legjobban meg lehessen védeni, az illetékes szervek rendszeresen végeznek technikai elhárítást a védett vezetők által használt helyiségekben. Ekkor – többek között – olyan megfigyelő, lehallgató stb. eszközöket keresnek, amelyekkel illetéktelenek megismerhetik a szobában zajló eseményeket, hozzájuthatnak az elhangzó beszélgetések tartalmához, vagy egyéb információkhoz. Természetesen a technikai elhárítás kiterjedhet a védett vezető által használt magánhelyiségekre (pl. saját lakás), vagy szállodai szobákra is.

A technikai elhárítás feladata, hogy felfedje, és ezáltal megakadályozza az illetéktelenek által folytatott információgyűjtést, felderítse a támadható, gyenge pontokat, sérülékenységeket, valamint felfedje az esetlegesen régebben végrehajtott információszerzés bizonyítékait (pl. mikrofon-fészek, falban maradt kábel stb.). Ma már nem elégséges az iroda, lakás, stb. „poloskátlanítása", hiszen sokkal könnyebben és kockázatmentesebben lehet információhoz jutni pl. egy postafiók feltörésével, vagy egy táblagépbe történő bejutással. Éppen ezért, a cél elérése érdekében az információvédelem komplex megközelítésére van szükség. Annak érdekében, hogy megérthessük, hogy a komplex megközelítés mit takar, először érdemes megvizsgálni, hogy milyen vizsgálatokkal célszerű kiterjeszteni a klasszikus értelemben vett technikai elhárítást annak érdekében, hogy a védett vezetők személyes (beleértve a hivatali és a magán) életterében az információbiztonságot garantálni lehessen.

Klasszikus technikai elhárítás kérdései

A címben a „klasszikus" jelző használata nem véletlen. Ebbe a kategóriába a technikai elhárítás hagyományos értelmezése szerinti feladatok tartoznak, ám a „technikai elhárítás" fogalmat már célszerűbb lenne a fentebb vázolt és a fejezet következő pontokban megadottak alapján kizárólag a kiterjesztett értelemben használni.

A technikai elhárítás (Technical Surveillance Countermeasures (TSCM)) meghatározásaként alapvetően elfogadhatjuk az USA Department of Defence által 2006-ban kiadott 5240.05 számú dokumentumban található definíciót, amely így szól:

„Olyan módszerek és intézkedések, amelyek felderítik, semlegesítik és/vagy kihasználják a minősített vagy érzékeny adatokhoz való illetéktelen hozzáférésre irányuló különféle (szervezett) bűnözői vagy külföldi titkosszolgálati információszerzési kísérleteket." [19]

Ugyanakkor az eltelt idő 2006 óta a technológia minden téren sokat fejlődött, amely az (illegális) információszerző lehetőségek bővülését is magával hozta. Ehhez a változáshoz természetesen a technikai elhárításnak is alkalmazkodnia kellett. Ezt az alkalmazkodást szemlélteti egy másik frappáns megfogalmazás, amely szerint a technikai elhárítás jelentése a következő:

„A TSCM vizsgálat egy szakképzett személyzet által nyújtott szolgáltatás technikai megfigyelő eszközök (helyiséglehallgató vagy más információszerző eszközök) jelenlétének és egyéb információbiztonsági veszélyek kimutatására, valamint azon technikai és kommunikációs biztonsági hiányosságok, sérülékenységek azonosítására, amelyek lehetőséget adhatnak a védett helyiségben történő technikai információszerzésre." [20]

A fenti megfogalmazásokból is látszik, hogy a technikai elhárítás alapvetően helyiséglehallgató és –megfigyelő eszközök keresésére vonatkozik, de ezen azért már lényegesen túlmutat. A felsorolt további feladatok azonban még mindig beleérthetők a klasszikusnak tekinthető technikai elhárítás fogalomkörébe, ám ennek részletesebben ismertetése nem tartozik a cikk céljai közé, így azokkal a továbbiakban nem foglalkozik.

Ugyanakkor kijelenthető, hogy bár a fenti meghatározások megfelelő általánosítással jól körülhatárolják a feladatokat, a kiterjesztett értelemben vett technikai elhárítás minden

lehetséges feladatát már nem foglalják magukban. A kiterjesztetten értelmezett technikai elhárítás pontos meghatározása szintén túlmutat a cikk keretein, ám az új definíció esetleges későbbi elkészítéséhez segítségül, valamint a cikk céljának eléréséhez célszerű áttekinteni, hogy melyek azok a feladatok, amelyeket mindenképpen bele kell érteni a kiterjesztett értelmezésbe. Ezeket a feladatokat mutatják be a következő részek.

Munkahelyi számítástechnikai eszközök biztonsági kérdései

A cím nem véletlen, ebbe a kategóriába kizárólag a munkahelyen található, nem hordozható számítástechnikai eszközöket (pl. asztali számítógép) értjük. Ugyanis a védett vezetők személyes használatában lehet(nek) az irodájában elhelyezett és a helyi hálózatba kötött (esetleg azon keresztül az internetet is elérő) számítógép(ek). Ezen hálózatok, eszközök védelme is az információbiztonsági feladat részét képezi, ugyanakkor ezek védelmét ketté kell választani.

Az általános IT biztonsági feladatok (pl. jogosultságok, biztonsági beállítások, vírusvédelem stb.) alapvetően a helyi biztonsági vezető és informatikáért felelős szervezet feladata és felelősségi köre. Az említett hálózatok, eszközök hardveres manipulálásának, esetlegesen ide elhelyezett információszerző eszközök (pl. lehallgató) keresése, felfedése azonban már a technikai elhárítás feladatkörébe tartozik. Hasonló kettősség mondható el az un. gyenge pontok kereséséről. A hagyományos értelemben vett IT sérülékenység-vizsgálat a helyi biztonsági vezető és informatikáért felelős szervezet feladata és felelősségi köre, míg a többi sebezhető pont feltárása a technikai elhárítóké.

Mindent egybevéve az irodai számítástechnikai eszközök védelme is hozzátartozik a védett vezető információbiztonságának megteremtéséhez, így bele kell érteni a technikai elhárítás kiterjesztett értelmezésébe.

Személyi használatú hordozható infokommunikációs eszközök biztonsági kérdései

A védett vezetők mindennapi tevékenységéhez szorosan hozzátartozik a kommunikáció, az információk cseréje, vagy adott esetben csupán azok gyors elérése. Ennek érdekében életük szerves részét képezi a személyi használatú, hordozható infokommunikációs eszközök használata. Ma már elképzelhetetlen, hogy az irodában rendelkezésre álló infokommunikációs eszközök, mint például az asztali számítógép, vagy a vezetékes (belső) telefon mellett ne használjanak mobiltelefont, hordozható számítógépet, vagy táblagépet. Ráadásul a technológiai konvergencia okán ezek egyre inkább egybeolvadnak, így biztosítva egy, kis méretű, hosszú üzemidejű készülékben a hang-, és adatkommunikációt. Ebbe a kategóriába kizárólag a hordozható eszközöket értjük (hordozható számítógép, táblagép, okostelefon, stb.), amelyek ráadásul sok esetben kettős célt (hivatali és személyes használat) szolgálnak.

Az információvédelem teljes körű megteremtéséhez, így a technikai elhárítás komplex értelmezéséhez ma már feltétlenül hozzátartozik a személyi használatú hordozható infokommunikációs eszközök, valamint az azokról igénybe vett internet-technológiára épülő szolgáltatások vizsgálata. Egyrészt azért, mert ma lényegesen egyszerűbb, veszélytelenebb bejutni egy védett vezető által használt infokommunikációs eszközbe, mint a fizikailag jól védett irodájába, az információszerzés ezen formájánál kisebb a felfedezés veszélye, ráadásul, ha ki is derül a támadás ténye, ebben az esetben még nehezebb a támadót azonosítani. Másrészt pedig azért, mert bizonyos szolgáltatások használatával „önként” ad meg magáról lényeges adatokat a felhasználó. Gondoljunk csak arra, amikor egy ingyenes alkalmazás letöltésekor elfogadjuk, hogy a szoftver gyűjtse, és a készítőhöz továbbítsa pl. az aktuális pozíciónkat, vagy akár a telefonkönyvünk tartalmát. Nem nehéz belátni, hogy ez is nem kívánt információszivárgáshoz vezet.

A fentiekből látható, hogy a védett vezetők információinak biztonsága érdekében a technikai elhárítást kiterjesztett értelemben kell használni, és a komplex információbiztonsági ellenőrzésnek ki kell terjednie a személyi használatú hordozható infokommunikációs eszközökre, valamint a védett vezető által használt internet-technológia alapú szolgáltatásokra is. Ahhoz azonban, hogy hatékonyan védekezni lehessen az itt felmerülő veszélyek ellen, először fel kell mérni majd csoportosítani azokat.

A veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások

A védett vezetők biztonságtudatossági oktatásának tematikáját, mint minden oktatási tematikát, csak megfelelő általánosítást és csoportosítást követően lehet kialakítani. Nem lehet teljesen személyre szabott (vagy pontosabban fogalmazva: teljesen, az éppen használt eszközökre és szolgáltatásokra szabott) oktatási tematikát kidolgozni. Egyrészt azért, mert a védett vezetők száma is elég nagy, így sok tematikát és azokhoz számtalan tartalmat kellene kidolgozni, oktatni. Másrészt pedig a folyamatosan megjelenő új eszközök, alkalmazások miatt is célszerű inkább általánosított jelenségekre, veszélyekre fókuszálni annak érdekében, hogy a jövőben megjelenő eszközök, szolgáltatások és fenyegetések esetében is használható ismeretekkel rendelkezzenek az oktatásban részesítettek.

Internet-technológiára épülő szolgáltatások és PC/SaaS rendszerek fogalmi vizsgálata

Már a cikk elején is felmerült, hogy az internet-technológiára épülő szolgáltatások, ezeken belül is kiemelten a felhő alapú rendszereket kell alaposabban megvizsgálni a kitűzött cél eléréséhez. A felhő alapú rendszerek esetében tovább lehet szűkíteni a kört, hiszen az „átlagfelhasználók” elsősorban a nyilvános számítási felhő (Public cloud (PC)) és szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)) típusú rendszereket (továbbiakban: PC/SaaS felhő alapú rendszerek) használják leggyakrabban. De nem csak az ők, hiszen ezek azok a szolgáltatások, amelyek bárki számára olcsón, sokszor ingyenesen elérhetők, azokat a védett vezetők is akár magán, akár hivatalos (pl. választókkal, szimpatizánsokkal való kapcsolattartásra, gondolataik gyors, széles rétegekhez történő eljuttatására [2] [3] [4]) célokra is használják.

A PC/SaaS rendszerek mindenképpen az internet-technológiára épülő szolgáltatások részhalmazának tekinthetők, ám a határvonalat, hogy mi tekinthető PC/SaaS rendszernek is, nagyon nehéz egyértelműen meghúzni. A PC/SaaS rendszerek meghatározásához a NIST (National Institute of Standards and Technology) Információtechnológiai Laboratóriuma (Information Technology Laboratory) által felállított, és mára már kvázi szabványként elfogadott definíciót és besorolást hívhatjuk segítségül. [21] Hozzá kell azonban tenni azt, hogy NIST munkatársai szerint is egy jelentősen fejlődő technológiáról van szó, ahol a definíciók is idővel fejlődni, változni, finomodni fognak. A NIST definíciója a lehető legáltalánosabban kívánja megfogalmazni a felhő alapú rendszerek alapvető tulajdonságait (igény szerinti önkiszolgálás, jó hálózati hozzáférés, erőforrás készletek, teljes rugalmasság, mért szolgáltatások), így azután lehetséges, hogy egy adott szolgáltatási-, vagy telepítési modellre rendkívüli módon jellemző tulajdonság nem, vagy csak korlátozott mértékben igaz a többire. A szolgáltatási-, és a telepítési modelleken belül leírtak is a lehető legszélesebb értelemben próbálják átfogni a felhő alapú rendszerek egyes típusait, ám minden valós rendszer más és más, ezért a besorolásnál mindig a főbb jellemzők teljesülését célszerű vizsgálni.

Az újonnan megjelenő funkciók, lehetőségek, az egy alkalmazás használatával elérhető többféle szolgáltatás, mind megnehezíti a besorolást. Gondoljunk például a Google szolgáltatásaira [22] Ezek egy része tisztán értelmezhető felhő alapú szolgáltatásként, egy

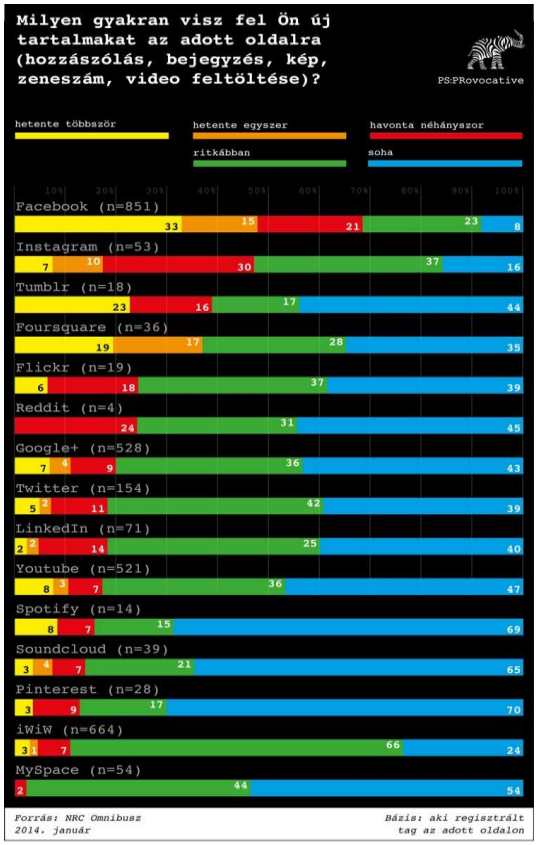
másik része kis jóindulattal, egy harmadik része pedig szinte egyáltalán nem. Éppen ezért a cikk, céljának eléréséhez, a kiterjesztőbb értelmű internet-technológiára épülő szolgáltatások megfogalmazást használja, de egyértelműen beleérti a PC/SaaS rendszereket is.

A leggyakrabban használt internet-technológiára épülő szolgáltatások jellemzői

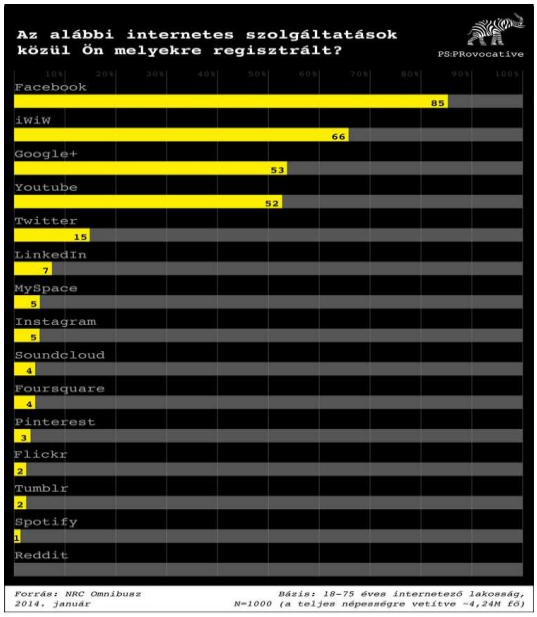
Megszámlálhatatlan azoknak az internet-alapú szolgáltatásoknak a száma, amelyeket bárki olcsón, sokszor ingyenesen használhat. Ráadásul szinte minden nap jelennek meg újak, amelyek között gyakran találkozhatunk teljesen új koncepción alapuló, vagy új igényeket kielégítő megoldásokkal. Éppen ezért rendkívül nehéz összefoglalni az említett szolgáltatások jellemzőit.

A védett vezetőknek kialakítandó biztonságtudatossági képzés okán az „átlagfelhasználók" által is leggyakrabban használt szolgáltatásokat érdemes megvizsgálni. Tehetjük ezt azért, mert a védett vezetőkről felhasználói szokásairól egyrészt nem elérhető kimutatás, statisztika, másrészt pedig azt feltételezzük, hogy azok ma nem térnek el jelentősen az „átlagfelhasználók" szokásaitól. A leggyakrabban használt internet-alapú szolgáltatások pedig a PC/SaaS legjellemzőbb tulajdonságaival bírnak, azaz a bárki által elérhető és igénybe vehetőek, használatukhoz a szükséges szoftvert a szolgáltató biztosítja (pl. böngészőben futtatott alkalmazás, vagy letölthető kliens program formájában [23]).

A kialakítandó képzés célját és az internet-alapú szolgáltatások népszerűségét tekintve elsősorban a valamiféle elektronikus úton folytatott kommunikációt [1] (pl. közösségi oldalak, levelezés, blogok, stb.) és a különféle adatok tárolását, megosztását lehetővé tevő szolgáltatásokat (pl. YouTube, Dropbox stb.) kell figyelembe venni. [24] [25] [26] Igaz ez a magyar viszonyokra is, mint ahogy azt egy a közösségi oldalak magyarok általi használatát vizsgáló felmérés is bizonyította. [27] Erre mutat jellemző adatokat az 1. és a 2. ábra.



1. ábra. Tartalomfeltöltési szokások
Forrás: http://psprovocative.com/kozossegi-elet-facebookon-tul/, (2014. 03. 14.)



2. ábra. Internetes szolgáltatások használati szokásai
Forrás: http://psprovocative.com/kozossegi-elet-facebookon-tul/, (2014. 03. 14.)

A leggyakrabban használt személyi használatú hordozható infokommunikációs eszközök jellemzői

Ma a leggyakrabban használt személyi használatú, hordozható infokommunikációs eszközöknek az okostelefonokat, a tableteket és a notebookokat tekinthetjük. Természetesen az elmúlt évek (évtizedek) tendenciája, a technológiák konvergenciája ebben a szegmensben is – ráadásul egyre gyorsuló formában – megtalálható, így valószínű, hogy néhány év múlva az említett három – jelenleg még markánsan elkülöníthető – csoport helyett csupán egy lesz jellemző. [28]

Az eszközök eltérő kivitelük, operációs rendszerük, stb. mellett is rendelkeznek közös tulajdonságokkal. Ilyenek az internet nagy sebességű, vezeték nélküli (pl. LTE, WiFi), ezáltal az internet-technológiára épülő szolgáltatások elérése, a kis méretek, a könnyű hordozhatóság, és a viszonylag nagy (akár tíz óra feletti) üzemidő. [29] [30] [31]

Miután a védett vezetők is a fenti három kategória valamelyik (vagy akár mindegyik) eszközét használják [5] [6] [32], ezért érdemes a veszélyek szempontjából is a három kategóriát együtt, azok közös jellemzői alapján vizsgálni.

Elemezendő biztonsági kategóriák

Az internet-technológián alapuló szolgáltatások esetében az elemezendő biztonsági kategóriák meghatározása elvégezhető a felhő alapú rendszereknél alkalmazott, kifejezetten a nemzetbiztonsági szolgálatok és a rendvédelmi szervek szempontjából megfogalmazottak szerint. [12] [33] (Természetesen a törvényes ellenőrzés vizsgálata a veszélyek feltárásához és a biztonságtudatos használat oktatási tematikájának kialakításához nem releváns, így attól eltekinthetünk.) Ugyanakkor ez a csoportosítás felhasználható a személyi használatú infokommunikációs eszközök biztonsági elemzésénél is, amelynek két oka is van. Az egyik, hogy az elérendő cél, azaz a védett vezető információbiztonságának garantálása a személyi használatú infokommunikációs eszközök, valamint az általa használt internet-technológia alapú szolgáltatások esetén szorosan összefügg, és nem érdemes az egyiket a másik nélkül vizsgálni. A másik pedig az, hogy a személyi használatú hordozható infokommunikációs eszközökre is értelmezhetőek ezek a kategóriák.

A vizsgálandó biztonsági kérdéseket – átvéve és elfogadva a [12] –ben leírtakat – az alábbi 3 fő csoportba célszerű sorolni:

- 1. üzembiztonság,
- 2. adatbiztonság,
- 3. egyéb (jogi, fizikai stb.) biztonság.

1. Üzembiztonság

Üzembiztonság kérdése azokat a jellemzőket foglalja össze, amelyek a rendszerek megbízható, üzemszerű működésével függnek össze. Ilyenek lehetnek például:

- elérhetőség: a tárolt adatok hozzáférhetősége onnan és akkor, ott és akkor, amikor a felhasználó szeretné;
- folyamatos szolgáltatás/rendelkezésre állás: internet-alapú szolgáltatásnál a szerződésben előírtak szerint (pl. 95%, de a szolgáltatás kiesés nem hosszabb, mint 30 perc), eszközök esetén kicsit másképp, de szintén értelmezhető kategória;
- katasztrófa utáni visszaállítás: terv a lehető leggyorsabban, és lehetőleg adatvesztés nélkül történő adat-visszaállításra;
- hordozhatóság/interoperabilitás: adatok, átvitele egyik szolgáltatótól a másikhoz, vagy egyik eszközről a másikra megoldható legyen, ha szolgáltatót, vagy eszközt kívánunk váltani;
- redundancia: magas rendelkezésre állás biztosítása a teljes infrastruktúra és a kapcsolódó eszközök tekintetében egyaránt.
- adatformátum: milyen formátumban állíjuk elő, tároljuk, továbbítjuk, stb. adatainkat hiszen az adatkonverzió sok időbe és pénzbe kerülhet.

2. Adatbiztonság

Adatbiztonsági kérdésnek tekinthetünk minden olyan tényezőt, amelyek a felhasználók adataihoz való biztonságos hozzáférés (kezelés, használat stb.), valamint az illetéktelen hozzáférések megakadályozása kapcsán felmerül. Ilyenek lehetnek például:

- adatszegregáció: többfelhasználós környezet lévén biztosítani kell, hogy az egyes felhasználók csak a saját adataikhoz férjenek hozzá.
- szolgáltatói adathozzáférés: internet-alapú szolgáltatás esetén számolni kell azzal, hogy a szolgáltató (és emberei) hozzáfér(het)nek a felhasználó adataihoz, legyen szó akár a munkájához kapcsolódó, akár szándékos (rosszindulatú) adatelérésről. (Eszközök esetében kicsit másképp, de szintén értelmezhető kérdés.)
- (nem biztonságos, vagy nem teljes) törlés: meg kell oldani, hogy ha a felhasználó töröl egy adatot, az biztosan törlődjön (a biztonsági mentések és a redundáns tárolás ellenére is), visszaállíthatatlanul, mindenhonnan.
- alkalmazásbiztonság: a használt, futó alkalmazások sérülékenységei is lehetőséget teremthetnek a felhasználó adataihoz való illetéktelenek általi hozzáférésére, ezért azokat ilyen szempontból is vizsgálni, tesztelni kell a szolgáltatásokat, eszközöket.
- titkosítás és kulcskezelés: internet-alapú szolgáltatásnál adataink a „felhőben” utaznak, ott tárolódnak, így elemi kérdés, hogy azokat a védelem érdekében tikosítsuk. (Eszközök esetében kicsit másképp, de szintén értelmezhető kérdés.)
- azonosítás és jogosultság kezelés: alapvető feltétel, hogy a bejelentkezőt nagy biztonsággal azonosítani lehessen, és csak azokhoz a szolgáltatásokhoz és adatokhoz férjen hozzá, amelyhez jogosultsággal rendelkezik.
- virtualizáció: a virtualizált környezet kapcsán új, korábban a „hagyományos” informatikában nem ismert támadások jelentek meg (pl. másik felhasználó adatainak elérése a közös fizikai memóriából), amelyekre fel kell készülni.

Az adatbiztonság kéréskörét az adatok életciklusán keresztül érdemes megvizsgálni, amelyet az 3. ábra szemléltet.

3. ábra. Az adatok életciklusa
Forrás: https://securosis.com/blog/data-security-lifecycle-2.0, (2012. 01. 05.)

Elsősorban az internet-alapú szolgáltatások használata miatt az adatok életciklusának 6 állomását biztonsági szempontból 2 fő csoportra célszerű bontani: az adatmozgással járó és az adatmozgással nem járó műveletekre. Ezt pedig azért célszerű megtenni, mert ha internet-alapú szolgáltatásokról beszélünk, akkor, ha a felhasználó bármilyen aktív műveletet végez, az az adatok mozgásával fog járni. Márpedig amennyiben ezt figyelembe vesszük, akkor a felhasználó és a szolgáltató felelősségi körét, ezáltal a felhasználó ráhatását veszélyekre, kockázatokra így jobban szét tudjuk választani.

3. Egyéb (jogi, fizikai stb.) biztonság

Ebbe a kategóriába tartozik minden olyan biztonsági kérdéskör, amelyeket nem technikai úton kezelünk, és akár egy harmadik fél is bevonásra kerülhet (pl. audit). Ide soroljuk azokat a jogi garanciákat (elsősorban a szerződésben foglalt, de lehet akár a törvény szerinti is), amelyek adott kérdésköröket egyértelműen rendeznek, beleértve az üzembiztonsági és adatbiztonsági kérdéseknél felmerült, ilyen módon megoldandó feladatokat is, vagy az adatközpontok fizikai védelmét. Ilyenek lehetnek:

- audit: internet-alapú szolgáltatásoknál ezt egy 3. cég bevonásával lehet végrehajtani, ha a szerződés egyáltalán lehetővé teszi, a készülékek esetében ez nem értelmezhető.
- hagyományos (fizikai) biztonság: hogyan gondoskodik a szolgáltató az adatközpontjai, vagy a felhasználó saját készülékei fizikai védelméről.
- adatok hosszú távú elérhetősége: internet-alapú szolgáltatásoknál értelmezhető, és azt tartalmazza, hogy hozzájuthatunk-e adatainkhoz akkor is, ha a szolgáltató csődbe megy, vagy felvásárolja egy másik cég.
- különféle logok és statisztikák tulajdonjoga: szintén az internet-alapú szolgáltatásoknál értelmezhető, alapvetően a felhasználási szerződés tartalmazhat kitételeket arról, hogy a szolgáltató mire használhatja az általa készített, ám érzékeny információkat is tartalmazó statisztikákat, logokat.
- szolgáltató általi szándékos adatlopás: kizárólag jogi úton kezelhető, de a használat megkezdése előtt gondolni kell erre is.
- alvállalkozók kérdése: az internet-alapú szolgáltatás üzemeltetője (pl. hardver eszközei karbantartásához), de a hordozható infokommunikációs eszköz gyártója (pl. szervizeléshez) alvállalkozókat is bevonhat a munkájába, akik adott esetben szintén

hozzáférhetnek a felhasználó adataihoz, ám rájuk a szolgáltató és a felhasználó között megkötött szerződések nem feltétlenül érvényesek.
– (nem biztonságos, vagy nem teljes) törlés: az internet-alapú szolgáltatások esetében ez jogi kérdés is, hiszen főként így szabályozható, a hordozható infokommunikációs eszközök esetében azonban teljesen a felhasználó hatás-, és felelősségi köre.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

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. 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, amelyhez a kellő alapot a lehetséges veszélyek áttekintése adhatja meg. Ez a cikksorozat második részének feladata.

Felhasznált irodalom

[1] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. Hadmérnök, VIII. Évfolyam 1. szám - 2013. március pp. 233 – 241 -ISSN 1788-1919

[2] https://www.facebook.com/orbanviktor (2014. 02. 22.)

[3] https://www.facebook.com/gyurcsanyf (2014. 02. 22.)

[4] https://twitter.com/FerencGyurcsany (2014. 02. 22.)

[5] IPadet kapnak a kormány tagjai (2011. 04. 27.) http://www.hir24.hu/belfold/2011/04/27/ipadet-kapnak-a-kormany-tagjai/?beuszo (2014. 02. 22.)

[6] iPadet kapnak a brit képviselők (2012. 03. 28.) http://beszeljukmac.com/index.php/weblog/comments/ipadet_kapnak_a_brit_kepviselok/ (2014. 02. 22.)

[7] Hackertámadás érte a Bank Austriát. Világgazdaság Online http://www.vg.hu/penzugy/hackertamadas-erte-a-bank-austriat-403251 (2014. 02. 17.)

[8] Netbankolás közben jött a hackertámadás. BAMA http://www.bama.hu/baranya/kek-hirek-bulvar/netbankolas-kozben-jott-a-hackertamadas-478955 (2014. 02. 17.)

[9] Adathalász e-mailekkel támadják az OTP Bank ügyfeleit http://hirek.prim.hu/cikk/102848/ (2014. 02. 17.)

[10] NSA Files: Decoded. The Guardian http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (2014. 02. 17.)

[11] Matt Chorley: iPads banned from Cabinet meetings over fears Chinese spies could use them as covert bugs to listen in on ministers. MailOnline http://www.dailymail.co.uk/news/article-2487026/iPads-banned-Cabinet-meetings-Chinese-spying-fears.html (2014. 02. 17.)

[12] Kovács Zoltán: Cloud Security in Terms of the Law Enforcement Agencies. Hadmérnök, VII. Évfolyam 1. szám - 2012. március pp. 144 – 156 -ISSN 1788-1919

[13] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Magyar Közlöny 47. szám 2013. március 21. pp. 6338 – 6342 http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (2014. 02. 17.)

[14] 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról. Magyar Közlöny 69. szám 2013. április 25. pp. 50241 – 50255 http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf (2014. 02. 17.)

[15] Kristóf Csaba: Kulcskérdés a BYOD összehangolása a biztonsággal http://bitport.hu/kulcskerdes-a-byod-oesszehangolasa-a-biztonsaggal (2014. 02. 17.)

[16] A Dell innovatív szoftverei a BYOD, a Big Data és az IT biztonság kérdéseire adnak választ http://www.dell.com/learn/hu/hu/hucorp1/press-releases/2013-12-12-dell-sajtokozlemeny-dell-world-dsg (2014. 02. 17.)

[17] Balogh B. Jenő: Világméretű probléma a BYOD biztonságának hiánya http://biztonsagpiac.hu/vilagmeretu-problema-a-byod-biztonsaganak-hianya (2014. 02. 17.)

[18] Balogh B. Jenő: Nagy biztonsági kockázat a BYOD http://biztonsagpiac.hu/nagy-biztonsagi-kockazat-a-byod (2014. 02. 17.)

[19] Department of Defense Instruction. (Subject: Technical Surveillance Countermeasures (TSCM) Program). Number 5240.05, February 22, 2006. http://www.dtic.mil/whs/directives/corres/pdf/524005p.pdf (2014. 02. 18.)

[20] Stephen Heskett: Technical Surveillance Countermeasures (TSCM) Frequently Asked Questions http://www.msainvestigations.com/tscm-faqs/bug-sweep/eavesdropping-Fequently-asked-questions/new-york/#subjectSpying (2014. 02. 18.)

[21] P. Mell, T. Grance : The NIST Definition of Cloud Computing Version 15, 10-7-09, National Institute of Standards and Technology, Information Technology Laboratory (http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf) (2011.10.21.)

[22] https://www.google.hu/ (2014. 02. 22.)

[23] https://www.dropbox.com/ (2014. 03. 14.)

[24] Craig Smith: How Many People Use 415 of the Top Social Media, Apps & Tools? (March 2014). http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/#.UyKrEvl5Ph5 (2014. 03. 14.)

[25] Top 15 Most Popular Social Networking Sites | March 2014 http://www.ebizmba.com/articles/social-networking-websites (2014. 03. 14.)

[26] Matt McGee: Google Is Most Visited Site Of 2013, Despite Big Drops In Desktop Traffic [Nielsen] http://marketingland.com/google-is-most-visited-site-of-2013-despite-big-drops-in-desktop-traffic-nielsen-68235 (2014. 03. 14.)

[27] Petrányi-Széll András: Közösségi élet a Facebookon túl http://psprovocative.com/kozossegi-elet-facebookon-tul/ (2014. 03. 14.)

[28] A Sony bemutatta legújabb tablet-notebook eszközeit http://androbit.net/news/3877/a_sony_bemutatta_legujabb_tablet_notebook_eszkozeit.html (2014. 02. 22.)

[29] http://www.apple.com/hu/ipad-air/specs/ (2014. 02. 22.)

[30] http://www.samsung.com/hu/consumer/mobile-phone/mobile-phones/galaxy-note/SM-N9005ZKEXEH-spec (2014. 02. 22.)

[31] http://www.asus.com/hu/Notebooks_Ultrabooks/TAICHI_31/#specifications (2014. 02. 22.)

[32] Galen Gruman: The real reason Obama can't swap his BlackBerry for an iPhone http://www.infoworld.com/d/mobile-technology/the-real-reason-obama-cant-swap-his-blackberry-iphone-232525 (2014. 02. 22.)

[33] Kovács Zoltán: Felhõ-alapú informatikai rendszerek, mint nemzetbiztonsági kihívás Hadtudomány, XXIII. Évfolyam 1-2. szám - 2013. március pp. 5 – 12 - ISSN 1215-4121

Ábrák jegyzéke