Szabó Tibor

Kormányzati informatikai hálózati infrastruktúrák védelmi rendszereinek új kihívásai a vezeték nélküli kommunikáció tükrében

A kormányzati informatikai hálózati infrastruktúrák tűzfalait, illetéktelen hálózati behatolást jelző rendszereit egyre magasabb biztonsági szintre hozzuk, továbbá korlátozzuk külső kapcsolati rendszerét egyetlen, megbízható internetszolgáltatóra annak érdekében, hogy az adatszivárgást megakadályozzuk. Ezen cél elérése érdekében viszont kevesebbet foglalkozunk egyrészt az egyre gyorsabban terjedő okostelefonok képességeinek és gyengeségeinek felismerésével, a hétköznapi használatukból adódó biztonsági rések keletkezésével, másrészt a „Snowden-ügy" kapcsán napvilágra került – esetlegesen működőképes – vezeték nélküli kommunikációt használó titkosszolgálati technikával.

Jelen cikk fel szeretné hívni a figyelmet néhány adatszivárgást elősegítő módszerre egy-egy példán keresztül, és rá szeretne mutatni (a téma összetettsége miatt a teljesség igénye nélkül), milyen egyéb technikai és szabályozási kérdésekkel kell foglalkozni az információk kiszivárgásának további minimalizálása érdekében.

Kulcsszavak: információbiztonság, vezeték nélküli kommunikáció, kormányzati vezeték nélküli, kommunikáció Snowden, okostelefon

Bevezetés

Az utóbbi években egyre több fórumon foglalkoznak a kormányzati informatikai hálózat biztonságával és a biztonsági szint növelésével. Mivel a kormány határozottsága és minőségjavítási igénye ezen a területen egyre növekszik, ezért érezhető változások következtek be.

Törekvések az információbiztonságért

Az információbiztonságot alapjaiban érintő, ezért talán a legfontosabb program az Interoperabilitási Átfogó Program. A program keretében először ki kellett dolgozni az E-közigazgatási Keretrendszert, mely az olyan fontos elveket rögzíti, mint az alkalmazásfüggő IT-biztonsági követelmények, szabványok vagy éppen az alkalmazásfejlesztési ke-

retrendszerek. Számos szabvány, ajánlás készült el az elmúlt években, ám ezek bevezetése és különösen felhasználása nem az elvárható mértékben történt meg. [1]

Annak ellenére, hogy az informatika évtizedek óta jelen van a kormányzati intézményekben, csak az elmúlt években – több évtizedes fejlődés után – sikerült eljutni arra a szintre, hogy ezeket a rendszereket a lehető legjobban összehangolják. Ez annak érdekében történt, hogy létrejöhessen a valódi szolgáltató állam, az állampolgárok és az üzleti élet szereplőinek lehető legjobb kiszolgálására.

A korábbi szigetszerű alkalmazásoktól való elszakadás sok jelentős lépésből állt. Ezek közül kiemelhető az Ügyfélkapu[1] létrehozása és a NISZ (Nemzeti Infokommunikációs Szolgáltató Zrt.) elindítása azon az úton, hogy stabilan biztosítsa, működtesse az államigazgatási szervek és országos hatáskörű intézmények egyes telephelyeinek összeköttetését, valamint internetes hozzáférését. [1]

Ennek a munkának az eredményeképpen egyre több közigazgatási intézmény csatlakozik ehhez a hálózathoz. Az egyes intézmények számítástechnikai szakemberei azon ténykednek, hogy vezetékes – és esetenként vezeték nélküli (bár ez egyre kevesebb) – belső hálózatukat (LAN) megóvják a súlyos károkat okozó adatszivárgástól és az internet felől érkező támadásoktól. Ennek érdekében a korszerű tűzfalas megoldásokon és proxiszervereken kívül a hálózati kapcsolókon és útválasztókon egyedi szabályrendszereket alkalmaznak. Ugyanekkor a NISZ rendszergazdái külön figyelmet fordítanak arra, hogy a kormányzati ügyfelek egyedi, védelmi megoldásai ne szenvedjenek csorbát az internet elérése során, továbbá a lokális hálózatok biztonsági hibái ne terjedjenek tovább a rendszeren belül – külön kezelve az intézmények hozzáféréseit.

A fentiekből levonható az a következtetés, hogy biztonság tekintetében a NISZ szakembergárdája csak a vezetékes összeköttetésekre és az azokon folyó adatkommunikációra van hatással. Az egyes intézmények helyi rendszereinek felépítése, topológiája és konfigurációja a látókörükön teljesen kívül esik.

Amennyiben feltételezzük, hogy az információbiztonságért felelős szakemberek kifogástalanul végezték munkájukat mind az államigazgatási szerveknél, mind a Nemzeti Infokommunikációs Szolgáltatónál, és ezáltal az internet felől majdhogynem „támadhatatlan" rendszert hoztak létre, emellett az adatszivárgást is tökéletesen megakadályozták az összekötetéseken keresztül, még akkor sem lehetünk biztosak abban, hogy az intézmény féltve őrzött dokumentumai nem kerülnek ki a falakon kívülre. Az iménti feltételezés még akkor is megállja helyét, amennyiben a munkatársak teljesen lojálisak munkáltatójukkal szemben, és megvan bennük minden jóindulat és együttműködési készség annak érdekében, hogy a minősített információk ne kerüljenek illetéktelenek kezébe.

A technika és technológia töretlen, nagyütemű fejlődése magával hozta az eszközök és eszközrendszerek fejlődését is. Az 1980-as évek végén, amikor a Budapest Műszaki

[1] Lehetővé tette, hogy az állampolgárok interneten keresztül intézzék hivatalos ügyeiket.

Egyetem Villamosmérnöki Karán létrehozták az informatikai tanszéket, egyértelművé vált, hogy speciális mérnököket kell képezni ennek a szakterületnek a művelésére. Ma már látjuk, hogy szinte csak a mérnökök vagy a hasonló gondolkodásúak képesek a technikai újdonságok teljes körű, gyors befogadására és alkalmazására. Az átlagemberek túlnyomó része a mobiltelefonok képességeinek csak a töredékét érti és használja, ezért egy állami alkalmazott olyan eszközt is használhat munkája során, aminek működését nem érti. A következőkben a vezeték nélküli kommunikáció néhány sajátosságának ismertetése után említünk egy-két példát annak illusztrálására, hogy milyen lehetőségek állnak rendelkezésre az információk intézményből való kijuttatására vezeték nélküli eszközök segítségével.

Vezeték nélküli kommunikáció

A kommunikációs rendszerek kulcsszerepet töltenek be a rendszerek elemei közötti összeköttetések megvalósításában, az együttműködés fenntartásában és az információk átadásában. a fizikai réteget tekintve – vagyis az átviteli közeg alapján – a kommunikációs rendszerek feloszthatók vezetékes és vezeték nélküli eszközökre. Ez utóbbi érdekes számunkra témánk szempontjából.

A vezeték nélküli kommunikációs berendezések besorolhatók frekvenciatartományuk szerint: [1]

- igen hosszú hullámú (néhány kHz, néhányszor tíz kHz frekvenciájú);
- hosszúhullámú (70 kHz – 500 kHz);
- középhullámú (500 kHz – 1500 kHz);
- rövidhullámú (1,5 MHz – 20, 30 MHz);
- ultrarövidhullámú (20, 30 MHz – 1 GHz)
- és mikrohullámú eszközök (1 GHz – 300 GHz).

Ahhoz, hogy általánosan használt eszközeinket el tudjuk helyezni ebben a listában, érdemes említeni közülük néhányat.

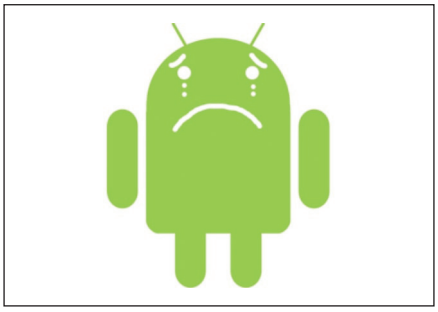
- A mobiltelefonok többsége hazánkban a 800/900/1800/2100 MHz-es frekvenciákat használja beszédre vagy adatátvitelre.
- A WiFi – vezeték nélküli mikrohullámú – adatátvitelre kifejlesztett kommunikáció a 2,4 GHz és 5 GHz közötti tartományokban működik, mely a hordozható telefonkészülékek túlnyomó többségében alapfunkcióként elérhető a felhasználók számára.
- A Bluetooth viszonylag kis hatótávolságú, adatcseréhez használt, vezeték nélküli szabvány a 2,4 GHz-es frekvenciatartományban, mellyel többnyire mobiltelefonok, hordozható számítógépek és egyéb készülékek (fejhallgatók, hangszórók stb.) között létesíthetünk rádiós kapcsolatot.

- Az NFC[2] 13,56 MHz-en működő, egészen kis (néhány centiméter) hatótávolságú kommunikációs szabvány a korszerű mobiltelefonok közötti – rádiós úton létrejövő – adatátvitelre vagy paramétercserére. Egymáshoz közel helyezve a készülékeket el lehet érni, hogy azok egyéb, kommunikációs kapcsolatok (WiFi, Bluetooth) létrehozásához szükséges beállítási adatokat cseréljenek. Az NFC-kapcsolódás passzív, energiatáplálást nem igénylő eszközzel (úgynevezett NFC-tag) is megvalósítható, például adatkiolvasás céljából.

Hogyan találhatjuk meg telefonunkat?

Fűződjön az első példánk egy olyan eszközhöz – a mobiltelefonhoz –, aminek használata egyre jobban terjed mindennapjainkban. Az okostelefonok eltűnése, lopása esetére, a keresés megkönnyítése érdekében leleményes fejlesztők készítettek egy olyan alkalmazást *Android Lost* néven, mely mindenki számára ingyenesen letölthető és telepíthető (értelemszerűen android operációs rendszerrel rendelkező) mobiltelefonokra. [2] A készülékhez – interneten keresztül vagy SMS segítségével – távoli elérést biztosító kis program (1. ábra) több mint harminc funkcióval rendelkezik, melyek közül kiemelnék néhányat:

- GPS-koordináta meghatározása,
- hívás átirányítása,
- SD-kártya[3] törlése,
- WiFi be-/kikapcsolása SMS segítségével,
- a program elrejtése a menüből,
- fotó készítése első/hátsó kamerával,
- adatkapcsolat be-/kikapcsolása SMS segítségével,
- hangfelvétel mikrofonnal.



1. ábra: Az *Android Lost* logója [2]

[2] Near Field Communication.
[3] Secure Digital – memóriakártya-típus hordozható készülékekbe.

A távoli elérés segítségével számos funkció támogatja az elveszett készülék megtalálását. SMS küldésével vagy az internetre csatlakozó számítógéppel számos információhoz hozzá lehet jutni arról a helyről, ahol telefonunk található, ezért több mint egymillió felhasználó már telepítette ezt a programot. A kiemelt funkciók alapján észrevehető, hogy másra is használható ez az alkalmazás, ami könnyen elkerüli az átlagemberek – köztük egyes állami alkalmazottak – figyelmét.

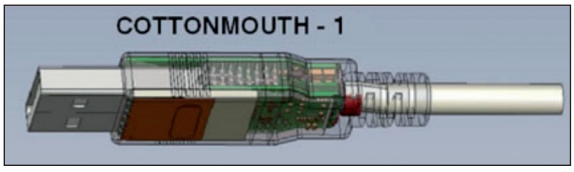
Amennyiben egy telefonra tulajdonosának tudta nélkül installálják az Android Lostot, akkor az továbbra is titokban maradhat, ha a menüből elrejtik a hozzá tartozó ikont. Távolról könnyen bekapcsolható a WiFi vagy az adatkapcsolat funkció, ami lehetőséget biztosít arra, hogy a telefon környezetében felvett hangokat és képeket továbbítani lehessen a fejlesztők által üzemeltetett szerverre. Szükséges hangsúlyozni, hogy ez a szerver külföldön van, tehát a keletkezett adatok először külföldre „vándorolnak", és csak utána kerülnek a titokban telepítő személy birtokába.

A látens, lassanként manifesztálódó belső aggodalom az alkalmazással szemben tovább fokozódik, amennyiben figyelembe vesszük az Android operációs rendszer alapú telefonoknak azt az alapvető tulajdonságát, hogy gmail-fiókkal regisztrált készülékre távolról rá lehet telepíteni ezt a programot, amennyiben ismerjük az e-mail-fiók azonosítóját és a hozzá tartozó jelszót. (A jelszó megszerzésének módja nem témája ennek az írásnak, mivel ezzel kapcsolatban számos cikk készült az elmúlt években.) A távoli telepítés néma lezajlása után a naplóállományban egy közönséges jegyzetszoftver ikonja jelenik meg, ami az avatatlan szemnek kevésbé feltűnő.

A „Snowden-féle" rádiós eszköz

A második példánkat a nagy sajtóbotrányt előidéző Snowden-ügyből vettük. Edward Snowden az amerikai Nemzetbiztonsági Ügynökség (NSA) és a Központi Hírszerző Ügynökség (CIA) volt számítógépes szakembere, aki azzal került reflektorfénybe, hogy nyilvánosságra hozott olyan szigorúan titkos dokumentumokat, melyek – többek között – rádiós kapcsolaton keresztül kommunikáló, adatszivárogtatást végző eszközöket tartalmaztak.

Az egyiket – mely COTTONMOUTH-I (CM-I) néven került nyilvánosságra – a számos rádiós eszköz közül azért érdemes kiemelni, mert leginkább ezen keresztül lehet bemutatni azt a technikai megoldást, amivel át lehet hidalni a vezetékes hálózaton gondosan kialakított védelmi rendszert (2. ábra).



2. ábra: COTTONMOUTH-I [3]

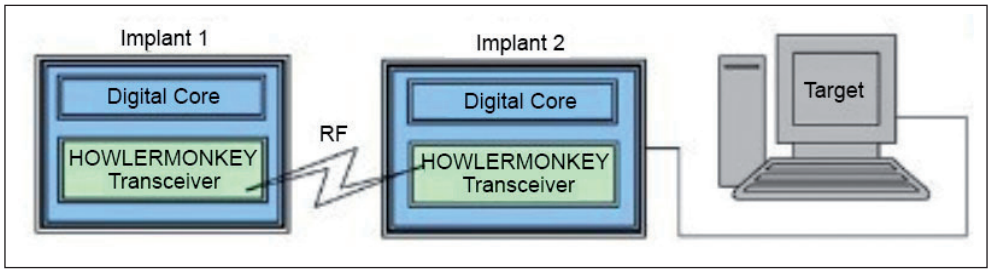
A CM-I képes hálózati szegmensek összekötésére a levegőben, szoftvermegtartó képességgel rendelkezik, újraprogramozható, képes rejtett kommunikációt folytatni a gazdagép beültetett szoftverével az USB-csatlakozón keresztül. A rádiós kapcsolat lehetőséget biztosít utasítások küldésére, adatok beszivárogtatására és kimenekítésére. A CM-I képes kommunikálni a Data Network Technologies speciális szoftverével az USB-csatlakozóban lévő, rejtett csatornát biztosító eszközön keresztül, melyen parancsokat és adatokat lehet továbbítani a hardver- és szoftverkomponenseknek.

A CM-I az alábbi digitális elemeket rejti magában:

- TRINITY mikroszámítógép, (mérete: kb. 10 mm x 21 mm),
- USB 1.1 hub[4] vagy switch,[5]
- HOWLERMONKEY (HM).

Ez utóbbi egy rádió adóvevő rövid- és középhullámú tartományban. [3] Az adási és vételi frekvencia pontos értéke nem ismert.

Az összes alkotóelem együttes mérete nem haladja meg egy normál USB-csatlakozó méretét. A tápellátás a számítógép USB-csatlakozójáról biztosítható. A HM öt különböző eszközben alkotóelem, melyek képesek egymással kommunikálni, ezáltal az egyik helyen keletkezett információk a rádiólánc segítségével eljuthatnak egy másik pontra is – figyelembe véve az adott eszköz hatósugarát (3. ábra).

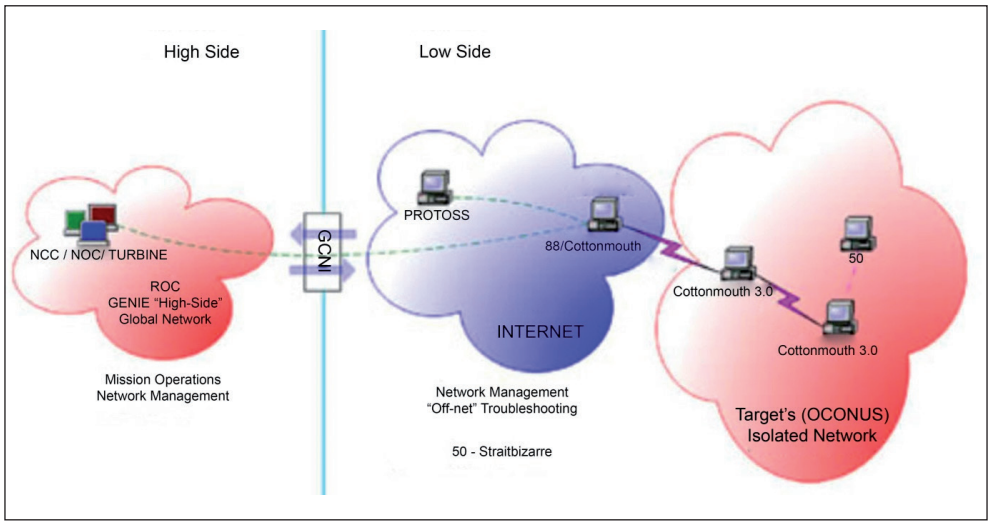


3. ábra: A HOWLERMONKEY együttműködése rádión keresztül [3]

A CM-I típushoz hasonló eszközökből létezik olyan, mely állandóan az USB-billentyűzetre csatlakozik. Egy másik változata olyan kialakítású, melynél az USB-kábel csak egyik vége van módosítva, míg a másik vége érintetlen. A HOWLERMONKEY adóvevőnek köszönhetően a CM-I rádiófrekvenciás összeköttetésen keresztül képes kommunikálni más CM-eszközökkel – egy speciális protokollt használva. [3] Ennek a képességnek a kihasználásával egy adott CM-pontot elérve ki lehet szivárogtatni az adatokat távolabbi – rádiós úton közvetlenül el nem érhető – számítógépekről is (4. ábra).

4 A hub egy olyan számítógépes hálózatban alkalmazott aktív eszköz, mely összekapcsolja a hálózati eszközöket. Amennyiben a hub egyik interfészén beérkezik egy keret, akkor az megjelenik minden más interfészén is.

5 Olyan számítógépes hálózatban alkalmazott aktív eszköz, mely összekapcsolja a hálózati eszközöket. A beérkező információ csak azon az interfészen jelenik meg, ahová az címezve volt.

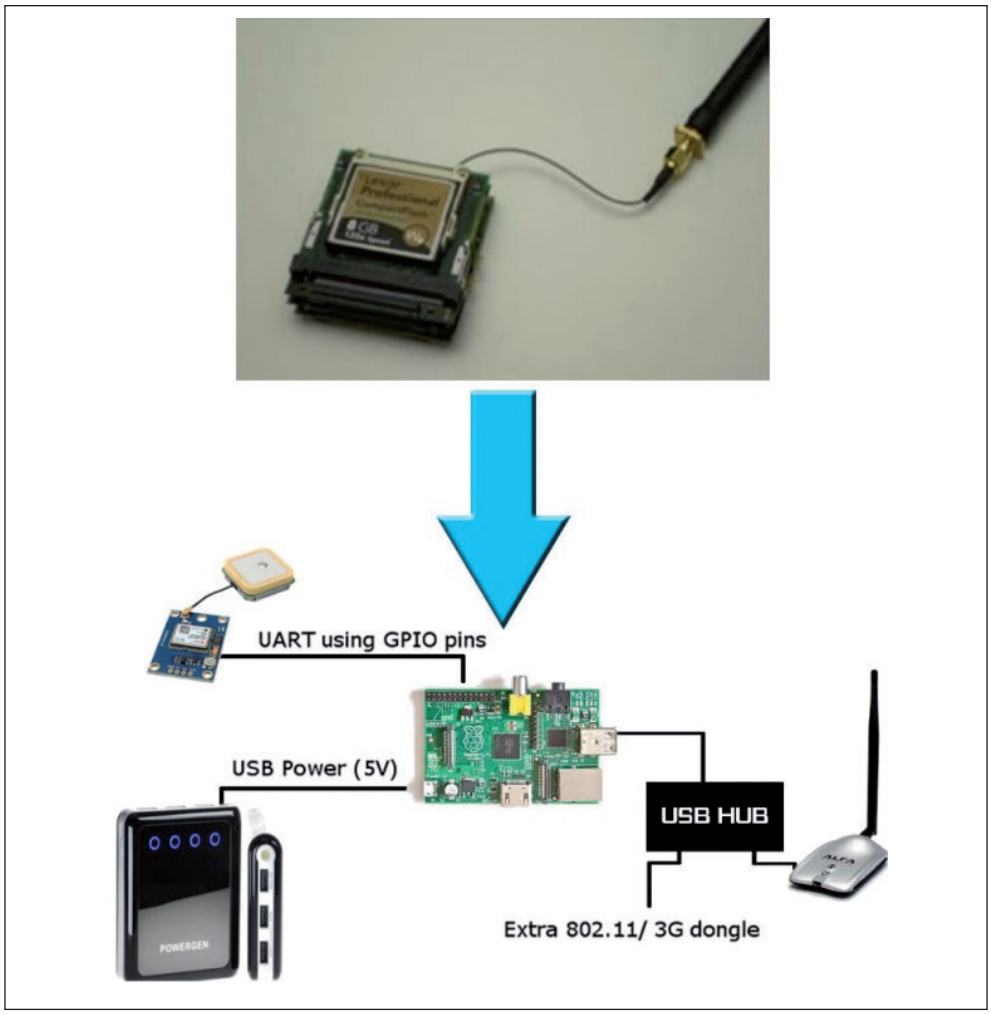


4. ábra: A CM-I rádiós kommunikációja [3]

Ebben a cikkben azt feltételezzük, hogy a részletezett eszköz létezik. Bár azoknak is igaza lehet, akik kételkednek abban, hogy a Snowden-ügy kapcsán sajtónyilvánosságra került dokumentumok valós és használható kellékeket tartalmaznak. Azonban ők sem hagyhatják figyelmen kívül, hogy a leírások egyeseket inspiráltak, és hasznosnak találva az ötletet – függetlenül attól, hogy működőképesek voltak-e a berendezések – megépítették őket az átlagemberek számára is hozzáférhető eszközökből, néhány hónap alatt. Példának okáért vegyük a Snowden-féle SPARROW II WLAN adatgyűjtő eszközrendszert, mely méreteiben és energia-felhasználásában ugyan eltér a házilag készített típustól (az előállítás költsége csak a negyvenede az eredetinek), de működése azonos (5. ábra). Amennyiben néhány berendezés leírása az amatőröknek felkeltette az érdeklődését, akkor feltételezhető, hogy fejlett technikai színvonalon lévő cégeknek és kormányoknak is.

A Snowden-ügy kapcsán az online sajtóban megjelent eszközleírások között több olyan, a rádiófrekvenciás tartományban üzemelő is található, amit most nem részletezünk. Mindez felhívja a figyelmet arra, hogy az ismert eszközök frekvenciáin kívül máshol is számítani kell aktivitásra a spektrumban. Ki kell emelni, hogy olyan eszközök is léteznek, melyek kisugárzása csak bizonyos külső jel hatására aktivizálódik, azaz távolról kapcsolható be. Csak úgy lehet meggyőződni arról, hogy van-e rejtett adó a környezettben, ha folyamatos és teljes spektrumú figyelést alkalmazunk az adott intézmény minden pontjára kiterjedően.

Felvetődhet a kérdés, hogyha létezik USB-kábelbe épített implantátum, akkor miért ne létezhetne monitorkábelbe, egérbe, billentyűzetbe vagy éppen monitorba rejtett eszköz is…



5. ábra: SPARROW II (fent) és házi verziója (lent) [3], [4]

Javasolt védelmi megoldások

A fentiek alapján látható, hogy az adatszivárgás kiküszöbölésére vagy minimalizálására intézkedéseket kell bevezetni. A védelmi megoldásokat az alábbi csoportokba oszthatjuk, melyekkel magas szintre lehet emelni az információbiztonság szintjét, kivédhető vagy nagymértékben csökkenthető az adatszivárgás valószínűsége:

- aktív,
- passzív,
- adminisztratív.

Aktív megoldás a teljes frekvenciaspektrumot lefedő zavarás. *Passzív* megoldás az árnyékolás, valamint a folyamatos monitorozás. Tehát az adatgyűjtést, a folyamatos ellenőrzést és elemzést ki kell terjeszteni az egész frekvenciaspektrumra az intézmény minden pontján. *Adminisztratív* megoldás:

- Eszköz vásárlása esetén: összehasonlító mérést (röntgenkép, fogyasztás stb.) kell végezni egy elemzett mintaeszközzel, majd a selejtezés után feltétel nélkül minden eszközt meg kell semmisíteni.
- Hordozható eszközök esetén: az eszközök leadása a portán, és olyan egységes – belső hálózattól független – rendszer használatának bevezetése egy adott intézménynél, mely elérhetővé teszi az alkalmazottak számára a leadott hordozható eszköz bizonyos szolgáltatásainak elérését. Ilyen szolgáltatások a hívás, SMS/MMS fogadása/indítása és híváslista elérése/módosítása.

A javasolt megoldások egyenkénti vagy kombinált alkalmazása eredményes lehet az információbiztonság megfelelő szintre hozásához azokban az intézményekben, ahol az adatszivárgás kockázati tényezője ezt indokolja. Egyértelmű, hogy a végcél – az adatszivárgás-mentesség – elérése több problémába is ütközik, mivel figyelembe kell venni az emberi tényezőt és azt, hogy a hardver- vagy szoftvergyártás egy része külföldi tulajdonú cégeknél zajlik.

Összegzés

Rávilágítottam, hogy hordozható eszközök esetén az alkalmazottak lojalitása és legjobb szándéka ellenére is előfordulhat, hogy olyan eszközt használnak a munkahelyükön, mely csak részben van az irányításuk alatt, tehát adatszivárgást lehet vele végrehajtani. Ez megtörténhet hangrögzítéssel, fénykép készítésével vagy GPS-koordináták rögzítésével is – a lehetséges adatlopási módok száma nagyon nagy. Az adattovábbítás történhet az illetéktelenek felé GSM- és WiFi-hálózaton, továbbá Bluetooth segítségével is. Fontos rámutatni, hogy az adatok rögzítése és továbbítása időben elkülönülhet. Tehát az adatok küldése akkor is bekövetkezhet, amikor a hordozható eszköz tulajdonosa már jó vételi viszonyok között van – hiába volt a munka körletében teljes rádiós zavarás, amikor az adatok rögzültek. Az adatok továbbításához egyre kevesebb időre van szükség, mivel a WiFi adatátviteli sebessége folyamatosan emelkedik. A napokban mutatta be a Huawei (egy távol-keleti elektronikai cég) a 10 Gbps-os WiFi-kapcsolatot. [5]

Magabiztosan állíthatjuk, hogy elégtelen csak a vezetékes hálózatra koncentrálnunk, amennyiben az információbiztonság teljes körű megvalósítása a cél. Az egyenszilárdságú védelem elérése érdekében a vezeték nélküli kommunikációs eszközök esetén jóval több intézkedést kell meghozni. Az ismert eszközök frekvenciáinak monitorozása csak részmegoldás, mivel az adatszivárgást előidéző eszközrendszerek – implantátum formájában – nagy valószínűséggel nemcsak itt üzemelnek.

Kevés intézmény vizsgálja át tüzetesen a beszerzett eszközöket, pedig azokon a területeken, ahol az adatszivárgás kockázati tényezője magas, ez létfontosságú lenne. Ismertettem, hogy technikailag milyen egyszerű eszközökbe vagy kábelek csatlakozóiba építeni különféle rejtett implantátumokat, amelyek könnyen bekerülhetnek a magánéleti és munkahelyi környezetünkbe.

Ismertettem néhány alapvető – a cikkben olvasható eszközökkel szemben alkalmazható – védelmi megoldást, mely jelentősen minimalizálhatja a vezeték nélküli kommunikációs rendszerek esetén az adatszivárogtatást.

Irodalomjegyzék

[1] Dr. Kovács László – Gyányi Sándor – Dr. Haig Zsolt – Illési Zsolt – Krasznay Csaba – Dr. Muha Lajos – Szabó András Miklós – Dr. Ványa László: *Számítógép-hálózati hadviselés: veszélyek és a védelem lehetséges megoldásai Magyarországon.* Tanulmány. Budapest, ZMNE, 2010.

[2] https://play.google.com/store/apps/details?id=com.androidlost&hl=hu (a letöltés ideje: 2014. 05. 25.)

[3] NSA's ANT Division Catalog of Exploits for Nearly Every Major Software/Hardware/Firmware, http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/ (a letöltés ideje: 2014. 05. 25.)

[4] Hardware – Open-Source NSA Technology (Airborne Wifi), http://hyperionbristol.co.uk/hardware-open-source-nsa-technology-airborne-wifi/ (a letöltés ideje: 2014. 05. 26.)

[5] Huawei demoing the new 10Gbps WiFi technology, www.gizmochina.com/2014/05/30/huawei-demoing-the-new-10gbps-wifi-technology// (a letöltés ideje: 2014. 06. 02.)

New challenges of governmental wireless information infrastructure protection systems

Szabó Tibor

Firewalls and unauthorized network intrusion detection systems of the government IT network infrastructure are brought to an even higher safety level also limiting any external link connections to reliable Internet service providers so as to prevent data leakage. In order to achieve this goal we are focusing less on detecting the rapidly growing smartphone capabilities and weaknesses and security holes due to everyday use. Moreover, we are paying less attention to wireless intelligence techniques that became published as a consequence of the "Snowden case".

This article – with the help of an example – would like to draw attention to some methods enabling data leakage, and would like to highlight some of the technical and regulatory issues (without being comprehensive) that need to be addressed in order to further minimize information leakage.

Keywords: information security, wireless communications, Snowden, smartphone, governmental wireless communication