HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Kovács Zoltán
zkovacs@nbsz.gov.hu

HORDOZHATÓ INFOKOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATÁHOZ KAPCSOLÓDÓ BIZTONSÁGTUDATOSSÁGI KÉPZÉSI TEMATIKA VÉDETT VEZETŐK SZÁMÁRA

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 "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" című cikksorozat áttekintette a védett vezetők információbiztonsági védelmének főbb kérdéseit, és összefoglalta az említett eszközök és szolgáltatások használata során jelentkező veszélyeket. Jelen cikk pontosítja a személyre szabott oktatás keretrendszerét, majd felállítja egy lehetséges, az említett eszközök és szolgáltatások használatára vonatkozó biztonságtudatossági alapképzés tematikáját.

The communication and the use of portable infocommunication devices (e.g. smartphone) 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 article series titled "The Risks of Using Portable Infocommunication Devices in Terms of Security Awareness Training for Protected Leaders" reviews the main issues of data security of protected leaders and summarizes the threats appearing while using the above mentioned devices and services. This article assigns the framework of the personalized training and establishes a possible theme of a basic security awareness training concerning the use of the devices and services mentioned above.

Kulcsszavak: *védett vezető, hordozható infokommunikációs eszközök, internet-technológián alapuló szolgáltatások, biztonságtudatossági képzés ~ protected leader, portable infocommunication device, Internet Based Services, security awareness training*

BEVEZETÉS

A védett vezetők mindennapi tevékenységéhez szorosan hozzátartozik a kommunikáció, és az ezekhez szükséges hordozható infokommunikációs eszközök (pl. okostelefon, táblagép, hordozható számítógép) használata. Gyorsan, egyszerűen, és nem utolsó sorban olcsón akarnak beszélni másokkal, adatokat, információkat elérni, cserélni, továbbítani. Sokszor mindezt úgy, hogy az érzékeny információkat csak az a néhány ember ismerhesse meg, akinek feltétlenül szükséges, az általuk közétenni kívánt információkhoz viszont az emberek széles köre is gyorsan, egyszerűen hozzáférhessen. Ez utóbbihoz sok esetben mindenki által elérhető, sokszor ingyenes internet-technológiára épülő szolgáltatásokat használnak fel, vagy kívánnak felhasználni. Ráadásul a hivatali-, és magánjellegű kommunikációt, az érzékeny és a széles körnek szánt információk továbbítását lehetőleg egyazon eszköz segítségével kívánják lebonyolítani. Ez azonban jelentős veszélyeket rejt magában.

Az elektronikus úton folytatott kommunikációs és adattovábbítási lehetőségek, az internet-technológiára épülő, ezen belül is a felhő alapú szolgáltatások rohamos fejlődése új, korábban nem ismert kihívások elé állította/állítja az illetékeseket, döntéshozókat és a szakembereket egyaránt. A kibertérben ma minden felhasználót veszélyek egész sora fenyegeti, a kiberbűnözéstől az idegen titkosszolgálatok adatszerző tevékenységéig. Fokozottan igaz ez a védett vezetőkre, akik mindig is kiemelt célpontjai voltak az információszerző támadásoknak. Ráadásul külön problémakánt jelentkezik, hogy a védett személyek által használt eszközök – hordozhatóságuk és személyhez rendeltségük okán – általában vegyes felhasználásúak, azaz hivatali és magán célokat egyaránt szolgálnak.

Éppen ezért fontos megvizsgálni, hogy mit is tehetünk a védett vezetők információinak – azon belül is legfőképpen elektronikus információinak – megvédése, biztonságának garantálása érdekében. Az internet-technológiára épülő szolgáltatások, és a személyi használatú hordozható infokommunikációs eszközök esetében a védekezés egyik leghatékonyabb módszere biztonságtudatos használata. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne a megfelelő szinten kialakítható.

A biztonságtudatos használatra fel lehet készíteni a védett vezetőket. Ehhez érdemes egy személyükre szabott, általános jellemzőiket figyelembe vevő oktatási tematikát kidolgozni. A "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" című cikksorozat első része áttekintette a védett vezetők információbiztonsági védelmének főbb kérdéseit, körülhatárolta a veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat, majd számba vette az elemezendő biztonsági kategóriákat. A második rész az elsőben megadott kritériumok alapján összefoglalta az említett eszközök és szolgáltatások használata során jelentkező veszélyeket. Ez pedig már megfelelő alapot teremt az oktatási tematika kidolgozásához.

Jelen cikkben a "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" című cikksorozatban leírtak, valamint saját tapasztalataim alapján fogalmazom meg gondolataimat a témáról.

A SZEMÉLYRE SZABÁS KERETRENDSZERE

A védett vezetők személyre szabott oktatási tematikája kidolgozásának egyik alapfeltétele tehát a lehetséges veszélyek felmérése. Ez a "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" [1] [2] című cikksorozatban megtalálható. A másik alapfeltétel a személyre szabáshoz a védett vezetők speciális helyzetének felmérése. Figyelembe kell venni ugyanis az élethelyzetükből,

munkájukból, elfoglaltságukból adódó feltételeket, amelyek egyfajta keretrendszert, feltételrendszert képzenek az oktatási tematikához.

Bár kifejezetten a védett vezetők felhasználói szokásairól nem készült felmérés a személyi használatú hordozható infokommunikációs eszközök, valamint az internet-technológiára épülő szolgáltatások használata kapcsán, ám a normál felhasználói szokásokból lehet általánosítani és ide vonatkozó következtetéseket levonni.

A figyelembe veendő feltevések, megállapítások a következőek:

- Használnak személyi infokommunikációs eszközöket.
- Az első egy értelemszerű, de fontos megállapítás.
- Hordozzák ezeket az eszközöket.

Szintén értelemszerű megállapítás, ám fontos tényező a kialakítandó biztonság szempontjából. Az eszközök hordozása ugyanis olyan plusz kockázatokat rejt, amelyeket már érdemes, vagy inkább be kell építeni a biztonságtudatos képzésbe. Ilyenek lehetnek a "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" [1] című cikksorozatban megtalálható veszélyek, mint például az eszközök felügyelete, mások általi hozzáférése, kapcsolódás más hálózatokhoz, stb.

Az eszközök jórészt normál kereskedelmi forgalomból származó, kommersz eszközök. Ez azt jelenti, hogy ezek jellemzően nem rendelkezik egyéni biztonsági funkcióval, ha igen azok is más országok által gyártottak. Ugyanakkor a világméretű elterjedtség, ismertség okán számos ismert sebezhetőséget, valamint akár a gyártó által beépített, esetleg ki is használt, információszivárgást okozó „funkciót" is tartalmaznak.

Vegyes (részben magán, részben hivatali) jellegű használat a jellemző. A személyi használatú, hordozható infokommunikációs eszközöket a védett vezetők általában hivatalból kapják, de – teljesen szabályos módon – magáncélra is használják, használhatják. Ez nem azonban nem csak a kommunikáció tartalma miatt, hanem a felhasznált internet-technológiára épülő szolgáltatások, ezáltal a készülékek ellenőrzése és a biztonságtudatossági képzés tartalma okán is figyelembe veendő tény. De éppen ezért az ellenőrzéshez és a biztonságtudatossági képzéshez is egészen más lehet a védett vezetők hozzáállása, mint egy tisztán hivatali célra igénybevett eszköz esetén.

Mások (pl. családtagok) is hozzáférhetnek az eszközökhöz, sőt használhatják is azokat. A magánjellegű használatból eredő kockázatot fokozza ez a kitétel, hiszen az eszközök egy részénél nehezen, vagy egyáltalán nem megvalósítható a jogosultságkezelés, a családtagok letölthetnek, telepíthetnek alkalmazásokat, esetleg véletlenül is feltölthetnek fájlokat. Ez pedig olyan, amelynek kockázatait, és azok csökkentésének lehetőségeit szintén ismertetni kell a képzés során.

Iskolai végzettségük (diplomáik szakterületei) óriási szórást mutat (pl. közgazdász, jogász, agrármérnök, stb.) A képzés kialakítása szempontjából ez egy meghatározó tényező, hiszen mindenki számára érthetően, sőt a későbbiekben alkalmazható módon kell az oktatást kialakítani.

Jellemzően nem mély számítástechnikai, informatikai, kommunikációs és információbiztonsági ismeretekkel rendelkeznek, sőt ez a tudás csekélynek tekinthető. Az előző ponthoz szorosan kapcsolódó, de az oktatás kialakítására nézve önállóan is fontos megállapítás.

Jellemzően az érdeklődés a normál használat iránt is vegyes. A védett vezetők egy része szereti „nyomkodni a telefonját, táblagépét", más részük normál felhasználónak tekinthető, míg vannak köztük olyanok is, akik csak akkor használják, amikor feltétlenül szükséges. Ez hatással van a felhasználói ismeretekre, de a védendő információk mennyiségére is.

A "megszokott" felhasználási módokat keresik, a biztonságosabb használat miatti korlátozásokat, nehezen fogadják el. Minden olyan elem, amely a biztonságot emeli, várhatóan

korlátozza a felhasználót és/vagy nehezíti a használatot. Ezt pedig akárcsak az „átlagfelhasználók" általában, a védett vezetők is nehezen fogadják, viselik el.

Bonyolult azonosítási, felhasználási eljárások a védett vezetőket elriasztják a használattól, vagy keresik az elkerülő lehetőségeket. Adott esetben a magasabb biztonsággal járó, bonyolultabb azonosítási eljárások okozta kényelmetlenségek ilyen reakciókat is kiválthatnak a védett vezetőkből. Ennek megelőzésében nem csupán az eljárások gondos megválogatása, hanem a biztonságtudatos képzés is sokat segíthet.

Egy részük szereti, sőt akár presztízskérdésnek fogja fel az új mobil infokommunikációs eszközök birtoklását. Az új eszközök új technikai lehetőségeket, ezáltal új biztonsági előnyöket és kockázatokat egyaránt jelentenek. Az oktatásnak figyelembe kell vennie, és a lehetőségekhez mérten fel kell készítenie a védett vezetőt egy új készülék használatából adódó biztonsági kockázatokra és lehetőségekre.

Számolni kell a személyes infokommunikációs eszközök elvesztésével, ellopásával. Az oktatás során ki kell térni az ebből adódó kockázatokra, valamint azok csökkentésére vonatkozó lehetséges ellenlépésekre is. Tudatosítani kell, hogy mi a felhasználó feladata és felelőssége, és mi az rendszergazdáké.

Jellemzően rendelkeznek közösségi oldalon, oldalakon profillal, és azt, azokat aktívan használják is. A közösségi oldalakkal kapcsolatos veszélyek részint tartalmazzák az egyéb internet-technológiára épülő szolgáltatásokkal kapcsolatos kockázatokat, ugyanakkor máshol nem, vagy legalábbis nem ilyen formában jelentkező veszélyeket is. Az oktatás során ezekre is fel kell hívni a figyelmet.

Jellemzően használnak egyéb felhő alapú szolgáltatásokat levelezésre, adattárolásra stb. (pl. gmail, dropbox). A közösségi oldalak mellett a felhő alapú rendszerek használata is rejt speciális, csak ezekre jellemző veszélyeket. Ezekre a jellegzetes problémákkal, kockázatokkal ugyanúgy foglalkozni kell az oktatás során, mint a közösségi oldalak esetében.

Jellemzően töltenek le és telepítenek újabb alkalmazásokat eszközeikre. Ma már a legegyszerűbb alkalmazások is szinte minden esetben teljes hozzáférést kének adatainkhoz, telefonkönyvünkhöz, pozíciónkhoz stb. A szerződés elfogadásával pedig a felhasználó saját maga járul hozzá ezek átadásához. Ráadásul, mint minden szoftver, ezek is tartalmaznak, tartalmazhatnak olyan sérülékenységeket, netán tudatosan beépített hátsó kapukat, amelyet kihasználva a támadók szintén hozzáférhetnek a felhasználó minden adatához. A biztonságtudatos használat egyik alappillére, hogy a védett vezető ezekkel a kockázatokkal is tisztában legyen.

Jellemzően a letöltött és telepített alkalmazások egy része, vagy akár egésze ingyenes. A fentiek kiemelten igazak abban az esetben, ha a kiválasztott alkalmazás ingyenes. Ekkor ugyanis jóval több hozzáférést kell engedélyezni a szerződés elfogadásakor, mint fizetős társaiknál. Különösen jól megfigyelhető ez azoknál a szoftvereknél, ahol fizetős és ingyenes verzió is létezik ugyanabból a verzióból.

Jellemzően kevés idővel rendelkeznek, amelyet oktatásra, biztonságtudatosság növelésére lehet fordítani. Lényeges szempont a tematika összeállításánál egy időkorlát meghatározása. Ez természetesen nemcsak azt is jelenti, hogy nem csak a képzés anyagát kell nagyon gondosan megválogatni és tömören, de érthetően előadni, hanem azt is, hogy az összeállított tematika egyfajta alapképzés lehet, amelyet a későbbiekben lehetőség és igény szerint további, akár hosszabb oktatásokkal kell kiegészíteni.

Az információbiztonság fontos számukra. Szintén egyértelmű tény, hogy a védett vezetők tisztában vannak azzal, hogy sokszor kezelnek érzékeny információkat, amelyek megvédése fontos számukra. Ezáltal fogékonyabbnak tekinthetők az információbiztonság területén jelentkező problémák megértésére, mint az „átlagfelhasználó". Ennek elősegítésére érdemes olyan példákat hozni az oktatásban, amely ismert, éppen ezért az információszerzés miatt kiemelt személyekkel kapcsolatosan mutat rá a lehetséges veszélyekre.

A védett vezetőknél technikai elhárítás is segíti az információbiztonságot. A védett vezetőknél az információbiztonság teljes körű garantálásának érdekében rendszeresen tartanak technikai elhárítást is. A "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" [1] című cikksorozatban megtalálható a technikai elhárítás kiterjesztett értelmezése. Az ebben megfogalmazottak szerint ennek ki kell terjednie a védett vezetők hordozható infokommunikációs eszközeire is. Ez pedig nagyobb fokú biztonságot garantál, amelyet meg kell ismertetni a védett vezetőkkel is.

OKTATÁSI TEMATIKA

Az említett cikksorozatban feltárt veszélyeket, valamint a fenti feltételeket és feltevéseket figyelembe véve már kidolgozható az védett vezetők számára a személyükre szabott oktatási tematika.

A fent leírtak alapján a védett vezetőknek szóló, a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások igénybevétele kapcsán jelentkező biztonságtudatos használatának alapképzési tematikájánál a következőkből célszerű kiindulni:

- A képzést célszerű a – kiterjesztett értelemben vett és végrehajtott – technikai elhárítással összekötni, azzal párhuzamosan végrehajtani. Ekkor ugyanis átvizsgálásra kerülnek a védett vezető eszközei, és feltérképezésre kerülnek az esetleges információszivárgási csatornák, lehetséges információbiztonsági veszélyek.
- Az oktatás megtartását célszerű a technikai elhárítást végző szervre bízni. Itt ugyanis a megfelelő időben rendelkezésre állnak a megfelelő ismerettel rendelkező szakemberek.
- Az alapképzés időtartamát célszerű körülbelül 60 percben meghatározni. Ennél több, egyedi oktatásban az alapképzésre fordítható ideje a védett vezetőknek várhatóan nem lesz több, ennyi viszont feltétlenül szükséges a megfelelő információ átadásához.

Mindent egybevetve a következő tematika alapján célszerű elvégezni az oktatást:

Oktatási cél: Az oktatás keretében a védett vezető ismerje meg a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások igénybevétele kapcsán jelentkező veszélyeket, azok elhárítása, vagy legalábbis csökkentése érdekében általa elvégzendő teendőket, a biztonságtudatos használatot.

Elvárt eredmények:

A védett vezető:

- megértse a veszélyeket és elfogadja a biztonság fontosságát,
- megértse és elfogadja a technikai elhárítás keretein belül a személyi használatú hordozható infokommunikációs eszközeinek vizsgálatát,
- megértse egy hosszabb idejű képzés fontosságát, a részvételhez érdeklődéssel és készségesen álljon hozzá,
- támogassa az oktatás és a vizsgálat kiterjesztését közvetlen munkatársaira és családtagjaira,
- az általa használt személyi használatú hordozható infokommunikációs eszközeit, valamint internet-technológiára épülő szolgáltatások a képzést követően a korábbiaknál sokkal nagyobb biztonságtudatossággal legyen képes használni.

Tematika:

1.	Veszélyek bemutatása példákkal
	a. Illetéktelen hozzáférés, lehallgatás
	i. Snowden ügy tanulságai,
	ii. Egy pénzlopás ügy rövid bemutatása,
	iii. Egy híres ember adatait illetéktelenül megszerzésének és felhasználásának esete rövid bemutatása
	b. Másodlagos adatok fontossága
	i. OSINT bemutatása, példával,
	ii. Helymeghatározás bemutatása, példával
	c. Adatvesztés bemutatása - Cryptolocker példa
	d. Nem valós adatfeltöltés, lejáratás bemutatása, példával
2.	Biztonság megteremtésének módjai, beállítások, biztonságtudatos használat
	a. Üzembiztonsághoz kapcsolódó lehetőségek
	i. Felhő alapú rendszerek – szerződés elfogadás/elutasítás
	ii. Eszköz - biztonsági mentés
	b. Egyéb biztonsághoz kapcsolódó lehetőségek
	i. Jogi lehetőségek - korlátozott lehetőségek bemutatása
	ii. Fizikai védelem - tudatos viselkedés bemutatása, példákkal
	c. Adatbiztonsághoz kapcsolódó lehetőségek
	i. Adatkészítés - biztonságos környezet kérdésköre
	1. Frissítések fontosságának bemutatása
	2. Minimalizált szoftverkörnyezet fontosságának bemutatása
	3. Új szoftvertelepítések elkerülésének fontossága
	4. Biztonsági szoftverek naprakészen tartásának fontossága
	5. Felhasználók kezelése, jogosultságok fontossága
	ii. Adattovábbítás kérdésköre
	1. Kapcsolódó(tt) hálózatok veszélyei, beleértve a hardveres eszközöket pl. BT billentyűzet is
	2. Távoli, passzív lehallgatás veszélyei
	3. Titkosítás fontosságai, korlátai
	iii. Bejelentkezés, adatmegadás, jelszó kérdésköre
	iv. Törlés, megsemmisítés, fióktörlés kérdésköre
	v. Social engineering veszélyei
3.	Ellenőrzés lehetőségei, fontossága
4.	Összefoglalás, kérdések

Ütemezés:

A technikai elhárítás alkalmával, kb. 60 perc időtartamban.

Irodalom és további információk:

- Az oktatók által elkészített 2-3 oldalas anyag, a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások biztonságtudatos használatához szükséges legfontosabb információkkal.
- Az oktatók által elkészített 2-3 oldalas anyag, a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használatához szükséges legfontosabb beállításokkal kapcsolatos információkkal.
- Az oktatók által elkészített rövid, 10-15 perces flash animáció, a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használatához szükséges legfontosabb beállításokkal kapcsolatos információkkal.
- Egy kontaktszemély adatainak átadása, akit a későbbiekben felmerülő kérdésekkel akár telefonon, akár e-mailben megkereshet.

A tematika alapján a tényleges, teljes ismeretanyag kidolgozása, annak napra készen tartása már a képzést tartó szervezet szakembereinek, vezetőinek a feladata.

A TOVÁBBLÉPÉS LEHETŐSÉGEI

Az oktatási tematika természetesen csak az első lépés a védett vezetők információbiztonságának minél magasabb szintű megteremtéséhez a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások használata során. Bár nyilvánvalóan 100 %-os védelmet nem lehet kialakítani, de mindenképpen törekedni kell rá. A jelen, valamint a korábban már hivatkozott „Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I.-II." című cikkből kiolvasható, hogy a felvázolt oktatási tematika tartalommal való megtöltése, és az oktatás végrehajtása mellett is vannak további feladatok, amelyek végrehajtásával a biztonsági szint tovább emelhető.

Ezek közül az első csoportba azok a feladatok tartoznak, amelyek minden, a cikkekben említett szereplőkön (védett vezető, technikai elhárítók, helyi biztonsági vezető, rendszergazdák) túlmutató, magasabb szintű megközelítést igényelnek. Ilyen például a megfelelő jogszabályi háttér kialakítása, átalakítása, ezen belül pedig bizonyos biztonsági elemek kötelezővé tétele. Ilyen kötelező elem lehet(ne) a kiterjesztett értelemben vett technikai elhárítás előírása bizonyos vezetői szintig, meghatározott biztonságtudatossági oktatáson való kötelező részvétel, vagy a hordozható infokommunikációs eszközök esetében, azok teljes életciklusára (fejlesztés, beszerzés, rendszerbe állítás, használat, kivonás stb.) vonatkoztatva kötelező biztonsági előírások kialakítása, betartatása, és hatósági ellenőrzése. Szintén a jogszabályi háttér kialakításakor kell gondolni a védett vezetők környezetben lévő személyekre, a technikai elhárítás rájuk történő kiterjesztésére is (pl. családtagok, közvetlen munkatársak, titkárság stb.). Ez azért is fontos, mert sokszor ők is kezelik a védett vezetőhöz kapcsolódó információkat, így az érzékeny adatok szivárgását náluk is meg kell előzni, akadályozni.

De ugyan ebbe a csoportba tartozik a védett vezetők felhasználási szokásainak felmérése is. Ilyen célzott felmérés ugyanis még nem készült, márpedig ez segítheti a specifikus kockázatelemzést. Bár jelen cikkben említett alap biztonságtudatossági képzéshez ez nem elengedhetetlenül szükséges, a hosszabb, például 1 napos képzések tematikájának kialakításában, valamint a szükséges biztonsági szintek meghatározásában nagy segítséget nyújthat. A felmérés során választ kell kapni azokra a kérdésekre, hogy ki, milyen személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat használ, és azokat mikor, hol, hogyan és mire. A felmérés természetesen – a lehetőségekhez mérten – lehet anonim, a „ki" kérdésnél sokkal érdekesebb a vezetési szint. Elsősorban azért, hogy meg lehessen állapítani, van-e statisztikailag is kimutatható markáns különbség az egyes vezetési szinteken lévő vezetők felhasználói szokásaiban.

A második csoportba a védett vezető által megtehető további feladatok tartoznak. Ilyen lehet a korábban említett, további hosszabb biztonságtudatossági képzésen való önkéntes részvétel, az önképzés, az egyéb lehetőségek, például konzultációs lehetőségek kiaknázása a biztonsági szakemberekkel, vagy a kiterjesztett értelemben vett technikai elhárítás aktív, segítő támogatása.

A harmadik csoportba sorolhatóak az eszközök üzemeltetéséért, biztonságáért permanensen felelős helyi biztonsági vezető, a rendszergazda és munkatársaik feladatai. Ide tartoznak a felhasználási előírások megalkotása, betartatása, a meghajtó programok és a feltelepített alkalmazások naprakészen tartása, az eszközök biztonságos működéséhez szükséges beállítások megtétele, ismert, de javítatlan biztonsági rések esetén az adott szoftver esetleges cseréje hasonló tudásúra, a felesleges, ezáltal biztonsági kockázatot jelentő szoftverek

eltávolítása, az incidensek kivizsgálását elősegítő alkalmazások telepítése, beállítások megtétele.

A negyedik csoportba sorolható további feladatok a technikai elhárításért felelős szervezetek felelősségi körébe tartoznak. Míg a helyi szervezetek feladata a permanens biztonság megteremtése, addig a technikai elhárítóké egy mélyebb biztonsági pillanatkép felvétele. Ebbe beletartozik a helyiségek mellett a hordozható infokommunikációs eszközök átvizsgálási metodikájának kidolgozása, majd gyakorlati megvalósítása, helyi előírások áttekintése, azok megvalósításának ellenőrzése, az eszközök speciális – hardver sebezhetőségi, kémszoftverek elleni – vizsgálata. Szintén ide sorolható a védett vezetők által leggyakrabban használt internet-technológiára épülő szolgáltatások, ezen belül is a felhő alapú rendszerek folyamatos vizsgálata, majd ezek alapján a védett vezető figyelmének felhívása az általa használt rendszerek ismert sérülékenységeire, kockázataira.

A feladatok részletes kibontása és az egyes szereplők közötti megosztása azonban már túlmutat jelen cikk keretein, az egy későbbi feladat.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Jelen cikk összefoglalta a védett vezetők személyi használatú hordozható infokommunikációs eszközei, valamint internet-technológiára épülő szolgáltatások használata kapcsán felmerülő biztonságtudatossági alapképzés keretfeltételeit, figyelembe véve a védett vezetők speciális helyzetét. Erre, valamint a „Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából” című cikksorozatra építve felvázolta az alapképzés egy lehetséges tematikáját, majd bemutatta a biztonsági szint további emelését elősegítő továbblépési lehetőségeket. Mindeközben olyan általánosításokat tett, amely lehetővé teszi, hogy az oktatott anyag nem csak a védett vezető által éppen aktuálisan használt eszközre és szolgáltatásra legyen megfelelő, hanem azokat a védett vezetők képesek legyenek alkalmazni például egy új szolgáltatás vagy eszköz igénybe vétele esetén is.

A továbblépés lehetőségeiben megfogalmazottak mellett azonban más, az alapképzéshez szorosan kapcsolódó feladatokat is célszerű elvégezni. Először is a cikkben leírt tematikát tartalommal kell kitölteni, amely a képzést tartó szervezet szakembereinek, vezetőinek a feladata. Ugyancsak az ő felelősségük az oktatáshoz kapcsolódó anyagok (2-3 oldalas leírások, flash animáció, stb.) elkészítése.

Szintén az ő feladatuk, hogy a későbbiekben figyelemmel kísérjék a technológiai változásokat, az új eszközök új tulajdonságait, a megjelenő új internet-technológiára épülő szolgáltatásokat, az azokból eredő új veszélyeket, és ezeknek megfelelően – ha szükséges – javítsák, módosítsák, változtassanak, frissítsenek a képzés tartalmán, vagy adott esetben magán a tematikán is.

Célszerű további elméleti kutatásokat végezni és a technikai elhárításra, annak kiterjesztett értelmezése szerint egy új, pontos definíciót adni. Ennek kapcsán kell részletezni, pontosítani és elhatárolni a technikai elhárítók, valamint a helyi, elektronikus biztonságért felelő személyek, szervezetek feladatait, hatáskörét.

Mihamarabb szükséges kidolgozni egy, az alapképzésnél jóval többet adó, az elektronikus információk védelmét előíró jogszabályokkal összhangban lévő, hosszabb időtartamú, képzés tematikáját. Ennek fontos pontja az alapképzéshez hasonlóan az alábbiak:

- veszélyek bemutatása,
- biztonság megteremtésének módjai, beállítások, biztonságtudatos használat,
- ellenőrzés.

Ezt a lehető leghamarabb el kell indítani, még azelőtt, hogy azt jogszabályban kötelezővé tennék az érintett vezetői körnek.

Bár a továbblépés lehetőségeinél már szerepel, de kiemelést érdemel, hogy ugyancsak a lehető leghamarabb célszerű jogszabályi javaslatot megfogalmazni a hordozható infokommunikációs eszközök teljes életciklusát átfogó hatósági felügyeletére. Ebbe bele kell foglalni a beszerzendő eszközök engedélyezésétől kezdve, a használathoz kapcsolódó biztonsági előírások jóváhagyásán keresztül, a kivonáskor a használt adathordozók megsemmisítésének ellenőrzéséig minden olyan feladatot, amely hatósági eszköztárral segíti az elektronikus információbiztonság további emelését.

Felhasznált irodalom

[1] Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I. Hadmérnök, IX. Évfolyam 2. szám - 2014. június pp. 277 – 289 -ISSN 1788-1919

[2] Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából II. Hadmérnök, IX. Évfolyam 2. szám - 2014. június pp. 290 – 296 -ISSN 1788-1919