PRISZNYÁK SZABOLCS

RENDÉSZETI INFORMATIKAI RENDSZEREK BIZTONSÁGA

Bevezetés

Napjainkban a modern társadalmakban szinte nincs olyan területe a mindennapi életnek, amelyek mögött ne állnának informatikai rendszerek. Igaz ez a néhány személyes mikro vállalkozásoktól kezdve a multinacionális cégekig. Ugyanez elmondható a közigazgatásban is, így a néhány személyes önkormányzat ugyanúgy számítógépes adatbázisokban tárolja információit, mint a kb. 40 ezres létszámú rendőrség. Az adatok, információk és különösen ezek összefüggései értéket jelentenek. A vállalkozások esetében legtöbb alkalommal közvetlenül anyagilag kifejezhető az adatok elvesztéséből, vagy akár a nem megfelelő időben történő rendelkezésre állásából keletkező kár. A közigazgatásban, - azon belül a rendvédelemben – az egyes szervezetek jogszerű működésének alapját biztosítják a jól működő, megfelelő időben hiteles adatokat szolgáltató informatikai rendszerek. Az adatok – akár ideiglenes - hiánya működésképtelenséget, vagy nem jogszerű működést eredményezhetnek, amely közvetetten anyagi károkat okoz.

Az adat és az információ egy informatikai rendszer végterméke. A végtermék előállításához egy nagy bonyolultságú rendszer minden elemének rendeltetésszerűen kell működnie. A működés biztosításához, valamennyi azt fenyegető körülményt elemezni kell. Az elemzés alapján pedig ki kell alakítani a szükséges védelmet. Több szakember szerint az egyik legnagyobb veszélyt maga az ember jelenti. Az ember az aki tudatosan, vagy tudatlanul kárt tud okozni egy informatikai rendszerben.

A cikkben bemutatom, hogy az ember milyen veszélyeket jelenthet az informatikai rendszerekre. Ezen belül ismertetem, hogy miért jelent ez különös veszélyt a rendvédelmi szervezetek esetében.

Kritikus infrastruktúra, kritikus információs infrastruktúra

A kritikus infrastruktúra fogalma a XX. század végén vált ismertté. Mint sok minden más, ami a fejlettséghez, fejlődéshez köthető ez is a gazdaságilag és iparilag legfejlettebb országból az Amerikai Egyesült Államokból származik. Az Egyesült Államokban már 1998-ban – Bill Clinton elnöksége idején - elnöki direktívát adtak ki a kritikus infrastruktúrák védelmére vonatkozóan[1]. Az Európai Unió is megalkotta a maga szabályait, igaz néhány év késlekedéssel. Ennek legfőbb oka az volt, hogy a korábbi gyakorlat szerint, minden felmerülő problémára valamelyik tagországban már meglévő módszert, megoldást terjesztettek ki, adoptáltak a többi tagországra is. Ez a terület azonban olyan újdonság volt, amelyre nem volt meglévő, működő megoldás, szabályozás egyetlen EU tagállamban sem. 2004 júniusában az Európai Tanács átfogó stratégia kidolgozására kérte fel a Bizottságot a létfontosságú infrastruktúrák védelmének javítása céljából. A Bizottság 2004. október 20-án közleményt adott ki „A létfontosságú infrastruktúrák

[1] http://fas.org/irp/offdocs/pdd/pdd-63.htm (Letöltés ideje: 2015.06.08.)

védelme a terrorizmus elleni küzdelemben”[2] címmel. Az Európai Bizottság 2005-ben adta ki a „Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról”[3] dokumentumot. Ezt követően 2006-ban szintén az Európai Bizottság adta ki a „Létfontosságú infrastruktúrák védelmére vonatkozó európai program”[4] című közleményt, amely a hivatalos lapban is megjelent. A közleményben az Európai Bizottság meghatározza az európai és nemzeti létfontosságú infrastruktúrák védelmére vonatkozó európai program (EPCIP) végrehajtásához szükséges elveket és eszközöket.

A közösségi jogalkotást a nemzeti szabályozás követte. Az első Magyarországon megjelenő közjogi szabályozó eszköz a 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról[5]. Ebben a Kormány közzétette a nemzeti Zöld Könyvet igazodva az európai szabályozáshoz. A Kormány határozat mellékletében 10 ágazat 43 alágazata került meghatározásra, köztük a „Közbiztonság – Védelem” elnevezésű ágazat két alágazattal, a „honvédelmi létesítmények, eszközök, hálózatok” és a „rendvédelmi szervek infrastruktúrái”. A Kormány határozat 2008.12.17 - 2014.03.05 közötti időszakban volt hatályos. Ezzel párhuzamosan törvényi szintre emelkedett a terület szabályozása, megjelent a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről[6], amely 2013.03.01-től hatályos. A törvényben az ágazatok és alágazatok csak kis mértékben módosultak, de ez a honvédelmi, rendvédelmi területet nem érintette. A jogszabály a kritikus infrastruktúra fogalom helyett a létfontosságú rendszerek megfogalmazást alkalmazza. A létfontosságú rendszerelem fogalmát a törvény az alábbiak szerint határozza meg: „ az 1-3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna” (az 1-3 mellékletben az ágazatok és az alágazatok felsorolása található). A megfogalmazás lényegét tekintve azonos a kritikus infrastruktúra fogalmával, így megállapítható, hogy az elnevezés változása csupán nyelvi jelentőségű, hiszen a létfontosságú rendszer nem tartalmaz idegen eredetű szót. Ugyanakkor a 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról[7] 1. § 25. pontja a kritikus infrastruktúra kifejezést használja.

Az infokommunikációs technológiák egy önálló ágazatot jelentenek a kritikus infrastruktúrák között, az alábbi alágazatokkal:

- információs rendszerek és hálózatok,
- eszköz-, automatikai és ellenőrzési rendszerek,
- internet-infrastruktúra és hozzáférés,
- vezetékes és mobil távközlési szolgáltatások,
- rádiós távközlés és navigáció,
- műholdas távközlés és navigáció,
- műsorszórás,

[2] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:l33259 letöltve: 2015.06.08.
[3] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52005DC0576 letöltve: 2015.06.08.
[4] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52006DC0786 letöltve: 2015.06.08.
[5] http://njt.hu/cgi_bin/njt_doc.cgi?docid=120562.173569 letöltve: 2015.06.08.
[6] http://njt.hu/cgi_bin/njt_doc.cgi?docid=155940.287727 letöltve: 2015.06.08.
[7] http://njt.hu/cgi_bin/njt_doc.cgi?docid=140039.291215 letöltve: 2015.06.08.

- postai szolgáltatások,
- kormányzati informatikai, elektronikus hálózatok.

Ezek a rendszerelemek gyakorlatilag lefedik a rendvédelmi szervek informatikai rendszereit is, hiszen az része a kormányzati informatikai rendszereknek. A rádiós távközlésbe beleértendő az Egységes Digitális Rádió-távközlő rendszer is. Meg kell említenünk ugyanakkor a kritikus információs infrastruktúrákat, amelyek ebben a megfogalmazásban nem képezik a kritikus infrastruktúrák részét, csupán azok hátterét adhatják. Mint korábban említettem a modern társadalmak szinte minden rendszerének a hátterét informatikai rendszerek képezik. Ebből logikusan az következik, hogy amennyiben egy kritikus infrastruktúra működését támogató, biztosító informatikai rendszerben rendellenes működés, káresemény, meghibásodás következik be, úgy a kritikus infrastruktúra rendeltetésszerű működése kerül veszélybe. Ebből következően a kritikus informatikai infrastruktúrát, annak egyes elemeit ugyanúgy védeni kell, mint magát a kritikus infrastruktúrát közvetlenül alkotó rendszerelemeket. Fentiek okán a rendvédelmi szervek informatikai rendszerei egyrészt a jogszabályból következően, másrészt, mint a működést támogató, biztosító háttér szolgáltatás is a védendő elemek közé tartoznak.

Informatikai rendszerek elemei, lehetséges kockázatok

Az informatikai rendszerek fogalma nem egy egzakt fogalom. Különböző kutatások más és más elemeket sorolnak az informatika, mint gyűjtőfogalom körébe. Az eltérő megállapítások elsősorban abból adódnak, hogy az informatika egy folyamatosan fejlődik, egyre szélesebb területeket hódít meg. A tudomány oldaláról történő megközelítéssel az informatika az információ gyűjtésével, tárolásával, továbbításával, feldolgozásával és szolgáltatásával foglalkozó tudomány. A gyakorlatban az informatika részét képezi a számítástechnika, valamint a vezetékes és vezeték nélküli távközlés. Fentiek alapján a védendő rendszerelemek az alábbiak szerint csoportosíthatók:

- *Hardver*
  - Munkaállomások
  - Perifériák
  - Szerverek
  - Központi infrastruktúra elemek (tároló egységek)
  - Működést biztosító szolgáltatások (áramellátás, klíma, stb.)
- *Szoftverek*
  - Operációs rendszerek (szerver, munkaállomás)
  - Általános célú alkalmazások
  - Funkcionális információs rendszerek
  - Adatbázisok
- *Hálózatok*
  - Helyi hálózatok (LAN)
  - Táv-adatátviteli hálózatok (WAN)
- *Távközlési rendszerek*
  - Telefonközpontok
  - Vezeték nélküli telefon (mobil),
  - Rádió-távközlési rendszer (EDR)
- *Biztonságtechnikai rendszerek*

Az informatikai rendszerek esetében felmerülő veszélyeket előzetesen fel kell mérni, hogy meg tudjuk tenni a megelőző intézkedéseket. Ezeket a kockázatelemzéseket célszerű nemzetközi szabványokban rögzítettek szerint elvégezni, hiszen ezzel egy komplex elemzést végezhetünk. Napjainkban az informatikai rendszerek kockázatelemzésére leggyakrabban az IEC/ISO 27005[8] szabvány alkalmazzák, e szabvány először 2008-ban[9] jelent meg, de napjainkban már az újabb 2011-ben kiadott változatot[10] alkalmazzák. A szabvány alapján az alábbi fő kockázatok merülhetnek fel egy informatikai rendszer vonatkozásában:

- Fizikai hatások: tűz, víz, szennyezés, berendezés megrongálódása, elvesztése stb.
- Természeti események: árvíz, meteorológiai jelenség (pl.:villámlás), vulkán, földrengés, éghajlat.
- Kulcsfontosságú szolgáltatás kiesése: klímaberendezés, áramellátás, telekommunikációs berendezések.
- Sugárzás miatti zavar: elektromágneses sugárzás, impulzus, hősugárzás.
- Technikai meghibásodás: eszközök, berendezések, szoftverek meghibásodása.
- Információ kompromittálódása: lehallgatás, távoli kémkedés, adathordozó, eszközök ellopása, kidobott média helyreállítása, árulás, hardverek, szoftverek elrontása, pozíció kinyomozása.
- Illetéktelen cselekedetek: eszköz-, és szoftverhasználat, illegális, hamis szoftverek, illegális, hamis adatok.
- Funkció kompromittálódása: jogokkal való visszaélés, tevékenység megtagadás, személyes hozzáférés megakadályozása

A kockázatelemzés nem végezhető el csupán az ismertetett szabványok alapján, a korrekt elemzéshez a területhez tartozó szakirodalom bővebb tanulmányozása szükséges. A kockázatelemzéssel kapcsolatosan iránymutatást ad Kerti András publikációja[11], amelyben a kockázatelemzés oktatásnak – és ezen keresztül gyakorlati végrehajtásának – buktatóit mutatja be a Magyar Honvédség vonatkozásában. Megállapításai helytállóak a rendvédelem területén is.

A hivatkozott szabvány alapján bemutatott lehetséges kockázatok közül – a felsorolás szerinti utolsó - három csoport az információ kompromittálódása, az illetéktelen cselekedetek valamint a funkció kompromittálódása az emberi tevékenységhez köthető kockázatok. Jelen publikáció további részében ennek alapján az emberre, mint a rendvédelmi szervek informatikai rendszerei esetében felmerülő kockázatra fókuszálok.

Kockázatot jelentő személyek csoportosítása

Egy vállalat, így a közigazgatás részeként a rendvédelmi szervek esetében is alapvetően két fő csoportra oszthatjuk az informatikai rendszerre valamilyen formában

[8] International Standard ISO/IEC 27005 Information technology – Security techniques – Information security risk management

[9] http://www.iso.org/iso/catalogue_detail?csnumber=42107 letöltve:2015.06.09

[10] https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en letöltve: 2015.06.08.

[11] Kerti András: Az információbiztonsági kockázatkezelés oktatásának buktatói = Kommunikáció 2013: Communications 2013, 2013. Nemzeti Közszolgálati Egyetem 53-60. o.

kockázatot jelentő személyeket. A két csoport valójában három, hiszen külön kell kezelni a két fő csoport metszetét alkotó harmadik csoportot.

Az első csoportot az adott szervezet saját dolgozói jelentik. Ezt a csoportot tovább bonthatjuk aszerint, hogy az informatikai rendszerhez – így a szervezet működéséhez szükséges információkhoz – milyen szintű, milyen jogosultságú hozzáféréssel rendelkeznek a különböző alcsoportok. A legszélesebb jogosultsággal az informatikai szakterület munkatársai – főként a rendszer adminisztrátorok (rendszergazdák) – bírnak. Ennek oka, hogy ez nélkülözhetetlen a napi rutinfeladataik végrehajtásához. Ezzel együtt ők jelentik a legnagyobb kockázatot egy szervezet informatikai működésének vonatkozásában. Sebestyén Attila részletesen feldolgozta a témakört doktori értekezésében[12], ennek alapján a fő kockázati okok a nélkülözhetetlenség, pótolhatatlanság hangsúlyozása, sértettség, zsarolás, anyagi haszonszerzés, véletlenül vagy tudatlanságból elkövetett hibás beállítás. A témát érinti Molnár Bálint és Kő Andrea Információrendszerek auditálása[13] című könyvében. További kockázatot jelentő személyek az adatgazdák, adatkezelők, adatfeldolgozók. Ezen személyek – jól szabályozott és ennek megfelelően konfigurált informatikai rendszerben – csak az információk egy szeletéhez férnek hozzá (pl. a gazdasági szakterület csak a gazdálkodással kapcsolatos rendszerekhez, a személyzeti szakterület csak a személyzeti rendszerhez, stb.). Ennek alapján is megállapítható, hogy a teljes rendszer vonatkozásában a rendszergazdák jelentik a legmagasabb kockázati tényezőt.

A másik csoportba az adott szervezeten kívüli személyeket soroljuk. Itt nem csak konkrét személyekre kell gondolnunk, hanem olyan személyekre, személyek csoportjára, akik egy másik – legális vagy illegális – szervezet tagjai. Természetesen ha információk, adatok eltulajdonításáról, informatikai rendszerek működésének ellehetetlenítéséről beszélünk, akkor az esetek többségében megállapítható, hogy illegális szervezetek végeznek ilyen tevékenységet. Amennyiben legális szervezet végez ilyen tevékenységet, akkor általában két ország szembenállásáról van szó, ahol a hagyományos fegyverek mellett a cyber térben is zajlik a harc. A cyber térben történő hadviselésről, információs műveletekről Haig Zsolt és Kovács László publikációja[14] ad bővebb képet. A külső személyek csoportját az informatikai rendszerekbe behatolók (ismertebb megnevezéssel: hackerek), illegális csoportok, politikai szervezetek esetleg egy állam legális szervezetei alkotják. A külső személyek és szervezetek elsősorban passzióból, szakmai tudásuk hangsúlyozása, speciális közösség elismerésének kivívása, anyagi, üzleti haszonszerzés, adat, információ felhasználása valamilyen későbbi előny megszerzése, vagy a kár csökkentése érdekében hatolnak be informatikai rendszerekbe, okoznak kárt, vagy szereznek meg adatot, információt.

A harmadik csoportba azok a személyek tartoznak, akik a formál logikát követve a külső személyek csoportjába tartoznak, hiszen hivatalosan nem tagjai, nem alkalmazottai az adott szervezetnek. Kockázatelemzés szempontjából azonban a belső és a külső személyek alkotta halmazok metszetét is egy külön csoportnak kell tekintenünk. Ebbe a csoportba tartoznak azok a személyek (szervezetek) akik az adott szervezettel valamilyen formális kapcsolatban vannak. Ide tartoznak pl. a szerződéssel a szervezetnél különböző rendszerességgel munkát végzők, az együttműködők, stb. Ezen személyek sok esetben az informatikai rendszerhez is rendelkeznek jogosultsággal, hiszen végezhetnek olyan munkát

[12] Sebestyén Attila: Stációk és determinánsok a rendvédelmi szervek informatikai működésének fejlődésében = doktori (Phd) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, 2009. 61-68. o.
[13] Molnár Bálint – Ko Andrea: Információrendszerek auditálása: Corvinno Kiadó, Budapest 2009. 76-101. o.
[14] Haig Zsolt – Kovács László: Fenyegetések a cybertérből = Nemzet és Biztonság 2008/5. 61-69. o.

ami ezt indokolja. Sokszor egyes informatikai szaktevékenységek kerülnek kiszervezésre – azaz olyan munkavállaló által történik munkavégzés, aki formálisan nem tagja a szervezetnek – ebben az esetben ezen személyek magas szintű jogosultsággal rendelkeznek. Gyakori, hogy a szervezetek, köztük a rendvédelmi szervek is olyan speciális szaktudást igénylő tevékenységet szerveznek ki, mint pl. központi hálózati eszközök konfigurálása, amely nagyon magas szintű hozzáférést jelenthet a szervezet informatikai rendszeréhez, amely ezzel együtt magas kockázatot is jelent. Azonban az információk megszerzéséhez nem minden esetben szükséges jogosultsággal rendelkezni, elegendő, hogy a kiszervezett munkavállalónak joga van az épületben, irodában tartózkodni, így kihasználhatja az ott dolgozók felületes, nem szabályszerű eljárásait (pl. a takarítással megbízott személy könnyen információhoz juthat a nem zárolt számítógépről, vagy az informatikai rendszerből kinyomtatott, de el nem zárt papírról is).

Érdekesség, hogy Sebestyén Attila fent hivatkozott értekezésében a szervezettől kilépett informatikai dolgozót is a belső dolgozókkal azonosan javasolja kezelni, az érintett rendelkezésére álló információk okán. Véleményem szerint a kilépett munkatársakat is a köztes kategóriába célszerű sorolni, de csak abban az esetben, ha az informatikai biztonsági szabályok érvényesítése valóban megtörténik (pl. a kilépés napján törlésre vagy letiltásra kerül a felhasználói azonosító, törlésre kerül az e-mail cím, és tiltásra kerül minden más olyan technikai lehetőség, amellyel a szervezet információs rendszere elérhető).

A kutatások azt támasztják alá, hogy legtöbb esetben a szervezet saját dolgozói okozzák a kárt az informatikai rendszerekben, ők tulajdonítják el az adatokat. Egy számítógépes információbiztonságról szóló könyvben[15] publikált felmérés szerint az adatlopások közel 82%-át a szervezetek saját dolgozói követik el. Bár a könyv megjelenése óta több, mint 15 év eltelt – ami a szakterület specialitásait, gyors fejlődését figyelembe véve – hosszú idő, de valószínűsíthető, hogy a tendenciák nem változtak. A terület kutatása nehézkes, hiszen ilyen jellegű információkat a vállalatok nem szívesen adnak ki, mert ezzel elismernék informatikai rendszerük sebezhetőségét, a belső szabályozás, ellenőrzés elégtelenségét.

Több informatikai biztonság területén elismert nemzetközi szakértő véleménye is azt támasztja alá, hogy a legnagyobb problémát a belső személyek okozzák. Kevin D. Mitnick könyvében[16] ismertette a „social engineering" fogalmát, amely a gyakorlatban az emberek megtévesztését jelenti. A fent ismertetett halmaz elméletet alapul véve a külsős személynek, akinek információra van szüksége kézenfekvőbb egy belső személytől valamilyen módon megszereznie azt, mint bonyolult informatikai rendszereken - kétes végeredménnyel kecsegtető - támadásokat indítania. A Mitnick által ismertetett módszer a belsős kollégák megtévesztésén alapul, amelynek pszichológiai háttere van. A másik módszer a megvesztegetés, esetleg zsarolás.

Bruce Schneier amerikai kriptográfus és informatikai biztonsági szakember alapgondolata szerint „Az amatőr a technikát, a profi a humánerőforrást támadja."[17]. Ez az állítás egybecseng Mitnick megállapításaival.

[15] Visnyei Aladár – Vörös Gábor: A számítógépes információbiztonság alapjai. LSI Oktatóközpont, Budapest, 1997. 18-19. o.
[16] Mitnick Kevin D.: A legendás hacker – A megtévesztés művészete. Perfact – Pro Kft., Budapest 2003. 6-10. o.
[17] http://www.bluekey.hu/veszelyes-rendszergazdak/ letöltve: 2015.07.30.

Szabályozás

Az informatika az 1990-es rendszerváltozást követően terjedt el Magyarországon. Ennek oka, hogy a technikai fejlődés ekkora jutott olyan szintre, hogy a vállalkozások és a közigazgatás számítógépeket alkalmazzon. Nem mellékes, hogy a CoCom lista[18] - multilaterális kereskedelmi embargó - miatt az egykori szocialista blokk tagjai, így Magyarország sem vásárolhatta meg az euro-atlanti országokban (összesen 17 országban) fejlesztett és gyártott számítástechnikai eszközöket. A szocialista országok által fejlesztett számítógépek viszont műszaki téren jelentős lemaradásban voltak a nyugati technikához képest. Az informatikai eszközök elterjedésének másik mozgatórugója, hogy a rendszerváltozással megtörténő gazdasági szerkezetváltás hatására Magyarországra települő nyugat-európai, amerikai, távol-keleti multinacionális nagyvállalatok az anyavállalatnál már sikeresen működő informatikai rendszereiket magyar leányvállalataikba is adoptálták. Ezen a téren a legfejlettebbek a pénzügyi szolgáltatók, bankok, biztosító társaságok voltak. Ezek a vállalatok a legtöbb esetben a vállalatok belső szabályozását is meghonosították, természetesen szükség esetén a hazai jogszabályokhoz igazítva. Így nem csak a technológia került az országba, hanem annak használatára vonatkozó szabályzói környezet, vállalati kultúra is.

Ez a folyamat azonban nem zajlott le a közigazgatásban. Az eszközök és alkalmazások számának robbanásszerű növekedését nem – vagy csak nagyon lassan - követte a szabályozás, sőt kezdetben egyáltalán nem voltak kifejezetten az informatikai rendszerek fejlesztésére, üzemeltetésére vonatkozó jogszabályok. A terület teljesen nem volt szabályozatlan, hiszen más jogszabályok által meghatározott előírásokat az informatikai rendszerekben is érvényesíteni kellett. Ilyen pl. a szerzői és szomszédos jogokról szóló jogszabályok, valamint az adatvédelmi jogszabályok. Az informatikai rendszerekben – különösen a közigazgatási, ezen belül a rendvédelmi rendszerekben - jellemzően adatkezelés történik, mégpedig annak speciális esete személyes, sőt különleges adatok (pl.: bűnügyi személyes adat, egészségügyi személyes adat, stb.) kezelése. A jogszabályokban foglaltakat az adatkezelés technológiájától függetlenül érvényesíteni kell, tehát függetlenül attól, hogy az adatkezelés papír alapon vagy elektronikusan történik (pl. a harmadik fél számára átadott adatokról adattovábbítási nyilvántartást kell vezetni).

A kifejezetten informatikai rendszerre vonatkozó jogszabályok hiánya elodázta a szervezetek belső szabályozási rendszerének kialakítását is. A jogi szabályozás hiánya elsősorban abból fakad, hogy az informatika fiatal, gyorsan fejlődő szakterület, amely nem csak mennyiségében, de minőségében, eszközrendszerében is napról napra változik. Egy a kiadás pillanatában aktuális szabályzó akár hónapok alatt technológiailag elavulttá válhat. A technológia követése pedig nem egy egyszerű módosítást jelent, hanem sok esetben az alapoktól induló gyökeres változtatást követel. A leglátványosabban a tárolóeszközök fejlődéséből vezethető le a technológia változása:

- floppy lemez (1,2 Mb, 1,44 Mb),
- CD lemez (700 Mb),
- DVD lemez (4,3 Gb = 4.300 Mb),
- USB stick, pen drive (ma már akár 512 Gb = 512.000 Mb, sőt akár 1 Tb),
- SD kártya (és más szabványú memóriakártyák) (ma már akár 512 Gb = 512.000 Mb),

[18]http://nyomaban.blog.hu/2014/08/21/cocom-lista_a_vagyott_nyugat_kereszthuzasai letöltve: 2015.05.10.

- mobiltelefonok (belső memória és memóriakártya tárolókapacitása),
- e-mail (több e-mailben gyakorlatilag korlátlan mennyiség), nincs fizikai eszköz,
- felhő alapú rendszerek (gyakorlatilag korlátlan), nincs fizikai eszköz.

Fenti példában jól követhető, hogy néhány év alatt milyen mértékben növekedett az egy-egy eszköztípuson tárolható adatmennyiség. Ráadásul a mennyiség növekedésével fordítottan arányosan az eszközök mérete egyre csökkent. Napjainkban nagy mennyiségű adat – akár illegális - mozgatásához már nincs szükség fizikai eszközre sem.

A késve történő szabályozás érvényesítése nehézkes, hiszen addigra már kialakul a rossz gyakorlat, amit utólagosan nehéz átalakítani. Az utólagos szabályzók esetében nem csak a gyakorlatban történő alkalmazás, hanem a szabálytalan eljárások szankcionálása is problémás.

Kifejezetten kormányzati informatikával foglalkozó törvényi szintű szabályozás csak 2013-ban jelent meg, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény[19]. A jogszabály 11. § (1) bekezdés C.) pontja kimondja, hogy valamennyi érintett szervezetnek az elektronikus információk biztonságáért felelős személyt (kiberbiztos) kell kijelölnie. A jogszabály alapján a szervezeti hierarchiában a kiberbiztos nem a szervezet informatikai szervezeti egységén belül helyezkedik el. A jogszabály valamennyi szervezet részére előírja elektronikus információs rendszereinek felmérését, nyilvántartását, osztályba sorolását. A szervezeteknek informatikai biztonsági politikát, stratégiát és szabályzatot kell készíteniük. A jogszabály meghatározza az elektronikus információs rendszerek felügyeletének kormányzati hierarchiáját. Ezzel a jogszabállyal a közigazgatás, ezen belül a rendvédelem megtette az első lépést az informatikai rendszerekre vonatkozó rendteremtés területén.

Nagyon lényeges, hogy a különböző dokumentumokban (stratégia, politika, szabályzat) foglaltakat folyamatosan oktatni kell a szervezetek személyi állományának. A technológiai fejlődésből következően a dokumentumok folyamatosan felülvizsgálatra, módosításra szorulnak, amit aztán ismét oktatni kell. A feladat tehát nem egy egyszer végrehajtandó lineáris folyamat megvalósítása, hanem egy folytonos ciklikus rendszer kialakítása. Szintén kiemelt cél a felhasználói tudatosság kialakítása, ezzel az informatikai kultúra szintjének emelése, pl.: a Büntetés-végrehajtás Országos Parancsnokságának Informatikai Biztonsági Szabályzatában foglaltak szerint: „*A szabályzat kifejezett célja a felhasználói tudatosság megteremtése az informatikai védelem és biztonság témakörében, nemcsak az egységes értelmezés, hanem a jelen szabályozásból fakadó szellemiség érvényesülése érdekében is. A felhasználók az alapelvek, a szabályzatban rögzített normatívák és az ezekből fakadó szellemiség alapján kötelesek felelősen végezni szolgálati feladataikat, és törekedni arra, hogy mások is e szerint járjanak el.*”[20]

Az ember, mint kockázati tényező esetében azonban a ciklikusságra nem csak fenti esetben, hanem a megelőzésben, ellenőrzésben is figyelemmel kell lennünk. Ványa László publikálta[21] „A biztonság területeinek felosztása a védelmi szférában” című ábráját, amely a rendvédelem területén is alkalmazható. Ebben alapvetően két fő részre osztja a biztonság

[19] http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.296212 letöltve: 2015.07.30.

[20] A büntetés-végrehajtás országos parancsnokának 1-1/13/2011.(III. 22.) OP intézkedése a büntetés-végrehajtási szervezet informatikai biztonsági szabályainak kiadásáról

[21] Ványa László: Vezetéstechnikai rendszerek védelmének alapjai (oktató cd), Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2008

területeit, ebből a személyi állománnyal összefüggő a „Műveleti biztonsági rendszabályok”, ennek részeiként pedig az alábbi területeket sorolja fel:

- személyi biztonság
- fizikai biztonság
- dokumentum biztonság
- elhárítás

A felsoroltak végrehajtásával járó feladatok, a vonatkozó szabályok betartása, azok ciklikus rendszerben történő ellenőrzése mind-mind szükségesek az elektronikus informatikai rendszerek legfőbb kockázati tényezője az ember által okozott károk minimalizálása érdekében.

Összegzés, javaslatok

Jelen publikációban bemutattam a rendvédelmi szervek informatikai rendszereit, mint kritikus infrastruktúra és egyben kritikus információs infrastruktúra. Ismertettem az informatikai rendszerek kockázatelemzésére alkalmazható – szabványos – módszert, bemutatva annak egyes elemeit. A lehetséges kockázatok közül kiemeltem azokat, ahol a legfőbb kockázati tényező az ember. Egy szempontrendszer alapján csoportosítottam a kockázatot jelentő személyeket (személyek csoportjait). Megállapítottam, hogy a legnagyobb kockázatot a szervezetek saját humánerőforrása jelenti. Ez a kockázat egyrészt a szabályzói rendszer késői kialakulásából következik, amelynek bemutattam okait. Ismertettem a területet érintő legfrissebb törvény legfontosabb előírásait. A mű végén felhívtam a figyelmet az oktatásra, valamint a megelőző, védelmi, ellenőrzési tevékenység ciklikusságának szükségességére.

A kutatás során tapasztaltak alapján célszerűnek tartom a legalább ágazati szintű egységes szabályozást az informatikai biztonság területén. E szerint a Belügyminisztériumnak kell irányítania, egységes mederbe terelnie az alárendeltségébe tartozó szervezetek, köztük kiemelten a rendvédelmi szervek informatikai biztonsági rendszereinek kialakítását. Ennek megvalósítása céljából célszerű lenne egy tudásbázist létrehozni, emellett a témában ágazati konzultációkat, fórumokat lehetne tartani. Ha megvalósul az egységes stratégia, politika és szabályozás, akkor célszerű egységes oktatási tematikát készíteni. Az informatikai biztonsággal kapcsolatosan elkészített tananyag oktatását a tudatosság, felelősségérzet kialakítása érdekében célszerűnek tartanám rendszeresíteni a rendészeti szak- és felsőoktatásban.

A közigazgatás, így a rendvédelem informatikai rendszereinek egy részét – ezek közül kiemelten a Nemzeti Kormányzati Gerinchálózatot – a kormányzati hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet[22] alapján a Nemzeti Infokommunikációs Zrt. (NISZ Zrt.) üzemelteti. A NISZ Zrt. bevonásával olyan – a szervezetek részéről igény szinten már megjelent – műszaki megoldásokat kell kialakítani, amelyek az informatikai biztonságot növelik. Pl. a közbeszerzések ellenőrzéséhez szükséges – jellemzően nagy méretű – dokumentációk jogszabály[23] szerinti elektronikus megküldése a Miniszterelnökség részére nem megoldott (vagy csak kerülő megoldásokkal megoldható). Célszerűnek tartanám – mint biztonsági kockázat csökkentő megoldást - a nagy méretű e-mail-ek

[22] http://njt.hu/cgi_bin/njt_doc.cgi?docid=133882.291204 letöltve: 2015.07.30.
[23] 46/2011. (III. 25.) Korm. rendelet a közbeszerzések központi ellenőrzéséről és engedélyezéséről

küldésére alkalmas kormányzati szolgáltatás megvalósítását a NISZ Zrt. által üzemeltetett Kormányzati Felhőt felhasználva.

Összegezve megállapítom, hogy az informatikai rendszerek kockázatai – köztük az ember jelentette kockázat – nem szüntethető meg, de törekedni kell erre.