HADMÉRNÖK

XI. Évfolyam 2. szám - 2016. június

Fehér Judit
feherjenator@gmail.com

A RENDŐRSÉGI INFORMATIKAI HÁLÓZATOK INFORMÁCIÓBIZTONSÁGI HÁTTERÉNEK MEGHATÁROZÁSA

Absztrakt

Az információbiztonság helyzetéről készülő felmérés, a biztonság, az irányítás és a kockázatkezelési területek helyzetéről adhat egyszerre objektív és átfogó képet. A hálózat információbiztonsági hátterének meghatározásához, valós értékek eléréséhez meg kell vizsgálni a hálózathoz tartozó dokumentumokat, az informatikai rendszerek és a hálózat lehetséges fenyegetéseit, veszélyhelyzeteit. Mindehhez sérülékenység vizsgálatokat kell lefolytatni, amely párhuzamosan kockázatelemzés elvégzését is feltételezi. A rendőrség egyes informatikai hálózatainak információbiztonsági hátterének vizsgálatai, illetve ezek eredményei valós, gyakorlat orientált információbiztonsági kérdéseket vetnek fel. A feltárt hiányosságokból és tapasztalatokból az informatikai hálózatok információbiztonsági követelményrendszerét lehet megállapítani annak érdekében, hogy a várható biztonsági szintnek és védettségnek az megfeleljen.

A survey about the situation of IT security provides an objective and a comprehensive picture about the situation of security, governance and risk management areas. To determine the network information security background and to the achieve fair values, should be examined documents belonging to the network, the potential threats and the risk positions of information systems and networks, which should be conducted vulnerability assessments with risk analysis. The results of some police information network of information security background investigation raises real practice-oriented information security issues. The identified deficiencies and experiences in the information security requirements of the IT network system can lead to ensure that the expected level of security and protection has been fulfilled.

***Kulcsszavak**: információbiztonság, informatikai irányítás, informatikai kockázatkezelési eljárások ~ information security, information management, information risk management*

BEVEZETÉS

A rendőrségi informatikai rendszereinek és különösen a hálózatainak információbiztonsági kérdéseinek feltárásához több irányú, területileg és időben eltolódó elemzést kell lefolytatni. Elsődlegesen a jelen helyzetből kell kiindulni. A rendőrségi informatikai rendszereken összességében a rendőrségi informatikai hálózatok kerülnek értelmezésre. A rendszerek információbiztonságának vizsgálatához az adminisztratív oldalról megközelítve dokumentumelemzéseket kell lefolytatni, mely során mintavételezéssel kerül meghatározásra az egyes rendőrségi informatikai hálózatok biztonsági helyzete, melyet a rendszer egészére ki lehet vetíteni. A valós értékek eléréséhez meg kell vizsgálni, a mintavételezés során kiemelt informatikai hálózatok lehetséges fenyegetéseit, veszélyhelyzeteit, melyhez dokumentum elemzéseket az adminisztratív területen, a fizikai területen pedig sérülékenység vizsgálatokat kell lefolytatni kockázat elemzéssel. Ezen eredmények a valós gyakorlat orientált információbiztonsági kérdéseket veti fel, mely alapján a hiányosságokból és tapasztalatokból a követelményrendszerét lehetne a kiemelt rendőrségi informatikai hálózatoknak megállapítani. Mindezt annak érdekében, hogy a várható biztonsági szintnek és védettségnek megfeleljenek rendszer szinten. Viszont jelen vizsgálat csak adminisztratív területre szorítkozva az információbiztonsági dokumentum elemzések eredményeit fogja feltárni, a fizikai vizsgálattal egybekötött teljes információbiztonsági hátteret, azok eszközrendszerét, a sérülékenység elemzés és kockázat elemzés eredményeit nem tárja fel.

Az információbiztonsági dokumentumok vizsgálata kiterjesztésre került mind a haza szakmai ajánlásokra, mind a nemzetközi ajánlásokra. Alapvető információbiztonsági dokumentumként kerül használatra a Rendőrségi Ideiglenes Informatikai Biztonsági Szabályzata, és az ISO/IEC 27001:2013 „A” melléklet 10.6 fejezete, a hálózatbiztonsági követelmények tekintetében.

A rendőrségi informatikai hálózatok információbiztonsági helyzetvizsgálata során a fenti dokumentumok átfogó elemzése került lefolytatásra. A dokumentumok szakterületi vonatkozásában az informatikai hálózatok információbiztonságával kapcsolatos rendelkezések köre térben és időben kerülnek szűkítésre. Időbeli vonatkozásában csak és kizárólag a jelen szakirányítási időszakban 2010-óta született és a rendőrségi informatikai hálózatok információbiztonságával kapcsolatos dokumentumok feldolgozására koncentrálódik. Pontosan ezen szempontrendszer miatt a fent említett két dokumentum analízisének célja felkutatni azon pontokat, ahol ráutaló szakmai meghatározásokat találhatunk a rendőrségi informatikai hálózatok információbiztonsági helyzetére vonatkozóan.

A vizsgálat területe korlátozásra került a Nagytávolságú és helyi hálózatok biztonsági osztályba sorolásának állapotában, helyzet felmérésében, a szükséges intézkedések meglétében, az érvényben lévő előírások alkalmazhatóságában, fizikai megvalósíthatóságában. Az elemzés nem terjed ki a minősített hálózatokra, és a kritikus infrastruktúra elemekre.

A vizsgálati pontok fogalmi szintjei:

- információbiztonsági helyzet felmérés,
- biztonsági osztályba sorolás vizsgálata,
- intézkedések megléte, kockázat kelezési eljárások
- előírások alkalmazhatósága,
- fizikai megvalósíthatósága.

A fenti pontok és az azokat övező utalások, a kiemelt informatikai hálózatok információbiztonság vizsgálati eredményei a rendőrségi informatikai hálózatok információbiztonsági helyzetének hátterét mutatják meg.

Ezek alapján a mintavételezésnek megfelelően kiválasztásra került a két legnagyobb terület a rendőrségi hálózatbiztonság területén:

- a rendőrség nagytávolságú informatikai hálózata,
- a rendőrség lokális (helyi) informatikai hálózata.

A RENDŐRSÉG NAGYTÁVOLSÁGÚ INFORMATIKAI HÁLÓZATA - KOMMUNIKÁCIÓS HÁLÓZAT HELYZETVIZSGÁLATA

Az elemzés első lépésében kijelölésre került a rendőrség nagytávolságú informatikai hálózata, azon belül a kommunikációs hálózatot. A vizsgálat szempontjai:

- információbiztonsági helyzet felmérés, a rendszer összetétele, a rendszer kapcsolatai, a rendszerek összekapcsolódásai,
- biztonsági osztályba sorolás, sérülékenység elemzés, kockázat kezelés
- specifikus előírások, előírások alkalmazhatósága,
- fizikai megvalósíthatóság, fizikai védelem.

A rendőrségi hálózatok megkülönböztetése:

- a nagytávolságú-,
- a helyi-,
- a minősített-,
- a zártcélú-,
- a nyíltcélú hálózat,
- a kritikus infrastruktúra.

A vizsgálati szempontrendszert szűkített spektrumának vizsgálatában a nagytávolságú hálózatokon belül elkülönítésre kerül speciális területként a kommunikációs hálózat.
Első elemzési pont a helyzet felmérés. A jelenlegi országos kommunikációs hálózat, az 1994-ben az ORFK és a BM Adatfeldolgozó Hivatal közös beruházásában üzembe helyezett zárt rendszerű X.25-ös táv-adatátviteli hálózat. A rendszer a megyei rendőr-főkapitányságok, és a budapesti kerületi kapitányságok részére biztosít hozzáférést a központi adatbázisokhoz. A városi kapitányságok modemes kapcsolattal a megyei főkapitányságokon keresztül érik el az X.25-ös hálózatot. A rendszerhez hozzáférésük van a BM, az ORFK és a BRFK központi szerveinek, valamint a közigazgatási hivataloknak és a határőrségi igazgatóságoknak.
Az X.25-ös hálózat mintegy 6 000 végponttal rendelkezik, pont-pont hierarchiájú kapcsolat van RIK és a megyei főkapitányságok között.

Második pontként a biztonsági osztályba sorolást vizsgálata következett. Az ORFK szakmai képviseletével történő egyezetések kerültek a vizsgálat érdekében lefolytatásra, továbbá a Nemzeti Elektronikus Információbiztonsági Hatósággal a rendőrségi nagytávolságú informatika hálózat biztonsági osztályba sorolásának tekintetében. Egyértelmű megállapítást nyert, hogy nem került besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak. A biztonsági osztályba sorolás hiányosságának vizsgálata során arra hiányosságra is fény derült, hogy nem lelhetőek fel sem intézkedések írásos formában, sem kockázat kezelési eljárások. A kutatás kiterjedt a sérülékenység elemzési vizsgálatok eredményeire is, de nem voltak fellelhetőek egyik irattárban sem.

Harmadik pontként az előírások alkalmazhatóságát tesztelésre került sorra. A dokumentum vizsgálatokból egyértelműen kiderült, hogy általános érvényű utalásokat lelhetőek fel a rendőrség Ideiglenes Informatikai Biztonsági Szabályzatában, viszont konkrétumokat nem fogalmazott meg, így azok alkalmazhatóságát nem lehetett vizsgálni. Ezen hiányosság abból következett, hogy a biztonsági osztályba sorolás nem történt meg, így specifikusan előírásokat nem lehetett megfogalmazni.

Negyedik pontként a fizikai megvalósíthatóság tekintetében a kommunikációs hálózatot a külvilágtól kívülről és az egyes szervezetek egymás között tűzfalakkal védik. A kábelezés fizikai védelmében viszont hézagokat lehetett felfedezni, sajnos a védelem nem megoldott, ezt kábelezési rajzok támasztották alá. Ez s egyértelmű eredményterméke volt az előírások hiányosságának.

A RENDŐRSÉG LOKÁLIS (HELYI) INFORMATIKAI HÁLÓZATAINAK HELYZETVIZSGÁLATA

A vizsgálat második lépésében kijelölésre került a lokális helyi informatika hálózatok analízise. A szempontrendszerében az előző vizsgálati elemeket figyelembe véve a nagyobb speciális területről haladva a kisebb terület felé volt az elsődleges. A cél a lokális hálózatok elemzésénél a közös használati szempontok helyett az egyéni szempontokat kerültek előtérbe.

Valamennyi kapitányság rendelkezik számítógépes hálózattal, amelyek lehetővé tették rendkívül sok, a rendőrségi szakmai munkát támogató alkalmazás fejlesztését és elterjesztését. A vizsgálat alapját képezték az ORFK szakmai dokumentumai.

Első pontként a helyzet vizsgálat során megállapítást nyert, hogy a lokális hálózatok többnyire NetWare 3.x, kisebb részben NetWare 4.x operációs rendszerre épülnek. Valamennyi hálózat jellemzője, hogy független információs 'szigetekként' működve, helyi alkalmazásokat szolgálnak ki, egymással –vagy egy központi informatikai rendszerrel - kommunikálni, adatot cserélni nem tudnak.

Kivételt képez ez alól a Teve utcai RIK, ahol a hierarchikus szoftvergerinc kiépítésének köszönhetően egységes és integrált informatikai infrastruktúráról beszélhetünk.

A lokális informatikai hálózatok munkaállomásai vegyesen 386, 486, illetve Pentium alapú PC-k. A korábbi évek informatikai beruházásainak nagy része ezeknek a személyi számítógépeknek amortizációs cseréjére irányult.

Második pontként a biztonsági osztályba sorolás vizsgálata során, a nagytávolságú informatikai hálózat részekre bontása után a helyi hálózatok kategorizálása, biztonsági osztály besorolás nem történt meg.

Harmadik pontként az intézkedések megléte során, fellelhető volt a NISZ mint KEKKH jogutódjának irattárában hálózat kábelezési rajzokat, melyek minősített iratok, így azokat a kutatás során nem lehetett felhasználni. Tehát intézkedések megfogalmazása nem volt fellelhető, így kockázat kezelési eljárásokat sem voltak.

Negyedik pontként az előírások alkalmazhatóság során kizárólagosan, a rendőrségi informatikai hálózatának információbiztonságát szavatoló előírást, utasítást információbiztonsági intézkedések az irattárban nem voltak fellelhetők. Csak általános érvényű utalásokat lehetett találni a rendőrség Ideiglenes Informatikai Biztonsági Szabályzatában, ezért azok alkalmazhatóságát nem lehetett vizsgálni.

Ötödik pontként az információbiztonsági fizikai megvalósíthatósága sok helyen (lokálisan) nem megoldott. A hálózatot a külvilágtól kívülről és az egyes szervezetek egymás között tűzfalakkal védik. A kábelezés fizikai védelme nem megoldott.

Az ORFK szakmai képviseletével továbbá a Nemzeti Elektronikus Információbiztonsági Hatósággal szakmai konzultációk kerültek lefolytatásra a rendőrségi helyi informatika hálózatainak biztonsági osztályba sorolásának tekintetében. Egyértelmű megállapítást nyert, hogy nem kerültek besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak. Ezen hiányosság egy olyan láncolatot vont maga után, mely során nem keletkeztek sem intézkedések, sem előírások így fizikai megvalósulásuk nem volt vizsgálható.

DOKUMENTUM KUTATÁS

A fent megnevezett témaköröket magába foglaló dokumentumok értelmezhető szinten utalásokat tartalmaztak a vizsgálatban érintett rendőrségi informatikai hálózatoknak információbiztonságával kapcsolatosan. Viszont az adminisztratív intézkedések hiánya fizikai intézkedések hiányához vezetett. Annak érdekében, hogy ezen hiányosságokat meg lehessen határozni, tovább kell a fent vizsgált dokumentumok tartalmát és alapjait meghatározó alapozó dokumentumok között kutatni.

Ezek alapján a tovább elemezve, szempontrendszerét meghatározva, elkülönítésre kerül egymástól a stratégiai szempontból fontos normatívák és a szakmai informatikai tárgyú dokumentációk. Ezek alapján a dokumentumok körében éles határ rajzolódik ki a rendőrségi informatikai hálózatok információbiztonsága fölötti szakirányítói szinten keletkezett dokumentumok, a vizsgált rendőrségi informatikai hálózatok információbiztonsági intézkedéseit meghatározó dokumentumok, azokat befolyásoló szakmai dokumentumok között.

A dokumentum kutatás első lépése olyan normatívákat felkutatása, amelyek a rendészeti informatika témakörben érinthetik a vizsgálat témáját. Az alábbi törvényeket és törvényerejű rendeletekben kerültek megvizsgálásra az információ védelem területi vonatkozásai és a hozzákapcsolódó adatvédelemi vonatkozásokat kutatva:

- 2009. évi CLV. tv a minősített adat védelméről,[1]
- 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,[2]
- 218/2011. a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól, [3]
- 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, [4]
- 92/2010. Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól, [5]
- 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, [6]
- Az adatvédelemmel, és az információ védelemmel kapcsolatos normatívák körében:
- 2010. évi CLVII. tv. a nemzeti adatvagyonról, [7]
- 38/2011. Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról, [8]
- 2011. évi CXCVI. tv. a nemzeti vagyonról, [9]
- 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról, [10]
- 2010. évi CLXXXV. tv. a médiaszolgáltatásokról és a tömegkommunikációról, [11]
- 2003. évi C. tv. az elektronikus hírközlésről [12]
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [13]
- 65/2013. (III.8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendeleteként [14]
- a 301/2013. (VII. 29.) Korm. rendelet „a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról” [15]
- 233/2013. (VI. 30.) Korm. rendelet „az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak,

valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről [16]
- 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról" [17]
- 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről [18]

A második lépcsőfok, az ágazati szintű informatikai védelmet meghatározó normatívák áttekintése. Ezek közül az alábbiak kerülnek kiemelésre:
- 1277/2010. Korm. határozat a kormányzati informatika konszolidációjához szükséges intézkedésekről, [19]
- 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról, [20]
- 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról, [21]
- 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról, [22]
- 8/2009. KHEM utasítás a Közlekedési Hírközlési és Energiaügyi Minisztérium Információbiztonsági Szabályzatáról. [23]

A fent megvizsgált dokumentációk ugyan érintik az informatikai hálózat információbiztonság tárgykörét, összefüggésbe hozhatóak a rendőrséggel, de egyértelműen egyik sem rendelkezik semmilyen meghatározással egyáltalán a rendőrségi informatikai hálózat információbiztonságának követelményrendszerire vonatkozó meghatározásokkal. Viszont mindegyik jól használható a fent feltárt hiányosságok pótlására.

Viszont más szemszögből tekintve a rendőrségi informatikai hálózatok információbiztonsági kérdésire, az elemzett dokumentumokban ha a rendőrséget a Belügyminisztérium ágazati szervezeteként beazonosítjuk, konkrét utalásokat találhatunk a hálózat biztonság területén. Például a 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiája dokumentum IV. Stratégiai fejlesztési irányok 1. Hálózatfejlesztési politika alfejezete élesen megfogalmazza „Törekedni kell a korszerű, virtuális technológiák alkalmazására, melyeket megfelelő adatfeldolgozó hálózat kiépítésével kell alátámasztani. Az informatikai szolgáltatásokat központosított és integrált rendszerekkel kell biztosítani." Mindemellett kitér a fizikai védelmi eszközrendszer létesítésére is „a szervezetek informatikai hálózatán határtűzfalakat kell létesítenie. Ki kell jelölnie a szervezete informatikai hálózatának határát, azon belül minden informatikai védelmet magának kell ellátnia. Olyan egyenszilárdságú hálózatvédelmi eszközöket és saját tulajdonú védelmi eljárásokat kell alkalmaznia, amelyek garantálják a szervezet informatikai hálózatán forgalmazott, tárolt adatok biztonságát."

A fizikai biztonságra nagy hangsúlyt fektetve kiemeli, hogy a „ BM-nek és ágazati szervének szervertermeit az ott tárolt adatok, rendszerek minősítési szintjének megfelelő biztonsági fokozatba kell sorolni és a vonatkozó szabályok szerinti fizikai védelmet kell biztosítani. A biztonsági rés csökkentése és az üzembiztonság növelése érdekében az amortizációs cserék segítségével el kell érni, hogy az informatikai eszközpark egyetlen eleme se legyen 6 évesnél idősebb." [24, 14.o.] Ezen intézkedések körének megjelenése nem volt tapasztalható az első vizsgálat során górcső alá vett dokumentumokban.

A 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiája dokumentum célzottan előírja a dokumentációs rendszer felállítását és kezelését, mely szerint „a BM és ágazati szervei informatikai hálózatának védelme érdekében az informatikai szakterületre kell koncentrálni az elektronikus adatok archiválását, szervezetenként központilag rendezett

címtárak létrehozatalát, kezelését, az informatikai rendszerekhez való hozzáférés nyilvántartás vezetését, az elektronikus és papír alapú másolás, továbbá nyomtatási folyamatok naplózását." [25, 15.o.]

Az elvonatkoztatás alapjait tekintve a helyi hálózatok tekintetében is találunk konkrét meghatározásokat: „a helyi hálózati infrastruktúra konszolidációja során közel 4000 db új UTP CAT5e hálózati végpont kerül létesítésre (a meglévő 5000 db felújítása mellett). A szerverparkok helyi hálózathoz csatlakozása gigabit Ethernet felületen kerül majd biztosításra, az aktív eszközök homogenizálásával és teljes körű cseréjével." [25, 15.o.]

A fenti eredmények tudatában - mely már jól hasznosítható a rendőrségi információbiztonsági dokumentációk továbbfejlesztésében -, át kell tekinteni, azokat a szakmai előírásokat, amelyek alapján a további kutatások lefolytatásra kerülhet és a korábban meghatározott pontokra pontos képet lehet alkotni. Sajnos a fent nevezett időkorlátban nem keletkezett további olyan szakmai irányt mutató anyag mellyel a vizsgálatot a hálózatok információbiztonsági területén lehetett volna folytatni. Ezért a fent említett dokumentumok szakmai forrásai kerülnek felkutatásra, annak érdekében, hogy javaslatot lehessen megfogalmazni az egyéb hiányosságok pótlására. Egyértelmű be lehetett azonosítani azokat nemzetközi és hazai szabványokat, melyeket a rendőrségi informatikai hálózatának biztonsági helyzeti vizsgálatára alkalmazni lehet. Ezek közül az alábbiak kerülnek felhasználásra:

- 2012. évi törvénytervezet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, [26]
- 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA), [27]
- 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK), [28]
- 25/1-3. kötet Az Informatikai Biztonság Irányításának Vizsgálata (IBIV), [29]
- 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR), [30]
- 25/2. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS). [31]

A nemzetközi szabványok közül:

- ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok, [32]
- ISO/IEC 27001:2005. [33]
- továbbá a ISO/IEC 27001:2013[34]

Az alkalmazhatóságuk szempontjából röviden összefoglalásra kerülnek a szabványok fontossága, amelyek a vizsgálat során figyelembe vételre kerültek:

A Miniszterelnöki Hivatal Elektronikuskormányzat-központ megrendelésére elkészült a Magyar Informatikai Biztonsági Ajánlások (MIBA) című ajánlássorozat. A MIBA fő célja, hogy biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő. A nemzetközi szabványokhoz és ajánlásokhoz igazodva a MIBA három fő részből áll:

A Magyar Informatikai Biztonsági Keretrendszer (MIBIK) [35] szervezeti szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBIK a biztonságos informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szól.

Részét képezi az Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX) [36], ami olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel.

A MIBIK az ISO/IEC 27001:2005, ISO/IEC 27002:2005 [37]és az ISO/IEC TR 13335 [38] nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR)1, amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelményei

(IBIK), amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányításának Vizsgálata (IBIV), amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

A Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS) [39] technológiai szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBÉTS célközönsége az informatikai rendszer kialakításáért, fejlesztéséért felelős vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését és tanúsítását végző szakemberek köre."[40, 5.o.]

Az informatikai biztonság kérdésével számos szabvány és ajánlás foglakozik. Gyakran hivatkoznak e területen az ITIL1-re [41] és a COBIT2-ra [42]. Az ITIL, „Az informatikaszolgáltatás módszertana" egy az informatika, mint szolgáltatás egészére kiterjedő, nemzetközileg széles körben elfogadott dokumentum. Az ITIL-ben a biztonságirányítás, bár önálló folyamat, amennyire csak lehetséges, integrálódik a többi folyamatba. Az ITIL Biztonságirányítás (Security Management) kötete a BS7799 [43] szabványt használja hivatkozásként, amikor a létező ITIL folyamatokat bővíti a biztonságirányítással. A COBIT az információrendszer ellenőrök egy nemzetközileg is ismert és elfogadott, az informatikai rendszerek szervezéséhez, és különösen az ellenőrzéséhez szükséges irányelveket tartalmazó dokumentum. A biztonság kérdésére nagy hangsúlyt fektet, de részleteiben nem foglalkozik a kérdéssel.

Az ISO/IEC 15408 szabvány (Common Criteria) [44] elsősorban technikai jellegű, főleg az informatikai termékek gyártóinak ad támogatást. Nagyon részletes és megbízható követelményeket, eljárásokat biztosít az informatikai eszközök biztonsági minősítésére. Nem tartalmaz ugyanakkor megfelelően, részletesen kidolgozott követelményeket, az informatikai rendszereket üzemeltető, felhasználó szervezetek számára.

Az informatikai biztonság területén egyre többen használják az ISO/IEC TR 13335 – Guidelines for the Management of Information Security (GMITS) [45] műszaki beszámoló. Az ISO/IEC TR 13335 nem szabvány, annak ellenére, hogy a Nemzetközi Szabványosítási Szervezet és a Nemzetközi Elektrotechnikai Bizottság szabványsorozatának részeként került kiadásra, de „Technical Report"-ként, ami ebben az esetben a megoldási lehetőségek, leírását jelenti, és ezt csak akkor vizsgálják felül, ha az abban foglaltak már nem érvényesek, vagy már nincsenek használatban. Az ISO/IEC TR 13335 öt részből áll:

1. Az informatikai biztonság koncepciója és modellje (Concepts and models for Information Security),
2. Az informatikai biztonság irányítása és tervezése (Managing and planning Information Security),
3. Az informatikai biztonság irányításának megoldásai (Techniques for the Management of Information Security),
4. A védelmi eljárások kiválasztása (Selection of Safeguards),
5. Hálózatbiztonsági megoldások (Safeguards for External Connections).

„Az ISO/IEC 27002:2013 szabvány nem csak azért kiemelt fontosságú, mert a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmazza, de a különböző nemzeti dokumentumok közül ez vált nemzetközi szabvánnyá, és emellett a „de facto" nemzetközi szabvánnyá vált ITIL is ezt használja hivatkozási alapként. Az ISO/IEC 27002 szabványt – bár kritikák is érik – a világ, és különösen az Európai Unió mind több országában fogadják el a különböző szervezetek informatikai rendszerük biztonságának alapjaként. Ezért a jelen követelményeknek ez a nemzetközi szabvány képezze az alapját, az ISO/IEC TR 13335

szabvány, továbbá a NATO (Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49) és az Európai Unió (Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK) releváns szabályozásai figyelembe vételével."[46., 32.o.]

A dokumentum elemzések a rendőrségi informatikai hálózatok információbiztonságának és védelmének tárgykörében a fenti struktúrában utalások sem közvetlenül sem közvetve nem voltak fellelhetőek.

ÖSSZEGZÉS

Az általam lefolytatott vizsgálat célja a rendőrségi informatikai hálózatai információbiztonsági hátterének feltárása volt.

Az elemzés alá vett informatikai hálózatok információbiztonsági hátterének kutatási eredményei alapján meg lehetett határozni azon rendőrségi informatikai hálózatok információbiztonsági helyzetét.

A dokumentumok vizsgálatával cél volt azon pontokat felkutatni, ahol ráutaló szakmai meghatározásokat találhatunk a rendőrségi informatikai hálózatok információbiztonsági helyzetére vonatkozóan. A kijelölt témaköröket magába foglaló dokumentumok értelmezhető szinten utalásokat tartalmaztak a vizsgálatban érintett rendőrségi informatikai hálózatoknak információbiztonságával kapcsolatosan.

Tekintettel a fentiekre, az elvégzett vizsgálat több irányú, területileg és időben eltolódó elemzéseket jelentett. Az analízisek a rendőrségi informatikai hálózatának nagyságára való tekintettel kerültek végrehajtásra. Elsődlegesen a jelen helyzet elemzése volt a kiindulópont. Ez az elemzés mind a releváns haza szakmai ajánlások, mind a nemzetközi ajánlások figyelembe vételével történt meg. Alapvető dokumentumként került felhasználásra a Rendőrségi Ideiglenes Informatikai Biztonsági Szabályzata, és az ISO/IEC 27001:2005 „A" melléklet 10.6 fejezete, a hálózat információbiztonsági követelmények elemzésekor.

A vizsgálat területe a mintavételezés eredményeképpen korlátozásra került a nagytávolságú és helyi hálózatok biztonsági osztályba sorolásának állapotában, helyzet felmérésében, a szükséges intézkedések meglétében, az érvényben lévő előírások alkalmazhatóságában, fizikai megvalósíthatóságában. Ennek okán a vizsgálat nem terjedt ki a minősített hálózatokra, a zártcélú és nyílt hálózatokra, továbbá a kritikus infrastruktúra elemekre. A kutatási pontok fogalmi szinten kerültek meghatározásra, úgy, mint helyzet felmérés, biztonsági osztályba sorolás vizsgálata, intézkedések megléte, előírások alkalmazhatósága, fizikai megvalósíthatósága.

19 olyan törvény és törvényerejű rendelet került vizsgálat és elemzés alá az információ védelem területi vonatkozásait és a hozzákapcsolódó adatvédelemi vonatkozásokat kutatva, amelyek során a rendőrségi informatikai hálózatának információbiztonsági hátterének kutatása folyt.

Miután ez nem vezetett eredményre így tovább folytatva további 5, az ágazati szintű informatikai védelmet meghatározó normatíva került áttekintésre. Ezek már érintették az informatikai hálózat információbiztonság tárgykörét, összefüggésbe voltak hozhatóak a rendőrséggel. Továbbá pontos meghatározásokat tartalmaztak a hálózat információbiztonsági szintjének emelésére, amely segítséget nyújthat a rendőrségi informatikai hálózat információbiztonságának követelményrendszerinek körvonalazásához. Így a kutatási kört szakmai forrásokra történő bővítésével, 8 nemzetközi és hazai szabványt került beazonosításra.

Az elméleti vizsgálódás mellet a vizsgálatban a gyakorlati megvalósulás is helyt kapott a rendőrségi nagytávolságú informatikai hálózata és kommunikációs hálózatának leírásai. A , helyzetvizsgálat keretében, egyértelmű megállapítást nyert, hogy nem került besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak.

A kutatás során áttekintésre került a rendőrségi lokális (helyi) informatikai hálózatainak leírásait, helyzetvizsgálat keretében, mely során egyértelmű megállapítást nyert, hogy nem került besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak.

Összegezve a fentieket az információbiztonság a stratégiai dokumentumokban előírt követelményekhez képest elmaradottnak tekinthető, mind az adminisztráció, mind az információvédelmi intézkedések területén. Kellő mélységű szabályozottság hiányában nem volt megállapítható a rendőrségi informatikai hálózatnak besorolási szintje. Nem volt fellelhető olyan dokumentáció, mely utalást tett volna a biztonsági besorolására, vagy annak információbiztonsági helyzetére, kockázat elemzésre, kockázat kezelésre, eljárásokra, intézkedésekre. Ez egy olyan sorozatos hiányosságot vont maga után, amely láncolatot épített fel az információbiztonsági előírások, intézkedések, eljárások és fizikai megvalósíthatóságuk nélkülözhetetlenségüknek a bizonyítására. Az egyes vizsgálati pontok által felfedezett hiányosságok ok-okozatot bizonyítottak a következő vizsgálati pontok közötti eredményekben. Viszont szakmai normatívákban egyértelmű utalások és meghatározások voltak beazonosíthatóak, és a rendőrségi informatikai hálózatok információbiztonsági szintjének fejlesztésére használhatóak, feldolgozhatóak. Ezen normatívák segítésével a dokumentációk olyan szintre fejleszthetőek melyek segítségével meghatározhatóak a a rendőrségi informatikai hálózatok a biztonsági osztályba sorolása. Mind emellett a besorolás körülményeinek bővítésével olyan intézkedések és eljárások kidolgozását helyezik kilátásába, melyek az információbiztonsági kockázatok csökkentését vonnák maguk után.

Konklúzió: a vizsgálat tárgyát képező rendszerek információbiztonsága, a biztonsági osztály általi besorolás eredményeképpen meghatározott intézkedések és eljárások láncolati felfűzésének összessége. Mely láncolat megszakadása egyértelmű ok okozatok eredményeit képezik le. Ezek az ok okozati összefüggések az informatikai információbiztonság fenyegetettségét vonják maguk után.

Felhasznált irodalom

[1] 2009. évi CLV. tv a minősített adat védelméről,

[2] 000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,

[3] 218/2011. a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól,

[4] 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól,

[5] 92/2010. Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól,

[6] 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről,

[7] 2010. évi CLVII. tv. a nemzeti adatvagyonról,

[8] 38/2011. Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról,

[9] 2011. évi CXCVI. tv. a nemzeti vagyonról,

[10] 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról,

[11] 2010. évi CLXXXV. tv. a médiaszolgáltatásokról és a tömegkommunikációról,

[12] 2003. évi C. tv. az elektronikus hírközlésről.

[13] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[14] 65/2013. (III.8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendeleteként

[15] a 301/2013. (VII. 29.) Korm. rendelet „a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról”

[16] 233/2013. (VI. 30.) Korm. rendelet „az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről

[17] 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról”

[18] 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

[19] 1277/2010. Korm. határozat a kormányzati informatika konszolidációjához szükséges intézkedésekről,

[20] 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról,

[21] 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról,

[22] 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról,

[23] 8/2009. KHEM utasítás a Közlekedési Hírközlési és Energiaügyi Minisztérium Információbiztonsági Szabályzatáról.

[24] 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról 14.o.

[25] 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról 15.o.

[26] 2012. évi törvénytervezet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,

[27] 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA),

[28] 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK),

[29] 25/1-3. kötet Az Informatikai Biztonság Irányításának Vizsgálata (IBIV),

[30] 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR),

[31] 25/2. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS).

[32] ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok,

[33] ISO/IEC 27001:2005. szabvány

[34] ISO/IEC 27001:2013. szabvány

[35] Magyar Informatikai Biztonsági Keretrendszer (MIBIK)

[36] Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)

[37] ISO/IEC 27002:2005. szabvány

[38] ISO/IEC TR 13335. szabvány

[39] Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)

[40] 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) pp. 5-7. 2008.

[41] Information Technology Infrastructure Library (ITIL)

[42] Control Objectives for Information and Related Technology (COBIT)

[43] BS7799

[44] ISO/IEC 15408 (Common Criteria)

[45] ISO/IEC TR 13335 – Guidelines for the Management of Information Security (GMITS)

[46] Dr. Ködmön István, Információbiztonság az ISO27001 tükrében, Hétpecsétes Történetek, Hétpecsét Információbiztonsági Egyesület, Budapest, 2008. pp.39.