Óbudai Egyetem

Doktori (PhD) értekezés

tézisfüzete

A Rendőrségi informatikai hálózat védelmének helyzete, a fejlesztés irányai, feladata

Fehér Judit

Témavezető:

Prof. Dr. Rajnai Zoltán egyetemi tanár

Biztonságtudományi Doktori Iskola

Budapest, 2018.

Tartalom

ABSTRACT 3

ABSZTRAKT 3

1. A KUTATÁS ELŐZMÉNYEI 4

2. CÉLKITŰZÉSEK 4

3. VIZSGÁLATI MÓDSZEREK 5

4. ÚJ TUDOMÁNYOS EREDMÉNYEK 5

5. AZ EREDMÉNYEK HASZNOSÍTÁSI LEHETŐSÉGE 7

6. IRODALOMJEGYZÉK 7

7. A TÉZISPONTOKHOZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEK 9

8. TOVÁBBI TUDOMÁNYOS KÖZLEMÉNYEK 10

ABSTRACT

Information networks and their services are already in the center of attention at the Police because law enforcement activities are based on online systems. Beyond its importance in police work, the quantity and contents of managed data also makes the implementation of the Police's Information Security Policy a priority on the agenda, as well as keeping it up-to-date or expanding it's scope. In spite of the internal policies in force, the ICT security of the Police still needs to be solved. Notwithstanding attention has already been drawn by numerous experts to the importance of the security of the Police information network services, its adoption and integration into the strategic goals of the Police has not yet finished. My research is dedicated to the current state of play of the protection of the Police's information network , the directions of development and the definition of the current and further tasks of the Police. I have invested long years into the deeper research of my chosen scientific topic, I have been working in my current job and position in the field of law enforcement ICT. Thus, I do not delve into the subject only in theory and I also try to put my research findings into practice. My goal is to complete the currently existing, and –insufficient, documents repository of internal policies with further policy documents and descriptions which could be used by future generations in their everyday practice, thus enhancing the security of electronic communication. I reckon the results of my research could be applied not only within the law enforcement department but they could also be interpreted into the field of further home affairs institutions' as well. After all, each organisation in this policy sector faces the same struggles regarding information security. My research does not cover information security incidents published in media.

ABSZTRAKT

A Rendőrségen az informatikai hálózatok és azok szolgáltatásai már a figyelem középpontjába kerültek, mert a szolgálat ellátás az on-line rendszerekre épülve történik. A rendészeti munkában betöltött fontosságán túl a kezelt adatok mennyisége és tartalma miatt is kiemelt napirendi pontot jelent a Rendőrség Informatikai Biztonsági Szabályzatának gyakorlatba történő átvezetése, naprakészen tartása, bővítése, de a Rendőrség informatikai biztonsága a szabályozások ellenére nem megoldott probléma. A Rendőrség informatikai hálózati szolgáltatások biztonságának fontosságára nagyon sok szakember már felhívta a figyelmet, de még mindig folyamatban van a Rendőrség stratégiai céljaiba való beépítése. Kutatásaimat a Rendőrségi informatikai hálózat védelmének helyzete, a fejlesztés irányai, feladatainak meghatározására szenteltem. A témaköröm mélyebb volumenű kutatását folytatom hosszú évek

óta, ennek javára dolgoztam és dolgozom jelenleg is a munkakörömben és végzem munkámat a rendészet informatikai szakterületén. Tehát nem csak elméleti síkon veszek részt a kutatásaim során, hanem a gyakorlatban is megpróbálom megvalósítani azokat. Célom az, hogy a jelenleg rendelkezésre álló hiányos dokumentum tárat szakmailag olyan szabályzókkal és leírásokkal töltsem meg, melyeket az utánunk következő generációk napi szinten a gyakorlatban tudnak majd alkalmazni munkájuk során, ezzel is biztonságossá téve az elektronikus kommunikációt. Azt gondolom, hogy kutatásom eredményeit nem csak a Rendőrség keretein belül lehet felhasználni, hanem a Belügyi ágazat más területein is lehet értelmezni, elvégre minden egyes ágazati szervezet ugyan azon gondokkal küzd az információbiztonság területén. A kutatásom nem a médiában megjelent információbiztonsági eseményeket dolgozza fel.

1. A KUTATÁS ELŐZMÉNYEI

Gyakorlati tapasztalataim és hosszú több éves megfigyeléseim, továbbá információgyűjtésemre támaszkodva megállapítom, hogy a kezdetleges szabályozások az informatikai hálózat biztonságát egy minimálisan teljesíthető követelményekkel ellátott szinthez igazítják a Rendőrségi informatikai hálózatok tekintetében. Az eddig szervezetenként, területenként eltérő szabályzások más és más biztonsági sávot húztak meg a hálózat biztonság területén. A központi szabályzás megpróbálja kiküszöbölni a nagy különbséget. De a központi szabályok visszabontása során nehéz feladat a következetesség biztosítása. A szabályzások csak megadják a védelem fejlesztésének alapját, viszont nem elegendőek. Nem megfelelően harmonizáltak a politikai elvek, az irányelvek, a filozófia, a stratégia, a követelményrendszerek az információvédelem területén, így a hálózatvédelem területén is. Megítélésem szerint ezeknek a hiányosságoknak a felfedésével szükség van a teljes informatikai védelem fejlesztésére. Értekezésem e témakörrel kapcsolatban, elsősorban a Rendőrségi informatikai hálózat védelmével szorosan összefüggő kérdéseket foglalja össze.

2. CÉLKITŰZÉSEK

A kutatás

A Rendőrségi informatikai hálózat védelme középtávú fejlesztési irányainak elemzésekre épített meghatározása.

A kutatás részcéljai

- A magyar Rendőrségi informatikai hálózata védelmével szemben támasztott követelmények meghatározása, rendszerezése.
- A magyar Rendőrségi informatikai hálózat védelme során alkalmazható eszközök és módszerek elemzése.
- A magyar Rendőrségi informatikai hálózat védelme fejlesztési irányainak és feladatainak meghatározása.

3. VIZSGÁLATI MÓDSZEREK

1. Kutató munkám kezdetén alapinformációk gyűjtését végeztem a Rendőrség informatikai hálózatáról. Ezeket az adatokat rendszereztem.
2. Az adatok elemzése során különböző információ halmazokat határolok el egymástól.
3. Behatárolom a kutatás témakörét, és a szükséges adatok feldolgozhatóságának törvény adta lehetőségeit.
4. Megfigyeléseket végzek a napi munkám során, mely lehetőséget adott a téma aktualitásának fenntartására.
5. Mindemellett felhasználom a kritikai adaptációt, más tanulmányok másodelemzésével összefüggéseket keresek, analízis, szintézis, indukció és dedukció módszereivel törekszem a részcélokon keresztül a kutatás célkitűzéseinek eleget tenni.
6. Kutatásaimat az Országos Rendőr-főkapitányság szakértőinek együttműködésében, a Belügyminisztérium által meghirdetett, gyakornoki rendszer keretében 2018.02.28. zártam le.

4. ÚJ TUDOMÁNYOS EREDMÉNYEK

1. Hipotéziseim első pontjában megfogalmazott álláspontomnak megfelelően definíció szerűen meghatároztam a Rendőrségi informatikai hálózat fogalmat, mely a következő formában határozható meg: *szűkebb értelemben a Rendőrség, tágabb értelemben emellett egyes rendőri feladatokat ellátó szervek felügyelete, irányítása alatt álló, információs szolgáltatásokat nyújtó technikai hálózatok összessége*. Bebizonyítottam, hogy a Rendőrségi informatikai hálózat olyan hálózat, amelynek rendeltetése a

Rendőrségi feladatok során felmerülő információs tevékenységek támogatása, megvalósítása, elemei technikai eszközök (rendszerek) és az elemek között információcserét biztosító valós fizikai, vagy absztrakt – más hálózatok szolgáltatásaira épülő – logikai kapcsolatok.

2. A hipotézisem második pontját tényadatokkal alátámasztva igazoltam, hogy a Rendőrség informatikai hálózatának védelmével szemben támasztott követelmény egyik alapvető eleme az, hogy a Rendőrség informatikai biztonság politikának alapvetően meg kellene határoznia az informatikai rendszerekben előállított, tárolt, használt és továbbított információk elégséges biztonságának megteremtéséhez szükséges intézkedéseket. Így a követelmények között meghatároztam, hogy a Rendőrség informatikai biztonság filozófiájának egy olyan jövőkép kell, hogy legyen, amely a rendszerekkel kapcsolatban lépő társadalmi környezetnek is szól. Be kell, hogy mutassa azokat az értékeket, amelyeket a Rendőrség követ, és elvár a munkatársaitól az informatikai rendszer kialakítása, üzemeltetése és fejlesztése során. Példákon keresztül igazoltam, hogy a Rendőrségi informatikai hálózatok védelemének biztosítania kell az informatikai rendszer megbízható üzemét fenyegető káresemények elhárítását, illetve hatásuk minimalizálását a megadott biztonsági követelmények szintjén. Olyan védelmi eljárásokat kell alkalmazni, amelyek garantálják, hogy az államigazgatás még akkor is hatékonyan működjön, ha akár egy szervezetét (tárca, intézmény, az országos hatáskörű szerv) is katasztrófa ér.

3. A hipotézisem harmadik pontját úgy bizonyítottam be, hogy az Ibtv.-ben meghatározott eljárást felhasználva új, - eddig sem jogszabályban vagy Rendőrségi normatívában nem rögzített – rendszerzési elvek szerint rendszereztem és csoportosítottam a Rendőrség elektronikus információs rendszereit. Továbbá meghatároztam a védelmi módszertani eljárást, mely szerint a Rendőrségi elektronikus információs rendszerek védelmi intézkedéseit ki lehet választani, meg lehet jelölni, melyet követően eszközrendszert állítottam fel a sérülékenységi mátrix meghatározásával a védendő faktorokra. Az eljárásokat összekötve az alkalmazott eszközökkel teljes értékű helyzetképet kaptam a Rendőrség informatikai hálózatának biztonság állapotáról, melyet egy sérülékenységi mátrixal prezentáltam.

4. A hipotézisem negyedik pontjában megfogalmazott feltevéseket igazolva

meghatároztam a fejlesztési pontokat, összegeztem azokat a végrehajtandó feladatcsoportokat mind a fizikai, mind az adminisztratív, mind a logikai területen melyek egyértelműen meghatározzák a Rendőrség informatikai hálózatának jövőképét, javaslatokat tettem a fejlesztési eljárásokra, a törvénynek való megfeleltetés ütemezésére. Egy olyan jövőképet alkottam mely szinte pénzmentesen átültethető a gyakorlatba a Rendőrség informatikai hálózatának védelmére.

5. AZ EREDMÉNYEK HASZNOSÍTÁSI LEHETŐSÉGE

1. Javaslom, hogy a Rendőrség az általam kidolgozott definíciókat alkalmazza, és a fogalmakkal alakítson ki újabb szakterületi szabályozókat, ezzel csökkenthetik a beruházások anyagi terheit a szervezetnél.
2. Javaslom, hogy a követelményrendszerek meglétét vizsgálja meg a Rendőrség minden egyes elektronikus információs rendszerével kapcsolatosan és tegyen intézkedéseket azok pótlására.
3. Javaslom, hogy az általam megjelölt fejlesztési pontokat részletesen dolgozzák, ki a felsorolt eszközökkel és módszerekkel.
4. Javaslom, hogy az értekezésem eredményeit, a fejlesztési pontokat, a fejleszti utak tervezésénél használják fel.
5. Javaslom, hogy általam megjelenített intézkedéseket és feladat köröket fontolják meg, mert ezek segítségével a teljes védelem a hálózat teljes spektrumán biztosítható.

6. IRODALOMJEGYZÉK

[1] Prof. Dr. Munk Sándor DSc - Horvayné Fehér Judit: A Rendőrségi informatikai hálózat fogalma, rendeltetése, Hadmérnök, Budapest,2011., VI. évfolyam, II. szám, pp. 217, 218, 219, 220, 221, 222, 223, 224, 225, 226

[2] HENK Tamás-NÉMETH Krisztián: *Távközlő hálózatok. Jegyzet.* – BME Távközlési és Médiainformatikai Tanszék, 2005. pp 3., 17.

[3] MUNK Sándor: *Katonai informatika III. A katonai informatika eszközrendszere.* Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003. pp 17.

[4] MUNK Sándor: *Katonai informatika II. Katonai informatikai rendszerek, alkalmazások.* Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006. pp 21.,

28.

[5] MUNK Sándor: *Katonai informatika I. A katonai informatika alapjai.* Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003. pp.60.

[6] PÁNDI Erik: *A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai- és közigazgatási kommunikációs rendszerek megszervezésére és irányítására. Doktori (PhD) értekezés.* – ZMNE, Budapest, 2005. pp.27., 54., 90., 94.

[7] *17/2009 (OT 10.) ORFK utasítás a Rendőrség Kutyás és Lovas Szolgálati Szabályzatáról*. 443-as pont

[8] *53/2010 (OT 31.) ORFK utasítás a Rendőrség ügyeleti szolgálata és a közreműködésével teljesítendő jelentési és tájékoztatási kötelezettség rendjéről. pp. 35. 106-os pont*

[9] 12/2009 (OT 7.) ORFK utasítás a Kriminalisztikai Archiváló Rendszer üzembeállításával és működtetésével kapcsolatos egyes feladatokról. pp. 15.

[10] *5/2009 (OT 3.) ORFK utasítása Rendőrség szervei hivatásos, köztisztviselői, közalkalmazotti állománya és a nyugállományba vonulók igazolványának, valamint a hivatásos állomány szolgálati azonosító jelvényének és hímzett azonosítójának kiadásáról és nyilvántartásának rendjéről*. pp. 10.

[11] *4/2008 (OT 4.) ORFK utasítás az Országos Rendőr-főkapitányság Szervezeti és Működési Szabályzatáról. pp. 20.*

[12] *23/2007 (OT 16.) ORFK utasítás az Országos Rendőr-főkapitányság telekommunikációs eszközökkel történő ellátásának rendjéről, valamint a távközlési szolgáltatások igénybevételének szabályairól. pp. 4., 12.*

[13] *ORFK Gazdasági Főigazgatóság, Informatikai Főosztály, Kommunikációs és Adatátviteli Osztály információi.*
[www.police.hu/content/organization?contentid=1996664, 2011.05.19.]

[14] *2009 (OT 15.) az Országos Rendőr-főkapitányság és a Magyar Barlangi Mentőszolgálat között kötött együttműködési megállapodás*. 2. e pont

[15] 45/2013. (XI. 15.) ORFK utasítás az intranethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer Rendőrségi igénybevételének szabályairól, pp.2.

[16] 21/2011. (VIII. 11.) BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról

60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról, Országos Rendőr-főkapitányságí Tájékoztató 32. száma, (5-1/60/2008. TÜK iktatószám), 2008. pp 2-63

[17] ITB 12-es 2. A BIZTONSÁGPOLITIKA MEGHATÁROZÁSA Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, Budapest, 1996. pp. 22.

[18] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, Magyar Közlöny 2013. évi 69. szám, pp. 50241., 50242., 50243., 50244., 50252.

[19] 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) pp. 5-7. 2008.

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

[21] Széll Kálmán terv pp 1-7

[22]Fehér Judit: A Rendőrségi elektronikus információs rendszerek (hálózatok) védelmére alkalmazható módszerek az „Információbiztonsági törvény" szemszögéből., A HADTUDOMÁNY ÉS A 21. SZÁZAD, Budapest, 2014. pp. 221-242.

[23] „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről" szóló 41/2015. (VII.15.) BM rendelet, Magyar Közlöny

[24] „a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól" szóló 185/2015. (VII. 13.) Korm. rendelet, Magyar Közlöny

[25] „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról" szóló 36/2013. (VII. 17.) BM rendelet, Magyar Közlöny 2013. évi 123. szám 7. §. (3), 64539.o.

[26] Muha Lajos: Fogalmak és definíciók, 2004 [In.: Az informatikai biztonság kézikönyve (szerk.: Muha Lajos), Budapest: Verlag Dashöfer Szakkiadó, ISBN 963 9313 12 2]

7. A TÉZISPONTOKHOZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEK

1. Horvayné Fehér Judit: Az informatikai biztonság szabályozásának kérdése a Magyar Rendőrségnél, Kommunikáció Konferencia, Budapest, 2010. ISBN 978-963-7060-21-2, pp.109-118

2. Prof. Dr. Munk Sándor DSc - Horvayné Fehér Judit: A rendőrségi informatikai hálózat fogalma, rendeltetése, Hadmérnök, Budapest,2011., VI. évfolyam, II. szám, pp. 217-226

3. Horvayné Fehér Judit: Elektronikus ügyiratok továbbításának megoldásai a Rendőrségnél, Hírvillám, Budapest, 2012. II. évfolyam 1. szám HU ISSN 2061-9499, pp 47-62.

4. Horvayné Fehér Judit: A Rendőrség informatikai biztonsági stratégiája alapjainak meghatározása, Hadmérnök, Budapest, 2011., VI. évfolyam IV. szám pp. 282-292.

5. Horvayné Fehér Judit: A Rendőrségi informatikai hálózatok fenyegetései, Hadmérnök, Budapest, 2012. VII évfolyam II. szám pp.260-275.

6. Fehér Judit: A Rendőrségi elektronikus információs rendszerek (hálózatok) védelmére alkalmazható módszerek az „Információbiztonsági törvény" szemszögéből., A HADTUDOMÁNY ÉS A 21. SZÁZAD, Budapest, 2014. pp. 221-242.

7. Fehér Judit: A Rendőrségi informatikai hálózatok információbiztonsági hátterének meghatározása, Hadmérnök, Budapest, 2016. XI. Évfolyam 2. szám - 2016. június pp.1-12.

8. Fehér Judit: A Rendőrség informatikai hálózat védelmének irányai és feladata, Belügyi szemle, Budapest, 2016. 64. évfolyam 6. szám pp. 120-126.

9. Fehér Judit: A Rendőrség informatikai hálózat információbiztonsági fejlesztési irányai - Areas for police information network information security development, Magyar rendészet, Budapest, 2016., XVI. évfolyam 3. szám pp.155-172.

8. TOVÁBBI TUDOMÁNYOS KÖZLEMÉNYEK

1. Fehér Judit: Elektronikus Bűnözés. Hazai és Külföldi tapasztalatok, Kommunikáció, Budapest, 2003., ISBN 9638622962, pp. 57-64

2. Fehér Judit: Integrált hálózatbiztonság a szolgáltatónál. Kommunikáció, Budapest, 2004., ISBN 963964415X, pp. 85-95.

3. Fehér Judit: Az állami és önkormányzati szervek incidens kezelése - Incident management of central and local goverment agencies, Military National Security Service kiadó National Security Review, BUDAPEST 2/2016, HU ISSN 2416-3732 pp.78-92.