Óbudai Egyetem

Doktori (PhD) értekezés

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

Fehér Judit

Témavezető:

Prof. Dr. Rajnai Zoltán egyetemi tanár

Biztonságtudományi Doktori Iskola

Budapest, 2018.

Komplex Vizsga Bizottság:

Elnök:

Prof. Dr. Berek Lajos, ÓE

Tagok:

Dr. Muha Lajos, külső

Dr. habil. Farkas Tibor, külső - NKE

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Berek Lajos, ÓE

Titkár:

Dr. Szűcs Endre, ÓE

Tagok:

Dr. Bérczi László, külső

Dr. Pándi Balázs, külső

Dr. Tick Andrea, külső - BGE

Bírálók:

Dr. Bozsó Zoltán, külső

Dr. Tóth András, külső - NKE

Nyilvános védés időpontja

……..

TARTALOM JEGYZÉK

BEVEZETŐ

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. 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.

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

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.

AZ ÉRTEKEZÉS TÁRGYA ÉS CÉLJA

Az értekezés tárgya

A Rendőrségi informatikai hálózat védelmének vizsgálata helyzetelemzése és jövőkép alkotásra.

Az értekezés célja

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.

A kutatás területei

I. Rendőrségi informatikai hálózatok és védelmük alapjai

A fejezet célja az informatikai hálózatok alapjainak összegzése, Rendőrségi informatikai hálózatok és sajátosságaik bemutatása, elemzése. A magyar Rendőrség informatikai hálózatának leírásán, és jellemzésén keresztül rámutatok az informatikai hálózatok biztonságának fontosságára, összegzem védelmének alapjait. Értékelem a magyar Rendőrség informatikai hálózatának biztonsági helyzetét.

II. A Rendőrség informatikai hálózatának védelmével szemben támasztott követelmények

A hálózat vizsgálatának segítségével a biztonsági követelményeket meghatározó tényezőket, és a körülményeket összegzem, rendszerezem. A Rendőrség informatikai hálózatának biztonságát veszélyeztető fenyegetések feltárásával és elemzésével kifejtem a biztonsági követelményekhez kapcsolódó kérdéseket. A kérdéseket ki kívánom fejteni a követelmények elemzésével a magyarországi dokumentumokban. Témához szorosan kapcsolódik, és

alapvetően meg is határozza a Rendőrség informatikai biztonsági filozófiája és politikája kereteinek megfogalmazása. Ezen alapelvek meghatározását követően körvonalazódnak ki a Rendőrség informatikai biztonsági célkitűzései. A fejezet célja a Rendőrség informatikai hálózatának védelmével szemben támasztott követelmények meghatározása.

III. A Rendőrség informatikai hálózatának védelme során alkalmazható eszközök és módszerek

A fejezetben célom a hálózatok védelme során alkalmazható módszereket, eszközöket, eljárásokat rendszerezni és elemezni. A fejezetben feltárom a Rendőrség informatikai hálózatában jelenleg alkalmazott védelmi módszereket, eszközöket. Bemutatom és értékelem az eljárásokat. A bemutatást követően meghatározom az eszközöknek és módszereknek a Rendőrségi informatikai hálózat védelme során történő alkalmazásának kritériumait, azok előnyeit és hátrányait. Ebben a fejezetben fontosnak tartom a Rendőrség informatikai hálózata védelme során alkalmazható eszközök és módszerek körének kialakítását és osztályozását.

IV. A Rendőrség informatikai hálózat védelmének fejlesztési irányai és feladatai

A fejezet célja a Rendőrség informatikai biztonsági stratégiája alapjainak meghatározása. A Rendőrségi informatikai hálózat védelme fejlesztési irányainak, területeinek feltárásával, az egyes fejlesztési területek célkitűzéseit és megvalósításuk feladatait körvonalazom.

Befejezés

Összegzés, következtetések, tudományos eredmények összefoglalása, javaslatok a fejlesztés irányaira.

TÉMAVÁLASZTÁS, HIPOTÉZISEK ÉS MÓDSZEREK

Témaválasztás

Napjaink informatikája már a hálózati megoldások informatikája, amely a különböző informatikai eszközök, rendszerek, alkalmazások összekapcsolódására, egymás szolgáltatásainak igénybevételére, egymás képességeit kölcsönösen erősítő együttműködésére épül. Hálózati lehetőségek nélkül az informatikai szolgáltatások jelentős része egyáltalán nem, vagy csak korlátozottan, szűkített funkciókészlettel működőképes. Hálózati megoldásokra épülnek a Rendőrség informatikai megoldásai is.

Hipotézisek

1. A Rendőrségnél alkalmazott informatikai hálózatok alapjainak összegzésével, továbbá fogalmi elemeinek meghatározása útján értelmezni lehet az informatikai hálózatok rendeltetését. és azok elemzésével meghatározható a Rendőrségi informatikai hálózat fogalma szűkebb és tágabb értelemben.
2. A Rendőrségi informatikai hálózat kockázat elemzésével rendszerezhető a biztonsági követelményeket meghatározó tényezők, amelyekből kikövetkeztethetőek a Rendőrség informatikai hálózatának védelmével szemben támasztható követelmények köre.
3. A Rendőrség által alkalmazott védelmi módszereinek, eszközeinek és eljárásainak vizsgálatával bizonyíthatóan megállapítható a Rendőrség informatikai hálózatának biztonsági helyzete.
4. A gyakorlatba is átültethető jövőképet alkotok a Rendőrség informatikai hálózatával kapcsolatban.

Kutatási 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.

Alaki és formai megjelenés

A szakirodalomból felhasznált részeket értekezésem törzsszövegében, az előfordulásuk sorrendjében [szögletes zárójelben] lévő számmal láttam el, valamint a „Sorszámozott hivatkozások” cím alatt rendszereztem. Sorszámozott lábjegyzetben fejtettem ki a megjegyzéseket. A feldolgozott, de nem hivatkozott irodalmat a „Feldolgozott Irodalom” cím alatt soroltam fel. Előfordulásuk sorrendjében jelenítettem meg az „Ábra jegyzékben” forrás

megjelölésével az ábrákat. Az értekezés végén külön jegyzékben kerültek kifejtésre az értekezésben használt rövidítések. A 2-es számú mellékletben került elhelyezésre a sérülékenységi mátrix.

I. RENDŐRSÉGI INFORMATIKAI HÁLÓZATOK ÉS VÉDELMÜK ALAPJAI

A fejezet elsődleges célja az informatikai hálózatok alapjainak összegzése, fogalmi elemeinek meghatározása. A fejezet másodlagos célja a Rendőrségi informatikai hálózatok rendeltetésének értelmezése, sajátosságainak bemutatása, felépítésének és szolgáltatási szempontú elemzésének lefolytatása.

BEVEZETÉS

A mai korszerű informatika szolgáltatásait már egyetlen alkalmazási terület sem nélkülözheti. Ez ugyanúgy jelenik meg a rendőri területen is, az eredményes és hatékony bűnügyi, közrendvédelmi, határrendészeti, közlekedés- és igazgatásrendészeti tevékenység egyre növekvő jelentőségű feltételrendszerét képezik az informatika által nyújtott szolgáltatások. Az Informatikai eszközök, továbbá rendszerek, és alkalmazások támogatják többek között a szervezeten belüli általános információáramlást. Így többek között a Rendőrség által is használt nyilvántartások kezelését, valamint az egyes szaktevékenységeket (bűnügyi vizsgálatok, okmányellenőrzés, közterület-megfigyelés, határellenőrzés, stb.).

Napjainkban az informatika már a hálózati megoldások informatikája, amely a különböző informatikai eszközök, rendszerek, alkalmazások összekapcsolódására, egymás szolgáltatásainak igénybevételére, egymás képességeit kölcsönösen erősítő együttműködésére épül. Az informatikai szolgáltatások, jelentős része hálózati lehetőségek nélkül csak korlátozottan, szűkített funkciókészlettel működőképes. A Rendőrség tekintetében hálózati megoldásokra épül többek között a Rendőrség univerzális feladatkörű Robotzsaru rendszere, a HERMON körözési információs rendszer, a HIDRA idegenrendészeti alkalmazás, az AFIS ujj- és tenyérlenyomat azonosító rendszer, a NEKOR okmány-minta nyilvántartó rendszer, vagy a HERR határellenőrzési rendszer és a SIS schengeni információs rendszer. Ezen rendszerek ismeretében vizsgálom jelen fejezetben a hálózati megoldásokat.

Általánosságban elmondható, hogy az informatikai hálózatok által nyújtott előnyök hátrányokkal, vagyis megbízhatósági és adatkezelési kockázatokkal is párosulnak. A hálózatok lényegi sajátosságai hogy az önálló (sok esetben külső) szolgáltatásként megjelenő globális és nagy kiterjedésű hálózatok kialakulásával az informatikai rendszerekhez történő hozzáférés könnyebbé válása jelentős és újszerű sebezhetőségeket eredményez, biztonsági kockázatokat hordoz magában. A hálózati biztonság az informatikai biztonság lényeges összetevőjévé, önálló szakterületévé vált, ami jelen esetünkben fokozottan érvényes a rendőri

alkalmazásra is.

A szakirodalom és a szakmai dokumentumok tanulmányozása során, egyértelmű megállapítást nyert, hogy az informatikai eszközöket, rendszereket összekapcsoló hálózatok fogalmi alapjaival kapcsolatban a szakmai körökben sem alakult ki egyetértés, egységesen elfogadott értelmezés. A szakirodalom vizsgálata során felfedezhetünk olyan kifejezéseket, mint az informatikai hálózatok, számítógép-hálózatok, távközlési hálózatok, kommunikációs hálózatok, infokommunikációs hálózatok, a legtöbb esetben a tartalmat leíró meghatározások nélkül. Ez akadályát képezi az eredményes tudományos-szakmai tevékenységnek; a kutatók, szakemberek együttműködésének.

A fentiek alapján jelen fejezet célja, hogy egységes hálózati fogalmi alap kerüljön kialakításra, meghatározásra kerüljön a Rendőrségi informatikai hálózat biztonsági kérdéseinek vizsgálati elemei. Ennek érdekében:

- összegzésre kerülnek az informatikai hálózatok alapvető fogalmai;
- bemutatásra kerül a kapcsolódó hálózat fogalmai, továbbá olyan kifejezések a Rendőrségi szakmai dokumentumokban, melyek alapot adhatnak a Rendőrségi informatikai hálózat javasolt fogalmának, továbbá rendeltetésének meghatározására

A fejezet megalkotásához Dr. Munk Sándorral közösen folytattunk kutatásokat a fogalmi alapok meghatározására.

1.1. A RENDŐRSÉGI INFORMATIKAI HÁLÓZAT FOGALMA, RENDELTETÉSE

1.1.1. INFORMATIKAI HÁLÓZATOK FOGALMI ALAPJAI

Jelen fejezetben az informatikai hálózat fogalom értelmezése és tartalmának vizsgálat kerül lefolytatásra. Kiindulásképpen alaptételként kerül definiálásra az elfogadható általános megállapítás, hogy „az informatikai hálózat olyan technikai (valós, működő) hálózat, amelynek rendeltetése információs szolgáltatások nyújtása, információs tevékenységek támogatása, megvalósítása, és amelynek elemei technikai eszközök (rendszerek), az elemek között pedig információcserét biztosító valós fizikai, vagy absztrakt logikai kapcsolatok állnak fent.”[1]

A fenti általános leíráson túl az informatikai hálózat fogalom tartalmát a különböző megközelítések, értelmezések közötti különbségek elemzésével azt keressük, hogy van-e és milyen szűkítés lehetséges a hálózat rendeltetésében (vagyis hogy a hálózat milyen szolgáltatásokat nyújt, milyen tevékenységeket támogat), illetve a hálózatot alkotó

eszközökre, vagy az információcsere során alkalmazott megoldásokra vonatkozóan. A szűkítések elemzése során az alábbiak kerültek megállapításra:

1.„Az ***információs szolgáltatásokat nyújtó technikai hálózatok*** témaköréhez kapcsolódóan számos különböző általános tartalmú kifejezéssel találkozhatunk, amelyek között kiemelt szerepet töltenek be a következők: távközlési hálózatok, műsorszóró hálózatok[1] és számítógép-hálózatok. Ezek közül a gyakorlatban elsőként az információtovábbítást támogató távközlési, illetve műsorszóró hálózatok jelentek meg, a későbbiekben alakultak ki az információcsere mellett a feldolgozási és tároló-képességek megosztását, összekapcsolását támogató számítógép-hálózatok is, napjainkban pedig már a különböző információs szolgáltatásokat nyújtó hálózatok integrálódásának korszakát éljük. A fenti fogalmakhoz a különböző szakmai dokumentumokban különböző meghatározások tartoznak."[1]

2. „A ***távközlési*** (távközlő, kommunikációs, híradó) ***hálózatok***[2] különböző meghatározásainak alapvető összetevője, hogy alaprendeltetésük információk eltérő helyek közötti átvitele. A továbbított információk formája (beszéd, hang, írott szöveg, álló és mozgókép, adat, technológiai folyamatok vezérlő jelei, stb.) alapján különböztethetőek meg a hálózatok által nyújtott távközlési szolgáltatások."[1]

Ha a történelmi utat vizsgáljuk, akkor kezdetben az egyes távíró, vagy távbeszélő távközlési hálózatok egy fajta konkrét szolgáltatást tudtak nyújtani, a végberendezések és az ezeket hálózatba kapcsoló vonalak, kapcsolóelemek szorosan egymáshoz tartoztak, melyeken keresztül adták a szolgáltatásokat. A későbbiekben olyan géptávíró/telex, fax hálózatokhoz már nem tartozott önálló technikai hálózati megoldás, az információk továbbítását megfelelő átalakítások után más elsősorban a távbeszélő hálózatok biztosították. A modemes átalakítás segítségével a hagyományos távközlési, azaz távbeszélő hálózatok egy meghatározott átviteli sebességig adatátviteli szolgáltatást nyújtottak. Később megjelentek a tervezetten több integrált szolgáltatást nyújtó ISDN távközlési hálózatok, melyeknél szétváltak a végfelhasználói (előfizetői) és a hálózati (hordozó) szolgáltatások.

3. „A ***számítógép-hálózatok***[3] alaprendeltetése nem elsősorban az információtovábbítás, információcsere, ez valójában csak egy szükséges feltétel az azonos, vagy hasonló információs képességeket, szolgáltatásokat nyújtó eszközök összekapcsolásához, az

1 Ezek részletesebb vizsgálatáról jelen publikáció célkitűzései figyelembevételével eltekintünk.
2 Telecommunication[s] network.
3 Computer network.

összetevők képességeinek egyszerű összegzését meghaladó, magasabb szintű, vagy akár új képességek kialakításához: különböző információs (rész)képességekkel rendelkező eszközökből meghatározott információs szolgáltatásokat nyújtó, egységes egészként működő – elosztott architektúrájú – eszközrendszerek felépítéséhez."[1]

A számítógép-hálózatok* alaprendeltetése az azonos, vagy hasonló információs képességeket, szolgáltatásokat nyújtó eszközök összekapcsolása, következménye pedig, hogy az összetevők képességeinek egyszerű összegzését meghaladó, magasabb szintű, vagy akár új képességek hozhatóak létre. Az adathálózatok az információ továbbítás és az információcsere segítségével a különböző (rész)képességekkel rendelkező eszközökből meghatározott szolgáltatásokat nyújtó, egységes egészként működő – elosztott architektúrájú – eszközrendszerek építhetőek fel.

A számítógép-hálózatok számítógépeket kapcsolnak össze, amely ma már nem ilyen egyértelmű. Egyes meghatározások számítógépeket vagy autonóm számítógépeket vesznek alapul, mások számítógépeket és más eszközöket jelenítenek meg, végül a harmadik csoport definícióiban adatfeldolgozó rendszerek, eszközök összességében szerepelnek. Ha ezeket összevetjük egymással, akkor álláspontom szerint a hálózat csomópontjai lehetnek bármilyen, adatfeldolgozási képességgel rendelkező eszközök.

A számítógép fogalmának tartalma alatt sokan a mindenki által használt általános célú számítógépeket értenek, holott a fogalom meghatározásai (amelyek lényege: automatizált adatfeldolgozó eszköz) kiterjed célszámítógépekre is. Az információs tevékenységeket támogató, integrált funkciójú technikai eszközök, mint az okostelefonok, GPS-készülékek, médialejátszók, stb. megnevezésére az informatikai eszköz kifejezés a legtalálóbb. Mind emellett megjegyzem, hogy egyre inkább terjedőben van az Internet Of Things vagyis minden eszköz hálózatba kötés fogalmának a használata.

„A híradástechnikai, távközlési, illetve a számítástechnikai, szűkebb értelemben vett informatikai ***szakterületek, megoldások, eszközök konvergenciája, integrációja*** egyre kevésbé teszi lehetővé a távközlési és a számítógép-hálózatok megkülönböztetését. Bár ez a megkülönböztetés a két szakterületen még létezik (az előbbi a számítógép-hálózatokat egy speciális típusnak, távközlő adathálózatnak tekinti, az utóbbi pedig a távközlési hálózatokat a számítógép-hálózatok fizikai összeköttetést megvalósító részeként kezeli), de alapjául már csak az egyes hálózatok eredete, kialakulása szerepel és egyes típusok esetében meg is fogalmazódik, hogy a besorolás szubjektív. A két hálózat-típus összefoglaló fogalmára, illetve az integrálódott hálózat-típus megnevezésére a BME távközlő hálózatok tantárgya az

információközlő hálózatok, illetve infokommunikációs hálózatok kifejezéseket használja.” [2] Ezek a kifejezések az informatikai szakterületen kevésbé használatosak. Ezért tágítani és egyben szűkíteni is kell az informatikai hálózatok fogalmi rendszerét.

4. „Az ***informatikai hálózatok*** fogalma szűkebb és tágabb tartalmakkal is értelmezhető. Ezek között a legszűkebb értelmezés: általános célú számítógépek, illetve számítógép-hálózati kapcsolóelemek[4] és a köztük fennálló valós, vagy absztrakt (fizikailag távközlési hálózatok által megvalósított) összeköttetések összessége. Eszerint az értelmezés szerint a hálózaton keresztül történő szolgáltatások közé csak az operációs rendszerek által biztosított képességmegosztó és információcsere szolgáltatások tartoznak. Mindezek csak alapot képeznek a felhasználók számára összetettebb, speciális szolgáltatások megvalósítására (hasonlóképpen ahhoz, ahogy egy számítógép és operációs rendszere csak egy platform az érdemi felhasználói szolgáltatásokat nyújtó alkalmazások számára)”.[1]

„Tágabb értelmezés szerint az informatikai hálózat részét képezik a számítógépeken futó alkalmazások is, amelyek így már speciális (hálózati) szolgáltatásokat nyújtanak felhasználóik számára. A legszűkebb, technikai jellegű értelmezéstől eltérően ez a megközelítés már felhasználói nézőpontú, szolgáltatás központú. Egy ilyen értelmezésű informatikai hálózat képes hagyományos távközlési (pld. távbeszélő, videokonferencia, fax, stb.) szolgáltatások nyújtására. Szolgáltatás-alapú megközelítésben tehát nincs ok a (hagyományos) távközlési és (hagyományos) számítógép-hálózatok megkülönböztetésére, ez gyakorlatilag technikai megvalósítási kérdéssé válik, ami a felhasználó számára érdektelen.”[1]

„A legtágabb értelmezés esetében az informatikai hálózat elemei nem kizárólag számítógépek, hanem bármilyen információs tevékenységet támogató rendeltetésű (tágabb értelemben vett informatikai), vagy egyszerűen csak más rendeltetésű, de információs képességekkel rendelkező (informatizált) technikai eszközök is lehetnek.„[3] Ezen elemzés szerint az informatikai hálózatok közé tartoznak tároló hálózatok, a térfigyelő rendszerek (infrastruktúrája), a vezeték nélküli szenzorhálózatok, vagy a felügyeleti, irányító és adatgyűjtő rendszerek (hálózatok) is.

Mind ezek után meg kell vizsgálni a ***hálózat és rendszer fogalmak*** viszonyát. Tapasztalataim szerint elmondhatom, hogy még a szakemberek körében is a keveredik a két kifejezés, mert azonos tartalomhoz kapcsolódóan találkozhatunk a rendszer és a hálózat kifejezésekkel, mint pld. távbeszélő rendszer és távbeszélő hálózat. Viszont álláspontom

4 Elosztók-erősítők (hub), kapcsolók (switch), útválasztók (router), átjárók (gateway).

szerint sok esetekben a jelzős kifejezések egyértelműen meghatározzák az eltérő tartalmát a két kifejezésnek pld. felügyeleti irányító és adatgyűjtő rendszer, illetve hálózat.

„A következőkben informatikai rendszer alatt eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására (információs szolgáltatások nyújtására) létrehozott (működő, technikai) rendszerét értjük." [4] Az informatikai rendszer fogalmába formális körülhatárolást és a működési, illetve irányítási, felügyeleti (működtetési, fejlesztési) fogalmakat értelmezünk általában. Ezekkel a jellemzőkkel különböztetjük meg az független autonóm rendszereket, az önállósággal rendelkező alrendszerekből felépülő rendszereket, szolgáltatásokat nyújtó és további szolgáltatásokat felhasználó önálló rendszerek, az egymással tervezetten együttműködő rendszereket (rendszerek rendszere), valamint az egymással dinamikusan változó rendszereket (rendszerek szövetsége) azaz összekapcsolódó rendszerek.

„Az informatikai hálózatok tartalmilag minden tekintetben megfelelnek a rendszerfogalom kritériumainak (működő technikai rendszerek), így elvileg minden informatikai hálózat egyben – egy speciális – informatikai rendszernek is tekinthető."[1] Tovább menve ezen gondolat soron az informatikát a szervezeten belül is kell tudni értelmezni.

„Az informatikai hálózat fogalma értelmezhető, sőt értelmezendő egy adott szervezet esetében is. A ***szervezet informatikai hálózata*** a szervezeten belüli információáramlás támogatásának, a szervezeti informatikai rendszerek, eszközök összekapcsolásának, valamint a szervezet és a környezet informatikai rendszerei, eszközei összekapcsolásának eszköze."[1]

A szervezet is az informatika viszonyából továbbá az informatikai hálózatok vizsgálatának tekintetében az infrastrukturális elemek is előtérbe helyeződnek.

„Szervezeti nézőpontból célszerű meghatározni a ***szervezet informatikai hálózata és informatikai infrastruktúrája*** viszonyát is. Az infrastruktúra tartalmi jellemzői, hogy szolgáltatásai alapvető igényeket elégítenek ki és széles körben, térbenileg kiterjedt módon, illetve időben stabilan férhetők hozzá." [5] Ennek megfelelően „a szervezeti informatikai infrastruktúra a szervezet egészének érdekeit szolgáló, többek által közösen használt informatikai erőforrások összessége, amelynek alapvető részét az informatikai rendszer további összetevőit rendszerbe integráló hálózat, a kiszolgáló eszközök nagyobb része, valamint a széles körben felhasználható alkalmazások és adathalmazok (adatállományok, adatbázisok, adattárházak, stb.) képezik. "[4]

Összességében a fenti elemzések alapján az informatikai hálózat fogalmát tág értelemben a

számítógép-, távközlési és egyes információs rendeltetésű technikai hálózatokat is magában foglaló módon használjuk, azaz olyan információs szolgáltatásokat nyújtó technikai hálózatokat érte, melyek csomópontjai információs tevékenységeket támogató eszközök, illetve kapcsolóelemek, továbbá információcserét biztosító valós fizikai, vagy absztrakt logikai kapcsolatok kötnek össze.

„Egy szervezet informatikai hálózata alatt szűkebb értelemben a szervezet informatikai rendszerének részét, a szervezet informatikai infrastruktúrájának alapvető összetevőjét, a hálózat csomópontjait alkotó informatikai eszközöket, valamint a szervezet felügyelete, irányítása alatt álló hálózati kapcsolóelemek és összeköttetések együttesét értjük. Tágabb értelemben a szervezet informatikai hálózatának részét képezik a külső szolgáltatók által biztosított – részben a szervezet által felügyelt, esetleg virtuális – kapcsolóelemek és összeköttetések is.”[1]

1.1.2. A RENDŐRSÉGI INFORMATIKAI HÁLÓZAT ÉRTELMEZÉSE

A 'Rendőrség informatikai hálózata' fogalom értelmezéséhez meg kell határozni a tartalmát, melynek célja a hálózat határainak kijelölése, hogy mely összetevők, elemek tartoznak a hálózathoz és melyek nem.

Dr. Munk Sándorral egyetértésben fontosnak tartom, hogy a fogalmi kérdések vizsgálata során nem az alkalmazott kifejezés az elsődleges, hanem a tartalom, melyhez különböző megnevezések rendelhetők.

A fogalom értelmezése céljából a következőkben Dr. Munk Sándor együttműködésében:

- összegezem a hálózat terjedelemére, határaira vonatkozó alapvető kérdéseket,
- röviden bemutatom a Rendőrség hálózatai fejlődését,
- áttekintem a kapcsolódó hálózatfogalmakat a szakmai dokumentumokban,
- meghatározom a Rendőrségi informatikai hálózat javasolt határait, összetevőit,
- meghatározom a hálózat működéséhez szükséges külső hálózatokat,
- bemutatom a hálózattal együttműködő legfontosabb külső hálózatokat.

A ***Rendőrségi informatikai hálózat tartalmának, határainak értelmezése*** során meg kell határozni azokat a szempontokat, amelyek alapján egyes elemekről, összetevőkről el kell tudni dönteni, hogy az adott hálózat részét képezik-e, vagy annak környezetéhez tartoznak. Ezen szempontok között vizsgálom az irányítási/felügyeleti, szolgáltatási és technológiai kérdéseket. Ezek a fajta megközelítések megjelennek a hálózat-megnevezésekben is. Ebben a

témakörben Munk Sándorral közösen folytattam le a kutatásaimat, melyeknek eredményeit az alábbiakban foglalom össze:”Az *irányítás/felügyelet központú megközelítés* szerint a hálózat határait az irányítási, felügyeleti jog- és feladatkör határai jelölik ki. Mindez megvalósítható mind alkalmazó, mind szolgáltató szervezetek szempontjából. Ennek megfelelően egy elem, összetevő akkor tartozik egy adott hálózathoz, ha afölött egységes irányítás érvényesül. Ez választ el egy adott informatikai hálózatot az általa felhasznált, de más irányítása, felügyelete alatt álló hálózatoktól. Az egységes irányítás meghatározott szabályozási keretek közötti követelménytámasztási, fejlesztési, felügyeleti, üzemeltetési szabadságot, egyben felelősséget tartalmaz. A határok kiszervezett feladatok, igénybe vett szolgáltatások esetében nem mindig könnyen jelölhetők ki. Esetünkben tehát vizsgálni kell, hogy a szóba jöhető hálózati elemek, összetevők körül mire terjed ki a Rendőrség irányítása, felügyelete.”[1]

„A *szolgáltatások oldaláról történő megközelítés* alapját egy kiválasztott szolgáltatási kör meghatározása képezi. Ennek megfelelően egy elem, összetevő akkor tartozik egy adott hálózathoz, ha hozzájárul a hálózati szolgáltatás megvalósulásához és nem tartozik oda, ha léte nincs hatással a nyújtott szolgáltatásra. E megközelítés nehézségei a különböző szolgáltatások egymásra épüléséből fakadnak. Ennek megfelelően a későbbiekben meg kell határozni, hogy miket kívánunk a Rendőrségi informatikai hálózat szolgáltatásai közé sorolni.”[1]

”A *technológiai szempontú megközelítés* az alkalmazott hálózati – fizikai, átviteli, kapcsolási, stb. – technológiákra épít. Ennek megfelelően egy hálózathoz azon elemek, összetevők tartoznak, amelyek egy adott technológia alkalmazására épülnek. A felsorolt három megközelítés közül felhasználói szempontból ennek van a legkisebb jelentősége. Ugyanazon (pld. távbeszélő) szolgáltatás számos különböző (pld. számítógép-, vagy műsorszóró) hálózati technológia segítségével, vagy ezek vegyes alkalmazásával is megvalósítható. Az elmondottak alapján véleményünk szerint ez a legkevésbé alkalmas a Rendőrségi informatikai hálózat határainak kijelöléséhez.”[1]

Az ***információs szolgáltatásokat nyújtó Rendőrségi hálózatok*** előzmény kutatását folytattam le, ezek közé a belügyi ágazat távközlési hálózatai[5] tartoztak, melyek üzemeltetése 1993-tól került át a Rendőrség (akkor az ORFK Híradástechnikai Szolgálata) feladatkörébe. 1999-ben jelent meg a Rendőrség és más rendvédelmi, rendészeti szervek számára szolgáltatásokat nyújtó Egységes Belügyi Digitális Hálózat (EBDH), mint a szolgáltatóktól

5 BM távhívó-távbeszélő hálózat, BM országos géptávíró hálózat, BM országos mozgószolgálati rádióhálózat, BM MRKB mobil rádiótelefon hálózat.

lehetőség szerint független, a meglévő alrendszerekre építkező zártcélú hálózat, amely a hagyományos beszéd- és adatátviteli alkalmazásokra épült. Az EBDH alapinfrastruktúráját egy 1990 és 2003 között önálló országos transzporthálózat képezte, amely vidéken alapvetően mikrohullámú, Budapesten kiegészült optikai, illetve vezetékes összeköttetésekre épült. „Az EBDH a BM Távközlési Szolgálat üzemeltette, és 2007 elején Zárt célú Rendészeti Hálózat (zRH) új megnevezéssel üzemeltetésre átkerült a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalához, majd átszervezést követően 2011. tavaszán a kormányzati hírközlési szolgáltatóhoz (Kopint-Datorg Zrt.)". [6] Ami jelenleg NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. A részvénytársaság neve 2011-ig Koping Datorg Zrt. volt. 2011-től a névváltoztatáson túl megkezdődött egy integrációs folyamat, melynek eredményeként a NISZ Zrt., illetve az alá tartozó szervezetek végzik a kormányzat távközlési és informatikai szolgáltatásokkal történő ellátását. (Pro M Zrt. akvizíció 2012) 2013-tól vált hangsúlyossá azon 2017-re beérő folyamat, hogy a központi kormányzati adatbázisok, nyilvántartások is tartozzanak a kormányzati Infokommunikációs szolgáltatóhoz. (2013 Idomsoft Zrt. megvásárlása, 2017 KEKKH beolvadása.)

A ***Rendőrségi szakmai dokumentumokban előforduló hálózatfogalmak*** áttekintéséhez Dr. Munk Sándorral közösen feldolgoztam a Rendőrséggel kapcsolatos jogszabályokat és ORFK utasításokat. Ezek között több hálózat kifejezéssel is találkoztam.[6] E fogalmakra egységesen igaz, hogy értelmezésüket, meghatározásukat a dokumentumok nem tartalmazzák és nem is hivatkoznak más olyan dokumentumra, forrásra, ahol ezek meghatározása megtalálható, tehát gyakorlatilag a kifejezések értelmezését ismertnek tekintik. Az '*informatikai hálózat*' kifejezéssel csak egyetlen ORFK utasításban (meglepő módon a kutyás és lovas szolgálati szabályzatban) [6] lelhető fel. Viszont a hálózati szolgáltatások fogalmával a 45/2013. (XI.) ORFK utasítás foglalkozik részletesen, melynek elemzését a későbbiekben szélesebb körben lefolytatom.

A leggyakrabban előforduló fogalom melyeket belső, országos belső zárt jelzőkkel szoktak ellátni, a "*intranet*"", vagy „intranetes hálózat", amelynek elfogadott értelmezése: „internet protokollokat használó, zárt – vagy csak biztonsági funkciókkal rendelkező eszközökön (tűzfal, átjáró) keresztül elérhető – számítógép-hálózat ("belső internet"= Intranet)". A "*számítógépes hálózat*"" kifejezést önállóan is fel lehet fedezni az ügyeleti szolgálattal, illetve az iratkezeléssel kapcsolatos szabályozásokban. [8][9]

6 A következőkben a több dokumentumban is előforduló hálózat kifejezések esetében csak egy, vagy néhány dokumentumra fogok hivatkozni.

Több szabályozóban is megtaláltam az „*adatátviteli hálózat*” fogalmat, az ”országos számítógépes” és a ”rejtjelezett” jelzőkkel. [10] Ennek elfogadott értelmezése: „adatátviteli szolgáltatások ellátására tervezett és optimalizált távközlő hálózat, amely hatékonyan képes adatok közvetítésére a hálózat végződései között, ahol adatátvitel alatt – a hagyományos analóg átvitellel szemben – digitális bitsorozatok, folyamok átvitelét”[1] kell érteni. Sok esetben a dokumentumok között fellelhető volt még a „*táv-adatátviteli hálózat*” kifejezés is [11], amely a nagyobb távolságra történő adatátvitelt biztosító hálózatok megnevezését takarta, azonban Dr. Munk Sándorral együttesen, megítélésünk szerint használata napjainkban a lehetőség általánossá válásával már idejétmúlt.

A hagyományos távközlési fogalmak közül a dokumentumokban a „'*távbeszélő hálózat”*' és a ”*távhívó hálózat*'„kifejezésekkel összekeveredve találkozhatunk a dokumentumokban. [12][13] A távhívás a helyi, egyetlen kapcsolóközpont segítségével lebonyolított hívás ellentéte, más távbeszélő hálózatba irányuló hívás, mely helyi központokat összekapcsoló távhívó központ(ok)on is átmegy. Ide kapcsolódik a „*hang-átviteli hálózat*” kifejezés, mely a beszédhangok átvitelét lehetővé tévő hálózat. Ezt a kifejezést a ”hang- és távadat-átviteli hálózat” összetételben található [11], ami egy integrált szolgáltatású hálózat megjelölése. Egy helyen fordult elő a ”*hír-összeköttetési hálózat*” kifejezés is [14], amelyet a híradás, kommunikáció, információkapcsolat egyes rendvédelmi területeken szinonimaként használtak.

A kutatás során Dr. Munk Sándorral a következő feladatként ***a Rendőrségi informatikai hálózat határai, összetevői*** körének kijelölését tűztük ki célul, vagyis annak meghatározása, hogy milyen kritériumok alapján mely összetevőket sorolunk a Rendőrségi informatikai hálózathoz és melyeket tekintjük azon kívül állónak. A megnevezéstől (az 'informatikai' jelzőtől) ideiglenesen eltekintve, tartalmi szempontból a hálózat határainak meghúzásánál megítélésünk szerint csak a felhasználó-központú, szolgáltatás-alapú kritérium lehet megfelelő megoldás.

A vizsgálat során a meghatározandó hálózat-fogalomnak álláspontom szerint, magában kell foglalnia az információs szolgáltatást nyújtó hálózatot, a távközlési, számítógépes és más (pld. térfigyelő, érzékelő, stb.) hálózatokat egyaránt.

A 'Rendőrségi' jelző használatának kritériuma, hogy a vizsgálat határa az ORFK irányítása, felügyelete szerint kerüljön meghúzásra mely szerint a Rendőrségi informatikai hálózat az ORFK irányítása, felügyelete alá tartozó hálózatokra, hálózati összetevőkre terjed ki és nem tartoznak bele a más (kormányzati és társ-) szervezetek által felügyelt hálózatok.

„Egy tágabb értelmezés szerint a Rendőrségi informatikai hálózat keretei közé sorolhatók a következő – a Rendőrségi tevékenységhez szorosan kapcsolódó jellegű, de nem a Rendőrség szervezetében, hanem a Belügyminisztérium irányítása, felügyelete alá tartozó – szervezetek (belügyi szervek): a Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK), a Nemzeti Védelmi Szolgálat (NVSZ), a Terrorelhárítási Központ (TEK) és a Rendőrtiszti Főiskola. (Nemzeti Közszolgálati Egyetem). E tágabb értelmezést indokolhatja a szervezeti informatikai hálózatok kiterjedt együttműködési kapcsolatrendszere, illetve a hálózatbiztonsági követelmények, kockázatok, megoldások jelentős hasonlósága, esetenként azonossága.”[1] Ennek megfelelően a továbbiakban erre az értelmezésre alapozok. Ezen tágabb megközelítés, csak a Rendőrséginek tekintett hálózat fogalmára terjed ki, de tagszervezetek közötti adatcserénél is meg kell határozni a belső átadási pontokat, ezek biztonságát és a szervezetek közötti adatkezelési szabályokat.

A Rendőrségi informatikai hálózat határ területének vizsgálata során – a ráépített (átfedő) hálózat[7] értelmezésében –***felhasznált külső hálózatok*** közé tartozik a Zártcélú Rendészeti Hálózat (a továbbiakban: zRH), az Nemzeti Távközlési Gerinchálózat (a továbbiakban: NTG), az Egységes Digitális Rádiótávközlő Rendszer (a továbbiakban: EDR), valamint egyes távközlési szolgáltatók hálózatai, melyeket a későbbi fejezetekben fogok elemezni. A Rendőrségi informatikai hálózat országos infrastruktúráját, gerinchálózatát a zRH biztosítja, és emellett funkcionálisan kiegészíti a BM országos távhívó távbeszélő hálózata, továbbá a fent említett hálózatok alkotják.

A fizikailag különálló *zRH*[8] az *NTG* virtuális kiegészítő gerinchálózatát, egyben annak melegtartalékát is képezi és fordítva, de mindkét hálózat önállóan felügyelhető, működésük egymást nem befolyásolja. [6] Az *EDR* hálózaton belül szervezeti szintű virtuális magánhálózatok (VPN-ek) működnek, erőforrásainak több mint 80%-át a rendészeti VPN használja, amely kiterjed a Rendőrség, a büntetés végrehajtás és a NVSZ felhasználói körére is. „A BM országos távhívó távbeszélő hálózata két budapesti főgyűjtő gócközpontot, mintegy 30 kormányzati és rendészeti célú objektum távbeszélő alközpontját, valamint az érintett épületek strukturált kábelhálózatát foglalja magában.”[1]

Végül röviden az ***együttműködő külső hálózatokról. Ezen hálózatok*** szorosan kapcsolódnak a Rendőrségi informatikai hálózathoz, a Rendőrségi informatikai hálózat biztonsági kérdéseinek elemzése, gyakorlati megvalósításában részt vállalnak. Az

7 Overlay network.
8 MPLS VPN Carrier Supporting Carrier.

együttműködő hálózatok terén mind rendőrszakmai, mind szolgáltatásfejlesztési szempontból a legnagyobb kihívást a NISZ Zrt. üzemeltetése alá tartozó e-közigazgatás folyamatban lévő kialakítása jelenti. Jelen vizsgálatnak nem képezi részét, ezek körének meghatározása, mert az érintett hálózatokkal a Rendőrségi informatikai hálózat több fajta módon – közvetlenül, vagy más felhasznált hálózatokon keresztül – is kapcsolatban állhat. Az együttműködő külső hálózatok főbb csoportjai lehetnek a kormányzati/közigazgatási hálózatok, a védelmi szféra más szervezeteinek úgy, mint a honvédség, a katasztrófavédelem, a nemzetbiztonsági szolgálatok, a mentőszolgálat, a büntetés végrehajtás, a Nemzeti Adó és Vámhivatal hálózatai, és egyes európai uniós és NATO hálózatok.

1.1.3. JAVASLAT A RENDŐRSÉGI INFORMATIKAI HÁLÓZAT FOGALMÁRA

Az eddigi kutatásaim alapján a Rendőrségi informatikai hálózat fogalmát az alábbiakban foglalom össze: „*szűkebb értelemben a Rendőrség, tágabb értelemben emellett egyes rendőri feladatokat ellátó szervek felügyelete, irányítása alatt álló, információs szolgáltatásokat nyújtó technikai hálózatok összessége*.”[1] Ennek megfelelően a Rendőrségi informatikai hálózat magában foglalja a hagyományos távközlési, vezetékes és mobil távbeszélő, (régen géptávíró), rádiótávközlő, hálózatokat, továbbá a számítógépes hálózatokat, valamint a speciális rendeltetésű térfigyelő, érzékelő hálózatokat.

A hálózat megnevezésére a magyar (szak)nyelvben elvileg több jelzős kifejezés – pld. információs, informatikai, infokommunikációs, információtechnológiai, stb. – létezik. A hálózatbiztonság szempontjából a Magyar Informatikai Biztonsági Ajánlások szerint az 'informatikai' jelző 'információs tevékenységeket támogató, megvalósító technikai [megoldás]' tartalmú használatát javasolja.

A fejezetben végzett kutatásokat összefoglalva a „Rendőrségi informatikai hálózat tehát 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 állnak fent.”[1]

1.2. A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁNAK FELÉPÍTÉSE, ÖSSZETEVŐI SZOLGÁLTATÁSI SZEMPONTBÓL

A Magyar Rendőrség informatikai hálózatának leírásán és jellemzésén keresztül rámutatok az informatikai hálózatok biztonságának fontosságára, összegzem védelmének alapjait.
A hálózati szolgáltatások fogalom körét jól körbeírja a 45/2013. (XI.) ORFK utasítás mely szerint hálózati szolgáltatásoknak nevezzük a: „számítógépes munkahelyről igénybe vehető, helyi hálózati intranetről elérhető szerverszolgáltatások, amelyek hálózati forgalommal járnak”[15]. Ezek alapján végeztem a szolgáltatásokhoz kötődő kutatásaimat a további alfejezetekben.

1.2.1. A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁNAK ÁTFOGÓ FELÉPÍTÉSE SZOLGÁLTATÁSI SZEMPONTBÓL

Szolgáltatás szempontból a Rendőrség informatikai hálózatát két részre bontom:

- Adatfeldolgozó

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv) 1§.(1) bekezdés 3. pontja szerint az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;
A fenti meghatározások nyomán, azokat összefoglalva az adatfeldolgozó hálózatok azok a technikai adatátviteli utak, melyek útján a Rendőrség meghatározott adat típusokat az előre rögzített követelmények szerint feldolgozza, szervezeten belül fogadja és továbbítja.

- Adatszolgáltató, kezelő

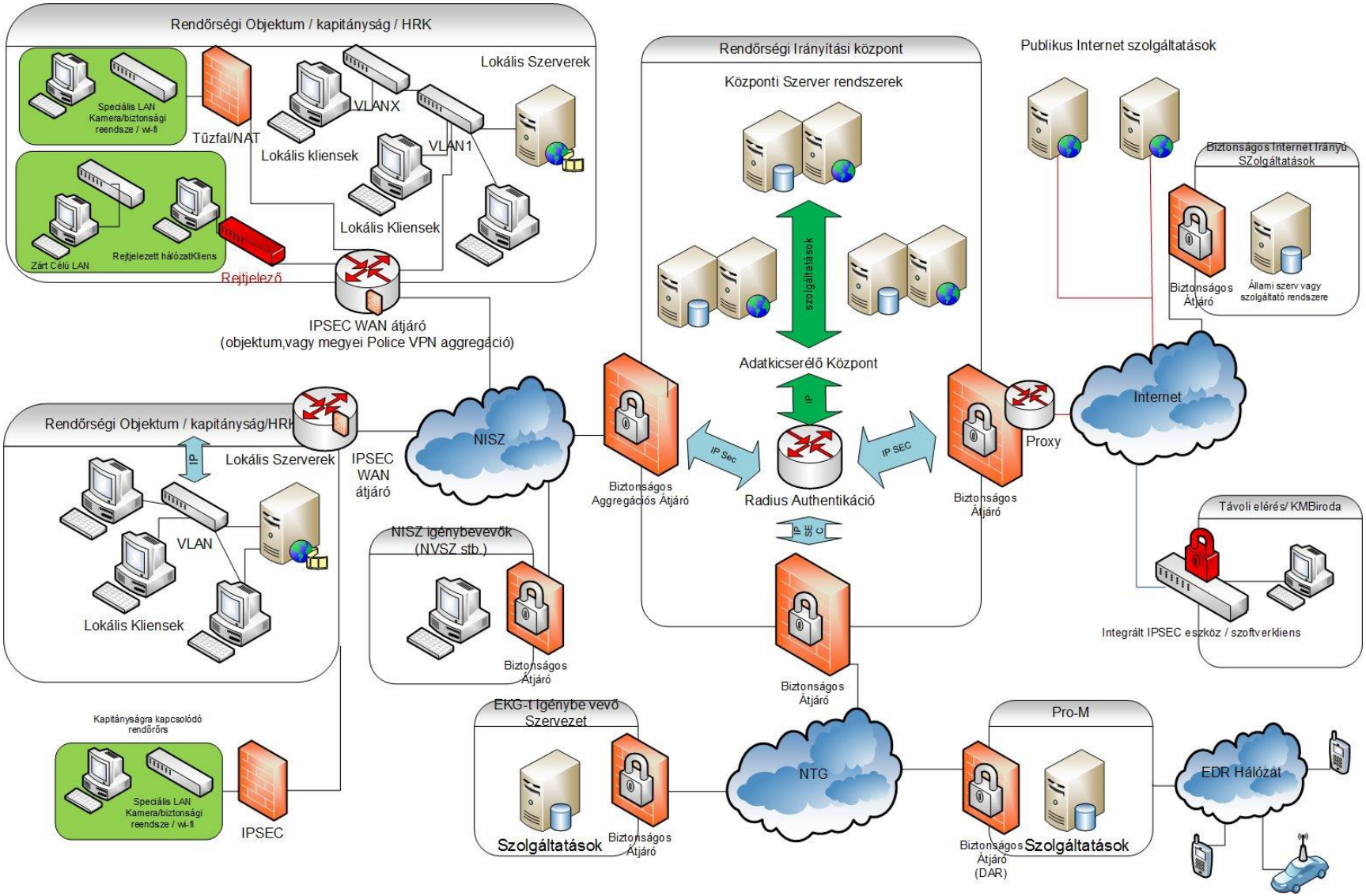
Az Ibtv.. 1§ (1) bekezdés 4. pontja szerint adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;
Az Ibtv. 1§ (1) bekezdés 5. adatkezelő: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;
A fenti meghatározások nyomán, azokat összefoglalva az adatszolgáltató-kezelő hálózatok mindazon adatátviteli utak, melyek segítségével meghatározott célú adatkezelés útján más

szervezet részére a meghatározott igény alapján elektronikus úton a Rendőrség adatszolgáltatás keretében adatokat ad át. Például az EDR vagy rejtjelzett hálózat.

1.2.2. ÖSSZETEVŐK TÍPUSAI

A Rendőrség informatikai hálózat összetevőinek szempontjából az alábbi típusokat különböztetem meg: (1. számú ábra: A Rendőrség informatikai hálózat összetevői szolgáltatás szempontjából)

- országos hálózatok. Országos szinten a Rendőrség minden egyes szervezete használja hozzáférés szabályozása mellett,
- az objektumokban kiépített helyi lokális hálózatok az országos gerinchálózatokra kapcsolódnak annak lokális részét képezik
- helyi szigetszerű lokális hálózatok. Helyi szinten, csak az adott szervezet használhatja, nyerhet ki belőle adatot, más szervezet semmilyen módon nem férhet hozzá, nincs összekötve más helyi hálózatokkal,
- funkcionális növelt biztonságú hálózatok. Adott feladat ellátására, megkülönböztetett szakterület használhatja szabályozott hozzáférés mellett.



1. számú ábra: A Rendőrség informatikai hálózat összetevői szolgáltatás szempontjából

A szolgáltatás és fizikai struktúra is országos rendszerű, a belső és külső kapcsolatok is országos kapcsolóközpontban vannak kezelve. (A szabályok alapján forgalom optimalizálásként felépülhetnek megyék közötti csatornák, de a vezérlés ez esetben is országos.)

Országos hálózatnak tekintjük a Rendészeti hálózatot melyen minden alkalmazás, rendszer és program elérhető csillagpontos technológiával a Rendőrség minden szervezete részére, mely feladatellátásához szükséges. Pl.: körözési rendszerek, nyilvántartások, az RZS központi nyilvántartása, ügyviteli rendszerek, stb. Továbbá ide soroljuk az EDR hálózatát, mely országos szinten ellátja a Rendőrség szervezetei számára a rádiós kommunikációt. Az országos hálózatot nem csak a szervezetek hálózatai alkotják, hanem a helyi lokális hálózatok is összetevőit képezik.

Helyi lokális hálózatnak tekintjük a megyei rendőr-főkapitányságok hálózatát a hozzátartozó kapitányságokkal és más szervezeti egységek lokális hálózatait. Melyek természetesen egyben az országos hálózat részét is képezik. Ezeken a hálózatokon az adott szervezeti egység helyileg keletkezett adatait tartják nyilván, lokális adatbázisok érhetőek el a hálózatban szereplők részére.

Funkcionális hálózatnak tekintjük az NVSZ hálózatát, a Műveleti hálózatokat és a Rejtjelzett hálózatokat. Ezeken a hálózatokon nem nyilvános adatokat és rejtjelzett minősített adatokat továbbítanak a hálózat szereplői. A hálózat szereplőihez tartoznak a Készenléti Rendőrség Nemzeti Nyomozó Iroda és kirendeltségei továbbá mindazon szervezetek melyek törvényi felhatalmazás által minősített adat feldolgozására hivatottak. Elemző értékelő és felderítő munkálatokat látnak el a hálózat segítségével. Ezek a hálózatok mind az országos hálózatoktól mind a lokális hálózatoktól elkülönülten kezeljük, mind amellett hogy rejtjelzett hálózat lehet lokális az adott épületben, és lehet akár országos is, amely szervezeti egységeket köt össze speciális eszközök alkalmazása révén.

1.2.2.1. Rendőrségi Informatikai Hálózatok Kapcsolatrendszere

A Rendőrség informatikai hálózatának kapcsolatrendszere három szintre tagozódik. (4. számú ábra: A Rendőrségi informatikai hálózat kapcsolatai)

1. Rendészeti hálózat szintje, melyhez csatlakozik a 20 db Megyei Rendőr-főkapitányság helyi lokális hálózata, a Rendészeti szakközépiskolák helyi hálózata és minden más az ORFK

alá rendelt szervezet.

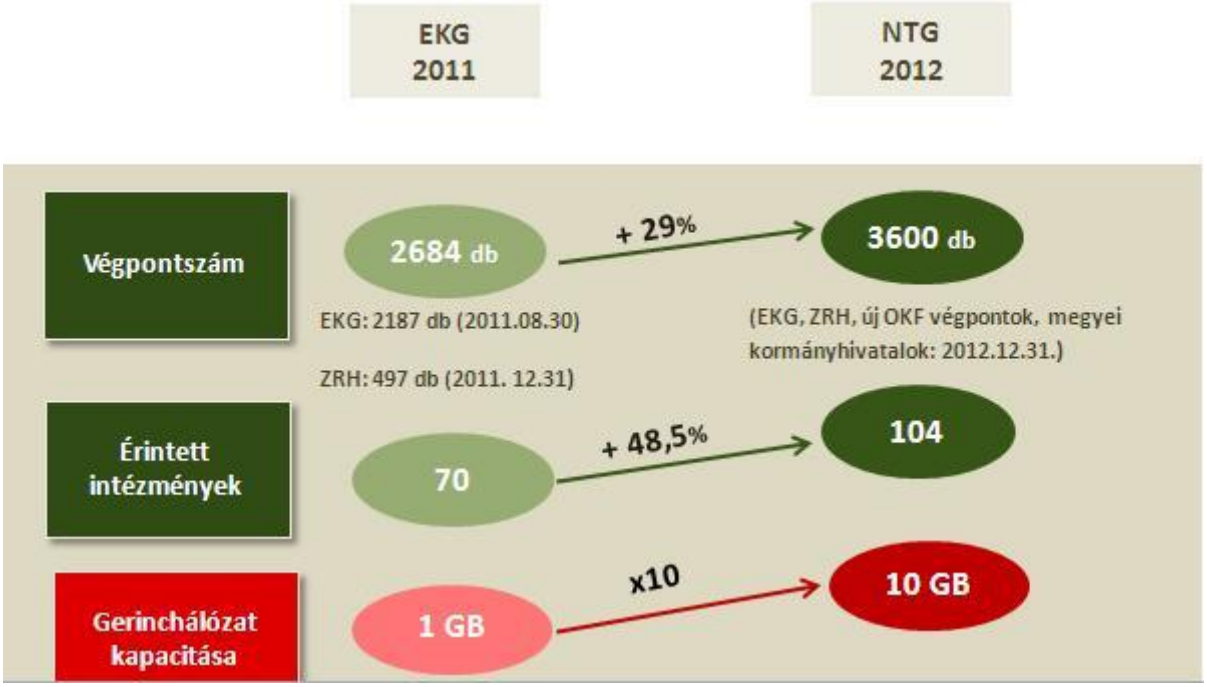
2. A zártcélú rendészeti hálózat szintje, melyhez az Országos Rendőr-főkapitányságon kívül csatlakozik a Belügyminisztérium, a TEK, a Készenléti Rendőrség Nemzeti Nyomozó Iroda, a Nemzeti Közszolgálati Egyetem és az NVSZ.

3. Az NTG szintjéhez csatlakozik közvetlenül a volt Köztársasági Őrezred utódszervezete, a Büntetés-végrehajtási Parancsnokság, a Bevándorlásügyi Hivatal, a Nemzetbiztonsági Szakszolgálat, az Országos Katasztrófavédelmi Főparancsnokság, az Alkotmányvédelmi Hivatal és a Kormányzati szervek.

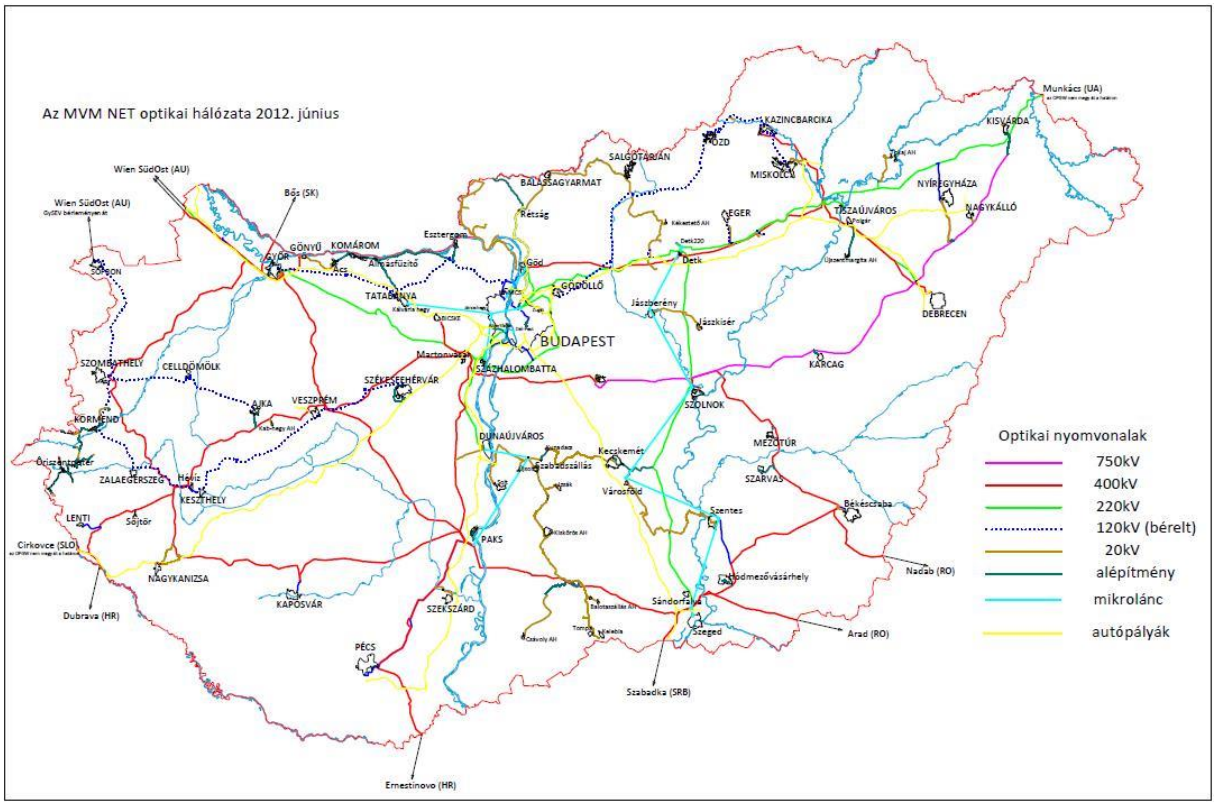
NTG: Nemzeti Távközlési Gerinchálózat. Az állami intézményrendszer részére, annak infrastruktúrájára támaszkodva állami tulajdonú társaságok biztosítják az elektronikus hírközlési szolgáltatásokat. A kialakítás célja az egységes minőség és a költséghatékonyság biztosítása.

A kormány a távközlési hálózatának fejlesztése során passzív (optikai gerinc) és aktív (átviteli és IP berendezések) elemekből álló korszerű, nagy kapacitású és kimagasló megbízhatóságú rendszert épített ki, amely teljes mértékben kielégíti a rendszerirányítás távközlési igényeit. Ezen az informatikai hálózaton kommunikál 104 állami intézmény 3600 végpontszámmal. (2-es számú ábra)

A Nemzeti távközlési gerinchálózat elsődleges rendszere MVM-net infrastruktúrája.



2. számú ábra: NTG és az EKG változásai

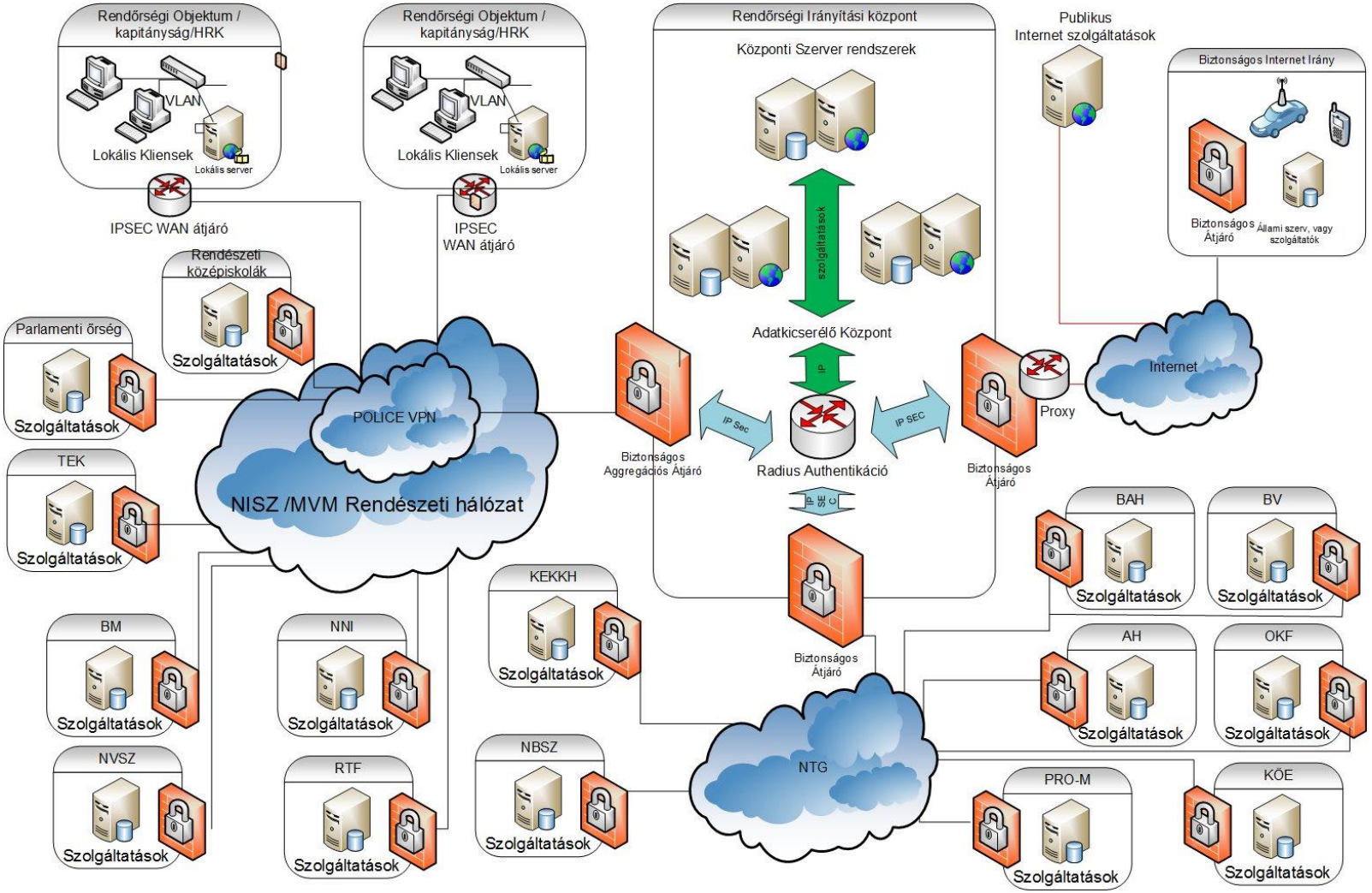


3. számú ábra: Az Nemzeti Távközlési Gerinchálózat Magyarországon

Az Országos Rendőr-főkapitányság, és rajta keresztül a Rendőrség csak közvetve kapcsolódik az NTG-hoz a zártcélú rendészeti hálózaton keresztül.

A Rendőrség szervei ezt az EKG irányú elérési utakat a rendészeti hálózat beiktatásával és biztonságos központi átjárón keresztül tudják csak elérni. Az NTG-vel a Rendőrség és a katasztrófavédelem korábbi, gyenge távközlési ellátottságot biztosító felhordó hálózatának kiváltása is megtörtént

.



4. számú ábra: A Rendőrségi informatikai hálózat kapcsolatai

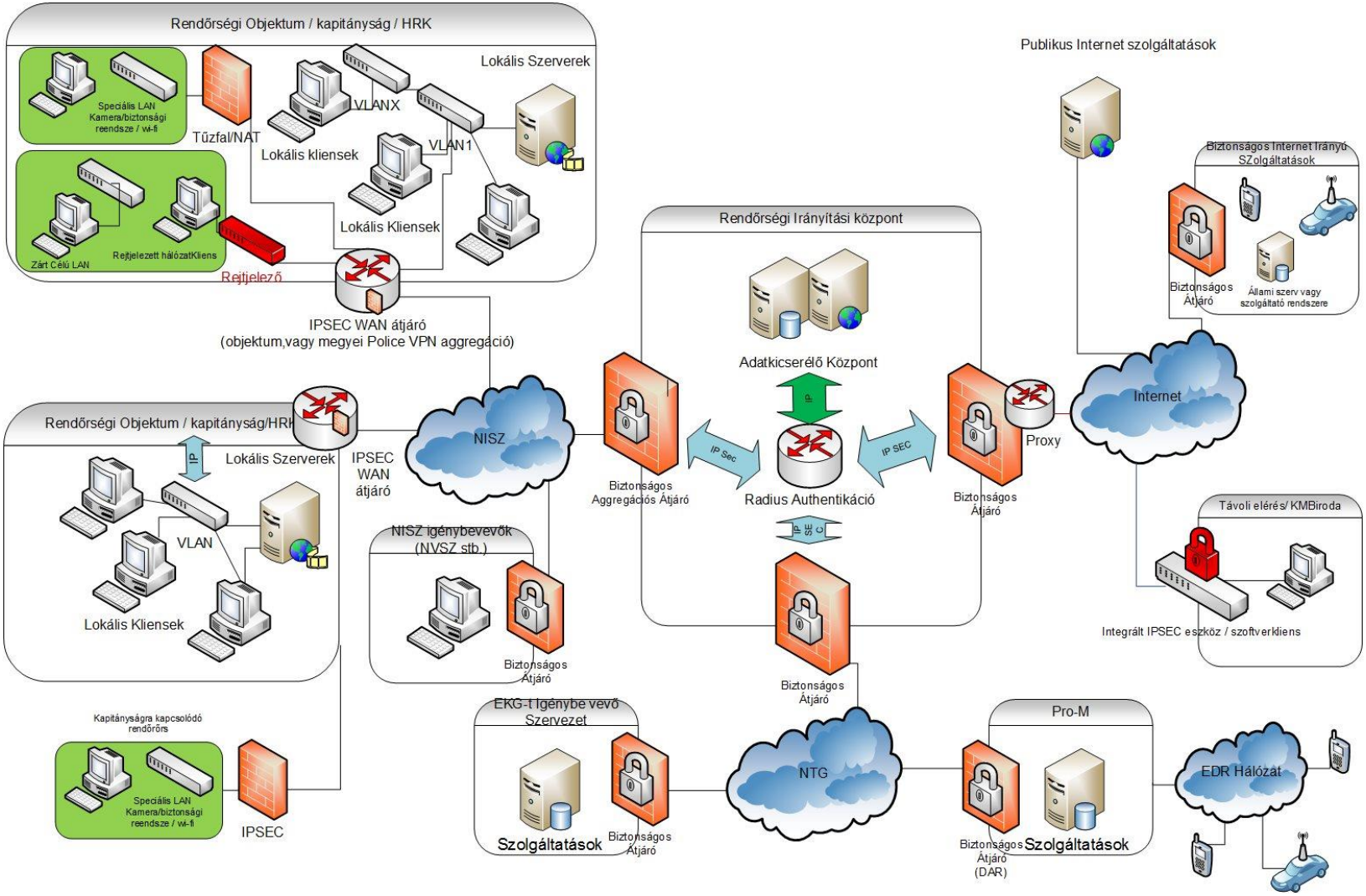
A zárt célú hálózat logikailag elkülönül az EKG-tól, de a NISZ által szolgáltatott vezetékes struktúra szintén az MVM gerinchálózatán alapul. A vezetékes hálózattal el nem látott igénybevételi helyeken a NISZ alapvetően az Antenna Hungáriával alakítatja ki a kapcsolatokat. A gyakorlati működés során a NISZ igénybevételének kötelezettsége gyakran jár nehézséggel, mert a szolgáltatás átadási pontokon gyakran más szolgáltatok magasabb megbízhatóságú, kapacitású és/vagy olcsóbb szolgáltatásai is elérhetőek. Bizonyos esetekben erre szabályos kompromisszumos megoldást adhat, ha a NISZ együttműködésével más szolgáltató fizikai struktúrája felett a szolgáltatást a Rendőrség a NISZ-en keresztül, veszi igénybe. (pl.: nagyvárosokban a NISZ mikrohullámú kapcsolatot tud biztosítani, de más szolgáltató optikai struktúrával rendelkezik ugyanott.)

1.2.2.2. Szervezeti szintekhez igazodó megjelenítés

A Rendőrség hierarchikus felépítését az informatikai hálózatának felépítésében is tapasztalhatjuk. Ezek alapján a szervezeti szintek tekintetében az alábbiakat különítem el egymástól (4. számú ábra: A Rendőrségi területi szintű informatikai hálózat). Ez hierarchikus ábra, nem informatikai hálózat. A KMB-sek ORFK VPN kártyán keresztül, vagy interneten, vagy mobilon kommunikálnak.

- Országos informatikai hálózat (az ábrán kék vonal feletti rész),
- Területi informatikai hálózat (az ábrán piros szaggatott vonal feletti rész),
- Helyi informatikai hálózat (az ábrán piros szaggatott vonal alatti rész).

A hálózatok elérése logikailag az ORFK-n keresztül történik, nem megyei szinten. A mobil kapcsolatos és tipikusan a vezetékes kmb-k is nem az őrsre kapcsolódnak. Az felhordó struktúrájuk internet, mobil APN, vagy az országos Rendőrségi hálózat.
Az őrsök esetében jellemző a kapitányságra való felhordás, de a KMB irodák szinte mindegyike közvetlen NISZ, vagy mobil APN kapcsolattal bír és ORFK-n kerül átvételre a NISZ zrt-től, vagy a mobil szolgáltatótól.



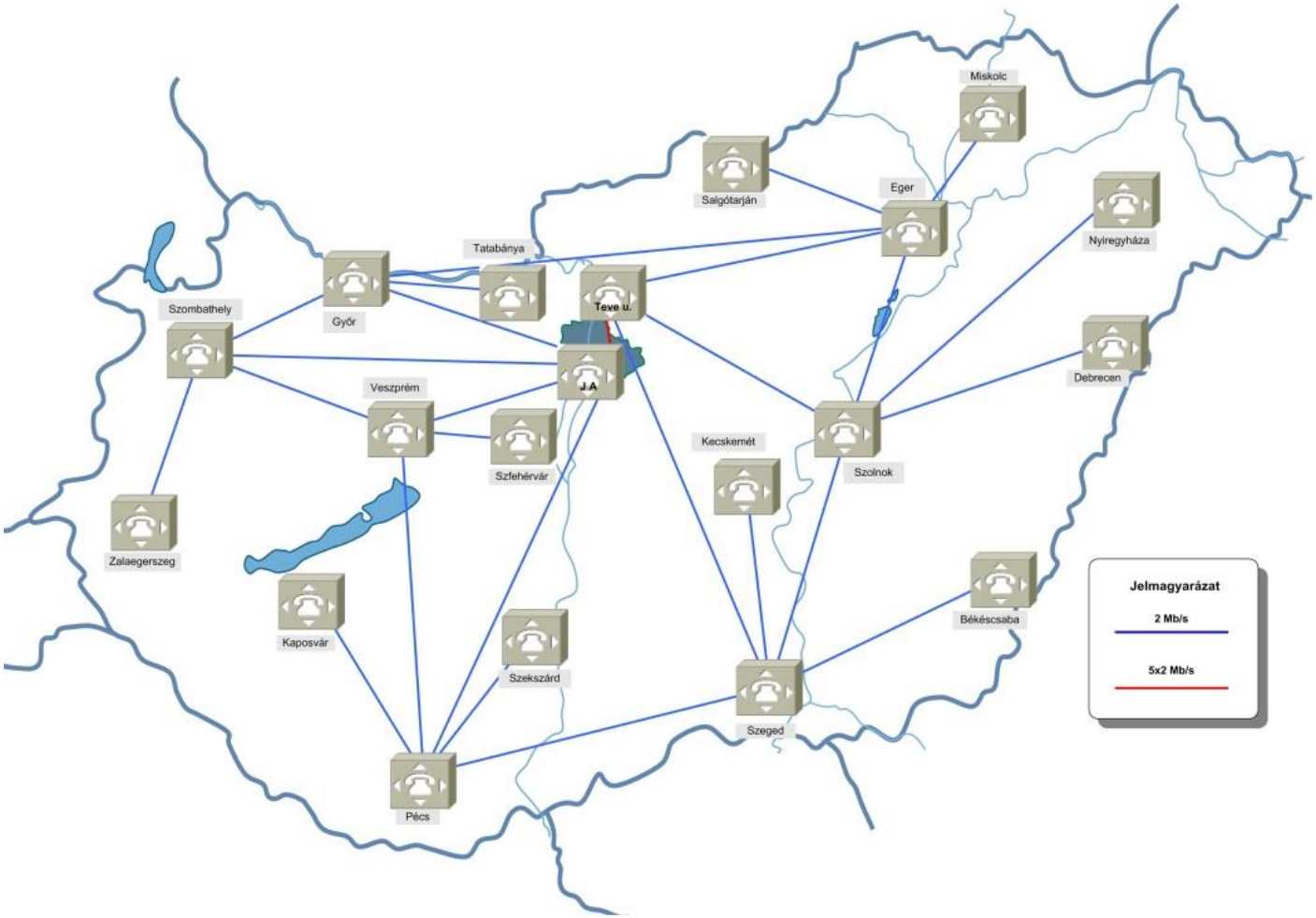
5. számú ábra: A Rendőrségi területi szintű informatikai hálózat

1.2.3. TÁVBESZÉLŐ SZOLGÁLTATÁST NYÚJTÓ ÖSSZETEVŐK

Távbeszélő, illetve adatátviteli összeköttetések országos viszonylatban a zRH biztosítja a rendészeti célú országos távbeszélő távhívó hálózat fő központjai közötti összeköttetéseket, illetve adatátviteli szempontból a különféle kormányzati és rendészeti felhasználók (Rendőrség, okmányirodák, BM, Katasztrófavédelmi szervek, BÁH, stb.) részére a virtuális hálózati szolgáltatásokat.

1.2.3.1.Távbeszélő szolgáltatást nyújtó, támogató (kiszolgáló) eszközök, hálózatrészek, alrendszerek.

A hálózatban üzemelő telefonközpontok által nyújtott szolgáltatások összességében mintegy 20.000 vonal nagyságrendű kapacitást érintenek. Az országos mikrohullámú hálózat 5 felügyelt távközlési létesítményt és további 228 db más objektumot érint. Ezen telephelyek nagyrészt saját, illetve bérelt ingatlanok. (6. számú ábra: A Rendőrségi Távbeszélő szolgáltatást nyújtó, támogató informatikai hálózat)



6. számú ábra: A Rendőrségi Távbeszélő szolgáltatást nyújtó, támogató informatikai hálózat.

1.2.3.2.Szervezeti szintű és országos összetevők, szolgáltatási jellemzőik, kapcsolatrendszerük, a Rendőrségi vezetékes telekommunikáció

A Rendőrségen alkalmazott vezetékes telekommunikáció elemei (rendészeti zártcélú hálózat, telefonközpontok, alközponti hálózat, végberendezések) nem képeznek homogén rendszert. A hálózatok, túlnyomó többségben a biztonságos strukturált kábelezési rendszer elemeinek felhasználásával lettek kialakítva (zárható rack szekrények, megfelelő gyengeáramú helységek, mikrohullámú vagy optikai trönk összeköttetések). A távbeszélő központok digitális vezérlésűek, de mellékoldali kiépítésükben többségben vannak az analóg mellékállomások a digitális illetve IP mellékekkel szemben. A lokális telefonközpontok felhordása tipikusan a helyszíni átjáró segítségével az adatátviteli hálózatba beágyazottan történik.

A teljes IP telfónia megvalósítása mind technikailag, mind szolgáltatás tekintetében, mind pénzügyileg célszerű lenne. A jelenlegi fokozatos átállás oka, hogy középtávon magasabb, de aktuálisan kisebb eseti összegekből megvalósítható, illetve nem szükséges hozzá a minden érintett közötti teljes rendszerre kiterjedő koncepcionális és technológia konszenzus kialakítása.

Az új megvalósításoknál és felújításoknál azonban priorítást kap a NISZ IP szolgáltatásának igénybevétele.

1.2.3.3.Mobil rádiótelefon adat és beszédkommunikáció

A Rendőrség a hazai szolgáltatok közül jelenleg elsődlegesen a Telecom Magyarország Zrt. céggel áll telekommunikációs üzleti kapcsolatban. Előfizetéseink egyedi üzleti díjcsomagba való besorolása alapvető biztonsági szintet tesz lehetővé (kártya PIN védelme, lopás esetén kártyatiltás). A vezetői és beosztotti szinten okos telefonok kerültek bevezetésre, melyeken a levelezés szinkronizálása lehetséges a Rendőrségi levelező rendszerrel szinkronizálni a felhasználók postafiókját. Speciális internet és APN adat továbbítási célra nagyobb mennyiségben Telenor, illetve minimális darabszámmal a Vodafone szolgáltatás is igénybe vételre kerül. (Rendszer lefedettség,átviteli kapacitás javítás, illetve beépített SIM költséges cseréje indokolja ezen szolgáltatások igénybevételét.)

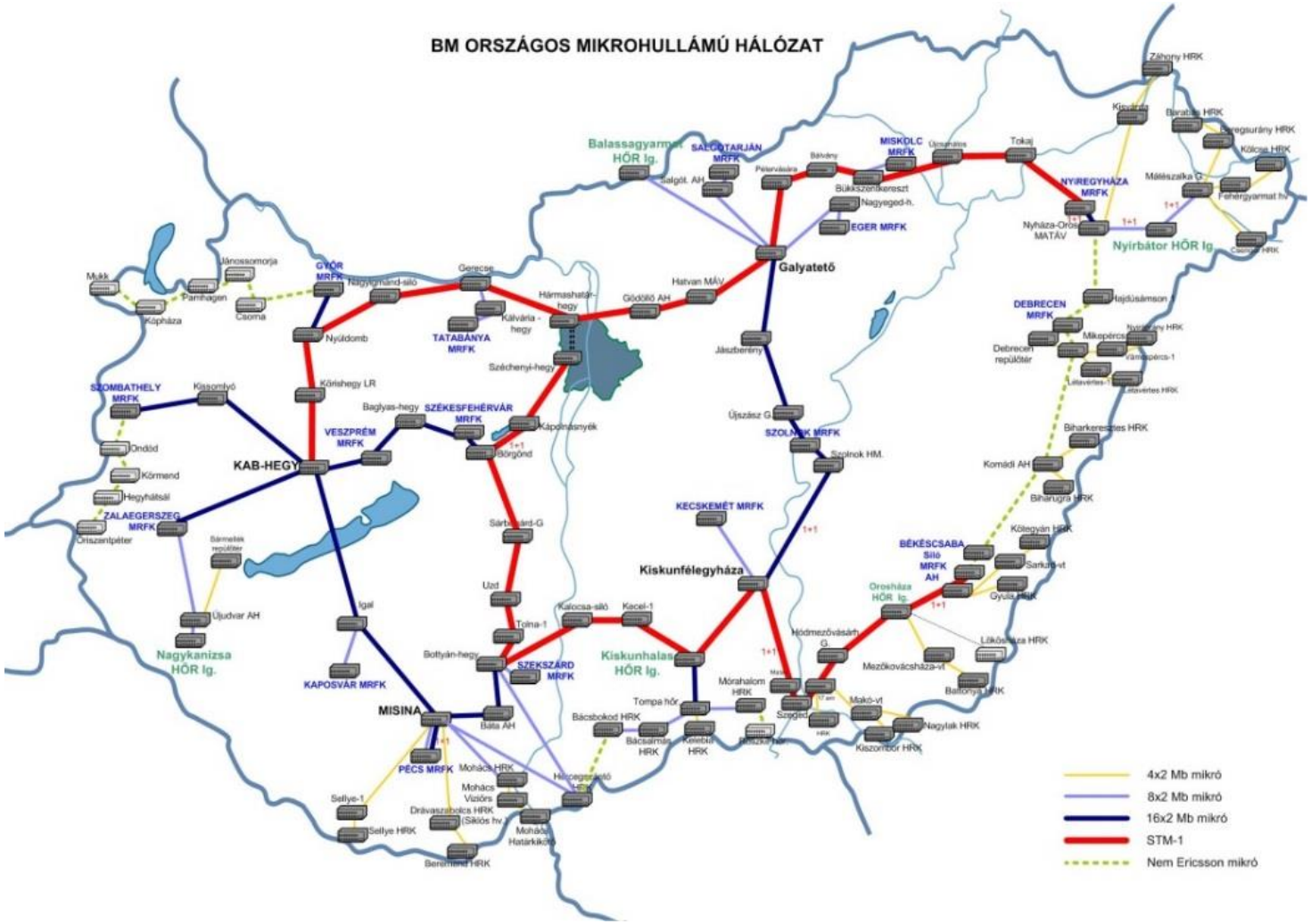
1.2.3.4.EDR rádió

A Rendőrség által is használt beszédkommunikációs hálózat az EDR rádió hálózata. A 2006-ban üzembe helyezett, csoportkommunikációs célra kiépített, TETRA szabványok alapján működő digitális rádiórendszer hálózati infrastruktúráját külön erre a célra létrehozott távközlési szolgáltató üzemelteti. Az EDR hálózaton belüli menedzsment feladatokat azonban – az Egységes Digitális Rádió-távközlő rendszerről szóló 109/2007. (V.15.) Kormány Rendelet alapján – a ProM. Zrt. végzi. 2017-ben a KEK KH beolvadt a NISZ Zrt-be, illetve néhány feladatot a Belügyminisztérium vette át. Az EDR hálózaton belül az egyes felhasználói szervezetek külön magánhálózatként szerepelnek, minden felhasználó a saját VPN-en belül teljes joggal rendelkezik, együttműködésüket a menedzser szervezet teszi lehetővé, így a Rendőrség is.

A magyarországi TETRA rendszer legnagyobb felhasználói a rendészeti szervek, melyek a hálózati erőforrások 82,5%-át használják. A rendészeti magánhálózat összesen 28.400 db rádióterminál kommunikációját biztosítja, amelynek rendszerszintű felügyeletét Rendészeti VPN menedzserek látják el. A rendszert jelenleg 27 szervezet használja. A rendszer a napi feladatokban, a bevetések során, a kárhelyszíni-, illetve a veszélyhelyzetekben is megfelelő kommunikációs csatornát biztosít a műveletirányítás és a szervezetek közötti együttműködésre. A hangkommunikáció mellett, a rendszer elméletileg biztosítja a feladatban résztvevő erők és eszközök pozíció adatainak térképen történő megjelenítését.

Az országos mikrohullámú hálózat tekintetében a kormányzati és közös sávban kijelölt frekvenciákat használ fel a Zrh. (7. számú ábra: A BM Országos mikrohullámú hálózata)

A zRH üzemelése Budapesten és országos viszonylatban több mint 220 db aktív eszköz (routerek, switchek) folyamatos üzemét jelenti, emellett a hálózatban további 200-300 db egyéb eszköz van jelen. A zRH tekintetében az optikai, illetve rézalapú „D” jelű, hozzávetőlegesen 610 km hosszúságú kábelhálózatot tesz ki. A kábelhálózaton keresztül biztosított szolgáltatásokat igénybe vevők köre kiterjed a különféle kormányzati és rendészeti szervekre, felhasználóink közé tartozik és tartozott többek között a MEH, IRM (BM), NBH, NBSZ, AH, IH, BÁH, BV, ÖM, OKF, ORFK, TIBEK stb.



7. számú ábra: A BM Országos mikrohullámú hálózata

1.2.4. HÁLÓZATI INFRASTRUKTÚRA, IGÉNYBEVETT KÜLSŐ SZOLGÁLTATÁSOK

Az információáramlás piramis csúcsa az NTG. A Rendőrséggel együtt már 219 központi közigazgatási intézményi végpont kapcsolódik rá.

A Belügyminisztérium egységes MPLS (Multiprotocol Label Swiching) VPN (Virtual Private Network) alapú hálózatot (BDH, Belügyi Digitális Hálózat) üzemeltet a Minisztérium szervezetei számára. Ezen az egységes hálózaton valósulnak meg az ORFK WAN kapcsolatai is.

A jelenlegi kommunikációs rendszer fő részét a Budapestet a megyei központokkal összekötő nagysebességű transzporthálózat alkotja, mely a különböző rendszerek (távbeszélő, adatátviteli) forgalmát bonyolítja le. Az átviteli gerinchálózathoz – megyén belül – az MRFK-n, Közigazgatási Hivatalon létesített csomópontokon keresztül lehet csatlakozni, melyeken keresztül az MPLS hordozóhálózaton át elérhetők a központi adattárak és alkalmazások, illetve szervezetek hálózatai (BM-József Attila u.; ORFK-Teve u., BM Központi Hivatal-Balázs Béla u.). A körgyűrűbe szerveződő országos központok (BM-József Attila u., ORFK-Teve u.; BM Központi Hivatal - Balázs Béla u.) elérhetőkké válnak. Ez az ATM technológia felépítését tükrözi, mely létezik, de nem ezen keresztül történik az adatkommunikáció.

A transzporthálózatot elsődlegesen a Belügyminisztérium kezelésében levő országos mikrohullámú rendszer összeköttetései alkotják, biztosítva a kerülőutak automatikus kialakításának lehetőségét is, másodsorban a közcélú távközlési szolgáltatóktól bérelt menedzselt adatátviteli összeköttetéseken keresztül létrehozott átviteli utak.

Az országos gerinchálózaton 34Mbit/sec sebességű mikrohullámú linkeken kialakított, gyűrűs topológiájú MPLS technológia került bevezetésre, ami távlatilag a felhasználók irányába integrált adat, hang, kép és mozgókép átvitelét biztosítja. A sávszélesség optimális kihasználását fejlett QoS szolgáltatással, az adatátvitel prioritásainak meghatározásával igyekszünk biztosítani.

A főváros vonatkozásában nagy kiterjedtségű optikai kábelhálózaton, egy időben többféle adatátviteli technológia került bevezetésre. Az nx2Mbit/sec áramkörigényeket SDH

rendszerek szolgálják ki: körgyűrűbe szervezve, STM1 adatátvitel valósul meg, node-onként 8-16 2Mbit/sec porttal. Az alkalmazás elsősorban a Rendőrség fővárosi kapcsolástechnikai hálózatának nem integrált hang összeköttetését biztosítja, ISDN30 rendszerű társközponti áramkörök formájában.

Az adatátviteli összeköttetések ATM és Gigabit Ethernet eszközök segítségével szintén optikai kábelközegen keresztül kerültek kiépítésre, tekintettel az időközben bekövetkezett technológiai változásokra, és a Gbit Ethernet technológia fajlagos árcsökkenésére és elterjedésére, a további fejlesztések is már erre a hierarchiára lettek alapozva. A hálózat korábbi elemeit fokozatosan felváltják az IP technológia alá fejlesztett kommunikációs módok, mint pl. a Voice over IP, illetve más, elsősorban pont-pont között felmerülő adatkommunikációs igények IP csatornákba történő „terelése”.

Az egységes digitális hálózathoz alapvetően (de nem kizárólagossággal) a rendészeti, rendvédelmi és közigazgatási szervezetek csatlakoznak elkülönült módon, virtuális magánhálózatok (VPN – virtual private network) kialakítása útján.

A látszólagos, logikailag elkülönített rendszerek lehetőséget biztosítanak egy közös adatátviteli közeg felhasználásával (alapvetően: ORFK mikrohullámú rendszer) a független, adatbiztonsági szempontból teljesen védett alrendszerek kialakítására, melyben a menedzsment tevékenységet is saját erőforrások (műszaki-technikai, humán) alkalmazásával lehet biztosítani, függetlenül a többi felhasználótól.

Az NTG ugyan MPLS VPN (Multiprotocol Label Switching és Virtual Private Network) hálózat, ami össz-belügyi szinten transzporthálózatnak készült, és a rácsatlakozó belügyminisztériumi szervek viszonylag szabadon alakíthatják ki a transzporthálózatra épülő saját hálózatukat, jelen felépítésében a transzporthálózatban generál titkosítás nem történik. Belügyi szervként csatlakozik erre a hálózatra a Rendőrség is. A Rendőrség esetében minden kapcsolódó objektum esetében IPSEC VPN titkosítás történik.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összegezve jelen fejezetben megalkottam az egységes hálózati fogalmi alapot, mely segítségével bemutattam a kapcsolódó hálózat fogalmakat, kifejezéseket a Rendőrségi szakmai dokumentumokban, értelmeztem a Rendőrségi informatikai hálózat fogalmát. Mindemellett új tudományos eredményként megfogalmaztam a Rendőrségi informatikai

hálózat általam javasolt fogalmát szűkebb és tágabb értelemben, továbbá javaslatot tettem a rendeltetésének értelmezésére. A fejezet további részcélját teljesítve összegeztem az informatikai hálózatok alapjait és röviden elemeztem a Rendőrségi informatikai hálózatokat sajátosságaik szerint. Így többek között elemeztem a Rendőrségi informatikai hálózatának összetevőit, felépítését szolgáltatási szempontból, meghatároztam az összetevők típusait, bemutattam a Rendőrség által használt távbeszélő szolgáltatást nyújtó hálózati összetevőket, összegeztem a külső hálózati szolgáltatókat és szolgáltatásokat. Egyértelmű megállapítást nyert, hogy az elmúlt hat évben a fenti területeken teljes strukturális változások nem következtek be, így ezen elemzések fő megállapításaikban még a mai napig relevánsak.

II. A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁNAK VÉDELMÉVEL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK

A fejezet célja a Rendőrség informatikai hálózatának védelmével szemben támasztott követelmények széleskörű meghatározása. A célkitűzéseket szem előtt tartva célzottan vizsgálandó területeket különítek el egymástól a Rendőrség informatikai hálózatának védelmi határvonalain. Az első vizsgálandó terület az elvi elgondolások és a szervezet biztonsági elhivatottságának vizsgálata, röviden a biztonsági filozófia és politika meghatározása. A vizsgálandó terület tekintetében másod ízben felmérem a Rendőrség informatikai hálózatok védelmi helyzetét. A fejezet harmadik céljaként a Rendőrség informatikai hálózatának biztonságát veszélyeztető fenyegetések feltárásával és elemzésével meghatározom a biztonsági követelményekhez kapcsolódó kérdéseket. A hálózat kockázat elemzésével rendszerezem a biztonsági követelményeket meghatározó tényezőket, összegzem a körülményeket.

BEVEZETÉS

Az informatikai biztonság feltételezésem szerint mérhető és meghatározható fogalom. Az informatikai biztonság célja az informatikai rendszer azon állapotának elérése, amelyben a kockázatok elfogadható intézkedésekkel elviselhető mértékűre csökkenthetők, és ez által a vállalat üzleti folyamatainak folytonossága a lehetséges mértékben biztosított. Ez az állapot olyan nemzetközi szabványokon alapuló előírások és megelőző biztonsági intézkedések betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik. Hipotézisem szerint, ezen intézkedéseket rendszerezve meghatározható az informatikai hálózatának védelmével szemben támasztható követelmények köre, jelen esetben speciálisan a Rendőrség informatikai hálózatának tulajdonságait figyelembe véve.

Témához szorosan kapcsolódik, és alapvetően meg is határozza a Rendőrség informatikai biztonsági filozófiája és politikája kereteinek megfogalmazása. Ezen alapelvek meghatározását követően körvonalazódhat ki a Rendőrség informatikai biztonsági célkitűzései.

Annak érdekében, hogy a Rendőrségen valaha is megjelent informatikai biztonsággal kapcsolatos elvi síkú iránymutatásokat összegezni tudjam, megvizsgálom a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatát. A fogalmakat és alapelveket összevetem az ágazatot irányító szervezet Informatikai biztonsági elvi állásfoglalásaival. Az előzőekben

megvizsgált dokumentumok elvi állásfoglalásait magasabb szintű, szakmai szervezetek által meghatározott alapelvekkel összevetem, és ezzel egyben körvonalazom a Rendőrség informatikai biztonsági filozófiájának alapjait, felfedem azonosságait és különbségeit a szakmai szabályozókkal.

Áttanulmányozva az ágazati szakirányító szervezetek iránymutatásait, meghatározom a Rendőrség azon specialitásait az informatikai biztonsági politika területén, melyek egyértelműen megkülönböztetik a szakmailag irányító szervezetektől.

Összehasonlítom a szakirányító szervezetek és a Rendőrség elvárásait a Rendőrség informatikai hálózatának védelmével kapcsolatban, és megállapításokat teszek a közös célok tekintetében.

A közös célok megállapítását követően sorra veszem azokat a szakmai dokumentumokat, melyek követelményeket határoznak meg a védelem biztosítása érdekében.

2.1. A RENDŐRSÉG INFORMATIKAI BIZTONSÁGI FILOZÓFIÁJA ÉS POLITIKÁJA KERETEINEK MEGFOGALMAZÁSA, INFORMATIKAI BIZTONSÁGI CÉLKITŰZÉSEI

A Rendőrség Informatikai Biztonsággal kapcsolatos témakörben meg kell vizsgálni, hogy milyen dokumentumok állnak rendelkezésre, amelyek meghatározóak az informatikai védelem területén. Ennek érdekében sorra vettem a szakterületet érintő hivatalos ajánlások közül az ISO 1779:2002 szabvány, a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 8., 12., 13., 16. és 17. számú ajánlásai, továbbá a 25. számú Magyar Informatikai Biztonsági Ajánlása, a Közigazgatási Informatikai Bizottság 19. számú ajánlása - alkalmazva a COBIT és az ITIL módszereket-. Ezeket az ajánlásokat dolgozta fel a Belügyminisztérium (a továbbiakban: BM) ágazati szinten meghatározott normatívában a 21/2011. (VIII. 11.) BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról követelményrendszerében is. A Rendőrségi normatívák között a biztonságpolitikai témakörre vonatkozóan konkrét jogszabályi előírást és hátteret nem leltem fel. További irodalomkutatást végeztem a Rendőrségi informatikai szakterület képviselői által készített publikációk és vélemények között. Egyértelműen megállapítást nyert, hogy a Rendőrségen folyamatban van megfogalmazásra a Rendőrség informatika politikai elvárási és filozófiai megállapításai, informatikai biztonsági célkitűzései.

Ezekből az okokból alap érvényűnek vettem a 21/2011-es BM utasítást, mint szakmai dokumentumnak, továbbá az informatikai biztonsággal foglalkozó területeket vizsgáltam a Rendőrségnél.

Adatkezelőként és Belügyminisztérium alá rendelet szervezetként a Magyar Rendőrségnek meg kell felelnie az Információbiztonságáról szóló 2013. évi L. törvénynek ,illetve a módosításáról szóló 2015. évi CXXX. törvénynek. (A módosítások 2015. július 16-án léptek hatályba.)

Az információbiztonsági törvény felülvizsgálatával párhuzamosan a Kormány, valamint a Belügyminisztérium elvégezte a végrehajtási rendeletek felülvizsgálatát is.

Ennek eredményeként a következő új Rendőrség működését érintő jogszabályok léptek hatályba:

- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

Az információ biztonsági törvény fontosságát az adja, hogy a hatálya alá tartozó szervezetek és adatkezelők működési folyamatait határozza meg, szemben a korábbi biztonsági intézkedéssel történő kiegészítési megközelítésekkel. Az IBT fontos elvi eleme, hogy a fokozatos megközelítésre, illetve a szükséges szint elérése után a fejlesztésre koncentrál, így szemben a merev szabályokkal összhangban van a valós folyamatokkal. A törvény végrehajtását megkönnyíti,hogy az ISO 27001 szabványra és az ITIL ajánlásokra épül.

Nemzetközi jogszabályok szintjén nagymértékű változás az új általános Uniós adat rendelet, a GDPR (General Data Protection Regulation) ,melynek 2018. május 25-től hatálybalépésétől szükséges megfelelni minden uniós állampolgár adatát kezelő szervezetnek. (EU országai esetében ez azt jelenti, hogy nem csak a többi tagállam lakosairól tárolt információk estében, hanem a nemzeti adattárnál is meg kell felelni az új előírásnak)

2.1.1. AZ INFORMATIKAI BIZTONSÁG FOGALMAI ÉS ALAPELVEI A RENDŐRSÉGNÉL

A 21/2011. (VIII. 11.) BM utasításban megfogalmazottak szerint: „Az informatikai biztonság politika egy iránymutatás, a szervezet és tagjainak az informatikai biztonsághoz elvárt viszonyulása, amely az érvényesítés alapelveit fogalmazza meg egységes szemlélettel és az intézmény egészére vonatkozóan."[16]

Ezzel a meghatározással összevetettem az ITB 12-es 2. Fejezetben A Biztonságpolitika meghatározása alfejezetben, rögzített „biztonság politika" meghatározását.
„Az államigazgatásban és az országos hatáskörű szervezetek kezelésében, valamint felügyeletükben működő és ezen szerveket kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára, bizalmas jellegére és biztonságára vonatkozó, ún. adatvédelmi törvényeknek megfelelően kell üzemeltetni. Ezek alapján a törvényesen védett adatokra vonatkozóan olyan védelmi eljárásokat kell alkalmazni, amelyek ellenőrizhetővé teszik a cselekményeket, lehetővé teszik az illetéktelen cselekedetek felderítését és a felelősök megállapítását.

Az informatikai rendszerekben az előbbieken kívüli adatot, információt és egyéb szellemi tulajdont a szervezet számára jelentkező értékével arányosan kell védeni az illetéktelen betekintéstől, a módosítástól, a megsemmisítéstől és a nyilvánosságra kerüléstől. A védelemnek 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.

Az informatikai biztonság rendszere olyan legyen, hogy minimális adminisztratív terhet jelentsen, az alkalmazottaktól ne igényeljen aránytalanul nagy erőfeszítést, csak amelyet a helyes munkavégzés gyakorlata során elvárhatunk. Elsősorban abban nyújtson támogatást, hogy állapítsa meg a kivételes eseteket és biztosítsa a normálállapotra való visszatérést a kivételes esemény leküzdése után." [17]

A két leírást ebben a formában a Rendőrségi normatívák között nem találtam, de a meghatározások tartalmi jegyeit nyomokban felleltem a BM iránymutatásaiban is.

A vizsgálat iránymutató dokumentumok szerint egyöntetűen rendelkeznek arról, hogy az informatikai biztonsági kérdések tekintetében a bizalmasság, sértetlenség és rendelkezésre állás alapelveit kell érvényesíteni. A vizsgálat tapasztalatait alapelvekbe szedtem, melyeket az alábbiakban összegezném:

*a) „*Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.”[18]

*b) „*Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.”[18].

*c) „*Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.”[18].

Az alapelvek és meghatározások mentén megvizsgáltam a Rendőrségi ideiglenes informatikai biztonsági szabályzatot, melyben az informatikai biztonság megteremtése érdekében rejtetten kivehetők a védelemmel szemben támasztott követelmények, mint politikai elgondolások, melyek az alábbiakban foglalok össze:

a) törvényesség biztosítása,

b) hitelesség biztosítása,

c) azonosítással hitelesítés,

d) elszámoltathatóság kialakítása,

e) hozzáférés-szabályozás,

f) jogosultság kiosztás és annak ellenőrzése,

g) auditálhatóság logikai védelmi funkcióinak megteremtése,

h) bizonyítékok rendszerének és folyamatának kialakítása,

i) a hibákat elsősorban nem kijavítani, hanem megelőzni kell.

A fenti politikai szintű elgondolás során véleményem szerint olyan védelmi eljárásokat is kellene megfogalmazni és alkalmazni, amelyek garantálják a hatékony működését, abban az esetben is, ha egy szervezetét katasztrófa éri. Ezen meghatározást, vagy ráutalást a rendészeti normatívában nem találtam.

A jelenlegi Rendőrségi működésben a katasztrófa kezelés technikailag részlegesen valósul meg, elsődlegesen 112 rendszerében, a Robotzsaru rendszerben és a telefóniában. Az informatikai adatbázisok terén a kritikus rendszereknél van törekvés a tartalék és földrajzilag elosztott megoldásokra, de a jelenlegi megvalósulás szintjén vannak olyan rendszerek és csomópontok, amelyek hibája országos szolgáltatás, vagy szolgáltatáscsoport kiesését eredményezheti,ezért szükséges a nemzetközi sztenderdekkel és az ITB-vel összhangban alapvető tényezővé tenni a rendszerek minimum két fizikailag elkülönült helyszínre.

Álláspontom szerint, a földrajzilag elkülönült katasztrófa site-al kiegészítve a követelményeket, a védelemnek biztosítania kell az informatikai rendszer megbízható üzemét fenyegető káresemények elhárítását, és hatásuk minimalizálását a megadott biztonság követelmények szintjén.

A vizsgált dokumentumok körét szélesítve, kitértem a Széll Kálmán tervben megfogalmazottakra, így a Nemzeti Adatvagyon védelmének elsődlegességét tartottam szem előtt. Következtetésként a két dokumentum feldolgozásával egy alapvető cél fogalmazódott meg, mely szerint - mind számítógépes adatátviteli, mind telekommunikációs - belső infrastruktúrájának üzemeltetési és felügyeleti feladatainak ellátása során minden esetben az önellátásra kell törekedni.

Ezek alól kivételt képeztek a Rendőrségen kívüli, külső személy által biztosított szolgáltatások, ahol a külső személy nem kerül kapcsolatba a szervezet adatvagyonával és azon adatvagyonok köre, melyeknél a külső személyt törvény határozza meg. A közös használatú és külső adat vagyonok esetében összhangba kell hozni az érintett szervezetek adatbiztonsági szabályait és felelősségeit. A többszereplős adatkezelésénél a biztonság feltétele az átadási pontok és szabályok pontosan rögzítése.

A fentieket összegezve az informatikai biztonság politikának a Rendőrségnél alapvetően meg kellene határoznia az informatikai rendszerekben előállított, tárolt, használt és továbbított információk elégséges biztonságának megteremtéséhez szükséges intézkedéseket.

2.1.2. A RENDŐRSÉGI INFORMATIKAI BIZTONSÁG FILOZÓFIA

A biztonság politikai elgondolások kutatását követően az informatikai biztonság következő lépcsőfokát vizsgálva megkezdtem a Rendőrségi informatikai biztonsági filozófia felkutatását a vizsgált dokumentációk körében. Feltételezésem szerint a Rendőrségi informatikai biztonság filozófia a Rendőrség vezetőinek és informatikai szervezetének nyilatkozatának kell

lennie arról, hogy a maximális informatikai biztonság megteremtésére törekednek.
Ennek nyomán, tovább feltételeztem, hogy az informatikai biztonság területén a Rendőrségnek egy olyan teljes körű biztonság szabályozó rendszer kialakítása a célja, ami hosszú távon felöleli az informatikai célkitűzéseit. Továbbá meghatározza, hogy kiket és hogyan szolgál az informatikai biztonság rendszer kialakítása során, milyen kiterjedtségű, és milyen mélységű intézkedéseket alkalmaz, valamint hogy mindezek segítségével milyen biztonsági szintre juttatja el az adott intézmény informatikai rendszerét. Kutatásaim alapján, megfogalmaztam a Rendőrségi informatikai biztonsági filozófiát, melyet az alábbiakban összegzek:

Az informatikai biztonság filozófiának 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. Ezen elvárások képezik majd alapját a biztonságos környezet megteremtéséhez szükséges emberi feltételrendszernek.

Az informatikai biztonság filozófia megfogalmazásával az alábbi informatikai biztonsági célok körvonalazódtak ki:

- Létrehozni a biztonságos informatika iránti igény általános légkörét, a megkívánt informatikai magatartást.
- Igazodási pontként szolgálni a munkatársak számára az elérendő informatikai biztonság célok és az alkalmazott informatikai rendszer lehetséges fejlesztési irányait illetően.
- Ezen az általános informatikai biztonsági célokat a saját informatikai tevékenységüknek megfelelő viselkedés és felelősség meghatározására lefordítsák az alkalmazók.
- Olyan biztonság technológiai és szabályozási megoldásokat kell alkalmazni, amelyek a munkavégzést támogatják, vagy ahol ez nem lehetséges legalább a korábbival azonos munkavégzési hatékonyságot tegyenek lehetővé.

A Rendőrség kultúráját és strukturális felépítését vizsgálva megállapítottam, hogy az informatikai biztonság filozófiának szoros kapcsolatban kell lennie a szervezeti kultúrával és meg kell alapoznia a biztonságpolitikáját és a stratégiát. Álláspontom szerint ezek az értékek fejezik ki a Rendőrség informatikai biztonság jellemzőit.

Strukturális felépítés vizsgálatának eredményeképpen arra a következtetésre jutottam, hogy az informatikai biztonság megteremtése elsődleges vezetői feladatnak mutatkozik. A hatékony és

megbízható informatikai rendszert (és ez a Rendőrség minden szakterületére elmondható) csak megfelelő szabályozással, és annak betartatásával lehet elérni. Az informatikai vezetők elmondása szerint megfelelően dokumentált és szabályozott rendszert lehet üzembe helyezni, reprodukálhatóvá és javíthatóvá tenni. Ezeket az álláspontokat, viszont egy filozófiai elgondolásba kellene megjeleníteni.

2.1.3. A RENDŐRSÉG INFORMATIKAI BIZTONSÁG POLITIKÁJÁNAK CÉLJAI

Az államigazgatási szervek biztonságpolitikájának elemzéséhez és meghatározásához azok alapfeladataiból, illetve az azokat gátló, veszélyeztető hatásokból kell kiindulni. Ezen körbe tartozik a Rendőrség is, ezért a célok kutatásában ebből az alaptételből indultam ki.

Alapfunkcióik a kormány képviseletében a nemzetgazdaság normális működésének biztosítása és továbbfejlesztése, az instabil helyzetek kialakulásának megelőzése, illetve azok kezelésének megoldása megfelelő döntések, intézkedések meghozatalával, a legfontosabb alapfeltételek megteremtésével. E tevékenységek együttesét az Alkotmány, számos törvény (pl. költségvetési törvény, államháztartási törvény stb.) és jogszabály szabályozza. Az alapfunkciók realizálása érdekében az államigazgatási szervek az alábbi alapfeladatokat hajtják végre:

- irányítás,
- engedélyezés,
- ellenőrzés,
- felügyelet,
- érdekvédelem,
- érdekképviselet,
- koordináció,
- szabályozó, kodifikáció-előkészítő tevékenység,
- befolyásolás.

Ezen alapfeladatok megjelennek a Rendőrségi feladatok között is. Az alapfeladatokat összevetve, a politikai és filozófiai elgondolással, melyet a korábbiakban feltártam, megfogalmaztam a Rendőrségi informatika biztonság politika célját: a Rendőrség informatikai rendszerei által kezelt adatok és információk bizalmasságának, hitelességének, teljességének, sértetlenségének és rendelkezésre állásának biztosítása.

Ehhez a vizsgált dokumentumokat figyelembe véve és a strukturális felépítését a

Rendőrségnek szem előtt tartva összefoglaltam azokat a szegmenseket, melyeknek a védelem során érvényesülniük kell:

- Irányelveket kell meghatározni az informatikai biztonsági feladatok összehangolt, tervszerű végrehajtásának biztosítása érdekében.
- A Rendőrségen belül az informatikai biztonsággal kapcsolatos felelősségi köröket el kell különíteni az informatikai rendszereket működtetőktől és a kiszolgáló szervezetek informatikai üzemeltetéssel kapcsolatos egységeitől, és ezeket együttműködési dokumentumokban kell rögzíteni.
- Széles körű útmutatást kell adni az érintett vezetőknek az informatikai biztonságot érintő döntések meghozataláról és következményeiről (minden területén a Rendőrségnek).
- Egységes információtechnológiai biztonsági követelményeket kell megfogalmazni, melyeknek érvényesülnie kell a külső felekkel szembeni elvárások során is.
- Az informatikai biztonsággal kapcsolatos jogszabályi kötelezettségeknek, nemzetközi és hazai szabványoknak és ajánlásoknak magas szinten kell megfelelni.

A megvizsgált dokumentumok a közigazgatási intézmények területére az általános biztonságpolitika megfogalmazását az ITB 12-es határozta meg a legtalálóbban:

„Az intézmény területén és kezelésében működő kommunikációs és informatikai rendszerek tervezésére, bevezetésére, üzemeltetésére és ellenőrzésére vonatkozó feladatokat úgy kell elvégezni, hogy a rendszerek védelme a jogszabályi előírásoknak eleget tegyen, valamint a védelem hiányából eredő kockázatokkal legyen arányos.„[17]

2.2. A RENDŐRSÉGI INFORMATIKAI HÁLÓZATOK BIZTONSÁGI HELYZET VIZSGÁLATA

A politikai és filozófia síkon történt elemzéseket követve, a célok meghatározása után vizsgálatot folytattam le a jelen helyzetkép felállítására, a gyakorlat feltárására. Jelen alfejezettel célom a Rendőrség informatikai hálózatának biztonsági kérdéseinek feltárása. Ehhez több irányú, területileg és időben eltolódó elemzést kell lefolytatnom. Elsődlegesen jelen helyzetből indulok ki. A Rendőrségi informatikai hálózatbiztonságának vizsgálatához ismételten dokumentum elemzéseket folytatok le. Ezek során meg kívánom határozni a Rendőrség informatikai hálózatának biztonsági helyzetét, a lehetséges fenyegetéseit,

veszélyhelyzeteit. Ahhoz mindezeket sorra tudjam venni sérülékenység-vizsgálatokat kell, hogy lefolytassak kockázat elemzéssel. Ezek eredményeként meg tudom határozni a Rendőrség informatikai hálózatának biztonsági kérdéseit, a hiányosságokból és tapasztalatokból a követelményrendszerét, hogy a várható biztonsági szintnek és védettségnek megfeleljen.

A dokumentumok vizsgálatát kiterjesztem mind a haza szakmai ajánlásokra, mind a nemzetközi ajánlásokra. Alapvető dokumentumként fogom használni a Rendőrségi Ideiglenes Informatikai Biztonsági Szabályzatát, és az ISO/IEC 27001:2005 „A" melléklet 10.6 fejezetét, a hálózatbiztonsági követelmények tekintetében.

A vizsgálat területét korlátoztam a Nagytávolságú és helyi hálózatok biztonsági osztályba sorolásának állapotában, helyzet felmérésében, a szükséges intézkedések meglétében, az érvényben lévő előírások alkalmazhatóságában, fizikai megvalósíthatóságában.

A kutatási pontokat fogalmi szinten határozom meg:

- helyzet felmérés,
- biztonsági osztályba sorolás vizsgálata,
- intézkedések megléte,
- előírások alkalmazhatósága,
- fizikai megvalósíthatósága.

Hipotézisem szerint, a fenti pontok és az azokat övező utalások, a hálózat biztonság vizsgálati eredménye alapján meg fogom határozni a Rendőrség informatikai hálózatának biztonsági helyzetét, feltárom a lehetséges fenyegetettségét, veszélyhelyzeteit és a Rendőrség informatikai hálózatának biztonsági követelményeit.

A Rendőrség informatikai hálózatának biztonsági helyzetvizsgálata során első lépésként a dokumentumok vizsgálatát határoztam meg. A dokumentumok szakterületi vonatkozásában az informatikai hálózat biztonsággal kapcsolatos rendelkezések körét térben és időben is szűkítettem. Időbeli vonatkozásában csak és kizárólag a jelen szakirányítási időszakban 2010-óta született Rendőrség informatikai hálózat biztonságával kapcsolatos dokumentumok feldolgozására koncentráltam.

A vizsgálat további szempontrendszerét meghatározva, elkülönítettem egymástól a stratégiai szempontból fontos normatívákat és a szakmai informatikai tárgyú dokumentációkat. Ezek alapján a dokumentumok körében éles határt húztam meg, meghatároztam a Rendőrség informatikai hálózati biztonsága fölötti szakirányítói szinten keletkezett dokumentumokat, a

Rendőrség informatikai hálózatának biztonsági intézkedéseit, meghatározó dokumentumokat, a Rendőrség informatikai hálózatának biztonságát befolyásoló szakmai dokumentumait.

Feltételezem, hogy a fent megnevezett témaköröket magába foglaló dokumentumok értelmezhető szinten utalásokat tartalmaznak a Rendőrség informatikai hálózatának biztonságával kapcsolatosan. A dokumentumok vizsgálatával célom felkutatni azon pontokat, ahol ráutaló szakmai meghatározásokat találhatunk a Rendőrség informatikai hálózatának biztonsági helyzetére vonatkozóan.

A dokumentum kutatásaim első lépéseként igyekeztem olyan normatívákat felkeresni, amelyek a rendészeti informatika témakörben érinthetik a kutatás témáját. Az alábbi törvényeket és törvényerejű rendeletekben vizsgáltam meg az információ védelem területi vonatkozásait és a hozzákapcsolódó adatvédelemi vonatkozásokat kutatva:

- 2009. évi CLV. tv a minősített adat védelméről,
- 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,
- 218/2011. a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól,
- 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól,
- 92/2010. Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól,
- 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről,
- Az adatvédelemmel, és az információ védelemmel kapcsolatos normatívák körében,
- 2010. évi CLVII. tv. a nemzeti adatvagyonról,
- 38/2011. Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról,
- 2011. évi CXCVI. tv. a nemzeti vagyonról,
- 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról,
- 2010. évi CLXXXV. tv. a médiaszolgáltatásokról és a tömegkommunikációról,
- 2003. évi C. tv. az elektronikus hírközlésről,
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,

- 65/2013. (III.8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendeleteként,
- 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”,
- 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,
- 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról”,
- 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben, illetve a módosításáról szóló 2015. évi CXXX. törvényben, meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről.

Második lépcsőfokként, fontosnak tartottam az ágazati szintű informatikai védelmet meghatározó normatívák áttekintését. Ezek közül kiemelném az alábbiakat:

- 1277/2010. Korm. határozat a kormányzati informatika konszolidációjához szükséges intézkedésekről,
- 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról,
- 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról,
- 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról,
- 8/2009. KHEM utasítás a Közlekedési Hírközlési és Energiaügyi Minisztérium Információbiztonsági Szabályzatáról, mely már a Nemzeti Jogtár hatályos részében nincs, de vonatkoztatható volt.
- 23/2013. (V.17.) ORFK utasítást a belső adatvédelmi és adatbiztonsági szabályzatról,
- 45/2013. (XI.15.) ORFK utasítást az internethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer Rendőrségi igénybevételének szabályairól.

A fent megvizsgált dokumentációk érintik az informatikai hálózatbiztonság tárgykörét, összefüggésbe hozhatók a Rendőrséggel, de egyértelműen egyik sem rendelkezik semmilyen meghatározással a Rendőrség informatikai hálózat biztonságának követelményrendszerire

vonatkozó meghatározásokkal. Az új Informatikai Biztonsági Szabályzat kidolgozás alatt áll, melyben ezeket a követelményrendszerek is rögzítésre kerülnek.

Biztonsági rész intézkedéseket találtam 23/2013. (V.17.) ORFK utasítást a belső adatvédelmi és adatbiztonsági szabályzatról, továbbá a 45/2013. (XI.15.) ORFK utasítást az internethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer Rendőrségi igénybevételének szabályairól szóló normatívákban, amelyek már jó alapjai lehetnek a követelmény rendszernek, de nem képezik azok egészét.

Ezen eredmény tudatában áttekintettem, azokat a szakmai előírásokat, amelyek alapján a vizsgálatot lefolytathatom és a korábban meghatározott pontokra pontos képet tudok alkotni. Sajnos a fent nevezett időkorlátban nem keletkezett olyan szakmai irányt mutató anyag, mellyel a vizsgálatot tovább tudtam volna folytatni. Ezért a fent említett dokumentumok szakmai forrásait kutattam fel. Egyértelmű be tudtam azonosítani azokat nemzetközi és hazai szabványokat, melyeket a Rendőrségi informatikai hálózatának biztonsági helyzeti vizsgálatára alkalmazni tudok. Ezek közül az alábbiakat kívánom a vizsgálat során felhasználni:

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

A nemzetközi szabványok közül:

- ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok,
- ISO/IEC 27001:2005,
- ISO/IEC 27001:2013.

Az alkalmazhatóságuk szempontjából néhány szóban összefoglalta a KIB 25. Ajánlás a szabványok fontosságát, melyből az alábbiakban idézek:

„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) 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.

A MIBIK az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 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."[1]

A Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS) „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."[20]

Az informatikai biztonság kérdésével számos szabvány és ajánlás foglakozik. Gyakran hivatkoznak e területen az ITIL1-re és a COBIT2-re. 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 szabványt használja hivatkozásként, amikor a létező ITIL folyamatokat bővíti a biztonságirányítással.

Az ITIL folyamatos fejlődésével különösen alkalmassá vált a Rendőrségi alkalmazásra, mert egyre inkább szolgálja az alapfolyamatok informatikai rendszerbe integrálását, illetve a folyamatos megközelítés és fejlődés már nem csak lehetőség, hanem az alapkoncepció része az aktuális ITIL v3-ban. [9]

---

9 https://www.google.hu/search?q=itil+v3&client=firefox-b-ab&dcr=0&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwjr3_S5r4nYAhUoAcAKHcs4CKkQsAQIRw&biw=1920&bih=927#imgrc=lX0HjLlIU2B52M

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) 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) 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(Legfrissebb elérhető verziója az MSZ EN ISO/IEC 27002:2017) 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."[21]

ISO/IEC 27001:2013 szabvány a ISO 27000-es szabványcsalád legfontosabb szabványa mely felülírja és érvényteleníti az ISO/IEC 27001:2006 szabványt. A szabvány rögzíti azt a fontos elvet, hogy az információbiztonsági irányítási rendszer (IBIR) a szervezeti folyamatoknak és az általános irányítási struktúrának része. Ez a szabvány követelményeket határoz meg a szervezeti környezetben egy információbiztonsági irányítási rendszer kialakítására, bevezetésére, fenntartására és folyamatos fejlesztésére, továbbá követelményeket tartalmaz az információbiztonsági kockázatok felmérésre és kezelésre is. Az „A" melléklete táblázatos formában összefoglalja azon intézkedéseket és szabályozási célokat, melyekből összerakható egy IBIR.

A ISO27001:2013 szabvány összhangban az ITIL v3-al logikájában magában hordozza a fejlődést, vagyis nem azonnal kell teljesíteni egy optimális szintet,hanem folyamatban gondolkodik amellyel egy alapszinttől fokozatosan el lehet érni egy jó szintig, majd pedig szervesen tovább fejlődni. Ez az elgondolás nem csak élővé teszi a biztonsági követelmény rendszert, de lehetőséget biztosít arra, hogy technikailag és pénzügyileg teljesíthető elvárás kerüljön megfogalmazásra. A nemzetközi tapasztalatok szerint a korábbi rugalmatlanabb elvárások sok esetben sziget megoldásokat, illetve elvben teljesülő, de a gyakorlati biztonságot nem megvalósító kényszer megoldásokat eredményeztek mind az üzleti, mind az állami szférában.

2.2.1. A RENDŐRSÉG NAGYTÁVOLSÁGÚ INFORMATIKAI HÁLÓZATA - KOMMUNIKÁCIÓS HÁLÓZAT HELYZETVIZSGÁLATA

A jelenlegi országos kommunikációs hálózat, a Rendőrség jelenleg IP (L2,L3 szinten) alapú hálózatot használ. Az NTG kapcsolattal rendelkező bármelyik szervezet egységtől titkosított IPSEC csatornán tud kapcsolódni a Rendőrség informatikai (intranet) hálózata.

A gerinc hálózat fizikailag alapvetően az MVM Net optikai hálózata, amelyet a NISZ Zrt. hálózat használati szerződés alapján vesz igénybe. A gerincből kilépő adatátadási pontoktól a NISZ Zrt. L3-as szolgáltatást ad, NTG néven a kormányzati felhasználók számára.

A szervezetek forgalmait zárt VPN különíti el egymástól. Az adatcserét szabályozottan tűzfal

rendszerek és a Rendőrség esetében tikosított csatornák biztosítják.

Az internet elérés a szervezetek részére egy kilépő ponton biztonságosan, felügyelten történik meg.

A Rendőrségi VPN-ben a Megyei Rendőr Főkapitányságok 1 Gbps sávszélességen, a városi Rendőr Kapitányságok 100 Mbps-on kapcsolódnak az NTG-hez. Néhány „kisebb" telephelyen, (például KMB) 10 Mbps-os vagy annál kisebb a felhordó kapcsolat sávszélessége. A kapcsolatok többsége optikai kapcsolat, de főként a kisebb és a nagy városoktól távol eső helyszíneken mikrohullámú eszközök biztosítják a gerinchálózati kapcsolatot. (A NISZ és így a Rendőrség Vezeték nélküli gerinchálózati szolgáltatója elsődlegesen az Antenna Hungária Rt.)

A Rendőrség számára biztosított sávszélességek kihasználható nettó kapacitása a fizikai csatorna és/vagy az aktív eszközök kapacitása, illetve beállítása miatt nem minden esetben éri el az adott kapcsolatoknál elvárható szintet. Ennek megoldására a NISZ folyamatos fejlesztést végez, illetve ahol szükséges a Rendőrség a titkosítást, szűrést és fogadást végző eszközeinek cseréjével csökkenti a szűk keresztmetszeteket. A tapasztalatok alapján általános projekt tervezési probléma, hogy a fejlesztések tervezésekor nem, vagy csak érintőlegesen foglalkoznak a projekt adatforgalmi és WAN hálózatbiztonsági kihatásaival. Ennek következtében a megoldás keresés csak akkor kezdődik meg, amikor az adatcsatornák telítődése miatt a szolgáltatás megbízhatóság leromlik. A megoldás pedig a kevésbé lefedett területeken fizikai (technikai) nehézségekbe ütközhet, illetve nagyadat mennyiségű és erősen központosított rendszerek esetében a hálózati fejlesztés járulékos költség igénye az alapberuházáshoz hasonló volument jelent, ami betervezés hiányában hibás ár/érték számításokat és forrás hiányt eredményeznek.

A Rendőrség speciális célra és a helyszíni munka támogatására mobil (2,3,4G és kormányzati LTE) internet,illetve VPN kapcsolatokat is használ. Nagy technikai és biztonsági kihívás, hogy a végrehajtó állomány közterületi munkavégzés során és gépjárműben is számára optimalizált informatikai rendszeren tudjon dolgozni. A pénzügyi lehetőségek és a társadalmi szükségszerűség miatt a saját tulajdonú eszközök munkára történő használata már nem üldözendő terület, hanem hatékony stratégia. Természetesen a privát és munkacélú közös használat feltétele a megbízható BDM technológiák kiválasztása és implementálása mind műszakilag, mind szabályzati szempontból.

Léteznek nemzetközi kapcsolatok, amik vagy az NTG internetes kijáratán, vagy bérelt (illetve virtuálisan bérelt) vonallal kezelődnek le.

Egyeztetéseket végeztem az ORFK szakmai képviseletével, és a Nemzeti Elektronikus Információbiztonsági Hatósággal a Rendőrségi nagytávolságú informatika hálózat biztonsági osztályba sorolásának tekintetében. Egyértelmű megállapítást nyert, hogy a nyílván tatásba vett informatikai szakrendszerek besorolásra kerültek.

2.2.2. A RENDŐRSÉG LOKÁLIS (HELYI) INFORMATIKAI HÁLÓZATAINAK HELYZETVIZSGÁLATA

Valamennyi kapitányság rendelkezik számítógépes hálózattal, amik lehetővé tették rendkívül sok, a Rendőrségi szakmai munkát támogató alkalmazás fejlesztését és elterjesztését. Általános jellemzőjük volt, hogy független információs 'szigetekként' működve, helyi alkalmazásokat szolgáltak ki, egymással –vagy egy központi informatikai rendszerrel - kommunikálni, adatot cserélni nem vagy csak részlegesen tudtak.

Az ORFK Központi szoftver fejlesztési részlegének kiemelt kezelésével és az egy központi rendszerbe (Robotzsaru NOVA) történő integrálási folyamatával a szigetszerűség jelentősen csökkent, a folyamat hátránya, hogy a szolgáltatások feladat orientáltsága, kezelhetősége sok esetben romlott, a munka nehézkessé vált. Tehát az integráció szükségszerű, de a forszírozott megvalósítás és a nem megfelelő megoldások hátrányokkal járnak. Koncepcionálisan a szabványos egymással adatot cserélő integrált belső és külső rendszerek jelenthetik a megoldást, amelynek a felső megjelenítési és jogosultsági rétege akár közös is lehet.

A Teve utcai RIK, már a kezdetektől informatikai központi szerepkört kapott és a gyakorlati kiépítésének is köszönhetően ebben az épületben egységes és integrált informatikai infrastruktúráról beszélhetünk. A jelenleg egy központú struktúra egyben nehezen kiszolgálható aggregált hálózati (átviteli, adatszűrési és titkosítási) kapacitás igényt jelent, egyben működés folytonossági kockázatot is. Tehát a RIK esetében nagyon fontos lenne a már a 2.1.1 pontban felvázolt katasztrófa site koncepció mielőbbi megvalósítása.

Nagyon fontos kihívás a Rendőrség számára, hogy a Belügyminisztérium stratégiája alapján a felhő alapú szolgáltatások kialakítása van folyamatban. A BM célja, hogy minden kritikus szolgáltatást a Kormányzati Adat Központban (KAK) egyesítse amint műszakilag, illetve pénzügyileg a végrehajtás kivitelezhető lesz. Minden Kormányzati Adat Központba (KAK) megvalósításában adatbiztonságilag nagy nehézséget fog jelenteni a rendszerek harmonizálása

és átmozgatása. Technikai szempontból pedig a megfelelő megbízhatóság és elérhetőség a logikailag közös, de fizikailag regionálisan elosztott struktúra jelenthet jó megoldást. A méretében optimalizált központokból álló elosztott rendszerek további előnye lenne, hogy megfelelő méretezéssel és a virtualizálásra is építő technológiával egyszerre lenne biztosítható a gyors magas tranzakció szám és a megbízhatóság dinamikus katasztrófa siteok általi biztosítása. A KAK kialakításával a RIK szerver termeiben költséghatékonyan lehetne lehelyezni (elsősorban a Rendőrség által használt) rendszerek katasztrófa sitejait, illetve az elosztott struktúra elemeinek egy részét.

A jelenlegi Rendőrségi rendszerben központi szolgáltatásokat érhetnek el a felhasználók, mint feladat specifikus programok (például Robotzsaru), levelezés, nyomtatás stb. Ezek a szolgáltatások windows, linux, unix és egyre csökkenő mértékben Novell platformokon futnak. A menedzselhetőség és a munkavégzés folyamatossága érdekében a régebbi fejlesztésű rendszerek cseréjükig, illetve kiváltásukig virtualizált blade szerver farmokra kerülnek átmozgatásra. Az új rendszerek esetében a megbízhatóság és a skálázhatóság érdekében nagymértékű a virtualizált környezet alkalmazása. Néhány speciális rendszert kivéve megtörtént az adatok központi SAN rendszerre történő átmozgatása. Szoftveres oldalról a fő irány, hogy minden szakrendszer váljon a Robotzsaru keretrendszer részévé. A Robotzsaru rendszer egy központi Oracle EXADATA infrastruktúrára épül, melyhez további alrendszerek és a központi NAS hálózat egészít ki.

A központi szolgáltatások a megyei főkapitányságokon, és városi kapitányságokon is elérhetőek, de kiegészülhetnek regionális szervereken futó szolgáltatásokkal is. Multifunkciós eszközökön, központi nyomtatás történik.

Minden olyan számítógépen, amely alkalmas rá minimum Windows 7-es operációs rendszer fut. A Windows 10 is megjelenését követően némi tapasztalati időt követően az új számítógépek ezen operációs rendszerrel kerültek beszerzésre. is. A régebbi klienseknél is megkezdődött az áttérés, de még a kötelező átállásra nem történt intézkedés. A főként Európai uniós forrásokra támaszkodó eszköz cserék eredményeként a kiemelt és központi szervezetek, így a BRFK is jelentős munkaállomás cserén esett át. Így a műszaki feltételek adottak a korszerű és biztonságos feladat végrehajtáshoz, feltéve, ha az lekövetkező években is legalább 20-30%-os munkaállomás csere fog történni. A kevésbé frekventált területeken, főként a vidéki kisebb kapitányságokon és őrsökön 3-5 évnyi eszközcsere elmaradására is szükség lehet a hatékony és biztonságos munka környezet megteremtéséhez. A speciális feladatok ellátását jelentős mennyiségben járműbe épített és kézi eszközök (telefonok, tabletek) támogatják, windows és Android-os operációs rendszerrel.

Fontos eredmény, hogy elkészítésre került a mobil eszközök Rendőrségi használatának

fejlesztési koncepciója. A koncepció eredménye, hogy egyértelmű keretet ad a kézi, hordozhatós és járműben elhelyezett eszközök alkalmazásának és a koncepcióban a biztonság kezelése is helyet kapott. Fejlesztési praktikum a céleszközökben az Android platform preferálása, amely azonban magában rejti ismét az egyplatformúság technikai és biztonsági kockázatát, figyelemmel arra, hogy korábban néhány mobil alkalmazásnál a beágyazott windows platform kizárólagossága miatt több évig magas áron, nem optimális műszaki paraméterű eszközök beszerzésével volt biztosítható a tovább működtetés.

Az elkészült koncepció keretei között a közeljövő jelentős kihívása mind műszaki, mind biztonsági szempontból a hordozható eszközök komplex szolgáltatási és biztonsági menedzselésének a megoldása.

Az ORFK szakmai dokumentumainak vizsgálatai eredményeképpen az alábbiakat állapítottam meg:

- Biztonsági osztályba sorolás vizsgálatának újbóli felülvizsgálata még nem fejeződött be, a nagytávolságú informatikai hálózat részekre bontása során, a helyi hálózatok biztonsági kategorizálása csak alapszinten és a speciális célú hálózatoknál történt meg. A biztonsági osztály besorolás pedig még nem fejeződött be.
- Találtam a NISZ mint KEKKH jogutódjának irattárában hálózat kábelezési rajzokat, melyek minősített iratok, így azokat a kutatás során nem tudtam felhasználni.
- Kizárólagosan, a Rendőrség informatikai hálózatának biztonságát szavatoló előírást, utasítást biztonsági intézkedések az irattárban nem voltak fellelhetők. Csak általános érvényű utalásokat találtam a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatában és alapvető meghatározásokat az üzemeltetési szabályzatokban, ezért azok alkalmazhatóságát részletesen nem tudtam vizsgálni.
- A biztonsági fizikai megvalósítása sok helyen nem megoldott. A hálózatot a külvilágtól kívülről és az egyes szervezetek egymás között tűzfalakkal védik. A kábelezés fizikai védelme a speciális célú hálózatok kivételével, csak standard technológia kiépítés szerinti. A hír és hálózati szerver szobák falai alapvető áthatolás védelemmel és/vagy biztonsági ajtóval védettek. A beléptetés elektronikus figyelése és védelme különösen a régebbi kialakítású helyszíneken csak részlegesen megoldott, de a területi ellenőrzések során vizsgálatra kerül és a megoldásra javaslat készül.

Egyeztetéseket végeztem az ORFK szakmai képviseletével, és a Nemzeti Elektronikus Információbiztonsági Hatósággal a Rendőrségi helyi informatika hálózatainak biztonsági osztályba sorolásának tekintetében. Egyértelmű megállapítást nyert, hogy még nem kerültek minden rendszer besorolásba, folyamatban van.

A besorolás hiányában a követelményrendszer megállapítása során összehasonlító elemzést kell folytatnom a Rendőrségi Ideiglenes Informatikai Biztonsági Szabályzata, és az ISO/IEC 27001:2013 nemzetközi szabvány hálózatbiztonsági elvonatkoztatásai között. Az összehasonlító elemzés lefolytatásához elengedhetetlennek tartom a fenyegetettség források meghatározását.

2.3. A RENDŐRSÉGI INFORMATIKAI HÁLÓZATOK LEHETSÉGES TÁMADÁSI CÉLPONTJAI

Mindenki, aki informatikai hálózattal rendelkezik (legyen a nagyvállalat, vagy egy kisebb vállalkozás) a legfontosabb számára hálózatának biztonsága. Miután a hálózatunkon lévő információ számunkra nagyon sok pénzbe kerül, így néha gondolkodás nélkül temérdek pénzt fordítunk annak védelmére. A szoftver- és hardver piacon a biztonsági cégek megszámlálhatatlan sok védelmi megoldással bombáznak minket. Ezek a védelmi megoldások átláthatatlan útvesztőbe terelnek be minket. Ezért kutatásokat folytattam, hogy mit kell védenünk, ha a hálózatunkat szeretnénk megvédeni, és egyáltalán milyen megoldások jöhetnek szóba.

Kutatásaimat a piacon fellelhető termékek vizsgálatain folytattam le. Egy nagyvállalati hálózaton, mint a Rendőrség informatikai hálózatán a biztonság szempontjából azokat a pontokat mutatom be, ahol a lehetséges összes támadási felület előfordulhat. Ezért olyan kritikus célpontokat határoztam meg, melyeket mind a már meglévő informatikai hálózatnál, mind egy fejlesztendő informatikai hálózatnál, vagy újonnan építendő informatikai hálózat védelménél figyelembe kell venni.

Jelen fejezetben második célom a Rendőrség informatikai hálózat biztonságát, fenyegető támadásokat feltárni. Rendőrségi pályafutásom során tapasztaltakat figyelembe véve, tipizálni kívánom a feltételezéseim szerint várható támadás fajtákat a teljesség igénye nélkül és megoldási javaslatokat teszi ezek felfedésére, esetleges megoldására. Ezek olyan lehetséges támadási célpontok, melyek bármely nagy vállalati közegben előfordulhatnak így akár a Rendőrség vonatkozásában is.

A routerek mint célpontok

Minden informatikai hálózatbiztonsági fejlesztés kritikus elemét jelenti a hálózati átjárók (routerek layer3 kapcsolók, tűzfallal kombinált komplex eszközök) biztonsága. A hálózati

átjárók feladata[10] az informatikai hálózatok közötti hozzáférés vezérlés, az informatikai hálózatok hirdetése és a felhasználásának szűrése, és potenciálisan egy támadó leginkább használható eszközei. A hálózati átjárók biztonságossá tétele azért szükséges, hogy a közvetlen kompromitálhatóságuk esélye csökkenthető legyen. A hálózati átjárók (geteway-ek) biztonságossá tételének vizsgálatakor a következő területeket tartottam a legfontosabbaknak:

- A telnet hozzáférésének tiltása/leszűkítése vagy más, biztonságos metódus (pl. SSH) alkalmazása. Rendőrségnél a kritikus központi és regionális eszközök szintjén ez megvalósításra került.
- A router SNMP hozzáférés leszűkítése és biztonságos beállítása.
- A router hozzáférés csak TACACS+ használatán keresztül történhessék. (Rendőrségnél a kritikus központi és regionális eszközök szintjén ez megvalósításra került.)
- Szükségtelen szolgáltatások kitiltása.
- Routing update-ek autentikációja.
- Biztonságosabb Switching funkciók[11] engedélyezése az átjáró eszközökön.

A switchek mint célpontok

A routerekhez hasonlóan, mind a Layer 2, mint pedig a Layer 3 switchek esetén megtalálhatóak az azokra jellemző biztonsági követelmények.

A switchek VLAN-okat használnak a Layer 2 forgalom szegmentálására. Az ún. Private Vlan technológia alkalmazása további forgalomszegmentálást és további biztonságot szolgáltat a VLAN-on belül. A private Vlan azt szabályozza, hogy egy adott VLAN-on belül mely portok tudnak más portokkal kommunikálni. A VLAN-on belül három port típus különül el egymástól: *isolated* portot, *community* portot és *promiscous* portot. Az isolated port egy VLAN-on belül csak promiscous portokkal tudnak kommunikálni; a community portok azonos community-n belüli portokkal és a promiscous portokkal tudnak kommunikálni, míg a promiscous portok bármilyen más porttal képesek kommunikálni. Ez a megoldás igen hatékonyan használható egy adott informatikai hálózati szegmensen kompromittált hoszt esetén jelentkező támadásokkor. A biztonság tovább növelhető, ha a VLAN-ok fizikailag is külön szegmenseket kapnak és az agregációs eszközökre VLAN-oként dedikált porton kerülnek felhordásra.

10 Megjegyzés: IP csomagok route-olása
11 Megjegyzés: mint, pl. Cisco Express Forwarding

Példa, ha egy rendszer kompromittálódik

Egy olyan példán szeretném egy rendszer kompromittálódását bemutatni, amely akár a Rendőrségre is lehet értelmezni, de konkrét adatok használatával adatvédelmi szabályokat sértenék, ha Rendőrségi közegben is megtörténhető módon azonosítanám be a problémát, ezért általánosságban fogok fogalmazni.

A következő példában tekintsünk egy általános, nyilvános szolgáltatásokat nyújtó szegmenst három hoszttal: egy FTP szolgáltatással, egy Web szolgáltatással és egy DNS szerverrel. Amennyiben a DNS szerver kompromitálódik, a támadó úgy tudja továbbvinni a támadását a két másik szerver irányába, hogy nem kell ismételten áthaladnia a tűzfalon. Private VLAN alkalmazása esetén, ha egy rendszer kompromitálódik, nem tud kommunikálni a nyilvános szegmens másik két rendszerével.

A védelem második vonalának tekintendő a Dynamic Address Resolution Protocol (ARP) vizsgálat, az IP spoofing védelem, és a Dynamic Host Control Protocol (DHCP) snooping védelem.

A Layer 2 szintű kapcsolatok tiltása által a Private VLAN-ok ugyan megnehezítik az informatikai hálózati hibák keresését, de jelentősen biztonságosabbá is teszik azokat. A fenti, „A routerek célpontok” című részben ismertetett informatikai hálózatbiztonsági technikák a switchek esetében is érvényesek, jóllehet léteznek csak a switchekre jellemző informatikai hálózati támadások is. A switchek esetén a következő jól bevált technikákat és óvintézkedéseket kell figyelembe venni:

- Ha minden nem használt portot kikapcsolunk, és áthelyezzük azokat egy nem használt VLAN-ba, akkor kivédhető, hogy a támadó egy használaton kívüli portra csatlakozva az informatikai hálózat többi részével kommunikálni tudjon.
- Ajánlatos minden trönk porton dedikált VLAN ID-t használni.
- DARP vizsgálattal biztosítható egy Layer 2 szintű támadás kompromittálása a switch ARP tábláján, és ezáltal lehetővé tehető a támadó számára, hogy a switchből illetéktelen adatokat szívjon le (sniffeljen). Amennyiben a DARP vizsgálat nem alkalmazható, a Private VLAN technológiát kell alkalmazni, hogy egy adott hoszt ne tudjon informatikai hálózati forgalmat lehallgatni egy adott informatikai hálózati szegmensen.
- Ha minden felhasználói portot non-trunking módba helyezünk, akkor ezáltal megakadályozzuk, hogy egy támadó egy saját switchet kapcsolva az informatikai hálózatra, trönk módban figyelhesse a másik switch VLAN-jaiból érkező informatikai

hálózati forgalmat.

- El kell kerülni a VLAN 1 használatát menedzsment célokra, és 802.1Q trönkök natív VLAN-ja esetén.
- Ahol lehetséges, a felhasználói portokon alkalmazzunk port security-t. (A Rendőrség központi helyszínen és az új telepítésű rendszerek egy részénél már bevezetésre került.)
- Tanácsos Layer 2 port autentikációt alkalmazni[12], hogy a felhasználók az informatikai hálózathoz kapcsolódási kísérleteit autentikálni tudjuk.
- Készítsünk biztonsági tervet a lehetséges ARP biztonsági problémákra. Ez tartalmazza a DHCP lopás (snooping) és IP forrás védelmi (source guard) technikákat, melyek a DHCP starvation jellegű támadások kivédésére, míg a DARP vizsgálat a MAC cím hamisítás ellen alkalmazható.
- Ha Spanning Tree Protokoll támadások kivédésére (BDPU guard, root guard) alkalmas technikákat alkalmazunk, akkor megelőzhető a támadó által az informatikai hálózati topológiába hamisított root bridge jellegű támadás, és az abból származtatott man-in-the-middle jellegű támadások.
- Ha private VLAN-okat a megfelelő helyeken használjuk, akkor a Layer 2 informatikai hálózatot további részekre tudjuk szeparálni.
- Csak a feltétlenül szükséges helyzetekben alkalmazzuk a Cisco Discovery Protocol-t. Az ebben található információkat a támadó könnyedén felhasználhatja informatikai hálózati információk gyűjtésére, beleértve az informatikai hálózati eszközök információit, típusszámait és a rajtuk futó szoftverek verzióit is.

Lássunk egy általános példát a biztonságos változáskezelés alkalmazására: **VTP jelszavak alkalmazásával a VTP hirdetések esetén.**

A változáskezelés (konfiguráció, szoftver verziók etc), és a konfiguráció analízis tekintetében alkalmazzunk olyan folyamatokat, amelyek biztosítják, hogy a változtatás biztonságos konfigurációs metóduson keresztül zajlik. Ez igen fontos olyan helyzetekben, amikor több szervezeti csoport felügyeli - egy közös switchet, és különös jelentőséggel bír hálózatbiztonsági fejlesztések esetén, melyek igen körültekintő figyelmet igényelnek.

A változás kezelési támadás elkerülése lehet a változás kezelés statikus, manuális

12 Megjegyzés: mint pl. 802.1X

megvalósíátsa, ennek kockázata viszont hogy aktualizálás elmaradása működési és biztonsági problémákat fog okozni. Rendőrségi méretű rendszerekben, a megfelelően védett és kritikus elemeiben nagy állandóságú konfiguráció aktualizálás megvalósítása lehet alegjobb megoldás.

A hosztok célpontok

Egy informatikai hálózati támadás legvalószínűbb célpontjai mégis csak a hosztok, melyek védelme biztonsági szempontból a legkomolyabb kihívások közé tartoznak. Számtalan hardver platform, operációs rendszer és alkalmazás létezik, melyekhez időben változó módon jelennek meg update-ek, fix-ek, patch-ek. Mivel a hosztok alkalmazásszolgáltatásokat nyújtanak más hosztok részére, ezért ezek az informatikai hálózaton kifejezetten könnyen hozzáférhető erőforrások. Az ilyen jellegű könnyű hozzáférhetőség, valamint az a tény, hogy a hosztok általában is tartalmaznak kritikus adatokat, mint pl. e-mail-eket, ezek tekinthetőek az informatikai hálózati behatolási kísérletek estén leggyakrabban támadásnak kitett eszközöknek. Nagy vállalati rendszereknél ezért szükséges a fontos adatokat központilag is tárolni és egyre fontosabb az adatelhelyezés menedzselése, különösen a hordozható eszközöknél.
Részben a fent említett biztonsági kihívások eredményeként a hosztok a legsikeresebben kompromittált rendszerek. Például egy adott Internet Web szerver rendelkezhet mind-mind különböző gyártótól származó hardver platformmal, hálózati kártyával, operációs rendszerrel, és Web szerver szoftverrel. Egy adott Web szerver számos alkalmazást futtathat, melyek szabadon terjeszthetők az Interneten, és amennyiben mondjuk a szerver kommunikációt folytat valamely adatbázis szerverrel, akkor a variációk száma végtelen lehet. Mindez nem feltétlenül jelenti, hogy a biztonsági sérülékenységek a több gyártó vagy forrás alkalmazásából származik, hanem a probléma leginkább a rendszer komplexitásának növekedéséből, és ez által a hiba valószínűségének növekedéséből származtatható.

Egy hoszt biztonságossá tételéhez szükséges a rendszer egyes komponenseinek vizsgálata. Tartsunk minden rendszert naprakész szinten a patch-ek és fix-ek tekintetében. Külön figyelmet érdemes fordítani arra, hogy a patch-ek milyen hatással vannak az egyes rendszerkomponensekre. Alkalmazzuk a patcheket először teszt rendszereken, mielőtt az éles rendszereken implementálásukra kerülne sor. Ellenkező esetben egy patch alkalmazása Denial of Service támadást eredményezhet. Az operációs rendszerek biztosítása igen fontos kérdés. Egy nagyvállalati környezetben a következő feladatok fogalmazható~~a~~k meg a hosztok

biztonságossá tétele során: erős jelszavak alkalmazása, file jogosultságok javítása a megosztások tekintetében, szükségtelen informatikai hálózati szolgáltatások kikapcsolása, nem használt hálózati protokollok kikapcsolása stb.

Amennyiben lehetséges célszerű törekedni a harmonizált, kevés típusú szoftver és hardver megoldásból történő építkezésre. (Az egyetlen teljesen egyforma platform kialakítása nem csak nehezen kivitelezhető és rossz hatékonyságú, de kritikus hiba esetén a teljes rendszer kompromittálódását eredményezheti, ezért nem javasolható megoldás.) Törekedni kell a nyílt forráskódú és széles körben elterjedt megoldások használatára, mert az egyedi fejlesztésekkel a hibák kiderülésének és megoldásának valószínűsége nagyobb. Az utóbbi évtizedekben, kiváltképp az internet terjedésével hamis biztonságérzet, hogy az egyedi rendszer biztonságosabb, inkább csak a hibái kevésbé derülnek ki. Viszont a célzottan támadónak megfelelő motiváltság estén ez nem feltétlenül akadály.

Mindezeken felül győződjünk meg arról, hogy a legfrissebb vírus és hoszt betörés-megelőző (IPS) szoftverekkel rendelkezünk.

A hoszt alapú betörés érzékelő rendszerek – Host Intrusion Prevention System (HIPS) a hosztok és szerverek biztonságát oly módon javítják, hogy szabályrendszereken keresztül vezérlik az operációs rendszer és az informatikai hálózati stack viselkedését. A processzorvezérlés limitálja a buffer overflow, registry update, rendszer könyvtárak írását végző, vagy telepítést végző programok tevékenységeit. Az informatikai hálózati forgalom szabályzása segít megelőzni, hogy egy hoszt FTP kapcsolatot kezdeményezzen, vagy fogadjon, limitálhatja egy DoS támadás forgalmait, kizárhatja a hálózati stack-et a DoS támadásban való részvétel alól.

Az ilyen jellegű biztonságpolitika kikényszerítése által az IPS rendszerek hatékonyak az ún. "zero-day" jellegű támadások ellen is. Az egyedi rendszerek esetén a szabályok kialakítása nehezebb, különösen ha a dokumentációban a biztonság kezelés nem kapott megfelelő hangsúlyt. A zero-day támadások esetén a féreg, vagy vírus buffer overflow jellegű támadást indít, felülírja a registry-t, vagy éppen a rendszer könyvtár tartalmát próbálja írni. A zero-day támadás elleni védekezés azt jelenti, hogy a hosztjaink és szervereink már a támadás Internetes megjelenésének napján védettek[13], mivel az IPS szoftver meggátolja, hogy a fertőzés elérje a munkaállomást vagy a szervert.

13 Úgy, hogy az adott biztonsági beállításokat valósítják meg, és nem az adott támadás bitmintáját vizsgálják.

Az informatikai hálózatok célpontok

Az informatikai hálózatokat célzó támadások a legnehezebben kivédhető támadások közé tartoznak, mivel az ilyen támadások tipikusan az informatikai hálózat valós működését, karakterisztikáját aknázzák ki. Az ilyen jellegű támadások közé tartoznak az ARP- és MAC alapú Layer 2 támadások, snifferek és Distributed Denial of Service (DDoS) támadások. Az ARP- és MAC támadások nagy része kivédhető a switchek és routerek esetén ismertetett technikákkal. A sniffer jellegű támadások kivédésének ismertetése később történik. A DDos jellegű támadások speciális figyelmet igényelnek.

Mind a Ddos támadások elhárítása, mind a használati igényekből, mind a meghibásodásból adódó túlterhelések ellen jó védelem, ha a rendszer útvonalait, kritikus keresztmetszeteit és kapcsolóeszközeinek processzálási teljesítményét megfelelően meg, illetve túl méretezzük. Különösen magasabb szintű szolgáltatást nyújtó eszközöknél jellemző, hogy egyfajta várható terhelésre, adatforgalom és művelet kombinációra méretezik. Így a valós átbocsájtó képesség különösen a routereknél nagyságrendileg is eltérhet a beépített interfészek elméleti sebességétől. (A szükséges adatok általában némi kereséssel a gyártónál is elérhetőek, illetve mások által elvégzett, vagy saját tesztelés alapján lehet eredményekhez jutni). Jellemző tapasztalat, hogy megfelelő tartalékkal méretezett nagyobb kategóriájú eszköz jelentősen kisebb összegbe kerül, mint a kisebb eszköz esetleges szoftver és hardver bővítésekkel csak részlegesen megfelelővé tett változata. Biztonság és működés optimális megteremtésében nagy szerepet kaphat, ha az ellátandó feladathoz megfelelő eszköz kerül kiválasztásra (pl. tűzfal funkciót routerrel megoldani sok esetben pénzügyileg és biztonságilag is rossz megoldás). Nehezen megválaszolandó kérdés, hogy a meglévő eszközparkkal harmonizáló priorizált gyártó relatíve magas költségű megoldása kerüljön kiválasztásra, vagy más megfelelően bizonyított más gyártó nagyobb teljesítményű, illetve kisebb költségű eszköze. Figyelembe véve néhány gyártó pl: Cisco árpolitikáját és a biztonsági résekkel kapcsolatos hozzá állását különösen a közép és alsóbb szintű eszközöknél a megfelelő kapacitás és funkcionalitások elérésén túl biztonsági oldalról is jobb megoldás lehet az alternatív gyártókból építkezés.

A legrosszabb támadás az, amelyet nem tudunk megállítani. A “megfelelő” módon indított DDos támadás ilyen. A DDos működési elve, hogy egyidejűleg akár több száz gép küld hamisított csomagot egy adott IP címre. Az ilyen támadás célja általában nem egy adott hoszt leállítása, hanem a teljes informatikai hálózat forgalomból való kizárása vagy egy szolgáltatás megakadályozása. Tekintsünk egy E1 (2,048 Mbps) Internet kapcsolattal rendelkező szervezetet. A szervezet a site tekintetében igen érzékeny a biztonságra: van tűzfal, betörés érzékelő rendszer, loggolás és valós idejű monitorozás is. Sajnos a fenti eszközök egyike sem

nyújt segítséget abban az esetben, ha egy szervezet sikeres DDoS támadást hajt végre. Tekintsünk 100 eszközt a világban, melyek mindegyike 500 Kbps DSL kapcsolattal rendelkezik. Ha ezen eszközöket kívülről megszólítják, hogy árasszák el forgalommal az Internet router soros vonali interfészét, ekkora mennyiségű támadó eszköz felhasználásával könnyedén kiterhelhető az E1 vonal. Még ha az egyes eszközök csak 100 Kbps forgalmat generálnak is (labor tesztek alapján a legáltalánosabb DDoS eszközök több mint 50 Mbps forgalom generálására képesek általános PC gépeken), ez a forgalom elegendő a vonal ötszörös túlterheléséhez, melyez a site már nem képes lekezelni. A tűzfal ugyan eldobja a hibás adatokat, de a forgalom már kiterhelte a WAN kapcsolatot, és a kapcsolat sávszélessége felemésztésre került.
A nagy sávszélességű kapcsolatok terjedésével két probléma növeli meg a DDOS támadások eredményességét:

- Az aggregációs pontokon a javasolt megoldás, hogy a gerinc irányú sávszélesség 10x kisebb, mint a csatlakoztatott végpontoké, azonban sok szolgáltató technikai problémák miatt, illetve takarékosságból kisebb gerinc átbocsájtó képességgel rendelkezik, vagy az előfizetők növekedéséhez csak késve igazítja a központi kapacitásokat. Ez mindaddig kevéssé okoz gondot, amíg a felhasználók tipikus tevékenységet végeznek, de ha ettől letérnek, vagy támadás történik, akkor gyorsan „bedugul” rosszabb esetben működésképtelenné válik a hálózat.

- A tűzfalak és átjárok főként a költségek miatt nem DDOS-ra, hanem egyfajta várható terhelésre (csomagméret, protokollok) vannak méretezve, ezért már jóval a fizikai csatorna telítődése előtt is kifuthatnak a processzor teljesítményből, így elérhetetlenné téve a mögöttük lévő szolgáltatásokat.
A kifinomultabb támadások a 80-as (HTTP) portot használják az ACK bit beállítása mellett, ami által a forgalom legitim Web tranzakciónak tűnik. Egy informatikai hálózati adminisztrátor, az Anomaly Detecrot megfelelő módon észlelni tudja az ilyen jellegű támadást. Mivel a nyugtázott TCP kommunikáció éppen az a forgalom, melyet az informatikai hálózatunkba be akarunk engedni. A SYN flood többszörös befelé irányú kérésnek álcázódik, de a célja az erőforrások korlátozása, a legitim kapcsolatok blokkolása. Jóllehet a stateful tűzfalak és más tartalom vizsgálatot végző eszközök képesek lehetnek az ilyen régebbi támadások kivédésére, a legújabb DDoS támadások által indított kapcsoltok teljes mértékben legitim forgalmaknak tekinthetők informatikai hálózati és protokolláris

szempontból. A forrásuk általában könnyen felderíthető, de a forrás maga általában egy kompromittált rendszer, vagy egy reflektor szerepet betöltő hoszt. Tekintsünk egy Website felé irányuló támadást. Ha minden kérés megfelel a HTTP specifikációban foglaltaknak, akkor a támadás típusától lehet megkülönböztetni a legitim kérésektől.

Csak az Internet/Intranet gerinchálózati Szolgáltatóval (ISP-vel) Rendőrség esetében nagy többségben a NISZ-el való szoros együttműködés biztosítja, hogy az ilyen jellegű támadásokat kivédhessük. A szolgáltató kifelé irányú ún. rate limiting-et konfigurálhat a szervezet felé mutató interfészen. Ez a rate limit képes eldobni a nem kívánatos forgalom azon részét, amely egy meghatározott sávszélesség határt átlép. Ilyen esetben kulcsfontosságú a nem kívánatos forgalom meghatározása. Egy másik lehetőség lehet az ISP által megvalósított ún. black-hole routing. Ez a folyamat a BGP, DNS és a statikus route alkalmazásának kombinációinak alkalmazásával a káros DDoS forgalmat a router egy null interfészére irányítja - azaz eldobja – ezáltal a támadást nem engedi a célcímre - és a támadást egy más címre, vagy informatikai hálózata irányítja. Az együttműködésben komoly nehézség, hogy az igénybe vevőnek a szolgáltatótól is védeni, vagyis titkosítania kell az adatait, azonban ha a titkosítás valóban hatékony, akkor a csatornán belüli adatfajtákat a szolgáltató nem tudja megkülönböztetni és eszerint priorizálni. Tehát a védekezés jelentős részét a nagyvállalatnak, illetve kormányzati szerveknek, esetünkben a Rendőrségnek kell megoldania.

A DDoS támadások gyakori típusai az Internet Control Message Protocol (ICMP) elárasztások, Transmission Control Protocol (TCP) SYN flood-ok, vagy User Datagram Protocol (UDP) flood-ok. E-commerce jellegű alkalmazásokat futtató környezetekben az ilyen jellegű forgalmakat meglehetősen egyszerű kategorizálni. Azonban a 80-as (HTTP) portra irányuló TCP SYN támadás elleni védekezés esetén az adminisztrátor a legitim felhasználói forgalom kizárásának kockázatával kell, hogy számoljon[14]. Mégis jobb, ha ideiglenesen kizárjuk az új, legitim felhasználói forgalmakat, mintha hagyjuk elveszíteni a routert (átjárót) és elveszítünk minden kapcsolódást.

Az ilyen jellegű támadások kezelésének egy másik módja lehet az RFC 1918, és az RFC 2827 ajánlásokban megfogalmazott szűrések alkalmazása. Az RFC 1918 specifikálja mindazon informatikai hálózatokat, amelyek privát felhasználásúak és ebből következően semmilyen körülmények között nem jelenhetnének meg az Interneten. Egy az Internethez kapcsolódó

14 Anomaly Detector

router befelé irányuló forgalmán elvégzett RFC 1918 és 2827 szűrés segít megakadályozni a szervezet informatikai hálózata felé irányuló jogosulatlan hozzáféréseket. Az ún. bogon szűrés az olyan címek szűrését tartalmazza, amelyek még nem, vagy aktuálisan nem kerültek kiosztásra az Interneten. Az ilyen szűrések alkalmazásával elérhető, hogy a DDoS támadások ilyen csomagokkal történjenek, és ez által a támadás alatt sávszélességet takaríthatunk meg. Amennyiben a világon az összes ISP implementálná az RFC 2827-ben foglaltakat a forrás címhamisításon alapuló támadások nagy része nem lenne alkalmazható. Jóllehet a fent említett stratégia nem közvetlenül véd meg a DDoS támadásoktól, megvéd azonban a hamisított forrás címek alkalmazásától, ezáltal megkönnyítve a forgalom forrásának visszakövethetőségét. (A Rendőrségnél a más szervezettekkel való összetett kapcsolatok és IPSEC átvitel, miatt hasonlóan más kormányzati intézményekhez és nagyvállatokhoz a hamis címek ellni védelem a szolgáltatónak és az igénybe vevőnek is jelentős feladat.)
Az ún. Unicast Reverse Path Forwarding (uRPF) technika szintén alkalmazható az IP cím hamisításon alapuló informatikai hálózati támadások kivédésekor. Az uRPF a route-olt interfész és az informatikai hálózati szomszédsági viszonyok kombinációját használja fel annak eldöntésére, hogy egy adott csomag valós-e, még mielőtt azt továbbítaná a következő informatikai hálózati ponthoz. Az átjárók és tűzfalak megfelelően szigorú beállításaival ennek kiszűrésére is van lehetőség.

Az alkalmazások célpontok

Az alkalmazások többségét emberek fejlesztik, ebből következően hibákat tartalmazhatnak. Az ilyen hibák lehetnek “jóindulatúak” (pl. egy olyan hiba, ami miatt a dokumentum helytelenül nyomtatódik ki) vagy “rosszindulatú” (pl. egy olyan hiba, ami miatt a bankkártya számok egy adatbázis szerveren anonymous ftp elérhetővé válnak). A Rendőrség esetében elsődlegesen a rosszindulatú hibák elhárítására kell koncentrálni. Ugyanakkor nem szankcionálási célzattal széleskörűen kell megtalálni és elemezni tudáshiányból, végrehajtási eredményesség érdekében végzett nem szabályos tevékenységeket és applikációs hibákat. Az elemzés alapján történő módosításokkal és tudatosítással a működés eredményessége növelhető, illetve csökken az emberek megtévesztésén alapuló, vagy rejtve maradó behatolások mértéke. A módosított rendszerek pedig az adatok megváltoztathatatlansága (érvényessége) és rendelkezésre állása terén is többet fognak nyújtani.

Minden rendszer tekintetében fokozott figyelemmel kell követni, hogy a kereskedelmi, vagy

nyilvános forráskódú szoftverek rendelkeznek-e a legfrissebb biztonsági fixekkel. A nyilvános forrású alkalmazások, éppúgy, mint az eseti fejlesztésű szoftverek kód ellenőrzést igényelnek, mivel csak ezáltal biztosítható, hogy egy alkalmazás a gyenge minőségű kódolásból következően nem jelent-e biztonsági kockázatot. A programozás ilyen jellegű ellenőrzése a következőkre terjedhet ki: hogyan hív meg egy alkalmazás más alkalmazásokat (vagy magát az operációs rendszert), az alkalmazás milyen privilégium szinten fut, az alkalmazás a környező rendszerrel szembeni bizalmi viszonya (trust kapcsolata), vagy annak a módszere, hogy az alkalmazás miként szállít adatot az informatikai hálózaton keresztül.

Széles körben alkalmazott rendszerek esetében a kritikus frissítéseket kivéve célszerű megvárni az elemző központok, rendszervédelmi fejlesztők visszajelzéseit, Mert sok esetben a nem megfelelően ellenőrzött frissítések okoznak komoly funkcionális hibákat, vagy rendszer ellehetetlenülést. A frissítések tekintetében fontos a forrás és az elektronikus aláírás megfelelőségének ellenőrzése, mert a behatolási kísérletek egy része gyári frissítésnek álcázott szoftver elemként próbál települni.

Az alkalmazások elleni védekezés eszközei az informatikai hálózati és a hoszt alapú IDS/IPS rendszerek. Az IDS/IPS rendszerek hasonlóak működnek a riasztórendszerekhez, ha egy rendszer valamely eseményt támadásnak minősít, vagy saját maga végez beavatkozó tevékenységet, vagy egy menedzsment rendszeren keresztül riasztást küld az adminisztrátornak. Egyes rendszerek képesek reagálni vagy megakadályozni bizonyos támadásokat. A HIPS rendszerek az egyes hoszt operációs rendszer és az alkalmazás szintű hívásait fogja el, és ez által állítja meg azt az alkalmazást vagy hosztot, amely a rosszindulatú szoftvert hordozza. Az IPS/IDS rendszerek folyamatos fejlődésben vannak, ezért a megfelelő biztonsághoz nem csak telepíteni, hanem karbantartani és olykor igen magas áron a támogatást is megvenni szükséges.

Biztonságos menedzselés és riportolás

“Ha logolunk – olvassuk el.” Bárki, aki tájékozott az informatikai hálózatbiztonság területén így nyilatkozik, noha több száz eszköz információt logolni[15] és átolvasni meglehetősen komoly kihívást jelentő feladat. Mely logok fontosak? Hogyan különböztessük meg a fontos és az informatív szintű log üzeneteket? Hogyan biztosítsuk, hogy a logok nem kerültek módosításra átvitel közben? Hogyan biztosítsuk, hogy az alkalmazott időbélyegzők egyezzenek, ha több eszköz ugyanazon riasztást küldeni? Milyen információkra van szükség,

15 Megjegyzés: Naplózni

ha bűnügyi nyomozás esetén log információkra van szükség? Hogyan birkózzunk meg a nagy informatikai hálózatok által generált üzenetek mennyiségével? A hatékony állománykezelés a fenti kérdéseket veti fel.
A riportolás terén várhatóan sok érintett számára teljesíthetetlen kihívást jelent az GDPR, hiszen hatálybalépésétől az adattal érintettek számára már azt is meg kell tudni adni, hogy adataik mikor, hol, ki által és milyen más adataikkal kontextusban kerültek kezelésre.
A menedzselés szempontjából más kérdések merülnek fel. Hogyan menedzseljünk biztonságosan egy eszközt? Hogyan emeljünk ki nyilvános szerverek tartalmát úgy, hogy biztosíthassuk a tartalom átvitel közbeni módosíthatatlanságát? Miképp történjék a változásmenedzselés támadás vagy informatikai hálózati hibából adódó hibakeresés közben?

Architekturális szempontból a sávon kívüli – Out Of Band (OOB) – informatikai hálózatmenedzselés tekinthető bármely menedzselési és riporttolási stratégiának. Semmiféle a szervezet tényleges működését érintő adatforgalom nem jelenik meg az ilyen OOB informatikai hálózatokon. Az egyes eszközöknek közvetlen kapcsolattal kell rendelkezniük az ilyen informatikai hálózatokhoz, illetve ahol ez földrajzi vagy más rendszer-specifikus okokból nem lehetséges, az eszköz titkosított csatornán keresztül kell, hogy kapcsolódjon a tényleges szervezeti informatikai hálózaton keresztül. Az ilyen csatornákat úgy kell konfigurálni, hogy azokon csak a menedzseléshez szükséges portokon keresztül lehessen használni, amelyek a menedzseléshez és riporttoláshoz szükségesek. A csatorna hozzáférését le kell szűkíteni oly módon, hogy csak az arra kijelölt hosztok tudjanak kapcsolatot kezdeményezni, vagy fogadni.
AZ OOB megvalósításának nehézségét az adja, hogy részben, vagy a maximális megbízhatóság érdekében teljes egészében dedikált hálózatot szükséges kiépíteni hozzá.
Az OOB informatikai hálózatmenedzselés megvalósítása után a logolás és a riportolás folyamata egyszerűbbé válik. A legtöbb informatikai hálózati eszköz syslog adatokat küld, melyek kiemelten fontosak egy informatikai hálózati hiba, vagy biztonsági incidens kezelésekor. Az ilyen adatokat a hálózatmenedzsment szegmensen elhelyezkedő egy, vagy több syslog analízis hosztnak küldjük. Az érintett eszköz függvényében választhatunk változó riasztási szintek között attól függően, hogy milyen mennyiségű és milyen mélységű log információt szeretnénk kinyerni. Emellett az analizáló szoftverben szükséges az egyes eszközök logjainak megjelölése, hogy lehetőség legyen a részletes áttekintésre és jelentések készítésére. Például egy támadás esetén egy Layer 2 switch által küldött log adat feltételezhetően kevésbé érdekes információt hordoz, mint egy IPS logjai. Speciális

alkalmazások – mint például az IDS/IPS rendszerek – általában saját protokollokat használnak a riasztási információk átvitelére. Az ilyen adatokat általában dedikált menedzsment rendszerekre kell naplózni, melyek egyedi módon kezelik támadások riasztását. A naplózó eszközöket kombinálva, a több eszközből származó logg információk alapján a teljes informatikai hálózat állapotára vonatkozó információk is kinyerhetők. A logg üzenetek időszinkronjának biztosítására a hosztok és informatikai hálózati eszközök óráit szinkronizálni kell. Azon eszközök, amelyek támogatják az Network Time Protocol (NTP) nyújt megoldást a pontos idő nyilvántartására. Egy támadás esetén a másodpercekre tehető időkülönbségnek is jelentősége van, mivel így deríthető ki a véghezvitt támadás sorrendisége.

Amennyiben egy informatikai hálózati eszköz kompromittálódik, minél tovább tart kitalálni a kompromittáltság mértékét, annál nagyobb annak a szervezetre gyakorolt pénzügyi és jogi hatása – ezért elsődleges az időtényező. A loggolást végző eszközök és szoftverek elsődleges funkciója, hogy egy informatikai hálózati támadás esetében minél hamarább értesítést tudjanak küldeni a biztonsági specialistának. Ennek hatékonysága érdekében egy biztonsági monitorozó eszköz vagy szoftver a következő képességekkel kell, hogy bírjon:

- Syslog és IDS/IPS riasztási adatok konszolidációja.
- Felhasználók által definiált szabályokon alapuló adat osztályzás.
- A biztonsági specialista valós idejű automatikus értesítése kritikus riasztások esetén.
- Kritikus riasztások automatikus elemzése.
- Gyors, flexibilis jelentési rendszerek biztosítása nagy mennyiségű syslog és IDS/IPS riasztási adat kezelésére.
- A riasztási adatok grafikus kezelése a könnyű és gyors támadástípus, támadás forrás és támadás célállomás analízis érdekében.

Mint minden log menedzsmentnél így az OOB-nél is komoly tervezési és megvalósítási feladat a mit és hogyan. Ebben sokat segíthetnek az általános és rendszer specifikus legjobb gyakorlatok. (Sok rendszernél csak a saját adatokkal kel módosítani a kész modulokat. A logolás másik kérdésköre az analízis, amelynek elvei viszonylag jól gyakorlata már kevésbé kidolgozott.

Az OOB menedzsment nem minden esetben kívánatos. Alkalmazása sok esetben a menedzsment alkalmazáson, és az alkalmazott protokollokon múlik. Tekintsünk egy olyan menedzsment eszközt, amely feladata az informatikai hálózatban található eszközök elérhetőségének meghatározása! Ha két gerinchálózati eszköz közötti kritikus OOB link meghibásodik, a menedzsment eszköz feladata az, hogy az adminisztrátort értesítse.

Amennyiben ez az eszköz OOB menedzsmenttel üzemel, akkor nem lesz képes detektálni az adott link meghibásodását, mivel az OOB informatikai hálózaton lévő eszközök egy közös informatikai hálózatként kezelődnek.

Az ilyen jellegű menedzsment alkalmazások esetén javasolt a menedzsment sávon belüli in-band megvalósítása. (Tehát a menedzsment adatok a normál és az OOB hálózaton is elküldésre kerülnek, illetve ha biztonsági szempontból ez megengedhető, akkor a távmenedzselés is mindkét hálózaton engedélyezésre kerülhet.) Az ilyen in-band menedzsment esetén azonban törekedni kell a lehető legbiztonságosabb menedzsment megvalósítására. OOB menedzsment megvalósítható egy menedzsment informatikai hálózaton is, amennyiben egy tűzfallal választjuk el a menedzsment hosztokat és a menedzselni kívánt eszközöket.

Amennyiben egy eszköz in-band menedzsmentet igényel, számos tényezőt kell figyelembe venni. Először is azt, hogy az eszköz mely menedzsment protokollokat támogatja. IP Security (IPSec) eszközök egyszerűen menedzselhetők egy a menedzsment állomástól a menedzselt eszközökig kifeszített tunnel segítségével. Az ilyen megvalósítás lehetővé teszi, hogy számos nem biztonságos menedzsment protokollt hajtsunk át ezen a titkosított csatornán keresztül. Amennyiben az IPSec nem támogatott egy adott eszközön, kevésbé biztonságos alternatívák közül kell választani. Egy eszköz konfigurációja esetén az SSH vagy SSL sok esetben rendelkezésre áll, és ezek az eszközök javasoltak a Telnet használatával szemben, mivel ezeket keresztül a bármilyen konfiguráció módosítás titkosítva végezhető. A fenti protokollok szintén gyakran használhatóak olyan esetben, amikor adatot kell fel- vagy letölteni az adott eszközre. Használjuk ezeket a nem biztonságosnak tekinthető FTP és TFTP helyett. Jóllehet, a TFTP igen gyakran használt metódus az informatikai hálózati eszközök konfigurációinak vagy szoftver frissítéseinek mozgatásakor. Az újabb típusú informatikai hálózati eszközök támogatják a Secure Copy Protocol (SCP) használatát, egy olyan file transzfer eszközt, amely az SSH előnyeit használja ki. A Rendőrség központi és regionális kritikus eszközeinél ezek a biztonságos menedzselési technológiák kialakításra kerültek.

A másik figyelembe veendő tényező az, hogy a menedzselési csatornáknak minden időben aktívnak kell lenniük. Ha ez nem teljesül, a tűzfalakon ideiglenes hozzáférés biztosítható a menedzsment funkciók elvégzésének időtartamára, melyeket használaton kívül tiltani, legalább időszakosan felülvizsgálni és az eredménytől függően eltávolítani szükséges. Jóllehet

az ilyen jellegű folyamat nem érvényes nagy mennyiségű eszköz esetében, nagyobb szervezetek estében nem kívánatos megoldásnak tekintendő. Amennyiben a csatornáknak minden időben aktívnak kell lenniük, mint pl. SNMP alkalmazása esetén, egy harmadik tényezőt is figyelembe kell venni: vajon valóban szükséges-e az adott menedzsment eszköz? SNMP alapú menedzsment eszközök gyakran használatosan az informatikai hálózatokban, mivel leegyszerűsítik a hibakeresés folyamatát és a konfigurálást. Ettől függetlenül az SNMP protokollt különös odafigyeléssel kell kezelni, mivel az alatta található protokollok saját biztonsági problémákat hordoznak. Amennyiben szükséges, alkalmazhatunk read-only SNMP hozzáférést az eszközökön, és kezelhetjük az SNMP community sztringet hasonló érzékenységgel minden rendszernél, ahogy egy UNIX hoszt esetén tennénk. Az SNMP hozzáféréseknél pedig a küldési és hozzáférési beállítások biztonságos átgondolt beállítása jelentősen csökkentheti a károkozás veszélyét. Érdemes tudni, hogy az SNMP hálózatba történő bevezetésekor egyben potenciális biztonsági sérülékenységek is kerülnek a hálózatba. Amennyiben az informatikai hálózati eszközök esetében lehetőség van titkosított SNMPv3 használatára, akkor az akár in-band akár OOB menedzsment estén is alkalmazható. Megjegyezném, hogy az SNMPv3 biztonságosabb, mint a korábbi verziók, mivel 56 bites DES védelemmel rendelkezik. Amennyiben az eszköz támogatja javasolt az AES, 3DES titkosítás használata, ez esetben nagy mennyiségű üzenet esetén vizsgálandó a küldő eszközön jelentkező erőforrás terhelés növekedés.

A konfiguráció változás menedzselése szintén a biztonságos menedzselés egy résztémaköre. Ha egy támadás van folyamatban, fontos hogy ismerjük a kritikus informatikai hálózati eszközök állapotát és az utoljára végrehajtott konfigurációs változtatásokat. A változás menedzselés tervének elkészítése a mindenkori biztonságpolitika része kell, hogy legyen, de minimális elvárás, hogy a változásokat autentikációs rendszerek alkalmazásával rögzítsük a változásokat, és a konfigurációkat FTP, TFTP vagy SCP segítségével archiváljuk. A menedzselést és rendszerbiztonságot különös tekintettel a jogosultságok karbantartására és az elemzésekre nagyban segítheti a címtár alapú authentikáció. Hamis érv a címtár integráció ellen megtörés kockázata. A sziget rendszerekben gyakori az aktualizálás elmaradás és nehezebb a művelt visszakeresés, nagyvállalati méretekben, amennyiben az adott rendszert önálló több pontos külső fél számára is elfogadott autentikációval akarjuk ellátni, akkor az adott rendszeren történő kivitelezés költsége összemérhető lesz a központi címtár kialakításával és többszörösen költségesebb, mint akár egy biztonsági szinttel magasabb besorolású a szervezet egészére vonatkozó címtárhoz való integráció esetében. A

Rendőrségnél több univerzális címtár van ezek egymással integráltak. Az alkalmazások szintjén még részleges az integráció. A Robotzsaru rendszernél jelentős törekvés van az önálló autentikációs rendszer fejlesztésére, amely kockázati költség és üzemeltetési szempontból sem tűnik szerencsés megoldásnak.

A fentieket összegezve, olyan általánosságban megfogalmazott kritikus célpontokat határoztam meg, melyeket mind a már meglévő informatikai hálózatnál, mind egy fejlesztendő informatikai hálózatnál, vagy újonnan építendő informatikai hálózat védelménél figyelembe kell venni, a teljesség igénye nélkül tipizáltam őket. Az általános megfogalmazás tudatos volt részemről, mert konkrét eset tanulmányozásával adatvédelmi szabályokat sértettem volna, így viszont lehetőségem nyílt a létező és lehetséges problémákat bemutatni, amelyekkel akár találkozhatunk a Rendőrségi informatikai hálózat támadási célpontjainak vizsgálódása során is.

2.4. A RENDŐRSÉGI INFORMATIKAI HÁLÓZATOKAT ÉRHETŐ, VÁRHATÓ FENYEGETÉSEK

A fenyegetettség tekintetében a Rendőrség informatikai hálózatát a nagy vállalatok informatikai hálózatához hasonlónak tekintem. Feltételezéseim szerint hasonló más, az Internetre csatlakozó informatikai hálózatokhoz. Léteznek belső felhasználók, akiknek kifelé irányú kapcsolatokra van szükségük, és léteznek külső felhasználók, szervezeten kívüli személyek, más rendszerek és saját felhasználók is, amikor rendszeren kívülről befelé irányú kapcsolatokat szeretnének kezdeményezni. Ezen fenyegetéseket csoportosítom és meghatározom jellemzőjüket.

Ahogy az a CSI és az FBI által készített jelentésekben is megjelent, a támadások többsége a belső hálózatról származtatható. Elégedetlen alkalmazottak, belső kémek, látogatók, vendégek, hibás teszt szoftverek, hosztok, amelyek vírusokkal és férgekkel fertőzik a hálózatot, és képzetlen felhasználók alkotják az ilyen jellegű támadások potenciális forrását.

A nagyvállalatok és állami szereplők estében az informatikai kultúra és vezetői elvárás függvényében a gyakorlati tapasztalatok szerint a jó szándékú tudatlanságból, vagy feladat gyors befejezését célzó szabálytalan rendszer használat mértéke jelentősen meg is haladhatja a rossz szándékú, illetve hibából adódó incidenseket. Tehát a nem romboló, adat eltulajdonító célú incidensek et is figyelembe kell venni a kockázatoknál.

A hálózatbiztonság tervezése során igen fontos a potenciális (jó, rossz szándékú és a hibából származó) belső fenyegetések figyelembe vétele.

A nyilvánosan címezhető hosztok, amelyek az Internetre vagy az extranet hálózatokon kapcsolódnak nagy valószínűséggel alkalmazás rétegbeli támadások várhatók, melyek privilegizált hozzáférés szerzésére irányulnak, vagy DoS támadáshoz vezetnek, melyek a rendszer üzembiztonságát fenyegetik. Az ellehetetlenülés és az adat módosítás ellen is jó megoldás, hogy a széles körben elérhető külső szolgáltatások külön infrastruktúrán fussanak és az alaprendszerekkel történő adat átadás megfelelően szabályozottan tűzfalon keresztül történjen.

Egy hacker megpróbálhat ún. war-dialer alkalmazásokon keresztül hálózati hozzáférést szerezni, úgy hogy az adatkapcsolati telefonszámokat szerzi meg. A war-dialer alkalmazások vagy hardverek működésének alapja, hogy számos telefonszámot felhívnak és megállapítják az azok mögött található rendszerek típusát. A személyes felhasználásra szánt távfelügyelet szoftverek vannak leginkább kitéve az efféle támadásoknak, mivel ezek tipikusan nem túl biztonságosak. Mivel az ilyen eszközök általában tűzfal mögött helyezkednek el, amennyiben egy hacker hozzáférést szerez a betárcsázás során, belső felhasználó szerepkörében tud feltűnni a belső hálózaton. A Rendőrségi rendszereknél ilyen betárcsázás nem engedélyezett, csak IP alapú kapcsolatok, illetve mobil VPN hálózaton SMS üzentek küldése lehetséges bejövő üzeneteknél a jelenlegi elvárások szerint csak információs üzenet érkezhet, konfiguráció nem.

A vezeték nélküli technológiák (WLAN) megjelenésével számos új fenyegetés típus jelent meg. Az ún. war-driving egyre népszerűbb a hackerek közt. Egy wireless kártya és egy sniffer alkalmazás segítségével a hacker könnyedén hozzáférhet a vállalati információkhoz, és belső jogosultságokat szerezhet. Rendőrségi hálózatban alapesetben tiltott a WIFI használata. Speciális felhasználásnál az építéskor specifikációs elvárás az üzleti kategóriájú, Radius authentikációra képes, behatolás detektálással és IPS tűzfallal ellátott WIFI kialakítás, adat forgalom tekintetében a 802.11ac protokoll és WPA2 titkosítás a minimum elvárás.

A DSL technológia, és más nagy sávszélességű permanens kapcsolatok térhódításának köszönhetően a vállalati környezet a dolgozók távmunka környezetivel, otthoni irodai környezetekkel bővültek. Az ilyen helyszíneken található munkaállomások szélesebb körű fenyegetéstípusoknak vannak kitéve, mint a vállalati hálózaton belüliek – és biztonsági szempontból egységes rendszerben kezelve lehet a legjobb eredményt elérni. A vállalati biztonságpolitika szinte minden esetben titkosítás alkalmazását írja elő ilyen kapcsolatok

esetén. A támadástípusokat az alábbiakban rendszereztem és ismertetem.

1. Jogosulatlan hozzáférés (Unauthorized Access)

Jóllehet ez önmagában nem egy specifikus támadásfajta, a jogosulatlan hozzáférésen alapuló támadások kategóriájába sorolhatóak a napjainkban előforduló hálózati támadások túlnyomó többsége. Ha egy brute-force alapokon nyugvó telnet támadást tekintünk, akkor első körben ennek kivitelezéséhez telnet prompt szerzése szükséges. Amennyiben egy telnet kapcsolat kiépítésére kerül sor, egy indítási üzenetben jelezhető, hogy pl. "az erőforrás használatához megfelelő jogosultság szükséges". Amennyiben a hacker további kísérleteket tesz, úgy ezek a kísérletek más jogosulatlan akciónak tekinthetők. Ilyen jellegű támadások érkezhetnek egyaránt a külső, és a belső hálózati szegmensek felől.

2. Alkalmazás szintű támadás (application layer attack)

Az alkalmazás szintű támadások rendszerint a szerverek operációs rendszerében, illetve a szerveren futó alkalmazásokban rejlő hibák kihasználásával juttatják a támadott magas szintű jogosultságokhoz.
Az egyik fő probléma az alkalmazás szintű támadásokkal, hogy gyakran olyan TCP / UDP portokon keresztül történik, melyek engedélyezve vannak a tűzfalakon. A támadások legnagyobb része valamilyen rendszer, vagy beállítási hibára, valamint ezek kombinációjára épül.

3. Jelszó megfejtés (password attack)

A számítógép hálózatok erőforrásait támadók számos módszerrel próbálkoznak a felhasználónevek és jelszavak megszerzésére, melyek közül a legelterjedtebb az ún. brute-force támadás. E támadási formánál rendszerint egy erre a célra kifejlesztett alkalmazás próbál különböző az alkalmazás adatbázisában levő, vagy generált jelszavakkal belépni egy elérhető hálózati erőforrásra. Amennyiben sikerül megtalálni egy adott felhasználó jelszavát, akkor ugyanolyan jogokkal rendelkezik a támadott hálózati erőforráson, mint a felhasználó.
Ennél sokkal nagyobb veszélyt jelent, hogy a felhasználók rendszerint valamennyi erőforráson ugyanazt a felhasználónév / jelszó párt használják, így ha a támadónak lehetősége van több hálózati erőforráshoz is hozzáférni a megszerzett jelszóval. A több pontos authentikációval és tevékenység hozzáférés szabályozással jelentősen csökkenthető a veszélye. (Honnan, mikor, jelszó bonyolultság, kitiltás, szokatlan tevékenység blokkolása.)

A jelszó megfejtésnél a kisebb erőforrást igénylő megoldás a szótárral történő támadás, ez még jelenleg is hatékony lehet ahol nem megfelelő a felhasználói tudatosság, illetve ha a hacker rendelkezik felhasználó specifikus információkkal. Jelenleg a leghatékonyabb támadásnak a kombinált szótár és variációs brute force támadás lehet.

4. Szolgáltatások blokkolása (Distributed Denial of Service)

A legelterjedtebb támadási forma a hálózatok ellen a Denial of Service (DoS) , vagy Distributed Denial of Service (DDoS) támadás, melyet a legnehezebb teljes egészében eliminálni a hálózatból. A DoS támadások különböznek az egyéb támadási módszerektől, mert a céljuk nem információk megszerzése védett hálózati erőforrásokról, hanem a hálózati erőforrások által nyújtott szolgáltatások elérhetőségének megakadályozása. Ezt a célt általában a hálózatban (alacsony sávszélességű összeköttetések), vagy hálózati aktív eszközök várható terhelésre méretezett számítási képességét túlzottan igénybe vevő forgalommal, vagy a védett erőforrás operációs rendszerében rejlő szűk keresztmetszetek (memória, processzor kapacitás) kihasználásával érik el.
A teljesség igénye nélkül néhány jól ismert támadás például a Code Red , Blaster, TCP SYN flood, Ping of Death, Tribe Flood Network (TFN) és Tribe Flood Network 2000 (TFN2K), Trinoo, Stacheldraht, Trinity, SoBig. [16]

5. IP cím hamisítás (IP spoofing)

IP cím hamisításról beszélünk, amikor egy illetéktelen személy akár a belső, akár a külső hálózaton jogosulatlanul használ olyan IP címet, melyről belső védett erőforrások elérhetők. Egy másik célja az IP címhamisításnak, hogy elfedje az illetéktelen támadó tényleges IP címét, ezáltal megnehezítve a támadó felkutatását.
Alaphelyzetben az IP címhamisítással csak egyirányú adatforgalom lehetséges, ezáltal egy kliensről lehet adatokat továbbítani egy védett erőforrás irányába, ezzel DoS támadást megvalósítva. Kétirányú adatforgalom megvalósításához a támadónak a hálózati eszközök routing tábláját is manipulálni kell.

16 Megjegyzés: Az első négy támadás alapvetően féregtámadás, és nem DoS vagy DDoS eszköz, azonban viselkedésük DoS típusú körülményeket teremt

6. Csomagok vizsgálata (packet sniffer)

A packet sniffer egy szoftver alkalmazás, vagy hardver eszköz, mely alkalmas egy fizikai összeköttetésre rácsatlakozva, az adott összeköttetésen áthaladó valamennyi csomagot összegyűjteni, majd analizálni. Mivel számos alkalmazás kódolatlanul továbbít információkat (például ftp, telnet, stb.), ezért a packet snifferek alkalmazásával ezen alkalmazások által továbbított adatok láthatóvá tehetők, így a felhasználónevek és a jelszavak is.
Különös veszélyt jelent, hogy a felhasználók többsége ugyanazt a felhasználónév / jelszó párt használja valamennyi alkalmazás esetén, így egy gyengébb hálózati protokoll monitorozása által megszerzett adatok felhasználásával, kritikusabb alkalmazásokhoz is hozzá lehet férni. Titkosított adatforgalommal és biztonságos autentikációval megnehezíthető a támadó dolga, igaz ehhez a rendszererőforrásokat megfelelően méretezni kell, hogy az üzemszerű használat ne okozzon túlterhelést a kiszolgálásban. Az informatika érdekes fintora, hogy a packet sniffer az egyik legfontosabb eszköz a hibás hálózati működés, illetve a támadás detektálás folyamatában.

7. Man-in-the-middle

A man-in-the-middle jellegű támadások során a hacker a hálózaton keresztülmenő csomagokhoz fér hozzá. Az ilyen támadások sok esetben a fent említett sniffer támadásokból indulnak ki, és más eszközök, routing, szállítás rétegbeli protokollok segítségével történik. Az ilyen támadások információ ellopáshoz, session eltérítéshez vezetnek. Eredményezhetnek forgalmi analízisen alapuló információszerzést, DoS támadást, az átvitt adat módosítását, és az információs sessionbe új adatok beillesztését. A megelőzés alapvető lépése a VLAN-ok megfelelő használata és a hozzáférhető hálózatokon a tikosított átvitel.

8. Hálózat feltérképezés (network reconnaissance)

A hálózat feltérképezés támadásnak tekintjük azokat a kísérleteket, melyek információk begyűjtésére irányulnak a hálózat topológiájáról, az operációs rendszerek fajtájáról, illetve az erőforrásokon futó alkalmazásokról. Az egyéb támadásokat rendszerint megelőzik a hálózat feltérképezésére irányuló támadás, mert az így megszerzett információk birtokában hatékonyabb támadási módszerek dolgozhatók ki. A hálózat feltérképezés leggyakoribb eszközei: DNS kérések, Ping sweep, Port scan. A feltérképezés terén kompromisszum kötésre lehet szükség, mert nagy rendszereknél ezen eszközök a működés ellenőrzést, hiba detektálást és a dinamikus változások követését szolgálják és ésszerűtlen szintű tiltásuk maga is

kockázatot jelent, kiváltsuk költséges és ronthatja a rendelkezésre állást, vagyis végső soron az adatok hozzáférhetőségét.

9. Trust[17] kapcsolatok kihasználása (trust exploitation)

A trust kapcsolatok kihasználása esetén a támadó valamely más támadási módszerrel hozzáfér egy elérhető erőforráshoz, majd kihasználja, hogy a megtámadott erőforrásról hozzá lehet férni más védett erőforrásokhoz. A leggyakoribb példa a trust kapcsolatok kihasználására a publikus szervereket tartalmazó tűzfal szegmens. Egy web szerver operációs rendszerében rejlő hiba kihasználásával a támadó hozzáférhet a web szerverhez, majd a web szerveren keresztül az azonos szegmensen levő levelező szervert is támadni tudja. A nem megfelelően felkészült hackerek esetében azon a területen van veszély, amíg valamilyen céleszközzel eljutnak, a felkészült támadók azonban az ilyen technológiákban tudnak kiteljesedni. Kliensek esetében a zombiként történő felhasználás lehet a magas kockázat, nagy vállatoknál viszont folyamatosan kezelni kell az ilyen egymásra épülő támadásokat.

10. Port átirányítás (port redirection)

A trust kapcsolatok kihasználásának egyik megoldása a port átirányítás. Képzeljünk el egy publikus szervereket tartalmazó tűzfal szegmensen! A publikus szerverek elérhetők a külvilág irányából, ugyanakkor publikus szerverek elérhetnek erőforrásokat a belső védett hálózaton is. Amennyiben a támadó sikeresen bejutott egy publikus szerverre, akkor egy egyszerű szoftver telepítésével megoldható, hogy a publikus szervernek szóló csomagok egy belső védett erőforrás felé továbbítódjanak, ezáltal a támadó megkerülheti a tűzfalat. A megoldás a tartalom vizsgálat, pontosan beállított belső tűzfalrendszer lehet.

11. Root kit-ek, vírusok és trójai falovak (root-kit, virus and Trojan horse attack)

A root kit szkriptek és programok olyan csomagja, melyet a hacker egy olyan hosztra telepít, amelyet már korábban kompromittált és azon adminisztrátori vagy root jogosultságot szerzett. A kit a rendszerprogramok trójai verzióit tartalmazzák (pl. cmd.exe, /bin/login/su), melyek installáció után lehetővé teszik a hacker számára, hogy autentikáció nélkül jusson teljes rendszerhozzáféréshez.

17 Megjegyzés: Bizalmas

A vírusok és a trójai falovak rendszerint a felhasználói munkaállomásokat támadják meg. A vírusok olyan szoftverek, melyek programokhoz kapcsolódnak, és nem kívánatos funkciókat hajtanak végre (pl. törölnek állományokat). A trójai falovak olyan programok, melynek másnak látszanak, mint amik (pl. egy játék program, mely rögzíti a leütött billentyűket, és továbbítja ezt az információt egy előre meghatározott helyre). A vírusoknak egy speciális fajtája az ún. férgek (worm), melyek egyaránt veszélyesek a munkaállomásokra és a szerverekre is. A munka állomásokhoz való hozzáférés veszélyét az adja, hogy minden az adott számítógép számára engedélyezett szolgáltatáshoz van esélye a hackernek hozzáférni, illetve a visszafejtéskor megnehezíti a visszafejtést.

12. Zero-day jellegű támadások (day-zero attack)

A zero-day jellegű támadások alá olyan féreg, vírus és trójai támadások tartoznak, melyeket még nem azonosítottak, és nincs hozzájuk kapcsolódó betörési minta, amelyek alapján a vírusirtók, és IDS rendszerek felismernék őket. A fejlettebb védelmi rendszerek esetében a megváltozott tevékenység alapján, illetve a terhelés változást figyelve lehet észrevenni az ilyen jellegű kísérleteket .

13. Layer 2 támadások

A layer 2 szintű hálózati közegeken indított támadások összefoglaló neve. Ezek alá tartozhatnak az Ethernet szintű támadások, vagy a wireless környezetet érintő támadások. Ezek a következők lehetnek például (a teljesség igénye nélkül): CAM Table Overflow, VLAN hopping, Spanning tree manipulation, MAC spoofing, DHCP snoofing, PVLAN attack, DHCP starvation, CDP attack, Denial vagy Degradation of Service, Packet sniffers, Jogosulatlan hozzáférés, MITM aktív támadások, Authentication forge, Passive Attack (FMS paper), Rough Access Point alkalmazása, Brute force dictionary attack, IP spoofing, Arp spoofing, topológia felderítése. A védekezés függ a támadás jellegétől, illetve általánosan a hálózati eszközök és a hozzáférés pontos beállításával, port, MAC cím és VLAN megfelelő konfigurálásával csökkenthető a kockázat. A jól méretezett szűk keresztmetszetektől mentes hálózat a túlterheléses jellegű támadások eredményességét csökkenti. A megfelelően konfigurált menedzsment rendszer már az eredményes támadás előtt figyelmeztethet a megváltozott forgalomra, illetve automatikus beavatkozás is lehetséges. A tapasztalatok szerint a legkevésbé támadható hálózati részek, amelyekben gyakorlatilag nincs forgalom, befolyásolási lehetőség, A védelmet ilyen struktúra esetében a hálózati határokon kell

megvalósítani. A magas szolgáltatási szintű, akár támadás kezelésre is képes eszközök esetében a beállított funkciókat jól megtervezetten kell megvalósítani, mert a részleges beállítás mind átbocsájtó képesség, mind biztonság tekintetében a szándékolttal ellentétes eredményt hozhat. pl. Egy korlátozó funkció adminisztrációs jógához jutva a támadó a felhasználók számára ellehetetlenítheti a szolgáltatások elérését saját rendszerei számára pedig a teljes hálózatot dedikálhatja.

14. URL és Content blocking támadások, kártékony kód futtatása

A támadók által gyakran alkalmazott módszer, hogy a web szervereket törik fel először. Az ilyen jellegű támadások hihetetlenül sokrétűek lehetnek, - beleértve a dotdot, url obfuscation, nem RFC megfelelő működés, MIME típuson nyugvó, URI hosszon alapuló, stb. támadásokat -. A web alapú támadások népszerű válfaja az ártalmas kód elhelyezése, melyet letöltve a kliensek gépén hajtódik végre.

A fenti felsorolásban igyekeztem a Rendőrség informatikai hálózatát általánosságban vizsgálni a támadások tekintetében. Megállapítottam, hogy számos olyan fenyegetés és támadás létezik, amelyek a kezdeti kompromittálás által egy hacker behatolása leegyszerűsödik és másodlagos támadásokat kezdeményezhet többek között, vagy az eredeti célnál megmarad a támadó. Rendkívül szerteágazó és széleskörű lehet a támadások köre. A fenti felsorolás csak az alapvető típusokat öleli fel, a speciális irányúakat jelen elemzés során figyelmen kívül hagytam.

2.5. A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁNAK VÉDELMI CÉLKITŰZÉSEI, BIZTONSÁGI KÖVETELMÉNYEK

Minden olyan tevékenység mely az informatikai hálózati szolgáltatást, Rendőrségi informatikai tevékenységének biztonsági szintjét alkotja és fenntartja, meghatározza az informatikai hálózat biztonság helyzetét, mely lehet személyi, szolgáltatási vagy tárgyi vonatkozású. Ezen tevékenységek ilyen sarkalatos szegmenseként értelmezem a veszélyhelyzeteket, az informatikai hálózatot, érő fenyegetéseket, és azok elleni védekezések meghatározása érdekében megfogalmazott kérdések körét.

A GDPR, a nemzeti biztonsági stratégia, ajánlások (KIB 25, kormányzati ajánlások) különösen IBIK, törvények különös tekintettel az információ biztonsági törvényre és egyéb jogszabályok (elektronikus kormányzati gerinchálózat, egységes digitális rádió rendszer előírásai stb.), helyi előírások (helyi szervezeti informatikai biztonsági stratégia, politika és

szabályzatok) felhasználásával vizsgálati szempontokat határozok meg. A felderítéssel célom meghatározni a Nagytávolságú és helyi hálózatok biztonsági osztályba sorolásának állapotát, helyzet felmérését, a szükséges intézkedések meglétét, az érvényben lévő előírások alkalmazhatóságát, fizikai megvalósíthatóságát.

Tézisem szerint, mindenki, aki informatikai hálózattal rendelkezik (legyen a nagyvállalat, vagy egy kisebb vállalkozás) elsődleges fontosságú számára a hálózatának biztonsága. Miután a Rendőrség informatikai hálózatán lévő információ nagyon sok pénzbe kerül, így néha rendszerezés nélkül temérdek pénzt fordítanak annak védelmére. A szoftver- és hardver piacon a biztonsági cégek megszámlálhatatlan sok védelmi megoldással bombázzák a vásárlókat, és ezek a védelmi megoldások átláthatatlan útvesztőbe terelik őket. A döntéshozókat pedig nagymértékben befolyásolja a divat, a trend és a marketing. A műszaki megfontolások, illetve a szervezet működésének megfelelő megoldások keresése pedig jó esetben is csak ezután következik. Ezért kutatásokat folytattam, hogy mit kell védenünk, ha a hálózatunkat szeretnénk biztonságban tudni és egyáltalán milyen megoldások jöhetnek szóba.

Kutatásaimat a piacon fellelhető termékek vizsgálatain folytattam le. Egy nagyvállalati, jelen esetben a Rendőrség informatikai hálózat biztonság szempontjából azokat a pontokat mutattam be, ahol a lehetséges összes támadási felület előfordulhat. A fenyegetettség tekintetében a nagy vállalatok informatikai hálózata hasonló más, az Internetre csatlakozó informatika hálózatokhoz. Léteznek belső felhasználók, akiknek kifelé irányú kapcsolatokra van szükségük, és léteznek külső felhasználók, akik befelé irányú kapcsolatokat szeretnének kezdeményezni. Számos olyan fenyegetés létezik, amelyek a kezdeti kompromittálás által egy hacker behatolása leegyszerűsödik, és másodlagos támadásokat kezdeményezhet. Ezen fenyegetéseket csoportosítottam és határoztam meg jellemzőjüket az előzőekben.

A fenti fenyegetettség vizsgálatot, és helyzet elemelemzéseket alapul véve, rendszereztem azon alapelveket, melyeknek a Rendőrség informatikai hálózatának alapvetően a meg kell felelnie, továbbá követelményként meghatároztam a területeket, melyeket érint. Ugyan a 23/2013. (V.17.) ORFK utasításban a belső adatvédelmi és adatbiztonsági szabályzatban fellelhető volt a jogosultság szabályozás bizonyos rendszerek esetében lekérdezések során, továbbá az objektumvédelmi feladatok ellátásának körében speciálisan adatok rögzítéséről és felhasználásáról találhattunk szabályzókat, viszont ezek mind speciálisan az adott rendszerre, az adott adattípus feldolgozására vonatkoztak. A Rendőrségi informatikai rendszerek tekintetében általános érvényű szabályzóinak kialakítása jelenleg zajlik. Ezen folyamat során,

a Rendőrség informatikai biztonságának megteremtése érdekében általános érvényűen, szabályozott formában gondoskodni kell:

- A biztonsági elvárásokat és követelményeit rögzítése az informatikai biztonság dokumentációs rendszerben.
- A szervezeti és hatásköri kérdések, valamint a Rendőrségen belüli és az azon kívüli adatkapcsolatok szabályozása.
- Az adat- és információs vagyon védelmét szolgáló minősítési és biztonsági osztályba sorolási eljárásokat ki kell alakítani, valamint annak ellenőrzési módjait meg kell határozni.
- Meg kell fogalmazni a személyekhez és szerepkörökhöz kapcsolódó biztonsági követelményeket, meg kell alkotni az oktatási és képzési terveket, valamint biztonsági események, és meghibásodások esetén szükséges eljárási rendeket kell kialakítani.
- Biztosítani kell az informatikai rendszerek fizikai és környezeti biztonságát.
- Törekedni kell arra, hogy a már meglévő biztonsági rendszerek kompatibilisek legyenek a kialakítani kívánt fizikai és környezeti biztonsági feltételekkel, és biztosított legyen a rendszerek közötti átjárhatóság.
- Az alkalmazott üzemeltetési és kommunikációs eljárások alkalmazása során meg kell határozni az informatikai biztonsági követelményrendszert.
- Ki kell alakítani az informatikai eszközökhöz, adatokhoz és informatikai szolgáltatásokhoz történő hozzáférés szabályait.
- Létre kell hozni az informatikai rendszerfejlesztési, infrastruktúra folyamatos működésének biztosítását szolgáló és karbantartási jogszabály megfelelőségét, biztosító eljárásokat.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Jelen fejezetben kettes számú hipotézisemben feltételeztem, hogy a Rendőrség informatikai hálózatával szemben támasztott követelményeket, és intézkedéseket rendszerezve meghatározható az informatikai hálózatának védelmével szemben támasztható követelmények köre. A feltételezésem valós volt, valóban a rendelkezésre álló szabványok és a Rendőrségi informatikai hálózat szegmenseit megvizsgálva felállítható a követelményrendszer. Viszont a Rendőrségen még nem került elfogadásra olyan dokumentum, amely egységes formában tartalmazza a Rendőrség informatika politikai elvárásait, filozófiai megállapításait és

informatikai biztonsági védelmi célkitűzéseit.

Ebben a fejezetben rendszereztem a Rendőrség informatikai hálózatával szemben támasztható körülményeket a vizsgált dokumentumokban meghatározottakat összevetve a Rendőrségi normatív szabályozókkal. Megállapítottam, hogy a Rendőrség nem rendelkezik teljes körűen a szükséges szabályozókkal, így azok hiánya miatt részben a napi gyakorlatot követve alakultak ki a védelmi mechanizmusok. Ezért összegeztem a kutatási tapasztalatok alapján a követelményrendszereket. Álláspontom szerint a védelemnek 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. Az informatikai biztonság rendszere olyan legyen, hogy minimális adminisztratív terhet jelentsen, az alkalmazottaktól ne igényeljen aránytalanul nagy erőfeszítést, csak amelyet a helyes munkavégzés gyakorlata során elvárhatunk. Elsősorban abban nyújtson támogatást, hogy állapítsa meg a kivételes eseteket és biztosítsa a normál állapotra való visszatérést a kivételes esemény leküzdése után.„[22] Minimum követelményként határozható meg, hogy biztonságos működésre történő áttérés után a feladat végrehajtás a korábbinál ne legyen nehezebb. ‚A munkafolyamatok átgondolásával, személyre szabott munkakörnyezettel és a legjobb gyakorlatok alkalmazásával (ISO27001,ITIL stb.) az is elérhető, hogy security elvárásoknak megfelelő rendszerkörnyezet egyben a feladat végzést a korábbinál egyszerűbbé és gyorsabbá tegye.

Ezért elemző kutatásokat folytattam, melyekkel igazoltam, hogy a harmadik hipotézisemben megfogalmazottak szerint, az elemzések során meghatározható a Rendőrség informatikai hálózat biztonság helyzete, személyi, szolgáltatási és tárgyi vonatkozású veszélyeztetettségi pontjai, az azokat érő fenyegetések, sérülékenységek. Összegezve a fentieket, tekintettel arra, hogy jelenleg a Rendőrség még nem rendelkezik olyan informatikai biztonsági dokumentációval, mely egyértelműen meghatározná a Rendőrség ilyen irányú elgondolásait, véleményem szerint az informatikai biztonság politikának a már megfogalmazott informatikai biztonság filozófiára kell épülnie, és megfelelő alapot kell teremtenie az informatikai biztonsági célkitűzések meghatározásához. Minden lehetséges esetben a megelőzésre törekvő magatartást kell előnyben részesítenie a követő magatartással szemben, elvégre alapozó dokumentumot kell létrehoznia a védelem érdekében. Az informatikai biztonsággal összefüggő szabályoknak, intézkedéseknek egységes értelmezését kell elősegítenie.

III. A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁNAK VÉDELME SORÁN ALKALMAZHATÓ ESZKÖZÖK ÉS MÓDSZEREK

A fejezetben célom az előző fejezetben megfogalmazott követelményeket alátámasztó, az informatikai hálózatok védelme során alkalmazható módszerek, eszközök, eljárásokat rendszerezni és elemezni. A fejezetben feltárom a Rendőrség informatikai hálózatában jelenleg alkalmazott védelmi módszereket, eszközöket, ezzel is tágítva az előzőekben bemutatott helyzetképet. Bemutatom és értékelem az eljárásokat. A bemutatást követően meghatározom az eszközöknek és módszereknek a Rendőrségi informatikai hálózat védelme során történő alkalmazásának kritériumait, azok előnyeit és hátrányait. Ebben a fejezetben fontosnak tartom a Rendőrség informatikai hálózata védelme során alkalmazható eszközök és módszerek körének kialakítását és osztályozását. Az elemzések lefolytatásához alap dokumentumként fogom használni az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt.

BEVEZETÉS

A védelem során alkalmazható eszközöket és módszereket Magyarországon az állami elektronikus rendszerek kapcsán jogszabály határozza meg.

Napjainkban kiemelten fontos az információs társadalmat érő fenyegetések miatt, a Rendőrség vagyonát képező elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, rendszerelemek biztonsága, melyet védelmük érdekében tett intézkedések útján tehetünk meg. Az intézkedések meghozatalához rendszerezni, csoportosítani és azonosítani kell az elektronikus információs rendszereket, rendszerelemeket. Az intézkedéseknek ki kell térniük a megelőzésre, a biztonsági eseménykezelésre és az incidensek kezelésére.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (a továbbiakban: Ibtv.), ez idáig jogilag nem szabályozott területet von szabályozás alá, többek között az állami és önkormányzati szféra elektronikus információs rendszereivel kapcsolatos hálózatbiztonsági kérdésköröket. A törvény végrehajtására több kormányhatározat, rendelet és utasítás született. Ezen szabályozás alá vont szakterületek közül jelen fejezetben a Rendőrség elektronikus információs rendszereit érintő jogszabályok által előírtakat vizsgálom, és azok megvalósításának lehetőségeit kutatom, ezzel rendszerezem és csoportosítom a Rendőrségi elektronikus információs rendszereket.

Magyarországon megvan annak az igénye, hogy az információs rendszerekben bekövetkezett szándékos, vagy más jellegű káresemények ellen a teljes hazai informatikai közösség fellépjen. Jelenleg folyamatban van az egyenszilárdságú szakmai elvek és tevékenység megteremtése az információbiztonság területén. Álláspontom szerint hiányzik az az összefogás nemzeti szinten, amivel a megelőzést, a tájékoztatást, az irányítást, a felügyeletet, továbbá az incidens kezelését és az ország nemzetközi szinten képviselni tudná. Korábban Magyarország rendelkezett képviselttel a CERT közösségben, mely jelentőségét jelen korban felismerve, új helyzetet teremtett az új szabályozással és az új irányvonalakkal. Jelenleg a Nemzeti Kibervédelmi Intézet látja el a magyarországi GOV CERT feladatokat. A Rendőrség, a rendészeti ágazati szervekkel és az NKI-val együttműködve aktív irányvonalakat jelölt ki. Másodlagos célként ezen irányvonalak mentén meg fogom határozni a vizsgálati módszereket és lehetőségeket, melyekkel a Rendőrségi információs rendszerek védelmi módszerei állíthatóak fel.

3.1. A HÁLÓZATOK VÉDELME SORÁN ALKALMAZHATÓ MÓDSZEREK, ESZKÖZÖK, ELJÁRÁSOKAT RENDSZEREZÉSE ÉS ELEMEZÉSEI

Az említett törvényünk előírja, hogy „társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme”[18].

Ezen társadalmi elvárás alapján, a Rendőrségnek is meg kellett teremtenie az elektronikus információs rendszereinek biztonságát, függetlenül a rendszerek céljától, vagy funkcionalitásától. Ezen védelmi eljárásra az Ibtv. konkrét előírásokat fogalmaz meg:

„elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos”[18].

Tekintettel a fentiekre, a Rendőrség elektronikus információs rendszerek védelmének vizsgálatát az alábbi védelmi területekre folytatom le:

- „zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő

védelem”[18];

- „teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;”[18];
- „folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem”[18];
- „kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével”[18].

Az említett védelmi területeken, mind 3 spektrumon (bizalmasság, sértetlenség és rendelkezésre állás) vizsgálva az Ibtv. és végrehajtási rendeletei szerint a Rendőrség elektronikus információs rendszereit 5 biztonsági osztályba lehet sorolni mind a 3 területen.

A biztonsági osztályba sorolás eljárás módszertanát a Belügyminisztérium dolgozta ki 41/2015. (VII.12.) BM rendelet keretében „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”.

A vizsgálati módszertan, mellyel a védelmi intézkedéseket meghatározhatjuk, az alábbiak szerint kell lefolytatni:

- A vizsgált rendszer által ellátandó célt meg kell határozni, így megállapítható, hogy nyílt vagy zárt célú rendszerről beszélünk.
- Következő lépésben a funkcióját kell kijelölni az elektronikus információs rendszernek, így megállapítható, hogy mely csoportba soroltuk.
- Az értékelést három spektrumon kell lefolytatnunk a bizalmasság, a sértetlenség és rendelkezésre állás szempontjából meg kell határozni, hogy melyiket milyen súllyal vesszük figyelembe az adott rendszernél. Vizsgálni kell az értékelés szempont rendszerében, hogy melyek azok a tulajdonságok, amelyeket súlyozottan előrébb sorolunk a többi előtt, amelyet fontosabbnak tartunk. Ezt a besorolást kockázat elemzés útján tehetjük meg. A kockázatelemzési módszertant ugyancsak a 41/2015. (VII.15.) BM rendelet taglalja.
- Az osztályba sorolásokat követően a 41/2015. (VII.15.) BM rendelet segítségével kijelölhetők a zárt védelem, teljes körű védelem, folytonos védelem, kockázatokkal arányos védelem érdekében megteendő intézkedések sora.

A normatívák előírásai szerint a Rendőrség az Ibtv. 26. §. előírásainak megfelelően megtette a

szervezetei biztonsági szintbe sorolását. Az elektronikus információs rendszereinek tekintetében a jelen állapotuk szerinti és az adattartammal azonos biztonsági osztály besorolását a bizalmasság, sértetlenség és rendelkezésre állás területén lefolytatta. A besorolást és a bejelentést követően, a törvény lehetőséget biztosít az elektronikus információs rendszerek jelen állapotuk szerinti besorolási szint és az adattartammal azonos besorolási szint közötti eltérést megszüntetésére a rendszerek három évenkénti felülvizsgálata során az újrasorolás módszertanával. Ezzel a módszerrel előre tervezhetők a védelem és a biztonság szempontjából az amortizációs cserék és fejlesztések irányai. A besorolást minden esetben az adott szervezet vezetőjének az adatgazdának kell megtennie a törvényben meghatározott információ biztonsági felelős személy javaslatai alapján. A szervezet vezetője a felelős a feltételek megteremtéséért, és az információ biztonsági felelős feladata a feltételek teljesülésének, az intézkedések végrehajtásának felügyelete.

A védelmi eljárások tekintetében a létfontosságú rendszerelemek esetében a korábban említett 65/2013. kormányrendelet szélesebb körű speciális előírásokat tartalmaz kiemelten a különleges jogrend idejére, melyekre jelen kutatásom nem terjed ki.

3.2. A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁBAN JELENLEG ALKALMAZOTT VÉDELMI MÓDSZEREK, ESZKÖZÖK

A Rendőrségi elektronikus információs rendszerekre vonatkozó Rendőrségi normatívák, vagy szabályozók csak általánosan készültek el. Részletes szabályozás helyett, jellemzően csak működésre vonatkozó műszaki leírások tartalmaztak a biztonságra vonatkozó jellemzően alapvető szabályokat. A hiányosságok pótlása érdekében az Ibtv. rendelkezései szerint az alábbi azonosítási eljárást folytattam le:

„elektronikus információs rendszernek kell tekinteni az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön (környezeti infrastruktúra, hardver, hálózat), egymással összefüggő eljárásokkal (szabályozás, szoftver és kapcsolódó folyamatok) azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttesét.” [18] Ennek megfelelően az elektronikus információs rendszerek által ellátandó cél tekintetében két csoportra választottam szét a rendszereket:

- Nyílt célú: „az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és

kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese” [18];

- Zárt célú: „jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer” [18].

Az elektronikus információs rendszerek további rendszerezéséhez funkcionalitásuk szempontjából vizsgáltam meg és a nyílt célú elektronikus információs rendszereket az korábbi kutatások alapján, és az Ibtv előírásait alkalmazva kerül kutatásomban megkülönböztetésre:

- „számítástechnikai rendszerek és hálózatok;
- helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;
- rádiós vagy műholdas navigáció;
- automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek);
- a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.” [18].

„Funkcionalitásuk szempontjából a zárt célú elektronikus információs rendszereket is megvizsgáltam és az alábbiakban rendszereztem:

- Elektronikus Iktatást és Ügyiratkezelést Támogató rendszerek,
- Elektronikus Személyügyi Információs rendszerek,
- Elektronikus Adatkezelő rendszerek,
- Elektronikus Műveleti rendszerek,
- Elektronikus információ Biztonságot Támogató rendszerek,
- Elektronikus Hírközlő információs rendszerek.”[22]

A fentiekben összefoglalt csoportosításokon és rendszerezésen túl a törvény rendelkezik jogszabályban rögzített megkülönböztetésről is, nevezetesen a létfontosságú információs rendszerelemekről:

„az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit

elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené” [18].

Az Ibtv. a létfontosságú információs rendszerelemeket megkülönböztetett figyelemmel kezeli, melyről külön rendelkezik a 65/2013. (III.8.) Kormányrendelet, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendeleteként.

A normatívák meghatározásai szerint az egyes létfontosságú rendszerelemeket ugyanúgy lehet zártcélú és nyíltcélú elektronikus információs rendszerek elemeiként azonosítani, abban az esetben, ha figyelembe vesszük a 2012. évi CLXVI. törvényt, mely szerint az azonosított különleges rendszerelemekre eltérő rendelkezés, kifejezetten csak különleges jogrend fennállásának esetére került meghatározásra

A fenti azonosítási eljárás eredményen, az alábbi példákkal illusztrálom (a teljesség igénye nélkül), az Ibtv. vonatkozó elektronikus információs rendszerek csoportosítási és azonosítási rendelkezéseit felhasználva, a Rendőrségi elektronikus információs rendszereire kivetítve:

- „nyílt célú elektronikus információs rendszer: HERMON - Körözés Információs Rendszer (KIR), HIDRA - Hazai Idegenrendészeti Ügymenetet Támogató Alkalmazás szakrendszer, stb.;
- zárt célú elektronikus információs rendszer: ROBOTZSARU – Integrált ügyviteli és ügyfeldolgozó rendszer, TrafficPoint Rendszer stb.;
- létfontosságú információs rendszerelem: Határ Ellenőrző és Regisztrációs Rendszer (HERR).”[22]

HERMON: Magyar Körözési Információs Rendszer, mely egy szökött rabszolgáról neveztek el. Hermon i. e. 145-ben tűnt el, és a keresésére kiadott szöveg, amely a legrégebbi fennmaradt ilyen típusú anyag, kimondottan jó személyleírást tartalmaz. Ebbe a rendszerbe rögzítik a Magyarországon keresett összes személyt, tárgyat, és gépjárművet.

HIDRA: Hazai idegenrendészeti ügymenet támogató Alkalmazás rendszer célja a Rendőrség által folytatott idegenrendészeti eljárások ügymenetének, az azzal kapcsolatos nyilvántartási előírások végrehajtásának, a szakmai feladatok elektronikus ellenőrzésének, valamint értékelő-elemző feladatainak támogatása.

ROBOTZSARU: a rendőri szervek alap informatikai rendszere, olyan informatikai alkalmazások együttese, amely egységes rendszerbe foglal valamennyi nyílt Rendőrségi tevékenységgel kapcsolatban keletkező, illetve beszerzett elektronikus adatot és iratot; a rendőri munka jellegéhez, illetve az egyes felhasználói csoportok feladat- és munkaköréhez igazodó felhasználói jogosultságok biztosításával komplex módon támogatja a rendőri

szervek munkáját az elektronikus iratkezelésen, adatszolgáltatáson és feldolgozáson keresztül. Részét képezi a Dokumentumtár, a Netzsaru rendszer és a Robotzsaru NEO rendszer;
A Robotzsaru rendszer fejlesztései során elsődleges céllá vált, hogy minden szakrendszer a Robotzsaru keret alá kerüljön integrálásra. Biztonsági és strukturális átalakítása ezért a Rendőrség minden folyamatára kiható kritikus folyamat.

TrafficPoint: a látogatók egyszerűen tájékozódhatnak a velük szemben az objektív felelősség hatálya alá tartozó szabályszegések elkövetése miatt folytatott közigazgatási eljárás adatairól és az ügyintézés állásáról, továbbá megtekinthetik a velük szemben folytatott eljárás alapjául szolgáló képi bizonyítékokat. Az alkalmazás segítségével az ügyfelek tájékozódhatnak jogaikról és kötelezettségeikről, továbbá lehetőségük nyílik a leggyakrabban használatos iratminták letöltésére. A rendszer mindezt az eljárás során a hatóság által hozott döntés iratazonosítója és a gépjármű rendszámának megadása esetén, gyorsan és egyszerűen biztosítja. (mikor, hol történt a szabályszegés, milyen KRESZ szabályt szegtek meg, mekkora a bírság összege).

HERR: Határ Ellenőrző és Regisztrációs Rendszer az államhatár rendjét sértő vagy veszélyeztető cselekmények megelőzését, felderítését és megszakítását, az államhatár átlépésének feltételeivel nem rendelkező személyek be-, át- és kiutazásának megakadályozását, a Magyarországon és a schengeni térségben jogellenesen tartózkodó személyek kiszűrését és az ezzel kapcsolatos idegenrendészeti intézkedések és eljárások összességét támogató informatikai rendszer.

3.3. AZ INFORMÁCIÓBIZTONSÁGI TÖRVÉNY ÉS VÉGREHAJTÁSI NORMATÍVÁI ADTA LEHETSÉGES MÓDSZEREK A RENDŐRSÉGI ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK VÉDELEMÉRE

Az Ibtv. végrehajtására a 24. §. több rendelet megalkotását írja elő. Azokat a normatívákat vettem vizsgálat tárgyának, amelyek a Rendőrség elektronikus információs rendszereinek védelme során alkalmazhatóak:

- 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” (a továbbiakban: NEIH) , amely kitér a hatóság feladatának részletes szabályaira, a hatósági ellenőrzés lefolytatásának részletes eljárási szabályaira.

- A 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” , amely kitér a kormányzati eseménykezelő központ és az ágazati eseménykezelő központok feladat- és hatáskörére.
- 187/2015. (VII. 13.) Korm. rendelet „az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról” amely kitér a rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek esetében a rendvédelmi szervet irányító miniszter az elektronikus információs rendszer biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályok rendeletben kerültek meghatározásra.
- 185/2015. (VII. 13.) Korm. rendelet 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.

Az Ibtv. a megelőzés, az eseménykezelés és az intézkedések meglétét jelöli meg mérföldkövekként a védelem területén.

Az Ibtv. afenti mérföldköveknek megfelelően a megelőző és eseménykezelési tevékenységek körében a 19. §. (1)-ben előírja a kormányzati eseménykezelő központ (a továbbiakban: Központ) létrehozatalát:

„A Kormány az e törvényben foglalt biztonsági események kezelése érdekében kormányzati eseménykezelő központot működtet a katasztrófák elleni védekezésért felelős miniszter irányítása alatt. A kormányzati eseménykezelő központhoz a 2. § (1) bekezdésben meghatározott szervek tartoznak.”[18].

Az Ibtv. a Központ munkáját elősegítve további felhatalmazásokat tesz a speciális elektronikus információs rendszerekkel (úgy, mint zárt célú elektronikus információs rendszerekkel) rendelkező szervezetek számára külön kapcsolódási felületet hozott létre, melyen keresztül az együttműködést az alábbiakban határozza meg:

„(2) A 2. § (4) bekezdésében meghatározott szervezetek és az önálló szabályozó szervek az eseménykezelési feladatok ellátása érdekében ágazati eseménykezelő központot hozhatnak létre.

(3) Az ágazati eseménykezelő központ a biztonsági eseményekhez kapcsolódó és az (5) bekezdés szerinti együttműködés során tudomására jutott biztonsági események adatait köteles haladéktalanul a kormányzati eseménykezelő központ részére továbbítani.

(4) A kormányzati eseménykezelő központ az európai kormányzati eseménykezelő csoport által akkreditált nemzeti eseménykezelő központként vesz részt a kormányzati eseménykezelő központok nemzetközi együttműködésében.

(5) Az ágazati eseménykezelő központok a fenntartó döntése alapján részt vehetnek az eseménykezelő központok nemzetközi együttműködésében, és e célból akkreditálhatók.

(6) Az ágazati eseménykezelő központok a kormányzati eseménykezelő központtal, mint nemzeti eseménykezelési koordinátorral, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal együttműködnek."[18]

A Központ nem tart direktben a kapcsolatot a kisebb szervezeti egységekkel, egy közbenső koordinatív szerepet játszó ágazati szervezet tudja fenntartani az akár on-line a kapcsolatot, így a Rendőrség, mint ágazati szervezeten a Belügyminisztériumon keresztül tudja fenn tartani a kapcsolatot a Központtal.

A kapcsolatfenntartásra a Belügyminisztérium több alkalommal felmérést végzett az ágazati szervezetei között, hogy mely szervezetek tartják szakmailag indokoltnak a belügyi ágazati eseménykezelő központ létrehozatalát, viszont ez minden esetben a humán kapacitás és szakértelem hiányára való hivatkozással egyik szervezet sem volt képes önerőből létrehozni és képviseltetni magát az ágazati eseménykezelő központok között, így többek között a Rendőrség sem.

Megoldásként a 36/2013. BM rendelettel létrehozásra került a Belügyminisztérium Miniszteri Kabinetében egy Központi Felügyelet, aki kapcsolatot tart fenn a NEIH, a Nemzeti Biztonsági Felügyelet (NBF), valamint a Központ és a belügyi ágazati szervezetek között. Feladatai között szakmai szakirányítási segítséget nyújt, például a biztonsági eseményeket jelenleg mindkét irányba be kell jelenteni, amely a koordináció és a megoldás közötti reakcióidőt meghosszabbítja. Folyamatban van ennek a problémának a feloldása azzal a normatíva javaslattal, hogy a biztonsági események bejelentése egycsatornás lenne, melyre technikailag a szervezetek már most képesek.

„Az Ibtv. a korábban meghatározott mérföldkövekkel összhangban, négy dimenzióban támogatja a Rendőrség elektronikus információs rendszereinek védelmét a Központ munkája útján:

1. Megelőzés

- Az Ibtv. felhatalmazást ad, hogy a már bejelentett, kivizsgált és megoldott incidenseket forrás nélkül megjelenítse a Központ, jelen esetünkben a Rendőrség részére is, és azonnal tájékoztassa őt róla.
- A 24 órás hálózatfigyelésnek köszönhetően a hálózaton jelentkező eseményekről 24 órában azonnal tájékoztatja a Rendőrséget, mint résztvevő szervezeteket. Figyelmeztethet az események megjelenésére, és a kivédésükre teendő intézkedéseket megfogalmazza.
- A nemzetközi trendekben megjelent újdonságokról, és a nemzetközileg publikált sérülékenységekről tájékoztathatja a Rendőrséget, mint résztvevő szervezetet adott esetben elektronikus úton, és a honlapján is.

2. Szakmai iránymutatás, szakirányítás

- Az ágazati eseménykezelő központok kiépítésének köszönhetően a szakmai iránymutatás kinyújtott karjaként jelennek meg az ágazati szervezetek a helyi szervezetek és a Központ között, így szakmailag biztosítottá válik az információs csatorna. Az ágazati eseménykezelő központokban szakemberek továbbítják az információt a szervezetek részére, így a Rendőrség a központi egységein keresztül az információkat azonnal megyei szintre tudja továbbítani. Ezzel időt spórol meg, és növeli a rendelkezésre állást, csökkentve a reakció időt.
- Azonnali figyelmeztetéseket tesz közzé a kritikus hálózatbiztonsági eseményekről a létfontosságú információs infrastruktúrát felügyelő szervezetek számára, melyek így azonnali segítségnyújtást jelentenek a Rendőrség számára.
- A Rendőrség a Központ útján együttműködik a hatósággal és a Nemzeti Biztonsági Felügyelettel, így meg tudja valósítani a szakmai tapasztalatok begyűjtését és megosztását minden fórumon.

3. Incidenskezelés

- Az Ibtv. elrendeli a biztonsági események bejelentését a Központ (Nemzeti Kibervédelmi Intézet) és a Hatóság (Nemzeti Elektronikus Információbiztonsági Hatóság) részére. Ezzel az incidens megjelenésének felismerését segíti elő, ha a Központ tudomást szerez róla, és megkezdheti a kivizsgálást.
- A bejelentésnek köszönhetően azonosítható az incidens megjelenési ideje, helye és típusa.
- A kivizsgálást követően a Központ útján történő megjelenés összevethető a

rendelkezésre álló tapasztalatokkal, és a kezelésére megkezdhetők az intézkedések, így csökkenthetők az anyagi és természeti károk.

4. Nemzetközi kapcsolatok

- Az Ibtv. rendelkezései szerint a Központ felkérésre részt vesz a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon, ahol a legfrissebb információkkal látja el a résztvevő szervezeteket.
- Ez a nemzetközi kapcsolat és információ megosztás a Rendőrség részéről az EDR mint, egy nemzetközi hírközlő rendszer része révén valóul meg. Itt a Rendőrség szintén tapasztalatokat fogalmaz meg, majd továbbítja a fórumok részére.
- Ezen hazai tapasztalatokat ez elektronikus információs rendszerek védelme kapcsán a Központ összefogja és képviseli Magyarországot GovCERT-ként a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon."[22]

A Központ mind nemzetközi, mind haza szintéren a Nemzeti Kiberbiztonsági Koordinációs Tanács útján az európai kormányzati eseménykezelő csoporttal kapcsolatot tart fenn. Sok esetben ez kapcsolat felvétel megvalósul a Rendőrség nemzetközi kapcsolatain keresztül, mint heterogén kapcsolatrendszer útján is, mellyel a Rendőrség az információk naprakészségét aktívan tudja támogatni. Az Ibtv. a 20. §-ban megfogalmazza továbbá az ellátandó feladatok körét az eseménykezelés területén, a Központ tekintetében, mely feladatok körét egészíti ki a 233/2013. (VI. 30.) Korm. rendelet. „Ezen rendeletből csoportosítottam az alábbiakban a feladatok körét:

- technikai védelmi,
- megelőző,
- koordinációs,
- valamint szakmai támogató,
- tájékoztatási tevékenységet végez,
- a hálózatbiztonság fenntartásának és fokozásának elősegítéséért tesz intézkedéseket,
- ellátja a Nemzeti Távközlési Gerinchálózat vonatkozásában a biztonsági eseménykezelés feladatait,
- a sérülékenységről, fenyegetettségről, káros szoftverekről, biztonsági eseményekről rendszeresen jelentéseket készít,
- biztonsági eseménykezelési támogatást nyújt,
- koordinál a hazai és nemzetközi szervezetek felé a biztonsági eseményt kiváltó okok

megszüntetése, illetve kezelése érdekében.”[22]

A Rendőrség szoros együttműködését a Hatósággal, a 301/2013. (VII. 29.) Korm. rendelet, továbbá a 41/2015. (VII.15.) BM rendelet az „állami és az 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 követelmények” határozzák meg. A 41/2015. (VII.15.) BM rendelet a 2009. évi CLV törvény és a 90/2010. (III.26.) kormányrendelet szakmai vonalát tükrözi, így megjelennek benne az adminisztratív védelmi intézkedések, a fizikai védelmi intézkedések, a logikai védelmi intézkedések, figyelembe véve az Ibtv. három spektrumát (bizalmasság, sértetlenség és rendelkezésre állás területén).

A biztonsági osztályba sorolás alap általános irányelveket, továbbá speciális veszélyeztetettség típusokat határoz meg, melyek bekövetkezésének valószínűségéhez igazodó kárérték szinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelményeinek teljesülését kell vizsgálnunk.

Ezen vizsgálatot a Rendőrségi elektronikus információs rendszerek esetében az adattartalomra, a rendszereket működtető szervezetek tükrében kell lefolytatnia a Rendőrségnek.

Amint a korábbiakban már említést tettem a biztonsági osztályba sorolás módszertanáról, a 41/2015. (VII.15.) BM rendelet biztonsági osztályba sorolás szakmai iránymutatását az alábbiakban foglalom össze:

„1.1. Az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti;

1.1.1. a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;

1.1.2. a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;

1.1.3. a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

1.2. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus

információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni."[23]

A védelmi intézkedések körét a Rendőrség részére tovább tágította az Ibtv. a Központ útján, mely szerint a185/2015. (VII. 13.) Korm. rendelet „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" új reformot alakít ki a sérülékenység észlelése, kezelése, és vizsgálata területén:

- a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítéséért,
- a biztonsági eseményekről személyes adatokat nem tartalmazó nyilvántartás vezetéséért, amely tartalmazza a biztonsági esemény kapcsán megtett intézkedéseket és azok eredményét, valamint
- az érintettek számára a biztonsági események kezelése során szakmai támogatás nyújtásáért"[24]

A sérülékenység észlelése és kezelése közötti időintervallumot a fenti vizsgálati módszertan, a kockázatkezelés jelenlegi eljárása véleményem szerint rendkívül meghosszabbítja, ezért a részletes kockázatértékelés eljárását elsődleges vizsgálatokkal meg lehetne előzni, ennek folytán csak kritikus,esetben kellene - ha a Központ konkrét álláspontja is hiányzik - a hatósággal, a Nemzeti Biztonsági Felügyelet, és az ügyben érintett szervekkel végeztetni az adott biztonsági esemény kezelését igazoló vizsgálatokat.

A 185/2015.(VII.13.) korm. rendelet a Rendőrség zárt célú elektronikus információs rendszereinek védelmi intézkedéseinek támogatásaképpen a sérülékenység vizsgálat tekintetében kitér a 14§-ban a rendészeti szervek vonatkozásában a vizsgálattal összefüggő feladatok ellátásának szabályozására, mely szerint az NBSZ a központi felügyeletnek a – kormányzati eseménykezelő központtal egyeztetett – megkeresése alapján végezheti a sérülékenység vizsgálatot. Ez szoros együttműködést és támogatást feltételez a Központtal, amelyben a Rendőrség is részt vesz, így különösen „a sérülékenység vizsgálat eredményéről, a sérülékenység vizsgálat során feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó javasolt intézkedésekről a vizsgálat lezárását követően az NBSZ haladéktalanul

tájékoztatja a központi felügyeletet, amely tájékoztatja a vizsgált belügyi szerv vezetőjét és a kormányzati eseménykezelő központot." [22] Itt jogi anomáliaként jelenik meg az, hogy ha a NEIH a hatósági ellenőrzése során sérülékenységet vélt felfedezni, minősített rendszerek esetében az NBF-et kéri fel, nyílt rendszerek esetében pedig a Nemzeti Kibervédelmi Intézetet a végrehajtásra, aki végül felhatalmazza az NBSZ-t a feladat végrehajtására. Jogilag az NBF jogkörrel a Rendőrség zárcélú elektronikus információs rendszereinek tekintetében nem rendelkezik, csak és kizárólag az NBSZ.

Tekintettel arra, hogy az Ibtv. végrehajtásának egyik fő felügyeleti szerve a NEIH a 41/2015. (VII.15.) BM rendeletben meghatározottak alapján, amely szervezet konkrét alapelveket fektet le, és a hazai ajánlásokat helyezi előtérbe, így tanulmányom nem terjed ki a nemzetközi ajánlások elemzésére.

A Központ biztonságiesemény-kezelési feladatkörében felelős a 185/2015.(VII.13.) Korm. alapán:

„a) a jutott biztonsági eseményekről az érintettek haladéktalan értesítéséért,

b) a biztonsági eseményekről személyes adatokat nem tartalmazó nyilvántartás vezetéséért, amely tartalmazza a biztonsági esemény kapcsán megtett intézkedéseket és azok eredményét, valamint

c) az érintettek számára a biztonsági események kezelése során szakmai támogatás nyújtásáért"[24]

Ezen feladatok ellátásának körében keletkezett információk együttműködés során cserélődnek a Központ és a Rendőrség között, ezzel is biztosítva naprakészséget.

„Az Ibtv. és a 2012. évi CLXVI. törvény 65/2013. (III.8.) végrehajtási kormányrendelete, az Ibtv. által megalkotott Hatóság segítségével besorolt és minősített rendszer elemekre és rendszerekre támaszkodva új területet jelenít meg a létfontosságú rendszerek és létesítmények eseménykezelő központjának létrehozatalával. Ennek érdekében a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság hálózatbiztonsági feladata körében, a honvédelmi szempontból létfontosságú rendszerek és létesítmények kivételével, nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenység ellátása érdekében, eseménykezelő központot működtet Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (a továbbiakban: LRLIBEK) elnevezéssel. Ezen szervezet támogatja a Rendőrség létfontosságú rendszerelemeinek körében felmerülő védelmi intézkedéseket. A LRLIBEK feladatkörében

ugyan úgy működik, mint az ágazati eseménykezelő központok, de a Központ feladatkörén túl hatásköre a Rendőrséget érintő speciális területet ölel magába:

- az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK irányelvnek való megfelelést szolgálja,
- vizsgálati területe a globális kibertérből a nemzeti létfontosságú rendszerelemet érintő, és az internet-forgalomba érkező beavatkozással érintett területek,
- képviseli a létfontosságú rendszereket és létesítményeket üzemeltető szervezeteket a hálózatbiztonság védelmére szakosodott együttműködési fórumokon és szervezetekben."[22]

A Létfontosságú rendszerek és létesítmények Eseménykezelő Központjának feladatait az Országos Katasztrófavédelmi Főigazgatóság látja el.

Az Ibtv. egyik fontos anomáliájára, hogy több szervezet és felügyelet is lát el - akár átfedéssel is - nemzetközi fórumokon hazai képviseletet az információbiztonság területén.

Az eddigi vizsgálataimból egyértelműen kitűnik, hogy sok olyan terület maradt, amelyek az Ibtv.-t alkalmazó szervezetek számára nem kerületek be a szabályozás alá, melyet úgy oldottak meg, hogy ledelegálta az ágazati szintre a tovább szabályozási jogokat.

Véleményem szerint a jelenleg is hiányzó alsóbb szintű szabályzókban kell a tátongó kiskapukat megszüntetni, ezzel is segítséget nyújtani az ágazati szervezetek számára. Álláspontom szerint a Rendőrség számára a 185/2015.(VII.13.) korm. rendelet adná meg a lehetőséget, ha a Rendőrségnél is megszületnének a 185/2015.(VII.13.) korm.. rendelet mintájára a végrehajtó szabályozók, a jogszabály által rendezetlen területek megszüntetésére és felállna Rendőrségi Eseménykezelő Központ.

Meggyőződésem, hogy a 36/2013. BM rendelet végrehajtására olyan utasításokat és belső szabályzókat kellene megalkotni, melyek információbiztonsági szakterületekre bontva pontos iránymutatásokkal segítené a Rendőrség információbiztonsági fejlődését és munkáját is. Példának okáért a 41/2015. (VII.15.) BM rendelet szabályozza az alábbi területeket, amelyek hiányoznak a Rendőrségi szabályozásból, így javasolnám szabályozás alá vonni az alábbi területeket:

- „az elektronikus információs rendszerek összekapcsolásának lépésről lépésre történő engedélyezési eljárása és konkrét feltételei,
- az új, önálló, a meglévőktől független elektronikus információs rendszer létesítése, a

meglévők megszüntetése, fejlesztése, korszerűsítése, átalakítása, valamint az üzemeltető szerv megváltoztatásához szükséges engedélyezési eljárások meghatározása,

- az elektronikus információs rendszerek határainak, felelősségi köreinek elválasztása és azok felügyelete,
- a Belügyminisztériumon belüli koordinációs munka és az ágazati szervezetek közötti koordinációs munkálatok az információbiztonság területein az Ibtv. gyakorlati végrehajtásának elősegítésére."[22]

3.4. A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁNAK VÉDELME SORÁN ALKALMAZHATÓ ESZKÖZ

A Rendőrség informatikai hálózatának védelmére alkalmazható eszközök kiválasztásához elsődlegesen meg kell határozni a hálózat sérülékenységi faktorait. A sérülékenység elemzés az az eszköz, mellyel meghatározhatjuk a védendő, azaz sérülékeny faktorokat. Ahhoz, hogy a Rendőrség informatikai hálózatának sérülékenységét meg tudjuk vizsgálni meg kell határozni az alapelveket, mely nyomán alapvetően a meg kell felelnie a biztonsági követelményeknek az informatikai hálózatnak. Célom jelen fejezetben, hogy a sérülékenység vizsgálat eredményét felhasználva meghatározzam a Rendőrség informatikai hálózatának biztonsági eszközrendszerét.

Alapelvek vizsgálatához a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatából az alábbiakat vettem alapul:

- azonosítás, hitelesítés,
- jogosultság kiosztás, ellenőrzés,
- hozzáférés-szabályozás,
- elszámoltathatóság,
- hitelesség garantálása,
- sértetlenség garantálása,
- auditálhatóság logikai védelmi funkciói,
- bizonyítékok rendszerének és folyamatának kialakítása.

A fenti alapelvek nyomán a korábbi fejezetekben alkalmazott ajánlások és az Ibtv. törvény szerint megkezdhettem a biztonsági osztályba sorolást. Az osztályba sorolásnak hatáselemzésen kell alapulnia, melynek elemei az alábbiak:

a) folyamatalapú kockázatelemzés,
b) működési hatáselemzés,
c) költségelemzés.

Az osztályba sorolást a fenti módszertan alapján az alábbi kockázati szempontok figyelembevételével kell maghatározni a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzata szerint:

a) az információs rendszer veszélyeztetettségének foka,
b) az információs rendszer területi kiterjedésének mértéke,
c) az információs rendszert fenyegető veszély, fenyegetés időbeli hatásai,
d) az információs rendszert fenyegető veszély, fenyegetés érintett személyi körre gyakorolt hatása,
e) az információs rendszer által kezelt adatok érzékenysége (minősített adat, nemzeti adatvagyon körébe tartozó vagyon, nem nyilvános adat, személyes adat).
f) sérülékenység menedzsment A folyamat az információs rendszerekben található biztonsági rések feltárását, a biztonsági problémák elhárítására megoldási javaslatok megfogalmazását, a hibajavítást illetve a hibajavítás ellenőrzését foglalja magában. A rendszeres vizsgálat-javítás-vizsgálat munkafolyamat biztosítja, hogy a rendszer sérülékenységeiről naprakész információ álljon rendelkezésre.

A kockázatelemzéshez, kockázatkezeléshez két módszertan közül választhattam a KIB 25-ös ajánlása alapján. Az első eljárásrend a NIST SP 800-303 és a FIPS 1994 dokumentumokon alapuló módszertan. Ez a módszertan viszonylag egyszerű, kis idő- és erőforrás igényű kockázatbecslést tesz lehetővé. A másik eljárásrend egy CRAMM5 alapú módszertan, amely MeH ITB 8. számú ajánlása (informatikai biztonsági módszertani kézikönyv) alapján, annak aktualizálásával készült kockázatelemzési módszertan. A CRAMM módszertan egy részletes, az egyes fenyegetések kockázatait feltáró eljárás, azonban idő- és erőforrás igénye nagy – ezért költséges.

Az elemzés alapjául két dokumentumot kívántam összehasonlítani, az IBIR és a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatát.

Az Informatikai Biztonsági Irányítási Rendszer1 (IBIR) az ISO 27001:2005 verziótól a szabvány alapvető fogalma. Az IBIR egy általános irányítási rendszer, amely az üzleti kockázat elemzésen alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot. Az irányítási rendszer magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az

eljárásokat, a folyamatokat és az erőforrásokat. Az ISO 27001:2013-ban jelentős változás, hogy nem lehetőség, hanem alapvető elem a fejlődés, tehát az elvárt szint folyamatos megközelítéssel is elérhető, majd tovább javítható. Ez az alapelv jobban közelíti a valóságos folyamatokat, illetve a biztonságos működésnek történő teljes megfelelés több lépésben történhet. A több lépés lehetőséget ad arra, hogy már rövid idő alatt jelentősen javuljon a biztonsági szint.
Az Informatikai Biztonsági Irányítási Rendszer akkor hatékony, ha hasznos a szervezet számára. Az információbiztonság a szervezet működési és üzleti kultúrájának szerves része kell, hogy legyen. Az információbiztonság a technikai problémákkal ellentétben elsődlegesen vezetői probléma, bár vannak nem elhanyagolható technikai problémák, különösen az informatikai használatától való általános függőség.
A jól irányított információbiztonság a sikeres üzleti tevékenység egyik alapfeltétele. Egyetlen szervezet sem tud napjainkban sikeres lenni információbiztonság nélkül. Az információbiztonság érdekében hozott, jól megválasztott vezetési intézkedések megfelelően megvalósítva, és pozitív hozzáállással használva nem csak költséget jelentenek, hanem sikeressé tehetik a szervezetet.

Egyértelműen látszik a két dokumentumból, hogy míg a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzata alapelveket fogalmaz meg, technikai részletes elemzéseket nem tartalmaz. Az IBIR a MIBIK alapelveire támaszkodva konkrét kezelési és elemzési módszertanokat határoz meg.

ISO/IEC 27001:2005 szabvány „rendelkezik jelen esetünkben konkrétan a hálózatbiztonsági kezelésére vonatkozólag. A szabvány céljából is kitűnik, hogy a kezelésnek célja a hálózatokban lévő információk megóvásának és támogató infrastruktúra védelmének biztosítása. „A hálózatbiztonsági szabályozást úgy kell kialakítani, hogy az kitérjen mind a hálózatok védelmére, mind a hálózati szolgáltatások biztonsága.” [25]

Sérülékenységi mátrix

A sérülékenység vizsgálat első eleme a kockázat elemzés. A kockázat elemzés nyomán egy sérülékenységi mátrixban összegezem a lehetséges fenyegetések és támadások eseti megjelenéseit. A mátrix megalkotása során meghatároztam a kockázati tényezőket, összegeztem a lehetséges meghibásodásokat, társítottam hozzá a kárértékeket, az előfordulási

gyakoriságát a meghibásodásnak, további tényezőként értékeltem a kritikusságát az eseménynek, az esemény bekövetkezésének hatását, az eseményre való reagálást és a reagálás időintervallumát.

Kockázati tényezőknél meg kell vizsgálni mind hardver, mind szoftver tekintetében az informatikai hálózati részegységeit. Így különös figyelmet kell fordítani az informatikai hálózat dokumentációira. A dokumentációkat biztonsági kockázatuk alapján szükség szerint minősíteni kell, ezt követően védelmüket az iratkezelési szabályok szavatolják. Hardver tekintetében különös figyelmet kell fordítani a kábelezésre és a hálózati végpontokra. A végpontoknál vizsgálni kell a szerverek hardveres meghibásodását, erősáramú betáplálási problémákat, szerverterem klimatizálás- és a természeti katasztrófák kockázatát. További vizsgálati tényezőnek tekintem a szerver szoftveres meghibásodását, a kliens hardveres meghibásodását, a kliens szoftveres meghibásodását és a hálózati összeköttetés meghibásodását.

Meghibásodási tényezőknél azt vizsgáltam, hogy a meghibásodás olyan elemet érint, mely redundáns, vagy nem redundáns, illetve a meghibásodott elemeik okozhatnak-e szerver kapacitás csökkenést. A meghibásodás következményeként vizsgáltam, hogy a rendszer használható marad, vagy nem és hogy a meghibásodás következményeként a kapcsolódó rendszerek és kliensek használhatóak maradnak-e vagy sem. A probléma megjelenésénél vizsgálni kell az érintett területetek környezetét is, így hogy egy kliens gépet érint, vagy a kliensek meghatározó részét, vagy mindet, vagy esetleg a szervert is. A környezeti tényezők meghibásodásánál számba kell venni az estleges áramszüneteket, melyek időtávját, és területi kiterjedését kell figyelembe venni, továbbá a táplált eszközök, mint például a klíma berendezés működőképessége megmarad, vagy az energia ellátás kimaradás a meghibásodását eredményezi. És végül a legrosszabb eshetőséget is figyelembe kell venni az elemzés során, hogy a hálózati egységeket magába foglaló körlet, vagy környéke, vagy a teljes épület megsemmisül

Kockázatkezelés

A rendszer elleni támadások a fenti csoportosítások szerinti lehetséges célja az, hogy:
a) beazonosítsák az információ kezelés helyszínét és a külső kapcsolatokat.
b) akadályozzák az üzemeltetést.

c) megrongálják az eszközöket.
d) megszerezzék az információt.
e) módosítsák az információt

„A rendszer elleni támadások következménye lehet:
a) A rendelkezésre állás elvesztése (a jogosult bejelentkezés megtagadása vagy a rendszer szolgáltatásainak hozzáférhetetlenné tétele).
b) A bizalmasság elvesztése (a rendszerbe történő jogosulatlan belépéssel a munkaállomáson feldolgozott vagy kezelt minősített adat illetéktelen személy számára hozzáférhetővé vagy megismerhetővé válik).
c) A sértetlenség elvesztése (a rendszer információinak jogosulatlan módosítása miatt a rendszer forrásainak hibás működése vagy a rendszeren kezelt információk valódiságának megszűnése). ” [5]

A sértetlenség elvesztése a legkritikusabb, mert ez szavatolja a károkozás későbbi el és felszámolhatóságát. Tehát minden esetben szükséges egy garantált tartalmú másolat.
A MeH ITB 12. számú ajánlást figyelembe véve megalkottam a sérülékenységi mátrixot, beintegrálva kockázat elemzést, és a kockázat kezelési feladatokat, a kapcsolódó intézkedéseket. (1. számú melléklet)

Az intézkedések megvalósíthatósága

A mátrixban különböző intézkedéseket fogalmaztam meg a szabványok figyelembe vételével. A mátrix alapját képezi a katasztrófa-elhárítás terv elkészítésének. A táblázatot kifejtve az alábbiakban két csoportot határoztam meg a sérülékenység tekintetében:
1. Teljes informatikai hálózat megsérülése

- infrastruktúra sérülése szolgáltatás szüneteltetés, mely elemi kár folyamán következett be
- hardver, szoftver fizikai sérülés rendszerleállást követően,
- adathordozók visszaállíthatatlan állapotú sérülése, megsemmisülése
- dokumentációk sérülése,
- adatok sérülése, adatvesztés
- kommunikáció, osztott rendszerek sérülése szolgáltatás szüneteltetés miatt,
- személyek kompromittálódása.

2. Részleges informatikai hálózat sérülése

- infrastruktúra sérülése áramszünet miatt,
- hardver, szoftver sérülése, visszaállítható állapotban,
- adathordozók sérülése, melyek visszaállítatók az archív anyagokból,
- dokumentációk sérülése, irattárból való visszaállíthatósága,
- adatok sérülése, melyek mentésekből visszaállíthatók,
- kommunikáció, osztott rendszerek sérülése, kiesési időn belüli visszaállíthatósága,
- személyek kompromittálódásának időbeni észlelése.

Ezek elkerülésére készíthetünk Megelőzési tervet. A terv készítése során az általános intézkedések között az alábbi területeknek kell megvizsgálni a sérülését, vagy esetleges hiányát, kompromittálódását.

- infrastruktúra: mindazon hardver és szoftver eszközök, informatikai rendszerek, hálózatok, alkalmazások, programok összessége, amelyek segítik és kiszolgálják a szervezet kommunikációs, adatfeldolgozó és adatátviteli tevékenységét,
- hardver: az informatikai rendszer eszközeit, fizikai elemeit alkotó részei; szoftver: Valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges,
- adathordozók,
- dokumentációk,
- adatok: Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája,
- kommunikáció, osztott rendszerek,
- személyek: az a személy vagy szervezet, aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához.[25]

Ha már bekövetkezett a probléma, akkor a katasztrófa elhárítás részét képezi a Visszaállítási rendek meghatározása. Ennek célja, hogy a katasztrófa következtében megsérült erőforrások eredeti állapotának biztosítása eredeti helyen. A visszaállítás érdekében az alábbi intézkedéseket kell követni:

- azonnali válasz (riadóterv)
- futtató környezet helyreállítása,
- funkcionális helyreállítás,
- üzemeltetési szintű helyreállítás,
- áttelepülés (katasztrófa esetén),

- normalizáció az áttelepülés után.

A fenti említett szabályozók nyomaiban általánosságban fellelhetők voltak a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatában, viszont nem kerültek speciálisan megfogalmazásra a Rendőrség informatikai hálózatával kapcsolatosan.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A fejezet céljakén az információbiztonságról szóló törvény és a végrehajtási rendeletei által támasztott elvárások nyomán, a szabályozó rendszer struktúrájának bemutatása útján, és az ezekből fakadó Rendőrségi védelmi feladatok körének vizsgálatával rávilágítást kívántam adni az információbiztonság tudatosság növelésére, fontosságára, a védelmi módszerekre. A feladatok sokrétűsége és információkat magában hordozó elektronikus információs rendszerek nagyfokú sebezhetősége véleményem szerint arra irányítja a figyelmet, hogy csak több szervezett által összehangolt, közös fellépéssel lehet az esetleges információs támadásokat kezelni, kivédeni. Ennek kezelésére és összehangolására az Ibtv. által több olyan szervezet jött létre, melyek mindezeket a célokat tűzték ki feladatul. A fejezetben leírtakból is kitűnik, hogy a hazai információbiztonsági szervezetek mindegyike azonos funkciókat lát el, csak más-más szervezeteket és területeket képviselnek. Megállapítottam a fejezetben, hogy a közös feladatok, funkciók az alábbiak köré csoportosíthatók: támadások elemzése; információcsere biztosítása; adatbázis létrehozása és folyamatos frissítése; együttműködések a különböző szervezetek között; intézkedések kidolgozása az incidensek kezelésére.

Álláspontom szerint az Ibtv. az információbiztonság területén stratégiát alkotva jelölheti ki a Rendőrség számára azon irányvonalakat, melyek mentén haladva, lépésről-lépésre, projektek megvalósításával elérheti a megfelelő információbiztonsági szintet. A fejezetben elért eredmények:

- bemutattam az Ibtv. Rendőrséget érintő előírásait,
- 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,
- az Ibtv. irányvonalakhoz igazodva, meghatároztam a védelmi módszertani eljárást, mely szerint a Rendőrségi elektronikus információs rendszerek védelmi intézkedéseit ki lehet választani, meg lehet jelölni,
- meghatároztam az Ibtv. és végrehajtási rendeletei által alkotott azon szervezeteinek

kiemelkedő feladatit, melyek a Rendőrség védelmi feladatait támogatják az elektronikus információs rendszereinek területén,

- felfedtem az Ibtv. egyes szabályozatlan, vagy olykor többszörösen szabályozott területei közül néhányat,
- javaslatokat tettem egyes, a Rendőrséget érintő szabályozatlan területek megszüntetésének módjára,
- eszközrendszert állítottam fel a sérülékenységi mátrix meghatározásával a védendő faktorokra.

A követelmények meglétének hiányát feltételezve, taglalni kívántam a sérülékenység mátrix-al, hogy milyen eredményeket okozhatnak az általam meghatározott támadások az informatikai hálózat biztonsági állapotában.

Összegezve, álláspontom szerint a védelem megteremtése kormányzati és Rendőrség oldaláról csak koordináltan történhet. E koordináció, pedig a hatékonyság maximalizálása érdekében egycsatornás kommunikációs módszertan szerint centralizálnia kell, amelynek legcélszerűbb módja – tekintve többek között az állam kiemelt felelősségét – az állami/kormányzati kézben lévő centralizáció, szakirányító felügyelet, a kormányzati eseménykezelő központ, illetve a jogkörök tisztázásával az eseménykezelő központ megerősítése.

IV. A RENDŐRSÉG INFORMATIKAI HÁLÓZAT VÉDELMÉNEK FEJLESZTÉSI IRÁNYAI ÉS FELADATAI

Jelen fejezetben célom a korábbi fejezetek elemzéseit és eredményeit felhasználva, a hipotézisek 4. pontjában megfogalmazott feltevések igazolása olyan fejlesztési területek meghatározásával, melyek elengedhetetlenek ahhoz, hogy a Rendőrségi informatikai hálózatok védelmét a törvények szerint a Rendőrség garantálni tudja. A fejlesztési javaslataim három irányt határoznak meg: első sorban az adminisztratív (szabályozási) irányvonalat, majd a logikai és fizikai irányvonalakat. Az irányvonalakat szervezeti szinten és a Rendőrségi informatikai hálózatok szintjén határozom meg. Az irányvonalak segítségével körvonalazom azon feladatok és egyben intézkedések körét, melyek segítségével érhetőek a védelmi stratégiai célkitűzések és teljesíthetők a követelményrendszerek.

AZ ELMÉLET MEGJELENÉSE A GYAKORLATBAN

Az előző fejezetekben a feltételezéseim bizonyítására felsorakoztattam mind azt az elméleti kutatási anyagot, mely jelen fejezetet megalapozza.
Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározottak szerint „a nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága. Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.”[18]

Az új uniós irányelv GDPR a technikai fejlődésre és a társadalmi elvárásra adott válasz, amely, minden uniós állampolgár adatát kezelőre vonatkozik. A kezelés szabályaiban jelentős változást hoz, hogy az adat összefüggések védelmére is kiterjed, továbbá az adatkezelések folyamatának az állampolgár kérésére visszakereshetőnek és elérhetőnek kell lennie.

A információ biztonsági törvény a GDPR-nél szűkebb az állami szervekre és a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira terjed ki. A jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói

egyben az állami szervek és az önkormányzatok is. A GDPR életbe lépése várhatóan az információ biztonsági törtvény elvárásainak kiszélesedésével fog járni főként az adatokon végzett műveletek dokumentálása és visszakeresése terén.

Alapvető elektronikus információbiztonsági követelmények között - minden a jogszabálya hatálya alá tartozó szervezetnek – az elektronikus információs rendszerek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják többek között a biztonsági események kezelését is. A biztonsági esemény kezelésének részét képezi a fenyegetettség felmérése.

„A fenyegetettség olyan művelet, vagy esemény, illetve ezek hiánya, amely sértheti az információs rendszer védettségét, biztonságát.”[18] Ebből következő, hogy a „kockázat a fenyegetettség mértéke, amely valamely fenyegető tényezőből ered. A kockázat mértéke a kárnagyság és a bekövetkezési valószínűség (gyakoriság) szorzata.”[18] Ezen mérték megállapítására kockázat elemzéseket kell végezni. „A kockázatelemzés olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési gyakoriságát.”[26]

Ha már a kockázat elemzésével és a fenyegetettség vizsgálat ismeretével rendelkezünk, akkor a biztonsági események kezelése következik. A biztonsági esemény „nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.”[18]

A biztonsági esemény kezelése „az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.”[18] Az észlelés „a biztonsági esemény bekövetkezésének felismerése.”[18]

A biztonsági események, egy részét képezik az incidensek. Az incidens valamilyen előre nem tervezett zavart jelent. Ezen incidensek megelőzése a védelem célja.

A fent felsorolt és levezetett elméleti megállapításoknak a gyakorlatba történő átvezetése és megvalósítása jelen fejezetnek és egyben a végső kutatásomnak a célja.

BEVEZETÉS

A fejlesztési irányvonalak meghatározásához alap dokumentumként tekintek a 41/2015. (VII.15.) BM rendelet keretében „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (Ibtv.) meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről” megalkotott eljárás módszertanára melyet a Belügyminisztérium dolgozott ki. A módszertan alapjaiban véve az Ibtv. törvény védelmi területeire koncentrálva, 3 spektrumon (bizalmasság, sértetlenség és rendelkezésre állás) vizsgálva a Rendőrség elektronikus információs rendszereit, 5 különböző szintbe sorolása mellet lehetőséget ad a Rendőrségi informatikai hálózatok védelmi fejlesztési irányvonalainak meghatározására. A kutatásom korábbi fejezeteiben sorra vettem az összes olyan normatívát és lehetséges szabályzót vagy ajánlást, hogy a védelmi követelményeket és helyzetét körvonalazzam a Rendőrségi informatikai hálózatoknak. Így ezen nyomvonalon tovább haladva, miután a jelenlegi helyzet ismeretes jelen fejezetben feltárom a hiányosságokat és azok megoldására javaslatot teszek.

Az irányvonalakat az alábbi területekre értelmeztem:

- adminisztratív (szabályozási),
- fizikai,
- logikai.

Az irányvonalakat szervezeti szinten és a Rendőrségi informatikai hálózatok szintjén fogom jelen fejezetben értelmezni.

4.1. ADMINISZTRATÍV FEJLESZTÉSI CÉLKITŰZÉSEK A RENDŐSÉGI SZERVEZET RÉSZÉRE

Miután az Ibtv.-t vettem alap dokumentumként a fejlesztési irányvonalak meghatározásánál, az elektronikus információs rendszereket – és így közvetve az informatikai hálózatokat – működtető szervezetet biztonsági szintbe kell sorolni, mint első adminisztratív irányvonali célkitűzésként határozom meg a Rendőrségi informatikai hálózatokkal való összefüggésében.
Az Ibtv megfogalmazása szerint:
„biztonsági szint: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
biztonsági szintbe sorolás: a szervezet felkészültségének meghatározása az e törvényben és a

végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;”[18]
Ezek alapján a Rendőrséget, mint szervezetet 4-es szintbe sorolom, mert:
„4. Az érintett szervezet biztonsági szintje 4., ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet, vagy fejleszt.
4.1. A 4. biztonsági szervezeti szint követelményei a 3. szinthez rendelt követelményeken túl:
4.1.1. az üzemeltetési, vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés, vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;
4.1.2. tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint;
4.1.3. azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt, vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges, vagy bekövetkezett biztonsági esemény kezelését is;
4.1.4. folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer, vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók, vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;
4.1.5. a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;
4.1.6. a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást, vagy biztonsági ellenőrzést kell végezni;
4.1.7. a tesztelés értékelése alapján megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;
4.1.8. az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.”[23]

Az Ibtv. általános irányelvei szerint a „az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a rendszer funkciójára tekintettel, ahhoz igazodó súllyal érvényesíti. Ezért a Rendőrség informatikai hálózatát megpróbáltam besorolni.

„biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;
biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;”[18]
Ezért a Rendőrség informatikai hálózatát besorolom 4 osztályba bizalmasság, sérthetetlenség és rendelkezésre állás spektrumán.
„2.5. A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel
2.5.1. különleges személyes adat nagy mennyiségben sérülhet;
2.5.2. személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
2.5.3. az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
2.5.4. a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;
2.5.5. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.”[23]

Ebből egyértelműen meghatározható első célja a Rendőrségnek, hogy megfogalmazza, az érintett szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az informatikai biztonsági stratégiát, amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését. Az informatikai biztonsági stratégiának rövid-, közép- és hosszú távú célokat kell megfogalmaznia, mellyel a teljes körű védelem hatását keltheti a szervezet. Álláspontom szerint mind emellett másodlagos céljának kell lennie, hogy belső szabályozásában, vagy magában az informatikai biztonsági stratégiában meghatározza az informatikai biztonsági stratégia felülvizsgálatának és frissítésének gyakoriságát ezzel biztosítva a folytonosság alapelvét összhangban az ISO 27001:2013 és ITIL V3 2011-el.
A Rendőrség harmadlagos célja, hogy gondoskodjon arról, hogy az informatikai biztonsági stratégia jogosulatlanok számára ne legyen megismerhető, módosítható. Véleményem szerit, gondoskodnia kell még arról is, hogy az informatikai biztonsági stratégia illeszkedjen az érintett szervezet más stratégiáihoz (így különösen a költségvetési és humánerőforrás tervezéshez, tevékenységi kör változáshoz, fejlesztéshez), jövőképéhez.
A4-es besorolásnak köszönhetően az alábbi adminisztratív követelmények kerültek még

megfogalmazásra a 41/2015. BM rendeletbe:

„4.1.1. az üzemeltetési, vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés, vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;

4.1.2. tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint;

4.1.3. azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt, vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges, vagy bekövetkezett biztonsági esemény kezelését is;

4.1.4. folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer, vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók, vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;

4.1.5. a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;

4.1.6. a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást, vagy biztonsági ellenőrzést kell végezni;

4.1.7. a tesztelés értékelése alapján megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;

4.1.8. az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.”[23]

A rendelet az adminisztratív védekezések tekintetében az alábbi területeket különíti el egymástól:

- Szervezeti szintű alapfeladatok,
- Kockázatelemzés,
- Rendszer és szolgáltatás beszerzés,
- Üzletmenet (ügymenet) folytonosság tervezése,
- Biztonsági események kezelése,
- Emberi tényezőket figyelembe vevő – személy – biztonság,
- Tudatosság és képzés.

Álláspontom szerint ezek olyan általános érvényű védelmi területek, amely szervezet szinten

kell megalkotni, a szervezet egészére kell értelmezni, és a Rendőrség informatikai hálózatok tekintetében az általános szabályokat lebontani és implementálni kell erre a szakterületre.
A szabályok területre bontása alapján meghatározhatóak a védelmi feladatok, a feladatok által pedig eljárás rendek és dokumentációk. Ebből a szemszögből elemzést folytattam le a rendelkezésre álló Rendőrségi dokumentációk és a jogszabályi elvárások között és az alábbiakat állapítottam meg:

- a Rendőrség az informatikai hálózatok tekintetében részletes eljárásokat, irányvonalakat nem fogalmaznak meg a dokumentációk,
- hiányoznak még a gyakorlatban is a fenti eljárások kidolgozásai, a fenti adminisztrációs tevékenységek eredményei,
- a részletezett feladatok még nem kerültek meghatározásra a fenti területeket illetően.

4.2. A FIZIKAI VÉDELMI TERÜLET FEJLESZTÉSI CÉLKITŰZÉSEI

A fizikai védelmi terület célkitűzéseknek meghatározásához rendelet iránymutatásait vettem alapul a 4-es szervezeti biztonsági osztályú besorolás szempontjából. A fizikai védelmi területének elemzéséhez feltételezem, hogy a Rendőrségnél, mint szervezetnél átlagban 4. biztonsági osztálynál magasabb besorolású rendszerek nincsenek, amelyet a Rendőrségi informatikai hálózatok magukba foglalnak. Viszont kutatásaim során megállapítottam, hogy az ESR-112 rendszer 5-ös besorolású rendszerként tartották nyílván.
Hipotézisem szerint a fizikai védelmi intézkedések kiterjednek az információs rendszerelemekhez történő fizikai hozzáférések felügyeletére és további védelmi eszközök alkalmazásával a rendszer fizikai egységeit védik a lehetséges fizikai károk és behatolás ellen. Feltételezem, hogy a Rendőrség, már végzett kockázat elemzést, és teljességgel tisztában van a Rendőrségi informatikai hálózatokat érintő fenyegetettségekkel.
A követelmények között a rendelet előtérbe helyezi a rendelkezésre állás fontosságát, mely szerint ezen besorolásnál feltételezi, hogy tartalék munkahelyek vannak kialakítva, vagy az érintett szervezet által meghatározottak szerint rendelkezésre állnak.
A 4-es besorolás tekintetében további követelményként jelenik meg stratégiai elemként, hogy „különleges személyes adat nagy mennyiségben sérülhet”[23]
A fenti követelményi felsorolásból egyértelműen kitűnik, hogy ezen előírásoknak történő teljes körű megfelelés a Rendőrségi információbiztonsági dokumentum elemzések során nem jelentek meg. Ergo célkitűzésként fogalmazódik meg az alábbi területekre koncentrált eljárások pótlása

- kockázat elemzés,
- fizikai fenyegetettségek vizsgálata,
- tartalék munkahelyek kialakítása.

4.3.A LOGIKAI VÉDELMI TERÜLET FEJLESZTÉSI CÉLKITŰZÉSEI

A logikai védelmi terület célkitűzéseknek meghatározásához a rendelet iránymutatásait vettem alapul a 4-es szervezeti biztonsági osztályú besorolás szempontjából. A logikai védelmi területének elemzéséhez feltételezem, hogy a Rendőrségnél, mint szervezetnél nincsenek 4. biztonsági osztálynál magasabb besorolású rendszerek, (ez alól kivételt képezett az ESR-112 rendszer 5-ös besorolású rendszer, mely a mintavételezésbe nem tartozott bele) amelyet a Rendőrségi informatikai hálózatok magukba foglalnak.
A terület vizsgálatánál a rendelet előtérbe helyezi a „kockázatokkal arányos védelmet. Mely szerint a védelem költségei arányosak a fenyegetések által okozható károk értékével. Ismételten azt a feltételezést érhetjük tetten, mely során a kockázatelemzésre alapozva döntés előkészítések sorozatát célozza meg a követelményrendszer. A biztonsági osztályba sorolás során feltételeznünk kell, hogy a kockázatelemzés eredményeit figyelembe vettük a biztonsági megoldások kidolgozásánál, jelen esetünkben a Rendőrségi informatikai hálózatok tekintetében. Ebből a követelményből is egyértelműen kitűnik, hogy a célkitűzések megvalósításához elengedhetetlen a kockázatelemzés lefolytatása.
Viszont a követelmény sorozatok között nem teljes körű az elvárás. Ezt a tényt az is alátámasztja, hogy a biztonságirányítási célokat és mérési módszereket nem csak meg kell határozni, de teljes körűen alkalmazni is kell. Mindemellett a rendelet egészére mondhatóan megjelenik a visszacsatolás, az ellenőrzés, a tesztelés „intézménye” minden védelmi eljárás terültén. A logikai védelmi terület elemzése során is fény derült arra a tényre, hogy a jogszabályi normatívák által meghatározott minimális elvárások nem jelennek meg a Rendőrség jelenlegi normatív szabályozásában a Rendőrségi informatikai hálózatok tekintetében, ezért logikai védelmi terület célkitűzéseit az alábbiakban rendszerezem:

- kockázat elemzés,
- biztonsági megoldások kidolgozása,
- mérési módszerek meghatározása,
- tesztelések,
- sérülékenység elemzés.

4.4. A CÉLKITŰZÉSEK MEGVALÓSÍTÁSÁNAK FELADATAI - INTÉZKEDÉSEK

A korábbi fejezeteket összegezve, azok eredményeit rendszerezve és a 4-es biztonsági szervezeti szintű besorolást figyelembe véve meghatároztam a bizalmasság, sértetlenség és rendelkezésre állás spektrumán a megvalósítandó biztonsági intézkedéseket alapul véve azt a tényt, hogy a Rendőrségi informatikai hálózatok hármas besorolásúnál magasabb elektronikus információs (fizikai alrendszerek) rendszereként csak a Robotzsaru 4-es besorolású rendszert foglalta magába. Az előzőekben rendszerezett célkitűzések megvalósításához intézkedéseket kell a rendelet szerint meghatározni. Az intézkedések megvalósításának sorrendjét intézkedési tervben kell rögzíteni.

Elemzést végeztem a rendelet mellékletében található útmutató táblázat és a NEIH által rendszeresített biztonsági osztályba sorolást segítő 1700 kérdés soros kérdőívvel kapcsolatban, továbbá a KEKKH által készített segédletet tekintettem át. Az elemzések alapján rendszereztem a Rendőrség számára legfontosabb intézkedések körét. Az intézkedések körét „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 szóló 41/2015. (VII.15.) BM rendelet 3. és 4. mellékleteiben meghatározottak szerint készítettem el, amely alapján az alábbi javaslatot teszem, mint fejlesztési javaslatot a Rendőrség informatikai hálózatának védelmének megteremtésére:

- adminisztratív védelmi intézkedések

Az adminisztratív védelmi intézkedéseket korábban rögzített területekre az alábbiakban rendszereztem:

Szervezeti szintű alapfeladatokra vonatkozó szabályozások

- Az alábbi alapdokumentumokat kell megalkotnia a Rendőrségnek.
- Informatikai biztonságpolitika: (amit ugyan a 2013 évi L.tv. 11.§(1) és d, e, pontokat a 2015. évi CXXX. tv. hatályon kívül helyezte, de a Rendőrségen szándék van rá ,hogy az új informatikai biztonsági szabályzat magába foglalja) megfogalmazza, és a Rendőrségre érvényes követelmények szerint dokumentálja, valamint a Rendőrségen belül kihirdeti az informatikai biztonságpolitikát. Belső szabályozásában, vagy magában az informatikai biztonságpolitikáról szóló dokumentumban meghatározza az informatikai biztonságpolitika

felülvizsgálatának és frissítésének gyakoriságát. Meg kell határozni a kiberbiztonsági célokat, fel kell állítani az informatikai biztonságpolitika Rendőrségi szempontú alapelveit. A politikában be kell mutatni a Rendőrség vezető beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítására és támogatására. A biztonságpolitikában ki kell fejteni a Rendőrségben alkalmazott biztonsági alapelveket és megfelelőségi követelményeket.

- Informatikai biztonsági stratégia: (amelyet ugyan jogszabály eltörölte, mint követelmény) a Rendőrség megfogalmazza, a Rendőrségre érvényes követelmények szerint dokumentálja, és a Rendőrségen belül kihirdeti az informatikai biztonsági stratégiát, amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését. A Rendőrség belső szabályozásában, vagy magában az informatikai biztonsági stratégiában meghatározza az informatikai biztonsági stratégia felülvizsgálatának és frissítésének gyakoriságát. A Rendőrség gondoskodik arról, hogy az informatikai biztonsági stratégia jogosulatlanok számára ne legyen megismerhető, módosítható. Az informatikai biztonsági stratégia rövid-, közép- és hosszú távú célokat tűz ki. Az informatikai biztonsági stratégia illeszkedik a Rendőrség más stratégiáihoz (így különösen a költségvetési és humánerőforrás tervezéshez, tevékenységi kör változáshoz, fejlesztéshez), jövőképéhez.
- Informatikai biztonsági szabályzata megfogalmazza, és a Rendőrségre érvényes követelmények szerint dokumentálja, valamint a Rendőrségen belül kihirdeti az informatikai biztonsági szabályzatot. A Rendőrség más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát. A Rendőrség gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható. Az informatikai biztonsági szabályzatban meg kell határozni:
    - a célokat, a szabályzat tárgyi és személyi hatályát,
    - az elektronikus információbiztonsággal kapcsolatos szerepköröket,
    - a szerepkörhöz rendelt tevékenységet,
    - a Rendőrség tevékenységhez kapcsolódó felelősséget,
    - Rendőrség az információbiztonság szervezetrendszerének belső együttműködését.
- Az informatikai biztonsági szabályzat elsősorban a következő elektronikus

információs rendszerbiztonsággal kapcsolatos területeket szabályozza:

- kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz),
- biztonsági helyzet-, és eseményértékelés eljárási rendje,
- az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (amennyiben az érintett szervezet ilyet végez, vagy végezhet),
- biztonsággal kapcsolatos tervezés (például: beszerzés, fejlesztés, eljárásrendek kialakítását),;
- fizikai és környezeti védelem szabályai, jellemzői,
- az emberi erőforrásokban rejlő veszélyek megakadályozása (pl.: személyzeti felvételi- és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése, stb.),
- az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében,
- az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (amennyiben az érintett szervezetnél ez értelmezhető),
- üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.),
- az elektronikus információs rendszerek karbantartásának rendje,
- az adathordozók fizikai és logikai védelmének szabályozása,
- az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése,
- a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása,
- az adatok mentésének, archiválásának rendje,
- a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárás, ideértve a helyreállítást;

- az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények.

– Az informatikai biztonsági szabályzat tartalmazza a Rendőrség elvárt biztonsági szintjét, valamint az érintett szervezet egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.
– A Szervezeti szintű alapfeladatok között ki kell nevezni az elektronikus információs rendszerek biztonságáért felelős személyeket, illetve biztonságért felelős szervezetet (mely a Rendőrségnél az E-Biztonság-felügyeleti Osztály létrehozásával megtörtént).
– Biztosítani kell a pénzügyi erőforrásokat. A költségvetés tervezés, és a beruházások, beszerzések során tervezni kell az informatikai biztonsági stratégia megvalósításához szükséges forrásokat, továbbá dokumentálni szükséges az e követelmény alá eső kivételeket. A Rendőrség. intézkedik a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állásának biztosítása iránt.
– Meg kell alkotni az intézkedési tervet és meg kell azon mérföldköveket határozni, amelyek a visszacsatolás alapját fogják képezni.
– Fel kell fektetni mindenre kiterjedően, és teljes körűen az elektronikus információs rendszerek nyilvántartását (mely felmérés értékelése a Rendőrségnél folyamatban van).
– Mérési módszertanokat kell bevezetni a biztonsági teljesítmény mérésére.
- Fel kell állítani a szervezeti szintű architektúrát.
- Ki kell dolgozni a kockázatkezelési stratégiát. A stratégia kiterjed: a lehetséges kockázatok felmérésére, a kockázatok kezelésének felelősségére, és a kockázatok kezelésének elvárt minőségére.
- Ki kell dolgozni az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárást.
- Tervet kell kidolgozni a tesztelési eljárásokra, képzésekre és felügyeleti jogkör gyakorlására.
- Kiemelt szerepet kell betölteni a kapcsolattartás területén az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel.

Kockázatelemzésre vonatkozó szabályozások

- Kockázatelemzési eljárásrend, melyben a Rendőrség megfogalmazza, és az érvényes követelmények szerint dokumentálja, valamint kihirdeti a kockázatelemzési eljárásrendet, mely a kockázatelemzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.
- Biztonsági osztályba sorolás.
- Kockázatelemzés (melyről már korábban részletesen írtam).
- Sérülékenység teszt. A Rendőrség informatikai hálózatokban sérülékenység tesztet végez, amennyiben azt a rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik. Meghatározott gyakorisággal, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel a hálózattal kapcsolatban, megismétli a sérülékenység tesztet. Kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;, majd ezek után végrehajtja az ellenőrzési listákat és tesztelési eljárásokat. Felméri a sérülékenység lehetséges hatásait és elemzi a sérülékenység teszt eredményét, amely alapján megosztja a sérülékenység teszt eredményét a szervezet által meghatározott személyekkel és szerepkörökkel.
  - Frissítési képesség: olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel. Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően kell végezni.
  - Privilegizált hozzáférés különleges jogosultsághoz kötött – úgynevezett privilegizált – hozzáférést biztosít a Rendőrség által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.
  - Felfedhető információk: egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat hajt végre.

Rendszer és szolgáltatás beszerzésre vonatkozó szabályozások

- Beszerzési eljárásrendben követelmények szerint dokumentálja a rendszerekhez kapcsolódó szolgáltatások és eszközök beszerzésére vonatkozó szabályait.
- Erőforrás igény felmérése során meghatározza a védelemhez szükséges eszközöket és szolgáltatásokat.
- Beszerzések rendszerre vagy rendszerelemre, szolgáltatásra (ideértve a fejlesztést, adaptálást, rendszerkövetést, karbantartást) vonatkozó szerződéseire szerződéses követelményeket határoz meg. Ilyen lehet funkcionális, garanciális, biztonsággal

kapcsolatos követelmények, védelmi intézkedések tervdokumentáció, megvalósíthatósági tanulmány.

- Az elektronikus rendszerre vonatkozó dokumentációkban a rendszer vagy rendszerelem konfigurációs, telepítési, üzemeltetési dokumentációi, felhasználói leírások, architektúrális leírások.
- Biztonságtervezési elveknél a rendszer vonatkozásában specifikációs meghatározások a tervezés, fejlesztés, kivitelezés, módosítás során.
- Külső elektronikus információs rendszerek szolgáltatásai között kötelezettségként kerül meghatározásra a rendszer információbiztonsági követelményeinek teljes körű betartása.
- Független értékelők esetében független ellenőrök alkalmazása.
- Folyamatos ellenőrzés ellenőrzési terv alapján ütemezetten történhet.

Ügyletmenet- (Ügymenet) folytonosság tervezésre vonatkozó szabályozások

- Üzletmenet-folytonosságra vonatkozó eljárásrendben érvényes követelményrendszert kell kidolgozni a folyamatrendszerekre.
- Üzletmenet-folytonossági terv informatikai erőforrás kiesésére a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára követelmények, kritikus rendszerek alapfunkciók meghatározása, kapacitás tervezés, alapfeladatok és folyamatok folytonossága.
- Folyamatos működésre felkészítő képzés során azon felelősségi körök és szerepkörök meghatározása ahol a képzéseket folyamatosan biztosítani kell.
- Üzletmenet folytonossági terv tesztelése, aktualizálása.
- Biztonsági tárolási helyszín kijelölése ahol a mentések másolatai az elsődleges helyszínnel azonos módon kerülnek eltárolásra.
- Tartalék feldolgozási helyszín biztosítása arra az esetre, amikor az elsődleges helyszín feldolgozási képessége nem áll rendelkezésre. Funkciója, hogy az előre meghatározott műveleteket, előre meghatározott időn belül, összhangban a meghatározott célokkal a tartalék helyszínen újra lehessen kezdeni, vagy folytatni, amíg az elsődleges helyszín helyre áll.
- Infokommunikációs szolgáltatások meghatározása, ahol ki kell szűrni a közös hiba lehetőségeket, priorizálni kell a szolgáltatásokat.
- Az elektronikus információs rendszer mentései, során meghatározott gyakorisággal kell a mentéseket végezni, megtervezni azok helyre állítási sorrendjét, és időintervallumát.

- Az elektronikus információs rendszer helyreállítása és újraindítása folyamán az utolsó ismert állapotba történő helyreállításról és újraindításról egy összeomlást vagy kompromittálódást, vagy hibát követően készített terv.

Biztonsági események kezelésre vonatkozó szabályozások

- Biztonságelemzési eljárásrend, melynek keretében meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.
- A Rendőrségi informatikai hálózat belső és külső kapcsolódásait rendszeresen vizsgálja és dokumentálja.
- Cselekvési tervet készít, ha a vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit, melynek végrehajtását folyamatos ellenőrzi.
- Automatikus eseménykezeléskor mechanizmusokat kell alkalmazni az eseménykezelési eljárások támogatására.
- Információ korrelációsorán a biztonsági események összekapcsolására kell törekedni a egyedi és a szervezeti szintű reagálások koordinálására.
- Biztonsági események figyelése során nyomon követése és dokumentálása a biztonsági eseményeknek.
- Automatikus nyomon követés, adatgyűjtés és vizsgálatánál az automatizált mechanizmusok alkalmazása a megfigyelésre.
- Biztonsági események jelentése során a veszélyhelyzetet és az erre utaló jeleket is kell jelenteni.
- Segítségnyújtás a biztonsági események kezeléséhez támogatás nyújtás a felhasználók irányába a bejelentés és kezelés tekintetében.
- Biztonsági eseménykezelési tervben iránymutatás a biztonsági események kezelésének módjára.
- Képzés a biztonsági események kezelésére a felhasználók számára kijelölt szerep- és felelősségi körökben folyamatos képzések tartása a biztonsági események kezelésére.

Emberi tényezőket figyelembe vevő – személy – biztonságra vonatkozó szabályozások

- Személybiztonsági eljárásrendet készít, melyben rögzíti a munkakörök, feladatok biztonsági szempontú besorolását, a személyek ellenőrzésének eljárását, automatikus figyelmeztetést ad ki ha veszélyhelyzet áll fenn és adott esetben fegyelmi intézkedéseket foganatosít.
- Munkakörök, feladatok biztonsági szempontú besorolásakor pl. nemzetbiztonsági ellenőrzés alá eső munkakörök meghatározása a fontos.
- Személyek ellenőrzésekor hozzáférési engedélyek megadása előtti ellenőrzések lefolytatása.
- Eljárás a jogviszony megszűnésekor meghatározott időpontban a hozzáféréseket meg kell szüntetni. Célszerűnek tartom az összes szoftveres rendszert közös címtárhoz kapcsolni, a módosítások és törlések automatikus átvezetése, valamint az esemény elemzések eredményesebb lefolytathatósága érdekében.
- Nyilvántartások segítségével az áthelyezések, átirányítások és kirendelések kezelése.
- Külön követelményeket kell meghatározni a Rendőrséggel szerződéses jogviszonyban álló (külső) szervezetre.
- Fegyelmi intézkedések során a belső információbiztonsági eljárásokat megszegőkkel szembeni eljárás lefolytatása.
- Viselkedési szabályok az Interneten, olyan nyílt interneten nyilvános internetes oldalak használatának engedélyezett módját és illegális közzététel tiltását tartalmazó dokumentum, amelyben a tevékenységi körök meghatározására törekszünk.

Tudatosság és képzésre vonatkozó szabályozások

- Képzési eljárásrendet készít a Rendőrségi informatikai hálózat kezelői részére, ahol kiemelt figyelmet kell fordítani a biztonság tudatosság és a belső fenyegetés téma területére. Szerepkör, vagy feladat alapú biztonsági képzést kell rendszeresen folytatni, melyeken az új trendekre felhívják a figyelmet.
- A biztonsági képzésre vonatkozóan állandóan rendelkezésre és elérhetővé tételre kell tenni a dokumentációkat.

- a fizikai védelmi intézkedések

A fizikai és környezeti védelmi intézkedéseket korábban rögzített területekre az alábbiakban rendszereztem:

Fizikai védelemre vonatkozó szabályozások

- Fizikai védelmi eljárásrendben az érintett létesítményekre vagy helyiségekre érvényes fizikai védelmi eljárásrendet, amely a Rendőrség elektronikus információbiztonsági, vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.
    - Fizikai belépési engedélyekben összeállítja, jóváhagyja és kezeli a Rendőrség informatikai hálózatainak helyt adó létesítményekbe belépésre jogosultak listáját. Továbbá a belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére. Mindemellett rendszeresen felül kell vizsgálni a belépésre jogosult személyek listáját és eltávolítani a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt. Az épületekbe történő belépés és zónákba történő bejutáshoz a kockázat elemzés és osztályba sorolás lapján elektronikus kártyás beléptetési rendszereket kell kialakítani célszerűen a nyilvántartásukat hozzákapcsolva a központi címtárhoz.
- A fizikai belépés ellenőrzése során a Rendőrség által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést. Naplózni kell a fizikai belépéseket és ellenőrzés alatt kell tartani a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket. Kísérni kell a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követni a tevékenységüket. Intézkedéseket kell tenni a kulcsok, hozzáférési kódok, és az egyéb fizikai hozzáférést ellenőrző eszközök védelmére. Nyilvántartást kell vezetni a fizikai belépést ellenőrző eszközről. A hozzáférési kódokat és kulcsokat meghatározott rendszerességgel meg kell változtatni akkor pedig azonnal, ha a kulcs elveszik vagy, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát. Az egyéni belépési engedélyeket a belépési pontokon kell ellenőrzi, továbbá a kijelölt pontokon való átjutást felügyelni kell a Rendőrség által meghatározott fizikai belépést ellenőrző rendszerrel, vagy eszközzel.
- Hozzáférés az adatátviteli eszközökhöz és csatornákhoz hozzáférés során meghatározott biztonsági védelemmel ellenőrzi kell az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

- Kimeneti eszközök hozzáférés ellenőrzése során a rendszer kimeneti eszközeihez való fizikai hozzáférést kell kontrollálni annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.
- A fizikai hozzáférések felügyelete során a Rendőrségi informatikai hálózatoknak helyet adó létesítményekbe történt fizikai hozzáféréseket felügyelni kell annak érdekében, hogy észlelésre kerüljön a fizikai biztonsági esemény és reagálás történjen. Ennek keretében rendszeresen át kell vizsgálni a fizikai hozzáférésekről készült naplókat össze kell hangolni a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.
- A látogatók ellenőrzésekor meg kell őrizni a látogatói belépésekről szóló információkat, és adott esetben ellenőrizni.
- Áramellátó berendezések és kábelezés esetén rendszert árammal ellátó berendezéseket és a kábelezést védeni kell a sérüléssel és rongálással szemben és tartalék áramellátás biztosítása szükséges.
- Vészkikapcsoláskor a rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására történik vészhelyzetben.
- Vészvilágítás területén, a Rendőrségen egy automatikus vészvilágítási rendszert kell alkalmaznia és karban kell tartania, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.
- Tűzvédelem esetén a Rendőrségi informatikai hálózatok számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket kell alkalmaznia, és karbantartania.
- Hőmérséklet és páratartalom ellenőrzése során az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) figyelni kell a hőmérséklet és páratartalom szintjét.
- Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem során a Rendőrségi informatikai hálózatokat védeni kell a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró szelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek legyenek. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során biztosítani kell, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.

- Be- és kiszállítás során a Rendőrség engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.
- Ellenőrzéskor ellenőrizni kell a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.
- Szállítási felügyelet során védeni kell az információt tartalmazó karbantartási eszközt a jogosulatlan elszállítással szemben.
- Karbantartók esetében ki kell alakítani egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről.

- a logikai védelmi intézkedések

A logikai védelmi intézkedéseket korábban rögzített területekre az alábbiakban rendszereztem:

Általános védelmi intézkedésekre vonatkozó szabályozások

- Engedélyezési eljárás rend, mely kiterjed emberi, fizikai és logikai erőforrásra. továbbá eljárási és védelmi szintre és folyamatra, illetve a kapcsolódásai belső és külső rendszerekhez.

Tervezésre vonatkozó szabályozások

- Biztonsági szabályzat rögzíti a biztonságtervezési eljárás folyamatait, valamint biztosítja annak ellenőrzését.
- Cselekvési terv, intézkedéseket határoz meg arra vonatkozóan, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosság kerül megállapításra.
- Személyi biztonság a hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet szabályozza.
- Információbiztonsági architektúra leírásban összegzi az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést. Megfogalmazza, hogy az

információbiztonsági architektúra miként illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt. Leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket. A szabályozás kialakítása során javasolt eljárni az ISO 27001:2013, illetve az ITIL V3 :2011 szerint.

Rendszer és szolgáltatás beszerzésre vonatkozó szabályozások

- Beszerzési eljárásrend keretében meg kell határozni az erőforrás igényeket felmérés keretében.
- A rendszerek teljes életútján, életciklusuk minden lépésénél figyelemmel kell kísérni informatikai biztonsági helyzetüket.
- A rendszer életciklusai: követelmény meghatározás, fejlesztés vagy beszerzés, megvalósítás vagy értékelés, üzemeltetés és fenntartás, kivonás (archiválás, megsemmisítés). Amennyiben a rendszernek van utód rendszere, akkor a kivonás előtt migráció vagy áttérés történik.
- Beszerzések keretében kiemelt figyelmet kell fordítani a funkciókra – protokollokra – szolgáltatásokra, továbbá a külső hálózati szolgáltatásaira.
- Fejlesztői változáskezelés során, a fejlesztő vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során.
- Fejlesztői biztonsági tesztelés: a fejlesztő készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat.
- Fejlesztési folyamat, szabványok és eszközök: meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat.
- Fejlesztői oktatás: oktatási kötelezettséget ír elő az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára.
- Fejlesztői biztonsági architektúra tervezés: specifikációt és biztonsági architektúrát kell megalkotni.

Biztonsági elemzésre vonatkozó szabályozások

- Biztonságelemzési eljárásrend, melynek keretében meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi

intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.

- Biztonsági értékeléseknél tervet kell készíteni, melynek tartalmaznia kell: az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseke.
- A speciális értékelés a védelmi intézkedések értékelése keretében bejelentés mellett, vagy bejelentés nélkül sérülékenység vizsgálatot, rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, az érintett szervezet által meghatározott egyéb biztonsági értékeléseket végeztet.
- A biztonsági teljesítmény mérése során kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

Tesztelés, képzés és felügyeletre vonatkozó szabályozások

- Felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.
- A biztonsági teljesítmény mérése, kifejleszti és felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.
- Sérülékenység teszt olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.

Konfigurációkezelésre vonatkozó szabályozások

- Konfigurációkezelési eljárásrendben a változások sorozatát rögzíti a Rendőrség az informatikai hálózatok felépítése során.
- Alapkonfiguráció, mely során az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.
- A konfigurációváltozások felügyelete (változáskezelés) mely során a Rendőrség meghatározza a változáskezelési felügyelet alá eső változástípusokat. Egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.). Röviden dokumentálja az elektronikus információs rendszerben történt változtatásokat és visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását, továbbá auditálja és felülvizsgálja

a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

- Előzetes tesztelés és megerősítés során a konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az informatikai hálózat változtatásait az éles rendszerben történő megvalósítása előtt.
- Biztonsági hatásvizsgálat során meg kell vizsgálni a Rendőrségi informatikai hálózatban tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.
- Konfigurációs beállítások során a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott módon – a „szükséges minimum" elv alapján – kell végezni a Rendőrség informatikai hálózatokban használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálnia kell. El kell végezni a konfigurációs beállításokat a Rendőrség informatikai hálózatok valamennyi elemében, majd a meghatározott elemek konfigurációs beállításaiban azonosítani, dokumentálni kell minden eltérést. Mindezek mellett figyelemmel kísérni és ellenőrizni kell a konfigurációs beállítások változtatásait, a Rendőrség belső szabályzataival és eljárásaival összhangban.
- Legszűkebb funkcionalitásokat meg kell határozni a Rendőrség informatikai hálózatokra, mely során olyan konfigurációt kell létrehozni, hogy az csak a szükséges szolgáltatásokat nyújtsa. Meg kell határozni a tiltott, vagy korlátozott, nem szükséges funkciókat, protokollokat, szolgáltatásokat, szoftverek használatát.
- A Rendőrség informatikai hálózatainak rendszerelemeiről leltárt kell készíteni (Forrás SQL), mely pontosan tükrözi az aktuális állapotát, a hatókörébe eső valamennyi hardver- és szoftverelemet. Kellően részletesnek kell lennie a nyomkövetéshez és a jelentéskészítéshez.
- Konfiguráció kezelési tervvel bevezet egy folyamatot a konfigurációelemek azonosítására a rendszer-fejlesztési életciklus folyamán és a konfigurációelemek konfigurációjának kezelésére.
- A szoftverhasználat korlátozásai: a Rendőrség informatikai hálózatokon kizárólag olyan szoftvereket és kapcsolódó dokumentációt lehet használni, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak. Másolatok, megosztások ellenőrzésére nyomon kell követni

a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát. Ebben a körben ellenőrizni és dokumentálni kell az állomány megosztásokat.

- A Rendőrség informatikai hálózatokon a felhasználó által telepített szoftverek körét alapesetben tiltani, illetve ellátott feladatkörhöz kötötten szükséges meghatározni a felhasználó által végezhető konfigurálási és telepítés műveletek körét.

Karbantartásra vonatkozó szabályozások

- A Rendőrség informatikai hálózatok karbantartási eljárásrendjében rögzíteni kell a rendszeres ütemezett karbantartásokat és javításokat Dokumentálni és felülvizsgálni kell a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a szervezeti követelményeknek megfelelően. Minden esetben nyilvántartást kell vezetni a karbantartókról.
- Távoli karbantartás esetén jóváhagyni, nyomon követni és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket.

Adathordozók védelmére vonatkozó szabályozások

- A Rendőrség informatikai hálózatokon alkalmazható adathordozók védelmére vonatkozó eljárásrendet kell készíteni, melyben rögzíteni kell a hozzáférések szabályait az adathordozókhoz. Az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát szabályzatban kell meghatározni.
- A Rendőrségi informatikai hálózatokon alkalmazható adathordozók törlése során a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal kell törölni az a meghatározott adathordozóikat a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt. A törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően kell alkalmazni.
- A Rendőrségi informatikai hálózatokon az adathordozók használatát a Rendőrség engedélyezheti, korlátozhatja, vagy tilthatja. Az egyes, vagy bármely adathordozó típusok használatát a Rendőrségi informatikai hálózatokon vagy elemeken működő biztonsági intézkedésekkel (eljárásrenddel és rendszerekkel) szükséges szabályozni.

- Az adathordozókhoz történő hozzáférés során ki kell jelölni az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát.
- Fel kell címkézni az adathordozókat, meg kell jelölni az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak
- Az adathordozók tárolásánál fizikailag ellenőrizni kell, hogy biztonságosan tárolja az adathordozókat, az arra engedélyezett vagy kijelölt helyen.
- Adathordozók szállításánál meghatározott biztonsági óvintézkedésekkel kell védeni és ellenőrizni az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán.

Azonosítás és hitelesítésre vonatkozó szabályozások

- Azonosítási és hitelesítési eljárásrendben rögzíteni kell azokat a Rendőrségi informatikai hálózatokon történő azonosítási és hitelesítési módszereket, szabályokat, melyek során az informatikai rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, továbbá naplózza a felhasználók által végzett tevékenységet.
- A Rendőrség informatikai hálózatokon a privilegizált fiókokhoz, illetve alkalmazásokhoz történő hálózati hozzáférések esetén többtényezős hitelesítést kell alkalmazni.
- A Rendőrség informatikai hálózatokon az azonosító kezelés az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a Rendőrség által meghatározott személyek vagy szerepkörök jogosultságához kell kötni. Hozzá kell rendelni az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz, meghatározott időtartamig meg kell akadályozni az azonosítók ismételt felhasználását, További intézkedéseket kell tenni a meghatározott időtartamú inaktivitás esetén, le kell tiltani az azonosítót.
- A hitelesítésre szolgáló eszközök kezelése során ellenőrizni kell a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát, kiosztását, visszavonását, visszacsatolását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket.
- Szervezeten kívüli felhasználók esetében az azonosítás és hitelesítés során egyedileg kell azonosítani és hitelesíteni a felhasználókat, és tevékenységüket.

- Hitelesítés szolgáltatók tanúsítványának elfogadása során csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el a Rendőrség, mint állami szervezet a szervezeten kívüli felhasználók hitelesítéséhez. A más szervezetekkel történő kapcsolattartás esetében a Rendőrségi iratoknak is ilyen módon hitelesítettnek kell lennie. A belső munkafolyamatokban is javasolt a NMHH által is elfogadott hitelesítés bevezetése. Költség és rendszer megbízhatóság szempontjából mérlegelendő a saját auditált elektronikus aláírási infrastruktúra megvalósítása.

Hozzáférés ellenőrzésre vonatkozó szabályozások

- Hozzáférés ellenőrzési eljárásrendben kezelni kell a felhasználói fiókokat, ki kell alakítani a csoport- és szerepkör tagsági feltételeket, létrehozni, engedélyezni, módosítani, letiltani, eltávolítani, és ellenőrizni a felhasználói fiókokat.
- Hozzáférés ellenőrzés érvényesítése során érvényesíteni kell a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.
- Sikertelen bejelentkezési kísérletek szabályozása során a Rendőrség által meghatározott esetszám korlátot kell alkalmazni a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. Ha ezt túllépi a felhasználó, automatikusan zárolni kell a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késleltetni kell a következő bejelentkezési kísérletet.
- A rendszerhasználat jelzése elengedhetetlen a Rendőrség esetében. Olyan figyelmeztető üzenetet vagy jelzést kell küldenie a hálózatot felhasználó számára a hozzáférés engedélyezése előtt, mely jelzi, hogy a felhasználó a Rendőrség informatikai hálózatát használja, mely használatot figyelhetik, rögzíthetik, naplózhatják, továbbá a jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár. Ez azt jelentheti, hogy a Rendőrségi informatikai hálózat használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti. Ezt a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn kell tartani, amíg a felhasználó közvetlen műveletet nem végez a hálózatba való bejelentkezéshez vagy további hozzáféréshez.
- A Rendőrségnél az azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek során ki kell jelöli azokat a felhasználói tevékenységeket, amelyeket a Rendőrségi informatikai hálózat azonosítás vagy hitelesítés nélkül is végre lehet hajtani. Ezeket

dokumentálni és indokolni kell a rendszerbiztonsági tervben, vagy más szabályzatban.

- A Rendőrségnél a távoli hozzáférés engedélyezéséhez ki kell dolgozni és dokumentálni kell minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat.
- A vezeték nélküli technológiák kapcsán belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót kell kiadni.
- Mobil eszközök hozzáférés ellenőrzésére olyan eljárást kell kidolgozni, melyben belső szabályozásában kell rögzíteni a felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót a szolgálati mobil eszközökre.
- A mobil hozzáférések esetében célszerű a teljes körű MDM rendszer kialakítása, mely megfelelő biztonsággal kezeli mind a szervezeti, mind a magántulajdonú eszközök hozzáférését és távoli security menedzselését.
- Külső hálózatok használatánál meg kell határozni, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső hálózatból hozzáférni a Rendőrségi informatikai hálózatához. A hozzáférés mellett a szabályozásban ki kell térni, hogy a külső hálózat segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a Rendőrség által ellenőrzött információkat.
- Nyilvánosan elérhető adat tartalom megjelenítése esetén ki kell jelölni azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető Rendőrségi informatikai hálózaton a Rendőrséggel kapcsolatos bármely információ közzétételére. A kijelölt személyeket képzésben kell részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat és mindemellett a közzététel előtt át kell vizsgálni a javasolt tartalmat.

Rendszer és információ sértetlenségre vonatkozó szabályozások

- Rendszer- (jelen esetben a hálózat) és információsértetlenségre vonatkozó eljárásrendet rögzíteni kell az informatikai biztonsági szabályzatban, melynek ki kell térni a vonatkozó szabályzatra és az ahhoz kapcsolódó ellenőrzések megvalósítását.
- Hibajavítás során olyan belső eljárásrendet kell kialakítani, amely során azonosítja, jelenti és kijavítja vagy kijavíttatja az Rendőrségi informatikai hálózatot üzemeltető személyzet a hibákat. Az eljárásrendnek tartalmaznia kell a szoftver és hardver

telepítések előtti teszteléseket, a hibajavítással kapcsolatos szoftverfrissítéseket a feladatellátás hatékonysága és a szóba jöhető következmények szempontjából. Kiemelt figyelmet kell benne fordítani a biztonságkritikus szoftverek frissítésének kiadását követő meghatározott időtartamon belül telepítésre. Be kell építeni a hibajavítást a konfigurációkezelési folyamatba.

- Kártékony kódok elleni védelemre olyan eljárást kell kidolgozni, mely a Rendőrség informatikai hálózatok belépési és kilépési pontjain védelmet alakít ki a kártékony kódok ellen, továbbá felderíti és megsemmisíti azokat. Folyamatosan frissíteni kell a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályokkal és eljárásokkal összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg. A kártékony kódok elleni védelmi mechanizmusokat úgy kell konfigurálni, hogy a védelem eszköze rendszeres ellenőrzéseket hajtson végre a Rendőrség informatikai hálózatokon, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon a biztonsági szabályzatnak megfelelően, a hálózati belépési, vagy kilépési pontokon, amikor a fájlokat letöltik, megnyitják, vagy elindítják. A kártékony kódot észlelése esetén blokkolni vagy karanténba kell helyezni, és azonnal riasztani kell a rendszeradminisztrátort. Az eljárás rendbe be kell építeni a rendszeres ellenőrzést, a téves riasztásokra, a kártékony kód észlelésére és megsemmisítése során, valamint figyelembe kell venni ezek lehetséges kihatását a Rendőrségi informatikai hálózatainak rendelkezésre állása szempontjából.
- A hálózati rendszer határokon adat szűrést forgalom szabályozást és szükség szerint titkosítást kell végezni.
- A Rendőrségi informatikai hálózat felügyelete során kiemelt figyelmet kell fordítani a kibertámadások észlelésére. Ki kell jelölni kibertámadások jeleit figyelő célokat, mely szerint fel kell tárni a jogosulatlan lokális, hálózati és távoli kapcsolatokat, melyeket azonnal azonosítani kell. Felügyeleti eszközöket kell alkalmazni olyan alapvető információk gyűjtése mint a Rendőrségi informatikai hálózat ad hoc területei és a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére. Folyamatosan védeni kell a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. A felügyelet során erősíteni és koncentrálni kell az erőforrásokat minden olyan esetben, amikor fokozott kockázatra utaló jel észlelése történt. Meghatározott gyakorisággal biztosítani kell az Ibtv. által előírt felügyeleti információkat az Ibtv.-ben meghatározott személyeknek és

szerepköröknek.

- Biztonsági riasztások és tájékoztatások kezelésének rendjét kell felállítani. Melyben folyamatosan figyelni kell a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, illetve a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket. Ha indokolt akkor ezek alapján belső biztonsági riasztást és figyelmeztetést kell kiadni az állomány irányába. Belső szabályzóban ki kell alakítani az Ibtv. végrehajtási rendeleteiben meghatározott esemény bejelentési kötelezettség rendszerét és naprakész kapcsolatot kell fenntartani a meghatározott szervekkel.
- A Rendőrségi informatikai hálózat kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kell kezelni és megőrizni.

Naplózás é elszámoltathatóságra vonatkozó szabályozások

- Naplózási eljárásrendben a meg kell határozni a naplózható és naplózandó eseményeket, melyre fel kell készíteni és alkalmassá kell tenni a Rendőrségi informatikai hálózatot. Olyan naplóeseményeket kell rögzíteni, amelyeknek megfelelőnek kell lenniük a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához. Kellő körültekintéssel meg kell határozni az eljárásrendben a napló tárkapacitását a Rendőrségi informatikai hálózat biztonsági osztályba sorolásához viszonyítva.
- Naplóbejegyzések tartalmát úgy kell meghatározni, hogy a naplóbejegyzésekben elegendő információ legyen ahhoz, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.
- Naplózási hiba kezelését az eljárás rendben kell rögzíteni, hogy naplózási hiba esetén riasztást küldjön a Rendőrségi informatikai hálózat felügyelő rendszer a dedikált személyeknek vagy szerepköröknek. Az eljárásrendben rögzíteni kell a végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását. stb.
- A naplókat rendszeresen felül kell vizsgálni és elemezni a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, melyről adott esetben jelentést kell készíteni a felettes szervnek megküldeni.
- A Rendőrségi informatikai hálózat időbélyeg alkalmazása során a belső rendszerórákat

kell használni a naplóbejegyzések időbélyegeinek előállításához. Az időbélyegeket rögzíteni kell a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a Rendőrség által meghatározott időmérési pontosságnak. Az állandó szinkronizálás érdekében meghatározott gyakorisággal össze kell hasonlítani a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálni kell a belső rendszerórákat a hiteles külső időforrással.

- A Rendőrségi informatikai hálózat naplóinformációit és a naplókezelő eszközöket meg kell védeni a jogosulatlan hozzáféréssel, módosítással és törléssel szemben, azokat csak privilegizált felhasználók jogosultak kezelni. A naplóinformációkat meghatározott gyakorisággal el kell menteni, egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszerelemre.
- A naplóbejegyzések meghatározott ideig meg kell őrizni a biztonsági események utólagos kivizsgálásának biztosítása érdekében.
- Naplógenerálás folyamatánál meg kell határozni, hogy mely naplózható események legyenek naplózva a Rendőrségi informatikai hálózat egyes elemeire.

Rendszer és kommunikációvédelemre vonatkozó szabályozások

- Rendszer- és kommunikációvédelmi eljárásrendben szét kell választani az Alkalmazásokat, a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat), az irányítási funkcionalitásokat, biztonsági funkciókat.
- A Rendőrségi informatikai hálózat határainak védelme során felügyelni és ellenőrizni kel a külső határain történő, valamint a hálózat kulcsfontosságú belső határain történő kommunikációt.
- A Rendőrségen a határvédelem és titkosítás rendszere egy hosszú folyamat eredményeként jött létre, a jelenlegi eljárásrend egységes rendszerbe foglalására és felülvizsgálatára van szükség.
- A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokba kell helyezni, el kell különíteni a belső szervezeti hálózattól. A biztonsági architektúrával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül lehet kapcsolódni külső hálózatokhoz. Korlátozni kell a külső hálózati kapcsolatok számát. Felügyelni kell a külső infokommunikációs szolgáltatáshoz kapcsolt interfészt, melyekre forgalomáramlási szabályokat kell kialakítani a tűzfalnyitási szabályzatban. Védeni kell az összes interfésznél az átvitelre

kerülő információk bizalmasságát és sértetlenségét. Minden forgalomáramlási szabályok alóli kivételt dokumentálni kell a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt. Naprakészen kell tartani a tűzfalnyitási szabályzatot, meghatározott gyakorisággal át kell tekinteni a forgalomáramlási szabályok alóli kivételeket, és el kell távolítani azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol. A Tűzfalszabályzatban rögzíteni kell az együttműködésen alapuló számítástechnikai eszközök használatának indokait és listáját.

- Titkosítási szabályzatban rögzíteni kell a Rendőrség titkosítási eljárás rendjét. Olyan kriptográfiai védelmet kell benne választani, amely szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg. A szabályzatban rögzíteni kell a kriptográfiai kulcs előállításának és kezelésének szétosztásának, tárolásának, hozzáférésének és megsemmisítésének szabályait.

A biztonsági eseményekre történő reagálás, a biztonsági eseményekre vonatkozó szabályozások

- Biztonsági eseménykezelési eljárásrendet kell felfektetni. Melyben rögzíteni kell a képzések rendjét a kijelölt szerepkörökkel és felelősségekkel összhangban a biztonsági események kezelésére, figyelésére, jelentésére, segítségnyújtásra. Az eljárásrendet folyamatos frissíteni kell szimulációs gyakorlatok keretében szerzett új tapasztalatok alapján.
- Biztonsági eseménykezelési tervet kell készíteni, mely magában foglalj az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást. Pontosan meg kell határozni a bejelentés köteles biztonsági eseményeket, azok kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszerét.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Jelen fejezetben, a hipotézisek negyedik pontjában feltételezettek bizonyítására, a korábbi fejezetek elemzéseit és eredményeit felhasználva, három fejlesztési területet határoltam el a Rendőrség informatikai hálózatok fejlesztési területén belül. Ezek olyan meghatározásokat öleltek fel, melyek elengedhetetlenek ahhoz, hogy a Rendőrségi informatikai hálózatok

védelmét a törvények szerint a Rendőrség garantálni tudja. A fejlesztési javaslataim alapvetően három irányt határoznak meg: első sorban az adminisztratív irányvonalat, majd a logikai és fizikai irányvonalakat. Az irányvonalakat szervezeti szinten és a Rendőrségi informatikai hálózatok szintjén határoztam meg. Az irányvonalak segítségével konkrét feladatokat és egyben intézkedések körét rendszereztem és csoportosítottam. Az intézkedések körét javaslataim alapján rögzíteni kell az alábbi szabályzatokban:

- Szervezeti szintű alapfeladatok, melyben ki kell térni az alábbi alszabályzókra
    - Kockázatelemzés,
    - Rendszer és szolgáltatás beszerzés,
    - Üzletmenet (ügymenet) folytonosság tervezése
    - Biztonsági események kezelése,
    - Emberi tényezőket figyelembe vevő – személy – biztonság,
    - Tudatosság és képzés.
- Fizikai védelmi eljárásrend, melynek magába kell foglalnia az alábbi rész szabályzókat
    - Fizikai belépési engedélyek,
    - A fizikai hozzáférések felügyelete,
    - A látogatók ellenőrzése,
    - Vészvilágítás,
    - Tűzvédelem,
    - Hőmérséklet és páratartalom ellenőrzése,
    - Be- és kiszállítás.
- Logikai védelmi eljárás rend, melynek ki kell térnie az alábbi szabályzatokra
    - Általános védelmi intézkedések
    - Tervezés,
    - Rendszer és szolgáltatás beszerzése,
    - Biztonsági elemzés,
    - Tesztelés, képzés és felügyelet,
    - Konfigurációkezelés,
    - Karbantartás,
    - Adathordozók védelme,
    - Azonosítás és hitelesítés,
    - Hozzáférés ellenőrzése,
    - Rendszer- és információsértetlenség,
    - Naplózás és elszámoltathatóság,

- Rendszer- és kommunikációvédelem,
- Reagálás a biztonsági eseményekre.

Összegezve jelen fejezetben bebizonyítottam, hogy a Rendőrség informatikai hálózatának jövőképe meghatározható, javaslatok teljesítése útján felépíthető. Olyan területek határoltam el a jövőkép alkotása során, melyeket, ha egyenként megvalósítanak a Rendőrség fejlesztői, már akkor is előrelépést és eredményeket érnek el a védelem és a biztonság területén. Egy olyan biztonságos informatikai hálózat jövőképét festettem fel a fejezetben, mely informatikai hálózat biztonsági szegmensei az Európai Unió bármely állami szervezetében megállná a helyét.

ÖSSZEFOGLALÁS

A kutatásaimat a Rendőrségi informatikai hálózat védelmének, vizsgálatának jelen idejű képbehelyezésre és jövőkép alkotásra irányítottam értekezésemben.
A kutatás célja a Rendőrségi informatikai hálózat védelme középtávú fejlesztési irányainak elemzésekre épített meghatározása volt, melyet négy fejezeten keresztül összefüggések vizsgálatán keresztül határoztam meg.

A kutatás részcéljai között meghatároztam

- a magyar Rendőrségi informatikai hálózata védelmével szemben támasztott követelményeket és rendszereztem azokat,
- a magyar Rendőrségi informatikai hálózat védelme során alkalmazható eszközöket és módszereket elemzések útján bemutattam,
- a magyar Rendőrségi informatikai hálózat védelme fejlesztési irányain keresztül meghatároztam azon intézkedések és feladatok körét mely útján a Rendőrség teljesítheti a törvények előírásait.

Rendőrségi informatikai hálózatok és védelmük alapjai fejezetben az informatikai hálózatok alapjait összegeztem. A Rendőrségi informatikai hálózatokat sajátosságaik alapján bemutattam, elemeztem. A Magyar Rendőrség informatikai hálózatának leírásán, és jellemzésén keresztül rámutattam az informatikai hálózatok biztonságának fontosságára, összegeztem védelmének alapjait. Értékeltem a Magyar Rendőrség informatikai hálózatának biztonsági helyzetét.

A Rendőrség informatikai hálózatának védelmével szemben támasztott követelmények fejezetben a hálózat vizsgálatának segítségével a biztonsági követelményeket meghatározó tényezőket, és a körülményeket összegeztem, rendszereztem. A Rendőrség informatikai hálózatának biztonságát veszélyeztető fenyegetések feltárásával és elemzésével feltártam a biztonsági követelményekhez kapcsolódó kérdéseket. A Rendőrség informatikai biztonsági filozófiája és politikája kereteinek megfogalmazását követően körvonalazódtak ki a Rendőrség informatikai biztonsági célkitűzései ezzel meghatározásra kerültek a Rendőrség informatikai hálózatának védelmével szemben támasztott követelményei.

A Rendőrség informatikai hálózatának védelme során alkalmazható eszközök és módszerek fejezetben a hálózatok védelme során alkalmazható módszereket, eszközöket, eljárásokat rendszereztem és elemeztem. A fejezetben feltártam a Rendőrség informatikai hálózatában jelenleg alkalmazott védelmi módszereket, eszközöket. Bemutattam és értékeltem az

eljárásokat, majd meghatároztam az eszközöknek és módszereknek a Rendőrségi informatikai hálózat védelme során történő alkalmazásának kritériumait, azok előnyeit és hátrányait.

A Rendőrség informatikai hálózat védelmének fejlesztési irányai és feladatai fejezetben a Rendőrség informatikai biztonsági stratégiai alapok meghatározásával megalkottam Rendőrségi informatikai hálózat védelmének fejlesztési irányait, az egyes fejlesztési területek célkitűzéseit megvalósításuk feladatait és intézkedéseit körvonalaztam.

Az értekezésben kiemelt kutatásokat folytattam, mely során meghatároztam a Rendőrség informatikai hálózat biztonság helyzetét, személyi, szolgáltatási és tárgyi vonatkozású veszélyeztetettségi pontjait, az azokat, érő fenyegetéseket, sérülékenységeit.
Tekintettel arra, hogy jelenleg a Rendőrség még nem rendelkezik, - csak folyamatban a kidolgozása – egy olyan elfogadott informatikai biztonsági dokumentációval, mely egyértelműen meghatározná a Rendőrség ilyen irányú elgondolásait, véleményem szerint az informatikai biztonság politikának a már megfogalmazott informatikai biztonság filozófiára kell épülnie, és megfelelő alapot kell teremtenie az informatikai biztonsági célkitűzések meghatározásához. Minden lehetséges esetben a megelőzésre törekvő magatartást kell előnyben részesítenie a követő magatartással szemben, elvégre alapozó dokumentumot kell létrehoznia a védelem érdekében. Az informatikai biztonsággal összefüggő szabályoknak, intézkedéseknek egységes értelmezését kell elősegítenie.

Az elemzéseim során a támadás típusok meghatározásával rá kívántam mutatni, hogy mely biztonsági követelmények meglétével védhetők ki a támadások. A követelmények meglétének hiányát feltételezve, taglalni kívántam a sérülékenység mátrixszal, hogy milyen eredményeket okozhatnak az általam meghatározott támadások az informatikai hálózat biztonsági állapotában.
Meghatároztam a Rendőrség informatikai hálózatának biztonsági osztályba sorolását és működés megbízhatóság szerinti osztályozását.
A kutatásaimat és azok eredményeinek valóság alapját a Belügyminisztérium tudományos kutatói gyakornoki rendszer keretében az Országos Rendőr-főkapitányság informatikai szakembereinek egyetértésében közösen átvizsgáltuk, melynek következtében kutatásaimat lezártam 2018.02.28-án.

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.

KÖVETKEZTETÉSEK

1. A magyar Rendőrségi informatikai hálózata védelmével szemben támasztott követelmények meghatározásával és rendszerezésével megállapíthatók a védelem során alkalmazható eszközök és módszerek.
2. A magyar Rendőrségi informatikai hálózat védelme fejlesztési irányain keresztül meghatározhatók azon intézkedések és feladatok köre mely segítségével a teljes védelem a hálózat teljes spektrumán biztosítható.

JAVASLATOK

A feldolgozott irodalmakat és elemzések eredményeit figyelembe véve a Rendőrség informatikai hálózatának biztonsági követelményeivel kapcsolatos kérdéskörökben az alábbi javaslatokat teszem:

1. 1. A MeH ITB 12. számú ajánlás Informatikai Rendszerek Biztonsági Követelményei fejezetében megfogalmazottak szerint és a 41/2015. (VII. 15.) BM rendelet osztályba sorolása alapján a Rendőrség informatikai hálózatát javasolnám a 4-

es szintbe sorolni, mert a Rendőrségi hálózaton zárt célú elektronikus információs rendszer üzemeltetése és fejlesztése folyik azon felül, hogy azon felül, hogy nagy tömegű különleges személyi adatok és a nagy értékű üzleti titkok feldolgozása, tárolása is történik. Alacsonyabb szint megkövetelése sértené a Rendőrség és az állampolgárok érdekeit, mert ez esetben a Rendőrség informatikai hálózatának sérülése során nem lenne megfelelően garantálható a három biztonsági alapelv (bizalmasság, rendelkezésre állás, sértetlenség) érvényre jutása.

2. Megbízhatósági elemzés alapján a Rendőrség informatikai hálózatát véleményem szerint megbízható működési kiemelt biztonsági (MM-K) osztály: 99,95%-nál magasabb rendelkezésre állású rendszerek közé sorolnám.
3. Szabályozott formában ki kell alakítani a biztonsági osztályba sorolást az informatikai hálózat elemein is.
4. Szabályozni kell a hálózat követelményrendszereit a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzata nyomán a szabályozás kialakításánál ügyelni kell arra, hogy minden hálózati szolgáltatást biztonsági jellemzőit, szolgáltatási szintjeit és irányítási követelményeit azonosítsák és foglalják bele a szolgáltatási megállapodásokba, legyen akár belső, akár külső (kiszervezett) szolgáltatásról szól.
5. Biztonsági követelmény rendszer kialakításnál alapvető tényezőként kell meghatározni a rendszerbiztonsági intézkedéseket. A kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együtteseként kell kezelni.
6. A szabályozás során elemenként intézkedéseket kell megjeleníteni, melyeknek ki kell térniük az általános intézkedések körére, kiemelt figyelmet kell fordítania az infrastruktúra, hardver, szoftver, adathordozók, dokumentációk, adatok, kommunikáció, osztott rendszerek, személyek védelmére.
7. Megelőzési tervet és visszaállítási trendeket kell megalkotni a katasztrófa-elhárítási terv részeként. A katasztrófa elhárítási tervben meg kell jeleníteni a:
   - Rendszerkiesési időt kell meghatározni informatikai hálózati elemenként,
   - Naplóállományok kezelésének szabályait,
   - Archiválási stratégiát kell alkotni, és szabályozni kell az archiválási tevékenységeket, különös képen az archiválásra jogosult körének meghatározásával, a megőrzési idő, a selejtezési idő, megsemmisítési idő mind a hálózati elemek, mind a kísérő- rögzítő dokumentációk tekintetében.

AJÁNLÁSOK

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

SZÁMOZOTT HIVATKOZÁSOK

[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]

FELDOLGOZOTT IRODALOM

- 2003. évi C. törvény az elektronikus hírközlésről
- 2010. évi CXLVII. törvény egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról
- 222/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás működtetéséről
- 276/2006. (XII. 23.) Korm. rendelet a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről
- 30/2011. (IX. 22.) BM rendelet a Rendőrség szolgálati szabályzatáról
- 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról Köteles Bernadett (összeállította): A kormányzati intézmények informatikai stratégiájának készítése - A Közigazgatási Informatikai Bizottság 22/1. számú (2.0 verzió) ajánlása – 2009.
- Sebestyén Attila: Stációk és determinánsok a rendvédelmi szervek informatikai működésének fejlődésében - doktori (PhD) értekezés (28. oldal) - Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest - 2009.- p.17-28.
- Rajnai Zoltán - Mógor Tamásné: Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása - Bolyai Szemle XXIII. évfolyam, 2014/2. szám-Nemzeti Közszolgálati Egyetem - ISSN 1416-1443 - p.43-59.
- Pándi Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmikatonai-, és közigazgatási kommunikációs rendszerek megszervezésére és irányítására - doktori (PhD) értekezés - Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest - 2005. - p. 21-68.
- Dorkó Zsolt: A Rendőrség informatikai rendszerét befolyásoló tényezők vizsgálata fejlődésében - doktori (PhD) értekezés (203. oldal) Óbudai Egyetem, http://www.lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Dorko_Zsolt_ertekezes.pdf
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében

történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) Az Európai Unió Hivatalos Lapja, 2016.5.4., L 119/1-88pp.

- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- 2009. évi CLV. tv a minősített adat védelméről,
- 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,
- 218/2011. a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól,
- 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól,
- 92/2010. Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól,
- 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről,
- Az adatvédelemmel, és az információ védelemmel kapcsolatos normatívák körében,
- 2010. évi CLVII. tv. a nemzeti adatvagyonról,
- 38/2011. Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról,
- 2011. évi CXCVI. tv. a nemzeti vagyonról,
- 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról,
- 2010. évi CLXXXV. tv. a médiaszolgáltatásokról és a tömegkommunikációról,
- 2003. évi C. tv. az elektronikus hírközlésről,

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,
- 65/2013. (III.8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendeleteként,
- 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”,
- 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,
- 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról”,
- 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben, illetve a módosításáról szóló 2015. évi CXXX. törvényben, meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről.
- 1277/2010. Korm. határozat a kormányzati informatika konszolidációjához szükséges intézkedésekről,
- 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról,
- 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról,
- 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról,
- 8/2009. KHEM utasítás a Közlekedési Hírközlési és Energiaügyi Minisztérium Információbiztonsági Szabályzatáról, mely már a Nemzeti Jogtár hatályos részében nincs, de vonatkoztatható volt.
- 23/2013. (V.17.) ORFK utasítást a belső adatvédelmi és adatbiztonsági szabályzatról,
- 45/2013. (XI.15.) ORFK utasítást az internethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer Rendőrségi igénybevételének szabályairól.
- 2012. évi törvénytervezet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,
- 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA),

- 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK),
- 25/1-3. kötet Az Informatikai Biztonság Irányításának Vizsgálata (IBIV),
- 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR),
- 25/2. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS).
- ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok,
- ISO/IEC 27001:2005,
- ISO/IEC 27001:2013.
- a185/2015. (VII. 13.) Korm. rendelet „a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól”

ÁBRAJEGYZÉK

RÖVIDÍTÉSEK JEGYZÉK

HERMON: Körözési Információs Rendszer

HIDRA: Idegenrendészeti Alkalmazás,

AFIS: Bűnügyi ujj-tenyérnyomat adatbázis

NEKOR: Elektronikus okmány nyilvántartó rendszer

HERR: Határregisztrációs és Határforgalmi Ellenőrző rendszer

SIS: Schengeni Információs Rendszer

GPS: Global Positioning System, Globális Helymeghatározó Rendszer

BME: Budapesti Műszaki és Gazdaságtudományi Egyetem

BM: Belügyminisztérium

MEH: Miniszterelnöki Hivatal

IRM: Igazságügyi és Rendészeti Minisztérium (jogutódja Belügyminisztérium)

ÖM: Önkormányzati Minisztérium

ORFK: Országos Rendőr-főkapitányság

BÁH: Bevándorlásügyi és Állampolgársági Hivatal

NVSZ: Nemzeti Védelmi Szolgálat

IH: Információs Hivatal

NBH: Nemzetbiztonsági Hivatal (jogutódja Alkotmányvédelmi Hivatal)

OKF: Országos Katasztrófavédelmi Főigazgatóság

SZEBEK: (jogutódja TIBEK)

BV: Büntetés-végrehajtási Intézet

EBDH: Egységes Belügyi Digitális Hálózat

BDH: Belügyi Digitális Hálózat

ZRH: Zártcélú Rendészeti Hálózat

EDR: Egységes Digitális Rádiótávközlő Rendszer

NTG: Nemzeti Távközlési Gerinchálózat

MPLS: Multiprotocol Label Swiching

VPN: Virtual Private Network

MIBIK: Magyar Informatikai Biztonsági Keretrendszer

IBIX: Informatikai Biztonsági Iránymutató Kis Szervezetek Számára

MIBÉTS: Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma

KAK: Kormányzati Adat Központba

NISZ: Nemzeti Infokommunikációs Zrt.

KEKKH: Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala

PUBLIKÁCIÓS JEGYZÉK

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. Horvayné Fehér Judit: Az informatikai biztonság szabályozásának kérdése a Magyar Rendőrségnél, Kommunikáció Konferencia, Budapest, 2010. ISBN 978-963-7060-21-2, pp.109-118
4. Prof. Dr. Munk Sándor DSc - Horvayné Fehér Judit: A Rendőrségi informatikai hálózat fogalma, rendeltetése, Hadmérnök, Budapest,2011., VI. évfolyam, II. szám, pp. 217-226
5. Horvayné Fehér Judit: Elektronikus ügyiratok továbbításának megoldásai a Rendőrségnél, Hírvillám, Budapest, 2012. II. évfolyam 1. szám HU ISSN 2061-9499, pp 47-62.
6. Horvayné Fehér Judit: A Rendőrség informatikai biztonsági stratégiája alapjainak meghatározása, Hadmérnök, Budapest, 2011., VI. évfolyam IV. szám pp. 282-292.
7. Horvayné Fehér Judit: A Rendőrségi informatikai hálózatok fenyegetései, Hadmérnök, Budapest, 2012. VII évfolyam II. szám pp.260-275.
8. 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.
9. Fehér Judit: A Rendőrségi informatikai hálózatok információbiztonsági hátterének meghatározása, Hadmérnök, Budapest, 2016. XI. Évfolyam 2. szám - 2016. június pp.1-12.
10. Fehér Judit: A Rendőrség informatikai hálózat védelmének irányai és feladata, Belügyi szemle, Budapest, 2016. 64. évfolyam 6. szám pp. 120-126.
11. 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.
12. 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.
13. Fehér Judit: Információbiztonsági események kezelése egy belügyi szervnél, Rendvédelem c. online folyóirat 2018. / különszám. Kiadja a Belügyi Tudományos Tanács, HU ISSN 2560-2349 . http://www.bm-tt.hu/firend.html pp. 5-19

1. SZÁMÚ MELLÉKLET SÉRÜLÉKENYSÉGI MÁTRIX

Megnevezés /kockázati tényező	meghibásodás	kárérték	előfordulási gyakoriság	kritikusság	hatás	reagálás	időintervallum
Szerver hardveres meghibásodása	A meghibásodás olyan elemet érint, mely nem redundáns.	3	1	4	A rendszer működésképtelenné válik.	A szerver javítását / cseréjét haladéktalanul el kell végezni.	1 nap
	A meghibásodás olyan elemet érint, mely redundáns. A szerver kapacitása csökken.	2	1	3	A rendszer működőképes marad, de a használhatósága csökken, a szerver meghibásodott alkatrésze a továbbiakban nem redundáns.	A szerver javítását / cseréjét haladéktalanul el kell végezni.	3 nap
	A meghibásodás olyan elemet érint, mely redundáns.	1	1	2	A rendszer működőképes marad, a szerver meghibásodott alkatrésze a továbbiakban nem redundáns.	A szerver javítását / cseréjét haladéktalanul el kell végezni.	1 hét
Szerver szoftveres meghibásodása	A meghibásodás következményeként a rendszer használható marad	0	2	2	A rendszer működőképes marad.	A szoftver javítását haladéktalanul el kell végezni	3 nap
	A meghibásodás következményeként a rendszer nem marad használható	2	1	3	A rendszer, vagy egyes moduljai működésképtelenné válnak.	A szoftver javítását haladéktalanul el kell végezni	1 nap
Kliens hardveres meghibásodása	A meghibásodás következményeként a kliens használható marad	0	2	2	A rendszer működőképes marad.	A kliens javítását el kell végezni	3 nap
	A meghibásodás következményeként a kliens nem marad használható	1	1	2	Az adott kliens használhatatlanná válik, de a rendszer többi eleme használható marad. A munka elvégezhető másik kliensről.	A kliens javítását el kell végezni	2 nap

Kliens szoftveres meghibásodása	A meghibásodás következményeként a rendszer használható marad	0	2	2	A rendszer működőképes marad.	A kliens javítását el kell végezni	3 nap
	A meghibásodás következményeként a rendszer nem marad használható	1	1	2	Az adott kliens használhatatlanná válik, de a rendszer többi eleme használható marad. A munka elvégezhető másik kliensről.	A kliens javítását el kell végezni	2 nap
Hálózat meghibásodása	A probléma csak egy kliens gépet érint	1	2	3	Az adott kliens használhatatlanná válik, de a rendszer többi eleme használható marad. A munka elvégezhető másik kliensről.	A hálózati elem javítását el kell végezni.	3 nap
	A probléma minden kliens gépet érinti	3	1	4	A rendszer használhatatlanná válik.	A hálózati elem javítását haladéktalanul el kell végezni.	1 nap
	A probléma a szervert érinti	4	1	5	A rendszer használhatatlanná válik.	A hálózati elem javítását haladéktalanul el kell végezni.	1 nap
	Átviteli út fizikai meghibásodása	4	1	5	A rendszer használhatatlanná válik.	A hálózati elem javítását haladéktalanul el kell végezni.	1 nap
Erősáramú betáplálási problémák	Rövid idejű áramszünet a területen (max. 1-2 perc)	1	2	3	A kliensgépek leállnak, de a munkamenetek nem vesznek el, az áramszünet után a munka folytatható		
	Közepes idejű áramszünet a területen (max 15. perc)	2	1	3	A kliensgépek leállnak, de a munkamenetek nem vesznek el, az áramszünet után a munka folytatható	Amennyiben az áramszünet 5 percnél tovább tart fel kell készülni a rendszer biztonságos leállítására	5 perc
	Hosszú idejű áramszünet a területen (több mint 15 perc)	3	1	4	A teljes rendszer működőképtelenné válik	Amennyiben az áramszünet 15 percnél tovább tart meg kell kezdeni a rendszer biztonságos leállítását.	15 perc

Szerverterem klímatizálási probléma	A klíma teljesítménye lecsökken	0	2	2	A szerverterem hőmérséklete megnövekszik, de még a kritikus szintet nem éri el.	A klíma berendezést meg kell javítani, a szerverterem hőmérsékletét napi 3x ellenőrizni kell.	2 óra
	A klíma működésképtelenné válik.	3	1	4	A szerverterem hőmérséklete megnövekszik, beavatkozás nélkül átlépheti a kritikus pontot, ami a rendszer meghibásodásával jár.	A klíma berendezést haladéktalanul meg kell javíttattni. Ha a szerverterem hőmérséklete átlépi a kritikus szintet (35C), meg kell kezdeni a rendszer biztonságos leállítását.	2 óra
Természeti katasztrófa	a teljes körlet megsemmisül	3	1	4	A rendszer működésképtelenné válik. Az adatok archivumból visszaállíthatóak.	Az archiv anyagok felhasználásával a rendszert újra kell építeni.	1 hónap
	a teljes épület megsemmisül	4	1	5	A rendszer működésképtelenné válik. Az adatok archivumból sem állíthatóak vissza.		

2. SZÁMÚ MELLÉKLET

Az Óbudai Egyetem további szabályzatai – III. Az Óbudai Egyetem tudományos, kutatási és pályázati tevékenységével kapcsolatos szabályzatok III/1.B. – Az Óbudai Egyetem Doktori és habilitációs szabályzata 7. melléklet szerint

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

Alulírott **Fehér Judit** kijelentem, hogy **A Rendőrségi informatikai hálózat védelmének helyzete, a fejlesztés irányai, feladata** című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Budapest, 2018. május 31.

……..
(aláírás)

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.

KÖSZÖNETNYILVÁNÍTÁS

A felkészítésben, a kutatás végrehajtásában, az eredmények publikálásában, valamint az értekezés összeállításában nyújtott önzetlen szakmai és emberi segítségükért,

a velem szemben tanúsított türelmükért köszönetemet fejezem ki

témavezetőmnek és egyben a Biztonságtudományi Doktori Iskola vezetőjének:

Prof. Dr. Rajnai Zoltán egyetemi tanár úrnak,

a kutatás támogatásáért a gyakornoki rendszerben a Belügyminiszter úrnak

DR. Pintér Sándor,

a szakmai támogatásáért az Országos Rendőr-főkapitány úrnak

Papp Károly r. altábornagy rendőrségi főtanácsos úrnak,

szakértői részvételükért az Országos Rendőr-főkapitányság Informatikai Szakértői kollégáknak

Hapka Sándor r. alezredes úr és Olár László r. alezredes uraknak