

FEHÉR JUDIT

A rendőrség informatikaihálózat-védelmének fejlesztési irányai és feladatai

A fejlesztési irányvonalak meghatározásához alapidokumentumként tekintek a 77/2013. (XII. 19.) NFM rendelet (a továbbiakban: rendelet) keretében az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.) meghatározott technológiai biztonsági, továbbá biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről megalkotott eljárás módszertanára. A módszertan alapjaiban véve az Ibtv. törvény védelmi területeire koncentrálna, három spektrumon (bizalmaság, sértetlenség és rendelkezésre állás) vizsgálva a rendőrség elektronikus információs rendszereit, öt biztonsági osztályba sorolása mellett lehetőséget ad a rendőrségi informatikai hálózatok védelmi fejlesztési irányvonalainak meghatározására. Az Ibtv. előírásaiban megjelenő védelmi területeket kívánom használni az irányvonalak meghatározásánál:

- „*zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem*”¹;
- „*teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem*”²;
- „*folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem*”³;
- „*kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével*”⁴.

Az irányvonalakat a következő területekre értelmeztem:

- adminisztratív;
- fizikai;
- logikai.

¹ Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. Magyar Közlöny 2013/69., 50244. o.

² Uo. 50243. o.

³ Uo. 50242. o.

⁴ Uo. 50243. o.

Az irányvonalakat szervezeti szinten és a rendőrségi informatikai hálózatok szintjén fogom értelmezni a törvény és végrehajtási rendeleteinek elemzett formájának erejéig.

Adminisztratív fejlesztési célkitűzések a rendőrségi szervezet részére

Miután az Ibtv.-t vettem alapdokumentumként a fejlesztési irányvonalak meghatározásánál, az elektronikus információs rendszereket – és így közvetve az informatikai hálózatokat – működtető szervezetet biztonsági szintbe kell sorolni, így első adminisztratív irányvonali célkitűzésként határozom meg a rendőrségi informatikai hálózatokkal való összefüggésében.

Az Ibtv. általános irányelvei szerint „*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, így például*

1.1.1. a nemzeti adatvagyonot 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”⁵.

Figyelembe véve a rendelet meghatározásait, és az Ibtv. 9. § (2) bekezdés b) alpontját, a rendőrséget mint szervezetet a minimális törvényi előírásoknak megfelelően 3-as biztonsági szintbe sorolom. Ez a besorolás azt feltételezi, hogy a rendőrségnél mint szervezetnél nincs 3. biztonsági osztálynál magasabb besorolású rendszer, és az „*érintett szervezet megköveteli, hogy az érintett szervezet elektronikus információbiztonsági folyamatai jól szabályozottak legyenek, a folyamatokat dokumentálják és az adminisztratív védelmi intézkedéseket hatékony logikai védelmi intézkedésekkel támogassák*”⁶.

Ez a meghatározás tágabban értelmezve a rendőrség esetében azt jelenti, hogy „*az elektronikus információs rendszerek biztonsági eljárásait meghatá-*

⁵ 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 77/2013. (XII. 19.) NFM rendelet 2. melléklet 1.1. Magyar Közlöny, 2013/214., 85388. o.

⁶ Uo. 2. melléklet 2.1. Magyar Közlöny, 2013/214., 85392. o.

rozták, és azokat összehangolták az informatikai biztonságpolitikával, informatikai biztonsági stratégiával, és az informatikai biztonsági szabállyal”⁷.

Ebből egyértelműen meghatározható a rendőrségnek az a célja, hogy megfogalmazza a stratégiáját és az érintett szervezetre érvényes követelmények szerint dokumentálja is azt. Mindemellett a szervezeten belül ki is kell hirdetnie az informatikai biztonsági stratégiát, amely pontosan meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését. Az informatikai biztonsági stratégiának rövid, közép- és hosszú távú célokat kell megfogalmaznia, ezzel a teljes körű védelem hatását keltheti a szervezet. Álláspontom szerint mindemellett 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 folytonosságot.

Tovább lépve ezen az irányvonalon, „*az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket meghatározták, és azokat az érintettek ismerik és elfogadják*”⁸.

A rendőrség tekintetében értelmezve ezt az előírást, a rendőrség harmadlagos célja gondoskodni arról, hogy az informatikai biztonsági stratégia jogosulatlanok számára ne legyen megismerhető, módosítható. Véleményem szerint gondoskodnia kell még arról is, hogy az informatikai biztonsági stratégia illeszkedjen az érintett szervezet más stratégiáihoz (így különösen a költségvetési és humán erőforrás-tervezéshez, tevékenységikör-változáshoz, fejlesztéshez), jövőképehez.

Mindemellett a rendelet megengedő ebben a témakörben, mert elvárás szinten fogalmazza csak meg, hogy a szervezetnél „*a biztonságtudatosságot megteremtették, és azt az érintett szervezet megköveteli, az informatikai és az általános szakmai területeken folynak biztonsági képzések, de azok ütemezése és a megtartása nem formalizált*”⁹. Tehát a szabályozottságot a védelem nem minden terére terjeszti ki.

A rendelet az adminisztratív védekezések tekintetében a következő területeket különíti el egymástól:

- Szervezeti szintű alapfeladatok.
- Kockázatelemzés.
- Tervezés.
- Rendszer- és szolgáltatásbeszerzés.

⁷ Uo. 2. melléklet 2.3. Magyar Közlöny, 2013/214., 85392. o.

⁸ Uo. 2. melléklet 2.3.2. Magyar Közlöny, 2013/214., 85392. o.

⁹ Uo. 2. melléklet 2.3.6. Magyar Közlöny, 2013/214., 85392. o.

- Biztonsági elemzés.
- Emberi tényezőket figyelembe vevő – személy- – biztonság.
- Tudatosság és képzés.

Álláspontom szerint ezeket az általános érvényű védelmi területeket szervezeti szinten kell megalkotni, a szervezet egészére kell értelmezni, és a rendőrségi informatikai hálózatok tekintetében csak közvetve alkalmazhatók.

Az említett területekhez védelmi feladatok csatolhatók, a feladatok által pedig eljárásrendek és dokumentációk. Ebből a szemszögből elemzést végeztem a rendelkezésre álló rendőrségi dokumentációk és a jogszabályi követelmények között, és a következőket állapítottam meg:

- a rendőrségnél az informatikai hálózatok tekintetében a vizsgált dokumentációk sem keresett eljárásokat sem irányvonalakat nem fogalmaz meg;
- még a gyakorlatban is egyértelműen hiányzik az említett eljárások kidolgozása, az adminisztrációs tevékenységek eredményei;
- az előbbi területek tekintetében nem határozták meg a feladatokat.

A fizikai védelmi terület fejlesztési célkitűzései

A fizikai védelmi terület célkitűzéseinek meghatározásához a rendelet iránymutatásait vettem alapul a 3-as szervezeti biztonsági osztályú besorolás tekintetében. A fizikai védelmi terület elemzéséhez feltételezem, hogy a rendőrségnél mint szervezetnél nincsenek 3. biztonsági osztálynál magasabb besorolású, a rendőrségi informatikai hálózatok által magukban foglalt rendszerek.

E hipotézis alapján a rendelet az általam megállapított szinthez követelményként határozza meg, hogy *„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 ellen”*¹⁰. E követelmény természetesen feltételezi, hogy a szervezet már végzett kockázatelemzést, és minden tekintetben tisztában van a rendőrségi informatikai hálózatokat érintő fenyegetettségekkel.

A követelmények között a rendelet előtérbe helyezi a rendelkezésre állás fontosságát, ami ennél a besorolásnál feltételezi, hogy *„tartalék munkahelyek vannak kialakítva, vagy az érintett szervezet által meghatározottak szerint rendelkezésre állnak”*.

¹⁰ Uo. 2. melléklet 2.3.7. Magyar Közlöny, 2013/214., 85392. o.

A 3-as besorolás tekintetében további követelmény, hogy „*az elektronikus információs rendszerek fejlesztésénél törekednek az integrált elektronikus információs rendszer biztonsági értékelésére vagy tanúsítására*”.

Az előbbi követelményi felsorolásból egyértelműen kitűnik, hogy ezek az előírások a rendőrségi információbiztonsági dokumentumelemzések folyamán nem jelentek meg. Vagyis célkitűzésként fogalmazódik meg a következő területekre koncentrált eljárások pótlása:

- kockázatelemzés;
- fizikai fenyegetettségek vizsgálata;
- tartalék munkahelyek kialakítása;
- tanúsítási rendszer kidolgozása.

A logikai védelmi terület fejlesztési célkitűzései

A logikai védelmi terület célkitűzéseinek meghatározásához a rendelet iránymutatásait vettem alapul a 3-as szervezeti biztonsági osztályú besorolás szempontjából. Feltételezem, hogy a rendőrségnél mint szervezetnél nincsenek 3. biztonsági osztállynál magasabb besorolású rendszerek, amelyet a rendőrségi informatikai hálózatok magukba foglalnak.

A terület vizsgálatánál a rendelet előtérbe helyezi a „*kockázatokkal arányos védelmet*”. E szerint a védelem költségei arányosak a fenyegetések által okozható károk értékeivel. Ismét azt a feltételezést érhetjük tetten, amelynek során a kockázatelemzésre alapozva döntés-előkészítések sorozatát célozza meg a követelményrendszer. A biztonsági osztályba soroláskor a rendelet feltételezi, hogy „*a kockázatelemzés eredményeit figyelembe vették a biztonsági megoldások kidolgozásánál*”¹¹, jelen esetben a rendőrségi informatikai hálózatok tekintetében. Ebből a követelményből is egyértelmű, hogy a célkitűzések megvalósításához elengedhetetlen a kockázatelemzés lefolytatása.

Viszont a követelménysorozatok között nem teljes körű az elvárás. Ezt a tényt az is alátámasztja, hogy „*a biztonságirányítási célokat és mérési módszereket meghatározták, de még nem teljes körűen alkalmazzák*”¹². Ebben a megfogalmazásban feltételezhető a végrehajtó halasztó hatályú jellege, amellyel előremutatásként lehetőség nyílik további védelmi célkitűzések megalkotására a teljes körű alkalmazás területén.

¹¹ Uo. 2. melléklet 2.3.3. Magyar Közlöny, 2013/214., 85392. o.

¹² Uo. 2. melléklet 2.3.4. Magyar Közlöny, 2013/214., 85392. o.

Mindemellett a rendelet egésze tekintetében megjelenik a visszajelzés, az ellenőrzés „intézménye” minden védelmi eljárás területén. Ez a védelmi visszajelző mechanizmus ezen az osztályba sorolási szinten is megjelenik: „*ese-ti biztonsági tesztelést és sérülékenységi teszteket végeznek*”¹³.

A logikai védelmi terület elemzésekor is fény derült arra a tényre, hogy a jogszabályi normák által meghatározott minimális követelmények nem jelennek meg a normatív szabályozásban a rendőrségi informatikai hálózatok tekintetében, ezért a logikai védelmi terület célkitűzéseit a következőképpen rendszerezem:

- kockázatelemzés;
- biztonsági megoldások kidolgozása;
- mérési módszerek meghatározása;
- tesztelések;
- sérülékenységelemzés.

A célkitűzések megvalósításának feladatai – intézkedések

A 3-as biztonsági szervezeti szintű besorolást figyelembe véve a bizalmaság, sértetlenség és rendelkezésre állás spektrumán a megvalósítandó biztonsági intézkedéseket alapul véve meghatároztam azt a tényt, hogy a rendőrségi informatikai hálózatok hármias besorolásúnál magasabb elektronikus információs rendszereket nem foglalnak magukban. Az előzőekben rendszerezett célkitűzések megvalósításához a rendelet szerint intézkedéseket kell meghatározni, megvalósításuk sorrendjét intézkedési tervben kell rögzíteni.

Elemzést végeztem a rendelet mellékletében található útmutató táblázat és a Nemzeti Elektronikus Információbiztonsági Hatóság által rendszeresített biztonsági osztályba sorolást segítő 1700 kérdéssoros kérdőív kapcsán, továbbá a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEKKH) által készített segédletet tekintettem át. Az elemzések alapján rendszereztem a rendőrség számára legfontosabb intézkedések körét. Mind ezt az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, továbbá a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet 3. és 4. mellékleteiben meghatározottak

¹³ Uo. 2. melléklet 2.3.5. Magyar Közlöny, 2013/214., 85392. o.

szerint készítettem el, ennek alapján a következő – fejlesztési – javaslatot teszem rendőrség informatikai hálózatának védelmének megteremtésére. Az intézkedések körét javaslom rögzíteni a következő szabályzatokban:

1. Szervezeti szintű alapfeladatok, amelyben ki kell térni a következő alszabályzókra:
 - a) kockázatelemzés;
 - b) tervezés;
 - c) rendszer- és szolgáltatásbeszerzés;
 - d) biztonsági elemzés;
 - e) emberi tényezőket figyelembe vevő – személy- – biztonság
 - f) tudatosság és képzés.
2. Fizikai védelmi eljárásrend, amelynek magában kell foglalnia a következő részszabályzókat:
 - a) fizikai belépési engedélyek;
 - b) a fizikai hozzáférések felügyelete;
 - c) a látogatók ellenőrzése;
 - d) vészvilágítás;
 - e) tűzvédelem;
 - f) hőmérséklet és páratartalom ellenőrzése;
 - g) be- és kiszállítás.
3. Logikai védelmi eljárás rend, amelynek ki kell térnie a következő szabályzatokra:
 - a) konfigurációkezelés;
 - b) üzletmenet (ügymenet) folytonosság tervezése;
 - c) karbantartás;
 - d) adathordozók védelme;
 - e) azonosítás és hitelesítés;
 - f) hozzáférés ellenőrzése;
 - g) rendszer- és információsértetlenség;
 - h) naplózás és elszámoltathatóság;
 - i) rendszer- és kommunikációvédelem;
 - j) reagálás a biztonsági eseményekre.