HADMÉRNÖK

VIII. Évfolyam 2. szám - 2013. június

Kassai Károly
karoly.kassai@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELEM NAPJAINKBAN AKTUÁLIS SZABÁLYOZÁSI KÉRDÉSEI A MAGYAR HONVÉDSÉGNÉL[1]

Absztrakt

A Magyar Honvédség szervezeteinek működéséhez szükséges vezetési és irányítási követelmények alapján alapvető katonai érdek a híradó és informatikai rendszerek biztonsághoz szükséges szabályozási kérdések azonosítása és menedzselése. Jelen cikk – a szerző korábbi cikkének folytatásaként2 – az egyre bonyolultabb híradó és informatikai rendszerek szolgáltatásainak biztonságához szükséges szabályozási kérdéseit vizsgálja, figyelembe véve az elmúlt évek tapasztalatait. A téma összetettsége miatt a vizsgálat nem teljes körű, csak a központi biztonsági követelményekre és az azokat támogató dokumentumokra koncentrál.

Based on the requirement of command and control of the Hungarian Defence Forces the identification and management of communications and information (CIS) security regulation issues are fundamental military interests. This article – as a continuation of previous article from the author – examines the security regulation issues of more and more sophisticated CIS services, taking into account the experiences in last years. Due to the complexity of the subject of the investigation is not complete, only focused on the core security requirements and supporting documents.

Kulcsszavak: *információbiztonság, elektronikus információbiztonság, kiberbiztonság, szabályozás ~ information security, electronic information security (INFOSEC, Information Assurance), cyber security, regulation.*

1 A cikk a szerző „Az elektronikus információvédelem szabályozási rendje, aktuális feladatok a Magyar Honvédségnél” című, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Felsőfokú Vezetőképző Tanfolyam 2013, évfolyamdolgozat felhasználásával készült.

2 Az elektronikus információvédelem szabályozási kérdései a közelmúltban, Hadmérnök, VIII. évfolyam 1. szám, 2013. március, p. 203-214.

1. ÁLTALÁNOS ÉS SPECIFIKUS BIZTONSÁGI KÖVETELMÉNYEK

Az MH-nál az információbiztonság felső szintű, logikailag egyes számú szabályozója a honvédelmi tárca információ biztonságpolitikája. A szabályozó feladata a nemzeti stratégiák, jogszabályozók és egyéb szervezetszabályozó jogi eszközök, NATO, EU követelmények közvetítése az információvédelmi feladatrendszer felé, és a szakmai követelmények, védelmi rendszabályok kialakításához a szükséges általános irányok meghatározása. A dokumentum meghatározza az információbiztonsági célkitűzéseket és alapelveket, az általános felelősségi rendet, a biztonsági osztályba sorolásra vonatkozó követelményeket, a kockázatkezelésre vonatkozó kötelező eljárásrendet, a szabályozási hierarchiát, valamint a fizikai-, személyi-, dokumentum és elektronikus információvédelemre vonatkozó általános irányokat.[3]

A nemzetközi szabványok, a NATO és EU követelmények, jogszabályok hatására az MH-nál kezd kialakulni a rendszer vagy szervezet-specifikus szabályzási rend, logikailag *biztonsági követelmények* és *védelmi rendszabályok* részre bontva.

Nem minősített adatok területén ez az MSZ/ISO 27000 szabványcsaláddal összhangban lévő szabályozás kezdetét jelenti. Az ilyen irányú szakmai döntés oka, hogy az informatikai szabályozást célzó nemzetközi ajánlások az elektronikus információbiztonsági szabványokra hivatkoznak, illetve a nemzeti ajánlások is e szabványok mentén alakultak ki.[4]

Első lépésként 2012-ben miniszteri utasítás formájában megtörtént a híradó és informatikai rendszerek esetében érvényesítendő *általános biztonsági követelmények meghatározása*. Ezt alapul véve egy-egy hálózat esetében minden hálózatgazdának (vagy szervezeti vezetőnek) el kell döntenie, hogy *szükség van-e az általános követelmények pontosítására, specializálására, melyet saját hatáskörben el kell, hogy végezzen*. Az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (KCEHH) vonatkozásában a döntést a miniszteri utasítás tartalmazza, mely szerint a *hálózatgazda szakutasítás formájában specializált biztonsági követelményt határoz meg a központi kiszolgáló, a hálózati szolgáltatásokat biztosító és a helyi üzemeltető szervezetek felé.* [1.]

A központi vagy a specializált helyi követelmények alapján az adott híradó és informatikai rendszer biztonságért felelős személy kidolgozza a szükséges védelmi rendszabályokat.[5] A szabályzat jóváhagyása a hálózatgazda hatásköre, így a központi rendszerek vonatkozásában a biztonsági dokumentumokat az MH KCEHH hálózatgazdának kell jóváhagynia.

Ez a szabályozási lépés kiváltotta az MH Informatikai Szabályzatban megfogalmazott helyi szabályozóra vonatkozó központi előírást [2.] úgy, hogy a korábbiaktól eltérően a tartalomra vonatkozóan szabvány alapú követelményeket határoz meg. Az utasítás másik jellegzetessége, hogy meghatározza *az üzemeltetésre és a felhasználói síkra vonatkozó biztonsági kérdések elkülönítését*, így megvalósítható, hogy az érintettek csak a munkájukhoz szükséges biztonsági kérdésekkel foglalkozzanak, abból szerezzenek ismereteket.

Aktuális feladatnak kell tekinteni a kidolgozói munka segítését központilag egy védelmi rendszabályokat tartalmazó szabályzó gyűjteménnyel (formailag szakutasítással), ami a helyi és hálózati sajátosságok szerinti megoldások kialakítását segíti. E szabályozó kialakításakor támaszkodni kell az elektronikus információbiztonságot szabályozó új törvény[6] végrehajtását támogató új végrehajtási rendeletekre.

---

[3] Az információ biztonságpolitika ismertetése, magyarázata a szerző korábbi cikkében olvasható: A honvédelmi tárca biztonságpolitikájában meghatározott követelmények, feladatok és azok fontosabb hatásai; Hadmérnök, IV. évfolyam 4. szám - 2009. december, p. 183-190.

[4] A szabványalapúság nyeresége lehet még a nemzetközi környezetben történő könnyebb működés, az együttműködéshez szükséges hálózati összekapcsolások áttekinthető támogatása.

[5] Elektronikus Információbiztonsági Szabályzat formájában.

[6] 2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról.

A biztonsági szempontok csak a híradó és informatikai szakterületi kérdésekkel összhangban vizsgálhatók, így alapvető szempontként kell kezelni a híradó, informatikai üzemeltetéssel – tágabban értelmezve a teljes életciklussal – összehangolt szabályozást. A gyakorlatban ez azt a feladatot jelenti, hogy a híradó, informatikai szabályozási irányokkal és lépésekkel összhangban rugalmasan változtatni kell a biztonságra vonatkozó szabályozást, a NATO követelmények és jogszabályok kereteinek lehető legjobb kihasználásával.

Minősített adatkezelés esetében a szabályozás a NATO és EU követelmények alapján szintén a vázolt logika mentén történik. A biztonsági követelményeknek – mint szabályozó dokumentumnak – szabott, bár nem szabvány alapú követelményei vannak, mely esetben *eldöntendő, hogy a szabályozásban e vonal követése történjen hazánkban, vagy élve a rendelkezésre álló lehetőséggel, nemzeti azonos eredményt biztosító szempontrendszer alakul ki*. Ugyanígy eldöntendő kérdés, hogy *a minősített elektronikus adatkezelésre vonatkozó jogszabályok „eltérítik-e" a nemzeti adatkezelés szabályozását a NATO, EU iránytól, vagy azok alkalmazása történik nemzeti adatok esetében is*.

Az eddigi tapasztalat szerint önálló nemzeti szempontrendszer kialakítása nincs napirenden, így *feladat a szövetségi és EU követelmények alkalmazása*. E területen *szakutasítás fogja meghatározni a biztonsági követelményeket meghatározó dokumentum formai és tartalmi követelményeit*, várhatóan a közeljövőben.

Az elektronikus minősített adatok kezelése tartalmazza a hálózatok összekapcsolását biztosító technikai rendszerek biztonsági kérdéseit is, így a szabályozás kialakításánál *a nemzeti – NATO rendszerek összekapcsolásának kérdését is kezelni kell*.

A biztonsági követelmények végrehajtását szolgáló védelmi rendszabályok (üzemeltetés biztonsági szabályzat) központi meghatározása és szakutasítás formájában történő kiadása 2012-ben megtörtént. A 2013-tól alkalmazandó szakutasítás mellékletei szerint kell kialakítani az új híradó és informatikai rendszerek biztonsági dokumentumait, míg a korábbi biztonsági dokumentumok a következő hatósági akkreditálásig érvényben maradhatnak. A *védelmi rendszabályokkal kapcsolatos szabályozás specializálódott*, és üzemeltető/biztonsági állomány – felhasználói állomány – hordozható eszköz felhasználó állomány kategóriákra bomlott. [3.]

A felső szintű szabályozás fontos kérdése *a rendszer-specifikus vagy helyi szabályozók megfelelőségének és tartalmi ellenőrzésének központi támogatása egy részletes ellenőrzési rend kidolgozásával* az érvényben lévő ideiglenes központi szabályozás szakterületi modernizálása érdekében. [4.] Ezzel a lépéssel *a helyi és az elöljárói ellenőrzési szempontrendszer egyértelművé válik*, jelentős mértékben *csökken az ellenőrzés szubjektív jellege*.

Minősített adatkezelés vonatkozásában az első szabályozási lépés már megtörtént, 2012-ben megjelent az üzemeltetés biztonsági szabályzathoz illesztett ellenőrzési szempontokat meghatározó szakutasítás. A 2013-tól alkalmazandó szakutasítás meghatározza az ellenőrzés gyakoriságát, a jegyzőkönyv készítésére és a hiányosságok felszámolására vonatkozó kötelezettséget. [5.] *A területen további feladat a nem minősített elektronikus adatkezelés szabályozójához illesztve szakutasítás formájában kiadni az ellenőrzési szempontokat.*

A szabályozóban az alkalmazó szervezetek támogatása érdekében szükség van a szárazföldi erők és a légierő NATO készenléti erőkre vonatkozó harcászati ellenőrzési rendjének adoptálására is. A távolabbi feladat az elektronikus biztonságra – mint állapotra – vonatkozó mérhetőség kialakítása rendszer (vagy szervezet) szinten, ami a naplózásnál és naplóelemzésnél, vagy eseti ellenőrzésnél lényegesen szélesebben értelmezett feladat.

A rejtjelzés szabályozása ehhez a rendhez igazítható. A vonatkozó, 2010-ben született jogszabály meghatározza, hogy a rejtjelzést rejtjelszabályzatban kell szabályozni, de a „mit"

kell szabályozni kérdés pontosan nem körülhatárolt.[7] A tartalmi meghatározáshoz a rejtjeltevékenység azonosítása az első lépés. Az általános meghatározás az MH – és a funkcionális eltérések figyelembe vételével más, nagyobb rejtjelzési kötelezettség alá eső közigazgatási szervek – esetében szükségszerűen tovább bontandó, melyre egy részleteket nem tartalmazó példa:[8]

- adatkezelő képességek rejtjelzéssel történő védelmének tervezése, a támogató folyamatok életcikluson át tartó szervezése, irányítása és ellenőrzése;
- rejtjelzés (a rejtjelzési kötelezettség alá eső minősített adatok rejtjeles védelmét biztosító rejtjelző eszközök, alkalmazások vagy eljárások alkalmazása);
- rejtjelző eszközök[9] fejlesztésében, gyártásában, javításában, installálásában való részvétel;
- rejtjelző eszközök telepítése, üzemeltetése, ellenőrzése, bontása;
- a rejtjelzéshez szükséges helyi működés feltételeinek kialakításában való részvétel;
- rejtjelző eszköz rendszeresítési vagy egyéb engedélyezési adminisztratív eljárásainak szervezése és végzése, rendszeresítési eljárásához kapcsolódó szakértői tevékenység végzése;
- rejtjelző eszközök, eljárások tesztelése;
- rejtjelző eszköz hardver és szoftver szinten történő támogatása;
- rejtjelkulcsok gyártása, sokszorosítása;
- rejtjelző eszközök beszerzése;
- rejtjelző eszköz vagy rejtjelanyag kompromittálódása esetén szükséges vizsgálati, jelentési, tájékoztatási és helyreállítási feladatok végzése;
- kapcsolattartás, együttműködés az illetékes hatóságokkal, az együttműködő nemzeti és külföldi adatkezelő rendszerek biztonsági menedzsmentjével, rejtjelző állományával;
- kapcsolattartás és együttműködés nemzeti és külföldi rejtjelanyagot biztosító szervezetekkel;
- rejtjelző eszközök, eljárások üzemeltetésének, kezelésének vagy felhasználói szintű ismereteinek oktatása;
- rejtjeltevékenységgel kapcsolatos feladatok ellátásához szükséges szakmai ismeretek megszerzését biztosító képzés, továbbképzés;
- rejtjelanyagok nyilvántartása, elosztása, tárolása;
- rejtjelanyagok megsemmisítése.

A rejtjelzés egyik kulcskérdésének tekinthető ügyviteli szakterület korszerű szabályozása szakutasítás formájában 2012-ben megtörtént.[10]

A kiadást követő néhány hónap alatt kiforrott, hogy a szabályozást ki kell egészíteni egy központi követelménnyel, ami a szubjektivitást kiszűri a gyakorlatból, és *szabályozza azt a kérdést, hogy egy iratot mikor kell rejtjelzés körébe utalni.* A cél a rejtjelzéshez szükséges, emelt szintű védelem alá tartozó esetek minimalizálása annak érdekében, hogy a rejtjelzést végző állomány napi élete során „ne tereljen be" olyan iratokat a rejtjelirat körébe, ami specializált védelmet nem igényel. Gyakorlati szempontok alapján az ügyintézőnek könnyebb

[7] A vonatkozó jogszabály szerint *rejtjeltevékenység* a rejtjelzés, valamint az azzal összefüggő rejtjelző eszköz fejlesztése, gyártása, javítása, értékesítése, az ezekkel kapcsolatos kiképzés, a rejtjelkulcs gyártása, megsemmisítése, az ezekkel kapcsolatos ügyvitel, továbbá a felsoroltak biztonságához közvetlenül kötődő feladatok ellátása. [6.]

[8] Az ilyen kibontás lehetővé teszi, hogy minden honvédelmi szervezetnél pontosan körvonalazható legyen, hogy milyen tevékenységet végezhet, illetve meghatározható az ezzel kapcsolatos változáskezelési eljárásrend.

[9] A nemzeti szabályozás szerint a rejtjelző „eszköz" kifejezés általános tartalmazza a szoftveres úton történő rejtjelzést is.

[10] 15/2012. (HK 11.) HVK HIICSF szakutasítása az MH rejtjelző szakiratkezelés szabályozásáról.

az elkülönített nyilvántartás használata, mint két nyilvántartás vezetése, ami feleslegesen terheli a rejtjelzés védelmi rendszerét, nem biztosít egységes eljárásrend az MH szervezeteinél, így *ellentétesnek kell, hogy legyen a biztonsági szemlélet fejlődésével.* Ezt a feladatot az említett rejtjelző szakiratkezelésre vonatkozó módosítás 2013-ban a következő rejtjeliratra vonatkozó lényegi csoportosítás meghatározásával végezte el:

- a rejtjeltevékenység általános adatai;
- rejtjelzéssel történő védelemre vonatkozó hadműveleti vagy alkalmazói követelmény;
- rejtjelző eszközre vonatkozó műszaki követelmény;
- rejtjelző szolgáltatásra vonatkozó kockázatelemzés körébe tartozó adatok;
- rejtjelző szolgáltatásra vonatkozó tesztelés adatai;
- rendszeresítés és egyéb hatósági eljárás adatai;
- telepítés;
- üzemeltetés;
- incidenskezelés;
- képzés;
- ellenőrzés;
- rejtjelzésre vonatkozó megoldások kivonása;
- megsemmisítés. [7.]

A rejtjelzés hatékonyságának másik kulcskérdése a szaktevékenység szolgáltatásokhoz és szervezetekhez szabott szabályozási rend kialakítása. Ennek lényege egy olyan központi szabályzat kialakítása, ami meghatározza a szolgáltatásokhoz tartozó általános követelményeket úgy, hogy az a lehető legjobban támogassa az MH szervezeteknél történő szabályozást. A központilag részletesen szabályozandó kérdések közé tartozik a rendszeresítési és hatósági eljárásokhoz szükséges feladatok, a megsemmisítés, a kompromittálódás és incidenskezelés, a fentiekben említett szakiratkezelés, a vészhelyzetek kezelése és az ellenőrzési feladatok.[11] A helyi szabályozás kialakítását az elöljáró szintnek szaktudással támogatnia kell, illetve a tipizálható feladatokat készen, központi kialakítás alapján rendelkezésre kell bocsátani a végrehajtók számára, amit még központilag szervezett képzéssel és továbbképzésekkel (képzési renddel) kell támogatni.

A szerteágazó feladatok miatt nem biztos, hogy minden rejtjelző eszközre, eljárásra érvényes, pontos központi követelmény fogalmazható meg az eltérő szervezetek, feladatok és üzemeltetési környezet miatt, ráadásul az új megoldásokat alkalmazó elektronikus adatkezelő szolgáltatások száma nagymértékben emelkedik. Az ilyen, nem szabályozott esetek megoldásának támogatása érdekében a központi követelmények témakörén belül célszerűnek látszik olyan általános irányelvek megfogalmazása is, melyek *részletes technikai vagy eljárási követelményt nem tartalmaznak, de legalább középtávon megfogalmazzák az ügyek, döntések rendezési irányait*.

2. A SZABÁLYOZÁSI KÖRNYEZET VÁLTOZÁSAI

A kiberbiztonság területén a 2012-es év a közigazgatási szervezetek útkereséseként jellemezhető. Az elektronikus információbiztonságot célzó jogszabály kialakítása 2011 decemberében megkezdődött, majd jelentős szabályozási változások következtek be, ami hatásokat fejt ki a felsőszintű szabályozási környezetre, ami végrehajtandó szakterületi feladatokat jelent az MH esetében is.

[11] A rejtjelzés szakterületén a szabályozás strukturálásának kérdését a szerző korábbi cikke részletezi: A katonai kommunikációs képességek rejtjelzéssel történő védelmének fontosabb kérdései; Hadmérnök, VII. Évfolyam 3. szám - 2012. október, p. 114-122.

Az *Alaptörvény* meghatározza, hogy „Az állam és a helyi önkormányzatok tulajdona nemzeti vagyon. A nemzeti vagyon kezelésének és védelmének célja a közérdek szolgálata, a közös szükségletek kielégítése és a természeti erőforrások megóvása, valamint a jövő nemzedékek szükségleteinek figyelembevétele." Az Alaptörvény meghatározza továbbá a különleges jogrend eseteit, ami az országvédelem vagy a szövetségesi kötelezettségvállalás teljesítése (vagy szövetségben történő katonai művelet) esetén információvédelmi feladatokat is jelent. [8.]

A *Nemzeti Biztonsági Stratégia* megállapítja hazánk függőségét a számítástechnikától, és megfogalmazza, hogy a kockázatok kezelésére, a kiberbiztonság garantálására, a kibervédelemre hazánknak is fel kell készülnie. Ennek feladatai a fenyegetések és kockázatok felmérése, priorizálása, a kormányzati koordináció, a társadalmi tudatosság fokozása, a nemzetközi együttműködési lehetőségek kihasználása. A nemzeti kritikus infrastruktúra védelem mellett feladatunk továbbá szövetségi, nemzetközi erőfeszítésekben való részvétel. [9.]

A Nemzeti Kiberbiztonsági Stratégia egyik célja a globális kibertér részét képező nemzeti kibertérben a nemzeti érdekek védelme. A globális kibertérben a védelmet az azonos értékrendet valló szövetségesekkel, a lehető legszélesebb körű kormányzati és nem kormányzati szereplők közötti együttműködésben kell megvalósítani. A Stratégiában a Magyar Honvédségre is értelmezhető, megvalósítandó célként szerepel a hatékony megelőzési, észlelési, reagálási, válaszadási és helyreállítási képességekkel kialakítása a kiberfenyegetések és véletlen információszivárgás ellen. Cél továbbá a nemzeti adatvagyon szükséges mértékű védelmének kialakítása és fenntartása, a létfontosságú rendszerek üzembiztonságához szükséges, a különleges jogrendben is alkalmazható helyreállítási képességek rendelkezésre állása. A termékek, szolgáltatások színvonalát a nemzetközi bevált gyakorlat szintjére kell emelni, beleértve a biztonsági tanúsítási szabványoknak való megfelelést. Az oktatás és képzés, a kutatás és fejlesztés színvonalának meg kell felelnie a nemzetközi bevált gyakorlatnak. A Stratégiában megtörtént a Magyar Honvédséget is érintő területek azonosítása, mint kormányzati koordináció, együttműködés, szakosított intézmények, szabályozás, nemzetközi együttműködések, tudatosság, valamint az oktatás és kutatás-fejlesztés. [10.]

A *Nemzeti Katonai Stratégiában* új kihívásként és potenciális veszélyforrásként szerepel a globális közjavak területén a kibertér hozzáférhetősége és használata, negatív hatásként értékelt az egyes állami és nem állami szereplők által alkalmazott modern infokommunikációs eszközök általi biztonsági kockázat. Az aszimmetrikus kihívások miatt bővült a háború és a támadás fogalmainak jelentése,[12] illetve a Stratégiában feladatként szerepel a fogalmi kérdések tisztázása és kibervédelmi képesség megteremtése:

- „A kiberfenyegetés jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását."
- (…) „erősíteni kell a Magyar Honvédség kibervédelmét, amihez koncepcionálisan megalapozott rendszabályok kidolgozása, modern eszközök beszerzése, valamint az állomány megfelelő felkészítése és kiképzése szükséges." [11.]

A nemzeti megfogalmazások a nemzetközi állásfoglalásokkal szinkronban vannak, ami két felső szintű biztonsági dokumentum megfogalmazásaival igazolhatók:

- Az Európai Unió Kiberbiztonsági Stratégiája (2013) a nyílt, megbízható és biztonságos kibertér szellemét képviseli. A virtuális teret meg kell védeni a biztonsági eseményektől, a rosszhiszemű tevékenységektől és a visszaélésektől; a

[12] „A károkozás mértékétől függően egy nem fegyveres támadás – megítélését tekintve – akár egy fegyveres támadással is egyenértékű lehet. Ilyen fenyegetést jelent elsősorban a kiber hadviselés, amely anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől."

kormányok fontos szerepet játszanak a szabad és biztonságos kibertér biztosításában. Az információs és kommunikációs technológiák sebezhető pontjait meg kell határozni, elemezni kell őket és a sebezhetőséget mérsékelni kell vagy meg kell szüntetni. Az állami szerveknek, a magánszektornak és az egyéneknek fel kell ismerni a közös felelősséget, és szükség esetén összehangolt lépéseket kell tenni a kiberbiztonság érdekében. [12.]

- A NATO 2010-ben elfogadott Stratégiai Koncepció kiemelt fontosságúnak minősíti a kibertérből eredő támadások elleni védelmi képességek kialakítását. [13.]

A Nemzeti Kiberbiztonsági Stratégiát támogató törvény[13] megjelenése kapcsán a honvédelmi tárcánál *várhatóan a következő szakfeladatok végrehajtására lesz szükség:*

- *Az elektronikus információs rendszerek osztályba sorolása.* A honvédelmi szervezeteknél az elektronikus információs rendszerek osztályba sorolásának felülvizsgálata, szükség szerinti pontosítása.[14]
- *A honvédelmi szervezetek biztonsági szintjének meghatározása.* A honvédelmi szervezetek biztonsági szintjének meghatározása, illetve besorolás felülvizsgálatának elrendelése.
- *Felelősség.* A honvédelmi szervezeteknél elektronikus információs rendszer biztonságáért felelős személyt kell kinevezni, vagy megbízni. Meg kell határozni az elektronikus információbiztonsági szervezeti egység létrehozására vonatkozó követelményeket, a biztonságért felelős személyekre, üzemeltetőkre és felhasználókra vonatkozó szabályokat, a hatósági tájékoztatásra vonatkozó feladatokat.
- *Szabályozás.* Az MH-nál minden honvédelmi szervezetre érvényes elektronikus információs[15] biztonságpolitikát, és biztonsági stratégiát kell kiadni.[16] A honvédelmi szervezeteknél elektronikus információs biztonsági szabályzatot kell kiadni. Meg kell határozni a kockázatelemzésre, ellenőrzésre és auditra vonatkozó követelményeket (a jogszabályoknak és a kockázatoknak való megfelelés). Meg kell határozni azt az általános követelményt, hogy külső közreműködő igénybevétele esetén a jogszabályban meghatározott követelmények szerződéses kötelemként legyenek érvényesíthetők.
- *Eseménykezelés.* Meg kell határozni elektronikus információs rendszer eseményeinek nyomon követhetőségére vonatkozó követelményeket és eljárásrendet. Rögzíteni kell az információbiztonsági események kezelésére vonatkozó követelményeket, eljárásokat, erőforrás elosztást. Ki kell dolgozni a biztonsági incidensek jelentési rendjét és a jogszabályban meghatározott hatóság felé történő tájékoztatási kötelezettséget, beleértve a centralizált incidenskezelésre vonatkozó átfogó követelményeket is.
- *Részvétel a kormányzati koordinációs tevékenységben.* Meg kell határozni a koordinációs tevékenységben való részvétel feladatait.
- *Oktatás – képzés.* Meg kell határozni a képzésért felelős szervezet (Nemzeti Közszolgálati Egyetem) felé történő specifikus képzési igények közlési rendjét, feladatait, az együttműködési kérdésekre vonatkozó alapvető követelményeket. Meg

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

[14] Az osztályba sorolás a honvédelmi szervezeteknél már meghatározott feladat, így az új jogszabály megjelenésekor a meghatározott eljárás megfelelőségét kell felülvizsgálni.

[15] A törvényben olvasható „informatikai" kifejezés egy korábbi jogszabály megfogalmazása miatt került a jogszabályba, ami tartalmilag az MH-nál alkalmazott „elektronikus információbiztonság" területét jelenti. Az egységes kormányzati szintű terminológia megjelenéséig - a tartalmi azonosság jelölése mellett - célszerű lenne az eddig alkalmazott kifejezéseket alkalmazni.

[16] Ezek már rendszerben lévő dokumentumok, így a szabályozási feladat a megfelelőség biztosítása lesz.

kell határozni a biztonsági tudatosság kialakítására és fenntartására vonatkozó, valamint a képzésekre, továbbképzésekre vonatkozó követelményeket.

- *Biztonsági felügyeleti és nyilvántartási feladatok.* A jogszabályban meghatározottak végrehajtása érdekében meg kell határozni a felügyelettel és a nyilvántartással kapcsolatos általános követelményeket.

A szabályozási feladat összetett, melyet több lépcsőben célszerű végrehajtani. A jogszabály a honvédelmi tárca esetében az általános felügyeleti rendtől való eltérést engedélyez, így az MH, a Katonai Biztonsági Szolgálat és HM Védelmi Hivatal feladatainak ellátásához szükséges egyedi rendszerek felügyeleti kérdéseit *honvédelmi miniszteri rendeletben kell meghatározni.*

A következő lépésben *a honvédelmi tárca információ biztonságpolitikára vonatkozó HM utasítást kell felülvizsgálni*, és a törvényben valamint a végrehajtást szabályozó rendeletekben megjelenő követelményekkel összehangolni.

Szűkebb szakterületi feladat a rejtjelzésre vonatkozó központi szabályozás kialakítása a már megkezdett lépések figyelembe vételével és szükség szerinti korrigálásával.[17]

A *specializált szabályozás* egyik esete a NATO központi rejtjelanyag elosztással kapcsolatos feladatrendszer. A feladatok *szövetségi kapcsolattartásra* és a Magyarországon belüli feladatokra bonthatók *saját feladatok* és *felügyeleti feladatok* csoportosításban:

- szövetségi kapcsolattartásként: NATO szervektől rejtjelanyagok átvétele (és kiküldése), más NATO elosztó szervekkel és felügyeleti szervekkel való kapcsolattartás;
- saját feladatok: az átvett NATO rejtjelanyagok nyilvántartása, kezelése és ellenőrzése;
- országos szintű, az MH szervezeti határait átlépő feladatok:
  - nyilvántartók létrehozásához és megszüntetéséhez szükséges követelmények meghatározása;
  - igény elbírálása után a rejtjelanyagok biztosítása;
  - a továbbosztás felügyelete;
  - központi ellenőrzési feladatok végrehajtása;
  - NATO rejtjelző eszközt használó szervezetek ellenőrzése.

A szakmai feladatok mellett szükség van annak továbbgondolására, hogy a fenti feladatokat milyen szabályozással lehet keretbe foglalni, tekintettel arra, hogy:

- a minősített hálózatok, szolgáltatások terjedésével, illetve a szervezeti feladatok bonyolultabbá válásával és az együttműködési szükséglet növekedésével egyre nagyobb mértékben szükség lesz NATO rejtjelanyagok szolgáltatására más tárcáknál, MH-n kívüli szervezeteknél is, másrészt
- pontosan meg kell húzni a határt az alkalmazó szervezet, a nemzeti hatóság és a NATO rejtjelelosztó szervezet között hatáskörök, feladatok között.

A fenti szabályozási lépések a meglévő híradó és informatikai rendszerek biztonságának kérdéseit fedik le, de *szükség van a fejlesztési kérdések rendezésére is*. A *szakterületi stratégia* területén az eddigi gyakorlat az elektronikus információbiztonsági kérdések MH Informatikai Stratégiában történő megjelenítése volt. Ezek a biztonsági kérdések a 2005-ös kormányzati követelmények szerint a következőkben összegezhetők:

- A Stratégiának figyelembe kell venni a kapcsolódó területek stratégiáit, valamint az ágazati stratégiákat.
- A jelenlegi informatikai helyzet bemutatásán belül ismertetni kell az üzemeltetési és biztonsági kérdések szabályozottságát (belső üzemeltetési és biztonsági szabályzat, egyéb szabályozók).

[17] A feladat elrendelése megtörtént (300/2012. HVKF intézkedés az MH rejtjelszabályzat kidolgozásáról).

- A biztonsági helyzetelemzésnél be kell mutatni a biztonsági alapelveket. A Stratégia részeként informatikai biztonsági stratégiai elveket kell megfogalmazni és meg kell határozni a megvalósításhoz szükséges feladatokat, projekteket.
- Biztonsági területen kiemelten kell kezelni az új kihívások megoldásainak kérdéseit.
- A jövőbeni célok elérése érdekében meg kell fogalmazni, hogy az informatikai biztonsággal szemben melyek az új, vagy bővített elvárások. [14.]

A korábban bemutatott, tervezett jogszabályban megfogalmazott követelmények alapján ezt a megoldást ki kell váltani egy szakterületi stratégiával.[18]

A szakterületi stratégia egyik fontos logikai eleme a fent bemutatott korábbi követelményekkel összhangban a fontosabb biztonsági trendek azonosítása a helyes fejlesztési irányok kialakítása érdekében. Az ENISA 2012-es tanulmánya korszerű összefoglalást ad a fenyegetések fő forrásairól (threat agents):

- *Vállalatok (szervezeti fenyegetés).* Vállalatok, szervezetek, vállalkozások, melyek a támadó taktika alkalmazását elfogadják, vagy abban részt vesznek. A motiváció a versenyelőny megszerzése, ami a szervezet mérete, a szektor függvényében jelentős képességeket is jelenthet technológiai vagy mérnöki intelligencia területén, különösen a saját szakterületen.
- *Kiberbűnözők.* Ellenséges természetű, anyagilag motivált, magasan képzett támadók, akik helyi, nemzeti vagy nemzetközi szinten szervezettek lehetnek, közöttük kapcsolatok alakulhatnak ki.
- *Alkalmazottak.* Fenyegetés forrásai lehetnek a szervezetek alkalmazottai, a szerződéses partnerek, beszállítók, az üzemeltető személyek, a biztonsági személyzet, akik belső hozzáférési jogokkal rendelkeznek és ellenséges vagy nem ellenséges szándékúak. Az ilyen személyek magas szintű ismeretei hatékony támadásokat tesznek lehetővé a szervezet (információs) vagyona ellen.
- *Motivált hackerek (Hacktivists).* Politikailag vagy szociálisan motivált személyek, akik számítógépes hálózatokat (szolgáltatásokat) alkalmaznak céljaik elérése, vagy tiltakozásuk kifejezése érdekében. Általában nagy érdeklődéssel figyelt weboldalakat, vállalatokat és szervezeteket, hírszerző ügynökségeket vagy katonai intézményeket céloznak meg.
- *Állami szereplők (Nation States).* Állami szinten jelentős, ellenséges fél ellen felhasználható offenzív jellegű kiber képességek állhatnak rendelkezésre. A rendelkezésre álló eszközök jellege és jelentősége miatt az államok fenyegetést jelenthetnek a kiberterületen vívott hadviselés (cyber warfare) területén.
- *Terroristák.* A terroristák kiterjesztették tevékenységüket a kibertámadásokra is. Motivációjuk lehet politikai vagy vallási jellegű, képzettségük szintje pedig változó. Többnyire a kritikus infrastruktúrákat célozzák, mint egészségügyi szolgáltatások, energiatermelés, távközlés, mely területen a hibák súlyos hatásokat okoznak a társadalomnak, kormányzatnak. Megjegyzendő, hogy a nyilvánosan elérhető források alapján a kiberterroristák profilja jelenleg még nem pontosan körvonalazott. [15.]

Hazánkban a Nemzeti Hálózatbiztonsági Központ 2012 évre vonatkozó értékelése szerint a fontosabbnak ítélt fenyegetések: külső támadás 23%, adatszivárgás 21%, belső szándékos károkozás 19 %, belső véletlen hibából adódó adatvesztés 19%, vírusfertőzés 16%. A magyar vállalatok adatvesztése 2012-ben a következő felosztást mutatja: nem tudnak róla 64%, céges laptopról 7.7 %, alkalmazott által küldve 7.7 %, alkalmazott másolt hordozható eszközre 6%, hordozható eszközön 6%, céges telefonon 3.4 %. [16.]

[18] Az elektronikus információbiztonsági stratégiára vonatkozó központi követelmény még nem ismert.

A fenyegetések forrásai, illetve az említett bekövetkezett károk rámutatnak arra, hogy ezek a tényezők az MH esetében is értelmezhetők, így ezeket az elemzéseket, illetve az egyéb forrásból származó értékeléseket gyűjteni kell, adataikat ki kell értékelni, és a védelmi rendszabályok kialakításánál figyelembe kell venni.

Az ENISA a hálózati technológiák fejlődése kapcsán kutatási területeket ajánl a biztonságos megoldások kialakítása érdekében, mely területek figyelemmel kísérése és a tapasztalatok feldolgozása egyértelműen támogathatja az MH híradó és informatikai rendszerek közép és hosszú távra vonatkozó fejlesztési elképzeléseit:

- *Felhő technológia (Cloud computing).* Megbízható modell kialakítása klienstől a szerverig, az adatok védelmének biztosítása. Az incidenskezelést elősegítő bevált gyakorlatok, politikák alkalmazása. A felhő alapú szolgáltatások vizsgálati és tanúsítási mechanizmusának kialakítása.
- *Valós idejű detektálási és diagnosztizálási rendszerek.* Hatékony detektálási és diagnosztizálási rendszerek, melyek biztosítják a hiba és az anomália detektálás kombinálásának előnyeit, minimalizálva a téves riasztást, ugyanakkor érzékelik az addig ismeretlen támadásokat is. Skálázható megoldásokra és technológiák. A vezeték-nélküli kommunikációs formák fejlődésének követése. A detektáló és diagnosztikai rendszerek teljesítménye és hatékonyság elemzése, a humán számítógép kapcsolat kérdései, a menedzsment és frissítések, sebezhetőség elemzés, az igazi valós idejű megoldások.
- *Vezeték-nélküli hálózatok.* A vezeték-nélküli technológiáknál a vezetékes megoldások hatékonyságához mérhető megoldások kialakítása. A vezeték-nélküli hálózatok rugalmasságára vonatkozó követelmények, a behatolás érzékelés és a helyreállítás kérdései.
- *Szenzor hálózatok.* Azonosítás és hozzáférés felügyelet, behatolás elleni védelem, adat és kulcsmenedzsment védelem, alacsony áramfelvétel, memóriahasználat.
- *Ellátási folyamatok sértetlensége (supply chain integrity).* Hálózati szinten az azonosíthatóság kérdései és új sértetlenség vizsgálati eszközök. Új, komplex megoldásokat biztosító modellek és mechanizmusok kialakítása az ellátási lánc biztonsága érdekében. Telepítés-hálózatépítés, konfigurálás és használat kérdései a magánszektorban, a kutatóintézetek, kormányzati és nemzetközi szervezetek szintjén. [17.]

Egy másik tanulmányban az ENISA kifejezetten biztonsági területen tesz javaslatokat a hálózatokat üzemeltetők számára, azonosítva, hogy az elemzések alapján milyen területeken kell az eljárásokat, mechanizmusokat fejleszteni. A tapasztalható trendek alapján a javaslatok a következők:

- *Adatgyűjtés és bizonyíték szolgáltatás fejlesztése a támadás jellemzőiről.* A hozzáférési és behatolási paraméterek adott támadás esetén is eltérőek lehetnek. Ki kell fejleszteni azokat a módszereket, melyek segítenek jobban megérteni a támadás folyamatát a belépési ponttól a cél eléréséig (ez az információ a jelenlegi fenyegetés jelentésekben nagyon ritkán áll rendelkezésre).
- *Adatgyűjtés és jobb bizonyíték szolgáltatás az ellenfél által okozott hatásokról.* A tanulmányokban elemzett anyagokban nem szerepelnek a sikeres támadások hatásairól szóló bizonyítékok. A hatások elemzésére és értelmezésére a támadók végső céljainak megértése és a védelmi rendszabályok priorozálása érdekében van szükség.
- *A fenyegető forrásokról (agents) az eddigiekhez képest minőségi információk gyűjtése és karbantartása.* Annak ellenére, hogy a szakirodalom szerint a fenyegető agentek léteznek, a valóságban problémát jelent, hogy nem található bizonyíték az incidensek és a fenyegetési források között.

- *Egységes terminológia használata.* Fontos kérdésként kell kezelni a közös szókincs kialakítását a fenyegetés menedzsment területén a szabványügyi testületeknél, nemzetközi szervezeteknél, kormányzatoknál és civil szervezeteknél.
- *A felhasználói szempontok figyelembe vétele.* Ez a szempont még hiányzik a rendelkezésre álló anyagokból. A felhasználói szempontok is tartalmazhatnak adatokat a felhasználókra irányuló fenyegetések hatásairól és segíthetik a fenyegetéssel kapcsolatos tudatosság (threat awareness) kifejlesztésére vonatkozó irányelvek kialakítását.
- *Tipizált esetek kifejlesztése a fenyegetési képhez.* Fontos lenne, hogy az információbiztonsági szakterület dolgozza ki a fenyegetési „látkép" eseteit és alakítson ki bevált gyakorlatokat, illessze be azokat az információbiztonsági menedzsment tevékenységbe, az életciklusba.
- *A biztonsággal kapcsolatos adatok gyűjtése.* A fenyegető tevékenységek növekedése és a támadások bonyolultabbá válása nélkülözhetetlenné teszi a jobb feltételek kialakítását a fenyegetések, kockázatok és kockázatcsökkentési technikák területén történő hírszerzéshez, valamint a közösen kialakított és a szervezetek közötti információ megosztás szolgáló tudástárak kialakítását igényli.
- *A védelmi rendszabályok váltása.* A külső határvédelemről és a széttagolt védelmi rendszabályokról el kell mozdulni a központosított adatok, az átfogó (hollistic) és egységes megközelítésű végponttól végpontig terjedő biztonsági politikákra és védelmi mechanizmusokra. [15.]

Tervezési dokumentumként az MH központi vagy egy-egy szakterületi szolgáltatás kialakítására vonatkozó koncepciók azonosíthatók. A környezeti változások követése érdekében célszerű az MH szinten szükséges kibervédelmi követelmények és feladatok átfogó jellegű koncepcióban történő megjelenítése. A koncepció célja, hogy felsővezetői jóváhagyással határozza meg a fontosabb szakmai követelményeket és irányokat, melyeket a tízéves, a négyéves (rövidtávú), és az éves beszerzési tervekben kell egyre részletesebben erőforrások, kapcsolódási pontok és határidők azonosításával kidolgozni az elektronikus információbiztonsági kérdéseket komplexen tartalmazó Stratégia ütemezése szerint.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az elektronikus információbiztonság területén az utolsó években megtörténtek azok a legfontosabb lépések, melyek az azonos területű feladatokat közös szabályozókba terelve, szabályozási rendként támogatják a végrehajtó szervezetek kidolgozó munkáját. *Ennek alapján megszüntethető a korábbi gyakorlat, mely szerint tartalmilag más területű dokumentumokba is bekerültek elektronikus információbiztonsági követelmények.*

Az új szabályozók elkülönítve kezelik az üzemeltető és biztonsági állomány, valamint a felhasználói környezetre vonatkozó biztonsági kérdéseket, így nem terhelik a felhasználókat rájuk nem vonatkozó, bonyolult rendszabályokkal, az üzemeltetésre vonatkozó követelményekkel.

A cikk azonosítja a soron lévő szakfeladatokat is, jelezve, hogy nem befejezett a központi szabályozók kialakítása, *a folyamatban lévő jogszabályi változások átvezetése napi szakmai irányítási feladatot is jelent.*

A szabályozás alapvető kérdése a pontos követelménytámasztás mellett az eredmények ellenőrizhetősége, így törekedni kell a védelmi rendszabályok egyértelmű megfogalmazására, a helyi vagy rendszerekhez köthető szaktevékenységet végző üzemeltető és biztonsági állomány támogatására, és átlátható, könnyen feldolgozható ellenőrzési rendszer és segédeszközök kidolgozására.

A közelmúltban kiadott szabályozók és a folyamatban lévő ügyek összetettek. A részletesen kidolgozott segédanyagok mellett szükség van a végrehajtók képzéssel és továbbképzéssel történő felkészítésére, így *járulékos feladat az át és továbbképzések rendjének, tematikáinak áttekintése*. Célszerű szabályozási területenként *a központi követelmények magyarázatával, példákkal gazdagított tananyag kialakítása, beleértve a távoktatással kapcsolatos lehetőségek kihasználását is*. Az egyre bonyolultabb szabályozási környezet miatt *meg kell találni a legjobb elektronikus adatkezelési formát az üzemeltető és biztonsági állomány támogatása érdekében, biztosítva rendszabályok gyors kereshetőségét, elérhetőségét*, mely célt a minősített adatokat tartalmazó szabályozók esetére is ki kell terjeszteni.

Az elektronikus információbiztonság területén történő szabályozás a híradó és informatikai szakterülettől nem szakítható el. A bemutatott nemzetközi trendek, ajánlások jól példázzák, hogy a hálózatok világa gyorsuló mértékben fejlődik, a szolgáltatások egyre szélesebb területeket fognak át. A szakterületek közötti *folyamatos egyeztetéssel biztosítani kell, hogy az üzemeltetési vagy menedzsment kérdések továbbgondolásakor a biztonsági szempontok már a legelső pillanattól kezdve integráltan megjelenjenek a tervezési és fejlesztési lépésekben*. Ez biztosíthatja, hogy a védelmi rendszabályok, biztonsági mechanizmusok ne váljanak a katonai vezetés és irányítás gátló tényezőivé, csak a szükséges korlátozásokat tartalmazzák.

A szabályozók modernizálása alapján tapasztalat, hogy *a szabályozó dokumentumok kialakításába már a kezdeti lépésektől fogva be kell vonni a végrehajtó állományt*. A szabályozási feladathoz tartozik a tudatos vezetői magatartás is, ami biztosítja az új szabályozó bevezetéséhez szükséges többlet energiát, valamint a felkészülést a hiányosságok kiszűrésére. A hibák azonnali felismerése közös érdek, így az időben történő korrekció, javítás nem kudarc, hanem korrekt szakmai irányítási eljárás.

Szakkifejezésekre vonatkozó megoldást a cikk nem tartalmaz, de *járulékos szabályozási feladatként kell tekinteni a terminológiai problémák megoldását*, lehetőség szerint a szabályozók kidolgozásával egyidejűleg, mely tevékenység során szintén vállalni kell a kiegészítéssel és felülvizsgálattal járó többlet feladatokat.

A nem minősített és minősített adatkezelésre tagolt jogszabályok végrehajtás szempontjából nem kedvező helyzetet alakítanak ki. A honvédelem által megkövetelt gyors reagálás, a különleges jogi helyzetekben rendezhető speciális helyzetek az elektronikus információbiztonsági szakterület számára felkészülést, a kétfajta szabályozás közötti átmenet lehetőségének kialakítását teszik szükségessé, melynek lépéseit mielőbb ki kell dolgozni.

Felhasznált irodalom

[1.] 3/2012. (I. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról, 3. § (1, 2), 4. § (1), 5. § (1-4) és (6)

[2.] A Magyar Honvédség Informatikai Szabályzata, Ált/210, 1993, 197. és 199. p.

[3.] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 9/2012. (HK 14.) HVK HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről, 4. p.

[4.] Ideiglenes szakutasítás a katonai szervezetek rendeltetésével összefüggő ellenőrzések követelményeire és értékelési rendjére (Ált/13), 2004; 7.3.1.6, 7.3.2.4, 7.3.5.4, 7.4.1, 7.4.4, 7.6.1, 7.6.2, 7.6.5, és 7.6.6. p.

[5.] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 10/2012. (HK 14.) HVK HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről, 5, 7, és 10. p.

[6.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 1. §. 13.
[7.] 3/2013. (HK. 2.) HVK HIICS szakutasítása az MH rejtjelző szakiratkezelés szabályozásáról szóló 15/2012. (HK 11.) HVK HIICSF szakutasítás módosításáról, 2. sz. melléklet
[8.] Magyarország Alaptörvénye (2011. április 25.), 38. cikk (1)
[9.] 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, 31. p.
[10.] 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 1. sz. melléklet, 1, 7, 9 és 10. p.
[11.] 1656/2012. (XII.20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájának elfogadásáról, 33, 34, és 82. p.
[12.] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér, Brüsszel, 2013.2.7. JOIN(2013) 1 final EU 1. 1. és 1. 2. p.
[13.] Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010, 12. p; http://www.nato.int/cps/ en/natolive/ official_texts_68580.htm
[14.] Kormányzati Informatikai Egyeztető Tárcaközi Bizottság 22. számú ajánlása, a kormányzati intézmények informatikai stratégiájának készítése, 2005. p. 9, 20-22. Az ajánlás alkalmazását elrendelte (időközben hatálytalanított): 44/2005. (III. 11.) kormányrendelet a kormányzati informatika koordinációjáról és a kapcsolódó eljárási rendről
[15.] ENISA Threat Landscape (Responding to the Evolving Threat Environment), 2012, p. 29-30.
[16.] PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ 2012. éves jelentés, p. 28 – 29.
[17.] Priorities for Research on Current and Emerging Network Technologies, (PROCENT), ENISA, 2010, p. 84-85.