HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Kassai Károly
karoly.kassai@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELMI RENDSZABÁLYOK KATONAI SPECIFIKÁCIÓJÁNAK KIALAKÍTÁSA, A CIVIL ÖNKÉNTES TÁMOGATÁS MEGVALÓSÍTÁSÁNAK FONTOSABB KÉRDÉSEI

Absztrakt

Az utóbbi öt évben a Parlament és a Kormány törvényeket és rendeleteket adott ki egy naprakész, NATO és EU interoperabilis menedzsment és adminisztratív követelmények, technikai rendszabályok jogi megalapozása érdekében a közigazgatási szervezetek megfelelő szintű információbiztonságáért. A követelmények közös alkalmazása nem mindennapi kihívást jelent az alkalmazó szervezetek számára beleértve a Magyar Honvédséget is. A cikk célja a híradó-informatikai rendszerek biztonsági osztályba sorolási problémájának-, a kár és káros hatás katonai specifikációjának-, valamint a honvédelmi szervezetek szervezeti biztonsági szintbe sorolásának megértése az új Információbiztonsági Törvény (Ibtv. 2013.) követelményeinek megfelelően. Végül a cikk a biztonságosabb katonai kibertér érdekében elkezdi azonosítani egy kezdeti civil önkéntes és katonai együttműködés alapelveit.

During the last five years the parliament and the government launched acts and edicts to establish the legal basis for updated NATO and EU interoperable managements and administrative requirements, technical controls of the appropriate level of information security at public service organisations. The common implementation of the requirements is an extraordinary challenge for the organisations including the Hungarian Defence Forces. The article aids in understanding the problem of security classification of communications and information systems (CIS), the military specification of damages and the organisation security level classification according to the new Information Security Act (2013). Finally, the article starts identifying some basic guides for an initiative civil volunteer and military cooperation for the more secure military cyber space.

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

BEVEZETÉS

A közelmúltban hatályba lépő jogszabályok új szabályozási környezetet jelentenek a közigazgatás, a Magyar Honvédség és a honvédelmi szervezetek számára.

A kilencvenes években megjelenő – majd a jelen évszázad elején újra feldolgozott – ajánlások szolgálhatnak némi támogatással, de az akkori és a mostani jogszabályok által határolt lehetőségek jelentősen eltérnek, így a helyzetet szakmai mérlegelés után, a katonai sajátosságok figyelembevételével, új megközelítéssel lehet, és kell megoldani.

Ez az új szabályozási környezet tekinthető hazánkban az első olyan keretrendszernek, ami – korlátozott hatókörrel – követelményeket határoz meg a minősített és a nem minősített adatkezelés összetett világára.

A honvédelmi szervezetek számára legfontosabb aktuális teendők a híradó-informatikai rendszerek biztonsági osztályba sorolása, a szervezeti biztonsági szint meghatározása, a jogszabályoknak megfelelő elektronikus információbiztonsági szabályozás kialakítása (a meglévő szabályozók pontosítása), így a cikk korábban megfogalmazott gondolatok folytatásaként[1] ezeket a kérdéseket világítja meg, segíti az értelmezést, illetve megoldási javaslatokat mutat be.

A BIZTONSÁGI OSZTÁLYBASOROLÁSHOZ SZÜKSÉGES KÁROK, KÁROS HATÁSOK KÉRDÉSEI

A biztonsági osztályba sorolás feladata nem ismeretlen hazánkban, a korábbi ajánlások már foglalkoztak ezzel a kérdéssel. [1] [2] Lényege, hogy a rendszereket (vagy vizsgálati szemponttól függően: az adatokat) csoportosítani kell annak érdekében, hogy a védelmi rendszabályokat ne egyedileg, később nehezen visszakereshető módon határozza meg az arra feljogosított személy. A szervezetnél előforduló adatok, adatkezelési folyamatok figyelembevételével elkészített besorolási rend lehetővé teszi a védelmi rendszabályok áttekinthető keretbe szervezését és központi menedzselését.

A hatályos jogszabály szerint (Ibtv.) a Magyar Honvédségnél az elektronikus adatokat kezelő híradó-informatikai rendszereket a bizalmasság, sértetlenség és rendelkezésre állás szerinti kármérték figyelembe vételével kell biztonsági osztályba sorolni (korábban ilyen jogszabályban rögzített követelmény hazánkban nem létezett). Az értékelést 1-től 5-ig számozott fokozatba sorolással kell végezni, a számozás emelkedésével párhuzamosan növekvő kármérték szerint. [3]

A jelenlegi jogszabályi követelmény a korábbi szabályozatlan környezettől eltér, így nyilvánvaló, hogy felül kell vizsgálni a Magyar Honvédségnél 2009-ben kialakított, a minősített és nem minősített adatokra vonatkozó közös besorolási rendet. [4]

A minősített adatokra vonatkozó kármérték a Mavtv. 1. számú melléklete szerint meghatározott, így az alkalmazó szervezeteknek e területen mérlegelési lehetőségük nincs. Az elektronikus adatkezelő rendszerekkel – katonai megfogalmazás szerint a híradó-informatikai rendszerekkel – kapcsolatban az adatkezelést megvalósító rendszerekre vonatkozó követelményeket a minősített adatok biztonsága szempontjából kell megfogalmazni. Ez azt jelenti, hogy a híradó-informatikai rendszerrel kapcsolatosan az a fő mérlegelési szempont, hogy a minősített adat illetéktelen megismerése megtörtént-e vagy nem, illetve megvalósult-e az az eset, hogy a rendszer szolgáltatásainak korlátai miatt az arra feljogosított személy nem férhetett hozzá a munkavégzéshez szükséges minősített adatot. A lényeg, hogy a rendszer adott állapotát (a sértetlenség és rendelkezésre állás szintjét) és a minősített adat bizalmasságát, sértetlenségét és rendelkezésre állását nem szabad összekeverni.

[1] Kassai Károly: A 2013. évi L. törvény végrehajtása érdekében a Magyar Honvédségnél szükséges elektronikus információvédelmi szakfeladatok, Hadmérnök, VIII. Évfolyam 4. szám - 2013. december.

A minősített adatokra vonatkozóan a Mavtv. szerinti kármérték nemzeti szinten általános megfogalmazású, az információbiztonsági célokra nincs felbontva (az alkalmazó szervezetek ezt a felbontást nagyobb probléma nélkül elvégezhetik).

Az Ibtv. által meghatározott ötös felosztás lehetőséget teremt a minősített adatok kezelésére feljogosított rendszerek esetében egy olyan lehetőségre, amikor a rendszer kiegészítője, eleme is besorolható, hozzá védelmi rendszabály rendelhető. Az első fokozatba sorolható a minősített adat kezelésére feljogosított híradó-informatikai rendszer azon eleme, ami minősített adatkezelést nem végez, de az adatkezeléshez nélkülözhetetlen szolgáltatást nyújt.[2] A 2-5 fokozatba a minősített adat minősítési szintjeit lehet azonosítani. A jogszabályban megfogalmazott besorolási kötelezettség ezzel végrehajtható, ugyanakkor figyelembe kell venni azt a tényt, hogy a későbbiekben a biztonsági osztályok alapján kell a védelmi rendszabályokat meghatározni. E területen a későbbiekben említettek szerint a funkcionalitásnak szükség esetén felül kell írnia a bizalmasság szerinti besorolást, különben értelmetlen és feleslegesen költséges védelmi rendszabályok alkalmazásának veszélye fenyeget. [5]

A nem minősített adatok biztonsági osztályba sorolása az előbbi eljárástól eltérő. Fontos kérdés a végrehajtási rendeletben rejlő rugalmasság felismerése, ami lehetőséget teremt az alkalmazó szervezetek számára, hogy „testre szabva" kijelöljék azt a szempontrendszert, mely szerint értékelni fogják azokat a károkat, káros hatásokat, melyek akadályozzák, korlátozzák a szervezeti célok megvalósulását. [5; 1. sz. melléklet, 1. 4. p.]

E lehetőséget figyelembe véve a honvédelmi szervezetek biztonsági osztályba soroláshoz a következő károkat, káros hatásokat célszerű figyelembe venni (egy megoldás):

1. Társadalmi-politikai szempontú-, vagy kötelezettség elmulasztásából fakadó káros hatások, károk:
   a) Az Alaptörvényben vagy jogszabályban meghatározott honvédelmi feladatok akadályozása, szövetségi – nemzetközi kötelezettségvállalás teljesítésére irányuló negatív hatás, szolgáltatások vagy a nemzeti adatvagyon körébe tartozó honvédelmi adatok megsemmisülése, sérülése, hozzáférhetetlensége következik be. A honvédelmi létfontosságú információs rendszer szolgáltatásaiban működési zavarok keletkeznek.
   b) A Magyar Honvédségre vonatkozó, jogszabályban meghatározott együttműködési, támogatási feladat, kötelezettség teljesítésének akadályozása vagy korlátozása következik be. A közérdekű adatszolgáltatással kapcsolatos kötelezettségek korlátozott végrehajtása vagy teljesítés elmaradása várható.
   c) A Magyar Honvédség társadalmi méretekben kimutatható bizalomvesztése, vagy szövetségesi-nemzetközi kötelezettségvállalás teljesítésére vonatkozó bizalomvesztés következik be.
2. A Magyar Honvédségnél katonai szervezeteket, csoportosításokat vagy személyeket érintő károk, káros hatások: jogszabályban meghatározott védelmet igénylő adatok bizalmasságának sérüléséből adódóan károk, káros hatások keletkeznek.
3. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi károk: a Magyar Honvédség híradó-informatikai rendszereivel vagy a kezelt elektronikus adataival kapcsolatos megsemmisülésből, meghibásodásból vagy információs károkozásból adódó közvetlen költségek.
4. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos közvetett anyagi károk:
   a) A Magyar Honvédség híradó-informatikai rendszereivel vagy a kezelt elektronikus adataival kapcsolatos helyreállítási költségek.

[2] Pl. biztonsági mechanizmus vagy nem minősített rejtjelző besorolású anyag.

b) A híradó-informatikai rendszerek meghibásodásaiból adódó, vagy a környezetet veszélyeztető események elhárítását célzó műveletek költségei.
c) A Magyar Honvédség híradó-informatikai rendszer működési hiányosságából, vagy adat bizalmasságának sérüléséből adódó perköltségek, vagy egyéb anyagi kötelezettségek.

A négy szempont mérlegelésekor kulcskérdés annak megértése, hogy a Magyar Honvédség szervezeteinek működése során, az adott szolgáltatás kiesésének, megszűnésének veszélyét a rendelkezésre álló adatkezelési alternatív megoldásokkal együtt kell értékelni. Ez egyrészt *rendszer szintű gondolkodást és szervezést igényel*, másrészt az *adatkezeléshez rendelt alternatív lehetőségek és megoldások kialakítását követeli meg*. A lényeget megvilágító tipikus kérdések:

- Ha meghibásodik az „xy" szolgáltatás, hogy kerül az adott felsővezetői intézkedés a katonai szervezethez? Más alakulaton keresztül, futárral, rádión!
- Mi történik, ha meghibásodik az „xy" számú munkaállomás? A felhasználó átül egy mások munkaállomáshoz, vagy egy másik felhasználó átveszi a kiesett funkciót!

Nem az a követelmény, hogy minden egyes elektronikus adatkezelő szolgáltatás minden eleme minden időpontban rendelkezésre álljon minden felhasználónak, hanem az, hogy *a szervezeti működést biztosító alternatív megoldások közül összességében annyi álljon rendelkezésre, ami a minimális szervezeti működést biztosítani tudja* (ami nem biztos, hogy elektronikus adatkezelő szolgáltatás) és a vezetésért és irányításért felelős vezetők ezeket az alternatív lehetőségeket ismerjék.

A fentiek mutatják a kettős feladatot: a honvédelmi szervezetek *minősített adatkezelés esetén alkalmazzák a törvényben meghatározott kármérték szerinti besorolást, nem minősített adatkezelés esetén pedig lehetőséget kapnak önálló besorolási rend kialakítására és alkalmazására*.

A minősített és a nem minősített híradó-informatikai rendszerek besorolásával kapcsolatos további, közös szempontok:

- *Az értékelést az adatkezelés funkciója szerint súlyozottan kell végezni.* A honvédelmi szervezetek elektronikus adatkezelésével kapcsolatos felelősség nem vonható el az adott rendszerért felelős vezetőtől. Megfontolt döntés szükséges arra vonatkozóan, hogy egy rendszer esetében melyik funkciót kell elsődlegesnek tekinteni a honvédelmi szervezetek vezetési és irányítási képességének működőképessége érdekében. A kérdés szokatlan lehet a minősített adatok kezeléséhez szokott gondolkodás esetén, amikor a fő feladat általában az adat bizalmasságának megőrzése. A bizalmasság szempontja mellett a sértetlenség és rendelkezésre állás más megközelítést jelent. Egy radar adat továbbítására szolgáló KORLÁTOZOTT TERJESZTÉSŰ minősített adatok kezelésére feljogosított rendszer rendelkezésre állási követelménye magasabb lehet egy olyan TITKOS minősített adatok kezelésére feljogosított rendszerénél (vagy önálló telepítésű számítógépénél), amelynek adatfeldolgozási funkciója féléves vagy éves periódusú. Nem lehet kijelenteni tehát, hogy „ami magasabb minősítésű az fontosabb" mert vannak olyan esetek, amikor ez az állítás nem állja meg a helyét. Ezért *kritikus fontosságú a honvédelmi szervezetek működésének pontos ismerete, a hadműveleti követelmények pontos azonosítása*.
- *Kiegészítő biztonsági célok követelményeit a biztonsági osztályba soroláskor figyelembe kell venni.* Amennyiben kiegészítő biztonsági célok azonosítása is megtörtént egy híradó-informatikai rendszer esetében, nyilvánvaló, hogy az ezzel kapcsolatos vizsgálati szempontokat rendszer-specifikusan kell kialakítani.

- *A biztonsági osztályba sorolást a híradó-informatikai rendszerért felelős vezető által jóváhagyott kockázatelemzés alapján kell végrehajtani.* Szakmai kihívás a rendszer szolgáltatásaival kapcsolatos lehetséges állapotok, esetek feltérképezése az akár kritikussá is forduló esetek elkerülése érdekében. Az áramellátás önmagában „nem a rendszer része", a szoftver licensz szerződések folytonossága szintén más szakterületen történő döntések és feladatok eredménye, így nyilvánvaló kihívás azon tényezők és hatások azonosítása, melyek hatással lehetnek az információbiztonsági célok teljesülésére.
- *A biztonsági osztályba soroláskor a biztonsági célok sérülését a fenyegetések és a sebezhetőségek bekövetkezési valószínűség szerint módosított hatásai szerint kell figyelembe venni.*

A bekövetkezési valószínűséggel kapcsolatban a jogszabályok követelményeket nem határoznak meg, így a Magyar Honvédség esetében ezt is központilag célszerű szabályozni, melyre egy megoldás a következő lehet:

A bekövetkezési valószínűséget 1-től 5-ig számozott fokozatba sorolással kell értékelni, a számozás emelkedésével párhuzamosan növekvő bekövetkezési valószínűség szerint:

- elhanyagolható bekövetkezési valószínűség (1);
- alacsony bekövetkezési valószínűség (2);
- közepes bekövetkezési valószínűség (3);
- nagy bekövetkezési valószínűség (4);
- kiemelkedően nagy bekövetkezési valószínűség (5).

A híradó-informatikai rendszerek biztonsági osztályba sorolásakor a bekövetkezési valószínűséggel súlyozott fenyegetésekből eredő kár, káros hatás szerint a következő módon lehet biztonsági osztályokat kialakítani (egy változat):

1. biztonsági osztály, jelentéktelen kár:
   a) Magyar Honvédség szinten társadalompolitikai károk, hatások nem azonosíthatók.
   b) A katonai szervezeteket, csoportosításokat vagy személyeket káros hatások érték, de Magyar Honvédség szintjén értékelhető kár nem keletkezett, jogszabályban meghatározott adat védelme nem-, vagy csak olyan mértékben sérült, ami katonai szervezet szintű megoldást igényel.
   c) A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi és közvetett anyagi kár elhanyagolható. A katonai szervezet híradó-informatikai szolgáltatásainak vagy a központi szolgáltatások üzembenntartási keretei között a kár kezelhető.
2. biztonsági osztály, csekély kár:
   a) A keletkezett társadalompolitikai károk katonai szervezet vagy középszintű vezető szerv szintjén kezelhetők.
   b) Jogszabály által védett adat bizalmassága sérült vagy adat, szolgáltatás sértetlenség és rendelkezésre állás követelményei nem teljesültek, melynek során katonai szervezeteket, csoportosításokat vagy személyeket csekély károk, káros hatások érték.
   c) A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi és közvetett anyagi károk az üzembenntartás központi keretei között kezelhetők. A helyreállítás vagy ideiglenes szolgáltatás biztosítása többlet műveleteket igényel.

3. biztonsági osztály, közepes kár:
    a) A keletkezett társadalompolitikai károk hatásaként katonai szervezetek, vagy középszintű vezető szerv működésével, műveleti képességeivel kapcsolatos bizalomvesztés keletkezik.
    b) A Magyar Honvédségre vonatkozó, jogszabályban meghatározott kötelezettség késve, vagy nem teljes mértékben teljesül.
    c) Jogszabály által védett adat bizalmassága sérül vagy adat, szolgáltatás sértetlensége és rendelkezésre állás követelményei több esetben – más közigazgatási szervezetek munkáját nehezítve – nem teljesülnek, melynek során katonai szervezeteket, csoportosításokat vagy személyeket kimutatható károk, káros hatások érnek.
    d) Honvédelmi létfontosságú információs rendszer működésében Magyar Honvédség szinten érzékelhető kiesés, vagy szolgáltatás csökkenés következik be. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi és közvetett anyagi károk az üzembenntartásra biztosított központi keretek között már nem kezelhetők. A helyreállítás, vagy ideiglenes szolgáltatás biztosítása Magyar Honvédség szinten többlet erőforrásokat igényel, ami más híradó-informatikai szolgáltatás rovására, más költségvetési keretek terhére történik.
4. biztonsági osztály, nagy kár:
    a) A keletkezett társadalompolitikai károk hatásaként a Magyar Honvédségre vonatkozóan az Alaptörvényben, jogszabályokban meghatározott feladatok – benne a szövetségesi kötelezettségek – elláthatósága, teljesíthetősége kapcsán bizalomvesztés keletkezik. A Magyar Honvédségre vonatkozó jogszabályokban meghatározott kötelezettségek teljesítése nem kiszámítható, megbízhatatlanná válik, más közigazgatási szervezet működésére is káros hatások alakulnak ki.
    b) Jogszabályban védelemre kötelezett adatok bizalmassága Magyar Honvédség szinten nagymértékben, tömeges adatokat érintve sérül, jelentős bizalomvesztést, nagyszámú peres eljárást okozhat, nehezen kezelhető személyi károk keletkezhetnek.
    c) Honvédelmi létfontosságú információs rendszer működésében Magyar Honvédség szinten megbízhatatlan működés következik be, a meghibásodások egymás hatását erősítik, a helyreállítások hatékonysága bizonytalan. A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi károk a híradó-informatikai szakterület üzemeltetésére és fejlesztésére tervezett központi keretekből nem biztosíthatók, a központi tartalék alkalmazására és tárca szintű belső átcsoportosításra van szükség. A közvetett anyagi károk a környezetvédelemre, jogi képviseletre és egyéb, kárenyhítésre tervezett tárca szintű központi keretekből nem biztosíthatók, belső átcsoportosítást igényelnek.
5. biztonsági osztály, kiemelkedően nagy kár:
    a) A keletkezett társadalompolitikai károk hatásaként a Magyar Honvédségre vonatkozóan az Alaptörvényben, jogszabályokban meghatározott feladatok – benne a szövetségesi kötelezettségek – elláthatósága, teljesíthetősége kapcsán súlyos, nemzeti és nemzetközi szinten érzékelhető bizalomvesztés keletkezik. Jogszabályban meghatározott feladatok végrehajtása elmaradhat, a Magyar Honvédség alaprendeltetéséhez köthető együttműködési kötelezettségek nem teljesülnek.

b) Magyar Honvédség szinten honvédelmi körbe tartozó nemzeti adatvagyon pótolhatatlanul megsemmisülhet, honvédelmi létfontosságú információs rendszer működése nem biztosított. Jogszabályban védelemre kötelezett adatok bizalmassága Magyar Honvédség központi adatbázisok szintjén sérülhet, melynek mértéke kiemelt, a kár hatásainak kezelése hosszú időszakot vesz igénybe.
c) A szolgáltatások és adatok sértetlenségével, rendelkezésre állásával kapcsolatos anyagi károk a híradó-informatikai szakterület, tárca szintű tartalék mellett kormányzati szintű keretek terhére biztosíthatók. A közvetett anyagi károk a környezetvédelemre, jogi képviseletre és egyéb kárenyhítésre tervezett tárca szintű központi keretekből és belső átcsoportosításból nem biztosíthatók, kormányzati keretekből történő megerősítés szükséges.

Az értelmezéshez célszerű irányelveket meghatározni a honvédelmi szervezetek közös értékelési rendjének kialakulása, az egységes gondolkodás érdekében, de meg kell jegyezni, hogy a bekövetkezési valószínűség, az információs kár meghatározása, a biztonsági célok közötti súlypont helyes azonosítása segédeszközök, programok alkalmazása esetén sem nélkülözheti a szubjektivitást.

Az egyéni nézőpontokból adódó hibák kiküszöbölésének eszköze a gyakorlás és képzés, a kontrollcsoportok alkalmazása, illetve a Magyar Honvédség sajátosságait tükröző minél pontosabb központi követelmények meghatározása.

A VÉDELMI RENDSZABÁLYOK KIALAKTÁSÁNAK TÁMOGATÁSA, A SZERVEZETI BIZTONSÁGI SZINT BESOROLÁS

A honvédelmi szervezetek híradó-informatikai rendszereinek biztonsági osztályba sorolása kockázatelemzés nélkül tartalmilag elképzelhetetlen, melynek általános feladatait egy korábbi cikk már megfogalmazta.[3] A kockázatelemzésre vonatkozó nemzeti követelmények annyit változtak, hogy az alkalmazó szervezetek számára jogszabály meghatározza a kockázatelemzési stratégia és eljárásrend kialakítását. [5; 3. sz. melléklet, 3. 1. 1. 10. p. és 3. 1. 2. részfejezet]

A részletek említése nélkül megfogalmazható, hogy a híradó-informatikai rendszerek kockázatelemzése több szempontból értelmezhető feladat. A honvédelmi szervezeteknél szükség van *az általános tervezési feladatok támogatására, részleteket is feltáró strukturált elemzésre, illetve egy-egy célterületre vagy adatkezelési funkcióra irányuló kockázatelemzési folyamatokra*.

A biztonsági osztályba sorolás elvégzése érdekében elégséges egy általános, rendszer szintű kockázatelemzés, ami a legjelentősebb fenyegetésekkel, sebezhetőségekkel számolva az egész rendszerre, adatkezelési folyamatra vonatkozóan feltárja az előnyöket és hátrányokat. Ebben az esetben elérendő cél, hogy a fentiekben példaként bemutatott biztonsági osztályba soroláshoz szükséges döntés megalapozott legyen. Ehhez jól láthatóan nem részletes paraméterek azonosítására van szükség, hanem az adott értékelt területnél az esetleges kárra, káros hatásra koncentrálva az előnyök és hátrányok számbavételére és az esetleges kiegészítő védelmi rendszabályok igényének vagy lehetőségének azonosítására.

A biztonsági osztályba sorolás szakterületi támogatása, a feladat egységes szemléletű végrehajtása érdekében *szükség van a hivatkozott követelmények szerinti specializált kockázatelemzési módszertan kialakítására*, az ehhez szükséges feladat elrendelésre és képzésre vonatkozó részfeladatokkal együtt.

[3] Kassai Károly: Az elektronikus adatkezelő rendszerek egyes biztonsági kérdései; Hadmérnök, V. Évfolyam 1. szám - 2010. március, p. 260-262.

A támogatási feladatok között említeni kell a képzést is, melynek biztosítania kell az Ibtv. végrehajtásához szükséges ismeretek elsajátítását. [6]

A képzési feladatokat meghatározó jogszabály követelményei szerint a Nemzeti Közszolgálati Egyetem 2014-ben elindítja, de a végrehajtás során gátló tényező lehet a két szemeszteres képzés személyenként félévre eső százezres nagyságrendű képzési költség, illetve a költségvetési tervezésre vonatkozó átfutási idő. Könnyítés, hogy gyakorlati tapasztalattal kiváltható a képzésre vonatkozó beiskolázási követelmény, illetve a Nemzeti Elektronikus Információbiztonsági Hatóság véleménye szerint a közigazgatásban elfogadható megoldás a szervezetek, önkormányzatok összefogása és az elektronikus információbiztonság közös menedzselése (az önkormányzati társaságok mintája e szakterületen is követhető), és a képzésre közösen delegált személyek biztosítása.

Az összetett szervezeti struktúrák számára elégséges a központi feladatokért felelős szervezeti elemek állományát beiskolázni, ami a Magyar Honvédség esetében a szakmai feladatok irányításáért felelős HM szerv, a középszintű vezető szerv, az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (KCEHH) központi üzemeltetési feladatait ellátó honvédelmi szervezet érintettségét jelzi (a képzési követelményekre vonatkozó döntést célszerű az első évfolyam utáni tapasztalatok feldolgozására alapozni).

A szervezet biztonsági szintjének meghatározásakor az alkalmazott híradó-informatikai rendszerek kockázatelemzésen alapuló biztonsági osztályát, az elektronikus adatkezelés kockázatainak a szervezeti feladatokra történő hatásait kell figyelembe venni.

A szervezet biztonsági szint meghatározása a szervezet vezetőjének hatáskörétől nem vonható el, de a Magyar Honvédség szinten egységes szintek kialakítása érdekében szükség van egy központi szakmai támogató tevékenységre, ami az Ibtv. végrehajtására kiadott jogszabályban meghatározott felügyeleti rend biztosít. [7] Az elöljáró szakmai szint szakértői tevékenysége biztosítja a szervezetnél kialakított döntési javaslat kontrollját, és főleg azokban az esetekben nyújt hasznos segítséget, amikor az általánostól való eltérőséget, a besorolás során alkalmazandó lehetséges eltéréseket, vagy következő szervezeti biztonsági szint eléréshez szükséges szakfeladatokat kell jóváhagyatni.

Irányelvként kell tekinteni, hogy a honvédelmi szervezet híradó-informatikai rendszer adatkezelését biztosító legmagasabb biztonsági osztályt akkor kell a szervezet biztonsági szint besorolás alapjául tekinteni, ha a szervezeti feladatokra történő hatás a legmagasabb biztonsági osztályba sorolt rendszer kockázata szerint a legnagyobb.

A legmagasabb biztonsági osztálytól eltérő szervezet biztonsági szint besorolásról szóló döntésnek tartalmaznia kell a honvédelmi szervezet híradó-informatikai rendszereivel kapcsolatos feladatokra történő kockázatok értékelését, az eltérés indoklását, melynek a felügyeleti rend szerinti elöljáró szervezet jóváhagyása egyben a besorolás objektivitását is biztosítja.

A szervezet biztonsági szintbe történő besorolásakor értékelni kell, hogy a híradó-informatikai rendszer:

- a honvédelmi szervezet üzemeltetésében van, vagy a biztonságért felelős vezetőnek csak a felhasználói szintű biztonsági feladatokra van hatása;
- a honvédelmi szervezet működését milyen mértékben, vagy időszakban biztosítja.

Híradó-informatikai rendszer szolgáltatásait más szervezet számára biztosító honvédelmi szervezet esetében a szervezeti biztonsági szint besoroláskor a kiszolgálói feladatokat és a felhasználói szintű feladatokat elkülönítve kell értékelni.

A híradó-informatikai rendszerek biztonsági osztályának változásakor, vagy a szervezeti elemek olyan átalakításakor, ami hatással van az adatkezelésre, a szervezeti biztonsági szint besorolást soron kívül el kell végezni.

A fentiek szerinti besorolási feladatok célja a védelmi rendszabályok meghatározásának támogatása, a biztonsági osztályonként egységes eljárásrend kialakítása.

Az Ibtv. végrehajtásával kapcsolatos rendelkezések tartalmaznak információvédelmi rendszabályokat, illetve a minősített adatok védelmére vonatkozó jogszabályok is határoznak meg követelményeket, így az alkalmazó szervezetek nyilvánvaló feladata az elkülönült jogszabályok közös, erőforrás takarékos végrehajtása.

A Magyar Honvédség esetében e mellett kiegészítő feladat, hogy a központilag meghatározott, a honvédelmi szervezeteknél készítendő Elektronikus Információbiztonsági Szabályzatra (EIBSZ) vonatkozó követelményt[4] ki kell egészíteni az új jogszabályban meghatározott védelmi rendszabályokkal.

CIVIL ÖNKÉNTES ÉS KATONA EGYÜTTMŰKÖDÉSE A BIZTONSÁGOS KATONAI KIBERTÉRÉRT

Napjainkban a Honvédség híradó-informatikai rendszerei, a vezetési és irányítási képességek nem különülnek el olyan jelentősen a polgári távközlési, informatikai megoldásoktól, mint hosszú évtizedekkel korábban.

A híradó-informatikai rendszerek kapcsolódási pontjai, a hasonló technikai megoldások – és az ezekkel kapcsolatban megjelenő fenyegetések és sebezhetőségek – nyilvánvalóvá teszik a polgári megoldásokból származó tudás alkalmazásának szükségességét.

A 2013-ban megindított Honvédelmi Kötelék Program kidolgozása a volt Magyar Honvédelmi Szövetséghez (MHSZ) hasonlítható kezdeményezés, amely az iskoláskorú fiatalság felé célozza a katonai értékek közvetítését, míg az Önkéntes Tartalékos Rendszer (ÖTR) a felnőtt korú állampolgárok számára ajánl olyan szerződéses viszonyt, ami lehetővé teszi a Honvédség képességeinek kiegészítését, a szervezettszerű társadalmi támogatást akár elektronikus információvédelem, – kibervédelem területén is. A két megoldás közötti célterület egy olyan lehetőség, ahol az arra elhivatott (vagy kíváncsi, tenni akaró) állampolgár önkéntes alapon, nem tartalékos állományban szabad akaratából, ellentételezés nélkül szakfeladatok megoldását ajánlja fel a Magyar Honvédség számára ezen az érzékeny szakterületen.

Azon személyek, akik szükséget éreznek arra, hogy tudásukat, tapasztalataikat vagy egyéb szellemi javaikat a nemzeti szempontból érzékeny terület – a Honvédelem – megerősítésére fordítsák, véleményükkel, szándékukkal nem hagyhatók figyelmen kívül.

A civil önkéntes oldal és katonai együttműködés megfogalmazásának első lépése a közös célok, együttműködési területek azonosítása.

Nyilvánvaló cél a magyar katonai kibertér biztonságának erősítése, az elektronikus információbiztonság szintjének a fenyegetésekkel és sebezhetőségekkel arányos kialakítása, erősítése a „civil erő” támogatásával.

Elektronikus információbiztonság területén az ilyen együttműködés előzmények nélküli, így a megoldás érdekében tett *minden lépés úttörő megoldásnak minősíthető*.

Az elektronikus információbiztonság – kiberbiztonság szakterülete az egész világon bizalmas területű kérdés, így *a valós információ megosztás és együttműködés alapos előkészítés, pontos együttműködési feltételek és alapelvek lefektetése után képzelhető el*.

Az alkalmazott megoldások, a fejlődés és a világban bekövetkező szakterületi események egyértelműsítik azt a feltételezést is, hogy egy folyamatosan átalakuló és alkalmazkodó együttműködési rendet érdemes elképzelni, melynek kötelező elemei *a naprakészség, a folyamatos konzultáció, a változások érzékelése és a rugalmasság*.

A részletek említése nélkül nyilvánvaló az a szakterületi sajátosság, hogy a közigazgatásban és a Magyar Honvédségnél az adatok védelméért felelős szervezeti elemek léteznek. Ennek *a*

[4] 3/2012. (I. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról.

felelősségnek az elvonása, csökkentése vagy megosztása csak az állami felelősségérzet csökkenését, hamis biztonsági kép kialakulását eredményezné, így le kell szögezni azt is, hogy *az önkéntes alapú hozzájárulás csak a kibervédelmi képességek erősítését, fejlesztését szolgálhatja, a honvédelmi szervezetek alaprendeltetésből adódó felelősségét nem vállalhatja át*.

A nemzetközi média, a szakirodalom egyre több hírt szentel a különböző nemzeti kormányzati, katonai és egyéb nem kormányzati megoldásoknak, a feltételezett, vagy sajtóban bejelentett kiberműveleti támadó képességek ismertetésének. E területen nyilvánvaló, hogy az önkéntes civil – katonai együttműködésnél alapvetőnek kell tekinteni *a nemzetközi szerződések, jogszabályok és egyéb normák tiszteletben tartását, és átlátható, elszámoltatható, egyértelműen kibervédelmi körbe tartozó* tevékenységet lehet csak célkitűzésként megfogalmazni.

A kibertérben zajló műveletek váratlansága, intenzitása, hatásmechanizmusa döbbenetes ütemben fejlődik, ami a váratlanul szükséges kibervédelmi műveletek során az önkéntes résztvevők – vagy az önkéntes tartalékosok – alkalmazásának lehetőségét nagymértékben korlátozza (gyakori az a magyarázat, hogy a támadó előre nem jelenti be, mire készül, így nehézkes erre az esetre bevonulást szervezni). Az együttműködési területek kijelölésénél ezt a sajátosságot figyelembe kell venni, és *az együttműködés során a képességfejlesztést, a tudás erősítését, a biztonságtudatosság növelését kell előtérbe helyezni*.

Szakértői tevékenység

Cél a civil önkéntesek tudásának, tapasztalatainak hasznosítása a Magyar Honvédség kiberbiztonsági fejlesztési és szabályozási tevékenységében.

- Kibervédelmi stratégiai dokumentumok, koncepciók és tervek szabályozók, előkészítésében való konzultáció, véleményezés és javaslattétel.
- Hatástanulmányok, modellezés és szakmai segítségnyújtás a szabályozás, képzés és egyéb specifikus területek támogatása érdekében.

Forráskutatás, elméleti támogatás

Cél az nemzetközi és nemzeti szakirodalom figyelemmel kísérése, feldolgozása során felhalmozódott ismeretek alapján javaslatok megfogalmazása, trendek és iránymutató jelenségek azonosítása a katonai kibervédelmi képességek fejlesztése érdekében.

- A kibervédelemmel kapcsolatos szakirodalom valamint nemzetközi és nemzeti források felkutatása, elemzése, javaslatok megfogalmazása. A nemzeti és nemzetközi stratégiai szintű dokumentumok változásainak követése, az aktuális trendek felismerése és következtetések megfogalmazása.
- A nemzetközi szakirodalomban a katonai kiberbiztonsággal kapcsolatos nyílt forrású dokumentumok felkutatása, értelmezése és javaslatok megfogalmazása.

Elemzés – értékelés

Cél a nemzeti kibertérrel kapcsolatos helyzet elemzésén és értékelésén alapuló tudatos tevékenység, a nemzeti katonai kibertér biztonságának támogatása elméleti támogatása.

- Az EU szabályozók változásainak figyelemmel kísérése, az EU szakirányú szervezeteinek állásfoglalásai és az aktuális szakirányú programok megismerése, értelmezése.
- A nemzeti szabályozórendszer folyamatos figyelése, a változásokkal kapcsolatos szakmai teendők megfogalmazása, a szakmailag illetékes hatóságok által megfogalmazott helyzetértékelések, állásfoglalások elemzése és értékelése.
- A magyar kibervédelem aktuális helyzetének elemzése, trendek azonosítása, javaslatok megfogalmazása katonai kibertér biztonságának növelése érdekében.

Oktatás, képzés és biztonságtudatossági programok

Cél a civil önkéntes tapasztalatok és tudás integrálása a Magyar Honvédség elektronikus információvédelmi – kibervédelmi át és továbbképzési rendszerbe, illetve specializált, egyedi programok, gyakorlatok kialakítása, rendezvények szervezése lehetőleg pontosan megfogalmazott témák feldolgozása érdekében.

- Kibervédelmi rendezvények szervezése, a katonai oktatási és képzési rendszer keretén belül oktatókkal, segédanyagokkal, ismeretekkel a humán erőforrás támogatása.
- Közös elméleti, gyakorlati foglakozásokkal kijelölt szakterületi kérdések vizsgálata értékelés és javaslattétel.

A szervezeti együttműködés megvalósítása

A kialakított civil önkéntes – katonai együttműködés során cél a lehetőségek, zajló folyamatok figyelemmel kísérése és a szükséges korrekciók megtétele, a felhalmozódott tudás rendszerezése, hasznosítási lehetőségeinek kutatása, az együttműködés szélesítése, a belső szabályozók kialakítása és fejlesztése.

- Az önkéntesség elvének megfelelő koncepcionális fejlesztés és tudatos építkezés, programok és együttműködési fórumok lehetőségének felkutatása és megvalósítása.
- A jogszabályokban megfogalmazott lehetőségek kiaknázása, illetve az önkéntes civil – katonai együttműködéshez szükséges jogszabályi változtatási javaslatok megfogalmazása.
- Szakmailag érdekes katonai rendezvényeken a civil önkéntes fél részvételének biztosítása (vagy arról információ biztosítása), a Magyar Honvédség szakterületi kérdéseinek bemutatása.

ÖSSZEGZÉS

A feladatokat nem részletesen tartalmazó cikk jól érzékelteti, hogy a korábban kevésbé szabályozott elektronikus információbiztonsági szakterületen megjelenő jogszabályok olyan új követelményeket határoznak meg, amelyek a közigazgatásban, *a Magyar Honvédségnél megkövetelik a helyzet pontos értékelését és a feladatok lehető legpontosabb specializálását*, „testre szabását”.

A kockázatelemzés – biztonsági osztályba sorolás – szervezet biztonsági szintbe sorolás – illetve a védelmi rendszabályokat meghatározó szabályozók kialakítása logikailag sorba illeszthető feladatok, de az ezzel kapcsolatos részletek több helyen *pontosítást követelnek, a végrehajtás területén pedig minden egyes szabályozási lépésnél szükség van a minősített és nem minősített adatok egységes elvek alapján történő összehangolására*.

A jogszabályok ismeretében hiányként tárható fel *a kockázatelemzésre vonatkozó egységes módszertan és kötelező érvényű eljárásrend hiánya*, ugyanakkor jelzésértékű, hogy kormányzati követelmény már tartalmazza a szervezetek ez irányú feladatait.

A híradó-informatikai rendszerek elektronikus információbiztonsági szabályozása a jelenlegi helyzetben sem tekinthető egyszerű esetnek. Jogszabályok jelenleg pontosan végrehajtható és ellenőrizhető formai és tartalmi követelményeket nem határoznak meg a minősített vagy a nem minősített elektronikus adatkezelés biztonságának szabályozására, így *az alkalmazó szervezeteknek ki kell alakítani azt a specializált szabályozási rendszert, ami egyaránt megfelel a jogszabályoknak és a szervezeti érdekeknek*.

Az utolsó témaként szereplő civil önkéntes – katonai együttműködés egyértelműen az új kihívásokhoz szükséges megoldások keresését célozza. A civil tudás legjobb hasznosítása nem nélkülözhető erőforrás, ugyanakkor a bizalmi kérdésként kezelendő szakterületen az együttműködés kialakítása számos kihívást, megoldandó feladatot rejteget.

Befejezésként köszönet a fontosabb kérdések megvilágításában segítő Magyar Honvédség elektronikus információbiztonsági szakterületű képviselőinek, illetve független szakértőknek, akik a cikk előkészítésekor véleményüket kifejezték, válaszokat adtak, illetve további kérdéseket tettek fel, vagy megoldásokra váró feladatokra hívták fel a figyelmet.

Felhasznált irodalom

[1] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, 1996.

[2] Közigazgatási Informatikai Bizottság 25. számú Ajánlása, Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 25/1-2. kötet Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió; 2008. június)

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 7. §.

[4] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról; 15. §.

[5] 77/2013. (XII. 19.) NFM rendelet Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről; 1. sz. melléklet, 1.1. p.

[6] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról, 4. §.

[7] 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről