HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Kassai Károly
kassai.karoly@hm.gov.hu

AZ ELEKTRONIKUS ADATKEZELŐ KÉPESSÉGEK MŰKÖDÉSFOLYTONOSSÁGÁVAL KAPCSOLATOS ÁLTALÁNOS FELADATOK

Absztrakt

A honvédelmi szervezetek működése napjainkban nem képzelhető el elektronikus adatkezelő képességek nélkül. Az ezt megvalósító eszközök, rendszerek, szolgáltatások egyre fontosabb szerepet játszanak, így kiemelt figyelmet érdemel rendelkezésre állásuk kérdése. Nem elégséges csak egy eszköz, rendszer beszerzésére koncentrálni, mert a hardver és szoftvertámogatás vagy a karbantartás hiánya a teljes életciklusra vetítve hiányosságokat és problémákat okozhat az üzemeltetés során. A meghatározott szinten történő üzemeltetés támogatás kihívásokat jelent a katonai üzemeltetési környezet, valamint az ezzel kapcsolatos információs fenyegetések és sebezhetőségek miatt.
A cikk az elektronikus adatkezelő szolgáltatások folytonos működésre vonatkozó feladatrendszerét vizsgálja. Támpontokat ajánl a híradó és informatikai rendszerek tervező, üzemeltető szerveinek, biztonsági menedzsmenteknek az elektronikus adatkezelés előre meghatározott szolgáltatási szinten történő biztosítása érdekében.

Nowadays the activity of military organisations unimaginable without electronic information handling capabilities. The communication equipments, systems have more and more importance so the availability aspect of these supporting capabilities requires focus point of view. The focus is not only on acquisition of equipments or systems because lack of hardware and software upgrading and maintenance during all life cycle can cause deficiencies and problems in service.
The agreed level service support has some challenges because of specific military environment, information threats and vulnerabilities. This article observes the business continuity framework of CIS and offers milestones to the planning, operating authorities and security managements for the agreed level electronic information handling capabilities.

Kulcsszavak: *biztonságpolitika, információbiztonság, információvédelem, rendelkezésre állás, működésfolytonosság ~ security policy, information security, information protection, availability, business continuity*

BEVEZETÉS

Az elektronikus adatkezelő képességek biztonságára vonatkozóan hazánkban átfogó jellegű, a közigazgatásra érvényes – így a Magyar Honvédségnél is kötelező jellegű – követelmény nem azonosítható. Az elektronikus információbiztonság hármas célkitűzésén belül (bizalmasság, sértetlenség, rendelkezésre állás) az adatokra és adatkezelő képességekre egyaránt értelmezhető sértetlenség és rendelkezésre állás követelményei jogszabályokban még pontosan nem azonosítottak.

A minősített adatkezelésre vonatkozó jogszabályok közvetlenül nem határoznak meg a szolgáltatások fenntartására irányuló biztonsági követelményeket, csak azt rögzítik, hogy *a hagyományos (papír alapú), vagy elektronikus adatkezelést helyi, illetve rendszer-specifikusan kell szabályozni*, melynek részleteit az adatkezelésért felelős vezetőnek kell meghatároznia [1.][2.].

Az iratkezelésre vonatkozó jogszabály az elektronikus iratkezelésre vonatkozóan rendelkezésre álláshoz köthető feladatokat nem tartalmaz, csak azt rögzíti, hogy az üzemeltetésre vonatkozó követelményeket az iratkezelő szerv vezetőjének kell meghatároznia [3.].

Az elektronikus közszolgáltatás biztonságát szabályozó jogszabályban a központi szolgáltató rendszerrel kapcsolatban a folytonos üzemeltetést célzó követelmények gyakorlatilag a katasztrófa elhárításra vonatkozó eljárásrendben nyilvánulnak meg, így ez a szabályozó sem tartalmaz alkalmazható eljárásrendet [4.].

A fentiek alapján megállapítható, hogy *jogszabály nem tartalmaz olyan követelményeket vagy módszertani segítséget, ami támpontot nyújtana az elektronikus adatkezelő képességek folytonos üzemeltetésének biztosítását célzó eljárások kialakításához.*

A Magyar Köztársaság Katonai Stratégiája szerint a Magyar Köztársaság biztonsági környezetében *biztonsági kockázatot jelenthetnek a kritikus infrastruktúra elleni támadások.*
A védelempolitika alapja, hogy a honvédelem – benne a katonai erő – legyen képes mind a Magyar Köztársaság védelmét, mind a külföldi műveletekben való részvételt a *hagyományos és az aszimmetrikus hadviselés viszonyai között egyaránt teljesíteni, melybe egyértelműen beleértendő az információs fenyegetések és a sebezhetőség kérdésének kezelése*.

A magyar haderővel szemben állított követelmények között szerepel az *erők védelme és megóvása*, a *hálózatközpontú környezetben való alkalmazás képessége*, a hatékony felderítés, *az információszerzés és –csere*, a telepíthetőség, mobilitás, a hosszú távú fenntarthatóság, mely kitűzések az elektronikus adatkezelő rendszerek (képességek) *szükséges mértékű rendelkezésre állásának biztosítása nélkül nem képzelhetők el* [5.].

A Stratégia általánosan megfogalmazott követelményeinek végrehajtását célzó miniszteri feladat meghatározásban az információbiztonsági követelmények mellett a rendelkezésre állás, az üzemeltetés folyamatos biztosítása is megjelenik, de a dokumentum jellegéből adódóan csak általános irányokat tűz ki, és nem határoz meg részterületi feladatokat [6.].

A honvédelmi tárcánál a fentiek mellett az *elektronikus adatkezelő képességek szolgáltatásainak folytonosságára specializált, általánosan alkalmazható, korszerű követelmény nincs kialakítva,* csak rendszerekhez kapcsolódó rendszabályok azonosíthatók.

A katonai szervezetek működéséhez nélkülözhetetlen elektronikus adatkezelő képességekre irányuló fenyegetések és a sebezhetőségek *nem csak a katasztrófa jellegű szolgáltatás megszűnés, hanem a szolgáltatás csökkenés vagy kiesés rendszer-specifikusan sokszínű formájában is jelentkezhetnek.* Emiatt a nemzetközi gyakorlattal összhangban *célszerűnek látszik szervezeti működés folytonosságához (nemzetközi szakirodalom és szabványok megfogalmazása szerint üzletmenet folytonossághoz) szükséges üzemeltetés támogatási kérdések vizsgálata,* az ezzel kapcsolatos alapvető eljárások megfogalmazása *a rendszer-specifikus védelmi rendszabályok kialakításának támogatása érdekében.*

A kialakítandó eljárásokhoz támpontot adhatnak a menedzsment szemléletű általános ajánlások [7.][8.][9.][10.]. Ezen túlmenően kiegészítésként célszerű a nemzetközi szabványok figyelembe vétele a katonai működési sajátosságok szerinti specializálás, valamint a NATO, EU minősített elektronikus adatkezelésre vonatkozó követelmények teljesítése érdekében [11.][12.][13.][14.][15.].

A cikk a honvédelmi szervezetek működésének folytonosságához szükséges IT szolgáltatások szervezet és rendszer-specifikus sajátosságok nélküli, keretrendszerű, általános követelményeinek kialakítását célozza (így nem feladat a tervezés és üzemeltetés körébe tartozóan a rendszerek hibatűrésére, redundanciájára vonatkozó követelmények, irányelvek meghatározása). *Az adott szervezet működéséhez szükséges képességek folytonosságát biztosító rendszabályok ezen általános követelmények alapján pontosíthatók.*

1. CÉLKITŰZÉSEK

A honvédelmi szervezetek működés-megszakadásának elhárítására irányuló tevékenységébe integrálva a kritikus folyamatokat védeni kell az információs rendszerek nagy hibáinak, vagy üzemzavarainak hatásaitól. A bekövetkezett negatív események hatásait mielőbb ki kell küszöbölni, és biztosítani kell a szolgáltatások kellő időben történő újrakezdését.

A szervezeti működésfolytonosság irányítási folyamatába olyan megelőző és helyreállító intézkedéseket kell bedolgozni, melyek az információs szolgáltatások szándékos vagy véletlen okból bekövetkezett kiesése esetén biztosítják a szervezetre gyakorolt hatás csökkentését.

Az üzemzavarok, meghibásodások, szolgáltatás elvesztés, biztonsági incidensek, illetve az információs szolgáltatások rendelkezésre állásra vonatkozó követelményeit működési hatáselemzéssel (business impact analysis; BIA) kell vizsgálni. A hatáselemzés alapján működésfolytonossági terveket kell kialakítani és bevezetni.

2. AZ INFORMÁCIÓBIZTONSÁG MŰKÖDÉSFOLYTONOSSÁGBA TÖRTÉNŐ INTEGRÁLÁSA

A honvédelmi szervezetek működésének folytonosságára irányuló vezetői, szervezési és szervezeti feladatok közé be kell sorolni azokat a felelősségeket, folyamatokat és feladatokat, amelyek biztosítják az adatkezelő képességek működésfolytonosságának támogatását. Az ehhez szükséges feladatok a következők:

1) a kritikus működési folyamatok azonosítása, az elsőbbségi sorrend megállapítása, valamint az ezekkel kapcsolatos szervezeti kockázatok azonosítása;
2) a kritikus működési folyamatokhoz szükséges információs szolgáltatások, az ehhez szükséges képességek azonosítása;

3) az információbiztonsági incidensek hatásainak azonosítása;
4) az esetleges biztosítási lehetőségek azonosítása;
5) a megelőző, illetve a negatív hatásokat mérséklő rendszabályok azonosítása;
6) a szükséges pénzügyi, szervezeti, technikai erőforrások azonosítása;
7) működésfolytonossági terv kidolgozása;
8) a működésfolytonossági terv felülvizsgálatának és naprakészségének biztosítása.

A fentiek alapján látható, hogy a hadműveleti (alkalmazói) követelmények hiányában, illetve csak úgy általánosságban nem hozható döntés annak meghatározására, hogy egy-egy esetben szükség van-e a működésfolytonossági kérdések vizsgálatára, vagy elégséges a napi üzemeltetés körébe tartozó fenntartási és javítási kapacitások alkalmazása. Amennyiben ezzel a kérdéssel foglalkozni kell, *a működésfolytonossági tervet be kell építeni a szervezeti folyamatokba és a működésfolytonossági folyamatokért való felelősséget megfelelő szervezeti elemekhez kell hozzárendelni*.

A szervezeti folyamatokba történő integrálás kulcskérdése annak felismerése és helyes kezelése, hogy *az IT képességekre vonatkozó működésfolytonosság követelményeinek meghatározása nem az informatikai vagy híradó szakterület feladata*. A szervezetek alapító okiratában, működési szabályzatában meghatározott feladatok tűrésen belüli kiesésének biztosításához szükséges *minimum adatkezelő igények felmérése, meghatározása és a tartalék megoldásokra vonatkozó lehetőségek feltárása összetett szervezeti feladat.*

3. A MŰKÖDÉSFOLYTONOSSÁG KOCKÁZATELEMZÉSSEL TÖRTÉNŐ TÁMOGATÁSA

A szervezeti szintű vizsgálat eredményeképpen az elektronikus adatkezelő rendszerekre irányuló kockázatelemzés és menedzselés a következő lépcső, ami segít a feladatok azonosításában és kidolgozásában. A kockázatok azonosításnak és felmérésének legjobb támogatása a meglévő szolgáltatások ismerete (service catalogue) és felügyelete a tipikus megfogalmazású „írjátok össze, hogy mink van, és mire lenne szükség” megközelítés helyett.

A feladat megoldását segíti a meglévő folyamatok monitorozása és a szolgáltatások rendelkezésre állásának naplózása. Az üzemeltetés során meg kell őrizni az üzemeltetésre vonatkozó adatokat, összehasonlításokat kell végeznie az IT szolgáltatásokra vonatkozó követelményekkel, és ki kell mutatni a hiányosságokat. Dokumentálni kell és ki kell vizsgálni a nem megfelelőséget (részleges vagy teljes kiesések, hibás működés), valamint lehetőség szerint előre kell jelezni a jövőben várható, a rendelkezésre állásra vonatkozó egyedi csúcsterheléseket (adatkezelési vagy feldolgozási határidők, gyakorlatok, rendezvények), vagy fejlesztési igényeket (létszámnövekedés vagy új alkalmazások által történő kapacitásbővítési szükséglet). Ahol lehetséges, előre kell jelezni a várható trendeket, kapacitás igényeket és megelőző jellegű tevékenységet kell végezni a sokkoló hatások elkerülése érdekében.

A kockázatelemzés során megtörténik az elektronikus adatkezelő képességek működéséhez szükséges elemek, üzemeltetési környezet, valamint az üzemeltetéshez szükséges humán és szervezeti feltételek azonosítása. Ennek során meg kell határozni a megszakadások valószínűségét és időbeli hatását, az okozott kár mértékét és a helyreállításhoz szükséges időt, valamint:
1) a megszakítástól kezdve a maximális időkiesést, mely még megengedhető;
2) a kiesés alatti minimális szolgáltatási szintet;
3) azt a határidőt, melyre a normál szolgáltatást helyre kell állítani.

Fel kell tárni a kulcsfontosságú tevékenységek szempontjából lényeges függőségeket, beleértve a beszállítókat, szolgáltatókat és külső partnereket, és azonosítani kell azon beszállító és együttműködő szervezeteket, akiktől a kritikus tevékenységek függenek, illetve azon szolgáltatásokat, melyeket ezen szervezetek biztosítanak.

A működésfolytonosság kockázatának felmérése során a működési források és folyamatok tulajdonosait teljes körűen be kell vonni. A különböző kockázati szempontokat össze kell kapcsolni, hogy a szervezet működésfolytonossági követelményeiről teljes kép alakuljon ki (a gyakorlatban is figyelembe kell venni az ok-okozati összefüggéseket, mert az áramszünet, csőtörés, épületgépészeti meghibásodás, vagy vegyi katasztrófa nem mindig tiszta esetként jelentkezik).

A felmérés azonosítsa, számszerűsítse és sorolja be a kockázatokat a szervezetre vonatkozó kritériumok és célok szerint, beleértve a kritikus erőforrásokat, a megszakadás hatásait, a megengedhető kiesési időket és a helyreállítási elsőbbségeket.

A kockázatfelmérés eredményére alapozva ki kell dolgozni a folyamatos működés biztosítását célzó feladatokat, és a tervet jóvá kell hagyatni.

Összetett elektronikus adatkezelő képességek, bonyolult szervezeti folyamatok esetén a terv készítése is erőforrás igényes, hosszú feladat. Ebben az esetben először működésfolytonossági stratégiát kell kialakítani az átfogó közelítés meghatározása érdekében. A stratégiát jóvá kell hagyatni és meg kell benne határozni a folyamatos működés biztosítását célzó terv (tervek) kialakítására, jóváhagyására, felülvizsgálatára vonatkozó követelményeket.

4. A MŰKÖDÉSFOLYTONOSSÁGI TERVEK KIDOLGOZÁSA ÉS MEGVALÓSÍTÁSA

A működésfolytonossági tervezés célja a meghatározott szintű működés biztosítása (a minimális szintű munkavégzéséhez szükséges szolgáltatások helyreállítása), így az egyéb feladatokat (a fenntartási feladatokhoz tartozó általános javítási feladatokat) külön kell tervezni és végrehajtani.

A honvédelmi szervezetnél rögzíteni kell, hogy az incidensek megoldását milyen tevékenységekkel kell megoldani, és hogyan lehet egy előre meghatározott szintre helyreállítani (és fenntartani) a megszakítás által okozott szolgáltatásokat. A tervnek:

1) meghatározott cél és hatáskört kell szolgálnia;
2) elérhetőnek kell lenni minden olyan személy számára, akinek használnia kell azt;
3) azonosítania kell a felülvizsgálatért, naprakészségért és jóváhagyásért felelős személyeket;
4) szabályoznia kell az incidens ideje alatt a külső szervezetekkel kapcsolatos eljárásokat.

A tervezés során:

1) azonosítani kell minden felelősséget és működésfolytonossági eljárást és azokat egyeztetni kell a szükséges együttműködő partnerekkel;
2) azonosítani kell az elfogadható információ- és szolgáltatásvesztést;
3) azonosítani kell a szükséges szolgáltatásokat és erőforrásokat, beleértve a személyzettel való ellátást, az egyéb szükséges szolgáltatásokat (pl. szállítás, helyigény, valamint a tartalék adatfeldolgozó eszközökre vonatkozó intézkedések);
4) eljárásokat kell bevezetni az üzemeltetés határidőre történő helyreállása, visszaállítása, érdekében;

5) eljárásokat kell kialakítani a helyreállítás függőben lévő befejezésének követésére;
6) meg kell határozni az egyeztetett eljárások és folyamatok dokumentálási feladatait;
7) meg kell határozni a helyreállítással kapcsolatos képzési feladatokat, beleértve a menetközben előforduló, előre nem várt események kezelésének fogásait is;
8) meg kell határozni a tervek felülvizsgálatának és pontosításának rendjét.

A működésfolytonossági tervek, dokumentumok, és a feladatok végrehajtásához szükséges anyagok tárolásakor fő szempont, hogy azok *mentesüljenek a fő helyszínen (telephelyen) bekövetkező üzemzavar miatti károsodás alól*.

A tartalék, és egyéb másodlagos üzemeltetési helyszíneken a védelmi rendszabályoknak az elsődleges üzemeltetési környezet szintjén kell lennie. A működésfolytonossági terveknek tartalmaznia kell:

1) a riasztáshoz és a helyzet megoldáshoz szükséges kommunikációs kapcsolatokat;
2) a feladatokat, és a végrehajtásukhoz szükséges támogató információkat;
3) a meghatározott személyek, szervezeti elemek felelősségét, feladatait a helyzet megoldása során, és azt követően;
4) a tervek aktivizálására vonatkozó felhatalmazást, valamint az eseteket, amikor azokat hatályba kell léptetni;
5) a tervek aktivizálásának módszerét;
6) a találkozási helyeket (és tartalékaikat), a naprakész elérhetőségi adatokat és a más szervezetek mozgósításhoz szükséges információkat;
7) azokat a folyamatokat, melyek az incidensek megoldását szolgálják;
8) a kapcsolatokat minden fontos személyhez, akiknek felelőssége, feladata lehet a helyzet megoldásában;
9) a kieséssel kapcsolatos azonnali teendőket:
   a) stratégiai és üzemeltetési változatokat a kiesés megoldására;
   b) a további szolgáltatás kiesések, vagy a rendelkezésre állás megszűnésének megakadályozására irányuló feladatokat;
10) az incidens megoldására vonatkozó tevékenységeket:
   a) a kritikus időszak alatti szolgáltatások;
   b) a helyreállításra irányuló tevékenységek;
11) a végrehajtás végző személyek magánkommunikációjára és az együttműködő szervezetekkel való kapcsolattartásra vonatkozó megoldásokat;
12) a média kommunikációval kapcsolatos feladatokat;
13) az incidensre, a végzett feladatokra és döntésekre vonatkozó fontos adatok rögzítésére vonatkozó eljárásokat;
14) az elvégzendő részletes feladatokat;
15) a működésfolytonossághoz és a helyreállításhoz szükséges erőforrásokat;
16) a kritikus tevékenységekhez rendelt helyreállítási sorrendet, szolgáltatási szinteket és határidőket.

A működésfolytonosságot biztosító tervnek, illetve a végrehajtását támogató dokumentumoknak, segédanyagoknak *gyakorlatban használható, pontosan kidolgozott üzemeltetési dokumentumoknak kell lenniük*. A bennük megfogalmazott műveletekre vonatkozó *biztonsági követelményeket és védelmi rendszabályokat az elektronikus adatkezelő képességek biztonsági dokumentumaiban kell megfogalmazni és jóváhagyatni*. Ez mutatja *az üzemeltetési és a biztonsági dokumentumok szoros kapcsolatát és összehangolásuk szükségességét*.

Önmagában a helyreállítási tevékenység tervezése és gyakorlása nem elégséges a helyzetek kezelésére. *A fenntartáshoz szükséges javító és karbantartó anyagok tervezése, beszerzése, készletezése, szétosztása és pótlása nélkül a folyamatos üzemeltetés nem képzelhető el.*

Ugyanígy szükség van a kritikus infrastruktúra körbe tartozó kritikus információs infrastruktúra elemek azonosítására és erre vonatkoztatva fontossági sorrend szerint helyreállítási és készletezési eljárások kialakítására és fenntartására. Abban az esetben, amikor nem lehetséges megfelelő mennyiségű tartalék képzése, *egyéb helyettesítő megoldások kialakítására van szükség (más rendszerek alkalmazása, külső szolgáltató igénybe vétele)*.

A költségvetési tartalékok kialakításakor figyelembe kell venni, hogy a katonai, speciális üzemeltetési sajátosságok miatt *kialakulhatnak olyan helyzetek, amikor a meghibásodások, kiesések előre nem látható kombinációja következik be*. Ezek leküzdése csak akkor lehetséges, ha az eszköz beszerzések, szolgáltatás szerződések területén *általános, azonnal aktivizálható tartalékok állnak rendelkezésre*.

5. A MŰKÖDÉSFOLYTONOSSÁGI TERVEK FELÜLVIZSGÁLATA, PONTOSÍTÁSA ÉS GYAKORLÁSA

Általános követelmény, hogy a működésfolytonossági tervek *folyamatosan pontosítva, minden szükséges helyen rendelkezésre álljanak*.

A helyreállítási csoportoknak és más, illetékes személyeknek ismerniük kell a működésfolytonossági tervet és felelősségét a működésfolytonosságért – ezen belül az információbiztonságért –, és ismerniük kell a tervek aktivizálásának kritériumait is.

A működésfolytonossági tervek felülvizsgálatának tartalmi követelményeit és gyakoriságát, valamint a felelős személyeket (szervezeti elemeket) az üzemeltetésért felelős vezetőnek kell meghatároznia. A felülvizsgálat ütemezésekor minden végrehajtandó feladat ellenőrzését ütemezni kell. A felülvizsgálathoz a következő módszereket (és azok kombinációit) kell alkalmazni:

1) a különböző forgatókönyvek asztali vizsgálata (a működés helyreállítási intézkedések tárgyalása, teszt megszakításokat alkalmazva);
2) szimulációk (különösen a személyek oktatásában, az incidensek utáni kríziskezelési feladatokban);
3) műszaki helyreállítási vizsgálat (annak biztosítása, hogy az információs rendszerek eredményesen visszaállíthatók);
4) a visszaállítás vizsgálata egy alternatív helyszínen (amikor a működési folyamatok a visszaállítási üzemeltetésekkel párhuzamosan futnak a főhelyszíntől távol);
5) a szállítók eszközeinek és szolgáltatásainak vizsgálata (biztosítva, hogy a külső felek által nyújtott szolgáltatások és termékek kielégítsék a szerződéses kötelezettségeket);
6) teljes próbák (annak vizsgálata, hogy a szervezet, a személyzet, a berendezés, az eszközök és a folyamatok képesek-e a meghibásodások vagy kiesések elhárítására).

A felülvizsgálatok végrehajtását dokumentálni kell. Minden esetben rögzíteni kell a megfelelőséget, a feltárt hiányosságokat és a változtatási javaslatokat. A változtatási javaslatokat a változáskezelési eljárások figyelembe vételével kell kezdeményezni, tesztelni, jóváhagyni, oktatni és hatályba léptetni.

A működésfolytonossági tervek változtatását mérlegelni kell a következő esetekben:

a) új berendezés beszerzése, a rendszerek bővítése, vagy
b) változások a következőkben:
   i) a személyzetben;
   ii) a címekben és telefonszámokban;
   iii) a szervezeti stratégiában, fontosabb feladatokban vagy folyamatokban;
   iv) a helyekben, eszközökben és erőforrásokban;
   v) a jogszabályokban;
   vi) a szerződő felekben, szállítókban és kulcsfontosságú vevőkben;
   vii) a kockázatban (üzemeltetési és pénzügyi).

A szervezetnél *a működésfolytonosságra vonatkozó tevékenységet gyakoroltatni kell* a szervezeti követelményeknek való megfelelőség biztosítása érdekében.

Az időszakosan tervezett és a meghatározott szintű változásokhoz kötött gyakorlásokat a gyakorlásból, képzésből adódó kockázatok csökkentése érdekében dokumentáltan kell tervezni; *a gyakorlás célját és hatókörét pontosan meg kell határozni*, a tervet jóvá kell hagyatni.

A működésfolytonossági tevékenységek teljes körének ellenőrzése, hatékonyságának igazolása érdekében különböző típusú és szintű gyakorlásokat kell tartani.

A gyakorlások után értékelni kell, hogy a cél megvalósult-e és a gyakorlatok lefedték-e a tervezett területeket. A gyakorlás eredményét dokumentálni kell, és *a felelős vezetőt tájékoztatni kell az eredményről*; javaslatokat kell tenni az esetleges változtatásokra.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az egyik legfontosabb levonható következtetés, hogy a működésfolytonossági tevékenységet egyrészt *integrálni kell a katonai szervezetek tevékenységébe*, másrészt azokat *előre meghatározott célok megvalósítása érdekében kell kialakítani*.

Fontos annak leszögezése is, hogy a kívánt célt – a szükséges mértékű rendelkezésre állást – csak tervezett, dokumentált, tesztelt, jóváhagyott, begyakorolt, felülvizsgált és pontosított eljárások szolgálhatják, a rögtönzés, összehangolatlan döntések (vagy döntések hiánya) a helyzetet csak ronthatják. Az előre jósolható, fontosabb eseteket modellezni kell, és *típus eljárásokat kell kidolgozni, ami elősegíti azt, hogy a különböző szintű vezetőknek csak a valóban egyedi esetekben kell döntést hoznia*.

A fentiek alapján megállapítható az is, hogy *a honvédelmi tárca információ biztonságpolitikája a működésfolytonosságra vonatkozóan kiegészítésre szorul [15.]*. A nyilvánvaló szoros összefüggések alapján a kiegészítés során *célszerű a Kritikus Infrastruktúra Védelem feladatainak támogatását is figyelembe venni*.

A keretrendszerű, általános feladatok megfogalmazása alapján az egyes elektronikus adatkezelő képességekre vonatkozó védelmi rendszabályok egyszerűen *pontosíthatók a képességekért felelős vezetők, üzemeltetők, biztonságért felelős személyek által, illetve könnyebben megfogalmazhatók azok a fenntartási feladatok melyek a logisztikai szakterületről nélkülözhetetlenek a szükséges mértékű rendelkezésre állás megvalósítása*.

HIVATKOZÁSOK

[1.] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, 58. §. 1-2. bekezdés

[2.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 1. §. 22. p. és 58-59.§.

[3.] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről, 7.§. d. és 8. §. (1)

[4.] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról, 2. sz. melléklet, a központi elektronikus szolgáltató rendszer informatikai katasztrófaelhárítási tervének alapkövetelményei

[5.] Magyar Köztársaság Katonai Stratégia, I, II, és IV. fejezetek

[6.] 103/2009. (XII. 31.) HM utasítás a honvédelmi tárca 2010. évi fő feladatainak és a 2011-12. évi tevékenysége fő irányainak meghatározására, 6. §. és 11. §.

[7.] COBIT 4. 1. DS 4.1 – 4. 10. p, DS 11. 1. és 11. 5. p. DS 13. 1 – 13. 4. p.

[8.] ITIL v.3. Service Operation, 4.1. Event Management, 4.4. Availability management, 4.5. IT Service Continuity Management

[9.] The Standard of Good Practice for Information Security; Information Security Forum (ISF), 2007, UE 4. 4.2. p, SM 5.2. 5.2.2. p. SM 5.3. 5. 3. 6. p.

[10.] A Chief Information Officer kézikönyve, 2003, Management Kiadó Kft. ISBN 963 86190 9 0; 7. 4. 6. p, 7. 5. 3. p, és 7. 7. 1. p.

[11.] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, „A” melléklet, A 14. 1 – 14. 1. 5. p.

[12.] ISO/IEC 17799: 2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2006), 14. 1 .1 – 14. 1. 5. p.

[13.] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, 14. fejezet

[14.] Business Continuity Management – Part 2. Specification (BS 25999-2:2007); 4. 4. 1. p, 4. 4. 3. p, és 4. 4. 2. p.

[15.] Informatika. Szolgáltatásirányítás 1. rész: Előírás (MSZ ISO/IEC 20000-1: 2007), 6. 3. fejezet

[16.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról