HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Kassai Károly
kassai.karoly@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELMI FELADATOK ÉS A FELELŐSSÉG

Absztrakt

Az elektronikus adatkezelés szabályozottsága, a szükséges mértékű védelmi rendszabályok a honvédelmi szervezeteknél biztonsági menedzsment kialakítását és fenntartását követelik meg. A védelemből adódó jellegzetességek miatt (időtényező, személyi és egyéb erőforrás igények, szervezeti problémák) ennek a követelménynek van néhány szervezeti szempontból negatívnak tekinthető hatása, így célszerű a biztonsági menedzsment kérdések vizsgálata, a fontosabb feladatok azonosítása. Jelen cikk az elektronikus adatkezelő rendszerek menedzseléséhez szükséges feladatok azonosítását célozza annak érdekében, hogy a rendszer életciklusnak megfelelően érthetőbbek legyenek a védelemmel kapcsolatos követelmények.

The regularization, appropriate level security measures of the electronic information handling at the military organisation requires establishing and permanently upgraded security management.

This requirement has some negative organisation impact because of the nature of security (time, additional human and other resources, and organisation problems) so should be useful to observe the security management issues and identify the important tasks.

This article identifies the tasks of electronic information handling security management for the understandable security requirements according to the system life cycle.

Kulcsszavak: *információbiztonság, információvédelem, személyi biztonság, biztonsági menedzsment, biztonsági követelmények ~ information security, protection of information, personal security, security management, securiry requirements*

Bevezetés

A honvédelmi szervezetek elektronikus adatkezelésének biztonsági kérdései alapvetően két kategóriára bonthatók: a *felhasználók által végzendő védelmi feladatokra* és a *biztonsági menedzsment feladatokra*.

Jelen cikk az *elektronikus információbiztonsági menedzsment végrehajtói szintű szakfeladataira koncentrál*, de figyelembe veszi azt a tény, hogy egyes rendszerek vagy helyszín esetében ezek a szakfeladatok élesen nem határolhatók el a fizikai-, személyi vagy dokumentumbiztonsági kérdésektől.

Az átfogó jellegű jogszabályi megfogalmazások mellett szükség van a végzendő feladatok részletesebb azonosítására és ezzel a honvédelmi szervezeteknél a rendszer-specifikus és a szervezeti típusú felelősségi körök meghatározásának támogatására, így e területen a cikk közvetlenül támogatja biztonsági dokumentumokban és munkaköri leírásokban történő megfogalmazásokat.

Jogszabály minősített elektronikus adatkezelő rendszer esetében határoz meg a védelmi feladatok ellátását végző személyek kijelölésére vonatkozó követelményt a rendszerbiztonsági felügyelő/felügyelet formájában [1.]; mely feladatkör alapesetben nem tartalmazza a rejtjelzéssel kapcsolatos feladatokat (de nem is zárja ki azon feladatok együttes végzését sem).

A nemzeti és nemzetközi szabványok [2, 3, 4.] és a vonatkozó kormányzati ajánlás [5.] szintén határoznak meg feladatokat a biztonságért felelőssé tehető személy azonosítása érdekében.

A honvédelmi tárca információ biztonságpolitikája az általános követelmények és ajánlások szerint a honvédelmi szervezeteknél az elektronikus információvédelmi feladatok ellátása érdekében szervezethez és rendszerhez köthető felelősöket azonosít [6.], amely kötelezettséget a korábbi kiadású informatikai szabályzat is azonosít. [7.]

Az előbbi követelmények, illetve ajánlásoknak megfelelően a honvédelmi szervezeteknél *a szervezeti és adatkezelési sajátosságok figyelembe vételével* az elektronikus adatkezelés biztonsági kérdéseit a következő általános szempontokat specializálva célszerű megoldani.

A szervezeti szintű elektronikus információvédelmi szakfeladatok

A szervezethez köthető elektronikus információbiztonságért felelős személy (vagy szervezeti elem) az elektronikus adatkezelő rendszerektől függetlenül, az egész szervezetre vonatkozó szakfeladatokat végez a kijelölt vezető beosztású személy szakmai vezetésével. Az ebbe a körbe tartozó feladatok:

a) a szervezetnél található elektronikus adatkezelő rendszerek (eszközök) nyilvántartása, azok biztonsági besorolása;
b) a rendszer szintű kockázatelemzés irányítása, a folyamatos kockázatkezelési tevékenység felügyelete;
c) a szervezeti szintű elektronikus információvédelmi rendszabályok azonosítása, helyi szabályozás kialakítása, jóváhagyatása és időszakos felülvizsgálata;

d) a szervezetnél végzendő helyi képzési, továbbképzési feladatok és biztonsági tudatosságot segítő programok szervezésével és végrehajtásával kapcsolatos tevékenység;
e) a rendszer-specifikus felelősök szakmai felügyelete, támogatása;
f) a szervezetnél található elektronikus adatkezelő rendszerek védelmének szabályozásához szükséges jogszabályok, állami irányítás egyéb jogi eszközei körébe tartozó szabályozók szabványok, ajánlások nyilvántartása, rendelkezésre állásuk biztosítása;
g) a szakmai kapcsolattartás az együttműködő szervekkel és szervezetekkel;
h) a rendszerek kialakítása, fejlesztése során a projekt tevékenységben való részvétel és a szervezet elektronikus információvédelmi képviselete;
i) az elektronikus adatkezelő rendszerek biztonságával kapcsolatos ellenőrzési tevékenység szervezése, ellenőrzések végrehajtása, a biztonsági incidensek kivizsgálása (annak irányítása) és a szükséges korrekciós lépések felügyelete.

Annak eldöntése, hogy a védelmi rendszabályok felügyelete elvégezhető-e egy fővel, vagy szervezeti elemet kell kialakítani, a szervezet és adatkezelés elemzése után történhet meg. Ugyanígy további eldöntendő kérdés, hogy a biztonsági feladatokat önálló beosztásban vagy megbízással kell ellátni az adott honvédelmi szervezetnél.

Napjainkban egyértelműen érzékelhető az elektronikus adatkezelés terjedése, bonyolultságának növekedése, illetve az ezzel kapcsolatos fenyegetések és sebezhetőség bővülése. Emiatt *egyre nagyobb az alkalmazandó ismeretanyag, egyre bonyolultabb tevékenységeket kell kialakítani és fenntartani*, így a jövő vélhetően az önálló beosztások formájában történő felügyelet lesz, de az ehhez vezető út hosszú és rögös a honvédelmi szervezetek életében.

Az elektronikus adatkezelés rendszer-specifikus felügyelete

A honvédelmi szervezetnél alkalmazott elektronikus adatkezelő rendszerek, eszközök valamint a kezelt adatok mennyisége, bonyolultsága, a szervezeti és alkalmazása sajátosságok alapján eldöntendő kérdés a védelmi rendszabályok felügyeletéért felelős személyek számának és feladatainak meghatározása.

Egyszerűbb esetben a szervezeti szintű felügyelet elláthatja ezt a feladatot, de a gyakorlatban az a jellemző, hogy a rendszer-specifikus szakfeladatokat megbízás alapján tevékenykedő személyek látják el a terhek jobb elosztása érdekében.

Alapelv, hogy az *összeférhetetlenségre vonatkozó követelmény alapján* a biztonsági menedzsment úgy legyen kialakítva, hogy a felügyeleti feladatok *az adatkezelési helyekhez kötötten minél kevesebb erőforrást igényeljenek, a problémák megoldási ideje a lehető legrövidebb legyen*.

Az elektronikus adatkezelő rendszerek elektronikus információvédelméért felelős személy feladatainak meghatározásakor a következő általános követelményeket célszerű rendszer-specifikusan alkalmazni.

Az elektronikus adatkezelő rendszer kialakítása során végzendő szakfeladatok

Az egyik legfontosabb feladat a hadműveleti követelmények, a rendszerre vonatkozó általános biztonsági követelmények azonosítása, illetve az ezzel kapcsolatos változások

naprakész ismerete. Ennek alapján végezhető a kezdeti kockázatelemzés, *az elfogadható kockázatok (acceptable risk) azonosítása, és jóváhagyatása*.

A kockázat értékelés és a jóváhagyott elfogadható kockázatok alapján történhet meg a rendszer-specifikus biztonsági követelmények meghatározása, majd jóváhagyatása, és annak alapján a szükséges védelmi rendszabályok bedolgozása a tervezési folyamat során.

A BIZALMAS vagy magasabb minősítésű elektronikus adatkezelés esetén a tervezéshez elengedhetetlenül szükség van az üzemeltetési környezet kompromittáló kisugárzás elleni védelmi zónázására, és az eszközökre, kábelvezetésre, árnyékolásra, biztonsági távolságokra, földelésre vonatkozó követelmények azonosítására, amely feladat a későbbiekben láthatóan önálló beosztás vagy megbízás formájában végezhető.

Az üzemeltetés előkészítéseként az egyik legtöbb gondot okozó feladat *az üzemeltetéshez szükséges állomány és a felhasználók kijelöltetése és a minősítési szintnek megfelelő személyi biztonsági adminisztráció elvégzése*. A későbbi problémák megelőzése érdekében ebben a fázisban végre kell hajtani a hozzáférési joggal rendelkező személyek általános biztonsági oktatását is.

Az üzemeltetési környezet kialakításakor a biztonsági kérdések felügyelete, illetve a kockázatelemzés pontosítása a soros feladat.

Hazánkban a NATO, EU követelményektől eltérően a korábbi és a jelenleg hatályos jogszabály önálló akkreditálást határoz meg a fizikai-, személyi- és dokumentum biztonsági követelményeknek való megfeleltetés érdekében, így az elektronikus adatkezelő rendszerek kialakításakor e feladatokat is figyelemmel kell kísérni. Ezzel párhuzamosan haladhat a biztonsági követelmények alapján *a rendszer-specifikus biztonsági dokumentumok elkészítése*, valamint az üzemeltetési és egyéb dokumentumokba (szervezeti szintű vagy funkcionális szabályozók) a szükséges védelmi rendszabályok bedolgozása. Ennek során szükségessé válik az akkreditáláshoz, jóváhagyáshoz szükséges *biztonsági tesztre vonatkozó követelmények meghatározása*, majd a teszt végrehajtásának szakmai támogatása.

Napjainkban közvetlenül érzékelhető a missziós tevékenységek, gyakorlatok illetve az állandó rendszerek esetében is *az adatcserére, újabb kifejezéssel az adatmegosztásra vonatkozó fokozott igény*. Az ezzel kapcsolatos technikai, szervezési, együttműködési szakfeladatokat nem szükséges külön kiemelni, de fontos annak megjegyzése, hogy *főleg nemzetközi környezetben és minősített adatmegosztás esetén az ezzel kapcsolatos feladatok a tervezés és üzemeltetés során többlet feladatot jelentenek* a biztonsági dokumentumok, az engedélyezés, a technikai és menedzsment szintű együttműködés területén.

A rendszerbeállítás érdekében elkerülhetetlen, gyakran több körös feladat *az akkreditáláshoz, jóváhagyáshoz szükséges dokumentumok elkészítése* az hatósági követelmények szerint. Az ekkor már rendelkezésre álló részletes adatok alapján az üzemeltető és felhasználó állomány számára a szükséges tájékoztatási, képzési feladatok maradéktalanul elvégezhetők, valamint lehetővé válik *az üzemeltetési szakasz képzési, továbbképzési feladatainak azonosítása*.

A telepítés során jellemzően végzendő feladat a biztonsági funkciók kialakításának felügyelete, a biztonsági beállítások ellenőrzése, a rendszer szintű, az üzemeltetés és biztonság szempontjából *kritikus hozzáférésekre vonatkozó felügyeleti lehetőségek kialakítása*, illetve általánosan fogalmazva *a telepítés teljes körű biztonsági felügyelete, dokumentálása*.

A rendszerbeállítás előtt az akkreditáláshoz, jóváhagyáshoz szükséges adminisztratív feladatokat kell elvégezni, illetve *a megfelelő szintű biztonság hitelesíthetősége érdekében az eljárás során szükség van adatok, bizonyítékok szolgáltatására*.

Az akkreditálás, jóváhagyás során üzemeltetési és biztonsági területű hiányosságok merülhetnek fel, amely esetben szükség lehet a felszámolásukhoz szükséges eljárás kialakítására.

Amennyiben az akkreditálás, jóváhagyás során az üzemeltetés engedélyezése korlátozással történik, *a korlátozások érvényesítéséhez szükséges eljárásokat be kell dolgozni a biztonsági és üzemeltetési dokumentumokba*, és a változásokról tájékoztatni kell az érintetteket (felhasználók, üzemeltetők, vezető állomány, együttműködő szervezetek).

Az elektronikus adatkezelő rendszer üzemeltetése során végzendő szakfeladatok

Általános feladat a biztonsági dokumentumok naprakészen tartása, meghatározott időszakonként történő felülvizsgálata, illetve a jogosultak felé történő rendelkezésre bocsátása. Ennek részeként kiemelendő az időszakos kockázatelemzés végrehajtása, az elfogadható kockázatok azonosítása és jóváhagyatása, szükség esetén kiegészítő védelmi rendszabályok kidolgozása, mert az üzemeltetési szakaszban történő változások negatív hatással is lehetnek az elektronikus adatkezelő rendszer biztonságára.

Logikailag ide tartozik a rendszer életútja során keletkező ellenőrzési jegyzőkönyvek, biztonságot is érintő dokumentumok, jelentések áttekintése, értelmezése és értékelése, a tapasztaltak alapján a szabályozásban szükséges változtatások tervezése és végrehajtása.

Szervezeti vagy rendszer-specifikus feladatként egyaránt megjelenhet az illetékes szervek és szervezetek felé tájékoztatási, adatszolgáltatási kötelezettség teljesítése.

Szintén általános feladatként fogalmazható meg a biztonsági dokumentumokban foglaltak pontos betartása és betartatása, a biztonsági incidensek jelentése, szükség szerint közreműködés a helyreállításban, kivizsgálásban, a felhasználók és az üzemeltetők időszakos továbbképzése illetve munkájának folyamatos támogatása, a biztonsági tudatosságot erősítő feladatok végzése.

Hosszú távú, ismétlődő feladat az időszakos újra-akkreditáláshoz, jóváhagyáshoz szükséges feladatok végzése, az elektronikus adatkezelő rendszer *hardver és szoftver konfiguráció időszakos ellenőrzése*, az elektronikus adatkezelő rendszer használatának biztonsági felügyelete, naplófájlok és meghatározott paraméterek ellenőrzése, *az adathordozók kezelésének ellenőrzése*, a rendszer szintű, az üzemeltetés és biztonság szempontjából kritikus hozzáférésekre vonatkozó rendszabályok betartatása, valamint *a biztonsági mentésekre vonatkozó tevékenység ellenőrzése*.

A folytonossági és helyreállítási rendszabályok érvényesülésének ellenőrzése (szükséges állomány megléte, képzettség, gyakorlás, dokumentumok pontossága), illetve a tevékenységhez szükséges tervezési és változáskezelési feladatok végzése olyan további rendszer-specifikus feladat, melyet a hadműveleti követelményekben meghatározott rendelkezésre állási paraméterek, valamint a fenyegetettség és sebezhetőség alapján kell végezni.

A változáskezeléshez tartozó feladathalmaz a rendszer változtatásának előkészítése, kockázatelemzés végzése, a változások biztonsági hatásainak vizsgálata, szükség esetén közreműködés a biztonsági teszt kialakításában és végrehajtásában, a konfiguráció változtatás, vagy rendszer kiterjesztésének engedélyeztetésével kapcsolatos adminisztratív feladatok végzése és az esetleges hatósági eljárások előkészítése, a változtatások átvezetése a biztonsági dokumentumokban, illetve részvétel a meghatározott képzéseken, továbbképzéseken és biztonsági tájékoztatókon.

A rendszerből történő kivonás során végzendő szakfeladatok

A kezelt adatokra vonatkozó követelmények alapján a rendszerből történő kivonáshoz azonosítani kell a szükséges adatmentési, továbbítási, archiválási követelményeket. *Pontosítani kell az információs műveletek védelméhez szükséges rendszabályokat*, illetve érvényre kell azokat juttatni.

Amennyiben olyan kivonás történik, melynek következtében később a mentett felhasználói adatok, vagy rendszeradatok olvasása nem biztosított, az üzemeltető állománnyal együttműködve gondoskodni kell a szükséges információs környezet kialakításáról és fenntartásáról, ami gyakran beruházást, telepítést, képzést és fenntartási feladatok rendszerbe állítását is jelenti.

A rendszerből történő kivonás során azonosítani kell a szükséges törlési és megsemmisítési eljárásokat, ki kell alakítani a végrehajtás feltételeit és felügyelni kell a végrehajtást.

Az üzemeltető esetenként nem képes (vagy nem jogosult) a kezelt felhasználói adatok, üzemeltetési adatok megőrzési idejéről vagy törölhetőségéről nyilatkozni, így esetenként az adathalmozódásból adódó bonyolult ügyek eldöntése több adatgazda és egyéb felelős személyek együttműködését igényli.

Utolsó feladatként a szükséges konfigurációváltozási feladatok, a törlés vagy megsemmisítés dokumentálása, jelentése azonosítható.

A kompromittáló kisugárzás elleni védelem menedzselése

A minősített adatkezelésnél az idén megjelent jogszabály a korábbihoz lényegesen megfoghatóbban határozza meg a kompromittáló kisugárzás elleni védelem (TEMPEST) szakfeladatait [8.].

A honvédelmi tárca információbiztonsági politikája ezt a szakfeladatot a rendszer biztonságáért felelős személy feladatai közé sorolja, vagy önálló beosztásként (vagy megbízásként) fogalmazza meg.

Ennek megfelelően a BIZALMAS, vagy magasabb minősítési szint esetén a TEMPEST szakfeladatokért való felelősséget a szervezeti szinttől, a felügyelt rendszertől, valamint az üzemeltetési környezettől függően (röviden *a TEMPEST védelmi rendszabályok bonyolultsága szerint*) kell specializálni.

A szakterület biztonsági követelményeire és védelmi rendszabályaira vonatkozó kérdések a továbbiakban csak az általános feladatok szintjén azonosíthatók.

A szakfeladatokat végző személynek ismernie kell a kompromittáló kisugárzás elleni védelemre vonatkozó általános követelményeket, ami megköveteli a szükséges szabályozók rendelkezésre állását és alkalmazói szintű ismeretét.

Az általános követelmények alapján irányítani kell a létesítmény zónázással, a TEMPEST eszközökre vonatkozó követelmények meghatározásával kapcsolatos feladatokat, valamint képesnek kell lenni - önállóan vagy szakirányítási segítséggel - *az üzemeltetési környezet kialakításához szükséges kiegészítő követelmények meghatározására* (biztonsági távolságok, földelés, árnyékolás, szűrés) illetve a kockázatelemzés során a szakterületi támogatás biztosítására.

A kialakításhoz köthetően *a védelmi rendszabályokat be kell dolgozni a rendszer-specifikus biztonsági dokumentumokba*, illetve ki kell alakítani azt a *nyilvántartási rendszert, ami támogatja a TEMPEST feladatokkal kapcsolatos azonnali tájékozódást és tájékoztatást*. Ugyanígy a kialakítással kapcsolatos feladat a védelmi rendszabályok megfelelőségének igazolásához szolgáló dokumentumok vagy tanúsítványok kialakítása, illetve beszerzése.

Az elektronikus adatkezelő rendszer bonyolultsága függvényében nem elhanyagolható feladat az üzemeltető, biztonsági és a felhasználói állomány TEMPEST védelmi rendszabályaival való megismertetése és a helyi feladatok meghatározása.

A TEMPEST szakfeladatokat felügyelő személynek a rendszer beüzemelése érdekében közvetlenül támogatnia kell az akkreditálási folyamatot.

Az üzemeltetési szakaszban fő feladatként azonosítható a TEMPEST ismeretek naprakészen tartása (szabályozók pontosítása, képzéseken és továbbképzéseken való részvétel, az ellenőrzések során tapasztaltak hasznosítása).

A védelmi megoldásokat a meghatározott rendben ellenőrizni kell, a rendszer üzemelésével kapcsolatos személyek ismereteit szinten kell tartani, a védelmi rendszabályok megfelelőségét a technikai követelményeknek megfelelően mérésekkel és ellenőrzésekkel kell fenntartani, illetve a rendszer újra-akkreditálása, illetve hatósági ellenőrzése során be kell mutatni *a védelmi rendszabályok megfelelőségét bizonyító adatokat*.

Az adatkezelő rendszerek ezen életút szakasza tartalmazza a karbantartások, javítások és módosítások, fejlesztések témakörét is, ami bonyolultabb esetben épületgépészeti, erős- és gyengeáramú kérdések rendezését igényli. Itt figyelemmel kell lenni a rendszabályok, a környezet, esetleg a minősítési szint változására, különben beruházások futhatnak zátonyra. A „múltkor is így akkreditálta a hatóság”, vagy „ez ugyanolyan megoldás” típusú tartalmas szakértői érveléseknek tűnő megnyilvánulások veszélyes csapdákat hordozhatnak, téves vezetői döntéseket eredményezhetnek.

A rendszerből történő kivonás a kompromittáló kisugárzás esetében különös feladatokat nem igényel, csak a szükséges figyelmet kívánja meg. Mivel a kompromittáló kisugárzás elleni védelmi rendszabályok egy része az infrastruktúrához köthető, így *fontos annak pontos megértése, hogy mely megoldások, infrastrukturális elemek használhatók a létesítményben kialakított új elektronikus adatkezelő rendszer védelmére, és milyen átalakításokat, kiegészítéseket kell elvégezni a szabályos üzemeltetés érdekében.*

Az üzemeltetéshez szükséges biztonsági feladatok

Meghatározott helyszínhez, elektronikus adatkezelő rendszer hálózati elemeihez és adatkezelő eszközeihez rendelt üzemeltetésért felelős személy (pl. rendszeradminisztrátor, üzemeltető mérnök, technikus) vagy szervezeti elem információvédelmi feladatait a következő követelmények szerint kell rendszer-specifikusan meghatározni.

A kialakítás során végzendő feladatok

Az üzemeltetőnek szükség szerinti részt kell vennie a rendszer kialakításának tervezésében, illetve a kezdeti kockázatelemzésben, majd a rendszer-specifikus biztonsági dokumentum kidolgozásában, valamint az ehhez szükséges képzéseken. Ezek után feladat az üzemeltetési rendszabályok kialakítása, beleértve a folytonossági tervezésre és helyreállításra vonatkozó folyamatok tervezését és a tevékenység szabályozását.

Az új képesség sajátossága szerint részt kell venni a telepítésben, vagy a rendszer kialakítására vonatkozó szabályozás szerint a rendszert telepítés és beüzemelés után át kell venni (konfigurálása, biztonsági funkciók kialakítása, biztonsági beállítások telepítése vagy

ezek ellenőrzése és üzemeltetési felelősségének átvétele, beleértve az azonosításra és hitelesítésre vonatkozó adatok változtatását), valamint tanúsítani kell a védelmi rendszabályok megismerését és tudomásul vételét.

Ki kell alakítani a szükséges konfiguráció nyilvántartást, vagy ellenőrzés után át kell azt venni. Itt érdemes megjegyezni, hogy nem csak az anyagi elszámolásról van szó, mert például *a dokumentációhoz képest az eszközben lévő több memória nem jó üzleti érzéket, hanem a dokumentáció pontatlanságát, az átvétel felszínességét mutatja*, esetlegesen a működés során is paraméterek változtatását okozhatja. A felhasználó számára történő rendelkezésre bocsátás érdekében ki kell alakítani a szükséges hozzáférési profilokat, a hozzáférési jogosultság igénylésére vonatkozó hiteles eljárásokat.

A hadműveleti (alkalmazói) követelmények kielégítése érdekében ki *kell alakítani a folytonossági és helyreállítási terveket és a végrehajtásukra szolgáló szabályozást* a rendszer biztonságáért felelős személy által meghatározott biztonsági paraméterek szerint.

A rendszer használatba vétele érdekében *segíteni kell a felhasználók képzését, a védelmi rendszabályok elsajátítását*.

Az akkreditálás, jóváhagyás érdekében biztonsági teszt tervet kell kialakítani a rendszer biztonsági felelős személy szakmai támogatásával, majd dokumentáltan végre kell hajtani a tesztet.

Az előbbi feladatok elvégzése és az esetleges problémák elhárítása után utolsó feladat az akkreditáláshoz, jóváhagyáshoz szükséges adminisztrációban *a rendszer biztonságért felelős személy szakmai támogatása, illetve az eljárásban való részvétel*.

Az üzemeltetés során végzendő feladatok

A rendszer életének e szakaszában az üzemeltető feladata az üzemeltetési dokumentumok naprakészen tartása, meghatározott időszakonkénti felülvizsgálata, illetve a dokumentáció rendelkezésre bocsátása.

Gyakorlati feladat a rendszer folyamatos üzemeltetése, a szoftverkarbantartással kapcsolatos feladatok folyamatos ellátása (vírusvédelmi, anti-spam és egyéb védelmi szoftver frissítések, az operációs rendszerek frissítése, a szükséges kiegészítő programok telepítése és dokumentálása), valamint kapcsolattartás a rendszer biztonsági felelőssel, rejtjelzővel, összekapcsolás esetén a csatlakozó rendszer üzemeltető állományával.

Az üzemeltetési kérdések egyik legproblémásabb feladata *a rendszer felhasználói és rendszer biztonsági felelősi tevékenységének szakmai támogatása*, illetve technikai oldalon a rendszer hardver és szoftver konfigurációjának naprakészen tartása.

A rendszer átalakítás, továbbfejlesztése során egyedi feladat a rendszer biztonságáért felelős személy biztonságra vonatkozó hatásvizsgálatának támogatása.

Konfiguráció változtatáskor, vagy a rendszer kiterjesztésének engedélyeztetésekor el kell végezni a szükséges adminisztratív feladatokat, elő kell készíteni a változtatások engedélyezéséhez szükséges hatósági eljárásokat, majd a műveletek elvégzése után a változtatások át kell vezetni az üzemeltetési és a biztonsági dokumentumokban.

Ismétlődő feladat az időszakos kockázatelemzésben, az elfogadható kockázatoknak megfelelően *a kiegészítő védelmi rendszabályok kidolgozásában való részvétel*, illetve az újraakkreditáláshoz, jóváhagyáshoz szükséges üzemeltetési feladatok ellátása.

Mindenkori feladatnak kell tekinteni a biztonsági incidensek jelentését, majd szükség szerint közreműködést a helyreállításban, kivizsgálásban.

Ugyanígy folyamatos feladatnak kell tekinteni a felhasználók képzését és továbbképzését. A biztonsági tudatosságot erősítő feladatok során lapvető szakmai követelmény a rendszer biztonsági felelős szakmai támogatása.

Az azonosított feladatok nyilvánvalóan naprakész információkat igényelnek, melynek érdekében követelmény a meghatározott szakmai képzéseken, továbbképzéseken és biztonsági tájékoztatókon való részvétel.

A rendszerből történő kivonáskor végzendő feladatok

Az elektronikus adatkezelő rendszer, eszköz életútjának végén az eddigiekhez hasonlóan találhatók olyan feladatok, melyek félreértése, elhanyagolása vagy figyelmen kívül hagyása későbbi szervezeti hátrányokat okozhat kompromittálódás, vagy meglévő de alkalmazhatatlan, esetleg hiányzó adat formájában. Emiatt a felszámolási műveletek előkészítésének alapvető feltétele a helyzet megértése és a végzendő feladatok pontos tervezése.

Ennek része lehet a szükséges adatmentési, továbbítási, archiválási feladatok tervezése és végrehajtása, és az információs műveletek védelméhez szükséges rendszabályok pontosítása és érvényre juttatása.

Gyakran elfelejtett követelmény, hogy az adatkezelő rendszereknek nem csak a felhasználói adatait, hanem az elektronikus adatkezelő rendszer napló adatait is a minősítéssel illetve az adatok érzékenységével arányos követelmények szerint kell tárolni, archiválni.

Amennyiben olyan kivonás történik, melynek következtében a jövőben a mentett felhasználói adatok, vagy rendszeradatok olvasása nem biztosított, a szükséges információs környezet kialakításával kapcsolatos tervezői és végrehajtói feladatokat is a kivonáshoz kell számolni.

A rendszerből történő kivonás során általános feladat az adatok érzékenységével arányos törlési és megsemmisítési eljárások azonosítása és a szükséges eljárásrend kialakítása.

A rendszerből történő kivonás utolsó feladata a konfiguráció változási feladatok dokumentálása, jelentése.

Összefoglalás, következtetések

Az előzőek rávilágíthattak arra, hogy az életciklus szemlélet segíthet az elektronikus adatkezelő képességek biztonsági kérdéseinek azonosításában.

Fontos annak hangsúlyozása, hogy a szervezeti feladatok közötti eltérések, a rendelkezésre álló elektronikus adatkezelő szolgáltatások jelenleg nem teszik lehetővé a minden helyzetben érvényes rendszabályok kialakítását.

A fenyegetések és sebezhetőség megértése, a szükséges szabályozók alkalmazás szintű ismerete, a változások nyomon követése egyre nagyobb figyelmet kíván a végrehajtó személyektől.

A nemzetközi szakirodalom egy része magyarul nem áll rendelkezésre, a NATO, EU adatkezelő rendszerekre vonatkozó követelmények is angol nyelvűek, így nyilvánvaló az a szakmai követelmény is, hogy az elektronikus biztonsági kérdésekért felelős személyek képesek legyenek az angol nyelvű kommunikációra, ismerjék a szakkifejezéseket és azok pontos tartalmi jelentését. A korábbi jogszabályokban található „biztonsági megbízott”, a „Rendszer Biztonsági Utasítás”, a „rendszer üzemeltetés biztonsági felelős”, vagy a „megerősített iroda” már mint nem használatos kifejezések mutatják *a szakmai nyelv szükségszerű fejlődését*, *amit honvédelmi területen még ki kell egészíteni a katonai szakkifejezésekkel is.*

Az információvédelmi szakfeladatok üzemeltetési szakaszra érvényes meghatározása mellett kiemelt fontosságú annak megértése, hogy *az információvédelmi szakfeladatokra*

történő kiválasztással, kijelöléssel, képzéssel, illetve a kinevezés (vagy megbízás) visszavonással kapcsolatosan az életciklus különböző szakaszaihoz köthetően számtalan feladat azonosítható még.

A biztonsági menedzsment feladata, hogy az elektronikus adatkezelő képességek védelméhez szükséges *biztonsági feladatkörök azonosításakor a honvédelmi szervezeteknél átfedések, illetve felügyelet nélküli területek ne legyenek.*

A fentiek rámutatnak arra is, hogy a bonyolultabb elektronikus adatkezelő képességekkel rendelkező honvédelmi szervezeteknél *a biztonság kérdések kézbentartása előrelátást igénylő, bonyolult, erőforrás és időigényes tevékenység.* A honvédelmi szervezetek vezetői, biztonsági vezetői ezt a kihívást csak *a biztonsági kérdések komplex kezelésével, a szükséges ismeretekkel és jártassággal rendelkező személyekre támaszkodva menedzselhetik.*

A honvédelmi szervezetek szakirányú támogatását az át és továbbképzések rendszerében fokozatosan továbbfejlesztett szakmai követelmények szerint évek óta végzi a Zrínyi Miklós Nemzetvédelmi Egyetem. Az oktatott tananyag *gyakorlat centrikusan, a NATO és EU követelményekre támaszkodva készíti fel a honvédelmi szervezetek biztonsági és üzemeltető állományát.* A képzés eredményessége *a hatósági ellenőrzések és akkreditálási eljárások, NATO biztonsági ellenőrzések eredményein keresztül közvetlenül jelentkezik.*

Hivatkozások

[1.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 9-10. §.

[2.] MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények; A melléklet, A 8.1- A 8.3. p.

[3.] MSZ ISO/IEC 17799 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002), 8.1 – 8-3. p.

[4.] ISO/IEC 20000-1 Information technology – Service management - Part 1: Specification; 3.3. p. és 6.6. p.

[5.] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, p. 76-87.

[6.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról, 5. §. (3) és 6. §. (1)

[7.] A Magyar Honvédség Informatikai Szabályzata (Ált/210), 199. p.

[8.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 49-51. §.