HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Kassai Károly
kassai.karoly@hm.gov.hu

A MINŐSÍTETT ADATOK KEZELÉSÉRE FELJOGOSÍTOTT HÍRADÓ-INFORMATIKAI RENDSZEREK VÁLTOZÁSKEZELÉSÉNEK KÉRDÉSEI A MAGYAR HONVÉDSÉGNÉL

Absztrakt

A biztonsági környezet változása, új felhasználói igények megjelenése, technológiai fejlődés, hálózati vagy felhasználói eszközök meghibásodása, vagy szoftverhiba, illetve más indokok miatt válhat szükség a rendszer hardver vagy szoftver konfigurációjának módosítása. A konfigurációváltoztatás egyes esetekben egyszerű, más esetekben összetett felkészülést és támogatást igénylő feladat. A katonai szervezetek vezetése és irányítása gyakran minősített adatok elektronikus kezelését igényli. A kommunikációs rendszerek az akkreditáló hatóság biztonsági felügyelete alatt állnak, így a változtatások engedélyezése esetenként bonyolult hivatalos ügyintézést igényel. A cikk a konfiguráció változás kérdéseit vizsgálja, használható megoldást keresve a katonai szervezetek támogatása érdekében.

Changes in the security environment, the emergence of new user requirements, technological development, network or user equipment failure, software malfunctions or other reasons may require modification in the hardware or software configuration. The configuration change simple in some cases, in other cases require complex preparation and support. Management and control of the military organizations often require electronic handling of classified information. The communications and information systems are under the control of the security accreditation authority, thus authorization of the changes requires official actions sometimes with some complications. The article examines the issue of configuration changes, in search of a solution used to support military organizations.

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

BEVEZETÉS

A Magyar Honvédség szervezeteinél a minősített adatok kezelése az Alaptörvényben és erre épített jogszabályokban meghatározott szervezeti feladatokból adódó követelmények miatt megkerülhetetlenül szükséges.

A minősített adatok kezelésére – kiemelt figyelemmel a minősített elektronikus adatkezelésre – vonatkozó jogszabályi követelmények hazánkban a NATO csatlakozáshoz kötötten 1999-ben, majd az EU csatlakozás kapcsán 2004-ben, illetve az előbbieket is integrálva, a nemzeti követelményeket is modernizálva 2009-ben jelentősen változtak.

A fejlődés nem kerülhette el a Magyar Honvédséget sem, így a felhalmozódott tapasztalatok alapján célszerű átfogóan, vagy egy-egy területet kiemelve áttekinteni az elektronikus információbiztonsági kérdéseket, ami segítheti a helyzet pontosabb megértését, támogatja a jövőbeli változások előkészítését.

A cikk témája egyszerű kérdést megoldását célozza: a minősített elektronikus adatkezelő rendszerek (katonai terminológia szerint: híradó-informatikai rendszerek) hatósági engedélyezéshez kötött változásaival kapcsolatos teendők egyszerűsítése, a változáskezelési folyamat felgyorsítása.

A kérdés tanulmányozását az a gyakorlati igény váltotta ki, hogy a Magyar Honvédség szervezetei egyre nagyobb számban rendelkeznek a Nemzeti Biztonsági Felügyelet – mint akkreditáló hatóság – által jóváhagyott, elektronikus minősített adatot kezelő híradó-informatikai rendszerekkel. Ezek a rendszerek az üzemeltetés során – ugyanúgy, mint minden más elektronikus adatkezelő rendszerek – meghibásodnak, új felhasználói igény, környezeti változás vagy amortizálódás, új sebezhetőség megjelenése miatt változásokat igényelnek.

A változások hatósági engedélyhez kötöttek, ami nyilvánvalóvá teszi az üzemeltető katonai szervezet, a középszintű vezető szerv, a szakmai irányítási feladatokat végző központi szerv és a hatóság közötti hivatalos kommunikációt. Ez a változási kérelem felterjesztését és az arra adott hivatalos válasz továbbítását jelenti, még a szükségesnek ítélt változások megkezdése előtt.

A katonai műveletek dinamikája, illetve a műveletek környezeti változásainak széles skálája eltérő a napi életben megszokott változási sebességtől. A harcászati környezet kihívásai lényeges ponton eltérnek a hadműveleti, stratégiai vezetési és irányítási rendszerek működési jellemzőitől. Ezek a sajátosságok természetesen nem tükröződnek a közigazgatásra vonatkozó, keretrendszerű jogszabályokban, eljárásokban. Ugyanakkor szükségszerű annak megállapítása, hogy a katonai műveletek támogatását szolgáló, minősített adatok kezelésére feljogosított (akkreditált) híradó-informatikai rendszerek nem mentesülnek a jogszabályokban megfogalmazott követelmények teljesítésétől.

A hatósági ügyintézéshez kapcsolódó szolgálati kommunikáció, az ezzel kapcsolatos nyilvántartási feladatok időigényesek, így nyilvánvaló szükséglet egyrészt a bürokráciacsökkentés, másrészt a katonai feladatok időbeli biztosításához szükséges gyors reagáló képesség kialakítása és biztosítása.

A megfogalmazott – jól láthatóan ellentmondásos – tényezők összehangolása, a bonyolult helyzet megoldása nem tűnik egyszerű feladatnak.

A változások menedzselése (change management), más kifejezéssel élve a változásfelügyelet (change control) kérdéskör nemzetközi szabványokban, nemzeti ajánlásokban, a „bevált gyakorlat (best practice)” típusú dokumentumokban és jogszabályokban más-más szemlélettel és részletezettségben olvasható, mely referenciák segíthetnek a probléma megértésében és a megoldás keresésében.

A cikk első részében e források – tudatosan nem teljes körű – bemutatása történik az általánosan elfogadottnak tekinthető tartalmi megközelítés szempontjainak vázolása érdekében, majd a katonai sajátosságoknak megfelelő válaszhoz szükséges megalapozás olvasható.

A VÁLTOZÁSOKRA VONATKOZÓ AJÁNLÁSOK, KÖVETELMÉNYEK

Az informatikai szolgáltatásirányításra vonatkozó szabvány értelmezése szerint a változásfelügyelet (change control): „azok az eljárások, amelyek biztosítják, hogy minden változás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, kivitelezését és a változás megvalósítás utáni áttekintését is."

A változáskezelés célja, hogy minden változtatás kiértékelése, jóváhagyása, megvalósítása és felülvizsgálata ellenőrzötten történjen. Ennek érdekében:

- a szolgáltatások és infrastruktúra területén szükséges változtatásokat pontosan meg kell határozni, a változások végrehajtását dokumentálni kell;
- a változásokra vonatkozó kérelmeket nyilvántartásba kell venni és osztályozni kell;
- a változásokra vonatkozó kérelmeket kockázatuk, hatásuk és hasznuk szerint értékelni kell;
- a változáskezelési folyamatnak tartalmaznia kell a sikertelennek bizonyuló változtatások után a kiindulási helyzet visszaállításához szükséges eljárásokat;
- a változtatásokat jóvá kell hagyni és a végrehajtásukat ellenőrizni kell;
- a változtatások után vizsgálni kell, hogy kitűzött célok megvalósultak-e, illetve az alkalmazott rendszabályok sikeresek voltak-e. [1]

A nemzetközi információbiztonsági menedzsment szabvány is foglalkozik a változások menedzselésével.

A szabvány az üzemeltetési eljárások és felelősség területén szabályozási célként javasolja az adatkezelő létesítmények helyes és biztonságos üzemeltetésének biztosítását. Ennek érdekében az üzemeltetési eljárásokat dokumentálni kell, és a szükséges dokumentumok elérhetőségét biztosítani kell minden olyan felhasználónak, akinek arra szüksége van.

A változások menedzselésére vonatkozó általános követelmény, hogy felügyelni kell a szervezeti változások során, vagy a működési vagy adatkezelő folyamatokban, adatkezelő rendszereknél bekövetkező változásokat, amelyeknek hatása van az információbiztonságra. [2]

Az Amerikai Egyesült Államok közigazgatási szervezeteire és elektronikus adatkezelő rendszereire vonatkozó követelmény szerint az alkalmazó szervezetnek ki kell alakítani, dokumentálni kell és alkalmazásba kell venni egy olyan konfiguráció felügyeleti eljárást, amely:

- meghatározza a szabályokat, felelősségeket, a konfigurációfelügyeleti folyamatokat és eljárásokat;
- folyamatokat határoz meg a rendszer teljes életútján keresztül a konfiguráció elemek azonosítása és a konfigurációfelügyelet érdekében;
- meghatározza az információs rendszerek konfiguráció elemeit és azokat a menedzsment felügyelet hatókörébe rendeli;
- védelmi rendszabályokat alakít ki a konfiguráció felügyeleti eljárás illetéktelen megismerése vagy módosítása ellen. [3]

Az ausztrál nemzeti ajánlás a változáskezelést áttekinthetően tárgyalja, melynek a lényegi elemei a következők.

A változtatás indoka:

- biztonsági sebezhetőség, új fenyegetés megjelenéséhez kötött kockázatnövekedés;
- felhasználó által azonosított problémák vagy a szolgáltatások kiterjesztése;
- a gyártó által kezdeményezett eszközfejlesztés vagy szoftverfrissítés;
- a gyártó által jelzett eszköz vagy életciklus támogatás megszüntetése;
- általános technológiai fejlődés;

- új rendszerek alkalmazása, ami miatt szükségessé válik a meglévő rendszerek változtatása;
- szervezeti változások;
- szervezeti folyamatok változásai;
- a szabványok fejlődése;
- kormányzati követelmények;
- incidensek bekövetkezése vagy a folyamatos szolgáltatásfejlesztési igény.

A változások lehetnek:

- eszköz bevezetése vagy modernizálása;
- szoftver bevezetése vagy frissítése;
- a védelmi rendszabályokban bekövetkezett fontos változás.

A szervezeteknek hivatalos változásmenedzsment folyamatot kell kialakítani, melynek jellemzői:

- azon változások kijelölése, melyek a hivatalos változásmenedzsment folyamaton keresztül valósíthatók meg;
- a változásokat dokumentálni kell;
- a változásra vonatkozó kérelmet hivatalosan jóvá kell hagyni;
- a változások naplóadatait auditálni kell, majd meg kell azokat őrizni;
- a jelentős változások előkészítésekor sebezhetőség vizsgálatot kell tartani;
- a jóváhagyott változásokat tesztelni kell;
- a biztonsági dokumentumokban át kell vezetni a szükséges változtatásokat;
- az érintett felhasználókat értesíteni kell, és ki kell képezni a változáshoz lehetőleg közeli időpontban;
- folyamatosan képezni kell a felhasználókat a változáskezeléssel kapcsolatos feladatokról.

A szervezeteknek biztosítani kell, hogy a normál (rutin) és a sürgősségi változások során:

- a vonatkozó biztonsági dokumentumban meghatározott eljárásokat betartsák a változás menedzsment folyamat során;
- a javasolt változásokat jóváhagyja az arra illetékes, hatóság, szervezet;
- bármilyen változás, melynek a rendszer biztonságára hatása lehet, fel legyen terjesztve az illetékes akkreditáló hatósághoz jóváhagyásra;
- a változásnak megfelelően minden biztonsági dokumentum pontosítva legyen. [4]

JOGSZABÁLYBAN VAGY FELSŐ SZINTŰ SZABÁLYOZÓBAN MEGFOGALMAZOTT KÖVETELMÉNYEK

Az elektronikus információbiztonságra vonatkozó törvény végrehajtási rendelete több szempontot is azonosít a konfigurációváltozások felügyelete (változáskezelés) területén.

Az érintett szervezet:

- meghatározza a változáskezelési felügyelet alá eső változástípusokat;
- meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek stb.);
- megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja, vagy elutasítja azokat;

- dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;
- megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;
- visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;
- auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

A későbbi problémák elkerülése érdekében a szervezetnek a változások megkezdése előtt vizsgálni kell a változások biztonságra irányuló hatásait (biztonsági hatásvizsgálat).

A változáskezelést támogatja az előzetes tesztelés és megerősítés. A tesztelést elkülönített tesztkörnyezetben kell végrehajtani, ahol kockázat nélkül vizsgálható a működés, a funkcionális sajátosságok, a kompatibilitás, esetleges sebezhetőségek.

A változások végrehajtása során pontosan meg kell határozni a hozzáférési jogosultságokat.

A változáskezelés kötelező része a felülvizsgálat, melynek célja a változások szabályszerűségének ellenőrzése, a kívánt cél eléréséről történő meggyőződés. [5]

A minősített elektronikus adatkezelésre vonatkozó alapvető hatósági követelmény a hatóság által jóváhagyott „biztonsági konfiguráció” alkalmazása.

Engedélyezett rendszeren „az elektronikus biztonságot érintő módosítást végrehajtani a Nemzeti Biztonsági Felügyelet által kiadott rendszerengedéllyel lehet”. [6]

A keretrendszerű jogszabály megfogalmazása egyértelmű, tartalmi kérdések elektronikus információ biztonság szempontjából a követelményekben nem vitathatók. Ezzel együtt az is kijelenthető, hogy az alkalmazó szervezetek működési sajátosságai, az elektronikus információ biztonsági szakmai kultúra, a műveleti sebesség lényegesen befolyásolhatja a jogszabály által megfogalmazott követelmény végrehajtására vonatkozó hatékonyságot.

A változáskezeléssel kapcsolatos kérdések szabályozása szerepel a Magyar Honvédség új Informatikai Szabályzatában is.

A Szabályzatban foglaltak szerint „a változáskezelés a híradó-informatikai rendszerben végrehajtott változtatások hatásának előrejelzésére, valamint a változások összehangoltságának és nyomon követésének biztosítására irányul, amely magában foglalja a kérésteljesítések és az esemény – probléma és incidenskezelések során végrehajtott változásokat”.

Az általános követelmény három pillérre támaszkodik, mint felelősségek, folyamat kijelölési kötelezettség és egyedi esetek kezelése, a következők szerint:

- az üzemeltető szervezetnek meg kell határoznia a változtatásokhoz kapcsolódó, javaslattevő, véleményező és döntésre jogosult, szervezetek, személyek körét;
- az üzemeltető szervezeteknek ki kell alakítaniuk a halasztást nem tűrő változtatások eljárás- és szabályrendszerét;
- központi szolgáltatás üzemeltetési tervétől vagy normatív változáskezelési eljárásrendjétől eltérő módosítás az MH Kormányzati Célú Elkülönült Hírközlő Hálózat hálózatgazdájának engedélyével hajtható végre;

A Szabályzat a híradó-informatikai rendszerek biztonságáról szóló fejezetben olvasható általános biztonsági követelmény között is szerepel a változáskezelés:

- új híradó-informatikai rendszer bevezetése, vagy változást követő alkalmazásba vétele csak a meghatározott engedélyezési eljárás sikeres lefolytatása után történhet;
- az üzemeltetési és biztonsági dokumentumokban azonosítani kell az engedélyezési jogosultságokkal rendelkező hatóságokat és szervezeteket, eljárásokat;
- az üzemeltetési és védelmi rendszabályok engedéllyel, a szükséges dokumentálási és képzési eljárások után változtathatók. [7]

A MAGYAR HONVÉDSÉGNÉL SZÜKSÉGES MEGOLDÁS KÖRVONALAZÁSA

A fentiek alapján az elektronikus minősített adatkezelésre feljogosított híradó-informatikai rendszerek változtatásával kapcsolatos hatósági engedélyezési eljárás a következőkben foglalható össze:

- A keretrendszerű jogszabály részletesen nem szabályozza (nem is szabályozhatja) részletesen a változásokra vonatkozó részletes követelményeket, így a kötelezően betartandó „irányelv"- ként történő értelmezés segíthet a megoldásban. Ez azt jelenti, hogy a jogszabály nem tiltja azt a megoldást, amit a szabványok és bevált gyakorlatként kezelhető dokumentumok ajánlanak: *a normál változáskezelési eljárás megfogalmazását, és a folyamat akkreditáló hatósággal történő jóváhagyatását*. Az akkreditáló hatóságnak így lehetősége van a kezdeményező fél által megfogalmazott eljárásrendet áttekinteni, elemezni, a szükségesnek tartott kiegészítéseket megtenni, majd *a változáskezelési eljárást jóváhagyni*. Az eljárásrend kialakítása során *meg kell fogalmazni a sürgősségi esetekre vonatkozó kivételeket, eljárást is*, mivel a katonai erők alkalmazása elképzelhető olyan helyzetekben, amikor a normál hatósági ügyintézés keretei nehezen alakíthatók ki.
- Az előbbi megállapítást támogatja, hogy a Magyar Honvédségnél lehetőség van a szakfeladatok szolgálati hierarchia szerinti felosztására, a felelősségek szervezeti szintek szerinti meghatározására. Ez azt jelenti, hogy egy honvédelmi szervezet esetében *az akkreditáló hatóság segítségére van a szakirányítási rend szerint a középszintű vezető szerv és a szakmai feladatok irányításáért felelős minisztériumi szerv felügyeleti tevékenysége* (alárendeltségi viszonytól függően egyik vagy mindkettő).
- A Magyar Honvédség esetében lehetőség van az elektronikus minősített adatkezelésre feljogosított híradó-informatikai rendszerek változtatására vonatkozó központi szabályozó kiadására, ami biztosítja az egységes végrehajtáshoz szükséges támogatást. Ez ezt jelenti, hogy *a Magyar Honvédség esetében pontosan meghatározható, hogy mely változási kérelmeket szükséges az akkreditáló hatósághoz felterjeszteni, és mely esetekben lehetséges a helyi engedélyezés (beleértve a szükséges dokumentálási kötelezettséget).*

A források áttekintése után szükség van annak megfogalmazására, hogy miért van szükség minősített elektronikus adatkezelés esetén a hatóság értesítésére, illetve a változások engedélyeztetésére.

Az adatkezelés engedélyezését célzó hatósági eljárás (akkreditálás) célja annak megállapítása, hogy az adott környezetben azonosított fenyegetések, a híradó-informatikai rendszer sebezhetősége és a meghatározott (jogszabályokban, NATO, EU követelményekben vagy hatósági állásfoglalás szerint egyedileg meghatározott) védelmi rendszabályok szerinti állapot az elfogadható kockázat kategóriába tartoznak, az adatkezelés nem tartalmaz nemzeti vagy szövetségi szintű felesleges kockázatokat. A *konfigurációelemek azonosítása (ellenőrzése) ennek megfelelően csak keskeny szeletét adják a hatósági mérlegelésnek*.

Az akkreditáló hatóság (egyszerűbben fogalmazva: a szakértő) így *az üzemeltető szervezet vezetőjének, biztonsági menedzsmentjének garanciát ad* arra, hogy az adott helyzetben, az adott konfiguráció a meghatározott üzemeltetési és védelmi rendszabályokkal felesleges kockázatvállalás nélkül üzemeltethető.

Amikor valamilyen ok miatt szükségessé válik a konfiguráció változtatása, akkor az előbb megfogalmazott *egyensúly felborulhat*, és szükséges lehet annak hatósági vizsgálata, hogy *a változások okán keletkezett-e újabb kockázat és azt milyen kiegészítő védelmi rendszabályokkal lehet ellensúlyozni*, vagy milyen szervezeti érdeket védő eljárást kell életbe léptetni a helyzet

folyamatos kézbenntartása érdekében. Ez az a kulcselem, melynek megértése segít eldönteni, hogy milyen adatok szükségesek a hatósági mérlegeléshez, illetve egyáltalán milyen esetekben van szükség a kockázatok teljes vagy részleges áttekintésére és a védelmi rendszabályok megfelelőségének vizsgálatára.

A jogszabályban meghatározott „biztonságot érintő módosítás" így más megvilágításba kerülhet. Egy meghibásodás miatt cserélendő billentyűzet, monitor, vagy akár az egész felhasználói környezetet biztosító számítógép cseréje a vázoltak szerint olyan változás, amelyet hatósági mérlegelés alá kell vonni? A válasz egyszerű: nem. A kijelölt üzemeltető és biztonsági állomány a biztonsági vezető felügyelete alatt ezeket a változtatási feladatokat kockázatmentesen el kell, hogy tudja végezni! Amennyiben ez kétséges, akkor már az adatkezelés engedélyezése is az volt (tekintettel a szekértői tudással rendelkező üzemeltető és biztonsági állomány hiányára)!

A hatóság szakértői mérlegelésére, *szakmai támogatására akkor van szükség, amikor a védelmi rendszabályok és a biztonsági környezet változásainak összehangolásával kapcsolatos feladatokban valami nem egyértelmű; nem könnyen eldönthető helyzet állt elő, ami felsőbb szintű szervezet hatáskörébe tartozó adatgyűjtést vagy döntést igényel, vagy több megoldásból szakértői tanácsadással lehetséges kiválasztani a fenyegetések ellensúlyozásához szükséges legjobb választ*.

A hatósági feladatok ellátása szempontjából három eset különíthető el:

- változás, ami a biztonsági szint csökkenésével kapcsolatos;
- változás, ami nem befolyásolja a híradó-informatikai rendszer biztonsági szintjét, de hatósági ügyintézést igényel;
- változás, ami nem befolyásolja a híradó-informatikai rendszer biztonsági szintjét, hatósági ügyintézést nem igényel, helyi engedélyezési és felügyeleti eljáráshoz kötött.

Csökkenő biztonsági szint

Ennél az esetnél az esetben az akkreditált konfigurációban vagy az alkalmazási körülmények során olyan változás következik be, ami a jóváhagyott védelmi rendszabályok csökkenését vagy megszűnését jelenti. Példák:

- vírusvédelmi rendszer megszűnése vagy frissítés hiánya;
- TEMPEST védelmi rendszabályok hiányossága, mint árnyékolás, szűrés, biztonsági távolság megszűnése vagy be nem tartása, a felügyelt terület csökkenése;
- fizikai biztonsági rendszabályok hiánya, mint beléptető rendszer kiesése, biztonsági tárolási feltételek megszűnése;
- olyan programok telepítése, melyek az operációs rendszer biztonsági beállításait módosítják;
- összekapcsolás más – esetleg alacsonyabb biztonsági szintű – adatkezelésre feljogosított híradó-informatikai rendszerrel.

Ebbe a kategóriába tartozik a híradó-informatikai rendszerhez kapcsolódó teszt engedélyeztetése is, ami az akkreditált konfigurációval vagy akkreditált környezeten belül történik – akár azonos minősítésű szint kezelésére akkreditált újabb eszközöket vagy rendszert is érinthet –, és új működési rendet vagy konfigurációváltozást okoz, ami az üzemeltetők, akkreditáló hatóság vagy biztonságért felelős személyek számára olyan előre nem látható helyzetet is teremthet, amelyben az adatok, szolgáltatások biztonsági szintje egyértelműen nem azonosítható.

Ezeket az eseteket azért kell jelenteni, mert az akkreditált körülményekhez képest viszonyított információbiztonsági szint csökken, amit kiegészítő rendszabályokkal kell

ellensúlyozni, vagy az új feltételek között kell az üzemeltetést engedélyeznie az akkreditáló hatóságnak.

A bejelentés célja, hogy *a hatóság az új biztonsági szintet mérlegelhesse, a szükséges döntéseket meghozhassa*. A döntések egy része az üzemeltetett híradó-informatikai rendszertől független is lehet, mint gyakoribb hatósági ellenőrzés, időszak utáni adatbekérés.

A döntések másik része lehet kiegészítő védelmi rendszabály vagy korlátozások meghatározása.

Változatlan biztonsági szint, lényeges akkreditálási paraméterek változnak

Az akkreditált híradó-informatikai rendszer környezetében, vagy az üzemeltetett eszközökkel kapcsolatban olyan változások következett be, ami a hatósági eljárás során rögzített olyan lényeges akkreditálási paraméter változását jelenti úgy, hogy a kezelt adatok minősítési szintjéhez rendelt biztonsági szint nem csökken.

A híradó-informatikai rendszer lényeges akkreditálási paraméterei:

- állandó telepítésű híradó-informatikai rendszer esetében a biztonsági terület pontos helye;
- kezelt adatok minősítési szintje;
- operációs rendszer típusa;
- biztonsági üzemmód;
- TEMPEST zónabesorolás csökkenése és ehhez kapcsolódóan az eszköz TEMPEST besorolási szint változása;
- engedélyezett adatcsere formája;
- engedélyezett hálózati kapcsolat technikai paraméter és minősítési szint.

Példák az ebbe a kategóriába tartozó változásokra:

- akkreditált eszköz áthelyezése egy másik, azonos vagy magasabb adatkezelési engedéllyel rendelkező helyiségbe;
- a kezelt adatok minősítési szintjének csökkenése;
- akkreditált eszköz ideiglenes áthelyezése egy biztosítási tervben szabályozott ideiglenes biztonsági környezetbe (gyakorlat, konferencia, bemutató);
- a fizikai biztonsági paraméterek változása, mint technikai védelem élőerős védelemmel történő helyettesítése;
- biztonsági üzemmód változása.

Az ebbe a kategóriába tartozó változások nagy valószínűséggel egyszerűsített hatósági eljárással engedélyezhetők, így ezeket az eseteket nem szabad az előző kategóriához sorolni. az ügyek menedzselésére egyszerűsített eljárást kell kialakítani.

Helyi engedélyezéshez kötött változási esetek

A híradó-informatikai rendszerben, vagy az üzemeltetési környezetben beállt olyan változás, ami a minősítési szinthez rendelt biztonsági szint változását nem okozza, és nem tartalmaz lényeges akkreditálási paraméterváltozást. A változtatás oka lehet meghibásodás, vagy felhasználói igény. Példák:

- új alkalmazás telepítése vagy törlése, amely az operációs rendszer biztonsági beállításaira nincs hatással;
- engedélyezett külső kapcsolat ideiglenes megszűnése;
- a rendszer működését vagy biztonságát nem veszélyeztető ideiglenes konfigurációváltozás, mint nyomtató, monitor vagy egyéb periféria ideiglenes lekapcsolása a rendszerről;

- TEMPEST besorolást nem változtató hardvercsere a híradó-informatikai eszközön úgy, hogy az akkreditálási feltételek a hardverelem változásán kívül nem változnak, mint monitor, billentyűzet, számítógép (egyéb aktív elem), merevlemez csere;
- TEMPEST besorolást pozitívan változtató hardvercsere;
- adatkezelés ideiglenes szüneteltetése felhasználói vagy üzemeltetői okokból, mint: az adott szolgáltatásra meghatározott ideig nincs szükség, az adatkezelő helyiségben a minősített adatkezelés szüneteltetése és a szükséges eszközök ideiglenes tárolásba helyezése munkavégzéshez kötötten (meszelés, szerelés, belső építési munkák, amelyek a fizikai biztonsági rendszabályokra nincsenek hatással és a végzett műveletek felügyelete biztosított).

A helyi engedélyezés lényege, hogy az akkreditáláshoz képest történő változás nyomon követhető legyen (mi változott, ki engedélyezte, ki végezte a változtatást és milyen ellenőrzések biztosították a biztonsági szint megőrzését). Az ideiglenes használaton kívül helyezés esetében lényeges annak biztosítása, hogy *ellenőrzés történjen az inaktív időszak kezdetén és végén a nem kívánt jelenségek azonosítása érdekében.*

Ezeknél az eseteknél a helyi nyilvántartási feladatok elvégezhetők, a konfigurációk nyomon követése és a végzett műszaki feladatok rögzíthetők. Az üzemeltető szervezetnek a változtatási művelethez szükséges üzemeltetői tapasztalattal, tudással rendelkeznie kell, így ezekben az esetekben a hatóságnak nincs szüksége a biztonsági szint változásával kapcsolatos mérlegelésre.

A félreértések elkerülése érdekében ennél a résznél érdemes arra is kitérni, hogy mely esetek nem tartoznak a cikk témája szerinti változáskezeléshez. A változáskezelés körétől eltérő feladatok közé tartoznak az akkreditált híradó-informatikai rendszer működési paramétereinek változtatása, mint egyik üzemmódról történő áttérés egy másik üzemmódra (helyi vezérlés-távvezérlés, rejjtelzéssel védett rádióhálóba történő be és kilépés vagy rádióháló üzemmód változás).

Ide sorolandó a rejtjelzés körébe tartozó teszt vagy gyakorló kulcsokkal történő üzemeltetés is, amikor egy eszköz vagy hálózat üzemképességéről kell meggyőződni, vagy a kezelő állomány képzése vagy ellenőrzése történik. Ezek a változások az üzemeltető szervezet illetékes vezetőjének döntését megvalósító feladatok, melyekkel kapcsolatos adatokat az üzemeltetési dokumentumokban kell rögzíteni, de kifejezetten biztonsági szempontból a műveletek nem tekinthetők engedélyezési eljárás alá esőnek.

ÖSSZEGZÉS

A feldolgozott szakirodalomban megfogalmazottak alapján egyértelműen kijelenthető, hogy a Magyar Honvédség szervezeteinél alkalmazott híradó-informatikai rendszerek esetében kidolgozható olyan eljárásrend, melynek segítségével a változáskezeléshez szükséges hatósági ügyintézés támogatható, gyorsítható.

A normál rendű változáskezelési eljárásban megkülönböztethetők azok az esetek, amikor az akkreditáló hatóság szaktudására és engedélyére van szükség, vagy csak adminisztratív típusú ügyintézésre van szükség. Ezen esetek a hatósággal felé felterjeszthetők, a kialakult lista a hatóság által jóváhagyatható. Az így kialakított „Magyar Honvédség elektronikus minősített adatkezelésre vonatkozó változáskezelési eljárásrend” a szabályozási rendbe beilleszthető és minden rendszerre általános érvényű szakutasítás adható ki a kérdés szabályozása érdekében. Új eset megjelenése, vagy a keletkezett tapasztalatok alapján saját vagy hatósági kezdeményezésre a szabályozás nagyobb probléma nélkül továbbfejleszthető.

Az eljárásrendbe természetesen a cikkben megfogalmazott saját hatáskörben szükséges engedélyezési folyamatot is meg kell fogalmazni.

Az elektronikus minősített adatkezelő rendszereket üzemeltető honvédelmi szervezetek egy ilyen központi szabályozással a jelenleginél lényegesen könnyebb helyzetbe kerülnek. *Az adott híradó-informatikai rendszere vonatkozó biztonsági követelmények és üzemeltetés biztonsági szabályzat dokumentumokba a központi követelmény alapján rendszer-specifikusan meg kell fogalmazni a változáskezelési eseteket és már rendelkezésre is áll a szükséges szabályozó.*

Távolabbi lépésként – már a kormányzati szintű szabályozás korszerűsítésére gondolva – *a jelenlegi kormányrendelet felülvizsgálatakor a keretrendszerű követelmény pontosítható ezzel a megoldással*, így a jogszabályt alkalmazó szervezetek is élhetnek azzal a megoldással, hogy szervezeti hierarchiájuk, működési sajátosságuk figyelembe vételével kialakíthatják saját változáskezelési eljárásrendjüket.

Összefoglalásként megállapítható, hogy a bonyolult szervezeti felépítés estén is van lehetőség a változáskezelési feladatok egyszerűsítésére a folyamatok gyorsítására, melynek megoldását testre szabottan a „bevált gyakorlat" alkalmazása és egyéb szakmai forrásokra támaszkodva ki lehet dolgozni. Az engedélyezés ezek alapján már az illetékes hatóság dolga, mely témakör már kívül áll jelen cikk hatókörén.

Felhasznált irodalom

[1] Informatika. Szolgáltatásirányítás; MSZ ISO/IEC 20000-1:2007; 25. p. és 9. 2 fejezet

[2] Information technology - Security techniques - Information security management systems - Requirements; ISO/IEC 27001:2013 (E); A.12 Operations security

[3] NIST Special Publication 800-53 (Revision 4) Security and Privacy Controls for Federal Information Systems and Organizations; appendix F, p. 75.

[4] Australian Information Security Manual 2012 Controls; p. 53-54.

[5] A nemzeti fejlesztési miniszter 77/2013. (XII. 19.) NFM rendelete 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; 4. melléklet NFM rendelethez; 3. 3. 1. 3 - 3. 3. 1. 5.p.

[6] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól 34. § (1) és 43. § (1).

[7] 39/2014. (05. 30.) HM utasítás a Magyar Honvédség Informatikai Szabályzatának kiadásáról, 1. sz. melléklet, 5. 5. 4, 8. 4. 3. és 8. 4. 4. p.