Kerti András – Pándi Erik – Töreki Ákos
kerti.andras@zmne.hu – pandi.erik@zmne.hu – toreki.akos@zmne.hu

A VEZETÉSI ÉS INFORMÁCIÓS RENDSZER BIZTONSÁGA[1]

Absztrakt

Jelen közlemény a vezetési és információs rendszer egyes biztonsági kérdéseit dolgozza fel.

This publication deals with some of the questions related to the security of the Command and Information System.

Kulcsszavak: *információvédelem, VIRTAR ~ information security, VIRTAR*

BEVEZETÉS

A kormányzati és üzleti szervezetek nagymértékben az információk használatára támaszkodnak üzleti tevékenységük irányítása során. Az információ és a szolgáltatások bizalmasságának, sértetlenségének, rendelkezésre állásának, letagadhatatlanságának, számonkérhetőségének, azonosíthatóságának és megbízhatóságának elvesztése igen káros hatással van a szervezet üzleti működésére. Következésképp az információk védelme és az informatikai rendszerek biztonságának menedzselése a szervezeten belül kritikus fontosságú [1]. Az MSZ 13335-es szabványból citált idézet sehol sem olyan aktuális, mint a honvédségi rendszerekben, ahol adott esetben (konfliktusok, missziók) emberéletek és akár a küldetés sikere is múlhat az információbiztonságon.

1. AZ INFORMÁCIÓBIZTONSÁG SZAKTERÜLETEI

Az információbiztonsági feladatok szakterületekre bontásához többfajta modell létezik, amelyek közül a vizsgálatunkhoz a NATO modellt választottuk. Az információbiztonság NATO modelljét a „C-M(2002)49 Security Within The North Atlantic Treaty Organisation (NATO)" című dokumentum foglalja magába, amely a NATO-n belül a minősített információk védelmének alapdokumentuma. A NATO az információbiztonság feladatait négy fő kategóriába osztja:

- fizikai biztonság;
- személyi biztonság;
- dokumentum biztonság;
- elektronikus információbiztonság.

Az elektronikus információbiztonság feladatai további öt feladatcsoportba oszthatók, úgymint:

- számítógép és helyi hálózat (LAN) biztonság;
- hálózatok biztonságos összekapcsolása;
- rejtjelbiztonság;

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

- elektromágneses kisugárzás biztonság vagy másképpen kompromittáló kisugárzás biztonság;
- átvitelbiztonság.

A biztonsági részterületek között fontossági sorrendet, alá-fölérendeltségi viszonyt nem lehet meghatározni.

2. AZ INFORMÁCIÓBIZTONSÁGI SZAKTERÜLETEK ALAPVETŐ FELADATAI

A szakterületek nem szeparálhatók el egymástól, néhol bizonyos átfedések lehetségesek. Az elektronikus információbiztonság két legrégebbi szakterülete a rejtjelbiztonság és az átvitelbiztonság (régi szakterminológiával élve híradóbiztonság) amelyeknek akkor van szerepük, ha az információ az ellenőrzött területen kívülre kerül. Mind a rejtjelbiztonság kérdéseivel, mind a többi három biztonsági területtel (számítógép és helyi hálózat [LAN] biztonság, a hálózatok biztonságos összekapcsolása, elektromágneses kisugárzás biztonság) a szakirodalom egyre bővülő tárháza foglalkozik, azonban az átvitelbiztonság kérdésköre nagyrészt feldolgozatlan.

3. ÁTVITELBIZTONSÁG

A szakterület feldolgozatlansága alapvetően két okra vezethető vissza:

- a katonai hálózatokban az átviteli rendszerek nem csak homogén számítógépes hálózatokból állnak, mint a mai polgári architektúrák, hanem tartalmaznak a katonai innfokommunikációs hálózatokra jellemző eszközöket is (pl.: különféle rádiók), egyúttal minden rendszerelem különböző fenyegetettségekkel is szembenéz, ezért nehézkes az egységes védelmi profil kidolgozása;
- a polgári életben a legtöbb szereplő az átviteli utat megvásárolja egy szolgáltatótól (pl.: Internet kapcsolat, mobiltelefonos szolgáltatás), így e rendszerek biztonságát a szolgáltatónak kell megoldania. A gyakorlat ugyanakkor azt mutatja, hogy behatárolt azon szolgáltatóknak a száma, amelyek e kérdéskörrel foglalkozni tudnak. A békeidőszakokban a katonai rendszerekben is ilyen jellegű megoldások dominálnak, azonban fel kell készülnünk olyan helyzetekre is amikor polgári cégek szolgáltatásait, vagy előre telepített zártcélú hálózatokat nem tudunk igénybe venni.

3.1. Az átviteli út és az átvitelbiztonság meghatározása

Az átvitelbiztonság feladatainak tisztázásához meg kell határozni az átviteli út és az átvitelbiztonság fogalmát. Első megközelítésben az átviteli út a transzporthálózatot megvalósító eszközök összessége. Amennyiben feltételezzük, hogy az ellenség minden olyan összeköttetésünket értékelni és manipulálni tudja, amelyet nem tartunk folyamatosan a felügyeletünk alatt akkor azt az összeköttetést is ide kell sorolni, ami ugyan a belső hálózat kapcsolatait valósítják meg, de az általunk ellenőrzött teret elhagyják, illetőleg elhagyhatják. Ennek tükrében az átviteli út fogalma nem más, mint: *Mindazon hír, adat és információ továbbító csatornák (továbbiakban összeköttetések), jellegüktől és felépítésüktől, összetételüktől és hosszúságuktól függetlenül, amelyek a szerepüket úgy töltik be, hogy közben az általunk ellenőrzött területet határain kívülre kerülnek vagy kerülhetnek.*

Adaptálva az információbiztonság elveit, az átviteli út biztonság, vagy másképpen az átvitel biztonság alapvető feladata: *Az információk rendelkezésre állásának, sértetlenségének, és bizalmasságának megőrzése az átviteli út folyamán, valamint az átviteli utat megvalósító eszközök rendelkezésre állásának, sértetlenségének biztosítása.*

3.2. Az átvitelbiztonság feladatainak és folyamatainak meghatározása

Véleményünk szerint egyrészről az átvitelbiztonság feladatainak és folyamatainak meghatározáshoz a kockázatkezelés végrehajtása a legjobb módszer. Másrészről a biztonsági ellenintézkedések minden esetben valamiféle gátak az információáramlás útjában, másrészt erőforrásokat emésztenek fel, éppen ezért a biztonsági ellenintézkedéseket gondosan, minden esetben az adott helyzetnek megfelelően, költséghatékonyan kell kivitelezni. Ennek végrehajtásához célszerű elkészíteni a vezetési és információs rendszer technikai alrendszerének (VIRTAR) kockázatelemzését és kockázat menedzsmentjét.

Az információs rendszerek kockázatkezelése az információbiztonság jelenleg egyik legjobban fejlődő részterülete, amely jelenleg nem mutat egységes képet a különböző szervezetek módszereiben. Az ISO és az IEC45 2008 júniusában kiadta a 27005-ös szabványát és ezzel egyrészt korszerűsítette a kockázatkezelés szemléletmódját, másrészt a 13335-ös szabványcsalád első négy tagját hatálytalanította. Ez a korszerűsítési folyamat még nem fejeződött be az összes információbiztonsággal foglalkozó szervezetnél. Erre jó példa lehet a 2008 júniusában megjelent Közigazgatási Informatikai Bizottság 25. számú ajánlása, amely még a 13335-ös szabványcsalád szerinti kockázatkezelést alkalmazza, valamint az ENISA, amely diplomatikusan nem tesz különbséget a különböző kockázatkezelési módszerek között, viszont a honlapján lehetőséget nyújt ezek összehasonlítására.

A Magyar Honvédség hivatalos információbiztonsági politikája e témakörben rögzíti, hogy a kockázatelemzést

- minősített adatokat kezelő rendszer, több szervezet által közösen használt vagy üzemeltetett rendszer, MH-szintű rendszer esetében kötelezően;
- egyéb adatkezelő rendszerek esetében a NATO, EU, nemzeti elektronikus adatkezelésre feljogosított rendszerek felügyeletét ellátó hatóság, illetve az információvédelem szakmai felügyeletét ellátó honvédelmi szerv döntése szerint kell végrehajtani [2].

Fentiek alapján a kockázatkezelési folyamatot az átviteli utak tekintetében végre kell hajtani, mivel kezelt adatok minősítési szintjétől függetlenül az átviteli utakat több szervezet használja (elöljáró-alárendelt). A kockázatkezelés azonban csak akkor lehet eredményes, ha ez nem egyszeri, hanem periodikus folyamat. Ezért a kockázatelemzés eredményeit időről időre felül kell vizsgálni és ha új kockázati tényező megjelenését tapasztaljuk újra kell tervezni az ellenintézkedéseket, illetve az egész kockázatkezelési folyamatot az új adatokkal meg kell ismételni.

Szintén az eredményességet javíthatja, ha a kockázatokkal kapcsolatos információkat megosztjuk a kockázatkezelést végző szervezetekkel, illetőleg ezeket a megosztott információkat felhasználjuk a kockázat menedzsmentben. A szabvány által bemutatott folyamat azonban olyan, mintha a végrehajtott folyamat egyszeri cselekvés lenne, azonban a kockázatkezelés (vagy kockázatmenedzsment) nem egy egyszeri cselekmény, hanem egy folyamat, amelyet az információ feldolgozó rendszer és így az átviteli teljes életciklusa alatt folyamatosan végre kell hajtani.

Véleményünk szerint az átvitelbiztonsági kockázatok értékelésekor, vagyis az átvitelbiztonság meghatározásához a legfontosabb feladat a hatókör meghatározása. Az ISO/IEC 27005 szabvány megítélésünk szerint erre nem ad elegendő fogódzót, ezért célszerűnek tartjuk a két szabvány munkafolyamatainak kombinációját alkalmazni.

A kockázatfelmérés folyamatában a különböző folyamatok még további cselekvésekre bonthatók. Annak érdekében, hogy a kockázatokat teljes mértékben azonosítani tudjuk a következő részfeladatokat kell végrehajtani:

- a vagyontárgyak azonosítása, amelyek közé a fizikai vagyontárgyakat, az információkat, a folyamatokat és a személyzetet sorolja a szabvány;
- fel kell mérni a valószínű fenyegetéseket, amelyek minden egyes esetben mások és mások lehetnek, de ha azonosak, akkor is hangsúlyuk különbözők;
- be kell azonosítani a már létező ellentevékenységeket és azonosítani kell a sebezhetőségeket, amelyeket a fenyegetések ki tudnak használni.

Amennyiben mindezeket a folyamatokat sikerült végrehajtanunk, akkor azonosítani tudjuk a kockázatok következményeit. A kockázatok becslésénél figyelembe kell venni és ki kell értékelni az azonosított következmények hatásait a vizsgált rendszerre, illetőleg figyelembe kell venni az azonosított és kiértékelt következmények előfordulásának valószínűségét. A két eredményből megkapjuk a kockázatok szintjét.

A kiértékelésekor a kockázatok szintjének figyelembevételével egy olyan sorba rendezett listát kapunk, amely megmutatja, hogy melyek azok a kockázatok, amiket el tudunk fogadni és melyek azok, amelyek ellen új ellenintézkedést kell bevezetnünk. Az ellenintézkedések megválasztása után meg kell vizsgálni, hogy a fennmaradó maradványkockázatok elérik-e az elfogadható szintet, avagy sem. Természetesen abban az esetben, amikor nem érik el ezt a szintet akkor új ellenintézkedéseket kell bevezetni.

3.3 A kockázatkezelés végrehajtása az átviteli út biztonsága tekintetében

Az átviteli út kockázatelemzése csak abban különbözik az egyéb kockázatelemzésektől, hogy más hangsúlyt kapnak a sebezhetőségek és fenyegetések. Ezen megállapítás kifejezetten igaz akkor, amennyiben egy missziós vagy egy harci feladatot hajt végre az adott katonai szervezet, ezért a továbbiakban erre az eshetőségre koncentrálva végezzük el a vizsgálatokat.

3.3.1. Az átvitelbiztonság hatókörének meghatározása

3.3.1.1 A szervezeti információbiztonság politika áttekintése

A jelenleg is érvényben levő MH információbiztonsági politika az átviteli út biztonságról a következőket fogalmazza meg: *„Az elektronikus adatkezelő rendszerekben alkalmazott átviteli eljárásokat és biztonsági mechanizmusokat a kezelt adatok bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó követelmények szerint kell kialakítani.”* [3]. Ebből az idézetből azonban nem derül ki, hogy melyek ezek a követelmények, illetőleg az sem, hogy a jogalkotó az átviteli útbiztonsággal, illetve az átviteli protokollokkal kívánt-e foglalkozni. Ezek alapján fontos kérdésként merül fel, hogy mi lehet az információbiztonság feladata az átviteli út vonatkozásában.

Első megközelítésben a C-M(2002)49-ből már citált idézet alapján első feladat az információk és a rendszer bizalmasságának, sértetlenségének, rendelkezésre állásának biztosítása. Véleményünk szerint bizonyos esetekben sokkal fontosabb, hogy a vezetés folytonosságát biztosítsuk.

Összefoglalva az információbiztonsági politika átviteli út biztonságával foglakozó részben le kell szögezni, hogy az információvédelmi rendszabályoknak az átviteli út során biztosítaniuk kell a vezetés folytonosságát, amennyiben szükséges a rejtett vezetést, miközben megőrzik az információk és a rendszer sértetlenségét, bizalmasságát, és rendelkezésre állását.

3.3.1.2 A hálózati architektúrák és alkalmazások áttekintése

Véleményünk szerint ahhoz, hogy a VIRTAR felépítését vizsgálni tudjuk célszerű áttekinteni a Magyar Honvédség által végrehajtott missziók információs kapcsolatait [4]. A missziót végrehajtó alakulatnak összeköttetésben kell lennie:

- az elöljáró szervezet törzsével, ahonnan gyakorlatilag a feladat végrehajtásához szükséges intézkedéseket, és egyéb információkat kapja;
- a hazai területen települt katonai vezető szervezettel, ami jelenleg a missziók esetében a Magyar Honvédség Műveleti Központ;
- azokkal az alárendelt csapatokkal, szervezetekkel, amelyek a feladataikat nem a szervezet települési helyén hajtják végre. Ilyenek lehetnek például a különböző járőrök, illetve az iraki misszió idején a konvoj kisérések.

Természetesen a szervezetnek kapcsolatot kell fenntartania a szomszédos egységekkel, alegységekkel, illetőleg a támogató szervezetekkel. Ezek lehetnek más nemzeti szervezetek, szövetséges csapatok és ebbe a kategóriába kell sorolnunk a nem katonai szervezeteket is, amelyek ugyanabban a misszióban tevékenykednek.

A misszió sikere érdekében a missziós csapatoknak el kell fogadtatni a misszió célját a helyi lakossággal, ezért mindenképpen összeköttetésben kell állniuk a helyi közigazgatási, illetve más civil szervezetekkel és helyi vezetőkkel [5].

Modern korunkban egy misszió sikere elképzelhetetlen a hazai közvélemény támogatása nélkül, ahhoz, hogy ezt a támogatást elnyerjük mindenképpen gondoskodnunk kell a misszióban szolgálatot teljesítő katonák hazai kapcsolattartási lehetőségeiről. Ez a feladat mind szervezési mind biztonsági szempontból nagy kockázatokat rejt, ezért fokozott gondossággal kell azt tervezni.

3.3.1.3 A hálózati kapcsolat típusainak azonosítása

A 13335-ös szabvány több kapcsolati típust felsorol, amelyek közül az átviteli út szempontjából figyelembe véve a kérdéskört az alábbi kapcsolati típusok lehetségesek [6]:

- Kapcsolódás egy szervezet földrajzilag elkülönülő részei között, pl.: a parancsnoki (helyi és nemzeti) kapcsolatok;
- A szervezet telephelyei közti kapcsolatok és a távmunkát végző személyek kapcsolódásai, pl.: az alárendeltekkel történő kapcsolattartás;
- Kapcsolódás más szervezetekkel, pl.: a helyi közigazgatási szervek, támogatók, együttműködőkkel történő kommunikációs csatornák;
- Kapcsolódás nyilvános környezetekkel pl.: a katonák kapcsolattartása a családjukkal.

3.3.1.4 A hálózati jellemzők, bizalmi kapcsolatok áttekintése

A VIRTAR-t elsősorban a hálózatok megvalósulása alapján célszerű csoportosítani. Ezek alapján kétféle hálózattípust lehet megkülönböztetni:

- a saját erőink által létesített hálózatok;
- szolgáltatótól bérelt hálózatok.

A szolgáltatótól bérelt hálózatokhoz soroljuk a szövetséges csapatok által számunkra rendelkezésre bocsátott hálózatokat is. Ezen hálózatoknak az átviteli út biztonság szempontjából problémája, hogy a biztonsági tulajdonságait nem tudjuk megváltoztatni, azokat csak megrendelni és értékelni tudjuk. Természetesen más biztonsági osztályba sorolhatjuk és másképpen értékelhetjük a hálózatokat, amennyiben egy NATO szövetséges vagy NATO által biztosított, másképpen, ha egy polgári szolgáltatótól bérelt hálózatról van szó. Az első esetben a NATO biztonságpolitikájában leírtak szerint csak annyit kell tudnunk, hogy az engedélyező és jóváhagyó hatóság megfelelőnek találata-e hálózatot, illetve a 3.3. alfejezetben említett kivételről van-e szó.

A második esetben a biztonsági értékelés nehezebb, de lehetséges. Tudnunk kell a szolgáltatóról hogyan kezeli a biztonságot, megfelel-e a különböző szabványoknak, netalán egy nemzetközi szabvány szerint auditált hálózatról van-e szó. Amennyiben lehetőségünk van választani a szolgáltatók közül azt a szolgáltatót kell választani, amelyik nagyobb garanciát nyújt az információbiztonság területén. A szolgáltatók és a szolgáltatások összehasonlításához szintén segítséget nyújthatnak a nemzetközi szabványok, mint például az MSZ ISO/IEC 15408 szabványcsalád.

A saját szakcsapataink által megvalósított átviteli utak felosztása a biztonsági kockázataik szerint követi a technikai megvalósítási struktúrát, amely alapján megkülönböztethetünk vezetékes és vezeték nélküli, illetve vegyes kivitelezésűeket [7]. A szabvány a bizalmi kapcsolatok között a különböző szintű csoportok közötti kapcsolatokat érti és így az alábbi hálózatokat különbözteti meg:

- hálózat ismeretlen felhasználói csoportokkal;
- hálózat ismert, kizárólag a szervezeten belüli felhasználói csoporttal;
- hálózat ismert, zárt üzleti csoporton (több szervezeten) belüli felhasználói csoportokkal.

Véleményünk szerint a katonai rendszerek átviteli út biztonságának szempontjából itt a különböző fontosságú kapcsolatokat kell beazonosítani, ennek okán elsősorban a vezetésfolytonosság biztosításában játszott szerepük szerint kell priorizálni az átviteli utakat.

3.3.2. Az átviteli út kockázatainak felmérése

A felmérés során az alábbi szakterületeken célszerű vizsgálódásokat lefolytatni a kitűzött cél eredményes elérése érdekében:

- vagyontárgyak azonosítása;
- fenyegetések azonosítása;
- sebezhetőségek azonosítása;
- létező ellentevékenységek felmérése;
- a kockázat bekövetkezési következményeinek azonosítása;
- a kockázatok becslése;
- a kockázatok kiértékelése.

3.3.3. Kockázatjavítás

A kockázatjavítás során dönthetjük el, hogy milyen ellenintézkedéseket tegyünk a kockázatok lehetséges következményeinek csökkentésére. Az ellenintézkedések lehetnek olyanok, amelyekkel teljesen elkerüljük a kockázatokat, illetőleg csökkentjük az események bekövetkezésének hatását vagy elkerüljük a kockázat előfordulását, valamint olyanok, amelyekkel a kockázatok negatív következményeit áthárítjuk egy másik félre [8]. Azt, hogy melyik ellentevékenységeket fogjuk alkalmazni az adott körülmények fogják eldönteni.

A kockázatjavítás során ki kell dolgozni azokat az ellenintézkedéseket, amelyeknek az értéke a kockázatok kiértékelésekor az elfogadható szint fölé került. Ezek az ellenintézkedések lehetnek technikai megvalósításúak és szervezésiek, valamint a kettő kombinációi.

Annak eldöntése, hogy milyen ellenintézkedéseket vezetünk be, függ attól, hogy milyen erőforrásaink vannak és milyen szinten kívánjuk megvalósítani az átvitel biztonságot.

3.3.4. Kockázatelfogadás

A kockázatok elfogadásának alapvetően két fajtája létezik. Az egyik esetében a kockázatelemzés folyamataként feltárt, kiértékelt és az ellenintézkedések érvénybe léptetésével olyan szintre csökkentettük a kockázatokat, amelyek már további intézkedést nem igényelnek, vagyis az elfogadható szint alá kerültek.

A második esetben a kockázatok létezésének tudatában vagyunk, de valamilyen okból nem tudatosan marad el intézkedünk a kockázat megszüntetésére.

Mindkét esetben azonban a kulcs szó a tudatosság, vagyis nem felelőtlenül abban bízunk, hogy a nem várt esemény nem következik be, hanem tudatában vagyunk a cselekedetünk teljes súlyával.

3.4. Incidenskezelés és vezetésfolytonosság tervezés

A végrehajtott, megfelelő szintű kockázatjavítás után a kockázatok csak a legritkább esetben szűnnek meg teljesen. A biztonsági állapot sehol nem annyira változékony, mint egy katonai feladat végrehajtása során, ezért a biztonsági környezetet folyamatosan figyelemmel kell kísérni. A biztonságban bekövetkezett negatív események hatásuk nagyságtól függően lehetnek:

- biztonsági események;
- biztonsági incidensek.

A katonai műveletek legnagyobb súlyú biztonsági incidense a vezetés megszakadása. A vezetés megszakadásának legvalószínűtlenebb forgatókönyve az egyszerre, hirtelen bekövetkező események hatása. Sokkal elképzelhetőbb, hogy több, akár egymástól független incidens sorozat eredményeként jutunk el a vezetés teljes hiányához. Ebből az okfejtésből is látszik, hogy nagy hangsúlyt kell fektetni a VIRTAR információbiztonsági incidenskezelésére.

Az átviteli út incidensei közé kell sorolni minden, az ellenséges tevékenységre utaló cselekményt, úgymint:

- berendezések támadása, rongálása;
- rádióforgalom zavarása, lefogása.

Szintén ebbe a kategóriába soroljuk azokat az eseményeket, amelyek az átviteli utak sávszélességének jelentős csökkenését okozzák az okok eredetétől (természeti hatások, ellenséges támadások, saját csapatok tevékenysége, stb.) függetlenül.

3.4.1. Az incidenskezelési terv

Az incidensek kezelése lehet ad-hoc jellegű, amikor a szakembereink meglévő szaktudására támaszkodunk, azonban célravezetőbb, ha elkészítünk egy incidenskezelési tervet. Természetesen minden eshetőséget nem tudunk feldolgozni, mivel előfordulhatnak váratlan,

eddig még nem tapasztalt események és incidensek, azonban egy meglévő terv sokat segíthet egy „éles” helyzetben.

Adaptálva az MSZ ISO/IEC TR 18044 szabvány 7. fejezetét véleményünk szerint az információbiztonsági incidenskezelési tervnek az átviteli út vonatkozásában az alábbiakat kell tartalmaznia:

- áttekintés az információbiztonsági esemény észleléséről, bejelentéséről, a lényeges információk összegyűjtéséről, valamint arról, hogy hogyan használják fel ezt az információt az információbiztonsági incidensek meghatározására. Az áttekintésnek tartalmaznia kell az információbiztonsági események lehetséges típusainak összefoglalását, azok bejelentési módját, azt hogy mit jelentsenek, hol és kinek és tartalmaznia kell azt is hogyan kezeljék az információbiztonsági események teljesen új típusait;
- az információbiztonsági incidensek bejelentésének folyamatát (ki a felelős, mi a teendő az esemény észlelésekor, bejelentésekor);
- egy információbiztonsági esemény információbiztonsági incidenssé történő átminősítését követően végrehajtott tevékenységek összefoglalása. Ennek tartalmaznia kell a következőket:
  - az azonnali megteendő intézkedések;
  - az incidens forrásának azonosítása;
  - mikor, milyen esetekben kell azonnal jelenteni az incidenseket a törzsfőnöknek vagy a parancsnoknak;
  - a másodlagosan megteendő intézkedések;
  - a felelősségek rögzítése;
  - az incidenskezelési tevékenység naplózási követelményei a későbbi elemzések számára, illetőleg az elektronikus bizonyítékok biztos megőrzésének biztosítása folyamatos megfigyeléssel;
  - az információbiztonsági incidenseket követő és megoldásukat szolgáló tevékenységek, beleértve a tanulságok levonását, valamint az eljárások megjavítását is;
  - az átviteli út rendszerdokumentációjának (beleértve az eljárásokat is) tárolási helye;
  - az információbiztonsági incidenskezelés oktatásának és képzésének feladatai.

3.4.2. A vezetésfolytonosság

A vezetés folytonosságának fenntartása a vezetés egységének egyik alapvető feltétele, így a sikeres tevékenység alapja. Az erők alkalmazásának időszakában a vezetés megszűnése a kitűzött célok elérésének meghiúsulását okozhatja. A parancsnok a műveletek teljes időszakára köteles megszervezni a helyettesítését, a vezetés átvételének rendjét. A vezetés folytonosságának fenntartása érdekében a feladatokat az alárendeltek részére úgy kell meghatározni, hogy az összeköttetés megszakadása esetén is garantálja a kitűzött célok teljesítését [9].

A legjobban megvalósított információbiztonsági ellenintézkedések, a legkiválóbban végzett információbiztonsági incidenskezelés ellenére is bekövetkezhet, hogy a vezető szervek valamilyen objektív oknál fogva nem tudják irányítani, vezetni az alárendeltjeiket. A vezetés megszakadása nem minden esetben csak a VIRTAR-ban bekövetkezett nem kívánt események következménye lehet, hanem más jellegű is, például a vezető szervek vezetésre képtelenné válása a vezetési pont megsemmisítése, vagy a vezetői állomány fogságba esése következtében. Ennél fogva a vezetésfolytonosság nem elsősorban a VIRTAR-t üzemeltető állomány feladata.

Gyakorlatilag az Összhaderőnemi Doktrínával megegyező az előzőekben már hivatkozott MSZ ISO/IEC TR 18044 szabvány meghatározásai is. A doktrínából az is következik, hogy az infokommunikációs összeköttetések teljes megszakadása sem feltétlenül jelenti egy katonai feladat kudarcát, ennek ellenére a VIRTAR üzemeltető állománynak mindent meg kell tennie azért, hogy a kor színvonalán álló, megfelelő sávszélességű csatornákat biztosítson a vezetés számára [10]. Áttekintve az átviteli utat biztosító személyzet feladatát, elmondható, hogy a szolgálati személyeknek:

- ismerni kell az általános helyzetet, miután ez nagymértékben kihat az összekötetések szervezésére;
- tisztában kell lenni, hogy ki, mikor, kit vezet, mert ez meghatározza az adott helyzet prioritásait;
- tisztában kell lenni, hogy az adott helyzetben milyen az infokommunikációs hálózat, milyen kerülő utakat tud elérni;
- tudni kell, hogyan lehet adott esetben a hírrendszerben átcsoportosításokat végrehajtani a kevésbé fontos csatornáktól a fontosabbak felé és természetesen tudni kell felállítani egy fontossági sorrendet az átvinni kívánt információk között;
- tisztában kell lenni, hogy melyek azok a minimális kommunikációs szolgáltatások, amelyek még biztosítják a vezetésfolytonosság infokommunkációs feltételeit.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Jelen közleményünkben megvizsgáltuk a VIRTAR információbiztonságának alapvető kérdéseit. Az információ és a szolgáltatások bizalmasságának, sértetlenségének, rendelkezésre állásának, letagadhatatlanságának, számonkérhetőségének, azonosíthatóságának és megbízhatóságának elvesztése igen káros hatással van a szervezet üzleti működésére. Következésképp az információk védelme és az informatikai rendszerek biztonságának menedzselése a honvédségi rendszerekben, ahol adott esetben (konfliktusok, missziók) emberéletek és akár a küldetés sikere is múlhat az információbiztonságon, kritikus fontosságú.

Az anyagban foglaltakat mérlegelve az alábbi következtetéseket vonjuk le:

- A VIRTAR-hoz kapcsolódó biztonsági területek kidolgozottsági foka az átvitelbiztonság részterületén tekinthető a legalacsonyabbnak;
- Az átviteli út biztonság feladatrendszerét a nemzetközi szabványok adaptálása révén célszerű meghatározni;
- A VIRTAR biztonságának fokozása érdekében incidenskezelési és vezetésfolytonossági tervet szükséges kimunkálni.

FELHASZNÁLT IRODALOM:

[1] MSZ ISO/IEC TR 13335-5 Informatika. Az informatikai biztonság menedzselésének

[2] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 16 § (4) bekezdés

[3] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 22 §

[4] Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben I. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 110-121. oldal)

[5] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal)

[6] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal)

[7] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal)

[8] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919)

[9] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919)

[10] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05-06.)