Király László – Pataki János

EGY MULTINACIONÁLIS NAGYVÁLLALAT KRITIKUS INFRASTRUKTÚRÁJÁNAK ILLESZKEDÉSE A HAZAI (VERTIKÁLIS ÉS HORIZONTÁLIS) KRITIKUS INFRASTRUKTÚRÁKHOZ

Rezümé:
Egy multinacionális nagyvállalatnál, amelynek exportvezérelt termelése az ország GDP-jének is meghatározó eleme, különösen fontos a termelési folyamatok biztonsága. Egy új termelőegység indítása során, már a tervezés első fázisától kezdve fontos szempont a biztonsági feltételrendszer kidolgozása. Ennek során összhangba kell hozni a külső szabályozókban általánosan megfogalmazott biztonsági követelményeket az adott beruházás költségkeretein belül megvalósítható „szükséges" biztonsággal. Ez egy optimum kereső folyamat, ahol a biztonság olyan közös érték, amely a külső és belső partnerek számára egyaránt fontos.

Kulcsszavak:
biztonság, beruházás, kritikus infrastruktúra, multinacionális nagyvállalat

László Király – János Pataki

A MULTINATIONAL COMPANY'S CRITICAL INFRASTRUCTURE'S CONNECTION WITH DOMESTIC CRITICAL INFRASTRUCTURE IN BOTH VERTICAL AND HORIZONTAL MANNERS

Abstract:
The production processes security is a priority feature for a multinational company that's export output volume plays a decisive role for the country's GDP. Security aspects must be considered from the beginning of the planning phase of a new production unit. The system of security has to be worked out and the conditions specified by the outer rules and regulations and the „necessary security" developed ont he basis of the investment's budget frames should be conciliated as mich as possible. This is always an optimum-seeking process where security is a common value for both of their external and internal partners.

Key words:
security, investment, critical infrastructure, multinational company

A fenti nagyvállalat kiemelt hangsúlyt fektet a biztonságon felül a termelési folyamatok folytonosságára is, amelynek exportvezérelt termelése az ország GDP-jének is meghatározó eleme. Ezt a cikkben tárgyalandó számos alrendszer szolgálja ki, amelyek a külső és belső szabályozás szempontjából külön-külön kritikus infrastruktúrát képeznek. Egy új termelőegység indítása során, már a tervezés első fázisától kezdve fontos szempont a biztonsági feltételrendszer kidolgozása. Ennek során összhangba kell hozni a külső szabályozókban általánosan és elvontan megfogalmazott, és ezáltal maximumra törekvő biztonsági követelményeket az adott beruházás költségkeretein belül megvalósítható „szükséges" biztonsággal (a biztonsági beruházás költségeinek meg kell térülni a piac által elismert termékárban). Ez egy szükségszerűen hosszú, optimum kereső folyamat, melynek során érdekeket kell egyeztetni, hiszen a biztonság olyan közös érték, ami a külső és belső partnerek számára egyaránt fontos.

A cikkünk elkészítésének célja, hogy a különböző „biztonsági szervezetek és hatóságok" egyformán értelmezzék a részükre meghatározott biztonsági és védelmi

feladatokat és azok kapcsolódási pontjait, valamint a kritikus infrastruktúrák létesítéséhez és működtetéséhez szükséges új biztonságtechnikai és taktikai elemek alkalmazását. Írásunk első részében röviden ismertetjük a Magyarországon kialakult biztonsági irányzatokat és a jogszabályi hátteret; a második részben a vállalati szinten működtetett biztonsági szervezetek általános feladatait; a harmadik részben egy új termelőegység beruházása során figyelembevett és megvalósuló biztonsági, a termelés folytonossága szempontjából kritikus infrastruktúrának számító elemek költségtényezőit/arányait.

ÁLLAMI/IGAZGATÁSI SZINT, JOGSZABÁLYI HÁTTÉR

A gazdaságbiztonsági szempontból kulcsfontosságú infrastruktúrák védelmének megvalósításában az állam partneri együttműködést törekszik kialakítani az infrastruktúra-tulajdonosokkal. Ez a védelmi ráfordításoknak a felelősség és a kockázatviselés arányának megfelelő megosztását jelenti. Az állam és a magánszféra partneri együttműködésén alapuló hazai program kezdetben önköltségi alapú vállalati finanszírozást, majd ezt követően fokozatosan elérendő meghatározott mértékű állami szerepvállalást igényel.

A magyarországi állapotokra jellemző, hogy az igazgatási, jogszabály-előkészítési és végrehajtási, valamint a vállalati alkalmazói szinten eltérő a szakmai felfogás, és nincs teljes körű egyetértés. Ez értelemszerűen adódik abból, hogy minden résztvevő a saját szempontjai szerint kíván optimalizálni a végrehajtás folyamatában. Az igazgatási szint jóval szélesebb kör, régió, országok és a lakosság szempontjait érvényesíti. A vállalati végrehajtás szűkebb érdek, a termelés biztonságára, az üzletmenet folytonosságára és a gazdaságossági szempontokra van figyelemmel. Ez természetesen visszahat a kritikus infrastruktúrák aktuális védelmi állapotára, esetenkénti hiányosságaikra.

A biztonság komplex fogalma és a kritikus infrastruktúra meghatározása

A mezopotámiai öntözőrendszerektől, a Római Birodalom hadiútjain át, Vásárhelyi Pál Tisza-szabályozásáig minden kornak és országnak megvolt a sajátos kritikus infrastruktúrája. Újabb kori példaként kell megemlíteni a 2000-ben végrehajtott dátumváltást megelőzően létrehozott Y2K nemzetközi és hazai ad hoc szervezetet, amely közigazgatási és iparági szakemberek együttműködésével készített az üzemviteli folytonosságot biztosító ún. kontingencia terveket az energetikai, távközlési és számos lakossági szolgáltatási rendszerben (kereskedelem, bank) elméletileg feltételezett, de szerencsére be nem következett zavarok kivédésére.

A modern társadalmak nagymértékben függenek a technikai és virtuális infrastruktúra rendszerektől (energiaellátás, ivóvíz ellátás, informatikai hálózatok stb.), amelyek komplex rendszerét is egymástól való függőségek jellemzik. E rendszerek működési zavarai, illetve egyes elemeinek ideiglenes kiesése, vagy megsemmisülése jelentős kihatással vannak mindennapi életünkre, a gazdaság és a kormányzat hatékony működésére.

A biztonságot legáltalánosabban – negatív definícióval – a veszély, a veszélyeztetettség hiányával szokták meghatározni. További lehetséges meghatározások:

- A biztonság a veszély hiánya.
- A biztonság az egyes emberek vagy csoportjaik, az államok és államcsoportok bizonyossága arról, hogy a lehetséges veszélyektől védve vannak.
- A biztonság olyan állapot, amelyben az egyéneket, csoportokat és az államokat komoly veszélyek nem fenyegetik, illetve azoktól védettnek érzik magukat, vagy – pozitívan kifejezve – amelyben biztosak abban, hogy jövőjüket saját elképzeléseik szerint alakíthatják.

A biztonság egyénekhez (egyes emberekhez), emberi közösségekhez (csoportokhoz), államokhoz (nemzetekhez), nemzetközi rendszerekhez köthető kategória, amely mindig valamilyen értékek ellen irányuló fenyegetés, veszély vagy kockázat megjelenése kapcsán felmerülő igényben fejeződik ki. A gazdasági és társadalmi fejlődés során, az urbanizáció előrehaladásával kialakuló, ember alkotta egymáshoz kapcsolódó infrastruktúrák kölcsönös függőségét (legyen az közvetlen vagy közvetett interdependencia) és kockázataikat elemző célzott alapkutatásnak kell feloldani az ismerethiányt és az abból fakadó szabályozatlanságot. Ez azt eredményezi, hogy a védekezés csak követi az egyre növekvő kockázatot.

Nemzeti és nemzetközi szinten a kutatás a komplex megoldások keresése, az univerzális szabályozás irányába mutat, amit jelenleg az eltérő fogalom és célmeghatározásból adódó definíciós problémák, a különböző pénzügyi lehetőségek nehezítenek, illetve akadályoznak. Így ma még messze nem beszélhetünk a *kritikus infrastruktúra* (KI), a *kritikus infrastruktúra védelme* (KIV) nemzetközileg elfogadott, egyenszilárdságú és koherens definíciójáról. Abban viszont egyetértés mutatkozik, hogy az energetikában; infokommunikációs technikában; a szállítás/elosztás területén; a víz- és élelmiszer ellátásban; és nem utolsó sorban, a banki-pénzügyi szférában olyan kölcsönösen összefüggő globális rendszereket (KI) alkotnak, amelyek legfontosabb tulajdonsága a hálózatalapúság. (1)

Az állam, a gazdaság szereplői, valamint a lakosság részéről elvárás, hogy ezen alapvető létfontosságú, vagy kritikus infrastruktúrák lehető legnagyobb biztonsággal működjenek. A kritikus infrastruktúra elemeinek terrorcselekményekkel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid, kivételes és kezelhető legyen. Kritikus infrastruktúra védelem a kritikus infrastruktúra elem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység.

A létfontosságú infrastruktúrákat kár érheti, működésükben zavar keletkezhet vagy azok meg is semmisülhetnek terrorcselekmény, természeti katasztrófa, hanyagság, baleset, számítógépes hackertevékenység, bűncselekmény vagy rosszhiszemű magatartás következtében. Az infrastruktúrák biztonságának növelése ezért elsőrendű kérdéssé vált a fejlett országok biztonságpolitikájában. A cikk véglegesítésének idején jelent meg a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. A törvény a legmagasabb szinten szabályozza azokat a feladatokat, amelyeket a hatóságoknak, az üzemeltetőknek és a tulajdonosoknak kell elvégezni a jogszabály alapján kijelölt infrastruktúra elemek védelme érdekében. Nem tekintjük feladatunknak a törvény

részletes ismertetését és kommentálását, de egy termelő vállalat szempontjából igen fontosnak tartjuk a horizontális és ágazati kritériumok megállapítását, mivel azok jelentik mindazon hálózati elemeket, amelyek a folytonos működés szempontjából meghatározóak.

Gazdaságbiztonsági szempontból kritikus infrastruktúra elem a gazdaság folyamatos működéséhez elengedhetetlen ágazatok (az energetika, a közlekedés, az informatika, a pénzügy), valamelyikébe tartozó eszköz, létesítmény, rendszer vagy ezek része, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, a gazdasági és szociális jóléthez, valamint amelynek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. A gazdaságbiztonsági szempontból kiemelten fontos ágazatok – az energetikai, a közlekedési, az informatikai, az ipari, a vízügyi, a pénzügyi ágazatok – működésének belső biztonsági szabályait ágazati törvények határozzák meg. A különleges jogrend időszakában bevezethető speciális védelmi intézkedések kidolgozása a rendkívüli intézkedések tervezése keretében történik.

A közszolgáltatások – válsághelyzetben is biztosítandó – még elégséges szintjét az ágazati törvények vagy azok felhatalmazásával készülő egyéb jogszabályok határozzák meg. A különleges jogrend időszakára kidolgozott rendkívüli intézkedések további korlátozásokat írhatnak elő, amit törvényi felhatalmazás alapján a Kormány a horizontális és az ágazati kritériumokról szóló rendeletében határoz meg.

Az infrastruktúrák biztonságnövelésének fő területei, az egyének, közösségek védelmének és a kritikus infrastruktúrák biztonságának magasabb szintre emelése. Mindhárom területen a veszélyek és fenyegetettségek fizikai, informatikai eredetűek vagy a rendszerek komplexitásból adódnak. A megoldást az új fenyegetettségek és kockázatok fizikai, informatikai és pszichológiai szintű okainak felderítése, összefüggéseik megértése és kezelése jelenti. Az EU és a hazai dokumentumok a KIV céljai az 1. ábrán láthatóak.

A KIV céljai

- Szolgáltatás folyamatosság – állami, gazdasági, lakossági funkciók és folyamatok működése.
- Biztonságos, ellenálló infrastruktúra.
- Változó veszély – kockázatos tervezés és reagálás.
- Új típusú biztonsági együttműködés.

1. ábra
A KIV céljai*

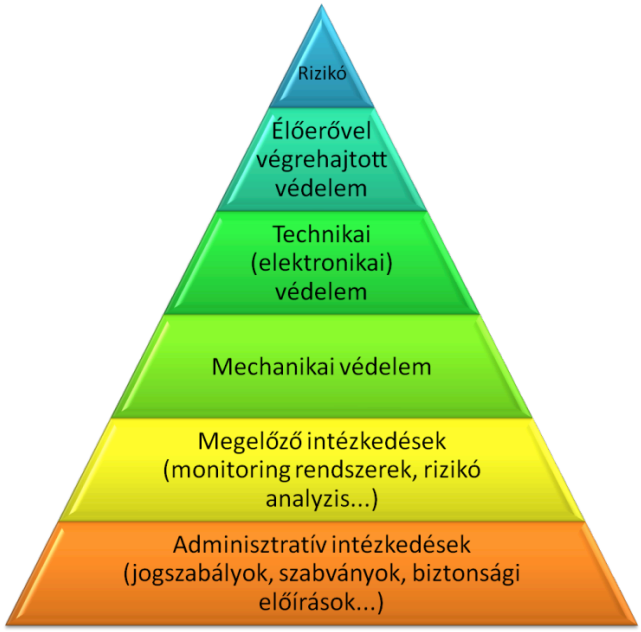
* Forrás: Király László−Medveczky Mihály: Védelemgazdasági ismeretek önkormányzati (védelmi igazgatási) válság menedzsereknek. Budapest, 2009. ZMNE. ISBN 978-963-7060-75-5. 61. oldal

A KIV-célok megvalósítására több irányítási modell létezik. Ilyenek például:

- A legfejlettebb a CIIP-modell, azaz a kritikus információs infrastruktúrák védelmének megszervezése, amely egy központi felelős koordinálása mellett több kormányzati szervre és a magánszférára is kiterjed (USA, UK, Hollandia, Németország, Kanada, Korea).
- Az „All Hazards” (összes veszély) modellben a felelős miniszter elsődleges irányításával az infrastruktúrák (a stratégiai szervezetek irányítása a fizikai

védelem és az ICT-biztonság, a polgári védelem, katasztrófakezelés) együttes kezelése a jellemző. Alapvetően kormányzati tevékenység, amely nem képes a magánszféra teljes bevonására, bár az infrastruktúrák jelentős része magánkézben van.

Külön-külön értékelve a különböző irányzatokat kijelenthetjük, hogy az egyes irányzatok nem azonos mértékben alkalmazzák a biztonság összes elemét, amelyeket a kockázatelemzéstől a jogszabály-alkotásig terjedő ún. biztonsági piramis mutat (ld. 2. ábra).



2. ábra:
Biztonsági piramis*
*Pataki János összeállítása

Európa létfontosságú infrastruktúrái nagymértékben összekapcsolódnak és egymástól függnek. A vállalategyesítés, az ipari racionalizáció, a hatékony üzleti gyakorlatok (például az éppen időben történő gyártás), valamint a népesség városi térségekbe történő tömörülése mind hozzájárult e helyzet kialakulásához. Európa létfontosságú infrastruktúrái esetében egyre inkább szükség van a közös információs technológiák (például az Internet vagy az űrben telepített rádiónavigáció és hírközlés) alkalmazására. A problémák végigvonulhatnak az egymással összefüggő infrastruktúrákon és az alapvető szolgáltatások váratlan és egyre komolyabb meghibásodását okozhatják. Az összekapcsolódás és az interdependencia (kölcsönös függőség) miatt ezek az infrastruktúrák kiszolgáltatottabbak az összeomlás vagy megsemmisítés szempontjából.

Tanulmányozni kell azon kritériumokat, amelyek miatt egy bizonyos infrastruktúra vagy az infrastruktúra egy bizonyos eleme létfontosságúnak tekinthető. A kiválasztási kritériumok megállapításánál ágazati és közös szakismereteket is fel kell használni. A létfontosságú infrastruktúrák meghatározásához három tényező alkalmazása ajánlott:

1. *Hatókör*. A létfontosságú infrastruktúra valamely elemével kapcsolatos veszteséget azon földrajzi terület nagysága alapján számítják ki, amelyet a

veszteség vagy az adott szolgáltatás megszűnése érinthet (nemzetközi, nemzeti, tartományi/területi vagy helyi).

2. *Nagyságrend*. A hatás mértékét a következőképpen lehet értékelni: nincs hatás, minimális, mérsékelt vagy jelentős. Többek között a következő szempontok alkalmazhatók a nagyságrend megállapításához:
    - a lakossággal kapcsolatos hatás (az érintett lakosság lélekszáma, áldozatok, betegségek, komoly sérülés, evakuálás);
    - gazdasági (GDP-hatás, a gazdasági veszteség jelentősége és/vagy a termékek vagy szolgáltatások színvonalának fokozatos romlása);
    - környezetvédelmi (a lakosságra és a környezetére gyakorolt hatás);
    - interdependencia (a létfontosságú infrastruktúrák egyéb elemei között);
    - politikai (az állam iránti bizalom);

3. *Időbeli hatás*. E szempont annak megállapítására szolgál, hogy egy adott infrastrukturális elemmel kapcsolatos veszteség mennyi idő elteltével fejthet ki komoly hatást (például azonnali, 24–48 óra, egy hét, egyéb).

A biztonsággal kapcsolatos irányításhoz a tagállamok létfontosságú infrastruktúrái elemeivel, valamint azok egymástól való függőségével kapcsolatos, a veszélyekre, váratlan eseményekre és a sebezhetőségre vonatkozó elemzés elvégzéséhez több forrásból származó információra van szükség. Minden ágazatnak és tagállamnak az EU harmonizált szabálya szerint a saját hatáskörén belül és a biztonságért felelős szervezetek vagy személyek segítségével kell meghatároznia a létfontosságú infrastruktúrákat.

Az EU az európai kritikus infrastruktúrák azonosításáról és kijelöléséről szóló 2008/114/EK tanácsi irányelvében határozza meg az egységes irányelveket a tagállamok részére. Magyarországon 2003-ban kezdődött meg a Kormányzati Koordinációs Bizottság szerveinél és a minisztériumokban a KIV-vel kapcsolatos kormányzati felmérő, elemző tevékenység, amelynek eredményeképp 2007-ben elfogadásra került a „Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról” című dokumentum.

A Zöld Könyv a KI fogalmát a következőképpen definiálja: *Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra-elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában. Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.*

Magyar (nemzeti) intézkedések:

- EU 2008/114/EK számú EU tanácsi irányelv alapján EU KI azonosítás, implementáció évenkénti felülvizsgálata, valamint későbbi kiterjesztése feladatok megkezdése;

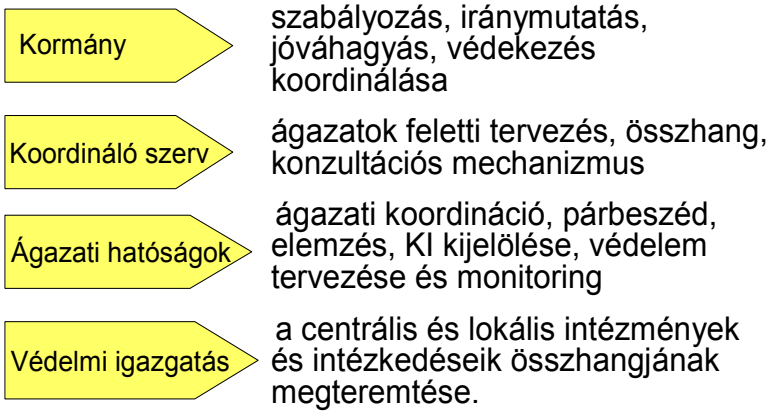
- a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. Korm. határozat, amely a hazai jogszabályi koncepció-alkotással, ágazati konzultációkkal, felmérésekkel foglalkozik;
- 1249/2010. (XI.19.) Korm. sz. határozat az EU KIV feladatokról;
- ágazati intézkedések;
- projektek, együttműködési megállapodások.

A definíciók és ágazati kritériumok alapján kritikusnak minősülő nemzeti infrastruktúrák:

I. Energia.
II. Infokommunikáció.
III. Közlekedés.
IV. Víz.
V. Élelmiszer.
VI. Egészségügy.
VII. Pénzügy.
VIII. Ipar.
IX. Jogrend – kormányzat.
X. Közbiztonság – védelem.

Előzetes elemzések alapján meghatározzák, mely szektorok és alrendszereik minősülhetnek kritikusnak az állampolgárok gazdasági, szociális jóléte, közegészség, közbiztonság, a nemzetbiztonság, a nemzetgazdaság és a kormányzat működése szempontjából. Az felsorolt ágazatok és alágazatok listája módosulhat a kritikus szolgáltatások és termékek értékelésére irányuló szektor elemzések során.

A KIV érdekében az állami/igazgatási szférában kifejtendő fő funkciók a 3. ábrán láthatók.



3. ábra
A KIV fő funkciói*

* Forrás: Király László−Medveczky Mihály: Védelemgazdasági ismeretek önkormányzati (védelmi igazgatási) válság menedzsereknek. Budapest, 2009. ZMNE. ISBN 978-963-7060-75-5. 76. oldal

Az infrastruktúrák döntő többsége napjainkban már hazai, illetve külföldi magánvállalatok tulajdonában, üzemeltetésében van. Az NKIV sikere a szereplők együttműködésén alapul. Ebben kiemelt fontossággal bírnak az infrastruktúra tulajdonosai és üzemeltetői. Az infrastruktúrák védelméért való elsődleges felelősség a tulajdonosokat, üzemeltetőket terheli. Az elemzések során, illetve a megfelelő védelmi stratégia alkalmazásában a kormányzat együttműködik az infrastruktúra-tulajdonosokkal és -üzemeltetőkkel a lehetséges kockázatok csökkentése érdekében. A vállalatok visszajelzést és támogatást kapnak az esetleges veszélyekkel és a legjobb gyakorlatok fejlesztésével kapcsolatban, továbbá közreműködnek az interdependenciák és sebezhető pontok értékelésében.

Az üzemeltetői biztonsági terv azonosítja a tulajdonos/üzemeltető létfontosságú infrastrukturális eszközeit, és azok védelmére megfelelő biztonsági megoldásokat alakít ki. Az üzemeltetői biztonsági terv meghatározza az energia és nemzeti KIV-programoknak és a vonatkozó ágazat specifikus programoknak való megfelelés érdekében követendő módszereket és eljárást. Az üzemeltetői biztonsági terv a KIV szabályozásában olyan lentről felfelé haladó megközelítést jelent, mely nagyobb cselekvési szabadságot biztosít (de nagyobb felelősséget is jelent) a magánszektor számára.

VÁLLALATI SZINT

A kritikus infrastruktúrát üzemeltető nem állami szereplőknek egységesen kell alkalmazni a biztonsági és védelmi intézkedéseket, amelyek alapján az adott szereplők egy egységes biztonságpolitikát valósítanak meg, és ehhez standartizált biztonsági szervezeteket építenek ki. Ez azért különösen fontos, mert itt már nem a hierarchikus kapcsolatok, hanem a vertikális kapcsolódások a jellemzőek.

Az EU Bizottság javasolja egy közös figyelmeztető (előrejelző) információs hálózat (CIWIN) létrehozását, mely elősegíti a megfelelő védekezési intézkedéseket, megkönnyíti a legjobb gyakorlatok biztonságos cseréjét, valamint továbbítja a közvetlen veszélyekre vonatkozó információkat és riasztásokat. A rendszer biztosítja, hogy az érintett személyek időben megkapják a megfelelő információkat.

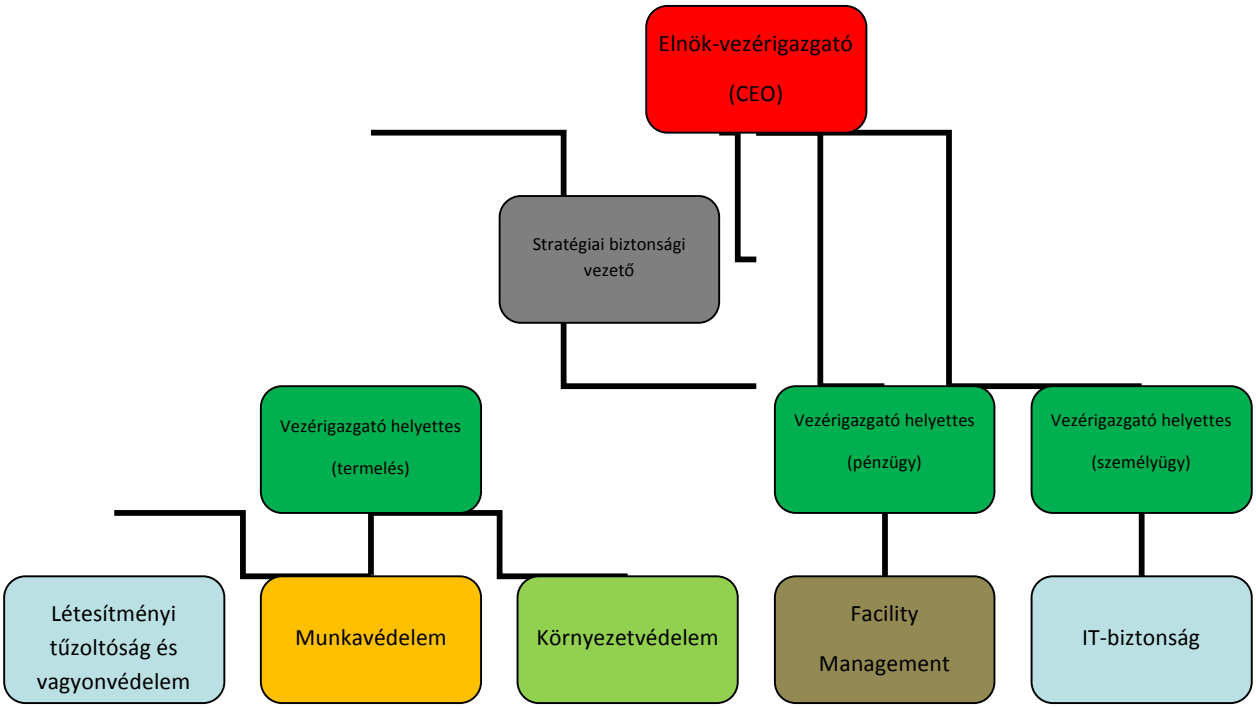
A vertikális kapcsolatok a stratégiai biztonsági vezetőhöz tartoznak (állami/igazgatási szint). A horizontális kapcsolatok jellemzően a kapcsolódó KI-t üzemeltető – pl. helyi – biztonsági hatóságokkal, szervezetekkel, az energia ellátást végző vállalatokkal az operatív (napi) biztonsági feladatokat végrehajtó szervezetek feladata.

A vállalati biztonság fogalma

A biztonság a vállalat azon állapotát mutatja, hogy milyen minimális veszélyeztetés mellett folytatható a vállalat üzleti/termelő tevékenysége. A megfelelő biztonsági intézkedések foglalkoznak minden veszélyforrással, amelyek lehetnek:

- szándékos tettek,
- vétlen emberi és technikai mulasztások,
- vis majorok.

Ezek egy átlagos/megengedhető vagy magasabb veszélyességi fokot érhetnek el. Ez vonatkozik mind az aktív veszélyekre (Security), mind a passzív veszélyekre (Safety).



4. ábra
Biztonsági szervezetek*
* Pataki János összeállítása

Biztonságpolitika

A vállalati biztonságpolitika fő szempontja a legfontosabb termelési tényező: az emberi élet és egészség védelme lehet. Másik fő szempont a vállalat működőképessége és a szolgáltatási piacok megtartása. Minden más aspektust ezeknek kell alárendelni.

100%-os biztonság nincs. A vállalat fenyegetettsége mindaddig fennáll, amíg a kiváltó okok meg nem szüntethetőek és/vagy a minimumra nem csökkenthetőek, addig a felmerülő költségeket a biztosító és/vagy a vállalat viseli.

A biztonság hordozói

A biztonságpolitika megvalósítása/végrehajtása a vállalatnál minden egyes dolgozó feladata. A biztonsági felelősség a vezetői felelősség része, azaz minden vezető köteles alkalmazni a biztonsági intézkedéseket saját területén és ebből következik, hogy a vezető felelős a hozzá tartozó területekért. Minden személy köteles magát alávetni az érvényes biztonsági szabályokban foglaltaknak a vállalat illetékességi területén.

Stratégiai szinten a vezetőket tanácsadással támogatják a szakterület biztonsági intézkedéseinek megvalósításában, valamint a vállalaton belüli biztonsági kérdések megválaszolásában. A biztonsági szabályok ismerete minden dolgozó feladata. Így előmozdítható a vállalat dolgozóinál a biztonsági felelősségtudat kialakulása.

A megbízott szakterületek feladata a különböző területek részére szükséges szabályok kidolgozása (minimum szabályok) és a vállalat felső vezetése az azokban meghatározottak alapján ellenőrzi ezek betartását. Emellett előmozdítja a szaktudáson és a kezdeményezőkészségen alapuló alkalmazást.

A vállalat működőképességét és tulajdonának biztonságát minden területen előtérbe kell helyezni. Ezen cél megvalósulása a vállalatnál a minimum szabályokban kerül meghatározásra, például:

- káresemények felderítése a korai időszakban;
- hatékony riasztási és kárelhárítási rendszer;
- külső erőszakos beavatkozás megakadályozása.

A káresemény lehetséges vagy valóságos eszkalációja egy bizonyos szint meghaladásakor megköveteli külső erők bevonását a kárelhárításba. Ezért már a beruházás tervezési fázisában ki kell dolgozni egy biztonsági koncepciót, amely tartalmazza:

- a globális kihívásokat,
- a helyi veszélyforrásokat és azok kockázatelemzését (rizikó analízist),
- az általános biztonsági szabályokat,
- a minimum előírásokat (információ-, objektumvédelem, beléptetés rendje),
- vagyonvédelem feladatait és elemeit,
- tűz-, katasztrófa- és polgári védelem, iparbiztonság feladatait és elemeit, valamint
- munkavédelem és munkabiztonság feladatait és elemeit, ideértve az egészségügyi szolgálat feladatait is.

A kritikus infrastruktúrák nemzeti fogalmának és kritériumainak meghatározása mellett, az ágazati sajátosságok érvényesítése érdekében meg kell határozni a nemzeti definíció megközelítésén alapuló ágazati fogalmakat és kritériumokat. Az ágazatért felelős miniszter saját hatáskörében, a biztonságért felelős szervezetek vagy személyek segítségével, az infrastruktúra tulajdonosok, üzemeltetők bevonásával határozza meg az ágazati fogalmakat, kritériumokat.

Tervezés és megvalósítás

A biztonsági intézkedéseket mindig az aktuális védelmi célok alapján kell kidolgozni. A biztonságpolitika és a kinyilvánított vállalati érdekek védelme a vállalat minimum szabályaiban kerülnek meghatározásra. Ezek a célok megvalósíthatók az integrált biztonságkoncepcióval és az ehhez tartozó egyedi intézkedésekkel.

A vállalat biztonságpolitikáját és minimum szabályait legalább évente egyszer, illetve különösen nagy kár esetén felül kell vizsgálni. A felső vezetés elemzi a káreseményt, a kiváltó okokat és jóváhagyja a megfelelő változtatásokat.

Az integrált biztonsági koncepciót a kiegészített technikai, szervezeti és pénzügyi biztonsági intézkedésekkel összhangban a telephely, a szervezeti egység (osztály) és a funkció szerinti bontásban kell kidolgozni és megvalósítani.

A minimum szabályok vonatkoznak minden munkaterületre, kiváltképp:

- az objektumvédelem,
- a beléptetés rendje és személyvédelem,
- az információvédelem,
- az üzemi katasztrófa-, tűz- és polgári védelem területére.

A minimum szabályokban foglaltak kötelezőek minden munkaterületre, így kizárt, hogy részlegenként eltérő követelményrendszert alakítsanak ki az IT-biztonság, a munkabiztonság, az egészségvédelem, a termékszavatosság, a folyamatbiztonság és a környezetvédelem kérdéseiben. Minden dolgozó köteles saját munkaterületén a szabályok betartására és ezzel a vállalat biztonságának támogatására.

Biztonsági szervezetek

Integrált biztonsági koncepció alapján kell kialakítani a biztonsági szervezeteket. Ez a biztonsági intézkedések célorientált és integrált tervezését és átalakítását jelenti, beillesztve egy olyan biztonsági rendszerbe, amely a „check and balance" elvén működik (szétválasztva a szervezeti egységek biztonsági felelősségét, támogatva a megbízott szakterületek és a létesítményi tűzoltóság és a vagyonvédelem részéről).

A biztonságpolitika átalakításával és a vállalati érdekek figyelembevételével kerültek a minimum szabályok kidolgozásra. Ezek tartalmazzák a törvényes és a vállalatra vonatkozó követelményeket és – ezen belül – az integrált biztonsági koncepcióhoz tartozó külön rendelkezések megvalósítását.

A biztonsági szervezetek működési alapelvei

A biztonsági szervezetek célja

A szervezeti alapelvek szolgálják a vállalat biztonságpolitikában foglalt célok megvalósítását, amelyek vonatkoznak:

- a szervezeti egységek biztonsági felelősségére (osztály),
- a megbízott szakterületekre,
- az üzembiztonsági szolgálatra.

Az illetékes vezető kötelessége a minimum szabályokban foglaltak betartása és betartatása. A megbízott szakterületek gondoskodnak az egész vállalat, illetve az egyes üzemek részére

- a biztonsági intézkedések megvalósításáról,
- a kiegyensúlyozott, szaktechnikai ismeretekről a vállalaton belül,
- a vezetők és a dolgozók biztonsági szemléletének támogatásáról és a minimum szabályok betartásának ellenőrzéséről.

Üzembiztonsági szolgálat területei a SitCen, a vagyonvédelem, a létesítményi tűzoltóság, a katasztrófavédelem, az iparbiztonság és a polgári védelem. Fontosabb feladatok:

- területek (épületek) berendezések őrzése,
- be- és kilépés ellenőrzése,
- aktív beavatkozás,
- nyomozások és kiértékelések végrehajtása,
- a biztonsági koncepció tervezése és működtetésének ellenőrzése a különböző
- szinteken (telephely, osztály),
- közreműködés a motivációban, a biztonságtudat kialakításában, utasítások
- kiadásában, gyakorlatok és ellenőrzések végrehajtásában.

Megbízott szakterületek

- stratégiai biztonsági vezető,
- egészségügyi szolgálat,
- munkabiztonság,
- környezetvédelem,
- IT-biztonság.

A stratégiai biztonsági vezető

A megbízott szakterületek között a stratégiai biztonsági vezetőé az a szakterület, amely biztosítja a szervezeti, technikai és építészeti biztonsági intézkedések szükséges integrációját tanácsadással, információval és koordinációval. A stratégiai biztonsági vezető feladatai:

- Kezdeményezi, hogy a biztonsági igények alapján, a kialakult gyenge pontok és kockázati tényezők helyzete rendszeresen meghatározásra kerüljön. Ehhez szükséges módszerek és eljárások kidolgozása.
- Tanácsadás és támogatás a megbízott szakterületek részére a Biztonsági Koncepció, illetve a biztonsági intézkedéseik tervezésében, realizálásában és felügyeletében az érvényes szabályok és a mindenkori szakismeretek alapján.
- Szúrópróbaszerű felülvizsgálata a szervezeti, technikai és építészeti biztonsági intézkedések működőképességének és a felelős szervezeti egységek által javasolt korrekciós intézkedéseknek.
- A biztonsági intézkedések és folyamatok kompatibilitásának ellenőrzése, adott esetben együttműködés az üzembiztonsággal.
- Együttműködés a biztonsági érdekekre fogékony dolgozókkal és vezetőkkel.
- Az új biztonsági rendszerek felülvizsgálatának dokumentálása és létrehozása.

A Stratégiai biztonsági vezető funkciójából adódóan integrálja a minimum szabályokban (ld. belépési szabályok, objektumvédelem, információvédelem, IT-biztonság) foglaltakat.

A védelmi képességfejlesztés és beruházás költségeinek viszonya

A kritikus infrastruktúra fejlesztésénél már a tervezés időszakában figyelembe kell venni a várható biztonsági költségeket. A biztonsággal kapcsolatos irányítás tudatos folyamat, amely a kockázat megállapítását, valamint az adott kockázat meghatározott, elfogadható költségek mellett elfogadható szintre való csökkentésére irányuló intézkedések meghozatalát és végrehajtását foglalja magában. E módszerre a kockázatoknak a kijelölt szintnek megfelelő megállapítása, mérése és ellenőrzése jellemző.

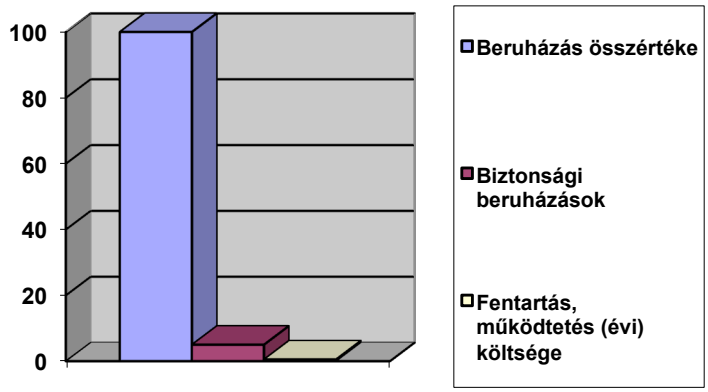
A katasztrófavédelmi felkészítés finanszírozásának 1/10-es szabálya szerint a potenciális vagy az elismert kár nagysága (K) egyrészt, a védelmi célú beruházásokra előirányzott fejlesztési forrás (B) másrészt és a folyó védekezési felkészülésre (a megelőzésre) fordítandó kiadások (V) aránya 1/10-es hányadosú mértani sorozatot alkot, azaz

$$K : B : V = 100 : 10 : 1.$$

Ebben a modellben – esetünkben − a potenciális kár az időegység alatti termeléskiesés/elmaradt haszon lehetne. Azonban a becslések bizonytalansága

miatt a nagyszámú tapasztalati adatot megkövetelő modellszámítás csak korlátozottan alkalmazható, ezért a beruházók/tervezők a kényelmesebb utat az ún. ökölszabályok alkalmazását választják.

A beruházások tervezésénél vannak „aranyszámok”, amelyeket a projekt tervezése során figyelembe kell venni. A következő értékekkel szokás számolni egy általános (nem atomerőmű) projektnél: a beruházás összköltségének 5%-a biztonsági költség, illetve a biztonsági rendszerek működtetési költsége 0,05%.



5. ábra
Költségek megoszlása*
*Pataki János összeállítása

A működési költségek már nem a projektet terhelik, hanem az objektum/intézmény/vállalat folyó költségvetését. A költségvetés tervezésénél a NATO által is alkalmazott „gördülő tervezést” ajánlott alkalmazni. A biztonsági költségek tartalmazzák a rendszerek tervezését, leszállítását, illetve beépítését (installálását).

Egy példán keresztül mutatjuk be a gyakorlatban egy beruházás biztonsági költségeinek felosztását. Ha egy beruházás összértéke 1000 Mrd HUF, akkor a fent említett „aranyszám” alapján a biztonsági rendszer költsége 50 Mrd HUF. (Természetesen ebbe az összegbe beleértendőek az építés során felmerülő őrzés, tűzvédelmi és egyéb más [munka-, környezetvédelmi] költségek is.)

1. Az építés fázisában:

- őrzés-védelem 150 M HUF;
- tűzvédelem 200 M HUF;
- munka-, környezetvédelem 300 M HUF.

2. A tervezés és megvalósítás fázisában:

- periféria védelem (kerítés, porták, beléptető és videó megfigyelő rendszer) 8 Mrd HUF;
- épületek, csarnokok vagyonvédelmi rendszerei 4 Mrd HUF;
- épületek, csarnokok tűz- és polgári védelmi, iparbiztonsági rendszerei 10 Mrd HUF;
- helyzetelemző Központ 3 Mrd HUF;
- létesítményi Tűzoltóság (gépjárművek, felszerelések stb.) 1 Mrd HUF;
- egyéb biztonsági rendszerek (vészvilágítás, szellőztetők stb.) 3 Mrd HUF;
- munkavédelmi berendezések, felszerelések 9 Mrd HUF;

- környezetvédelmi berendezések, felszerelések 8 Mrd HUF;
- egészségügyi szolgáltatások 3 Mrd HUF.

Természetesen ezen összegek csak tájékoztató jellegűek. Ezt több tényező határozza meg, mint például az alkalmazott technológiák, anyagok, tevékenység jelleg stb. A beruházás működtetésénél számolni kell a biztonsági személyzet bérével és egyéb más költségeivel, a karbantartási költségekkel, illetve a bevont külső szolgáltatók szerződésben foglalt költségeivel. Ez a beruházás összköltségének 0,05%-a, azaz 5 Mrd HUF. Ezen összeg a következő megoszlásban jelentkezik a különböző biztonsági szervezeteknél:

- vagyonvédelem 500 M HUF;
- tűzvédelem 400 M HUF;
- katasztrófavédelem, iparbiztonság, polgári védelem 100 M HUF;
- munkabiztonság, munkavédelem 1 100 M HUF;
- környezetvédelem 2 400 M HUF;
- egészségügyi szolgálat 500 M HUF.

Természetesen ezen adatok is csak tájékoztató jellegűek. Az aranyszám és a bemutatott tételek összege nem egyező, az tervezési tartalék.

Következtetések

Tanulmányunkban bemutattuk, hogy egy multinacionális nagyvállalat milyen sok szálon kapcsolódik az ország kritikus infrastruktúráihoz és a saját működési prioritásai (termelési/piaci működési folytonosság) szinte teljes egészében leképezik az EU-kritériumok szerinti elsődleges (energia-ellátás, infokommunikáció, közlekedés) és az ágazati kritériumok szerinti NKIV szektorokat. Így a felső vezetés vezetői felelősségének szerves része a vállalati biztonságpolitika kialakítása és érvényre juttatása. Ebben belső munkatársak és külső szakértők támogatják és döntésre készítik elő azokat a kérdéseket, amelyek a KIV-re vonatkozó jogszabályi előírások (amelyeket a külső, vertikális kapcsolatok közvetítenek), és a belső kritikus infrastruktúra, a termelési feltételek megengedhető kockázatokkal való megvalósítása és működtetése során felmerülnek.

A biztonsági szakfeladatok egy jelentős részét belső erőkkel nem lehet gazdaságosan megoldani, ezért szükséges külső erőforrások igénybevétele.

A kritikus infrastruktúrák biztosításában növekvő szerep hárul a civil biztonsági vállalkozásokra. A kritikus infrastruktúrák biztosításába be kell vonni azon vagyonvédelmi és biztonságtechnikai cégeket, amelyek rendelkeznek „NATO beszállító”, illetve „Minősített NATO beszállító” minősítéssel. Alkalmazásuknál figyelembe kell venni a hazai és nemzetközi jogi előírásokat és belső utasításokat.

Természetesen a korábban kialakult rendszer szerint kell megszervezni a különböző kritikus infrastruktúrák védelmét. Ez azt jelenti, hogy a teljes körű megrendelést pályáztatás útján kell kiválasztani, a legjobb feltételeket és legkedvezőbb anyagi ráfordítást garantáló gazdasági társaságnak. Így kialakult egy komplex feladatrendszer, ami azonban nem jelentheti azt, hogy a törvényekben rögzített állami feladatokat vesznek át civil biztonsági cégek. Ennek során a rendőrségi hatáskörökön kívül eső feladatokat, mint például vagyonvédelmi, biztonságtechnikai és katasztrófavédelmi teendőket hajtanak végre megfelelő ellenőrzés mellett.

FORRÁSOK

Jogszabályok:
A TANÁCS 2008/114/EK IRÁNYELVE (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről
2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
1249/2010. (XI.19.) Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

Felhasznált irodalom:
Sicherheitspolitik in neuen Dimensionen. 2009 by Verlag E.S Mittler & Sohn GmbH, Hamburg
Unternehmenschutz. Richard Boorberg Verlag, 2007, Stuttgart
Király László − Medveczky Mihály: Védelemgazdasági ismeretek önkormányzati (védelmi igazgatási) válság menedzsereknek. Budapest, 2009. ZMNE. ISBN 978-963-7060-75-5