Bakos Tamás

Kijelölt létfontosságú rendszerelem védelme a pandémiás veszélyhelyzet idején

Absztrakt

A kijelölt létfontosságú rendszerelemek, a szabályzó rendeletek értelmében rendelkeznek a folyamatos üzem biztosítását szolgáló Üzemeltetői Biztonsági Tervvel és az abban meghatározott biztonsági tervekkel. A 2019-es pandémiás veszélyhelyzet mégis olyan speciális körülményeket teremtett, amelyek szükségessé tették a legrészletesebben kidolgozott biztonsági intézkedések és tervek felülvizsgálatát is.
Célom megvizsgálni, hogy milyen módon volt szükséges változtatni a meglévő biztonsági terveket, és milyen új, különleges intézkedések bevezetésére volt szükség, amelyek tovább fokozták a létfontosságú rendszerelem biztonságos és folyamatos üzemeltetését, valamint bemutatni, hogy ezek az intézkedések – amelyek rövid távon emelték a létfontosságú rendszerelem biztonságát – hogyan hatottak hosszú távon a folyamatos üzemeltetésre és feladat-végrehajtásra.
Kulcsszavak: *létfontosságú rendszer, fizikai védelem, pandémiás veszélyhelyzet*

Physical Protection of Critical Infrastructures during the Pandemic Emergency

The designated critical infrastructures have an Operator Safety Plan and the other safety plans specified therein in accordance with the regulatory practice. Yet the 2019 pandemic emergency created special circumstances that necessitated a review of even the most detailed security measures and plans.
My aim is to examine the way it became necessary to change the existing security plans and what new special measures were needed to further enhance the safety and continuous operation of the critical infrastructures. Moreover, to demonstrate that these measures, which raised the safe of critical infrastructures in the short-term, also affected the plan and execution of tasks in the long-term.
Keywords: *critical infrastructures, physical protection, pandemic emergency*

Bevezetés

Az emberi civilizáció sikere és fejlődése, fejlődésének üteme arra épül, hogy környezetünket hogyan tudjuk szükségleteink szerint alakítani, az adott kor technikai színvonalának megfelelő eszközökkel, technológiákkal előállított erőforrások rendelkezésre állását folyamatosan, zavartalanul biztosítani. Ezt a rendszert, amely napjainkra már szerves része életünknek, nevezzük infrastruktúrának. Mondhatjuk, hogy nemcsak szerves része, de elengedhetetlen feltétele modern életünknek ezen infrastruktúrák folyamatos,

https://doi.org/10.36250/01059_01

zavartalan üzeme, sőt egyes infrastruktúra-elemek már annyira életünk részét képezik, hogy kiesésük igen komoly károkat okozhat. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy az infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket védeni kell.

A kritikus infrastruktúra mint fogalom az elmúlt évtizedben jelent meg a hazai szakmai életben. A kritikusnak minősített infrastruktúrák kijelölésére, védelmére vonatkozó külön szabályozás szükségessége hamar egyértelművé vált. Az európai szabályozást[1] gyorsan követte a magyar intézkedések megjelenése,[2] amely szabályozási folyamat napjainkig tart. Fogalomköre bővült, változott, így hazánkban jelenleg a *létfontosságú rendszer* elnevezés használatos. 2012. november 22-én a Parlament megszavazta a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényt, illetve 2013-ban a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendeletet. A törvény pontosítja az alapfogalmakat és meghatározza a nemzeti, illetve az európai létfontosságú rendszerelemekkel kapcsolatos kijelölés vagy visszavonás folyamatát, megadja a folyamathoz kapcsolódó feltételeket, de a kijelölést követő feladatokat, védelmi intézkedések meghozatalát, fejlesztését már a létfontosságú rendszerelem üzemeltetőire delegálja.

Az üzemeltetőkre terhelt feladatok igen nagy hátránya, hogy bár minden létfontosságú rendszerelem üzemeltetője rendelkezik a kijelölési folyamat végére az előírt dokumentumokkal (kockázatelemzés, üzemeltetői biztonsági terv, egyéb előírt védelmi tervek), de azok és az általuk előírt védelmi intézkedések minősége már nagyban függ a létfontosságú rendszerelem erőforrásaitól. Például egy megyei közlekedési hálózatot üzemeltető vállalat nem képes olyan erőforrásokat biztosítani a védelmi intézkedések fejlesztésére és végrehajtására, mint egy országos lefedettségű, magas bevétellel rendelkező pénzügyi vagy energetikai hálózattal foglalkozó vállalat. Pedig mindegyiket *nemzeti létfontosságú rendszerelemmé* jelölték ki.

Létfontosságú rendszerelemmé történő kijelölés résztvevői és folyamata

A létfontosságú rendszerelemmé történő kijelölés természetesen többszereplős folyamat. Az üzemeltető lehet természetes vagy jogi személy, szervezet is, aki az adott létesítmény napi működéséért felelős, tulajdonosa, engedélyese vagy rendelkezésre jogosultja.

[1] A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.

[2] 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.

Az üzemeltető részéről a biztonsági összekötő személy tartja a kapcsolatot hatóságokkal és vesz részt közvetlenül a kijelölés folyamatában.

A kijelölésben részt vevő állami hatóság az *ágazati javaslattevő hatóság,* amely rendelkezik azzal a szakmai háttérrel az adott ágazaton belül, hogy javasolhatja a kijelölést, akár az üzemeltetőtől függetlenül is. Az *ágazati kijelölő hatóság* hozza meg a döntést a kijelölésről – az előzetes javaslatok és vizsgálatok alapján – és határozza meg az üzemeltető további feladatait. Az ágazati ellenőrzést koordináló szerv az előírt kötelezettségek betartásának ellenőrzésére jogosult. A *nyilvántartó hatóság* a folyamatban részt vevők adatait és a kijelölés dokumentumait hivatott kezelni.

Alapesetben a potenciális létfontosságú rendszer vagy rendszerelem üzemeltetője kezdeményezi a kijelölési eljárást, egy azonosítási jelentés benyújtásával. A javaslattevő hatóság is kezdeményezheti az azonosítási eljárás lefolytatását a kijelölő hatóságnál, ha az üzemeltető ezt korábban még nem tette meg. A létfontosságú rendszerelemmé minősítés alapja egy olyan vizsgálat, amelyben megállapítják, hogy az adott létesítmény, objektum, eszköz vagy akár egy szoftver, szolgáltatás teljesít e bizonyos rá jellemző vagy tőle függő feltételeket. Ezeket a feltételeket a törvény kritériumoknak nevezi, amelyek lehetnek ágazati vagy horizontális kritériumok.

Az ágazati kritériumokat az adott ágazat szakmai irányításáért felelős szervek, szervezetek dolgozzák ki, adják meg, és külön ágazati kormányrendeletben hirdetik ki:

> „[Á]gazati kritérium: azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének megzavarása vagy megsemmisítése (a továbbiakban együtt: kiesés) által kiváltott hatásra vonatkoznak, és amelyek teljesülése esetén az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki azzal szoros összefüggésben, hogy mely ágazatba tartozik."[3]

Az ágazati kritériumok mellett a törvény meghatározza a horizontális kritériumok teljesülési feltételeit is, amelynek lényege, hogy az adott rendszerelem kiesése esetén olyan nagyarányú veszteségekkel, gazdasági, társadalmi, politikai, illetve környezeti hatásokkal kellene számolni, amelyek okán – ágazati hovatartozástól függetlenül – a vizsgált elemet nemzeti létfontosságú rendszerelemmé kell nyilvánítani. A horizontális kritériumok teljesülését minden esetben szakhatósági eljárásban vizsgálják.

Amennyiben a vizsgált potenciálisan létfontosságú rendszerelem teljesíti valamely kritériumot, az ágazati kijelölő hatóság lefolytatja a létfontosságú rendszerré vagy rendszerelemmé történő kijelölésre vonatkozó közigazgatási hatósági eljárást. A kijelölés visszavonása is hasonló hatósági eljárás keretében zajlik.

Mint azt már korábban említettem, a létfontosságú rendszerelemmé történő kijelölés kötelezettségeket ró az üzemeltetőre. Első lépésként kockázatelemzést és az alapján *üzemeltetői biztonsági tervet* kell készítenie, amelynek határidejét a kijelölő hatóság a kijelöléskor adja meg. Ezenfelül a kijelölő hatóság további, a létfontosságú rendszerelem

[3] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 1. § *a).*

védelmével összefüggő, a rendszerelem egyedi sajátosságaihoz, környezetéhez, a rendszerelem által potenciálisan előidézhető veszély mértékéhez igazodó feltételeket írhat elő az üzemeltető részére.

Az üzemeltetői biztonsági terv (ÜBT)

Az ÜBT lehetséges tartalmi követelményeit a 65/2013. (III. 8.) Korm. rendelet 2. melléklete foglalja össze.[4] A kormányrendelet részletes tartalmi összefoglalót ad egy kijelölt létfontosságú rendszerelem ÜBT-tartalmáról, és annak elfogadásáról az ágazati kijelölő hatóság dönt. Egy teljes körű kockázatelemzés alapján, részletesen kidolgozott ÜBT, illetve az ÜBT-hez kapcsolódó védelmi tervek és intézkedések – amelyeket a képzett szakállomány be is tart – már hatékony védelmet képesek biztosítani egy adott létfontosságú rendszerelem számára.

Általános bemutatás

Az ÜBT első részében az üzemeltető általános bemutatása történik. Számos esetben a kijelölt létfontosságú rendszerelem üzemeltetése több jogi személy, szervezet szerződéssel alátámasztott együttműködése alapján valósul meg. Az ÜBT-ben ki kell fejteni a tulajdonosi, rendelkezési jogosultság struktúráját, a kiszervezett tevékenységek és kapcsolatok összefüggéseit annak érdekében, hogy a felelősségi köröket a lehető legpontosabban meg lehessen állapítani. Ebben a fejezetben szükséges pontosítani az üzemeltető emberierőforrás-hátterét, szervezeti felépítését, vezetési struktúráját és a kapcsolódó létesítmények beazonosítását is, amely alapján tovább pontosítható a felelősségi kör.

Az általános bemutatást követően részletesen szükséges tisztázni a létfontosságú rendszerelem fő feladatait, az ahhoz tartozó alfeladatokat, azok kihasználtságát, forgalmi adatait, tehát az adott létfontosságú rendszer vagy rendszerelem képességeinek teljes palettáját. Itt ki kell emelni azokat a képességeiket is, amelyek valamilyen oknál fogva ugyan nincsenek használatban, de képességként megjelennek. A feladatok, képességek, lehetőségek leírása, jellemzése mellett értelmezni kell az azok közötti logikai, függőségi viszonyokat is, valamint az ágazatok és alágazatok közötti függőségi viszonyokat, amelyek a létfontosságú rendszerelem működésénél relevánsak.

Környezet bemutatása

A következő részek a létfontosságú rendszerelemek környezetének bemutatásáról szólnak. Idetartozik az érintett területek beazonosítása, részletes jellemzése. A különböző

[4] 65/2013. (III. 8.) Korm. rendelet 2. mell. 14.

méretarányú térképek segítségével pontosan megadható az érintett területek, objektumok elhelyezkedése. A részletes jellemzés tartalmazza a beépítettség és a lakosság jellegét, a közlekedési hálózatot, a kulturális és turisztikai szempontból jelentősebb objektumok, illetve a területen található intézmények, közintézmények bemutatását, forgalmát, fizikai jellemzőit. Szükséges kiemelni a védelem szempontjából lényeges objektumokat, jellemzőket, mint például közeli fegyveres szerv, ipari létesítmény elhelyezkedése, feltöltöttsége; közúti és egyéb megközelítési útvonalakat, lehetőségeket. Természetesen ezen adatokat és elemzéseket meg kell adni a létfontosságú rendszerelem minden telephelyére. A környezet bemutatása tartalmazza az éves időjárási adatokat (átlaghőmérsékletek, csapadék), lehetőség szerint a környezet geológiai és hidrológiai jellemzőit is.

Kijelölt rendszerelem részletes bemutatása

A részletes bemutatás – az előző pontokra építve – már tartalmazza a kijelölt rendszerelem valamennyi elemének működési rendjét, az ahhoz kapcsolódó eszközök, technológiák, berendezések leírását. Idetartoznak a rendeltetésszerű üzemeltetés elemei és azok kiváltását biztosító tartalék elemei, illetve azon erőforrások, amelyek ezen elemek működéséhez szükségesek. Részletesen be kell mutatni a létfontosságú rendszerelem folyamatos üzemeltetéséhez szükséges belső infrastruktúra-hálózat felépítését, kapacitását, kiesés esetére beállított tartalékrendszerét, karbantartását. Amennyiben az üzemeltetéshez szükséges olyan infrastrukturális elem, amely csak külső szolgáltató által vehető igénybe, abban az esetben a külső szolgáltató részletes bemutatása is szükséges.

Kockázatelemzés

A létfontosságú rendszer előzőekben tárgyalt részletes bemutatása, illetve a létfontosságú rendszerelem pontos logikai, függőségi elhelyezkedése ebben a rendszerben nagyon jó alapot ad a pontos *kockázatelemzésnek.*

Önállóan működő, teljesen zárt infrastruktúra-rendszer nem létezik. Minden üzem, objektum, létesítmény, szolgáltatás kapcsolatban áll másokkal, egy-egy részelemének működése függ vagy befolyásol más folyamatokat. Ez a kölcsönös függőség vagy interdependencia olyan vizsgálati vonalakat nyithat meg, amelyek már túlmutatnak a konkrét létfontosságú rendszerelem keretein. Tehát az interdependencia vizsgálata fontos eleme a kockázatelemzésnek, amelynek alapja a létfontosságú rendszerelem működése szempontjából kritikus szolgáltatók meghatározása.

A kritikus szolgáltatók körének meghatározásához az összes külső – tehát nem a létfontosságú rendszerelem üzemeltetéséhez tartozó – szolgáltatót vizsgálni kell olyan szempontból, hogy a szolgáltatás kiesésének van-e azonnali hatása a működésre. Ezt a hatást pontosan meg kell határozni, és vizsgálni, hogy kiesése esetén van-e lehetőség a pótlására vagy helyettesítésére olyan határidőn belül, amely még nem okoz jelentős problémát

a létfontosságú rendszerelem folyamatos üzemében. Így eldönthető, hogy az adott külső szolgáltató kritikus-e, vagy nem.

Amennyiben egy külső szolgáltató kritikusnak minősül, szükséges meghatározni, hogy kiesése esetén milyen azonnali és további intézkedésekre van szükség a létfontosságú rendszerelem folyamatos üzemeltetése érdekében. Ez jelentheti a saját erőforrások ideiglenes felhasználását vagy egy hasonló képességekkel rendelkező másik szolgáltató bevonását is. Amennyiben az adott szolgáltatás fenntartása komolyabb erőforrásokat, szervezést vagy rendszert igényel, az esetleges kiesés pótlására és az üzemfolytonosság biztosítására előzetes terveket kell készíteni, amelyek az ÜBT mellékletét képezik.

A kritikus szolgáltatók vizsgálata mellett elemezni kell a létfontosságú rendszerelemet és üzemfolytonosságot veszélyeztető kockázatokat. A kockázatok áttekintéséhez nagy segítséget adhat a német információbiztonsági szabványosítási intézet (BSI, Bundesamt für Sicherheit in der Informationstechnik) honlapján[5] megtalálható fenyegetéskatalógus, amelyet ki lehet egészíteni a helyi sajátosságokból és geopolitikai változásokból eredő tételekkel.

A létfontosságú rendszerelem teljes fenyegetéslistája tartalmazza a természeti vagy ipari katasztrófák, balesetek, meghibásodások lehetőségein túl a fizikai, informatikai vagy egyéb úton bekövetkező, gondatlanságból eredő vagy szándékos károkozást, akadályozást, jogosulatlan hozzáférés lehetőségeit is. Ezen fenyegetések részletes leírása, elemzése alapján meghatározható minden típusú fenyegetésre egy külön védekezési protokoll, amely – az előzőekben leírtakhoz hasonlóan – speciális védelmi tervben is szabályozható. Ebben a listában azt is meghatározzák, hogy az adott fenyegetésnek mekkora a becsült gyakorisága, és milyen mértékben veszélyezteti az üzemfolytonosságot.

Az elemzések alapján kialakuló adathalmazból már könnyen készíthető olyan mátrix, illetve kockázattérkép, amely megadja a létfontosságú rendszerelem kritikus pontjait. Az alábbiakban egy példát mutatok be, amely természetesen – a létfontosságú rendszerelem típusától függően – eltérő lehet mind tartalmában, mind felépítésében. A gyakoriság lehet akár szofisztikáltabb, több sort tartalmazó, a súlyosság pedig a létfontosságú rendszerelem profilja szerinti meghatározással készülhet. A súlyosság szempontját vizsgálva alapul vehetők a 65/2013. (III. 8.) számú kormányrendeletben meghatározott horizontális kritériumok szempontjai: emberélet-veszteség, gazdasági, társadalmi, politikai, környezeti vagy infrastrukturális hatás. A legegyszerűbb mátrix mindössze néhány elemből épül fel. Gyakoriság szempontjából vegyünk fel négy elemet.

1. táblázat: Példa egy létfontosságú rendszerelem kritikus pontjainak meghatározásához

Gyakoriság	Előfordulási gyakoriság meghatározása
Nagyon ritka	Kevesebb mint 5 évente egyszer fordulhat elő
Ritka	1–5 évente egyszer fordulhat elő
Gyakori	Évente egyszer fordulhat elő
Nagyon gyakori	Havonta egyszer fordulhat elő

[5] Lásd: www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

A következmények szempontjából az alábbi súlyossági kategóriákat lehet alkalmazni:

Súlyosság	Következmény
Kicsi	Kevesebb mint 100 fő ideiglenes kitelepítése válik szükségessé
Közepes	100–1000 fő kitelepítése válik szükségessé
Magas	Több mint 1000 fő tartós kitelepítése válik szükségessé

Ha a kockázattérkép egyes celláit – amelyek tartalmazzák a fenyegetéslista soraihoz rendelt sorszámokat – színekkel jelöljük:

Színjelölés	Kockázat mértéke
Fehér	Nagyon alacsony
Zöld	Alacsony
Sárga	Közepes
Piros	Magas

Abban az esetben jól átlátható kockázatmátrixot kapunk:

Kockázatmátrix			
Gyakoriság	Súlyosság		
	Kicsi	Közepes	Nagy
Nagyon ritka	2	5, 7, 9	3
Ritka	4, 12, 16, 17	1, 6, 8, 10	11, 13
Gyakori	18, 22	19,	20, 21
Nagyon gyakori	14, 15		

Forrás: a szerző szerkesztése

A kockázatmátrixban szereplő értékeknél már figyelembe kell venni a meghozott védelmi intézkedéseket a következmények osztályozása során.

A kockázatelemzést követően az ÜBT részletesen tárgyalja a szükséges védelmi intézkedéseket. A létfontosságú rendszerelem védelmével kapcsolatos fő célkitűzések priorizált felsorolása érthetőbbé teszi a védelmi intézkedések elveit, tartalmát. Az ÜBT ezen részében szükséges felsorolni a védelem és az üzemfolytonosság biztosítását szolgáló szerveket, kontrollelemeket. Ilyen lehet például a létesítményi tűzoltóság, különböző helyekre és feltételekkel szervezett biztonsági őrség, belső ellenőr, elemző és naplózó személyzet, de akár a számítógépes vírusvédelem vagy az informatikai rendszer biztonságát szolgáló tűzfalrendszer vagy védelmi szoftver, szolgáltatás is.

A védelmi intézkedések

Az alábbiakban áttekintem, hogy milyen védelmi intézkedések biztosíthatják egy létfontosságú rendszerelem teljes körű védelmét és üzemfolytonosságát.

Emberi erőforrások biztonsága

Megfelelő ember a megfelelő helyen. Normál működés esetén ez az elv kiváló üzemeltetést eredményez. De létfontosságú rendszerek üzemeltetése esetén fel kell készülni a speciális, vészhelyzeti üzemeltetésre is. Ezt el lehet érni a munkatársak megfelelő és folyamatosan fejlesztett szaktudásával, a hasonló szakterületen dolgozók oldalirányú képzésével, amely lehetőséget ad a hasonló munkakörökben dolgozók helyettesítésére is. A pszichoszociális kockázatok felmérésével és azok elemzésével olyan akcióterv dolgozható ki, amely figyelembe veszi a munkatársak szaktudásának hosszú távú fejlesztését, a változás- és stresszkezelési technikák és a szakmai látókört szélesítő tudás elsajátítását.

Belső audit

Akár önálló szervezet, akár ideiglenesen létrehozott felügyeleti elem látja el, fontos feladata az elmúlt időszak üzemeltetéssel kapcsolatos tapasztalatainak, problémáinak javító szándékú feltárása. Az üzemeltetéssel kapcsolatos folyamatok ellenőrzését érdemes tervszerűen, ciklusos formában végrehajtani, így az eltérések, változások könnyen elemezhetők. Amennyiben hiányosság, probléma merül fel egy folyamatban, annak pótlására, javítására intézkedési tervet kell készíteni, és az ebben lévő határidőket és a végrehajtást ugyancsak fontos visszaellenőrizni.

Az üzemeltetéssel kapcsolatos folyamatok változásai természetesen nem csak akaratlanul kerülhetnek a rendszerbe. A működési környezet változása tervezett változtatásokat, a társadalmak fejlődése tervezett fejlesztéseket igényel. A létfontosságú rendszerelemnek érdemes változáskezelő rendszert alkalmazni, amely épülhet a belső audit rendszerére is.

Fizikai védelem

A megfelelő fizikai védelem kialakításához a védendő objektumot és környezetét magában foglaló zónákat kell kialakítani. Ezen zónák fizikai védelme a zónák típusától, felépítésétől és a védelem szükséges szintjétől függ.

A külső biztonsági zóna védelme az objektum rejtett vagy engedély nélküli megközelítését hivatott megakadályozni. Kiterjedése és átláthatósága miatt megnehezíti az észrevétlen megközelítést vagy megfigyelést, illetve a nemkívánatos eszközök, szerkezetek vagy anyagok bejuttatását. A biztonsági távolság méreteit a veszélyeztetettség mértéke, illetve természetesen az objektív lehetőségek határozzák meg. Itt alkalmazhatók mechanikai (terelő elemek, sorompók, kerítés stb.) vagy elektronikai (jelzőrendszer, kamerarendszer, mozgásérzékelők stb.) biztonságtechnikai eszközök.

A következő fizikai védelmi zóna maga az objektum, amelynek építészeti kialakításával, belső elektronikai biztonságtechnikai eszközök használatával komoly biztonsági szint építhető ki. Ezen belül a létfontosságú rendszerelem kritikus pontjai (szerverterem,

vezérlő egységek, UPS) külön megerősített, belső zónában helyezhetők el, amely akár függetlenül is működhet a védelem egyéb elemeitől.

Fontos kiemelni, hogy e védelmi zónák csak akkor működhetnek igazán hatékonyan, ha kiegészülnek a szükséges adminisztratív és humán védelemmel. Vagyis a megfelelően képzett, a vész- és stresszhelyzetekre felkészített szakemberek üzemeltetik, és rendelkezik a szükséges szintű beléptető rendszerrel.

A fizikai védelem komplexitásából eredően érdemes külön *fizikai védelmi tervben* megfogalmazni a követelményeit és a végrehajtás módját.

Informatikai biztonság

Napjainkban az egyik legérzékenyebb terület, amelynek védelme külön erőforrásokat igényel. Az informatikai biztonság szervezésében mindenképpen érdemes olyan többrétegű védelmi rendszert létrehozni, amelyben a védelem egyes szintjei és elemei kapcsolatban állnak egymással, de működésükben függetlenek, az egyes védelmi elemek kiesése nem befolyásolja a többi elem által biztosított védelem szintjét.

Az informatikai védelmi rendszer elemeinek üzemeltetése széles körű, speciális ismereteket, képzettséget igényel, és ez még fontosabbá teszi az emberierőforrás-biztonság kiemelt kezelését.

Hasonlóképpen a fizikai védelemhez, az informatikai védelem komplexitásából eredően is szükséges lehet külön *informatikai és információvédelmi tervben* megfogalmazni a követelményeket és a végrehajtás módját.

Tartalék rendszerek

Az üzemfolytonosság biztosításának legbiztosabb – és legköltségesebb – módja a kritikus rendszerek duplikálása. A létfontosságú rendszerelem kritikus elemeit vizsgálva meghatározható, hogy költség-érték arányában mely kritikus elemet érdemes duplikálni. Ilyenek lehetnek a központi szerverszámítógépek, a kommunikációs rendszerek, de akár a belső infrastruktúrák vagy akár maga a befogadó objektum is.

A duplikációnál kiemelt figyelmet kell fordítani arra, hogy a létfontosságú rendszerelem kritikus pontjai üzembiztonságának ellenőrzésekor a duplikált elemet is ugyanolyan szintű ellenőrzésnek kell alávetni. Az üzemfolytonosság-vizsgálatoknál a duplikációk közötti váltás hatékonyságát és az átváltás folyamatának biztonságát is vizsgálni kell.

Karbantartási terv

A folyamatos üzemeltetéshez szükséges napi és ciklikus rendszerű karbantartásokról a karbantartási terv szól. Az ebben megfogalmazott teendők előre tervezhetők,

az esetleges meghibásodások rutinszerűen, gyorsan javíthatók. A részletesen kidolgozott karbantartási terv alapján rendszeresen végrehajtott ellenőrzések, karbantartások és javítások nagyban növelik a létfontosságú rendszerelem üzemfolytonosságát.

Tájékoztatási és értesítési rendszer

A tájékoztatási és értesítési rendszer terve az információvédelmi terv egyes részeivel összhangban meghatározza az alkalmazható kommunikációs eszközöket, illetve azon protokollokat, amelyek alkalmazásával minden irányba – külső és belső – a megfelelő szintű információ jut ki, nem veszélyeztetve ezzel a létfontosságú rendszerelem érzékeny adatait.

Részletesen tartalmazza, hogy veszélyhelyzet esetén milyen csatornákon és milyen sorrendben jut el a megfelelő információ a vezetőséghez és a kollégákhoz.

Egyéb biztonsági tervek

A különböző törvények és rendeletek alapján[6] minden szervezetnek – nem csak a létfontosságú rendszerelemeknek – rendelkeznie kell az alapvető biztonsági tervekkel, mint például:

- munka- és balesetvédelmi terv;
- tűzvédelmi vagy tűzriadóterv;
- környezetvédelmi terv;
- kiürítési terv;
- belső védelmi terv;
- egészségvédelmi terv;
- műszaki mentési terv.

A fent felsorolt tervek mellett egy üzem rendelkezhet külön biztonsági tervvel, a sajátosságainak megfelelően. Egy nagy vagy speciális területen elhelyezkedő üzem (például bánya, olajfinomító) rendelkezhet belső közlekedési tervvel vagy egyéb speciális védelmi, biztonsági tervekkel is.

Természetesen ezen biztonsági tervekkel egy kijelölt létfontosságú rendszerelem is rendelkezik, de fontos, hogy a kijelölés előtt meglévő biztonsági terveket össze kell hangolni az ÜBT-vel. Gyakori hiba, hogy az újonnan készülő ÜBT-t „ráhangolják”

[6] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról; 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról; 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól; 1993. évi XCIII. törvény a munkavédelemről; 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról.

a meglévő biztonsági tervekre, így olyan hamis biztonságérzet keletkezik, amely szerint a meglévő védelmi intézkedések elegendők a kijelölt létfontosságú rendszerelem üzemfolytonosságának fenntartásához. Ez az elv azért helytelen, mert a meglévő biztonsági tervek a bekövetkező vészhelyzet vagy katasztrófa esetére írnak elő szabályokat az élet- és vagyonvédelem érdekében, míg a helyesen kidolgozott ÜBT a széles körű megelőzésre is koncentrál. Tehát bővebb és más elveket követ.

A pandémiás veszélyhelyzet kezelése

A tökéletesen kidolgozott ÜBT és a kapcsolódó védelmi tervek, az előírt és tervezett intézkedések kiépítése, protokollok végrehajtása, oktatása, visszaellenőrzése mellett még egy nagyon fontos képessége kell hogy legyen egy létfontosságú rendszerelem védelmének: a rugalmasság. A legrészletesebben kidolgozott terveknek is pontosításra, finomhangolásra van szükségük abban az esetben, amikor nagyléptékű, konkrét események fenyegetik az üzemfolytonosságot.

A korábbi években, évtizedekben a védelmi tervek kidolgozásánál számoltak természeti vagy ipari katasztrófákkal, terrortámadással, illetéktelen behatolással, de a 2019-es pandémiás veszélyhelyzet megmutatta, hogy mindig van – és lesz – olyan esemény, amelyre nem voltunk teljesen felkészülve, nem tudunk teljesen felkészülni. A jól kidolgozott védelmi tervekkel és az események gyors, rugalmas követésével mégis fenntartható az üzemfolytonosság.

A továbbiakban azokat az intézkedéseket mutatom be, amelyekkel pontosítva, kiegészítve a védelmi terveket, a munkatársak védelme és az üzemfolytonosság biztosítva volt.

Otthoni munkavégzés

Több szervezet, vállalat is élt ezzel a lehetőséggel mint a helyzethez alkalmazkodó logikus lépéssel. Természetesen csak olyan munkakörökről lehet szó, amelyek nem igényelnek személyes jelenlétet. Megvalósításához olyan informatikai háttérre van szükség, amely biztosítja az informatikai rendszer stabilitását és védelmét távoli elérés esetén is. Ez plusz eszközöket, speciális szoftvereket és hardvereket igényel.

Előnye – a pandémiás veszélyhelyzet idején –, hogy minimalizálni lehet a személyes kontaktusok számát, megbetegedés esetén nem kell számolni kontakttal, illetve előre tervezhető a helyettesítés.

Munkavállalói oldalról az otthoni környezet lehet előny és hátrány is. Többen az otthoni nyugodt környezetet inkább előnyként írták le az első időszakban, de 2–3 hónap után már – saját bevallásuk szerint is – csökkent a munkavégzés hatékonysága, hiányoztak a munkatársakkal való szakmai és szociális kapcsolatok.

A hatékonyság csökkenését hosszabb távon a vezetőség is érzékelte. A videókonferenciák hosszú távon nem tudták 100%-ban helyettesíteni a személyes

munkacsoport-megbeszéléseket, a folyamatok lelassultak, a gyors döntést igénylő pontok elakadtak. Megoldást jelentettek a kisebb létszámú, személyes részvétellel megvalósított munkacsoport-értekezletek, amelyeket feladatonként egymástól független időben, a pandémiás veszélyhelyzetre jellemző legszigorúbb óvintézkedések mellett szerveztek meg.

Személyes jelenlétet igénylő munkakörök

Természetesen nem lehetséges minden munkakört a napi működést biztosító telephelyről kiszervezni. Ilyen személyes jelenlétet igénylő munkakörök lehetnek – például – a 24 órás felügyeletet igénylő informatikai vagy vezérlő elemek kezelői, a biztonsági őrség, technikai, műszaki üzemeltető személyek, fizikai küldemény átvételéért, kezeléséért felelős személyek. A minimális üzemeltetési személyzet és létszám meghatározásával könnyebben tervezhetők a speciális védelmi intézkedések és rendszabályok, amelyeket a pandémiás veszélyhelyzet idején volt szükséges bevezetni a munkatársak védelme és az üzemfolytonosság fenntartása érdekében.

- A munkába járás egyik kritikus része a telephelyre, munkahelyre történő bejutás. Kerülni kell a tömegközlekedés használatát. Ennek érdekében a munkavállaló saját gépjármű használata esetén az üzemanyagot és egyéb költségeit elszámolhatja a munkaadó felé, illetve – ha szükséges – taxi- vagy sofőrszolgáltatást vehet igénybe. Ezt a lehetőséget segíti a munkaadó által biztosított ingyenes parkolási, illetve motorkerékpár- és kerékpártárolási lehetőség.
- A beléptetés is szigorúbb szabályok szerint történik, minden személyes megjelenést előre egyeztetni kell a biztonsági vezetőséggel, és csak az engedélyezett, megadott időkapuban lehet bent tartózkodni. Így elkerülhetők az érintkezések. A folyosókat, lifteket, beléptető kapukat egyszerre csak egy munkavállaló használhatja.
- A telephelyre, munkahelyre történő bejutást követően a belső mozgásokat és kontaktusokat is korlátozni kell. Adott személyek – például egy bizonyos osztály, részleg munkatársai – csak a kijelölt mosdót, teakonyhát használhatják, a normál működési rendtől eltérően a telephely, munkahely csak egy bizonyos részén közlekedhetnek, amely kijelölt részek nem fedik át egymást. A munkahelyen tartózkodás ideje alatt kötelező a maszkviselés és a gyakori kézfertőtlenítés a kihelyezett fertőtlenítő pontokon.
- A közlekedés és a mozgások szigorú korlátozásával is számolva tervezni lehet a bent maradó, kulcsfontosságú munkakörben dolgozó személyek részére fektető anyag, napi élelmezési ellátás és egyéb szükségletek biztosításával.

Fizikai küldemények átadás-átvételének szabályozása

A pandémiás időszakban veszélyforrásként jelent meg a szigorúan személyes átvételre beérkező fizikai küldemények átadás-átvétele. A fertőzésveszély szempontjából

előzetesen nem ellenőrzött küldemények kezelésének szabályait a normál időszakhoz képest szigorítani kellett. Egy lehetséges protokoll szerint a következőképpen lehet eljárni:

– a csomagot kézbesítő személy nem léphet az üzem/telephely területére;
– az átadás-átvétel lebonyolításához más személy által nem használt helyiség használható;
– a fizikai küldemények átvételével megbízott munkavállaló védőfelszerelést (szájmaszkot, egyszer használatos gumikesztyűt) használ, a védőfelszerelések az átadás-átvétel után tovább nem használhatók;
– az átvett csomag – lehetőség szerint – 48 órát elzárva tartandó az erre kijelölt helyen.

Tömeges megbetegedések kezelésére vonatkozó terv

A részletesen kidolgozott ÜBT és a kapcsolódó védelmi tervek, illetve a pandémiás helyzetre vonatkozó speciális rendszabályok bevezetése mellett szükséges egy „vészforgatókönyv" kidolgozása, amely arra az esetre vonatkozik, ha valamely előre nem látható oknál fogva a létfontosságú rendszerelem munkavállalói közül nagyobb létszámban betegednek meg, vagyis az üzemfolytonosság veszélybe kerül, esetleg megszakad.

Ebben az esetben szükséges lehet megvizsgálni a helyettesítés lehetőségét. A helyettesítés jelentheti az adott munkavállaló helyettesítését külső személlyel, akinek a szakértelme megfelelő az adott munkakör betöltéséhez, de jelentheti a teljes szolgáltatás vagy elem külső erőforrásból történő pótlását is. Ez a lehetőség előzetes egyeztetéseket igényel külső szakemberekkel, bizonyos esetekben előzetes megállapodások megkötését szolgáltatókkal, hasonló szakterületen működő vállalatokkal.

Összefoglalás

Ha áttekintjük egy létfontosságú rendszerelem teljes védelmi struktúráját és a pandémiás vészhelyzet alatt hozott speciális intézkedéseit, láthatjuk, hogy a jól kidolgozott védelmi tervekkel és az események gyors, rugalmas követésével fenntartható az üzemfolytonosság, vészhelyzetekben is megvalósítható hatékony védelem.

Viszont az is megfigyelhető, hogy a részletesen és jól kidolgozott üzemeltetői biztonsági tervben és a kapcsolódó védelmi tervekben előírt intézkedések és protokollok előkészítése és normál időszakban történő fenntartása olyan erőforrásokat igényelhet, amelyeket nem minden kijelölt létfontosságú rendszerelem engedhet meg magának. Pedig ez lenne a speciális vészhelyzeti üzemeltetés alapja. Amennyiben ezek az alapok nem adottak, egy speciális vészhelyzetben a létfontosságú rendszerelem üzemfolytonossága vagy nem biztosítható, vagy irreális erőforrásokkal, költségekkel járna.

Ezen indokok miatt tartom fontosnak, hogy létfontosságú rendszerelemmé történő kijelölés esetén ne a minimális és elégséges védelmi szintet célozzuk meg, hanem próbál-

juk megtalálni azt az arany középutat, amely nem ró túl nagy terheket az üzemeltetőre, mégis biztosítja az üzemfolytonosság fenntarthatóságát vészhelyzet idején is.

Felhasznált irodalom

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.

1993. évi XCIII. törvény a munkavédelemről.

1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról.

2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról.

54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról.

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

A Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Brüsszel, 2008. december 23.

Federal Office for Information Security: *IT Grundschutz*. Online: www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html