HADMÉRNÖK

X. Évfolyam 2. szám - 2015. június

SÁGI Gábor
gabor.sagi@yahoo.com

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME
A HAZAI SZABÁLYOZÁS ÉS A „FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY" FIGYELEMBEVÉTELÉVEL

Absztrakt

A kritikus infrastruktúrák és kritikus információs infrastruktúrák elfogadható működése elengedhetetlen feltétele a gazdaság, társadalom, védelem zavartalan működésének. A kritikus infrastruktúrák biztonságos működésének egyik alapfeltétele, hogy az üzemeltető szervezet ismerje az infrastruktúra elemeit és az azokat veszélyeztető fenyegetések. Az információbiztonsági szint felméréséhez és javításához nyújtanak segítséget a kormányzati és egyéb szervezetek által kidolgozott jogszabályok, szabványok, ajánlások, keretrendszerek.

The critical infrastructures and critical information infrastructures is essential for acceptable operation of the economy, society, defense. Essential for secure operation of the critical infrastructure is that the organization is familiar with the assets of the organization and the threats of the infrastructure. The laws, standards, recommendations and frameworks which are prepared by governments and other organizations, can help to analyze and improve the level of cybersecurity of organizations. The author wishes to present connection between the local law of critical infrastructure defend and Framework for Improving Critical Infrastructure Cybersecurity document.

Kulcsszavak: *kritikus információs infrastruktúrák fogalma, kritikus információs infrastruktúrák védelme, kritikus infrastruktúrák keretrendszere ~ critical information infrastructure definition, critical information infrastructure defend, Framework for Improving Critical Infrastructure Cybersecurity*

BEVEZETÉS

A XX. század második fele és a XXI. század kétségtelenül az információs társadalom kialakulásáról, (ki)fejlődéséről szól. A számítástechnika őskorával szemben, amikor „csak a bennfentesek" férhettek hozzá informatikai eszközökhöz, mára már szinte nincs olyan része az világnak, területe a társadalomnak, gazdaságnak ahol nem használnánk informatikai eszközöket, ne vennénk igénybe informatikai szolgáltatásokat, ahol nem alakultak ki információs infrastruktúrák vagy informatikai rendszerekkel támogatott infrastruktúrák. E fejlődés hatására közvetve vagy közvetlenül majdnem mindenki felhasználójává, szereplőjévé vált az információs társadalomnak.

Az információs társadalom kialakulásával az informatikai szolgáltatásokat széles körben (fel)használók életének is nélkülözhetetlen részévé vált az információs infrastruktúra által nyújtott szolgáltatások igénybevétele, legyen szó akár az internetről, egy levelező szolgáltatásról, banki szolgáltatásról, egy informatikai infrastruktúrával támogatott közműszolgáltatásról, informatikai eszközzel támogatott gyártósorról, döntéstámogató rendszerek által nyújtott szolgáltatásokról, vagy akár elektronikus adóbevallásról.

A gazdasági, társadalmi élet szempontjából kiemelten fontos azon kritikus információs infrastruktúrák működésének biztosítása, amelyek közvetlen vagy közvetett úton, de jelentős hatással vannak/lehetnek a szolgáltatást igénybe vevők egészségére, biztonságára, védelmére vagy a gazdaság működésére. Ezen kritikus információs infrastruktúrák elérhetőségének csökkenése, működésének zavara, megszűnése sokszor előre nem látható komoly következményekkel járhatnak, szélsőséges esetben akár egy ország gazdasági összeomlásával is.

KRITIKUS INFRASTRUKTÚRÁK, KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK

Kritikus infrastruktúrák, kritikus információs infrastruktúrák fogalma

A kritikus infrastruktúra fogalma az Egyesült Államokban 1998-ban PDD-63 elnöki irányelvben [1] jelent meg először, majd 2001-ben Patriot Act törvényben [2] emelkedett törvényi szintre. A törvényben megfogalmazott definíció szerint kritikus infrastruktúrák „azok a fizikai és virtuális rendszerek, eszközök tartoznak, melyek olyannyira létfontosságúak az Egyesül Államok számára, hogy e rendszerek és eszközök működésképtelensége vagy megsemmisülése gyengítené a védelmet, a nemzeti gazdaságbiztonságát, a nemzeti közegészséget és biztonságot vagy mindezek kombinációját." [2]

Az Európai Unión és az EGK tagországain belül a történelmi, jogi, társadalmi hagyományok hatására egymástól eltérő fogalmak kerültek meghatározásra a törvényhozások részéről. Ugyanakkor a megfogalmazott EU Bizottsági közlemény szerint „a kritikus infrastruktúrákhoz azok a fizikai és információs technológiai berendezések és hálózatok, szolgáltatások és eszközök tartoznak, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a tagállamok kormányainak hatékony működése szempontjából. A kritikus infrastruktúrák több gazdasági ágazatra kiterjednek, többek között a bankügyletekre és pénzügyekre, a szállításra és forgalmazásra, az energiaiparra, a közművekre, az egészségügyre, az élelmiszerellátásra és tájékoztatásra, valamint a kulcsfontosságú állami szolgáltatásokra. Ezen ágazatok néhány kritikus eleme nem tartozik a szigorúan vett „infrastruktúra" fogalmába, de valójában olyan hálózatok vagy ellátási láncok, amelyek valamely alapvető termék vagy szolgáltatás biztosítását támogatják. Például a jelentős városi térségek élelmiszer- vagy vízellátása néhány

kulcsfontosságú létesítménytől függ, ugyanakkor a termelők, feldolgozók, gyártók, forgalmazók és kiskereskedők összetett hálózata is szükséges az ellátás biztosításához."[3]

Magyarországon a 2080/2008 (VI. 30) Korm. határozatával kiadta a „Kormányzati Koordinációs Bizottság javaslatára elfogadja a hazai infrastruktúra létfontosságú elemeinek védelméhez kapcsolódó további konzultációk alapjául a nemzeti programról szóló Zöld Könyvet"[4], amelyet 2012-ben felváltott a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (továbbiakban: Lrtv.) [5], valamint a törvény végrehajtására kiadott 65/2013 (III. 8.) kormányrendelet [6].

A törvény és a kapcsolódó kormányrendelet a kritikus infrastruktúra kifejezés helyett bevezette a létfontosságú rendszert, mint kifejezést és megfogalmazta ezen infrastruktúrák fogalomrendszerét, amely némileg eltér az EU Bizottsági közleményben, illetve a Zöld Könyvben megfogalmazottaktól, de lényegét tekintve megegyezik azzal:

- európai létfontosságú rendszerelem: az Lrtv. alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne - az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve - legalább két EGT-államra,
- létfontosságú rendszerelem: az Lrtv. 1-3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához -, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna,
- nemzeti létfontosságú rendszerelem: az Lrtv. alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt jelentős hatása lenne Magyarországon,

illetve meghatározta a kritikus infrastruktúra védelmének fogalmát is:

- létfontosságú rendszerelem védelme: a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység. [5]

A végrehajtási rendeletben újdonságként megjelent a kritikus információs infrastruktúra fogalma:

- létfontosságú információs rendszer és létesítmény: a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.[6]

A törvény rendelkezik a kijelölés folyamatáról, visszavonásáról, a kijelölésben érintett és a kritikus infrastruktúrát üzemeltető szervezetek feladatairól, valamint az ágazati, alágazati besorolásról. A kormányrendelet pontosan megnevezi az azonosításban, kijelölésben, kijelölés visszavonásában közreműködő szervezeteket, rendelkezik az üzemeltetési biztonsági tervről, az ellenőrzés rendjéről, a kritikus infrastruktúrák nyilvántartásával kapcsolatos feladatokról.

A létfontosságú rendszerek kijelölési folyamata bizonyos ágazatok esetében már elindult, azonban jó néhány ágazat esetében nem történt meg az ágazati szabályzó kiadása, így annak ellenére nem történtek meg a kritikus infrastruktúra elemek kijelölése, hogy a kormányrendelet már meghatározta a kijelölésnél figyelembe veendő horizontális kritériumokat is.

A kritikus információs rendszerek védelmének megteremtése érdekében fontos előrelépés volt az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) [7], valamint a végrehajtására kiadott 77/2013 (XII.19.) NFM rendelet.[8] Az Ibtv. 2.§ (2) c) pontja az Ibtv. alapján, az Ibtv. hatálya kiterjed „…az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján

kijelölt rendszerelemek…”-re. Az Ibtv. törvény rendelkezik a törvény hatálya alá tartozó rendszerek biztonsági osztályba sorolásáról, a törvény hatálya alá tartozó rendszerrel rendelkező szervezetek biztonsági szintjéről, a rendszereket üzemeltető szervezetek feladatairól, az állami felügyeleti rendszerről, valamint az eseménykezelés rendszeréről. A végrehajtási rendelet többek között részletesen szabályozza kijelölési folyamatot, a szervezet biztonsági szintbe sorolását, valamint a szervezet üzemeltetésében lévő rendszerek biztonsági osztályba sorolását, illetve az egyes osztályokhoz tartozó szervezeti, szabályozói, biztonsági megfelelési követelményeket. A követelményjegyzék alapját –megítélésem szerint - a NIST 800-53 publikációja [9] adja, amely az informatikai rendszerek biztonsági és adatvédelmi kontrolljait tartalmazza. A NIST által publikált kontrolljegyzék folyamatosan frissül a kor kihívásainak megfelelően, amelyet szükséges lenne a hazai szabályozásnak is tükröznie.

A NIST 800-53 H. melléklete tartalmazza az ISO/IEC 27001, valamint az ISO/IEC 15408 szabványokkal való megfeleltetést, ami segítséget nyújthat az információs szabványok, ajánlások közötti átjárásban, a meglévő megfelelőségek fenntartásában.

A kritikus információ infrastruktúrák védelmének keretrendszere

Az USA elnökének 13636 számú elnöki rendeletében [10] kapott feladat alapján a NIST kidolgozta és 2014 februárjában kiadta a kritikus infrastruktúrák informatikai biztonsági szintjének növelése érdekében használható keretrendszerét (Framework for Improving Critical Infrastructure Cybersecurity).[11]

A keretrendszer a kormányzati és a magánszektor közös termékként született meg, ágazat és technológia független módon, így könnyítve meg az alkalmazhatóságát és szükség szerinti fejlesztését.

A keretrendszer használata nem kötelező jellegű, és nem váltja ki a szervezetnél alkalmazott információbiztonsági és kockázatmenedzsment folyamatokat, de a benne megfogalmazottak segíthetek

- a szervezet aktuális biztonsági szintjének megállapításban,
- a szervezet információbiztonsági céljának megfogalmazásában,
- folyamatosan és ismétlődő módon azonosítani és rangsorolni a fejlesztési lehetőségek,
- a szervezet céljának eléréséhez szükséges lépések meghatározásában,
- a kommunikációban a külső és belső érdekeltek irányába információbiztonsági kockázatok vonatkozásában.

A keretrendszer kockázatalapú megközelítéssel a kritikus infrastruktúrák teljes védelmi életciklusával kapcsolatban tesz javaslatot. A keretrendszer részei erősítik a kapcsolatot az üzleti célok és a biztonsági célok vonatkozásában.

A keretrendszer három fő részből áll:

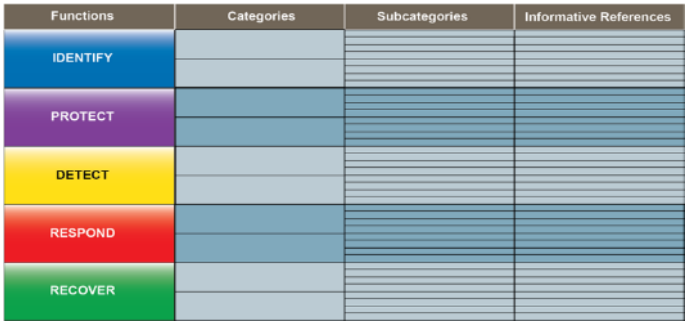
1. Keretrendszer központi része, magja (Framework Core): tartalmazza azokat a védelmi intézkedéseket, amely egy biztonsági cél eléréséhez szükségesek. A védelmi intézkedések nem teljes körűek, így nem tekinthető ellenőrzési listának. A keretrendszer központi része négy szintre osztja az információbiztonsági tevékenységeket: Alapfunkciók (Function), Feladatcsoportok (Category), Feladatok (Subcategory) és a Referencia irányelvek, gyakorlatok, hivatkozások (ISO, NIST 800, COBIT, ISA, CCS). A mag öt Alapfunkciót tartalmaz: Megismerés, Védelem, Esemény észlelés, Esemény kezelés, Helyreállítás, amely lefedi a rendszer teljes információbiztonsági életciklusát.
2. Keretrendszer besorolási szint (Framework Triers): a szintek megmutatják, hogy a szervezet biztonsági elgondolása, koncepciója és a tényleges gyakorlat milyen viszonyban van egymással. A négyszintű besorolás az ad-hoc, nem szervezett védelmi tevékenységtől a legjobb gyakorlatot alkalmazó, proaktív megoldásokat megvalósító védelmi szintig tart. Magasabb védelmi szintre történő lépés nem minden esetben

szükséges a szervezet számára és nem mindig költséghatékony és védelemarányos. A besorolási szint nem jelent egyben érettségi szintet is.

3. A hazai szabályozás 5 szintű besorolást határoz meg, ami miatt a keretrendszer implementációja során mindenképpen szükséges a keretrendszer hazai szabályzókhoz történő igazítása.
4. Keretrendszer profilja (Framework Profile): a profil a szabványok, iránymutatások, gyakorlatok testre szabása az adott szervezetre. A pillanatnyi állapot megmutatja azon eredményeket, amelyek az üzleti igényeknek megfelelően eddig meg lettek valósítva. Egy jelenbeli és egy kívánt profil összehasonlítása segítséget nyújthat, hogy a szervezet hatékonyan meghatározza azon prioritásokat, amellyel hatékonyan el tud jutni egy jövőbeni tervezett biztonsági állapotba, figyelembe véve az üzleti elvárásokat, a szervezet kockázattűrő képességét, a rendelkezésre álló erőforrásokat.

Keretrendszer központi rész (mag)

A keretrendszer központi része által meghatározott folyamatok kiterjednek a teljes védelmi életciklusra:



1. ábra. A keretrendszer magja

- Megismerés (Identify): a keretrendszer hatékony működtetésének legfontosabb része. Az üzleti környezet, az infrastruktúrát támogató elemek, veszélyforrások megismerésével a szervezet képes az üzleti igények és a kockázatmenedzsment stratégia figyelembevételével hatékonyan priorizálni információbiztonsági tevékenységeit. A funkció részei: erőforrás kezelés, üzleti környezet, szabályozás, kockázatelemzés, kockázatmenedzsment stratégia
- Védelem (Protect): ezen folyamathoz tartozó tevékenységek segítenek a megfelelő védelem kialakításába annak érdekében, hogy a veszélyforrások ne váljanak eseménnyé. Ezen funkció része a hozzáférés kezelés, oktatás, tudatosítás, adatbiztonság, információbiztonsági eljárások, folyamatok, üzemeltetési feladatok, védelmi technológiák
- Esemény észlelés (Detect): ezen folyamathoz tartozó tevékenységek segítenek a időben felfedezni az információbiztonsági eseményeket. A funkció része az anomáliák-, események jelzése, folyamatos biztonsági monitorozás, esemény felismerési technikák
- Esemény kezelés (Respond): ezen folyamathoz tartozó tevékenységek segítenek a biztonsági eseményre adott válasz előkészítésében. A funkció része a válasz tervezése, kommunikációs terv, esemény elemzése, kezelése, és a javítási tevékenységek
- Helyreállítás (Recover): ezen funkcióhoz tartozó tevékenységek segítenek egy esemény utáni hatékony visszaállás megvalósításában. A funkció része visszaállítási terv, tapasztalatok alapján szükséges javítások és a kommunikáció

Az egyes folyamatok kapcsolatban vannak egymással, de valamennyi folyamat önálló és önmagában is változhat. Az egyes Alapfolyamatok, Feladatcsoportok, Feladatok, Alkalmazott irányelvek változása magával hozhat más elemben történő változtatást is.

Keretrendszer besorolási szintje

A besorolási szint megmutatja, hogy az adott szervezet milyen szinten van az információbiztonsági kockázatok kezelésében, illetve az információ biztonsági kockázat menedzsment mennyire fejlett és hogyan illeszkedik a szervezet kockázatmenedzsment rendszeréhez. Magasabb szint elérése csökkentheti a szervezet információbiztonsági kockázati szintjét és költséghatékonyabbá tudja tenni a kockázatmenedzsmentet. A keretrendszer négy szintet különböztet meg, melynek jellemzői:

1. szint Részleges (Partial): nincs formalizált kockázat menedzsment, a kockázatok kezelése ad-hoc módon történik, a védelmi tevékenységek nincsenek összehangolva az üzleti igényekkel, valamint a fenyegetettségekkel. Nincs szervezeti szintű információbiztonsági tudatosító tevékenység, nincs egységes kockázatmenedzsment. A kockázatok kezelése a résztvevők korábbi tapasztalata és a külső források alapján történik.

2. szint Formális kockázatkezelés (Risk Informed): a vezetőség által el van fogadva kockázatkezelési gyakorlat, de nincs a teljes szervezetre kiterjesztve. A védelmi intézkedések sorrendje a szervezeti kockázatoktól, a fenyegetettségi környezettől, vagy az üzleti igényektől függ. Van vállalati szintű információbiztonsági tudatosítás, de nincs kialakítva szervezeti szintű kockázat kezelés. A kockázatkezelésnek elfogadott folyamata van és a szervezet megfelelő erőforrással rendelkezik a kockázatok kezelésére. Az egyes szervezeti egységek között van kommunikáció az informatikai kockázatok vonatkozásában. A szervezet ismeri az elterjedt szabályokat, de nincs formalizált eljárás a külső partnerekkel történő interakcióra, az információ megosztására.

3. szint Megismételhető (Repeatable): a szervezet kockázatmenedzsment folyamata formálisan el van fogadva és ki van terjesztve. Az üzleti és technológia változások miatt módosítások rendszeresen megtörténnek. Az informatikai kockázatmenedzsment vállalti szinten működik. A kockázati információs szabályok, eljárások, folyamatok definiálva és implementálva vannak, valamint megtörténik a felülvizsgálatuk is. Következetes metódusok állnak rendelkezésre, hogy hatékonyan lehessen reagálni a kockázatok változására. A szervezet ismeri a függőségeit, a partnereitől megkapja a szükséges információkat a kockázat alapú döntésekhez, eseménykezeléshez.

4. szint Adaptív (Adaptive): a szervezet informatikai védelmi gyakorlata a tapasztalatokon, a korábbi és a jelenlegi védelmi aktivitásokból származó előrejelző indikátorokon alapul. A fejlett technológiák és gyakorlatok alkalmazkodásával a folyamatos fejlődés lehetővé teszi a szervezet számára, hogy aktívan tudjon alkalmazkodni a változó biztonsági környezethez és időben tudjon reagálni a kifinomult fenyegetésekre. Szervezeti szintű kockázatmenedzsment megközelítés, alkalmazott kockázat információs folyamatok, eljárások segítenek a potenciális események kezelésében. Az információbiztonsági kockázatok kezelése része a vállalati kultúrának, amely a korábbi tevékenységek tudatosításából, az egyéb forrásból származó információkból és a szervezet rendszereivel, hálózatával kapcsolatos folyamatos információból származik. A szervezet az információbiztonsági esemény bekövetkezése előtt is folyamatosan megosztja partnereivel a kockázatokat és tevékenységét és a szervezet is megkapja az információkat, amelyek szükségesek az információbiztonsági szintjének növeléséhez.

Keretrendszer profil

A profil a keretrendszer magjának segítségével leírja a szervezet milyen szinten áll az információbiztonság területén, mely védelmi intézkedések működnek és melyek nem. A profil lehetőséget biztosít egy jövőbeli, elérendő állapot definiálására. A profil kialakításához a Alapfolyamatokon, Feladatcsoportokon és Feladatokon keresztül a referencia irányelveknek történő megfelelés vagy nem megfelelés nyújt segítséget. A profilok összehasonlítása az üzleti igények, a kockázatok és a fenyegetési környezet segítségével lehetőséget biztosít a kockázatarányos és költséghatékony információbiztonsági védelmi rendszer kialakításához.

Keretrendszer alkalmazása a hazai jogszabályok tükrében

A keretrendszer leírásában többször szerepel, hogy a dokumentum egy általános, fakultatívan bevezethető, szektorokon átnyúló és a keretrendszert alkalmazó szervezetek számára testre szabandó rendszer. A keretrendszer testre szabásával, adoptálásával a hazai szervezetek is ki tudják alakítani az Ibtv.-ben és a végrehajtási utasításában megfogalmazott jogszabályi elvárásokat.

Az Ibtv. és a végrehajtási rendeletének segítségével a kritikus információs infrastruktúrát üzemeltető szervezet – figyelembe véve a szervezet kockázattűrő képességét – meghatározhatja az informatikai rendszer elvárt biztonsági szintjét. A biztonsági szint meghatározását követően a szervezet fel tudja mérni pillanatnyi profilját, valamint meg tudja határozni az elérendő célját, amihez segítséget nyújthat a 77/2013. NFM rendelet, illetve a keretrendszer magjában felsorolt referenciák, irányelvek.

A pillanatnyi helyzet felmérése során pontos képet kaphat a felsővezetés a szervezet aktuális biztonsági szintjéről, világosan láthatóvá válik, hogy mely területek felelnek meg az adott biztonsági szint elvárásainak és mely területeken szükséges további intézkedések meghozatala, figyelembe véve a szervezet erőforrásait. A felmérés során feltárt hiányosságok kockázatainak feltárása segítséget nyújthat a meghozatandó intézkedések priorizálásában, a kockázat arányos védelem kialakításában. Az intézkedések priorizálása segíthet a kockázatarányos védelem kialakítására, a szervezet anyagi és egyéb erőforrásai által biztosított keret függvényében.

Ugyanakkor a keretrendszer csak egy részét képezi a szervezeti információbiztonsági tevékenységének, annak csak egy jól integrálható részének kezeléséhez ad iránymutatást. A további információbiztonsági tevékenységeket a szervezetnek továbbra is működtetni, fejleszteni kel.

Fontos megjegyezni továbbá, hogy a magyar szabályozás vélhetően nem tudja, nem fogja tudni követni a NIST 800-53 és egyéb szabványok módosításait, ezért abban az esetben, ha a szervezetet nem csak a jogszabályi elvárásoknak szeretne megfelelni, hanem tényleges kockázatarányos információbiztonságot szeretne megvalósítani mindenképpen szükséges a szervezet informatikai infrastruktúrájának megfelelően figyelemmel kísérni nemzetközi szervezetek (pl. ISO/IEC, NIST) által kiadott szabványokat, ajánlásokat.

ÖSSZEGZÉS

A kritikus infrastruktúrák és kritikus információs infrastruktúrák megfelelő szintű védelme elengedhetetlen a társadalom, a gazdaság, a védelmi szektor működéséhez. Az infrastruktúrák működési zavarai, kiesése jelentős hatással lehetnek a mindennapi életre, a társadalom-, gazdaság működésére. A kritikus infrastruktúrákat érintő fenyegetések növekedésével párhuzamosan, egyre nagyobb figyelem irányult ezen rendszerek információbiztonsági állapotára.

Nemzetközi és hazai szinten is megszülettek azon szabványok, szabályzók, amelyek nélkül az egyenszilárdságú információbiztonsági szint elérése lehetetlen. Kormányzati szinten létrehozásra kerültek azon szervezetek, amelyek ágazati szinten belül, ágazatokon és országhatárokon átnyúlóan tudja koordinálni az infrastruktúrák információbiztonsági védelmét.

Az egyes országok, szabványügyi szervezetek és egyéb szervezetek által kidolgozott módszerek, keretrendszerek alkalmasak lehetnek egy – a szervezet számára optimális – információbiztonsági rendszer kialakítására, a már meglévő rendszer fejlesztésére.

Felhasznált irodalom

[1] PRESIDENTIAL DECISION DIRECTIVE/NSC-63
http://fas.org/irp/offdocs/pdd/pdd-63.htm (letöltés: 2014.10.10.)

[2] US Patriot Act, 1016(e) Public Law 107-56 (42 U.S.C. 5195c(e))

[3] Communication from the Commission to the Council and the European Parliament, Brussels, 20.10.2004. COM(2004) 702 Final, Critical Infrastructure Protection in the fight against terrorism

[4] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[5] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[6] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

[7] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szóló

[8] 77/2013 (XII.19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

[9] NIST Special Publication 800-53 revision 4 Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (letöltve: 2014.10.12.)

[10] Executive Order -- Improving Critical Infrastructure Cybersecurity http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (letöltve: 2014.10.14)

[11] NIST Cybersecurity Framework http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (letöltve: 2014.10.30.)