Műszaki Tudományos Közlemények vol. 9. (2018) 215–218.
https://doi.org/10.33895/mtk-2018.09.49,
https://eda.eme.ro/handle/10598/30333
Angol nyelven: https://doi.org/10.33894/mtk-2018.09.49

A NYUGDÍJFOLYÓSÍTÁS MINT KRITIKUS INFRASTRUKTÚRA

PENSION PAYMENT AS A CRITICAL INFRASTRUCTURE

Szabó Zsolt Mihály

Óbudai Egyetem, Biztonságtudományi Doktori Iskola, H-1081 Magyarország, Budapest, Népszínház utca 8. fszt., +36-1-666-5375, zsolt@tamiyary.hu

Abstract

Today, the state, its organizations and its citizens have become vulnerable to the complexity of complex electronic information systems in the cyber space of Hungary, without which state operations and the provision and use of different services become unworkable. In addition to the modern economic system, society is not prepared to operate without lost infrastructures, assets or services, so they must be protected - clearly - in particular that the information used and generated in their operation and the data managed there are significant assets represent.

***Keywords**: pension payments, retirement security, information security, IT security, threats and risks.*

Összefoglalás

Napjainkban az állam, annak minden szervezete valamint polgára kiszolgáltatottá vált a többszörösen összetett elektronikus információs rendszereknek Magyarország kiberterében, amelyek nélkül az állami működés, különböző szolgáltatások biztosítása és igénybevétele megvalósíthatatlanná válik. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket - egyértelműen - védeni kell, különös tekintettel arra, hogy azok működése során felhasznált és keletkező információk, továbbá az azokban kezelt adatok jelentős vagyont képviselnek.

***Kulcsszavak:** nyugdíjfolyósítás, nyugdíjbiztonság, információbiztonság, informatikai biztonság, fenyegetettségek és kockázatok.*

1. Bevezetés

Biztonság alatt azt az állapotot értjük, amelyben a szervezet számára fontos tevékenységek zavartalanul végezhetők.

A szervezeti tevékenységek biztonságát szavatoló rendszereknek le kell fednie minden olyan tevékenységet, amelyet a szervezeti stratégia érint [1].

A szervezeti és az informatikai biztonsági stratégia együtt garantálja a biztonság teljeskörűségét és egységes szintjét. Az informatikai biztonsági rendszernek olyan megoldásokra van szüksége, amelyek a biztonsági követelményeket a lehető legkisebb, már elfogadott maradványkockázattal elégítik ki [4].

A támadások célja alapvetően az adat, melyet különböző rendszerelemek vesznek körül, folyamatok kezelnek. A kiber fenyegetettségek a rendszerelemek meghatározott láncán keresztül az adatokat és azokat kezelő folyamatokat veszélyeztetik [7].

2. Kritikus infrastruktúra

A Belügyminisztérium alá tartozó Országos Katasztrófavédelmi Főigazgatóság hónlapján található meg kritikus infrastruktúra általános fogalma, azaz egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtő, a gazdaság működését elősegítő vagy lehetővé tévő azon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége vagy ezek részei, amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire negatív hatással jár [12].

A fentiek alapján meghatározható a kritikus infrastruktúra egy lehetséges hazai definíciója: egymással összekapcsolódó, interaktív (egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózata), az ország működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű biztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában [2].

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK tanácsi irányelvet (irányelv) tagállami kötelezettségünk átültetni a hazai jogrendszerbe [11]. Ezen jogharmonizációs kötelezettség mentén tagállami szinten meg kell hozni azokat az intézkedéseket, amelyek beültetik az irányelvet a magyar jogrendszerbe. A 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről [10], mely f) pontja leírja mely ágazatokat kell létfontosságú rendszerelemként tekinteni. A 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.

Az említett törvény 2. melléklet a 2012. évi CLXVI. törvényhez 16b része szól a társadalombiztosítási ágazatról. A társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások a létfontosságú rendszerek közé tartozik. Így a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról iránymutatásait figyelembe kell venni [10]. A Kormányrendelet alapján 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.

Továbbá kockázatelemzés kell végezni: fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából [2]. Egy lehetséges eljárás lehet a CRAMM (CCTA Risk Analysis and Management Method) alapú módszertan [6] [8], amely a MeH ITB 8. számú ajánlás (Informatikai biztonsági módszertani kézikönyv) átvett és az egyik legelfogadottabb metodológia napjainkban. Ez a módszer leírja a számítástechnikai rendszerek sebezhető pontjait, és javaslatokat tesz ellenintézkedésekre [3] [4].

3. Kritikus infrastruktúra védelme

A kritikus infrastruktúra védelme (KIV) a mai kor kihívása, amely a globális terro-

rizmus terjedésével került a figyelem fókuszába világszerte. A kritikusnak minősített infrastruktúrák azok, amelyeknek köszönhetően tud alapvetően működni egy társadalom, egy gazdaság. A védelem különösen fontos ma, az ún. negyedik generációs (4GW) vagy aszimmetrikus hadviselés korában, amikor információs hadviselési eszközökkel szinte bármely érdekcsoport tudja érdekeit érvényesíteni, nála jóval nagyobb ellenfelével – tipikusan nemzetállamokkal – szemben. Ezen támadások fő célpontjai a kritikus infrastruktúrák (KI), különösen a kritikus információs infrastruktúrák (KII) [5]. Kritikusinfrastruktúra-elemek segítségével tartja nyilván állampolgárai adatait az állam, ezek igénybevételével működik a közigazgatás (nem csak az e-közigazgatás), és ezek segítségével nyújt az állam (nem csak e-kormányzati) szolgáltatásokat. Ezek védelme tehát jórészt állami feladat, a védelem megszervezése pedig kifejezetten az. Állami feladat már csak azért is, mivel az állam maga is ezekre az infrastruktúrákra támaszkodik [12]. Egy ilyen kritikusinfrastruktúra-elem bármilyen okból történő kiesése pedig gyakorlatilag káoszba, anarchiába tudja sodorni az adott nemzetállamot. Ezért a feladatok pontos végrehajtására, a védelem folyamatos fenntartására kell az államnak koncentrálnia.

2012. évi CLXVI. törvény e) pontja alapján, mely a létfontosságú rendszerelem védelmét alábbiak szerint határozza meg: a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység [10].

4. Nyugdíjfolyósító, mint létfontosságú rendszer védelme

Az **1. táblázat** mutatja, hogy nyugdíjfolyósítási informatikai rendszer és a hozzá kapcsolódó rendszerek (folyamatok) kárhatás-elemzés alapján kiemelt fontosságúak (kritikusak) a szervezet működése számára [6] [7].

1. táblázat. *Példa a magas prioritású folyamatokra*

Folyamat (Rendszer) Neve	Rendszer prioritás szint	Elhárítási idő
Nyugdíjfolyósítási informatikai rendszer	5 (Kritikus)	4 óra
Nyugdíjfolyósítási adatok lekérdező rendszer	5 (Kritikus)	4 óra
Nyugdíjelbírálás	5(Kritikus)	4 óra
Iktatási rendszer	5(Kritikus)	4 óra

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról írja elő, hogy az állami szervek informatikai rendszerének képesnek kell lennie a szervezet működése szempontjából meghatározó hardver– és szoftvereszközök kritikus biztonsági eseményeinek megfigyelésére és naplózására, illetve ezen események automatizált kezelésére [9]. Egy állami szervezet informatikai rendszerének és biztonsági menedzsmentjének kialakításakor a fenti követelményeken túl fontos, hogy a biztonsági rendszerben egyszerűen legyen leképezhető és ellenőrizhető a szervezet biztonságpolitikájának megvalósítása [1]. A biztonsági menedzsmentnek legyen szerves része a hálózat-, felhasználó-, szoftver-, tűzfalmenedzsment, a levelező rendszer tartalomszűrése, vírusvédelme és egyéb más informatikai rendszerek. Az információbiztonság három alapvető követelmény (bizalmassága, sértetlensége, rendelkezésre állás) együttes teljesülése esetén valósítható meg. Ez a három követelmény az információkkal kapcsolatos [3]. Ha ezek a követelmények nem teljesülnek, elveszhet, sérülhet az IT rendszer, illetve az általa kezelt adatok:

– Bizalmassága: az információt más is megismerheti, mint aki jogosult;
– Sértetlensége: az információ átadása során megváltozhat;
– Rendelkezésre állás funkcionalitása: az információ kellő időben nem hozzáférhető.

Egy nagyobb szervezetnél adminisztratív védelemnek szervezeti és rendszerszintekre tagolt hierarchikus szerkezetét kell kialakítani.

5. Következtetések

A komplex informatikai biztonság átgondolt tervezése egyrészt meghatározza a rendelkezésre álló informatikai erőforrásokkal és befektetésekkel kapcsolatos főbb igényeket, másrészt megadja azt a keretet, amelyben a súlypontok és a megvalósításra vonatkozó felelősségek kijelölése, valamint az erőforrások kulcsterületekre való koncentrálása történik. Kizárólag a részletes előzetes tervezés biztosítja, hogy az informatikában rejlő valamennyi lehetőséget kihasználhassuk a szervezet törekvéseinek és céljainak támogatására. A tervezés feladata biztosítani, hogy az alkalmazni kívánt megoldások az adott pénzügyi keretek közé illeszthetők, műszakilag megvalósíthatók, megfelelő kontroll alatt tarthatók és minden érintett számára értelmezhetők legyenek.

Szakirodalmi hivatkozások

[1] Michelberger, P., Lábodi, Cs. (2012): *Vállalati információbiztonság szervezése.* In Nagy Imre Zoltán (szerk.), Vállalkozásfejlesztés a XXI. században II. Tanulmánykötet, Óbudai Egyetem. 241–302.

[2] Mógor, T., Rajnai Z. (2014): *Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása*, Bolyai Szemle, 33/2, 2014, 43–59.

[3] Muha, L., Krasznay, Cs. (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest. NKE Vezető- és Továbbképzési Intézet. 1–120.

[4] Répás, S., Dalicsek, I. (2015): *Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében.* A NKE állam- és közigazgatás-tudományi szakmai folyóirata 2015. 4. 22–33.

[5] Sik, Z. N. (2011): *A kritikus információs infrastruktúra védelme és a közigazgatás*. Vezetéstudomány XLII. ÉVF. 2011. 3. szám. ISSN 0133-0179 42–47.

[6] Szabó, Zs. M. (2017): *A nyugdíjfolyósítás információbiztonsági és informatikai biztonsági kérdései.* In: Bitay Enikő (szerk.) A XXII. FMTÜ előadásai: Proceedings of the XXII-th International Scientific Conference of Young Engineers. 2017. 363–366.

[7] Szabó, Zs. M. (2017): *A nyugdíjfolyósítás kiberbiztonsági kérdései*. In: Ács K, Bódog F, Mechler M, Mészáros O, Pónusz R. (szerk.) VI. IDK2017. Tanulmánykötet 507–517.

[8] Szádeczky, T. (2014): *Információbiztonsági szabványok.* NKE. Budapest. 1-50.

[9] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.). Magyar közlöny 2013. évi 68. sz. 50241–50255.

[10] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv.). Magyar közlöny 2013. évi 40. sz. 4043–4051.

[11] A Tanács 2008/114/EK Irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (EGT-vonatkozású szöveg) Európai Unió Hivatalos Lapja. 1–8.

[12] Katasztrófavédelmi Oktatási Központ (2013): Létfontosságú Rendszerek és Létesítmények Védelme. 1–19.