Váczi Dániel

Az emberi tényezõ kockázatainak modellezési lehetõsége Fuzzy-logikával a vasútnál, mint kritikus infrastruktúrában[1]

DOI 10.17047/HADTUD.2019.29.3.80

A kiberbiztonsági kockázatok feltérképezésére használt módszerek csak részben tárják fel a valóságot, a célzott támadások ellen kevésbé hatékonyak. A cikk a magyarországi vasúti informatikai infrastruktúra példáján tárja fel egy pontosabb számítási módszer lehetõségét a Fuzzy-logika alkalmazásával.

Napjaink egyik legnagyobb kiberbiztonsági problémája, hogy az internet, a mobil eszközök, a közösségi média elterjedésével mindenki potenciális áldozatává vált a kibertámadásoknak. Igaz ez közvetve a társadalom offline részére is, hiszen a velük kapcsolatban élõ online világ õket is kitetté teszi. Naponta különbözõ minõségû és típusú támadásnak esik áldozatul számtalan eszköz és azokkal együtt a használójuk, tulajdonosuk. A biztonsági szakma pedig úgy próbál meg védekezni, hogy kontrolljaival, eszközeivel, megoldásaival minél nagyobb területet kísérel meg lefedni a potenciális fenyegetettségek kivédésére. Mindezt teszi úgy, hogy általánosságban a kockázatarányosságának elve alapján próbálja megjósolni, hogy adott fenyegetettség milyen valószínûséggel fog bekövetkezni.

Egy cég vagy állami szereplõ saját belsõ erõforrásai segítségével, esetleg egy tanácsadó cég által kidolgozott módszertan alapján, figyelembe véve az éppen aktuális trendeket, megpróbál egy lépést tenni a biztonság növelése érdekében. A probléma az, hogy ezzel nem valósul meg valódi kockázatarányos védelem. Tudomásul kell venni, hogy a szakma által folyton hangoztatott, szinte szállóigévé váló mondat (ti. mindig az ember a leggyengébb láncszem) nem csak egy hangzatos hívó szó. Az általános támadások elleni védekezésre megoldást nyújthatnak a korábbi módszerek, azonban a célzott támadások ellen kevésbé hatásosak. A személyre szabott módszerekben kódolva van a siker.

---

1 A publikáció alapjául szolgáló kutatás a „Integrált Intelligens Vasútfelügyeleti Rendszer kifejlesztése” címû projekt keretében zajlott. (Pályázati azonosító: GINOP-2.2.1-15-2017-00098)

A cikkben a szerzõ a kockázatarányosság egy, a szokásostól eltérõ dimenziójú és módszerû irányával foglalkozik. Célja, hogy kutatásával a valósághoz minél közelebbi kép tárulhasson a biztonsági rendszereket tervezõ szakemberek elé. A kutatás szemléltetése érdekében a magyarországi vasúti infrastruktúrát választotta, mivel annak összetettsége, rétegzõdése és különbözõ felelõsségi körei alapvetõen megnehezítik a kockázatok megfelelõ rendszerszintû azonosítását.

A kutatás alapjául a szerzõ azon feltételezése szolgál, miszerint létezik olyan matematikai (Fuzzy-logika alapján mûködõ) algoritmus, mely segítségével meghatározható az adott kritikus infrastruktúránál dolgozó azon személyeknek a köre, akik kiemelten veszélyeztetettek információbiztonság szempontjából. Ezért számukra az átlagosnál komolyabb védelemre, magasabb információbiztonsági tudatossági képzésre van szükség, hiszen nagyobb valószínûséggel lesznek egy célzott támadás áldozatai.

A kibertér fenyegetettségei a kritikus infrastruktúrák szemszögében

A kritikus infrastruktúrák, létfontosságú rendszerelemek védelmével kapcsolatban mind hazai, mind nemzetközi szinten számos jogszabály foglalkozik. A társadalom számára fontos objektumok kiválasztása és azoknak a védelme a 2001. szeptember 11-ei terrortámadás után egy magasabb szintre került[2] világszerte. A tragikus esemény után elõször az Amerikai Egyesült Államok emelte törvényi szintre[3] az 1998-ban lefektetett elnöki direktívát.[4] A különbözõ nemzetállamok a saját szabályozásuk alapjául tekintettek erre a jogszabályra és ezt emelték be jogrendjükbe, a saját igényeikre szabva.[5] Nemcsak nemzetállami szinten történtek szabályozások. Többek között az Európai Unió szintén kiadta 2005-ben a kritikus infrastruktúrák védelmérõl szóló Zöld Könyvet.[6]

Meghatározták azokat a területeket, melyek kiesése az egész társadalomra vagy annak nagy részére hatással lennének. A kiemelt területek az energetika, az információtechnológia, a telekommunikáció, a kémiai anyagok és vegyi üzemek, a közlekedési rendszerek, a vészhelyzeti mentõszervek, a mezõgazdaság és élelmiszeripar, a közegészségügy, a vízellátás, a banki és pénzügyi szektor, a nemzeti emlékmûvek, valamint a védelmi szféra.[7] A magyarországi szabályzó,[8] a *2012. évi CLXVI. törvény*

---

2 Horváth Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. Fejezetek a kritikus infrastruktúra védelembõl. Magyar Hadtudományi Társaság, Budapest, 2013., ISBN 9789630869263, http://mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf (Letöltés ideje: 2018. 05. 12.) p. 22.

3 Egyesült Államok. Uniting and Strengthening America, by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001-es 107-56-os törvény, 1016-os szekció, más nevén a Kritikus Infrastruktúrák védelmérõl szóló 2001-es törvény, https://www.selectagents.gov/resources/USApatriotAct.pdf (Letöltés ideje: 2018. 11. 10.)

4 PPD 63 – 1998. május 22. Protecting America's critical infrastructures, https://fas.org/irp/offdocs/pdd/pdd-63.htm (Letöltés ideje: 2018. 11. 10.)

5 Szádeczky Tamás: Information Security Law and Strategy in Hungary. Academic and Applied Research in Military and Public Management Science 14: (4) 2015, ISSN 2064-0021

6 A Tanács 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelölésérõl, valamint védelmük javítása szükségességének értékelésérõl, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32008L0114 (Letöltés ideje: 2018. 11. 10.)

a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelmérõl, 1. mellékletében is gyakorlatilag ezek az ágazatok szerepelnek.

A felsorolt ágazatok nagy része önmagában informatikavezérelt, legyen szó internetre publikált szolgáltatásokról, vagy az erõmûvekben található SCADA-rendszerekrõl. Kiberbiztonsági szempontból azonban az információs társadalom információtechnológiák általi kiszolgáltatottsága miatt[9] nélkülözhetetlenek az úgynevezett kritikus információs infrastruktúrák. Ezek védelmének kialakítása még inkább szükséges. A Zöld Könyv szerint a meghatározás pontosan így szól: *„… kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minõsülnek, vagy az infrastruktúrák mûködése szempontjából fontosak (például távközlés, számítógép hardver/szoftver, internet, mûholdak stb.)”.*[10]

A változást látva nemcsak a jogi szakma kezdett el foglalkozni koncentráltabban a témával, hanem a gazdasági, a biztonságpolitikai és természetesen az informatika egyre szélesebb körû térnyerésével a technológiai, IT-szakmai is[11] jelentõs erõforrásokat fektetnek a biztonságosabbá tételbe.

Számos problémának a megoldása foglalkoztatja ezeknek a létesítményeknek a védelméért felelõs személyeket. Legyen szó az információs társadalom által generált új szociológiai jelenségekrõl (például a közösségi médiában az életüket megosztó munkatársak kezelése), a mobil eszközök által okozott fenyegetések (például GPS-jeleket folyamatosan rögzítõ sérülékeny mobilalkalmazások), esetleg azoknak az ipari eszközöknek a védelmérõl, melyeket a könnyebb kezelhetõség miatt rákötnek védettnek hitt hálózatra megfelelõ védelem nélkül. Az egyik megoldandó probléma, hogy valódi kockázatarányos védelmet lehessen kialakítani, mely során mind a technikai támadási lehetõségeket, mind a humán faktort megfelelõen figyelembe veszik.

Ahhoz, hogy egy személyrõl megállapítható legyen potenciálisan, milyen kibervészélyeknek van kitéve, azaz milyen fenyegetettségi szinten van, minimum a következõ befolyásoló tényezõket kell figyelembe venni:

- életkora,
- generációs jellemzõi,
- alaptermészete,
- szociális helyzete,
- zsarolhatósága,
- céges pozíciója,
- a társadalomban betöltött helye,
- a szociális hálóban betöltött szerepe,

---

7 Haig Zsolt – Hajnal Béla – Kovács László – Muha Lajos – Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. Budapest, ENO Advisory Kft., http://www.certhungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf (Letöltés ideje: 2018. 05. 12.)

8 Szádeczky Tamás: Az IT biztonság szabályozásának konfliktusa. Infokommunikáció és jog. 2013. X. évf. 56. sz. ISSN 1786-0776

9 Horváth Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. Fejezetek a kritikus infrastruktúra védelemből. Magyar Hadtudományi Társaság, Budapest, 2013., ISBN 9789630869263, http://mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf (Letöltés ideje: 2018. 05. 12.) pp. 28–35.

10 Kovács László: Kritikus információs infrastruktúrák Magyarországon. Hadmérnök, 2007. november 27. ISSN 17881919, http://hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html (Letöltés ideje: 2018. 05. 17.)

11 Horrock, Cristopher: Baudrillard és a millenium. Pécsi Direkt Kft. 2003 ISBN 9633684595, pp. 48–51.

– családi helyzete,
– anyagi helyzete,
– saját egyéni érdekei,
– vallási háttere,
– etnikai háttere,
– függõségei,
– technológiai kompetenciái,
– biztonságtudatossága,
– az õt körülvevõ informatikai eszközök,
– az informatikai eszközök használata,
– az online jelenlétének minõsége,
– a privátszféra helyzete.

A magyarországi vasúti infrastruktúra releváns összefüggései

A létfontosságú rendszerelemek sérülései a társadalmi hatás tekintetében súlyosak lehetnek. Ráadásul minden rendszerelem valamilyen módon a másikhoz kapcsolódik, így akár többszörös kár is keletkezhet. A teljes hatásrendszer bemutatása a tanulmány keretein túlmutat, azonban a magyarországi vasúti IT-rendszerek egy szeletének ismertetése segít a komplexitás megértésében.

Magyarországon a vasúti közlekedés elsõsorban a MÁV-csoporthoz köthetõ, ezért a nyíltan elérhetõ információk alapján e szervezeten keresztül kerül bemutatásra, hogy milyen informatikai infrastruktúrával szükséges foglalkozni. A cégcsoport különbözõ tagjai más és más feladatot látnak el a vasúti teher- és személyszállítás üzemeltetése érdekében.

A MÁV Zrt. felügyeli Magyarország közforgalmú vasúti pályahálózatának nagy részét, mely tevékenység magában foglalja az üzemeltetési, forgalomirányítási, karbantartási és felújítási feladatokat.[12] A MÁV Zrt. különbözõ szolgáltatásokat nyújt az általa felügyelt hálózatot igénybevevõ több mint 30 vasúttársaságnak. E feladatok ellátásához a modern vasutak üzemeltetõi különbözõ térinformatikai, illetve más nyilvántartó rendszereket használnak.

A MÁV-START Zrt. személyszállítással foglalkozó tagvállalata látja el az utazóközönség kiszolgálását (jegy-, kocsivizsgálás, jegyértékesítés stb.), melyek nagy része elsõsorban szintén digitális alapon, egy integrált irányítási rendszeren keresztül történik az utas-elégedettség növelése érdekében.[13]

A MÁV Szolgáltató központ hat alappillérének egyike az IT-üzletág, mely a funkcionális folyamatok informatikai hátterének biztosítása mellett az alkalmazott informatikai rendszerek integrációját, illetve az IT-biztonság fejlesztését látja el.[14] Ezen kívül fontos szerepet játszik az országos vasúti közlekedésben a MÁV Csoporttól független VPE Vasúti Pályakapacitás-elosztó Kft., mely a forgalom megfelelõ elosztását irányítja országosan.[15]

A vasúti közlekedésben e négy szervezeten kívül máshol is használnak különbözõ informatikai eszközöket, rendszereket, melyek ellen egy összehangolt támadás komoly károkat (például üzleti, jogi kár, presztízsveszteség) okozhat. Megkülönböztetünk strukturális (infrastruktúra, energia, pályamenti ellenõrzõ-irányító és jelzõ

12 https://www.mavcsoport.hu/mav/bemutatkozas
13 https://www.mavcsoport.hu/mav-start/bemutatkozas/integralt-iranyitasi-rendszer
14 https://www.mavcsoport.hu/mav-szk/bemutatkozas-mav-szolgaltato-kozpont-zrt
15 https://www2.vpe.hu/szervezet/cegismerteto

alrendszer, fedélzeti ellenõrzõ-irányító és jelzõ alrendszer, járművek) és funkcionális (forgalomüzemeltetés és forgalomirányítás, karbantartás, telematikai alkalmazások a személyszállítási és áruszállítási szolgáltatások céljára) területeket.[16] Tehát beszélhetünk különbözõ karbantartási, elszámoló, forgalomirányítási, diagnosztikai rendszerekrõl, különbözõ IoT-mérõeszközökrõl *(lásd a 25. lábjegyzetet)*, mûholdas, illetve GSM-alapú technológiákról, melyekhez társulnak az utas-tájékoztatás, a jegyértékesítés, az alapvetõ informatikai rendszerek, mely a cégek mûködését szolgálják ki.

Az információbiztonsági kockázatmenedzsment jelenlegi mûködése

A Fuzzy-logika használatóságának megértéséhez szükséges áttekinteni a kockázatmenedzsment mûködését. Általánosan a folyamat a kockázatok azonosítását, elemzését, kezelésük tervezését, majd megoldásukat foglalja magában.

Egy adott vállalatnak, szervezetnek elsõ lépésben szükséges valós képet látnia a saját folyamatairól, biztonsági- és érettségi szintjérõl. Ennek a felmérése történhet számos módszer alapján, például a cég által felállított követelménylista segítségével vagy valamilyen nemzetközi, nemzeti szabvány, jogszabály alapján. Tipikusan Magyarországon (is) az ISO 27001 szabvány[17] szerint történik a felmérés. A pénzintézetek sokszor a Magyar Nemzeti Bank 7/2017. (VII.5.) számú, az informatikai rendszerek védelmérõl szóló ajánlása[18] alapján haladnak a felmérés során. A kormányzati szervek sokszor veszik alapul az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényre[19] alapuló 41/2015. BM rendelet[20] követelményeit.

A kockázatok azonosításához a szervezet különbözõ területeinek (információbiztonság, IT, szabályozás, pénzügy stb.) együttmûködése szükséges, hiszen nemcsak a bekövetkezés valószínûségét, de az üzleti hatást is figyelembe kell venni. A folyamat lényege, hogy egy képet mutasson mind a szakemberek, mind a menedzsment számára a jelenlegi helyzetrõl. Ennek alapja a szervezet által meghatározott, konszenzuson alapuló biztonsági osztályok, illetve a kárértékek meghatározása a különbözõ információbiztonsági követelményeknek (bizalmasság, sértetlenség, rendelkezésre állás) megfelelõen.

A létfontosságú rendszerelemek informatikai kockázatfelmérése alkalmával az általános gyakorlat mellett kiemelt hangsúlyt kell fektetni az infrastruktúra fõ tevékenységére. Az elemzésnek ki kell térnie a természeti katasztrófák és mûszaki károk mellett az emberi hibákra, visszaélések kínálta veszélyekre is. A folyamat eredményeképpen

16 Az Európai Parlament és a Tanács 2008/57/EK Irányelve a vasúti rendszer Közösségen belüli kölcsönös átjárhatóságáról.

17 ISO/IEC 27001 Information technology. Security techniques. Information security management systems. Requirements – Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények.

18 Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlása az informatikai rendszerek védelmérõl.

19 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

20 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekrõl.

készül el a hiányosságok listája. Figyelembe véve a szervezeti adottságokat, elkészül a bekövetkezés valószínûségével súlyozott kockázatelemzés. A végeredmény segítségével a vezetés el tudja dönteni, hogy mik azok a fenyegetettségek, amelyekre új technikai, adminisztratív vagy logikai védelmet kell kialakítani, esetleg mely már meglévõket kell rövid, közép és hosszútávon megerõsíteni.

Annak az értéke, hogy valamelyik kockázati tényezõ milyen valószínûséggel következik be, sokszor csak tapasztalati adatokból következtethetõ ki, melyhez ráadásul sokszor kevés korábbi valós eset társul. Vannak olyan módszerek, amelyek különbözõ statisztikákat vesznek figyelembe, esetleg más számítási módszerekkel próbálnak a megfelelõ eredményre jutni. Azok a kockázatelemzések nevezhetõek valóban használhatónak, amelyek nemcsak egy szabvány szerinti lista szerint készülnek, de a helyi adottságokat, specialitásokat úgy veszik figyelembe, hogy valós technikai teszteket végeznek, melyeket beépítenek az elemzési módszertanba, illetve beemelik az üzleti oldali kockázatokat is. A szervezet ezután valamilyen cselekvési terv mentén elõkészíti azokat a lépéseket, melyek mentén fejlesztheti információbiztonsági szintjét.

Figyelembe kell venni azt a környezeti körülményt is, hogy az olyan összetett infrastruktúráknál, ahol a különbözõ informatikai rendszerek ugyan hatással vannak egymásra, azonban mégis más-más az üzemeltetõ, így a felelõs is, ott szélesíteni kell a látószöget. Egy célzott támadás során, feltételezhetõen nem egy infrastruktúra-elem támadására korlátozódik a károkozás. Eltérõ (az üzemeltetõ felkészültségétõl, megelõzõ lépéseitõl függõ) mértékben ugyanúgy veszélyben vannak a kiszolgáló informatikai rendszerek, a térinformatika, a logisztikai és ügyfélkapcsolati rendszerek, a fedélzeti és irányítási eszközök.

A humánfaktor bevonásának növelése

A biztonsági rendszerek bevezetése a kockázatelemzés után történik meg, annak megfelelõen, hogy adott intézkedéssel minél nagyobb és többféle kockázatot lehessen lefedni. Természetesen ez a követendõ megoldás.

Tételezzük fel, hogy az adott vasúti szervezet – mint kritikus infrastruktúra – minden tõle telhetõt megtesz annak érdekében, hogy a lehetõ legszélesebb körûen alakítsa ki az információbiztonsági védelmét. Az informatikai határvédelme jól átgondolt, megfelelõen van szegmentálva a hálózat, a mentési-, naplózási-, jogosultságkezelési rendszere jól mûködik. A kritikus infrastruktúrák esetében azonban számolni kell azzal, hogy az objektum és a benne dolgozó személyek potenciális célpontjai lehetnek egy célzott kibertámadásnak.

A 2010-ben megvalósított, fizikai kárral is járó Stuxnet-támadás[21] jó példa arra, hogy milyen károk okozhatóak egy alapvetõen jól védett rendszerben. Hasonló eset volt a 2007-es észt túlterheléses támadás,[22] melynek alkalmával az állami közigazgatási

21 Shakarian, Paulo – Shakarian, Jana – Ruef, Andrew (2013): RuefIntroduction to Cyber-Warfare. Elsevier Inc. Waltham, ISBN: 9780124078147 pp. 223–239.

22 Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány 2013/1. elektronikus lapszám pp. 188–209.

rendszert blokkolták a támadók. A kibertörténelem tele van olyan sikeres támadásokkal, amelyek azért sikerülhettek, mert emberek lévén egy célzott támadás alkalmával könnyen kijátszhatóak, befolyásolhatóak vagyunk. Külön irodalma[23] van annak, hogy az emberi tényezõt hogyan lehet használni az informatikai rendszerek elleni támadások alkalmával.

A kockázatelemzési módszerek, mint például az ISO 27005, kitérnek a humánfaktorra és beépítik az elemzés lépései közé. Azokban az esetekben, ahol figyelnek is a teljeskörûségre a biztonság építésénél, ott tesznek is lépéseket annak érdekében, hogy ezt a kockázati tényezõt is csökkentsék, azonban a módszertan kiválasztása és alkalmazása, így a felelõsség vállalása is az adott szervezeten múlik.

Jellemzõen valamilyen social engineering audit alkalmával mérik fel, hogy a dolgozók mennyire tudatosak. Az itt született eredményt pedig felhasználják az információbiztonsági tudatosságot célzó oktatások alkalmával. Az így átadott tudás mélysége nagyban függ az elõadó felkészültségétõl és a képzésen résztvevõk befogadóképességétõl. Abban az esetben, ha mind a két feltétel adott, akkor egy általános biztonságtudatosság átadás történhet meg. A tudatosság növelésének hatékonyságát az aktív tanuláson alapuló módszerek jelentõsen megnövelik, melyek fejlesztése és elterjedése az elmúlt néhány évben kezdõdött el.

A tradicionális, kevésbé hatékony információbiztonsági oktatások és a célzott, kifinomult támadások jellege (mint például a Stuxnet) miatt továbbra is könnyedén támadhatók meg az emberi tényezõn keresztül az informatikai rendszerek. Ezek a szofisztikált támadások túlmutatnak az egyszerû vírusok bejuttatásán.

A támadók számos körülményt vizsgálnak meg. Elemzik a célobjektumot, megnézik, kik lehetnek a gyenge láncszemei a munkavállalók körének.[24] Az így kiválasztott célszemély életvitelét, az általa használt eszközöket, az õt körülvevõ IoT- eszközöket,[25] a rajtuk futó szolgáltatásokat, operációsrendszereket, szoftver és hardver verziókat. Megvizsgálják, hogy ezeknek milyen ismert vagy még nem publikált (zero-day) sérülékenysége van. A közösségi médiára feltöltött adatok, illetve az egyéb internetes tartalom (videók, nyilatkozatok stb.) tovább segítik a támadások személyre szabhatóságát. Ez az alapja a célzott adathalászatnak (például Spear-phishing), illetve a kifinomult APT- támadások[26] is felhasználhatják a rendszerekrõl szerzett információkat.

Az természetesen nem kivitelezhetõ, hogy egy adott kritikus infrastruktúra esetében minden munkavállalónak egy olyan mély ismertet lehessen átadni, ami alapján felismerik az õket érõ kifinomult támadásokat. Mint ahogy az sem elvárás az

23 Hadnagy, Cristopher (2011): Social Engineering – The Art of Human Hacking. Wiley Publishing, Indianapolis, ISBN 9780470639535

24 Kiss Dávid – Váczi Dániel (2018): A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján. Hadmérnök, 2018/1. ISSN 17881919
http://real.mtak.hu/77916/1/HT20181_153_170_u.pdf (Letöltés ideje: 2018. március 31.)

25 Internet of Things = a dolgok internete: internetre kötött különbözõ passzív és aktív eszközök hálózata.

26 APT (Advanced Persistent Threat): olyan fejlett támadások, melyek célja az információszerzés úgy, hogy egy adott rendszerben minél tovább rejtett módon tudjon jelen lenni a támadó.

informatikai rendszereket védõkkel szemben, hogy minden támadásra felkészítsék az infrastruktúrát. Azonban a technológiai oldalon már megszületett az a gondolkodás, hogy különbözõ biztonsági szinttel kell rendelkeznie adott rendszernek. Például *a 41/2015. BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekrõl* a hatálya alá esõ szervezeteket 5 biztonsági szintbe sorolja. Az általuk használt elektronikus információs rendszereket pedig 5 biztonsági osztályba sorolja. A szervezetnél dolgozók biztonsági szintjét azonban nem említi. A besorolásnál a humánfaktor és annak képzettsége megjelenik a következõ pontokban:

- „Emberi tényezõket figyelembe vevõ (személy-) biztonság:
  - személybiztonsági eljárásrend,
  - munkakörök, feladatok biztonsági szempontú besorolása,
  - a személyek ellenõrzése,
  - eljárás a jogviszony megszûnésekor,
  - az áthelyezések, átirányítások és kirendelések kezelése,
  - az érintett szervezettel szerzõdéses jogviszonyban álló (külsõ) szervezetre vonatkozó követelmények,
  - fegyelmi intézkedések,
  - belsõ egyeztetés,
  - viselkedési szabályok az interneten.
- Tudatosság és képzés
  - kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel,
  - képzési eljárásrend,
  - biztonságtudatosság képzés,
  - belsõ fenyegetés,
  - szerepkör, vagy feladat alapú biztonsági képzés,
  - a biztonsági képzésre vonatkozó dokumentációk.”[27]

A felsorolást figyelembe véve érdemes lehet a kritikus infrastruktúrák biztonsági szintjének tervezése alkalmával figyelembe venni azt a tényt, hogy teljesen más védelmi, tudatossági szintet kell a különbözõ pozíciót betöltõ embereknek elérni. Szükséges tehát egy, a valóságot a lehetõ legjobban megközelítõ metódus létrehozása.

A Fuzzy-logika alkalmazhatósága az információbiztonsági szempontból kritikus személyek kiválasztására

Az egyének különbözõségének beépítése egy kockázatelemzésbe nem evidens kérdés. A probléma megoldásának nehézsége, hogy sok különbözõ típusú, nagyon

27 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekrõl.

bizonytalan tényezõbõl szükséges egy kellõen megbízható eredményre jutni. Ez azért fontos, mert a feltételezés az, hogy több energiát szükséges belefektetni bizonyos munkavállalók védelmébe, tudatosságának növelésébe, képzésébe, mint a felkészültebb, tudatosabb személyekébe. Ez természetesen többletköltséggel jár, azonban jól alkalmazva valószínûleg megtérülne a befektetés.

Ha a problémát modellezni kell, akkor az alapvetõ kérdés az, hogy egy adott munkavállaló által birtokolt információk, titkok védendõek-e vagy sem? Más szempontból tekintve, a kritikus infrastruktúrák szintjétõl eltávolodva nézzük meg, hogy egy országban kik a kritikus személyek. Ha valaki a vezetõ politikusokra, a magas szintû bírókra, a védelmi szféra vezetõire gondol és felteszi magának a kérdést, hogy szükséges-e õket jobban védjék vagy képezzék-e a biztonságtudatos gondolkodásra, a válasz valószínûleg igen lenne. De nem mindenki számára, hiszen ez egy szubjektív érték. Hol van az a határ, akinek a biztonsági szintjére oda kell figyelni?

A 2012. évi CLXVI. Törvény[28] szerint a közlekedési, így a vasúti szektor is beletartozik a létfontosságú rendszerelemek kategóriájába. Az ott dolgozó takarító valószínûleg okozhat problémát, azonban kevésbé érezzük, hogy kiemeltebben kellene foglalkozni vele. Ennek ellenére a Paksi Atomerõmû vezérlõközpontja takarítójának képzését többen gondolhatják fontos feladatnak. Ugyanaz a pozíció, mégis érzésre tudjuk, hogy melyik helyszínen dolgozó személy a kritikusabb.

A vasútnál maradva, vajon kit érdemesebb magasabb biztonsági szintbe sorolni? Az említett takarítót, aki minden fontos helyszínre bejárhat és egy adandó alkalommal elállíthat rendszereket, lophat ki papíralapú minõsített információt vagy a létesítmény pénzügyi vezetõjét, aki a pénzügyi adatokhoz dedikáltan fér hozzá? Ennek eldöntése már kevésbé egyértelmû, hiszen a pozíció nem feltétlen mérvadó. A hozzáférések köre, a képzettség, az egyéni motivációk, a családi-, anyagi helyzet sok-sok olyan tényezõ, ami árnyalja a képet. A befolyásoló tényezõk sora közel sem véges és egyikrõl sem jelenthetõ ki, egyértelmûen igen-nem válasszal, hogy számít-e.

A példa kedvéért ragadjunk ki egy tényezõt: az anyagi javakat. Figyelembe kell-e venni a biztonsági kockázat kalkulálásakor, hogy valakinek az anyagi helyzete milyen? Valószínûleg igen, hiszen egy kritikus infrastruktúránál dolgozó szegényebb személyt könnyebb anyagi juttatás ígéretében rábírni egy romboló cselekedetre, mint egy tehetõsebbet. Azonban önmagában az, hogy valaki szûkölködik a pénzben az nem egy egzakt fogalom. Ki számít szegénynek? Ezt mindig a körülményeket figyelembe véve kell eldönteni. Az sem egyértelmû általában, hogy ennek a tényezõnek mi az úgynevezett valóságértéke, azaz, hogy valaki kicsit, félig meddig, eléggé, nagyon szegény-e.

Egy modell alkotásánál tehát nem alkalmazhatóak a BOOLE-algebra kétértékû (0, 1) logikai bemenetei,[29] ahol a válasz igen vagy nem. Szegény-e vagy sem. Kritikus az adott vasúthoz kapcsolódó informatikai rendszer vagy sem? Az efféle esetek

28 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelmérõl.

29 Kóczy T. László – Tikk Domonkos: Fuzzy rendszerek. Typotex Kiadó, 2001. ISBN 9639132551, https://www.tankonyvtar.hu/hu/tartalom/tkt/fuzzy-rendszerek-fuzzy/adatok.html (Letöltés ideje: 2018. 06. 02.) pp. 6–8.

megvalósítására alkalmas a Fuzzy-logika,[30] ahol adott bemenetekhez úgynevezett tagsági függvények tartoznak. Ha például az anyagi helyzetet vizsgáljuk, a szegénység nem eldönthetõ, mert minden társadalomban, mást jelent. Értéket sem lehet egzakt módon hozzárendelni a fogalomhoz. A példa kedvéért vizsgáljunk meg egy összeget, 200 000 forintot. Nem lehetséges azt mondani, hogy ha valakinek 200 000 forint megtakarítása van az még szegény, aki pedig 200 001 forint tartalékkal rendelkezik, az nem az. Más értéknél ugyanez a szituáció. Tételezzük fel, hogy egy gazdag személy megtakarítása X forint. Ha folyamatosan elkezdjük csökkenteni az összeget egy forinttal, akkor a kérdés az, hogy hol van az a pont, ahol már azt mondjuk, hogy nem tehetõs. Nyilvánvalóan X-100 forint még nem jelenti azt, hogy szegény lett az illetõ.

Érezhetõ, hogy itt valamiféle skálázásra van szükség, hiszen a normál BOOLE-logikával eldöntendõ kérdésnél egyértelmûen hozzá lehet rendelni egy kérdéshez az igen (1) vagy nem (0) értéket, míg a tárgyalt esetekben nem. Erre ad megoldást a Fuzzy-logika, hiszen tudja kezelni azt, hogy valaki „kicsit", más „nagyon" (jelen esetben) szegény. Az alapja, hogy minden elemhez a halmazon belül egy [0;1] zárt intervallumon belüli értéket rendel, mely a mértékét jelöli az adott feltételnek.

A korábban felsorolt, az egyén fenyegetettségi szintjét befolyásoló tényezõknél tehát meg kell tudni határozni olyan értékeket, melyek az adott egyén tulajdonságait kellõképpen leírják, így segítenek egy értéket hozzárendelni a kockázati szint besorolásánál. Ilyen lehet például a családi helyzet esetében a kiegyensúlyozott, egyéni értékeknél a becsületes, vagy a függõségek tekintetében az addiktív.

A módszer alkalmazhatósága azokban az esetekben lehetséges, ahol a munkavállalóról ezek az adatok, vagy legalább egy részük már a munkáltató rendelkezésére állnak, például egy nemzetbiztonsági átvizsgálás eredményeként. Az esetek nagy részében a személyiségi jogok miatt ezek az adatok nagy része nem áll rendelkezésre. Ilyen esetekben olyan metrikákat lehet alkalmazni, amelyek alapvetõen az adott szervezet rendelkezésére állnak (például a fizetések nagysága általában összefüggésben van a személy anyagi helyzetével).

A kockázatelemzés e lehetséges metódusa számos jogi, szabályozási kérdést vet fel, melyek tisztázása után a valóságot sokkal jobban tükrözõ eredményt kaphat a munkáltató. Ilyen módon személyre szabott képzéseket adhat a munkavállalói számára és egy sokkal magasabb biztonsági szint valósítható meg.

Összefoglalás

Szükség van egy olyan modellre, mely alapján egy kritikus infrastruktúrában, így például a vasúthoz kapcsolódó szervezetekben dolgozó személy biztonsági szintje pontosabban meghatározható. Azok a körülmények, melyek befolyásolják az eredményt, korábban nem voltak meghatározhatóak egyértelmûen. A Fuzzy-halmazok alkalmazása és a velük végzett mûveletek egy olyan lehetõséget adnak a biztonsági

30 Jager, René: Fuzzy Logic in Control. Thesis Technische Universiteit Delft, 1995, ISBN, ftp://ftp.ucauca.edu.co/Facultades/FIET/DEIC/Materias/Control%20Inteligente/documentos/Jager.pdf (Letöltés ideje: 2018. 06. 02.)

szakemberek kezébe, mely segíti meghatározni azoknak a körét, akiknél a védelem fizikai, vagy tudatossági szintjét növelni kell. Egy jól megalkotott modell lehetõséget biztosít arra, hogy az eredményei segítségével tudatosan lehessen erõforrásokat allokálni a különbözõ informatikai rendszerek biztonsági szintjének növelésére azáltal, hogy a felhasználóik kockázatát mérik fel.

A modell alkotásánál figyelembe kell venni azt a tényt, hogy egy-egy ember alapvetõ emberi jogai ne kerüljenek megsértésre, így ne érhesse õt hátrányos megkülönböztetés semmilyen vallási, politikai, etnikai stb. hovatartozása miatt. Az alkalmazása ezáltal mindenképpen valamilyen hozzájárulással kell, hogy történjen. Ilyen lehet például a nemzetbiztonsági ellenõrzés körébe tartozó személyek védelmének kialakítása. Ezekben az esetekben ugyanis a munkavállaló hozzájárul azoknak az adatoknak a megadásához, melyek a modell bemeneti információit képzik.

Az így meghatározott eredmények tehát az információbiztonsági kockázatmenedzsmentben jól alkalmazható módon, egzakt számításokkal és nem „érzésre" vehetõek figyelembe.

IRODALOMJEGYZÉK

Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány, 2013/1. elektronikus lapszám, pp. 188-209.

Hadnagy, Cristopher: Social Engineering – The Art of Human Hacking. Wiley Publishing, Indianapolis 2011. ISBN 9780470639535

Haig Zsolt – Hajnal Béla – Kovács László – Muha Lajos – Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. Budapest, ENO Advisory Kft., http://www.certhungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf (Letöltés ideje: 2018. 05. 12.)

Horrock, Cristopher: Baudrillard és a millenium. Pécsi Direkt Kft. 2003 pp. 48–51. ISBN 9633684595

Horváth Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. Fejezetek a kritikus infrastruktúra védelemből. Magyar Hadtudományi Társaság, Budapest, 2013. ISBN 9789630869263, http://mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf (Letöltés ideje: 2018. 05. 12.)

Jager, René: Fuzzy Logic in Control. Thesis Technische Universiteit Delft, 1995, ftp://ftp.ucauca.edu.co/Facultades/FIET/DEIC/Materias/Control%20Inteligente/documentos/Jager.pdf (Letöltés ideje: 2018. 06. 02.)

Kiss Dávid – Váczi Dániel (2018): A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján. Hadmérnök, 2018/1, ISSN 17881919, http://real.mtak.hu/77916/1/HT20181_153_170_u.pdf (Letöltés ideje: 2018. március 31.)

Kovács László: Kritikus információs infrastruktúrák Magyarországon. Hadmérnök, 2007. november 27. ISSN 17881919, http://hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html (Letöltés ideje: 2018. 05. 17.)

Kóczy T. László – Tikk Domonkos: Fuzzy rendszerek. Typotex Kiadó, 2001, ISBN 9639132551, https://www.tankonyvtar.hu/hu/tartalom/tkt/fuzzy-rendszerek-fuzzy/adatok.html (Letöltés ideje: 2018. 06. 02.)

Shakarian, Paulo – Shakarian, Jana – Ruef, Andrew (2013): RuefIntroduction to Cyber-Warfare. Elsevier Inc. Waltham, ISBN: 9780124078147

Szádeczky Tamás: Az IT biztonság szabályozásának konfliktusa. Infokommunikáció és jog, 2013. X. évf. 56. sz. ISSN 1786-0776

Szádeczky Tamás: Information Security Law and Strategy in Hungary. Academic and Applied Research in Military and Public Management Science 14: (4) 2015, ISSN 2064-0021

JOGSZABÁLYOK ÉS SZABVÁNYOK

Egyesült Államok. Uniting and Strengthening America, by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001-es 107-56-os törvény, 1016-os szekció, más nevén a Kritikus Infrastruktúrák védelmérõl szóló 2001-es törvény, https://www.selectagents.gov/resources/USApatriotAct.pdf (Letöltés ideje: 2018. 11. 10.)

PPD 63 – 1998. május 22. Protecting America's critical infrastructures; https://fas.org/irp/offdocs/pdd/pdd-63.htm (Letöltés ideje: 2018. 11. 10.)

A Tanács 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről; https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32008L0114 (Letöltés ideje: 2018. 11. 10.)

ISO/IEC 27001 Information technology. Security techniques. Information security managemnet systems. Requirements – Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények.

Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlása az informatikai rendszerek védelmérõl; https://www.mnb.hu/letoltes/7-2017-informatikai-rendsz-ved.pdf (Letöltés ideje: 2018. 11. 10.)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról; https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (Letöltés ideje: 2018. 11. 10.)

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekrõl; https://net.jogtar.hu/jogszabaly?docid=a1500041.bm (Letöltés ideje: 2018. 11. 10.)

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelmérõl; https://net.jogtar.hu/getpdf?docid=a1200166.tv&targetdate=20180101&printTitle=2012.+%C3%A9vi+CLXVI.+t%C3%B6rv%C3%A9ny (Letöltés ideje: 2018. 11. 10.)

Az Európai Parlament és a Tanács 2008/57/EK Irányelve a vasúti rendszer Közösségen belüli kölcsönös átjárhatóságáról; https://publications.europa.eu/hu/publication-detail/-/publication/57247db4-1188-45fc-90d7-b5d96eaa4f39/language-hu (Letöltés ideje: 2018. 11. 10.)