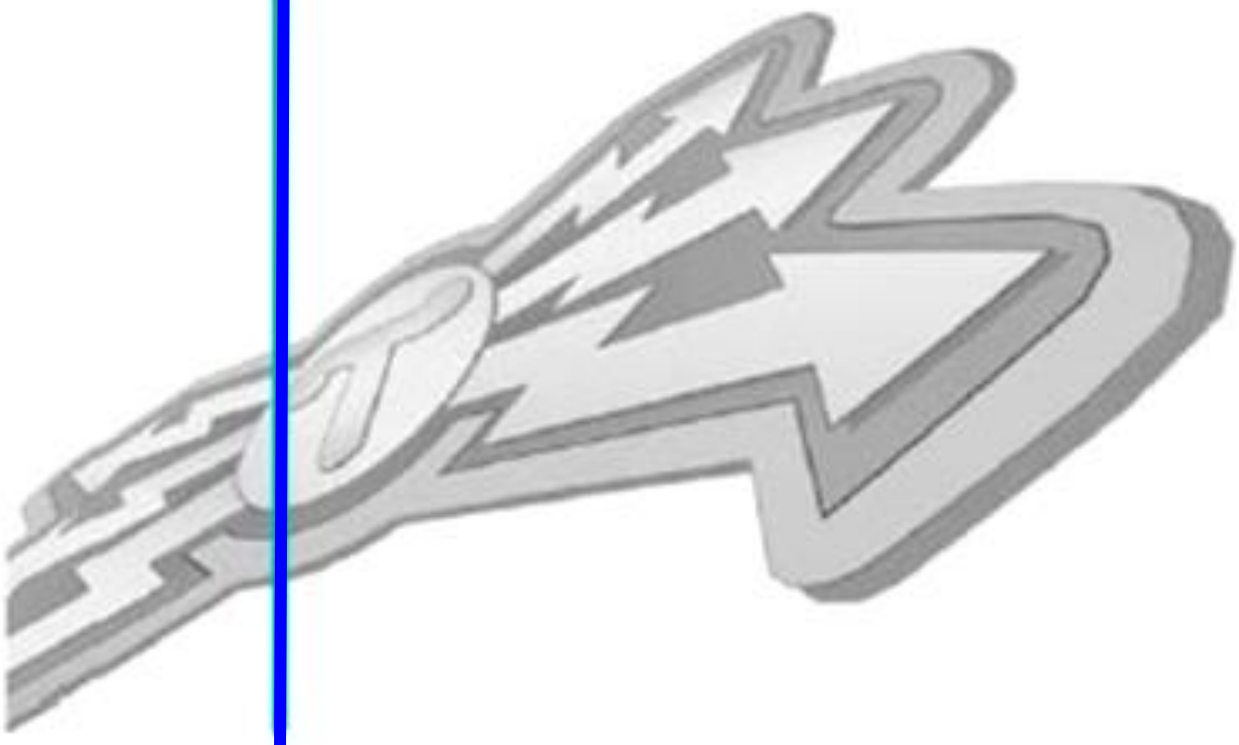
HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the National University of Public Service

7. évfolyam 1. szám
2016



2016. július 1.

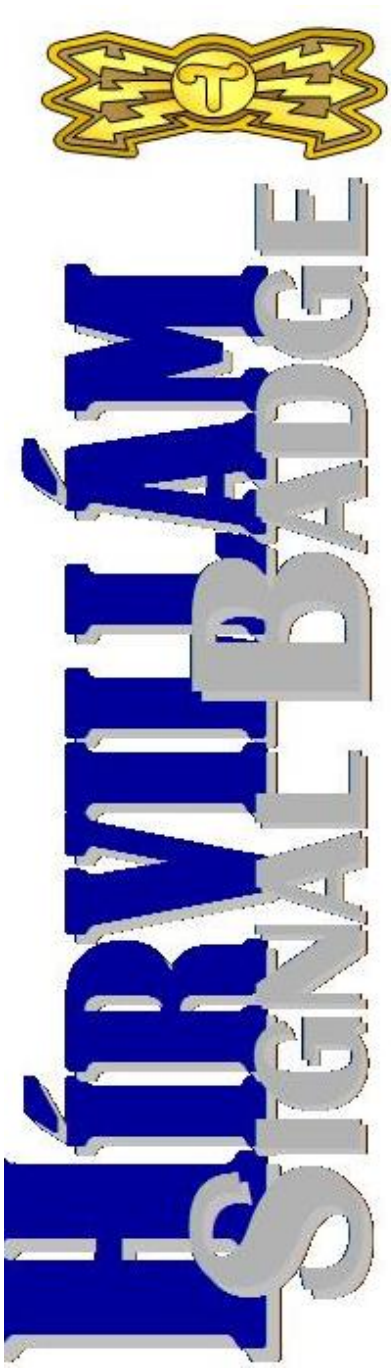
HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem Híradó Tanszék
tudományos időszaki kiadványa

SIGNAL BADGE
Professional Journal of the Signal Departement
at the National University of Public Service

Megjelenik évente két alkalommal
Published twice a year

7. évfolyam 1. szám

Budapest, 2016



Felelős kiadó/Editor in Chief
Dr. Fekete Károly alezredes

Szerkesztőbizottság/Editorial Board

Elnök/Chairman of the Board
Prof. Dr. Rajnai Zoltán

Főszerkesztő/Co-ordinating Editor
Dr. habil. Kerti András alezredes

Tagok/Members
Dr. habil. Farkas Tibor százados
Dr. Horváth Zoltán alezredes
Jobbágy Szabolcs százados
Dr. Kassai Károly ezredes
Megyeri Lajos alezredes
Dr. Németh József Lajos
Paráda István hadnagy
Prof. Dr. Rajnai Zoltán
Dr. Szöllősi Sándor ny. őrnagy
Dr. Tóth András százados

Szerkesztette/Co-ordinating Editor
Dr. Tóth András százados

HU ISSN 2061-9499

NKE Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-407 mellék)

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

Tavaszi félévünk sikeres volt. Kimondottan. Hallgatóinkkal csak egy bajunk volt, nem volt velük baj. Terveink sikerültek mind oktatási, mind tudományos szempontból.

Tehát a 2014/15. tanév tavaszi szemesztere kedvezően alakult oktatási egységünk számára. Szokásainkhoz híven ismételten megszerveztük Balatonkenesén a Nemzetközi Katonai Információbiztonsági Konferenciát, amelyet eredményesnek értékelték mind a résztvevők, mind a szervezők.

Természetesen a társ tanszékek együttműködésével sikeres kiképzési gyakorlatokat folytattunk Püspökszilágyon, illetve Ócsán.

Hasonlóan az elmúlt évhez, szintén az ERASMUS programnak köszönhetően a külföldi hallgatói részképzés mellett fiatal oktató kollégáink rendszeresen tartottak előadásokat társintézményeinkben a környező országokban, valamint különböző nemzetközi konferenciákon.

Végzős hallgatóink sikeres záróvizsgát tettek Angyal Gergő htj., Bene Róbert htj., Deák Péter htj., Havasi Bence htj., Nagy Balázs Bence htj., Ottmayer-Réti Bence htj.), így augusztus 20-át követően elfoglalhatják új, felelősségteljes beosztásukat.

Remélem, hogy egy kellemes nyári kikapcsolódást követően, ősszel, közösségünk ismét folytatja oktatási, kutatási és tudományos munkáját szakmai kultúránk elmélyítése és hírnevünk bővítése érdekében.

Ezen gondolatok jegyében kívánunk kellemes időtöltést az idei év első számának áttekintéséhez!

Budapest, 2016. június 30.

Kerti András
a Szerkesztőbizottság
elnöke

Nagy Balázs: Nemzetbiztonsági szolgálatok közötti együttműködés

Absztrakt

A legnagyobb értékünk a biztonság és szabadság. Ezeket az értékeket a mai globalizált és felgyorsult világunkba megtartani nem kis kihívást jelent a szolgálatok számára. A globalizáció előnyei mellett, megmutatkoznak a hátrányai is. Számolnunk kell azzal, hogy bizonyos jelen kori fenyegetések hamarabb elérik határainkat, mint korábban bármikor. Jelen anyag hivatott szemléltetni az ország biztonságát körül határoló feladatait és kihívásait, az erre létrehozott stratégiákat és jogszabályokat, valamint az ezek által életre keltett nemzetbiztonsági szolgálatokat. A történelem során bebizonyosodott, hogy együtt sokkal erősebben vagyunk, mint külön-külön és nincs ez másképpen sem a nemzetbiztonsági szolgálatok terén sem. Kiemeleten figyelembe veendő ez az állítás, ha országunk nagyobb kihívásokkal néz szembe és az együttműködésre nagyobb szükség van mint valaha. Remélem és bízom benne, hogy a leírt dolgok és következtetések egy eredményesebb együttműködés felé viszik majd szolgálatainkat, biztosítva ezzel a hatékonyabb biztonságunkat.

Kulcsszavak: *nemzetbiztonság, Információs Hivatal, Nemzetviztonsági Szolgálat, Alkotmányvédelmi Hivatal,*

„A nemzetbiztonsági szolgálatok alapvető feladata Magyarország függetlenségének és törvényes rendjének védelme, nemzetbiztonsági érdekeinek érvényesítése.”[1] Lefekteti Magyarország Alaptörvénye továbbá, hogy a nemzetbiztonsági szolgálatok szervezetére, működésére vonatkozó részletes szabályokat,

[1] Magyar Köztársaság Hivatalos Lapja, Magyar Közlöny 43. szám, Magyarország Alaptörvénye 46. cikk (3) bekezdés, 2011. április 25.

titkosszolgálati eszközök és módszerek alkalmazásának szabályait, valamint a nemzetbiztonsági tevékenységgel összefüggő szabályokat sarkalatos törvény határozza meg. Erre építve az Országgyűlés, hogy biztosítsa Magyarország függetlenségét és törvényes rendjének védelmét alkotta meg a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényt (a továbbiakban: Nbtv.). E törvény keretei között szabályozzák a nemzetbiztonsági szolgálatok szervezetét és jogállását, feladatait, irányítását és vezetését, parlamenti ellenőrzését, személyi állományát, működési alapelveit, általuk alkalmazható intézkedéseket, adatkezelésüket, külső engedélyhez kötött és nem kötött, illetve kivételes engedélyezésű információgyűjtésüket, az ezekkel kapcsolatos gazdálkodási szabályokat, védelem és ellenőrzés szabályait, a nemzetbiztonsági ellenőrzés lefolytatását, szüneteltetését és megszűntetését, felülvizsgálati eljárást, valamint a jogorvoslatot. Ugyan 25 évet tudhat maga mögött az említett jogszabály, de megjegyzendő, hogy tartalmát tekintve részletesen taglalja és lefedi törvényi szinten a szolgálatokkal kapcsolatos tételeket, így újabb verzió megalkotására ezidáig nem volt szükség.

Fontosnak tartom megemlíteni a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (III. 21.) Kormányhatározatot is, mely „… meghatározza azokat a nemzeti célokat, feladatokat és átfogó kormányzati eszközöket, amelyekkel Magyarország a nemzetközi politikai, biztonsági rendszerben érvényesíteni tudja nemzeti biztonsági érdekeit.”[2] Ennek keretén belül a stratégia kitér Magyaroroszág földrajzi és gazdasági nyitottságára, mely előbbi adottságait tekintve sebezhetővé teszi az országot. Kiemelt figyelmet érdemel ezen belül az ország energiabiztonsággal, az ellátási útvonalakkal és környezeti biztonsággal kapcsolatos kérdéskörök. Felhívja a figyelmet a dokumentum Magyarország biztonságpolitikai

[2] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról 1 melléklet 1 pont

környezetét illetően, hogy a biztonság fogalma egyre átfogóbb, biztonsági környezetünk folyamatosan változik, így a kockázatok, fenyegetések és kockázati tényezők ma már az egyének, közösségek, államok és régiók szintjén, valamint globális szinten vannak jelen. E koncepció alapján elengedhetetlen a biztonságpolitikai, katonai, gazdasági, és pénzügyi, társadalmi, valamint környezeti biztonság összefüggéseinek együttes kezelése. A stratégia kijelenti, hogy „Magyarország egyetlen országot sem tekint ellenségének, vitás kérdéseit az Egyesült Nemzetek Szervezete (ENSZ) Alapokmányának elveivel és a nemzetközi jog normáival összhangban, békés eszközökkel kívánja rendezni.”[3], valamint egy hagyományos fegyverekkel végrehajtott támadás veszélyét is elenyészőnek tartja, de továbbra sem lehet azonban figyelmen kívül hagyni bizonyos kockázatokat és fenyegetéseket. Tekintettel kell lenni egyes szomszédos régiók biztonságának törékenységére és az ezzel járó katonai beavatkozásra a konfliktus rendezésében. Jelen értekezéshez kapcsolódóan a stratégia felhívja a figyelmet a globalizált világunkban bekövetkező veszélyforrások területi hatályaira is. Leírja, hogy a biztonság nem a határainknál kezdődik. A távoli veszélyforrások is hihetetlen gyorsasággal kerülhetnek határinkon belülre is. A terrorizmus, a tömegpusztító fegyverek és hordozóeszközök világszintű proliferációja, valamint a fegyverkezések erősödése az egyes régiókban növelik a bizonytalanságot és ezzel párhuzamosan növelik a veszélyt Magyarországra nézve.

Magyarország Nemzeti Biztonsági Stratégiájából származtatják Magyarország Nemzeti Katonai Stratégiáját, mely ágazati stratégia katonai aspektusból vizsgálja meg az ország biztonsági környezetét és az ezzel kapcsolatos kihívásokat, valamint feladatokat.

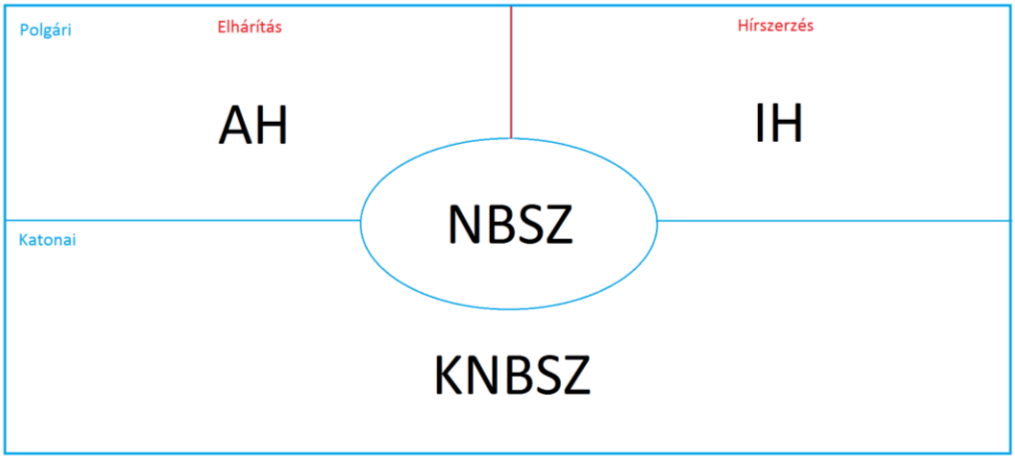
[3] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról 1 melléklet 8 pont

A felsorolt jogszabályok, valamint stratégiák egy jó „kapaszkodót” nyújtanak a nemzetbiztonsági szolgálatok feladatrendszerét tekintve, továbbá következtetéseket vonhatunk le a honi nemzetbiztonsági és egyéb szolgálatok együttműködésére a hatékonyabb felderítés és elhárítás érdekében, valamint a nemzetközi együttműködésre a globális veszélyekkel és fenyegetettségekkel kapcsolatban. A tevékenységüket nagy általánosságban megfogalmazza a jogszabály azonban a konkrét eljárásokra, valamint az együttműködésben résztvevő felekre és a velük való kapcsolattartás részletszabályaira csak az egyes szolgálatok minősített belső szabályzóiban találhatnánk iránymutatásokat.

Magyarországon négy titkosszolgálatot különböztethetünk meg. A polgári oldalon elhárító területen az Alkotmányvédelmi Hivatalt (a továbbiakban: AH), hírszerző területen az Információs Hivatalt (a továbbiakban: IH). Katonai területen pedig a Magyar Köztársaság Katonai Felderítő Hivatal és a Magyar Köztársaság Katonai Biztonsági Hivatal 2012. január 1-i integrációjából létrejött Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) tölti be nemzetbiztonsági funkcióit. A negyedik egyben legnagyobb költségvetéssel rendelkező szervezet pedig a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ), mely „szolgálat magasan képzett szakembereivel, folyamatosan fejlesztett eszközeinek és módszereinek alkalmazásával, titkos információgyűjtési és adatszerzési, továbbá szakértői szolgáltatásokat nyújt az igénybevételre törvényi jogosultsággal rendelkező nemzetbiztonsági és bűnüldöző szerveknek.”[4]

Az alábbi ábra struktúrában szemlélteti a fent említett szolgálatokat, illetékességük szerint:

[4] http://nbsz.hu/?mid=14 Letöltve: 2016. 05. 19.



1. számú ábra: Titkosszolgálatok

Alkotmányvédelmi Hivatal

A Kormány irányítja a Belügyminiszter útján, főigazgató látja el a vezetését.

Főigazgató: Dr. Kiss Zoltán dandártábornok

Székhelye: 1055 Budapest, Falk Miksa utca 9-11.

Web: http://ah.gov.hu/index.html

Rendeltetését tekintve az Nbtv. 5§-ban meghatározott feladatok alapján általános hatáskörű, honi illetékességű, elhárító és alkotmányvédelmi feladatokat ellátó biztonsági szolgálatként határozható meg. A hivatal feladati ellátása érdekében operatív feladatokat folytat, amelynek során nyílt és titkosinformációgyűjtés külső és belő engedélyhez kötött eszközeit és módszereit alkalmazza.

Információkat szerez[5]:

- nemzeti, etnikai, faji vagy vallási csoport tagjai elleni erőszak;
- visszaélés szigorúan titkos és titkos minősítésű adattal;
- közveszély-okozás;
- nemzetközi gazdasági tilalom megszegése;
- légi, vízi, vasúti, közúti tömegközlekedéssel vagy tömeges áruszállításra alkalmas jármű hatalomba kerítése;
- közösség elleni izgatás;
- rémhírterjesztés;
- közveszéllyel fenyegetés bűncselekményekre vonatkozóan.

Információs Hivatal

A Kormány irányítja a Miniszterelnökséget vezető miniszter útján, főigazgató látja el a vezetését.

Főigazgató: Pásztor István vezérőrnagy

Elérhetőség: 1539 Budapest, Postafiók: 600.

Web: http://www.ih.gov.hu/index.shtml

Polgári hírszerző szolgálat, mely elsődlegesen az országhatáron kívül tevékenykedik. Általános rendeltetése, hogy a külföldre vonatkozó vagy külföldi eredetű bizalmas információk megszerzésével segítse elő a magyar nemzeti érdekek érvényesülését,

[5] Dr. Dobák Imre: A nemzetbiztonság általános elmélete, 141-142. oldal, Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet, Budapest, 2014., ISBN: 978-615-5305-49-8

működjék közre Magyarország függetlenségének biztosításában és törvényes rendjének védelmében.

Feladatkörei:

- kül- és biztonságpolitika;
- nemzetközi terrorizmus;
- gazdaságbiztonság;
- szervezett bűnözés;
- non-ploriferáció;
- exportellenőrzés;
- külföldi titkosszolgálatok;
- biztonsági védelem;
- rejtjeles információvédelem;
- nemzetbiztonsági ellenőrzés.

Katonai Nemzetbiztonsági Szolgálat

A Kormány irányítja a Honvédelmi Miniszter útján, főigazgató látja el a vezetését.

Főigazgató: Kovács József altábornagy

Székhely: 1111 Budapest, Bartók Béla út 24-26.

Web: http://www.kfh.hu/hu/index.html

A katonai hírszerzés és elhárítás egységes működésének célja a Magyarország biztonsága ellen irányuló törekvések felfedése és akadályozása, a politikai és katonai döntéshozatal, valamint a nemzeti érdekérvényesítő képesség támogatása.

A Szolgálat egyik legfontosabb feladata a Honvédelmi Minisztérium és a Magyar Honvédség törvényes működésének biztosítása, a nemzetközi katonai műveletekben szolgáló magyar katonák hírszerző támogatása és biztonsági védelme.

Információt gyűjt[6]:

- kémkedés, titoksértés;
- terrorszervezetek, csoportosulások;
- szélsőséges csoportok;
- szervezett bűnözés;
- fegyverrel, lőszerrel való visszaélés;
- külföldre szökés;
- közösség elleni izgatás;
- anyagi jellegű visszaélések.

Nemzetbiztonsági Szakszolgálat

A Kormány irányítja a Belügyminiszter útján, főigazgató látja el a vezetését.

Főigazgató: Dr. Szabó Hedvig nb. dandártábornok

Székhely: 1022 Budapest, Törökvész út 32-34.

Web: http://nbsz.hu/?mid=2

[6] Dr. Dobák Imre: A nemzetbiztonság általános elmélete, 144. oldal, Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet, Budapest, 2014., ISBN: 978-615-5305-49-8

„A Nemzetbiztonsági Szakszolgálat feladata Magyarország nemzetbiztonsági védelmének, a bűncselekmények megelőzésének és feltárásának, valamint az igazságszolgáltatás hatékonyságának elősegítése. A szolgálat magasan képzett szakembereivel, folyamatosan fejlesztett eszközeinek és módszereinek alkalmazásával, titkos információgyűjtési és adatszerzési, továbbá szakértői szolgáltatásokat nyújt az igénybevételre törvényi jogosultsággal rendelkező nemzetbiztonsági és bűnüldöző szerveknek.”[7]

Az egyes szolgálatok feladatköreit és információgyűjtési igényeit összevetve az előttük ismertetett jogszabályokkal és stratégiákkal, következtethetünk az általuk elvégzendő feladatokról és az együttműködésük néhány aspektusáról. Bár a belső szabályzó rendszerük értelemszerűen a kívülállók számára védve vannak a betekintés ellen, a felsorolt szempontok jó támpontokként szolgálnak a következtetésekre. Láthatjuk, hogy a hazai együttműködésben kiemelt szerepet kap az NBSZ.

A feladatrendszereken túl, különös tekintettel figyelembe véve, hogy az egyes szervezetek a jogszabályokban és stratégiákban foglaltak alapján az ország szuverenitását, területi integritását és biztonságát hivatottak megőrizni, nem szabad figyelmen kívül hagyni a vele jár hatalmat is, ami ilyenkor az egyes főigazgatók kezében összepontosul. Az esetleges jogtalan visszaélések és úgynevezett „túlkapások” elkerülése végett hozta létre az Országgyűlés a Nemzetbiztonsági Bizottságot, mely bizottság feladatait az Nbtv. 14§-a rögzíti.

[7] http://nbsz.hu/?mid=14 letöltve: 2016. 05. 19.

A következő ábrán láthatjuk Magyarországgal határos országok titkosszolgálatait:

2. számú ábra: Magyarország és határos országok[8]

A határos országok titkosszolgálatai:

- Szlovákia
  - Szlovák Információ Szolgálat (SIS)
  - Nemzetbiztonsági Hivatal (NBU)
  - Katonai Hírszerzés (VS)
- Ukrajna
  - Ukrán Biztonsági Szolgálat (SZBU)
  - Katonai Felderítő Főcsoportfőnökség (HUR)
  - Ukrán Külső Hírszerző Szolgálat (SZRU)
  - Határőrség Felderítő Főcsoportfőnökség (OPR)
- Románia
  - Román Hírszerző Szolgálat (SRI)

[8] https://upload.wikimedia.org/wikipedia/commons/thumb/a/ac/Hungary_location_map.svg/570px-Hungary_location_map.svg.png letöltve: 2016. 05. 19.

  - Külföldi Hírszerző Szolgálat (SIE)
  - Őrző Védő Szolgálat (SPP)
  - Speciális Távközlési Szolgálat (STS)
  - Belső Védelmi Államtitkárság (DIPI)
  - Védelmi Információs Főigazgatóság (DGIA)
- Szerbia
  - Biztonsági Információs Ügynökség (BIA)
  - Katonai Felderítő Ügynökség (VOA)
  - Katonai Biztonsági Ügynökség (VBA)
- Horvátország
  - Biztonsági Hírszerző Ügynökség (SOA)
  - Katonai Biztonsági Hírszerző Ügynökség (VSOA)
- Szlovénia
  - Szlovén Hírszerző és Biztonsági Ügynökség (SOVA)
  - Hírszerző és Biztonsági Szolgálat (OVS)
- Ausztira
  - Katonai Hírszerző Hivatal (HNAA)

- Katonai Elhárító Hivatal (HAA)
- Szövetségi Alkotmányvédelmi és Terrorelhárító Hivatal (BVT)

3. számú ábra: V4[9]

Fontosnak tartom megemlíteni még a visegrádi együttműködés országait (a visegrádi országok, visegrádi négyek, V4-ek pedig: Csehország, Lengyelország, Szlovákia és Magyarország), ugyanis együttműködésből fakadó kötelezettségeinket tekintve partnerországaink jelentősen hozzájárulhatnak Magyaroroszág biztonságának erősítéshez akár a hírigényeket vesszük alapul, akár más aspektusból vizsgáljuk az együttműködést. Az együttműködés célja ezen középeurópai országok gazdasági, diplomáciai és politikai érdekeinek közös képviselete, esetleges lépéseinek összehangolása. Így nem mehetünk el a tény mellett, hogy bizonyos

[9] https://upload.wikimedia.org/wikipedia/commons/thumb/b/b9/Visegrad_group_countries.svg/1280px-Visegrad_group_countries.svg.png letöltve: 2016. 05. 19.

dolgok esetében hosszútávú perspektívákban gondolkodva félre kell rakni az egyes önös érdekeinket és a történelemből fakadó sérelmeinket. Koherens egységként nyomósabb szempontot állítva tudja alakítani geopolitikai helyzetünket.

A visegrádi négyek (az előbbiekben fel nem sorolt országok) titkosszolgálati, országonkénti megbontásban:

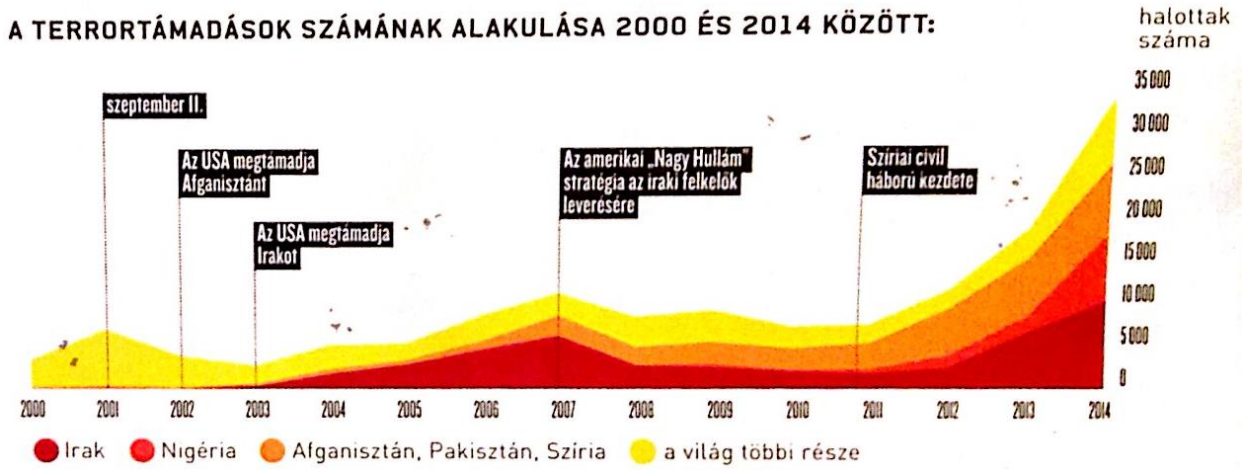
- Lengyelroszág
    - Hírszerző Ügynökség (AW)
    - Belbiztonsági Ügynökség (ABW)
    - Központi Korrupcióellenes Iroda (CBA)
    - Katonai Hírszerző Szolgálat (SWW)
    - Katonai Elhárító Szolgálat (SKW)
- Csehország
    - Biztonsági Információs Szolgálat (BIS)
    - Külföldi Kapcsolatok és Információs Hivatal (UZSI)
    - Katonai Hírszerzés (VZ)

Egyeztetve a szolgálatok illetékes emberével a konkrét együttműködésre nem kaptam választ viszont tanúbizonyságot nyert az a következtetés mely szerint a Kormány megrendelésére, a Miniszter utasításai alapján elrendelhetnek együttműködéséket adott megrendelésre történő információszerzéshez. A folyamat részletszabályait úgy, mint az együttműködők és együttműködés információáramlását, valamint információ átadás részletszabályait is belső szabályzók taglalják, melyek minősítettek és külső személy jogosulatlan betekintése ellen védettek.

A honi kihívásoknál maradva az ország számára aktualitással rendelkezik a nemzetbiztonságát is érintő migráció kérdéskör. A helyzet vizsgálata nem nézhető csupán egyfajta szemszögből, hiszen az illegális migráció nem szabályozott folyamat, így sok embert hoz kapcsolatba a szervezett bűnözéssel, e témakörben különös tekintettel az embercsempészetre, ahol ezreket mozgattak meg határokon keresztül. Jelen esetben rendszer szintű üzletről beszélünk, melynek leépítése sok időbe és energiába telik. Továbbá nem hagyható figyelmen kívül az esetleges radikalizálódás eshetősége sem, ahol az egyén ideológiai nézeteit a szorult helyzetének megsegítéséből kiindulva formálják. Az európai népek ellenérzésének növekedése pedig egyfajta erőszakspirálként erősítheti a radikálisok számát, mely a végeérhetetlen folyamathoz vezethet.

Egy másik jelen anyaghoz kapcsoló aspektusból vizsgálva a migrációs tényt a nemzetbiztonsági szolgálatok számára is komoly feladatot és leterheltséget ró, és az eddigieknél is intenzívebb együttműködést. Elkerülhetetlen, hogy ekkora létszámban érkező embertömeg közül ne akadna olyan, aki képviseli az ellenérdekelt ország nézeteit és akár szerveződéssel, akár információgyűjtéssel segítené ezeket az érdekeket.

A biztonság, béke és terrorizmus kérdéskörében figyelembe kell vennünk az országunk geostratégiai helyzetét, ahol enyhítő körülményt jelent, hogy jelenleg csak tranzit országként szerepelünk. Ugyanakkor a 2000 és 2014 között fellelhető terrortámadások száma igen nyugtalanító:



4. számú ábra: Terrortámadások 2000-2014[10]

Az ausztrál Gazdaság és Béke Intézet (a továbbiakban: GPI) által kidolgozott globális békeindex mutató, mely alapján a benne feldolgozott 162 országot 22 részmutató alapján értékelik, figyelembe véve többek között a szomszédokkal való viszonyt, a bűnözés szintjét, a menekültek számát, a politikai stabilitást, a terrorcselekményeket, a bebörtönzöttek számát vagy a haderő kapacitását. A 2015-ös felmérés alapján a GPI sereghajtói: Szíria, Irak, Afganisztán, Dél-Szudán és Közép Afrikai Köztársaság.

Megemlítendő Social Progress Imperative nonprofit szervezet mutatója is (a továbbiakban: SPI) mely 133 országot rangsorol 12 mutató segítségével. Megvizsgálja, adottak-e az alapvető életfeltételek (táplálék, víz, lakás, biztonság), azok javításának eszközei (oktatás, tájékoztatás, egészségügy, fenntartható környezet), illetve hogy mindenki számára megvan-e az esély álmai megvalósításához (személyiségi jogok, döntési szabadság, tolerancia, hozzáférés a modern tudáshoz). Sajnálatos módon az előző sereghatjókhoz képest itt is

[10] HVG extra 2016 I. szám 49. oldal

hasonlóságokat tapasztalhatunk: Közép Afrikai Köztársaság, Csád, Afganisztán, Guinea, Angola.[11]

Ha figyelembe vesszük a tényeket, hogy jelen helyzetben, mely térségekből áramlanak a migránsok nyugtalanító ámbár világos következtetésekre juthatunk a biztonságunkat nézve, különös tekintettel az alacsonyabb iskolázottsági szinttel, ámbár annál nagyobb vízióval, illetve tévhittel érkező egyénekre vonatkozóan.

Ugyanezen folyóirat másik cikke teszi világossá, hogy ha a világban 10 százalékkal kevesebbet kellene költeni az erőszak kezelésére, az 1,43 trillió dollárt szabadítana fel, amit olyan iparágakba lehetne fektetni, amelyek segítenek megteremteni vagy fenntartani a békét.[12]

Bár a belső szabályzó rendszerek megismerésére érthető okokból nem tehettem szert, így a konkrét információáramlási-átadási mechanizmusba nem tekinthettem be, konzultációkból következtetni lehet a bürokratikus eljárások időbeni hatályának hosszadalmasságára, mely a megrendeléstől a feladat végrehajtáson át a válasz információ kézhezvételéig kritikus méretű időtartamot ölelhet fel. A jogszabályok lehetővé teszik azonban, hogy a főigazgatók kezébe adják az azonnali végrehajtás elrendelésének lehetőségét, de az ellenőrzési mechanizmusnak köszönhetően az utólagos jogi szabályosságnak megfelelő procedúra ebben az esetben sem kerülhető el.

Egy központi „tudásbank”, úgynevezett Fúziós Központ létrehozása, mely hozzáférések tekintetében szem előtt tartja a szükséges ismeret elvét, tartalmazná az eddigi események tapasztalatainak feldolgozását, a nyers és elemzett-értékel

[11] HVG extra 2016 I. szám 48. oldal
[12] HVG extra 2016 I. szám 49. oldal

információkat, valamint az aktuális állapotokat, véleményem szerint nagyban hozzájárulna a fent említett veszélyek és fenyegetések jobb pozícióból történő kezelésére.

Mindemellett egy platformként is szolgálhatna a későbbi együttműködések rendezéseként egy biztonságos csatornákon keresztül, melyben a megrendelések és teljesítések, valamint a konzultációk gyorsabban áramolhatnának.

Felhasznált irodalom

- Boda József: A magyar állambiztonsági és nemzetbiztonsági szervek vezetése, irányítása és ellenőrzése 1942-2015 között,
- Boda József: A felderítés, hírszerzés, titkos információgyűjtés elvei és gyakorlata
- Dr. Kis-Benedek József: A nemzetbiztonsági szolgálatok nemzetközi együttműködése
- Dr. Kis-Benedek József: A nemzetközi együttműködés néhány aspektusa
- Kendernay Zsolt, Pándi Erik ,Tóth András: A készenléti szervek informatikai rendszereinek helyzete, várható fejlesztési irányai, HÍRVILLÁM = SIGNAL BADGE 2010:(1) pp. 178-188., 2010
- Dr. Dobák Imre: A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet, Budapest, 2014., ISBN: 978-615-5305-49-8
- 1995. évi CXXV. törvény - a nemzetbiztonsági szolgálatokról
- http://ah.gov.hu/
- http://www.ih.gov.hu/
- http://www.nbsz.hu/

- http://www.kfh.hu/

Jozsef SZENDI: Investigating power supply faults at the FMCG sector

Abstract

At the FMCG sector switching mode power supplies and uninterrupted power supplies are used in the supply chain to ensure the right power for the machinery. Mostly the server rooms, the fire alarm systems, the SCADA and ID system are using uninterrupted power supplies in this sector, but some units, like cutters in the meat industry also might contain this technology. At the FMCG the main problem is the moisture and water flow, as the cleaning procedures are usually containing water rinsing procedure. Most equipment is not really designed for pressure washing. This article provides support for the Engineering Manager, how to identify technical damage and which are the most common faults of these type of systems.

Keywords: *Engineering Management in FMCG, Electric shock, Switching Mode PSU, Power Generator safety*

IMPLEMENT

Due to IFS [1] and HACCP [2] regulations most food manufacturing equipment must be cleaned on a regular basis. As this cleaning procedure usually contains a rinsing process also, most equipment might become wet inside also after a while. Actually modern manufacturing machines are microprocessor controlled. The controller is installed most cases to FR4 based PCB boards [3] and usually they are not able to function too long in wet condition without varnish impregnation.

In case of any controller fault the Engineering Manager of the site should order the repair. As the repairs need sources, the root case should be investigated than additional preventive action should be taken to prevent the similar fault. On Fig. 1

there is an INOTEC made mixer. This unit can cook and process liver pate or other similar meat based products. In this industry the main heat source is mostly steam energy. The unit also has electric supply and water supply feed connected. The electric panel on the front is made of stainless steel. In its original condition the control panel unit is water proof.

Fig.1 Inotec mixer. Source: [4]

As soon as the unit starts to operate, regular heating and cooling processes start to stress the parts. The surfaces should be cleaned in a regular basis. Actually one of the weakest point is the control panel, as the console panel can be worn out after about a year of normal use. This type of machinery is usually installed into a chilled area, as all of the products must be kept below a low room temperature, usually under 10 Degrees Celsius during the manufacturing process.

As the stainless steel surface is cold, and the steam heats up the rest of the unit, all the metals sheets are usually wet due to the condensation. This condensation affects all PCB boards including the switching mode power supplies and the

controllers as well. Most of the controllers are usually powered from low voltages supply. Most visible affect is non-functional keyboard or bad LCD bars on the screen. If this fault is being ignored, other boards might be affected such like the power supplies. Unfortunately the switching mode power supply (SMPS) has much different property than an average low voltage PCB. As the mains are in the EC usually 230 or 400 Volts, the direct connected PCB boards cannot stand the wet conditions and the power supply can easily burn out.

The problem builds up, because even the spear part is built in and repaired, the situation comes back over and over in a regular basis making massive costs in the maintenance budget. As soon as the PSU is removed and arrives into a dry room, most symptoms are going away, so the 3rd party service engineer blames the wet conditions, the Engineering Manager blames the service provider. Same technology is used in fire alarm and ammonia alarm systems. FR4 based PCB-s are mostly everywhere in the factories.

As fire alarm systems, RF ID systems and access control system [5] are all available in modern factories, the author is stating starting, that an un managed root cause fault can mess up the whole objet security and cause higher risks of accidents and malfunction.

Investigation

The Engineering Manager must understand the main conditions and the normal operations of the units. The author is stating that the Electrical and Mechanical qualifications are essential in this position, and structural understanding are much less required such like architecture. Even the architect is an important person during the install like he/she is responsible for the foundation and other structures,

the main root is usually the meeting of vaporised steam and high voltage. Operating an object with just architect based qualification is a security whole. [6]

One of the best practice is, if a group of engineers (specialist team) is responsible for the investigations. The method of work starts with the proper logging of the faults. The log (worksheet) should contain at least the following data.

- Description of the fault.
- Date of fault finding.
- Which unit was affected.
- Risk if the unit is lost.
- The investigator name.

Extras:

- Pictures should be taken.
- The whole log should be digitalized and saved.
- The log should be treated as business confidential data.

As the fault is identified, actually due to business goals it must be repaired - even if it is in-house or subcontractor's fault. To reduce the costs the main task is after the repairs to identify the root cause itself.

Trend of faults

As above, the responsible manager should pull in procedures to cover the fault tracking. The administration should track the fault, the exact date, the repairs timeframe. The report should include some pictures if possible. As future reference short video log will be a very good solution as the fault is linked to a timeframe,

allowing better identification. If the fault comes only one time per a long period might be only a discrete fault. As soon as it comes back in a regular basis the fault should be investigated further as it might cause other consequential damages.

Logging the start up

The start-up procedure is usually a complex process in case of machinery units. After the unit is turned on it's controllers and safety devices should start up. If there is no power the whole unit fails. Most power supply units (PSU) even the normal and the uninterrupted ones are failing mostly during the start-up sequence. The starting up current might reach the limit of the weakest part. Within the PSU there is a start-up sequence also. After the PSU started, it makes some heat, which eliminates the moisture inside the cabinet. Basically a standard FMCG manufacturing equipment will fail more often during the Monday start up, than on the rest of the week. The author is stating, that the general manager should provide enough human resources to cover the star up timeframe. If the required sources are cut due to HR budget, the main root is not in the engineering side, but it can be identified actually at the HR Directorates.

Lighting is also affected. Due to the Energy saving policies some lights are switched off too often. Actually the costs of the repairs might be more than the energy bill itself. The decision has to be made only after investigation of the lifecycle of the whole project. On Fig2 we can determinate that the electrolit capacitor is un-stabilised. This construction is not recommended to use in any part of the factory, where the structure is vibrating.

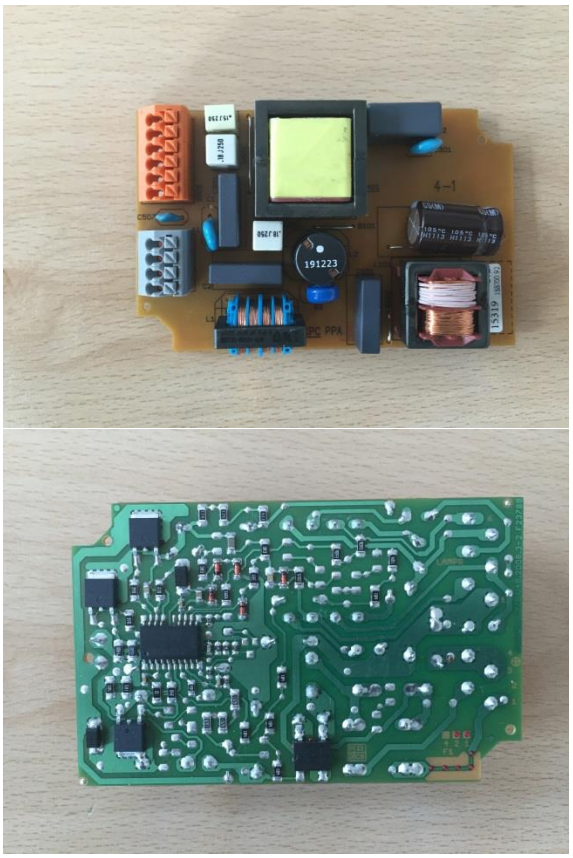


Fig. 2/a. Fluorescent tube inverter PCB top Fig. 2/a Fluorescent tube inverter PCB bottom (Photo made by the Author.)

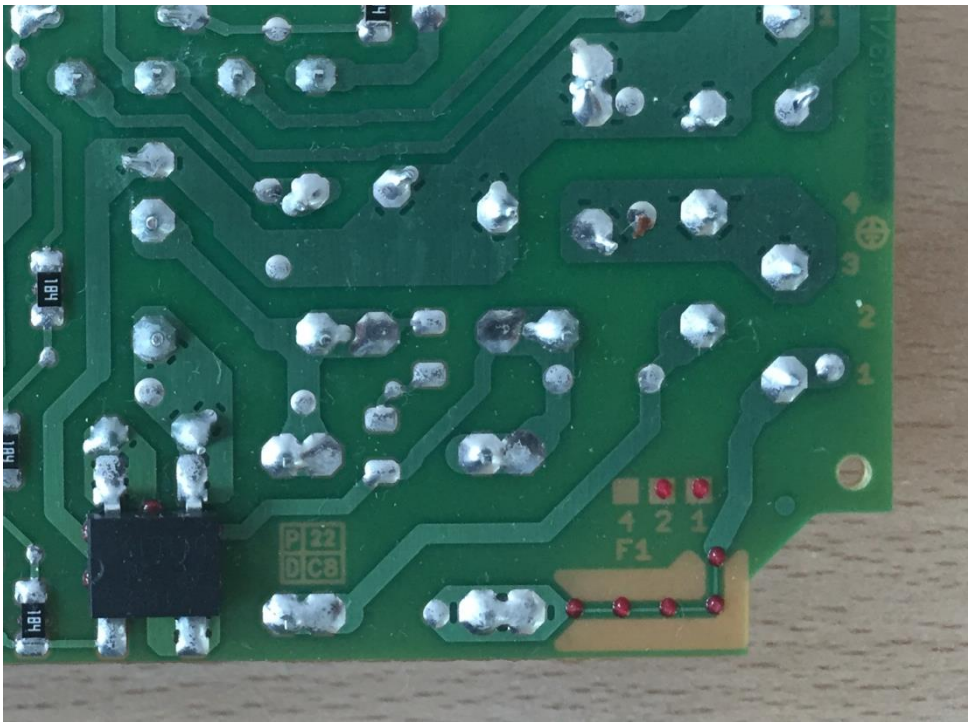


Fig. 3 Fuse integrated on the board. [Photo made by the Author]

In case of moisture in the box the PCB might fail. As a result of the failing the F1 fuse usually burns. Actually this part is not a spark resistant. When the F1 area of the PCB board burns away, it shows up as a risk of spark (ignition). The 4 spots are made to reduce the arc. This design actually prevents that the customer fits a bigger fuse, but not a good option is confined spaces, as it has bigger risk of fire than the standard ceramic based fuse. In industrial environment the ceramic based sand filled fuse is much better choice. Also in areas where gas leak might be a case just special equipment should be used.

Trending the shifts

Usually in a 3 shift pattern the people's performance is not identical. Depending on the rota some operators might provide more stress for the machinery than others. They all might meet the company standards, but the unit can fail mostly in one shift. This case, other procedures like leadership should be reviewed. Actually a proper fault logging can point out human fault as well. As soon as the better integrity is expected, usually the number of the faults are shrinking instantly.

Trending the maintenance sheets

Some problems related to the Fire Alarm System or Access Control System are usually pre-estimated on their maintenance sheets. At Hungary the regulation is very straight forward nowadays. The OTSZ (Hungarian Fire Preventive Regulation) [7] expects regular checks related to Fire Alarm Systems and Gas Detectors on a regular basis. The data should be logged into the Fire Maintenance Logbook. This document is a printed matter, there is no digital alternative legally.

As soon as the logbook is checked, regular faults can be tracked and the root might be identified.

Trending test reports

Most factories, server rooms have uninterrupted power supplies. Their back up is mostly a Diesel Generator. All generators should be tested and stressed on a regular basis. Most of the time the IT cuts the test, reporting as risk of data loss. Best practise is to test the hardware and rather have a planned issue, than a night job. Using the trends we can find the root cause.

EXAMPLES

Example 1:

Original fault:

- Fire alarm detector is faulty.

Response:

- Report of fault.
- Contractor replaces the faulty unit.
- Sign the work off.

Original fault:

- Fire alarm detector is faulty.
- Fire alarm detector was faulty 4 Month before also.

Response:

- Report of fault.
- Contractor replaces the faulty unit.
- Engineering Manager identifies the timeframe of the return.
- Team checks the area and identify, that the area is dusty.
- Air Handler Filter was cracked.
- Replacement of fire alarm detector
- Replace of Air Handler Filter
- Change Air Handler maintenance contractor as a solution (Root Case Management)

- Sign the work off.

Example 2:

Original fault:

- Diesel generator failed to start

Response:

- Report of fault.
- Contractor identifies low fuel level.
- Fill fuel tank, even as per the maintenance book the tank should be full.
- Sign the work off.

Original fault:

- Diesel generator failed to start

Response:

- Report of fault.
- Contractor identifies low fuel level.
- Checking cameras, no sign of opening the plantroom by unauthorised person.
- Fill fuel tank, even as per the maintenance book the tanks should be full. Lock the cap with UV based permanent marker
- Sign the work off.

Original fault:

- Diesel generator failed to start within 3 Month again.

Response:

- Report of fault.
- Maintenance Manager is booted due to too often power faults. (Root Case Management from CEO)
- Contractor replaces identifies low fuel level.
- Checking cameras, no sign of opening the plantroom by unauthorised person.
- Install cameras around the plantroom as per the instructions.
- Fill fuel tank, even as per the maintenance book shows full. Lock the cap with UV based permanent marker.
- Sign the work off.

And the fault comes again…

As per the camera report someone opened the cooling grill and drained the fuel tank. As the grill was outside the factory the UV marker was not able to identified by the guards. The root was a security hole in the factories security process. Actually the Maintenance Manager was booted, but really the Security Officer was ordered to make savings during the camera install, so basically the real root was located somewhere in the General Directors office called “project savings”. Actually project savings are often the main root of general faults.

Method of technical investigation

Most PSU-s should have at least FR4 type of PCB board material, with additional high voltage (HV) varnish on it. The author was dealing with bedpan washers which where custom built units. All parameters where close to the meat factories conditions. Wet condition in aggressive chemical vapour is normal in a hospital environment. The coil had a small part on its side with a diode and a resistor. There

where insulated together during the manufacturing. As the heat had no chance to leave the coil, every Friday when the washers had test run, about 10 % of the equipment's door failed to open causing extreme costs and financial penalty.

Many suppliers try to sell energy saving projects. Modern lighting solutions are LED based, which has an expected lifecycle about 50000 hours, and a driver which might fail in a very short period of time. Taking apart the unit helps to find the route cause. Mostly the heat, the cold, the moisture the dust and the missing maintenance makes the lifecycle shorter.

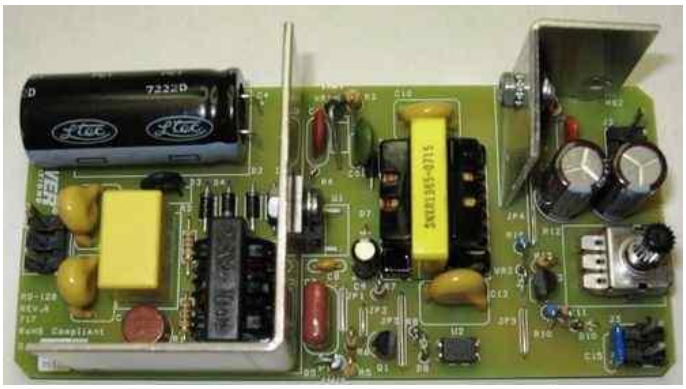


Fig. 4. Commercial SMPS. [Photo made by the Author]

Investigating the SMPS seen of Fig. 3 the left electric capacitor is not fixed to the PCB. The heat sink is too close to the filter coil. On the secunder side there is a variable resistor on PCB. This is not acceptable in wet conditions at all due to as it increases the contact fault risks. The board does not have holes to for fixing structures to fix it to any boxes. Actually this power supply is rather a commercial equipment, than industrial. If any sales provider wants to sell an equipment such like above should be filtered by the Engineering Team.

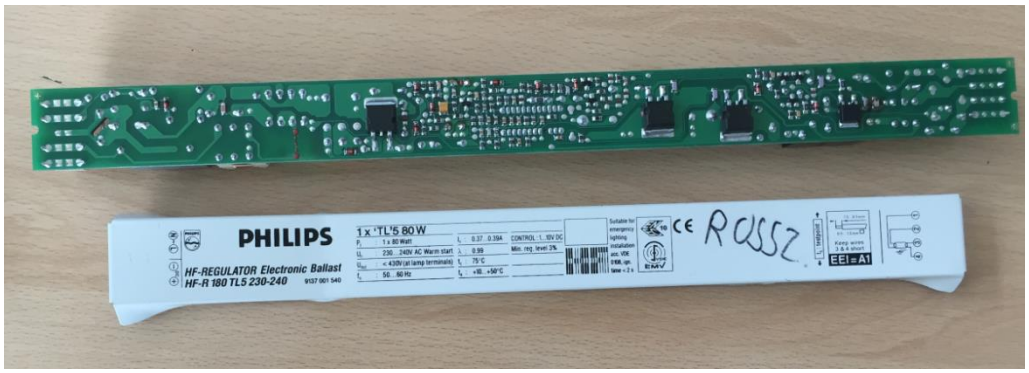


Fig. 5. Phillips driver [Photo made by the Author]

On Fig. 5 the Phillips made lighting ballast is full with SMD parts. It also contains the PCB based fuse, probably because it is cheap to manufacture. This equipment has much more better design than the commercial SMPS as no moving parts are on the board. Actually this unit was burned away. On Fig. 6 can be seen, that one of the SMD parts is melted. All of the units are designed with planned obsolescence. The problem with them, that in an office based environment they might work for about 8-10 years lifecycle, but in a factory where the conditions are worse they, might worn out earlier. To identify the root case, many samples should be taken and the overall trend together should be analysed.

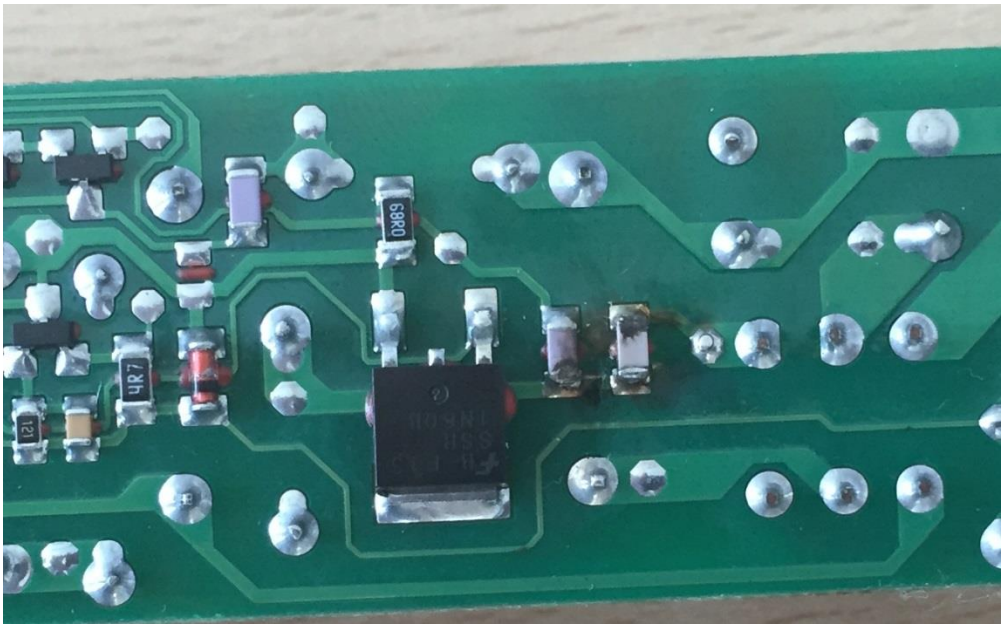


Fig. 6. Phillips driver fault [Photo made by the Author]

Results

In industrial environment well stabilised, massive PCB board are better than fake product. As part of the object security the best practice is, if all the materials are inspected and authorised prior to building in.

As per my research if the bill of the materials are well filtered the overall security level increases, as risk of the fire and the risk of the regular faults are eliminated prior to the factory start up.

Conclusion

Most PCB-s are designed to work in a dry condition room temperature environment. Nowadays the units are designed with planned obsolescence, so the lifecycle of the equipment is quite short. During fault investigation the root cause

should be investigated carefully. Some cases even the original construction and the install meet with the standards the unit fails even the conditions where perfect. To find the best response, the trend of the faults should be investigated and action plan should be pulled in to reduce the costs.

References

[1] IFS - International Food Standard, Online: http://www.dnvba.com/hu/Elelmiszeripar/Elelmiszerbiztonsag/Pages/IFS---International-Food-Standard.aspx, (Downloaded: 2016.05.19)

[2] HACCP: Mit jelent a HACCP rövidítés, Online: http://www.haccpengedely.hu/haccp-engedely-mit-jelent, (Downloaded : 2016.04.18)

[3] FR4 PCB Datasheet, Online: https://atlas-proj-tgc.web.cern.ch/atlas-proj-tgc/TGC_cons_DS.pdf, (Downloaded: 2016.05.18)

[4] Innotec Webpage, Online: http://www.inotectechnology.com/117-1-Standard-Machine-Range.html, (Downloaded: 2016.05.20)

[5] Bodrácska Gyula- Berek Tamás: Megelőző intézkedések szerepe a complex vagyonvédelem területén, építőipari beruházások biztosítása során, Hadmérnök, V. Évfolyam 1. szám, ISSN 1788-1919

[6] Jennifer Martinez: How to Patch Security Holes, Online: http://us.norton.com/yoursecurityresource/detail.jsp?aid=patch_holes, (Downloaded: 2016.04.18)

[7] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról

Som Zoltán — Papp Gergely Zoltán: Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban

Absztrakt

Napjainkban a jelszó, mint egyfaktoros authentikáció nem tekinthető megfelelően biztonságos védelemnek. Ennek a védelemnek az erősségét természetesen további emberi és technikai tényezők befolyásolhatják. Az awareness, azaz a tudatosság és az oktatás az emberi tényező biztonsági szintjének emelésére irányuló eljárások akár hatékonyabbak is lehetnek, mint a technikai eszközök, az optimális hatékonyságot, egymást kiegészítve tudják elérni. A jelszóhasználattal kapcsolatos egyéni és munkahelyi szokások szorosan összefügghetnek az általános információbiztonsági tudatossági szinttel, annak részét képzik. Sőt az informatikai írástudással, az informatikai, mobil eszköz és alkalmazáshasználattal is. Ezen felhasználói attitűd, vagy bizalom meghatározhatja, hogyan viszonyul az állampolgár, mint ügyfél [1] az e- és m-közigazgatási szolgáltatások igénybevételéhez. Felmerül a kérdés, hogy milyen további tényezők befolyásolják az e-befogadást? Milyen nemzetközi tapasztalatok állnak rendelkezésre, milyen veszélyeket rejthet magában az e- és m-szolgáltatások elterjedése. Milyen tudás és milyen szabályok, szabályozás ismerete szükséges ezen szolgáltatások, szélesebb körben történő elterjedéséhez és biztonságos használatához.

Kulcsszavak: *e- és m-közigazgatás, információbiztonság, jelszó használati szokások, digitális írástudás, e-befogadás, informatikai biztonság, jó jelszó, tudatossági oktatás.*

Információbiztonság a magyar közigazgatásban

Magyarország Országgyűlése 2013. április 15-én elfogadta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt [2] amely kiemelkedő csúcspontja annak az összetett kormányzati stratégiának, amely szerint a magyar állam kezelni kívánja azokat a modern kihívásokat és fenyegetéseket, amelyeket az egyre jobban elterjedő digitális infrastruktúra és a kibertér jelent. [3] Láthatóan koncepcionális és szisztematikus munka valósul meg,[1] tanulmányunkban a jelenre koncentrálva egy pillanatfelvételt mutatunk be, rövid nemzetközi kitekintéssel és a veszélyekre való figyelemfelhívással, a jelszóhasználati szokások fókuszba emelésével.

A nemzetközi és hazai kutatások, események, mind azt mutatják, hogy az információ és az információs rendszerek feletti befolyásra napjainkban már komoly figyelmet kell fordítani, kiterjesztve az említett rendszerek működésének garantálására, a benne lévő információk védelmére, annak bizalmasságára, sértetlenségére és a rendelkezésre állására. [4] A globális kibertér eseményeire[2] számos példát lehet felsorolni[3], ezekkel komolyan foglalkozni szükséges. [5] A közigazgatás kiszolgáltatottsága jelentős, mivel „…tény, hogy közigazgatás megszervezése a mai világban informatikai számítástechnikai eszközök nélkül nem lehetséges”. [6] A kibertudatosság [2] szinten tartása, növelése, a szervezeti

[1] Sorrendben egymást részben fedő és erősítő területeken szisztematikus fejlesztő munka valósul meg: Digitális Megújulás Cselekvési Terv, Egyszerű Állam: a vállalkozások adminisztratív terheit csökkentő középtávú kormányzati program, Magyary Zoltán Közigazgatás-fejlesztési Program, Magyarország nemzeti kiberbiztonsági stratégiája, Nemzeti Infokommunikációs Stratégia 2014-2020, Ibtv.

[2] Kiberfenyegetések, kiberhadviselés, kibertámadások, kiberterrorizmus, hacktivizmus, egyéb az információs rendszereket fenyegető veszélyek.

[3] Tengerentúli, Európai Uniós és Magyarországi példák egyaránt tükrözik az információbiztonsági incidensek számának növekedését.

egyenszilárdság megteremtése érdekében komoly lépéseket kell tenni. Ezen lépéssorozat egyike a Nemzet Közszolgálati Egyetemen elindult képzés [4] is, amelynek jól érzékelhető, reális eredményeit évek múlva lehet majd kimutatni. Ennek oka feltételezhetően az, hogy a szervezeti egyenszilárdság megteremtése kultúra kérdése is, azaz nem lehetséges csak tisztán szabályozással, a szabályozás változásával gyors és tartós sikereket elérni. Magyarország az EU tagállamok mezőnyében jó helyen áll a szabályozási, törvényi keretrendszer szempontjából, azonban még sok a teendő.[5]

A számos nemzetközi információbiztonsági incidensből [7] – a közigazgatás érintettsége miatt – a 2007-es Észtországi esetet emeljük ki. Hetekre megbénult Észtország számos elektronikus szolgáltatása, internetes támadások miatt. Fontos megjegyezni, hogy az országban már akkoriban is nagyon elterjedt volt az e-szolgáltatások igénybevétele, így a probléma komoly fennakadásokat okozott. Feltehetjük a kérdést: ki tanul majd Észtország esetéből? Lesz-e olyan, aki nem ebből, hanem saját kárán fogja megtanulni az információbiztonság kiemelt jelentőségét? Magyarország esetében egy gondolatkísérletet vázol a Digitális Mohács tanulmány, [8] amelynek fő mondanivalója talán éppen a felkészülés, felkészítés fontossága. Ki kell térni a közigazgatás kapcsán a szabályozásra is. Be kell látni, hogy a szabályozás mindig általános lesz, soha nem mehet le technikai mélységekig. Ebből fakadóan mindig az egyénen belüli lehetséges konfliktusforrás lesz, hiszen az informatikai biztonság jogi szabályozása kapcsán szakadék tapasztalható a jogalkotás és jogalkalmazás (jogászok) valamint az intézkedések végrehajtói (informatikusok) között. Hiszen a jogi előírásokat az informatikának kell

[4] NKE Elektronikus információbiztonsági vezető szakirányú továbbképzési szak
[5] Az Európai Unió információbizontásgért felelős szervezete az ENISA számos ajánlást bocsájt ki, ezek azonban nem kötelező érvényűek a tagállamokra.

a napi gyakorlatba lefordítani, egyes esetekben pedig jogi terminusokban használt, technológia független megfogalmazás a napi ügymenetet, a jogalkalmazást rendkívüli módon megnehezítheti. [9], [10] Így könnyen belátható, hogy további kutatások tárgya kell, hogy legyen a humán faktor, az egyén, a tudatosság fejlesztése és az edukáció, hiszen végső soron „fejben dől el minden", azaz a technológia független paragrafusok értelmezése más-más technológiai környezetben jelentősen eltérő is lehet.[6]

Az információbiztonság és annak közigazgatási vetületének is rendkívüli interdiszciplinaritásából következően jogi, igazgatási és szabályozási, technikai, közigazgatási, emberi,[7] oktatási és informatikai kontextusai is vannak. Ezen kontextusokat tudni kell egymással párhuzamosan kezelni és fejleszteni, annak érdekében, hogy az adott szervezet legelemibb egysége, a munkavállaló képes legyen hatékonyan részt venni a folyamataiban. [12]

Az elindult folyamatok bizakodásra adnak okot, azonban a hazai kutatásokból [3], [11] levont következtetések alapján arra kell rávilágítani, hogy hamis biztonságérzetről árulkodik a kutatás. Ez sokféleképpen interpretálható, megfigyeléseink alapján viszont kritikus ez az intervallum, hiszen még nincs meg azon kritikus tömeg az információbiztonsági pozíciókban, amelynek ilyen irányú ismerete és főleg tapasztalata lenne. Így a szervezeti kultúra fejlesztése még nem vett mindenhol erős lendületet. A törvény adta határidő miatt a jelenleg EIV

[6] Sőt az is megállapítható, hogy egyforma technológiai környezetben is eltérő lehet adott jogszabály vagy paragrafus értelmezése.

[7] Human behaviour, az emberi viselkedésre számos hazai és nemzetközi kutatás fókuszál. Felismerik, hogy napjaink minden területen jelen lévő infokommunikációs rendszereinek kezeléséhez mind a kiszolgáló személyzet, mind pedig a ügyfelek megfelelő felkészítése kulcsfontosságú. NETEN A HIVATAL) című, ÁROP-2.2.18-2012-2012-0001 kódszámú kiemelt projekt. http://hirlevel.egov.hu/2014/10/07/felmeres-a-kozszferaban-az-elektronikus-kozigazgatas-human-tenyezoirol/

képzésben résztvevők száma, a prognosztizált számhoz képest optimista becslés szerint is szinte elhanyagolhatóan alacsony[8], [9] Azaz a folyamat katalizálása szempontjából figyelmet kell fordítani az elmúlt időszak tapasztalataira, elsősorban arra, hogy az információbiztonsági vezetőnek milyen sokrétű és szerteágazó feladatai vannak (lesznek) és feltenni a kérdés, hogy munkaerő szervezési szempontból vizsgálva, lehetséges-e az oktatás, képzés, megbeszélésen való részvétel, stb. feladatköröket esetenként egyetlen munkavállalóra terhelni? Képesek lesznek-e az alacsony részvételi arány és a jellemzően meglévő feladatkörök mellé rendelt információbiztonsági vezetői pozícióban helyt állni, de sokkal inkább utat mutatni és szervezeti kultúrát is építeni?

Információbiztonsági alapok és jelszóhasználat - avagy ajánlások vs. gyakorlat

Valószínűleg még évekig, évtizedekig nem vonható ki teljesen a jelszóhasználat a napi gyakorlatból. Természetesen láthatóak már most is kiemelt területek, ahol a többfaktoros authentikáció, a digitális aláírás előfordul, azonban ezek esetlegesen, szigetszerűen jelennek meg. Éppen ezért nagyon fontos az általánosan elterjedő többfaktoros authentikációg is (és abban az esetben is) a jelszóhasználat (password awareness) fogalomtárának létrehozása, oktatása, fejlesztése a közigazgatásban.[10] Itt kiemeljük, hogy természetesen nem csak a közigazgatásban dolgozókról, hanem az ügyfélként megjelenő állampolgárokról is szó van.[1] Annak érdekében, hogy az elektronikus ügyintézés minél szélesebb körben elterjedjen, [13] hogy minél

[8] A képzés indítása óta nagyságrendileg 60 fő iratkozott be, ez a várható létszámnak elképzelhető, hogy az 5%-át se éri el.
[9] A jelenlegi információbiztonsági szintet jól tükrözi a részvételi arány.
[10] Az információbiztonságnak számos további vetülete van, ahogy az információbiztonsági vezető munkája, feladatköre is rendkívül komplex. Oktatás, szabályzatok fejlesztése, beszállítók ellenőrzése, stb. A szabályozási területen a szervezettre és alkalmazásra szabott jelszó házirend, valamint ennek oktatási vetületét egyaránt meg kell határozni, kifejleszteni.

nagyobb tempóban növekedjen az e-befogadási hajlandóság, fontos, hogy a jelszóhasználati szokások és gyakorlatok is a lehető legnagyobb biztonságot biztosító irányok mentén, a lehető legdinamikusabban alakuljanak. A biztonság fogalma pedig két kontextusban vizsgálandó, ugyanis mind a szolgáltató, mind a felhasználó oldalán megfogalmazódik a bizalom kérdése. A jelszóhasználat önmagában még nem teremt egyensúlyi helyzetet ebben a kérdésben, csak, mint egyfajta mennyiségi elem jelenik meg: egy plusz lépés, amit meg kell tennie ahhoz, hogy az általa választott szolgáltatást igénybe vehesse. Ahhoz azonban, hogy a bizalom mindkét oldalon elérje a kívánt szintet, a jelszónak minőségi elemmé is kell válnia. Ehhez szükséges első lépésben a „minőségi" jelszó jelentőségének elfogadtatása a szakma berkeiben, majd a fent említett, a szélesebb definiálás és a hatékony edukáció lehet. [14]

Jelszó alapok és alapfogalmak

Ha vizsgálat alá vesszük a védelem feladatait,[11] [15] akkor a jó jelszó a megelőzés fázisába sorolható be leginkább, ahogy az oktatás, képzés, tudatossági program is.[12] Ahhoz, hogy a megfelelő, kockázatarányos, jó védelem a „jó jelszó" [16], [17], [18], [19] képében megvalósuljon, röviden vizsgáljuk meg a szükséges alapfogalmakat és befolyásoló tényezőket: 1) jó jelszó: a megfelelő jelszó a precízebb kifejezés, hiszen a környezet, a rendszer, a csillapítás és további technikai, logikai, humán tényezők befolyásolhatják; 2) technikai tényezők; 3) a humán faktor: az emberi komponens; 3) a használható biztonság: mennyire van összhangban a napi munkafolyamatokkal

[11] A védelem feladatai: 1) megelőzés és korai figyelmeztetés, 2) észlelés, 3) reagálás, 4) incidens v. krízis menedzsment, Muha
[12] Bár az oktatás több kategóriában is elhelyezkedhet.

[13] ; 4) csillapítás: olyan technikai, fizikai, egyéb körülmények, amelyek a próbálkozások számát vagy gyakoriságát képesek befolyásolni, csökkenteni[14].

Az egynél több faktoros authentikációt – amikor már nem elegendő a felhasználónév–jelszó páros – többfaktoros authentikációnak nevezzük. Az egyfaktoros authentikáció nem tekinthető minden esetben komoly védelemnek, ezt számos további körülmény összessége határozza meg.[15]

A jó jelszót, mint belépő szintű biztonságot az adott rendszerhez, a folyamatokhoz, a felhasználókhoz, a technikai, fizikai környezethez egyaránt hozzá kell igazítani. A használható biztonság, az értéket szállító biztonság érdekében pedig kockázatarányosan kell megvalósítani a jelszószabályozást is. A biztonság összetevői[16] közül a jelszó jól alkalmazható a fenti peremfeltételek mellett. Ennek megvalósulása érdekében komplex, multi-level tudatossági képzésnek kell megvalósulnia,[17] hiszen az eltérő pozíciók, rendszerek, folyamatok következtében javasolt a célcsoportoknak szánt oktatás testre szabása.

[13] Például ilyen hátráltató tényező lehet, ha 3 percen belül lezár az eszköz képernyője. Természetesen bizonyos környezetben ez teljesen elfogadható és támogatja a biztonságot.
[14] Például: a mobiltelefon pin kódját alapesetben háromszor lehet megpróbálni, ez egy jellemző csillapítás. Egyes rendszereknél pedig a harmadik próbálkozás után bizonyos időre zárol a rendszer.
[15] Például: csillapítás, jelszó életkor, a használt szekvenciák száma, egyediség, komplexitás, eseménykezelés és reagálási idő, stb. Ezek együttesen képesek a megfelelő védelem elérésének biztosítására. Természetesen további tényezők is léteznek, amelyekre most itt terjedelmi okokból nem térünk ki
[16] 1) Zárt védelem: az összes releváns fenyegetést figyelembe veszi; 2) Teljes körű védelem: a rendszer valamennyi elemére kiterjed; 3) Folytonos védelem: az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul
[17] A tudatossági képzés és a jelszóhasználati szabályozás, továbbá ezek metszete a jelszóhasználati tudatossági oktatási is célcsoportra szabottan kell, hogy megvalósuljon. Könnyen belátható, hogy eltérő pozícióban lévő alkalmazottak, eltérő alkalmazásokat használó felhasználói csoportok részére eltérő információk szükségesek, célcsoportra kell szabni a tréningeket és a szabályzatokat is.

Tipikus támadási felületek és támadók valamint lehetséges védekezés

A tudatossági képzéseken tisztázni kell, hogy ki ellen és milyen mértékben véd a jelszó. A jelszó támadására számos technikai[18] és social enginering[19] forma létezik. A megfelelő jelszóválasztással, tudatossági képzéssel és technikai támogatással jelentősen csökkenthető ezen, jelszó elleni támadási formák hatékonysága. Napjainkban folyamatosan nő a számítási kapacitás, így akár napi több milliárd jelszót is végig lehet próbálni. Érdemes tehát tisztában lenni azzal, hogy ki ellen és mennyi ideig képes megvédeni a jó jelszó.

A jelszavakra irányuló támadások sokféle módszerrel és eszközzel valósulhatnak meg, ezek közül a leggyakoribb típusok, veszályek amelyekkel a legnagyobb eséllyel találkozhatunk a mindennapokban, az alábbiak: hacker típusú támadások, a jelszólelesés, a keylogger, social enginering jellegű támadás[20], [21] közös, több személy által közösen használt jelszavak.

A jelszó-életkor akkor indul, mikor megváltoztatjuk egy adott rendszerben használt jelszavunkat. Innentől kezdve folyamatosan növekszik annak a veszélye, hogy valamilyen helyzetben, vagy módon redukálódjon a funkciója.

A jelszóhasználati szokásokat számos tényező befolyásolhatja. Ezek lehetnek technikai és szabályozási feltételek, Másik fő kategória a felhasználó gondolkodását

[18] Smart gueesses, dictionary attack, brute-force attack, rainbow tables, egyéb.
[19] A social enginering jellegű támadások elsősorban az ember, a munkavállalót veszik célpontba, ide tartozhat a jelszó lelesése, a pszichikai nyomás alkalmazása, a sürgetés, látszólagos ajándék vagy nyeremény felkínálása, stb.
[20] A magyar jelszóadatbázis elemzés rámutat, hogy hozzávetőleg a jelszavak 20%-a tartalmaz személyneveket.
[21] Olyan állomány, amelyben az egyénre, érdeklődésére, családjára, közösségi hálózatokon elérhető és egyéb módon megszerzett információkból szavak állnak.

befolyásoló tényezők és ismeretek, amelyek a technikai feltételekhez alkalmazkodva sokkal jelentősebben befolyásolni képesek a jelszóválasztást.

Megállapítások

A jelszóhasználati kultúra alakítása – ahogy az a fentiekben is említésre került – elengedhetetlen feltétele az elektronikus ügyintézési hajlandóság,[22] [20] sőt már önmagában a digitális írástudás, az e-befogadás terjedésének is. Ennek a kultúrának pedig nem csak a technikai megoldások fejlesztésére, bővítésére irányuló – a szakemberek oldalán megjelenő – szándék a része, hanem rendkívül fontos eleme a tájékozottság, a tudás, a bizalom és az arra építhető motiváció is. Mindezek elérésének eszköze pedig az oktatás, edukáció, a tudásszint emelése, amelyek eredményeire építve pedig elérhetővé válik az a szint, amely már képes befogadni a többfaktoros azonosítást, a további alternatív azonosítási lehetőségeket is. [21] Olyan kulturális és fogalmi alapismeret-rendszer létrehozására van szükség, amelyben a tisztázott alapfogalmak segítségével hatékonyan lehet tovább építkezni, megteremtve ezzel a bevonódást és az érdekeltséget, az alapfogalmak ismeretét, a miértekre adott érthető válaszok segítségével. [22]

Az információbiztonsági vezetőnek és oktatónak pedig tisztában kell lennie azon körülményekkel, amelyek segítségével kialakítható a szervezetre, alkalmazásra, felhasználói körökre érvényes jelszó házirend és ajánlás. Jelenleg általános gyakorlat a szervezetet egészben, egyben kezelni szándékozó információbiztonsági

[22] A „Miért nem intézett, mi akadályozta meg ebben?”(elektronikus ügyintézésre vonatkozott a kérdés) kérdésre 28% azt válaszolta, hogy nincs internete, 12% pedig azt, hogy nem ért az internethez vagy a számítógéphez. Közszolgálat a közigazgatásban, ÁROP-2011/1.1.12, Reich Jenő, Döme Zsolt

szabályzat és oktatás. Középtávon, a most képzésben részesülő információbiztonsági vezetőkre komoly feladat hárul, mivel saját szervezetükben kommunikálniuk kell a vezetés felé a megfelelő, kockázatarányos döntésekhez szükséges javaslatokat. A munkavállalók meggyőzése nem lehetséges, csupán olyan új információk átadására van lehetőség, amely alapján más döntéseket hoznak, olyanokat melyek összhangban lesznek a szervezeti biztonsági szabályzatokkal. [23]

Felhasznált irodalom

[1] Papp Gergely, Ügyfélelégedettség-mérés a közigazgatási ügyfélkiszolgálásban, 2014, Letöltve:2014.10.01 Forrás: http://ktk.uni-nke.hu/kutatas-es-tudomanyos-elet/esemenyek_-konferenciak?tag=2014

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, Letöltve: 2014.10.01

[3] Illéssy-Nemeslaki-Som, Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs társadalom, Társadalomtudományi folyóirat, XIV. évfolyam, 1. szám (p.:52-73) ISSN:1587-8694

[4] Som Zoltán, Hitelesítési kérdések a magyar (e-) közigazgatásban, Tavaszi szél konferencia

[5] Som Zoltán, Fejezetek a kritikus infrastruktúra védelemből" tanulmánykötet, recenzív összehasonlító elemzés,

[6] Dr. Bukovics István, A fenntartható közigazgatás, fenntartható biztonság elmélete

[7] Som Zoltán, 13. Robothadviselés konferencia, Kibertudatossággal a kiberhadviselés ellen

[8] Kovács – Krasznay, Digitális Mohács, Nemzet és Biztonság, 2010

[9] Reidenberg, Joel R, Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review, Vol. 76, 1998/3. p. 584.,.

[10] Szádeczky Tamás, Az IT biztonság szabályozásának konfliktusa, Infokommunikáció és jog,

[11] NETEN A HIVATAL című, ÁROP-2.2.18-2012-2012-0001 kódszámú kiemelt projekt. http://hirlevel.egov.hu/2014/10/07/felmeres-a-kozszferaban-az-elektronikus-kozigazgatas-human-tenyezoirol/

[12] Matthew Reis, Judith Geller, A Manager's Guide to Human Behavior, ISBN-10: 0-7612-1241-8

[13] Az EU 2020 programja is előirányozza a szélessávú internetkapcsolatok és az e-közigazgatási szolgáltatások fejlesztését. Communication from the commission, EUROPE 2020, A European strategy for smart, sustainable and inclusive growth, http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf Letöltve: 2014.10.01

[14] Danuvasin Charoen - Murali Raman - Lorne Olfman, Improving End User Behaviour in Password Utilization An Action Research Initiative, 2007 Springer Science+Business Media, LLC 2007, DOI 10.1007/s11213-007-9082-4

[15] Muha Lajos, A védelem feladatai: 1) megelőzés és korai figyelmeztetés, 2) észlelés, 3) reagálás, 4) incidens v. krízis menedzsment,

[16] Tihanyi Norbert, Comparison of two hungarian password databases, Pollack Periodica, vol. 8, no. 2, pp. 179–186 (2013)

[17] A tízezer legrosszabb jelszó. Nagyjából 6 millió adatrekord elemzésével készült el a jelszóhasználati statisztika, https://xato.net/passwords/more-top-worst-passwords/

[18] Wei Wang, Hongwei Wang, Yuan Meng, A Large-scale Survey on Password Habits of Internet Users in China,

[19] Mark Burnet: Perfect password selection, protection authentication, ISBN 1-59749-041-5

[20] Reich Jenő, Döme Zsolt, Közszolgálat a közigazgatásban, ÁROP-2011/1.1.12,

[21] L. Tama, M. Glassmana, M. Vandenwauverb: The psychology of password management: a tradeoff between security and convenience, Behaviour & Information Technology, Vol. 29, No. 3, May–June 2010, 233–244

[22] Ken H. Guo, Yufei Yuan, Norman P. Archer, and Catherine E., Connelly, Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, Journal of Management Information Systems, ISSN: 0742-1222, Business and Management, Computer Science, Management Information Systems and Information Technology, Volume 28, Pages 203-236, DOI: 10.2753/MIS0742-1222280208, 2011

[23] Papp – Som, Jelszóhasználati trendek és az ügyfélbizalom értéke, avagy a jelszó, a bizalom és az e-befogadás és ezek kapcsolata napjainkban, 2014

Kocsis István: Lássuk biztosabban a bizonytalant! – kockázati térképek

Absztrakt

Az egyes szervezeteknél, legyenek az államigazgatás vagy a versenyszféra szereplői, kis vagy nagy vállalatok, egyaránt minden belső döntés és minden környezeti hatás vagy befolyás valamilyen szintű kockázatot hordoz. Ezen kockázatok megfelelő szintű figyelembevétele, elemzése, és értékelése az utóbbi években egyre inkább általános igénnyé vált, illetve válik.

A kockázatkezelés területének szakemberei az idők során számos módszertant, eljárást és eszközt fejlesztettek ki.

Ezek közül most egy viszonylag egyszerű, hagyományosan széles körben alkalmazott eszközt, a kockázati mátrixot, illetve az azzal kapcsolatos fogalmakat tekintjük át, az egyértelműség kedvéért hivatkozva az aktuális ISO 31000-es szabványcsaládra. A kockázati mátrix, mint látni fogjuk, egyrészt értékelési, másrészt döntéshozatali, harmadrészt kommunikációs eszköz.

Ezt követően a kockázati térképet, mint hasonló elvi alapokon nyugvó eszközt írjuk le. Áttekintjük a kockázati mátrixok és a kockázati térképek hasonlóságait és eltérő vonásait a kockázatok elemzése, a döntéshozatal, illetve a kommunikáció szempontjából.

Konkrét példákon szemléltetjük a kockázati térképeken megjeleníthető többlet információkat, és bemutatunk néhány kreatív diagramtípust is.

Végül összehasonlítjuk a két elemző és megjelenítési eszköz tulajdonságait, utalva alkalmazásuk korlátaira is.

Kulcsszavak: *kockázat, kockázatkezelés, kockázati mátrix, kockázati térkép*

Bevezetés

Az egyes szervezeteknél, legyenek az államigazgatás vagy a versenyszféra szereplői, kis vagy nagy vállalatok, egyaránt minden belső döntés és minden környezeti hatás vagy befolyás valamilyen szintű kockázatot hordoz.

Minden, aminek nem determináltan előre ismert a kimenetele, azaz másképp is történhet, mint ahogy elvárjuk, már kockázatot hordoz magában.

A vállalatok sikerének egyik jelentős tényezője, hogy a kockázatait mennyire ismeri jól, mennyire értékeli helyesen, és ezeket az információkat mennyire tudja hatékonyan felhasználni a vállalati döntéshozatalban.

A lehetséges fenyegetettségek, azok bekövetkezése és hatása rendkívül sokrétű. Értékelésük számos bizonyosan és jól ismert adatra, illetve számos bizonytalan és kevéssé számszerűsíthető információra alapul.

A modern menedzsmentrendszerek – pl. környezetközpontú irányítási rendszer, információbiztonsági irányítási rendszer, munkahelyi egészségbiztonsági irányítási rendszer, stb. – egyre inkább kockázatalapú irányítási rendszerek, megkövetelik a kockázatok figyelését és kezelését.

A kockázatok előfordulási területe, hatásmechanizmusa, kárjellege nagyon sokrétű lehet. Ezen információk megfelelő, arányos mértékű „becsatornázása” a vezetői döntéshozatalba nem könnyű feladat. Feltétlenül szükséges az információk szűrése, súlyozása, értékelése, és a vezetők számára történő áttekinthető bemutatása oly

módon, hogy ezen rendkívül eltérő jellegű kockázati tényezők minél egyszerűbben értékelhetők, összehasonlíthatók és áttekinthetőek legyenek.

Ezekre az elvárásokra és követelményekre reagálva elsősorban az értékelés, illetve a döntéshozatal támogatása során a grafikus megjelenítés irányába mutató eljárások terjedtek, illetve terjednek.

A kockázatok térképezésére, kategorizálására és értékelésére használhatunk kockázati mátrixokat. Ezen mátrixok legtöbbször a minőségi (kvalitatív) kockázatértékelés alapjai, és a valóságnak természetesen – hol jobban, hol kevésbé – egyszerűsített képét mutatják.

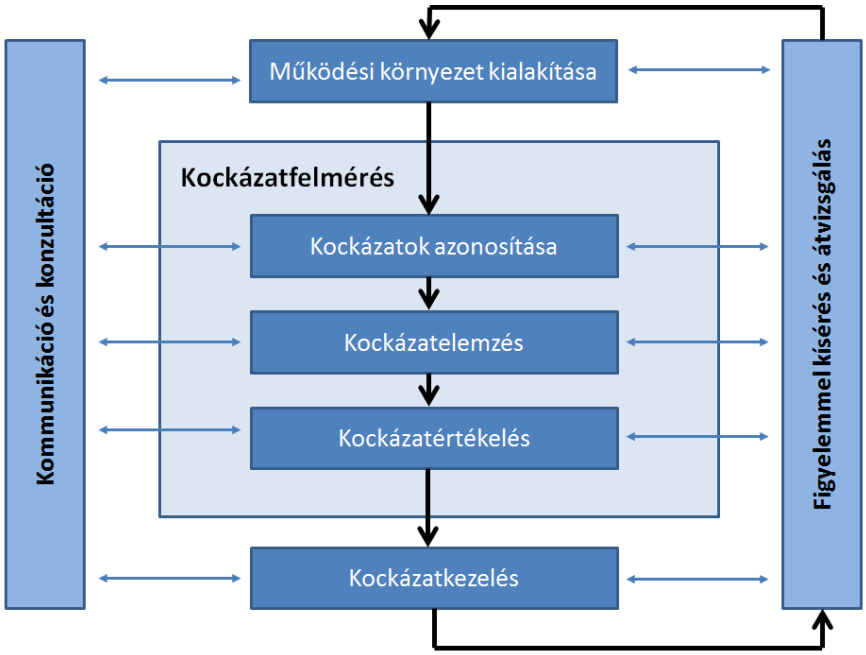
A kockázati térképek alkalmasak a kockázatok és a hozzájuk kapcsolódó tényezők folyamatos átmenetének egyidejű, szemléletes bemutatására, összehasonlítására és – igény szerint – kategorizálására. Ezért találkozhatunk velük vállalkozások, pénzintézetek, államigazgatási szervek, és nemzetközi szervezetek kockázatelemzéseiben.

A konkrét alkalmazási területek rendkívül változatosak az általános működési kockázatok bemutatásától adott projektek kockázatelemzésén keresztül az egyedi események kockázatainak értékeléséig.

A téma tárgyalása során a megfelelő hivatkozási alap biztosítása és az egységes terminológia érdekében visszanyúlunk a témakör alapjait biztosító szabványokhoz. A fogalommeghatározások magyarázatát, elemzését nem tűzzük ki célul.

A kockázatok felmérésének folyamata

Az alábbi ábra a kockázatkezelés folyamatmodelljét mutatja az ISO 31000:2015-ös szabvány szerint [1]. A modellfolyamatok közül a **kockázatfelmérést**, mint az ISO 31000-es szabvány **5.4-es jelű folyamatát** ragadjuk ki, mivel az az a részfolyamat, melyhez a kockázati mátrixok és a kockázati térképek, mint technikai segédeszközök a legszorosabban kapcsolhatók.



1. ábra: A kockázatkezelés folyamatainak áttekintése az ISO 31000-es szabvány alapján

A szabvány értelmezése szerint a **kockázat** (*[1] 2.1. risk*): a bizonytalanság hatása a célokra.

Az egységes megalapozás kedvéért vegyünk még ide a szabványból néhány alapfogalmat. Az **esemény** (*[1] 2.17. event*) bizonyos körülmények bekövetkezése vagy megváltozása, **következmény**nek (*[1] 2.18. consequence*) pedig a célok elérését befolyásoló adott esemény kimenetelét nevezzük. A **valószínűség** (*[1] 2.19. likelihood*) annak esélye, hogy valami történik.

A **kockázatfelmérés** (*[1] 2.14. risk assessment*) folyamata magában foglalja a kockázatazonosítást, a kockázatelemzést, valamint a kockázatértékelést.

Ennek során a **kockázatazonosítás** (*[1] 2.15. risk identification*) a kockázat elemeinek feltárására, felismerésére és leírására szolgáló folyamat.

A **kockázatelemzés** (*[1] 2.21*. risk analysis) egyrészt a kockázat sajátosságának megértését, másrészt a kockázati szint meghatározását foglalja magában.

A **kockázatértékelés** (*[1] 2.24. risk evaluation*) a kockázatelemzés eredményének összevetése a kockázati kritériumokkal annak megállapítására, hogy az adott kockázat és/vagy annak nagysága elfogadható-e vagy elviselhető-e).

A **kockázati kritériumok** (*[1] 2.22. risk criteria*) jelentik azokat a feltételeket, amelyek mellett a kockázat jelentőségét megítélik.

A **kockázati szint** (*[1] 2.23. level of risk*) egy vagy több kockázat nagysága vagy valószínűsége és következménye kombinációjaként fejezhető ki.

A kockázati mátrix

A **kockázati**, vagy precízebben a **következmény-valószínűségi mátrix** egy, közvetlenül a kockázat fogalmán alapuló kvalitatív eszköz. Kockázati mátrixon olyan

táblázatot értünk, amelynek celláiba az összegyűjtött, és valamilyen szinten megismert kockázati eseményeket helyezzük el. A táblázat oszlopkategóriái felelnek meg az események bekövetkezési valószínűségi kategóriáinak 0-100%-ig növekvő sorrendben. A gyakorlatban általában 3 és 7 közötti számú kategóriát szokás képezni. A táblázat sorai a kockázati események bekövetkezése esetén várható kár, vagy veszteség – általában negatív következmény mértékét tartalmazzák, szintén 3 – 7 kategóriába sorolva (l. alább részletesebben!). A mátrix alsó soraiban szerepelnek a kisebb, felfelé haladva a növekvően az egyre nagyobb lehetséges kárt okozó események. A lényegen természetesen nem változtat, ha a mátrix sorait és oszlopait felcseréljük.

Ez az elrendezés azt eredményezi, hogy a mátrix bal alsó tartományába kerülnek a kis kárt okozó, és kis valószínűséggel bekövetkező, vagyis a kis kockázatot jelentő kockázati események. A jobb felső sarokban találhatjuk a bekövetkezésük esetén nagy kárt okozó, és egyben nagy valószínűséggel bekövetkező eseményeket. Ezek képviselik a nagy kockázatokat. A mátrix bal felső (kis valószínűség és nagy kár), középső (közepes gyakoriság és közepes méretű káresemény), valamint a jobb alsó (nagy valószínűséggel előforduló kisebb jelentőségű károk) tartományai képviselik a különböző mértékű közepes kockázatokat.

A mátrix celláit a kockázatok mértéke szerint kategóriákba csoportosíthatjuk. Beoszthatjuk például elhanyagolható, kis, közepes, nagy és katasztrofális kockázati tartományokra. A besorolás alapján alapvetően meghatározhatjuk, hogy az adott kockázati eseményt milyen módon kívánjuk kezelni. Például lehet, hogy az elhanyagolható kockázatokkal nem akarunk foglalkozni, a katasztrofális események kockázatait viszont mindenképpen el akarjuk kerülni. A közbenső mértékű

kockázatokra különböző megelőző, vagy bekövetkezési valószínűségüket csökkentő, vagy azok esetleges következményeit enyhítő intézkedéseket tervezhetünk be.

A kockázati mátrix eredete

A kockázati, vagy kockázatbecslési mátrix módszerének gyökereit, fogalmi alapjait a tárgyalásunkhoz közelfekvő módon talán legkorábban amerikai katonai szabványokban találhatjuk meg. Az 1949-től kezdődően fokozatosan fejlődő MIL-STD-1629-es szabvány [3] a hibamód- és hatáselemzés (FMEA, vagy FMCA) módszer alapján a hibák okaira és a meghibásodási valószínűségekre összpontosít. A módszer fontos célja, hogy ezeket az eseményeket sorrendbe állítsa, és ezáltal a kezelésükre prioritási sorrendet állítson fel.

A MIL-STD-882-es szabvány 2000-es változata már színkódokkal ellátott kockázatbecslési mátrixot mutat be [4], mely az ISO szabványban leírtaknak felel meg, lényegében csak elrendezésében tér el attól. Megjegyzendő, hogy a dokumentum teljes és részletes folyamat-végrehajtási modellt tartalmaz.

A NASA szerzői módszertani könyvtárat állítottak össze a rendszerfejlesztő mérnökök számára [5], melyben a biztonsági és megbízhatósági módszertanok, illetve eszközök közt a kockázatbecslési mátrixot írták le a módszerek közül legelsőként. Ebben az anyagban hangsúlyosan szerepel, hogy a módszer lényeges célja a kockázatok kezelésére vonatkozó intézkedések kidolgozása érdekében a kockázatok kategorizálása.

A kockázati mátrix módszere az ISO 31010 szabvány szerint

Az ISO 31010-es (l. [2]) szabvány leír számos, a kockázatértékelés során alkalmazható eljárást. Ezek közül a B.29-es fejezet foglalkozik a

következmény/valószínűség mátrix, vagy elterjedt nevén a **kockázati mátrix** módszerének leírásával.

A szabvány szerint a „következmény/valószínűség mátrix a következmény és a valószínűség minőségi vagy félig mennyiségi rangsorolásának kombinált eszköze egy kockázati szint vagy kockázati rangsor előállítására”. (l. [2] B29.1)

A kockázati mátrix egyes forrásokban található, egymással nem mindig teljesen egybevágó értelmezései, vagy az esetlegesen félreértések elkerülése érdekében foglaljuk össze a kockázati mátrix elkészítésének folyamatát a szabványt követve (nem törekedve szó szerinti idézetek kiemelésére).

Bemeneti információként vesszük az azonosított – hagyományosan legtöbbször negatív hatásúnak tekintett – kockázatokat[1]. A kockázatok listája tartalmazza általában a kockázat (kockázati esemény) megnevezését (célszerűen egy egyértelmű azonosítókóddal ellátva), az esemény bekövetkezésének valószínűségét (gyakoriság, a bekövetkezés esélye), illetve az esemény bekövetkezése esetén várható negatív következmény (kár, veszteség, súlyosság, kihatás) nagyságát.

Az egyes kockázatokat célszerű azok területei szerint kategóriákba sorolni, mint például pénzügyi kockázatok, egészségügyi kockázatok, egészségi és biztonsági kockázatok, környezeti kockázatok, hírnév- és jogi kockázatok, hogy a szabvány példájából néhányat említsünk.

A bekövetkezési valószínűségre felállíthatjuk például a következő ötfokozatú skálás: „valószínű”, „lehetséges”, „valószínűtlen”, „ritka”, „nem valószínű”. A gyakorlatban

[1] Az egyszerűség kedvéért a tárgyalásban maradunk ennél a megközelítésnél. Ne feledjük azonban, hogy az új szabvány a kockázatra nem csak, nem feltétlenül negatív eseményként, hanem pozitív eseményként, lehetőségként is tekint.

– a célszerűség és a terület igényei szerint – 3-tól 7 kategóriát alkalmaznak. Több kategória alkalmazásának – a kvalitatív megközelítés miatt – nem nagyon van létjogosultsága. A skálára – ha a lehetőségek engedik, illetve a célszerűség is úgy kívánja, illeszthetünk numerikus skálát. Az előbbi ötfokozatú skálához alkalmazhatjuk például a 0-20%, 20-40%, 40-60%, 60-80%, illetve 80-100% valószínűségi tartományok. Választhatunk nem lineáris skálát. Ennek tipikus esete az, amikor a „valószínű", illetve a „nem valószínű" kategóriatartományokat akarjuk szűkíteni, és például a 0-5-35-65-95-100% osztást alkalmazzuk.

Hasonló a helyzet a következmények kategorizálása esetén, azzal az eltéréssel, hogy míg a bekövetkezési valószínűségek esetén numerikus skálák bevezetésekor egyértelműn %-os értékeket alkalmazhatunk, addig a következmények nagysága esetén a következménykategóriákhoz próbálunk igazodni. A pénzügyi kockázatokat igyekszünk pénzösszegekben kifejezni. Az egyéb jellegű (egészség, biztonság,…) kockázatokat természetes mértékegységekben, vagy ezeket értékelve, pénzben kifejezve adhatjuk meg. Amennyiben ez nem lehetséges, vagy túl bonyolult az elérendő célok tükrében, maradhatunk a becsült, kvalitatív skálánál.

Ezt követően a következmény nagysága (következményrangsor), illetve a valószínűségek rangsora szerint felállítjuk a következmény/valószínűség mátrixot. Ennek celláihoz rendeljük hozzá a kár mértéke és a bekövetkezés valószínűsége szerint az egyes kockázatokat. Az alábbi ábra a szabványban felrajzolt 6*5-ös mátrixot mutatja.

Valószínűségi rangsor							
	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		Következményrangsor					

2. ábra: Minta kockázati mátrix az ISO 31010-es szabvány szerint

A mátrix összekapcsolja a kármértékeket a valószínűségekkel, és lehetőséget ad az egyes kockázatok mértéke szerinti kockázatkategóriák kialakítására. A kockázatkategóriák a kockázati mátrixban tipikusan bal-felső, jobb-alsó irányú átlós tartományokat alkotnak.

A mátrix alkalmazásának jogosságát – a szabványt követve – úgy magyarázhatjuk, hogy nyilván teljesen elfogadhatatlan egy nagy kárt okozó esemény nagy valószínűségű bekövetkezése. Ez lenne a fenti mátrixban a I., az „elfogadhatatlan” kockázatok kategóriája. A növekvő római számok az egyre alacsonyabb kockázati szinteket jelölik.

Ugyanakkor bizonyára meg lehet barátkozni egy nagyon kis kárt okozó olyan eseménnyel, mely valószínűleg sosem fog bekövetkezni. Ez felel meg a fenti ábrán a római V-tel jelölt cellák tartományának, melyhez az elfogadhatóan kis kockázatok tartoznak.

Az egyes kockázati kategóriákat gyakran jelölik színkódokkal, ahol „természetesen” a piros jelöli a nagy, a zöld szín pedig az alacsony kockázatú tartományokat.

A folyamat végén a korábbiakban meghatározott kockázati szinteket döntési szabályokhoz kapcsolhatjuk, mint például: V – feltétlenül kezelendő, I – nem foglalkozunk vele. A döntési kategóriák a kockázatkezelési intézkedések olyan fontos paramétereit határozzák meg, mint: az odafigyelés szintje (pontosság, hiba-tolerancia, megfigyelési gyakoriság); az elhárítási képességre fordítandó erőforrások nagysága; a szükséges válasz (ellenintézkedés) időskálája (prioritás, sürgősség).

Megjegyeztük a fentiekben, hogy az értékelésekhez használhatunk kvalitatív, illetve kvantitatív hozzárendelési skálákat is, a szabvány nem köti meg a kezünket. Az is logikusan követhető a „józan paraszti ész” segítségével, hogy a nagy valószínűséggel bekövetkező katasztrófa nagy kockázati szintet jelent, a szinte sosem megtörténő „apróságok”-kal viszont foglalkozni sem kell. Hogyan kapcsolódnak egymáshoz, illetve hogyan indokolhatók valójában a kockázati mátrix kockázati szintjeinek általában átlós, sávszerű kockázati tartományai?

Tegyük fel azt az esetet, hogy alkalmazási esetünkben tisztán kvalitatív skáláknál maradtunk. Számozzuk be mind a vízszintes következményrangsor, mind a függőleges valószínűség kategóriáinkat egytől kezdve növekvően. Képezzük a mátrix minden egyes cellájára a vízszintes, illetve a függőleges tengelykategóriák számértékeinek szorzatát. Látható, hogy a bal alsó cellára 1, a jobb felső cellára 30-as értéket kapunk, s egyébként az azonos értékű cellák kirajzolják az átlós sávokat.

A szabvány szerint a mátrix módszer erősségei az egyszerű használat, és a kockázatok kockázati szintekbe való gyors besorolhatósága. Hátrányként említi, hogy a módszert a körülményekhez kell testre szabni; nehéz, és szubjektív a skálák meghatározása; a kockázatokat nem szabad összegezni (n db kis kockázat nem

azonos 1 db közepes kockázattal); nehéz a különböző kockázati dimenziók összehasonlítása; az eredmények az elemzés részletességétől függenek. A további megjegyzések részleteitől most tekintsünk el. Feltétlenül elmondható azonban, hogy a „fent", átfogó szinten viszonylag egyszerű módszer a valóságban, az egyes események részletes értékelésekor mégis csak sok munkát igényel.

A mátrix módszer alkalmazása – éppen annak egyszerűsége miatt – manapság elég széles körben elterjedt. Nem csak pénzügyi, vállalati kockázatelemzéseknek képezik sokszor alapeszközét. Alkalmazzák szervezetek, önkormányzatok, sőt a jogi szabályozásban is egyre többször alkalmazzák [6].

A kockázati mátrixok kritikája

Nem meglepő, hogy a kockázati mátrix módszerek és azok egyes változatai – mint régóta és széles körben alkalmazott eljárások – számos értékelésnek, kritikai megjegyzéseknek képezték tárgyát. (l. például [7], [8], [9], [10], [11], [12]). Ebben a cikkben nem célunk ezen felvetések részletes tárgyalása. A mátrix-módszer legfontosabb kritikai szempontjaiból azért emelünk ki itt néhányat, hogy elősegítsük a kockázati mátrix és a kockázati térkép alkalmazási szempontjainak jobb elkülönítését.

- Megbízhatatlanság: A mátrixok a tényleges kockázatoknak véletlenül és önkényesen kiválasztott, sokszor igen csak kis töredékét tartalmazzák.
- Gyenge felbontás: Nagyon eltérő kockázatokat rendelnek azonos kategóriákhoz.
- Hiba: Egy esetlegesen lehetséges kvantitatív értékeléshez képest torzító kvalitatív értékelést adnak.

- A mátrixok kategóriabeosztásaival nem biztosítható hatékony erőforrásfelhasználás.
- Mind a bemenő, mind a kimenő adatok értékei, és értékelése bizonytalanok.

Kockázati térképek

Egy kis kirándulás

Nézzük a kérdést kissé messzebbről! Akár kvalitatív, akár kvantitatív skálán dolgozunk, feltételezhető, hogy a nagyobb kárértékek a vízszintes skálán jobbra, a nagyobb valószínűségek a függőleges skálán feljebb helyezkednek el – feltételezve, hogy a mérések, vagy a szakértői becslések során nem tévedtünk. Érezzük, hogy minél nagyobb a kár mértéke, és minél valószínűbb az esemény bekövetkezése, annál nagyobb az érzékelhető a kockázati szint.

Váltsunk a kvalitatív módszerekről minden szempontból kvalitatív értékelésre. A kockázati mátrix módszerben – amennyiben a kockázati szintet nem csupán a mátrix egyes celláihoz való kvalitatív hozzárendeléssel, hanem számszerű értékelés céljából számítási úton is szeretnénk meghatározni, a fentiekből szinte adódik, hogy a kockázatot a kár mértéke és a bekövetkezési valószínűség szorzataként számolhatjuk. Erre vonatkozóan ad szélesebb kitekintést Zambon és munkatársainak cikke [13], ahol az általa 5-ös kategóriába sorolt, hagyományos kockázatszámítási eljárást a következők szerint adja meg:

Kockázat(Esemény, Érték) = Valószínűség(Esemény) * Következmény(Esemény, Érték)[2]

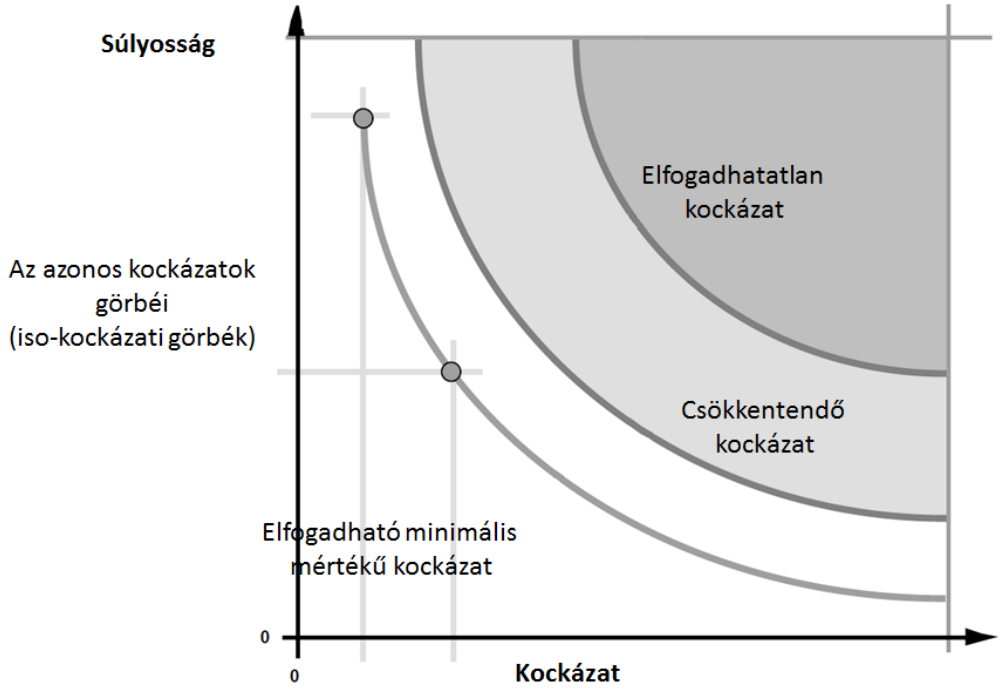
Ezekkel a lépésekkel odajutottunk, hogy az eredetileg döntően kvalitatív módszerben a fél-kvantitatív megoldásokon át eljutottunk a kvantitatív elemzés lehetőségéig.

A hagyományos kockázati térkép

A kockázati térkép esetében a kockázati esemény jellemzőit szintén két tengely mentén mérjük fel, és így ábrázoljuk azt a koordinátarendszer síkjában. Hagyományosan a kockázati mátrix módszeréhez hasonlóan legtöbbször ez esetben is a kockázati esemény hatásának nagyságát ábrázoljuk a vízszintes tengelyen, és az esemény bekövetkezési valószínűségét a függőleges tengelyen, vagy éppen fordítva, ami a lényegen természetesen nem változtat. A kockázati térképek legtöbbjén a mennyiségeket abszolút értékben szokás szemléltetni.

A NASA korábban hivatkozott kockázatbecslési eszköztárában [5] a kockázati mátrix módszerhez kapcsolódóan sematikus kockázati térképet mutat be. Ennek ott elsődleges célja, hogy a fenti Kockázat = Valószínűség * Következmény összefüggést, és az annak megfelelő azonos kockázatokat reprezentáló ún. iso-kockázati görbéket szemléltesse. (Az ábra átvéve a NASA hivatkozott dokumentumából.)

[2] Megjegyzendő, hogy a szerzők a szorzásjel helyett általánosításként a ⊗ szimbólumot használták annak érzékeltetésére, hogy a művelet lehet szorzás, vagy általában „szorzásjellegű” művelet. A szorzásjel használata a tárgyalásunk szempontjából teljesen megfelelő.



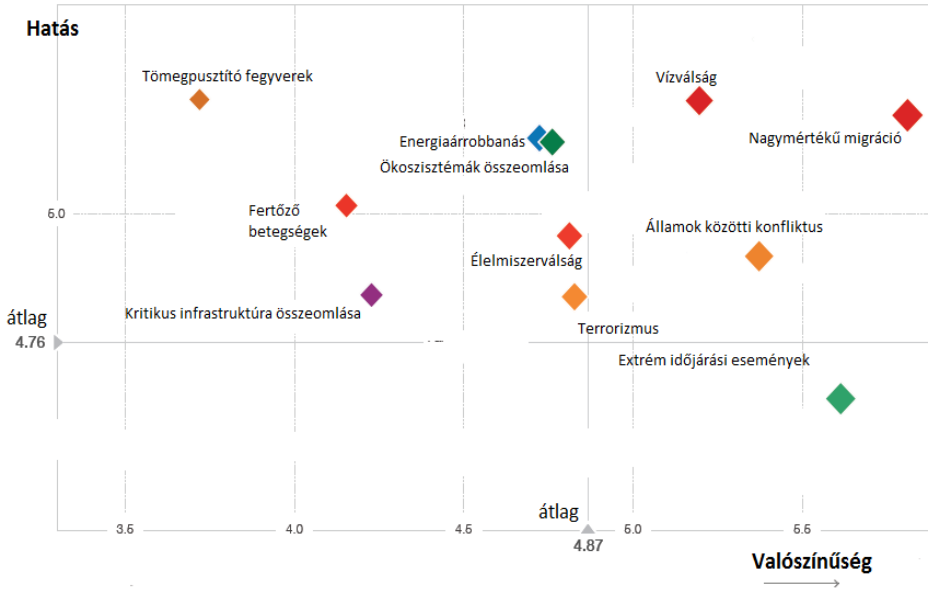
3. ábra: A kockázati mátrix módszer alapján létrejövő azonos kockázati görbék szemléltetése a NASA kockázatkezelési eszköztára alapján

Mennyiben léptünk előre a kockázati mátrixokhoz képest?

A kockázati térkép alkalmazásának úgy van valójában értelme és létjogosultsága, ha a kockázatelemzést teljes mértékben kvantitatív módon végezzük. Természetesen adódhatnak határesetek, vagy kivételek is.

A kockázati térképekről tehát általánosan azt mondhatjuk, hogy azok a kockázati eseményeket pontszerűen ábrázolják. A szemléltetés kedvéért álljon itt egy kockázati térkép a globális kockázati jelentés 2016-os kiadványból [14].

(Figyelem: az alábbi ábra a hivatkozott irodalom töredékes, átszerkesztett változata, kizárólag csak szemléltetésre alkalmas, viszont jól szemlélteti a manapság „divatos” nemzetközi ábrázolási módszereket.)



4. ábra: Példa egyszerű kockázati térképre

Mi az előnye ennek az ábrázolásnak a kockázati mátrixokhoz képest?

Először is, ahogyan már megállapítottuk, a valószínűségeket és a hatások mértékét kvantitatív skálán ábrázoljuk. Ebből az egyszerű tényből azonban számos más előny következik. Egyrészt ez a megközelítés sokkal nagyobb felbontást tesz lehetővé. Az egyes kockázatok mértékét, kisebb-nagyobb viszonyukat egymáshoz képest pontosan szemléltethetjük. A térképen az egymáshoz közel fekvő eseményeket is elkülönülten jeleníthetjük meg.

A kockázati térkép az emberi szemlélő számára automatikusan közvetíthet további jelentéstartalmakat. Ilyen lehet például a kockázati események számossága egy

tartományban, vagy az ábrázolt pontok valamilyen szabályszerűségre – például korreláció – utaló elhelyezkedése. Az emberi szemlélő számára azonnal felfedezhető például a pontcsoportok sűrűsödése esetleges is, ami alapján a gyakorlathoz jól, vagy jobban igazodó kategorizálást végezhetünk, mint pusztán csak mechanikus módszerek alkalmazásával.

Kiegészítő lehetőségek

Kockázati kategóriák

A kockázati mátrixokban a kockázatkezelési kategóriák – tehát pl. tűrhetetlen, csökkentendő, elfogadható – érzékeltetésre szokás színkódokat használni. Ha átváltunk a kockázati mátrixon alapuló ábrázolásról a kockázati térképen történő megjelenítésre, első ránézésre is feltűnik, hogy mivel minden egyes kockázati eseményt külön pontban ábrázolhatunk, lehetőségünk van arra, hogy minden egyes eseményt külön színkóddal lássunk el. Felhasználhatjuk ezt a pótlólagos lehetőséget az adott kockázatok kockázati kategóriájának megjelenítésére, mint ahogyan a globális kockázati jelentés fenti ábráján a kék szín gazdasági kockázatot, a zöld szín környezeti kockázatot, a piros társadalmi kockázatot, stb. jelent.

A mennyiségek pontossága

Megállapítottuk, hogy a kockázati térképeken egyértelműen kvantitatív ábrázolási lehetőségünk van. Ez egyben azt is jelenti, hogy az adott mennyiségek ábrázolásához hibahatárokat is megjelölhetünk, melyekkel utalunk a valószínűségek becslése, vagy a kockázat várható hatásnak megállapítása során alkalmazott eljárások bizonytalanságára. Ezeket a hibalehetőségeket a

diagramokon célszerűen hagyományos módon a hibahatárokat jelölő vonalakkal, szakaszokkal mutathatjuk be.

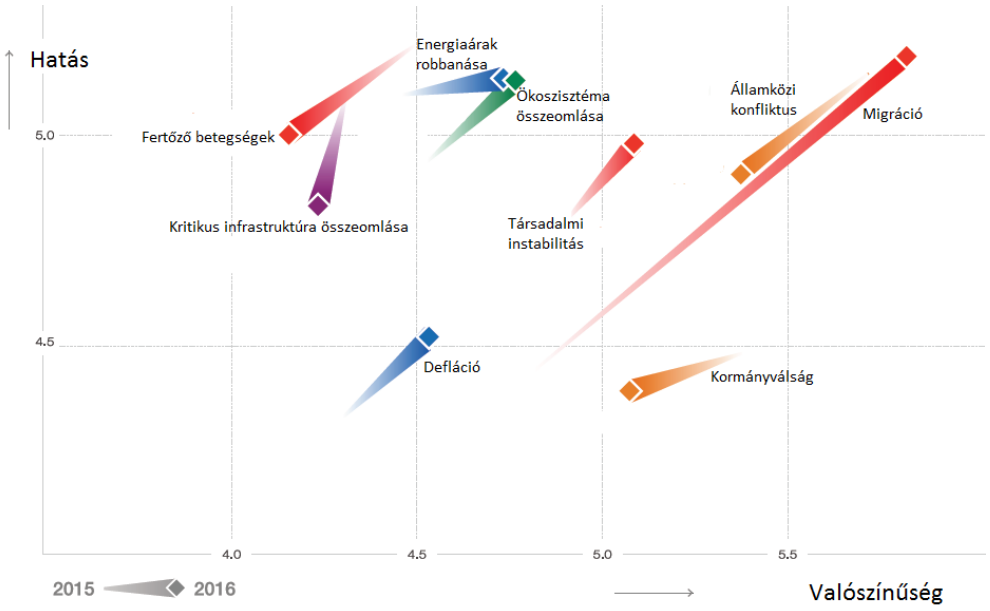
Erre a lehetőségre azért szeretnénk külön és hangsúlyosan is rámutatni, mert a hibaértékek megjelenítésével lehetőségünk van arra, hogy a döntéshozó, mint a kockázati térkép felhasználójának figyelmét felhívjuk az információ bizonytalanságára. Ilyen kiegészítő információk megfelelő bemutatásával, és természetesen az ehhez szükséges háttérinformációk biztosításával elvileg (!) részben csökkenthető a téves döntéshozatal kockázata.

A kockázat időbeli fejlődésének ábrázolása

A kérdéses kockázati események időbeli fejlődésének szemléltetése különösen fontos lehet például egy vállalat vezetősége számára, hiszen a változás irányvonalainak meghosszabbítása, extrapolálása révén előre jelezhetjük az ugyan még éppen nem a „tűrhetetlen” kategóriába eső, de várhatóan oda fejlődő kockázatokat.

a) Időszaki változás szemléltetése

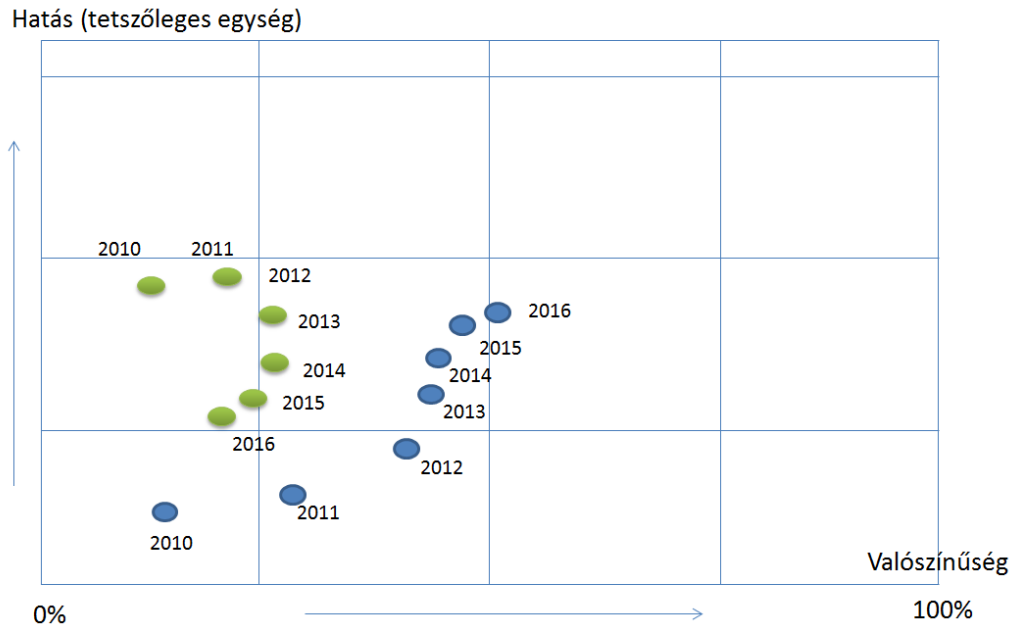
Az alábbi ábrán a globális kockázati jelentésből [14] vett ábra kiválasztott kockázatok változását szemlélteti a 2015-ös évről a 2016-os évre vonatkozóan a diagram bal alsó sarkában látható jelölés szerint. (az ábra ez esetben is kivágott, szerkesztett részlete az eredetinek, kifejezetten szemléltetési céllal).



5. ábra: Példa éves változás megjelenítésére kockázati térképen

b) Időbeli fejlődés szemléltetése

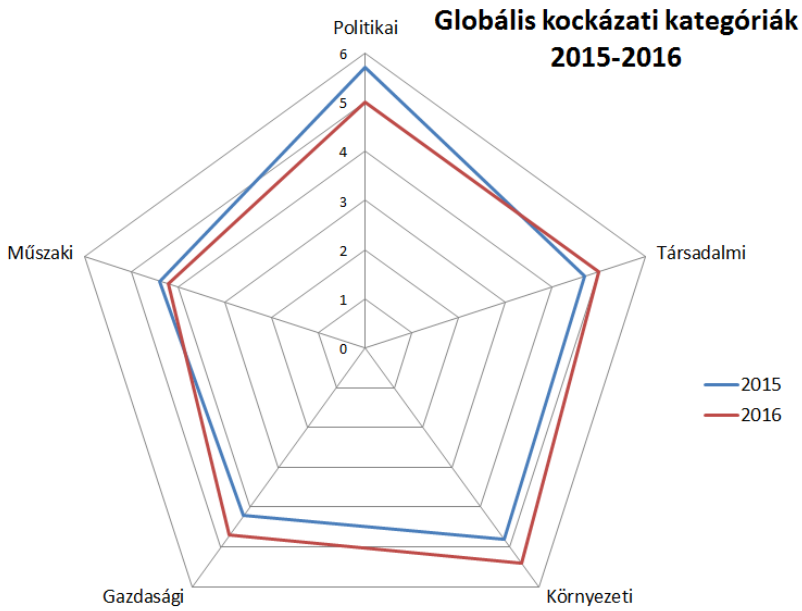
A következő kockázati térkép két lehetséges kockázati esemény időbeli fejlődését szemlélteti hosszabb időtávon (saját szerkesztés). A korábbi példák alapján érzékelhetjük, hogy még rengeteg információ megjelenítésére lenne lehetőségünk további képi elemek felhasználásával.



6. ábra: Példa hosszabb időbeli fejlődés megjelenítésére kockázati térképen

Csak, hogy néhány példát említsünk: a kockázati pontok szimbólumának alakja jelölheti a kockázati kategóriát (pl. rombusz: pénzügyi kockázat, kör: környezeti kockázat, stb.); a szimbólum színe jelölhetné az időegység alatti változás sebességét, és/vagy irányát (pl. zöld: lassú változás, vagy a kockázat mértéke csökken; piros: gyors változás, vagy a kockázat növekszik, illetve közelít a kritikus mértékhez). A szimbólum mérete jelölheti a kockázattal érintett egyedek számát (például csődveszélyben, vagy likviditási problémákkal küzdő vállalatpopulációk nagysága; adott betegség kockázatának kitett lakosok száma, stb.).

Különböző kockázati dimenziók ábrázolása



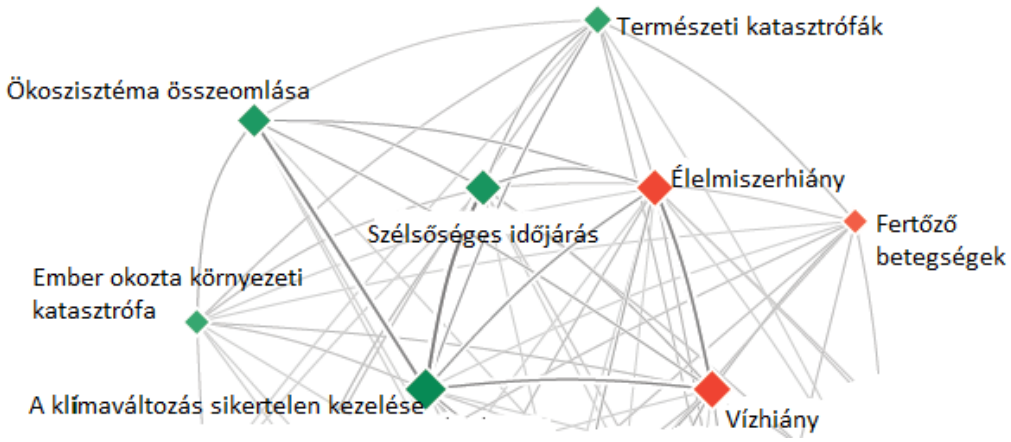
7. ábra: Szemléltető példa különböző kockázati dimenziók, például kockázati kategóriák szemléltetésére (A diagramon kizárólag szemléltetési céllal készült, az egyébként hivatkozott [14] irodalom valós adataival nem áll összefüggésben.)

A 7. ábra diagramja egy, a több kockázati dimenzió bemutatására alkalmas ún. sugárdiagramot mutatja be. A tengelyek mentén az egyes kockázati események meghatározott paramétereit, vagy – ahogyan a minta mutatja – a már számított kockázat értékét vehetjük fel. Jelentéstartalommal bírhatnak az egyes tengelyekre felvett konkrét értékek, illetve az ezekből valamilyen számítással meghatározott módon származtatott mennyiségek értékei. Ilyen szemléletes mennyiség lehet például a pontok által kirajzolt sokszög területe.

A kockázatok további kreatív ábrázolási lehetőségei

Ebben a szakaszban a kockázatok néhány olyan ábrázolására mutatunk példákat, melyek tulajdonképpen nem tartoznak a hagyományos értelemben vett kockázati térképekhez. Nem feltétlenül az adott kockázati események paramétereit ábrázoljuk, sőt nem is feltétlenül koordinátarendszerben helyezzük el a kockázati pontokat.

A korábbi példával összefüggésben az alábbi ábra a globális kockázati jelentésből [14] mutat példát a gráfokkal kapcsolt kockázatok ábrázolására (az eredeti diagramnak szintén csak részleges, szemléltetésre használható, szerkesztett változata). A hivatkozott forrásban a diagram célja a kockázatok közötti kapcsolatok erősségének szemléltetése. A vastagabb gráfélek erősebb kapcsolatot, vagy összefüggést szemléltetnek. A megjelenítési módot használhatjuk például korreláció, vagy ok-okozati összefüggések erősségének szemléltetésére is.

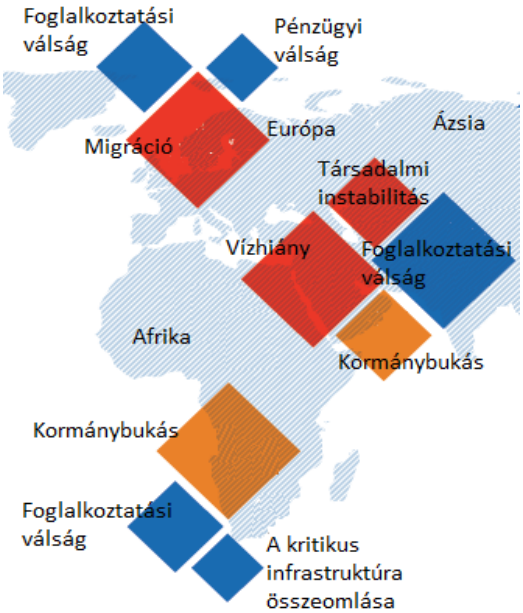


8. ábra: Példa az egyes kockázatok közötti logikai összefüggések, vagy a kapcsolatok erősségének megjelenítésére kockázati térképen

További információ megjelenítésére alkalmas ez esetben is a kockázati eseményt jelző pont színkódja, mely ebben a példában változatlanul a kockázati kategóriát jelöli. A kockázati esemény szimbólumának méretét is változtathatjuk. Ebben a példában a kockázati pont mérete az adott pontba összefutó élek számával növekszik.

Kockázati térképek a „térkép" szó valódi értelmében

a) Regionális kockázati térkép



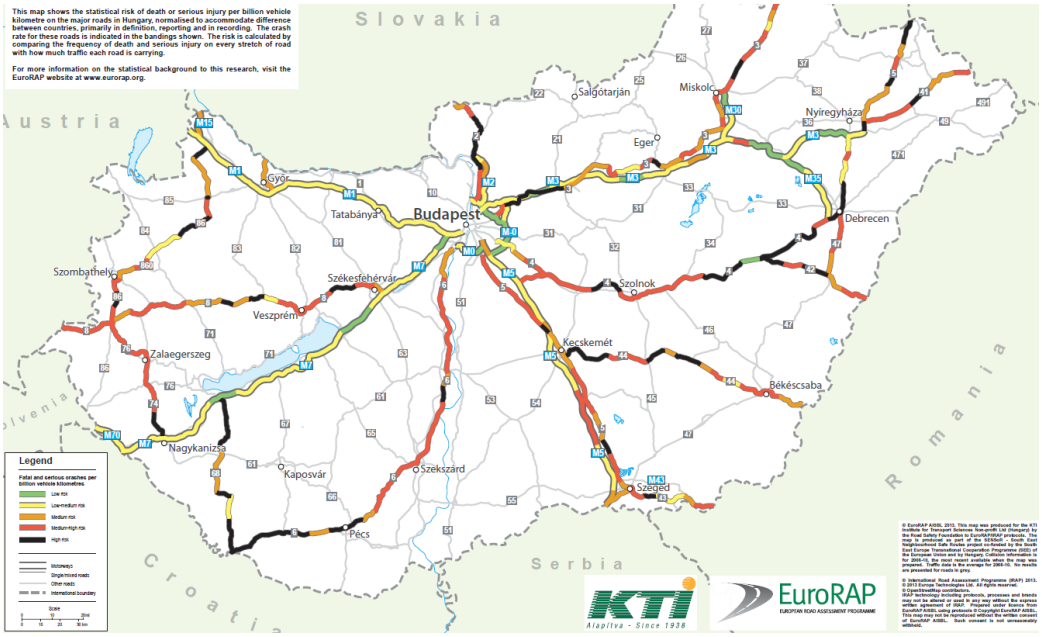
9. ábra: Az egyes régiók kiemelt kockázatainak megjelenítése

A 9. ábrán a globális kockázati jelentésből [5] szemlélteti régiónként az első három legfontosabb kockázati tényezőt.

Ez esetben valóban a hagyományos értelemben vett térképet láthatunk. A négyzetek mérete a kockázat nagyságát jelzi. (A hivatkozott irodalomból vett, szerkesztett ábrarészlet, kizárólag az ábrázolás módjának illusztrálására alkalmas.)

b) Közúti balesetkockázati térkép

A SENSOR projekt keretében készült magyar közúti kockázati térképet láthatjuk alább (l. [15]). A kockázati térkép a milliárd útkilométerre eső halálos, vagy súlyos sérülésekkel járó balesetek számát ábrázolja az ország valóságos közúti térképére vetítve, és így valóban szemléletes képet mutat a közutak baleseti kockázatáról.



10. ábra: Baleseti kockázat nagyságának ábrázolása tényleges térképen

Összefoglalás

A cikkben összefoglaltuk a kockázati mátrixok és a kockázati térképek legfontosabb tulajdonságait. A kockázati mátrix módszerét az ISO 31010-es szabvány alapján a pontatlanságok elkerülése érdekében röviden és egyszerűen leírtuk.

A kockázati térképeket fogalmilag definiáltuk. Konkrét meghatározott módszertan, vagy szabvány hiányában ezek felépítését, alkalmazási lehetőségeiket és a kockázatok szemléltetésében játszott szerepüket leírtuk. Szerteágazó típusait és az ezekhez kapcsolódó lehetőségeket számos, lényegesen eltérő változaton szemléltettük.

Az alábbiakban összefoglaljuk a kockázati mátrixok és a kockázati térképek legfontosabb jellemzőit, illetve az alkalmazás során felmerülő leggyakoribb szempontokat: a röviden megfogalmazható előnyöket és korlátokat.

Tulajdonság	**Kockázati mátrix**	**Kockázati térkép**
Kategóriák száma	általában 3 – 7	folytonos leképezés
Az ábrázolt mennyiségek	kvalitatív	kvantitatív
Szabványos	igen, pl. ISO 31010	nem
A módszer előnyei	• egyszerű, szemléletes • kis ráfordítással elkészíthető, könnyen	• szemléletes • további mennyiségek széleskörű megjelenítési

	alkalmazható • elterjedt, szabványos • a kockázatkezelési intézkedési kategóriák egyszerűen hozzárendelhetők a mátrix tartományaihoz • a diagram akár kézzel is egyszerűen lerajzolható	lehetőségei (szimbólumok alakja, színe, mérete; időszaki, időbeli fejlődés) • az ábrázolt mennyiségek pontossága, illetve bizonytalansága (!) megjeleníthető (hibahatárok a diagramon) • kreatív ábrázolási lehetőségek • valódi térképhez rendelt szemléltetés lehetősége
Korlátok	• a kategorizálás sokszor nem elegendő • az egy kategóriába rendelt elemek közötti viszonyt nem szemlélteti • a színkódolást a mátrix celláira elhasználjuk • az egyedi kockázatokra vonatkozó információkat nem tudjuk szemléltetni	• elkészítése bonyolultabb • csak viszonylag pontos bemenő adatok esetén alkalmazható • nagyobb, pontosabb előkészítő munkát igényel • a diagram elkészítése számítógépes eszközt igényel

A kockázati mátrixok tehát letisztult, egyszerűen alkalmazható, kiváló egyszerűsítő eszközei a kockázatkezelésnek. Természetesen tisztában kell lennünk a korlátaival, és csak a módszer egyszerűsége mögött álló – sokszor nagyon is túlegyszerűsítő – feltételezések tudatában, megfelelő gondossággal és óvatossággal szabad, illetve kell őket alkalmazni.

A kockázati térképek leírása közben megemlítettük, hogy adott esetben több olyan funkciójuk is van, vagy lehet, melyeket nyugodtan nevezhetünk magán a grafikus ábrázoláson túlmutató hozzáadott értéknek. Ilyenek lehetnek például a kockázati térkép típusa szerint „szemre", vagy „ránézésre" megállapítható többletinformációk: egyértelmű nagyságbeli viszonyok megállapítása; szabályszerűségek megállapítása klaszterképzéssel; az időbeli változások iránya, szabályszerűségei; előrejelzés, előretekintés, korai figyelmeztetés.

Külön kiemeltük, hogy a kockázati térképeken akár az információ bizonytalanságának mértékét is megjeleníthetjük. Ennek a lehetőségnek azért tulajdonítunk elviekben is új lehetőséget, mert ezzel csökkenthetjük a nem megfelelő mélységig értelmezett, elemzett és ábrázolt kockázati mennyiségek miatti téves döntéshozatal kockázatát.

Az információknak valódi térképekhez való hozzárendelését, azokon való ábrázolását inkább tekinthetjük a kockázati térképek továbbfejlesztésének, vagy új diagramtípusnak. Így tűnik tárgyilagosnak ez esetben az összevetés a kockázati térképen való ábrázolások és a kockázati mátrixon való szemléltetések között. Ezt a megközelítést támasztja alá véleményünk szerint az a tény is, hogy a földrajzi térképen való ábrázoláshoz – az azonosított és megismert kockázatok adatain túl – a térképészeti adatokat is fel kell használnunk. Vagyis adott alkalmazási területek

esetén a nagyobb szemléltető erőt többletinformáció – nevezetesen földrajzi térképek – felhasználásával érhetjük el.

A kockázati térképek egy más típusú hozzáadott értéke a nagyobb kommunikatív érték, mely elsősorban a több információt hordozó részleten, és az azokat jobban alátámasztó látványelemeken alapul. Szerepét tekintve jobban szolgálhatja a figyelem felkeltését, befolyásolja a döntést, jobban meggyőzheti a kérdéses döntések érintettjeit.

A projektek és a vállalatok külső kommunikációjában is jóval nagyobb lehet az információs szerepük és az általuk közvetített üzenetek átütő ereje.

Következtetés

Megállapítottuk, hogy mind a kockázati mátrixok, mind a kockázati térképek a kockázatelemzés hasznos segédeszközei.

Szerepüket a kockázatkezelés folyamatában főként a következő pontokhoz köthetjük:

- az azonosított kockázatok szemléltető ábrázolása
- a szemléltetés hozzájárulása a kockázatok esetleges jobb megértéséhez
- a kockázatok kategorizálása a kockázatkezelésre vonatkozó intézkedési válaszok szükségessége és azok szükségletei szerint, jobb minőségű döntéselőkészítés
- hozzájárulás a vezetői információkhoz, a minőségi vezetői döntés elősegítése

Azt, hogy mely eszközt milyen esetben miért, hogyan, esetleg a döntési lánc mely szakaszában, vagy esetleg kombinálva alkalmazzuk, az előnyök és a hátrányok mérlegelésével általában egyedi mérlegeléssel célszerű eldönteni. A mérlegelés során nem hagyhatjuk el a gazdaságosság kérdését sem, vagyis hogy az adott módszer alkalmazása mekkora erőforrásráfordítással jár, és ettől milyen előnyök remélhetők.

Ezen a ponton még egyszer hangsúlyozzuk, hogy a megfelelő kockázati térkép kiválasztása és alkalmazása a kockázatelemzésben valódi hozzáadott értéket jelenthet. Egy jól megválasztott „színes és szagos" kockázati diagram adott körülmények között jóval nagyobb kommunikatív értékkel és átütőbb meggyőző erővel bírhat, mint egy egyszerű kockázati mátrix.

Kockázati mátrix, vagy kockázati térkép? Az alkalmazás tekintetében nem állíthatjuk egymással szembe a két eszközt. Az egyik nem jobb, vagy nem rosszabb, mint a másik, csak kissé más. Mindkét eszközt a korlátaik és a mögöttük álló egyszerűsítések tudatában kell alkalmazni. Ez sok esetben lehet, hogy nem vagy-vagy kérdés. Alkalmazhatjuk mindkettőt egymás kiegészítésére is az éppen elérendő célok tükrében.

Források és hivatkozások

[1] MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek. Magyar Szabványügyi Testület. Budapest, 2015.

[2] MSZ EN 31010:2010 Kockázatkezelés. Kockázatfelmérési eljárások (IEC/ISO 31010:2009). Magyar Szabványügyi Testület. Budapest, 2010.

[3] Procedures for Performing a Failure Mode, Effects and Criticality Analysis. U.S. Department of Defense. MIL–P–1629. 1949.

[4] System Safety. Department of Defense, Standard Practice. U.S. Department of Defense. MIL-STD-882E. 2000.

[5] B.E. Goldberg, K. Everhart, R. Stevens, N. Babbitt III, P. Clemens, and L. Stout: System Engineering "Toolbox" for Design-Oriented Engineers. NASA Reference Publication 1358. 1994.

[6] A Kormány 234/2011. (XI.10.) Korm. rendelete a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról. Magyar Közlöny (131. sz. 32252-32297. o.). Budapest. 2011.

[7] COX, L. A. T., Jr. What's Wrong with Risk Matrices? Risk Analysis, Vol. 28, No. 2, 2008.

[8] PICKERING, A., COWLEY, S. P.: Risk Matrices: implied accuracy and false assumptions. Journal of Health & Safety Research & Practice. vol. 2. issue 1. october 2010.

[9] PEACE, C.: Advice ont he risk estimation matrix used by DAFF Biosecurity as part of the Import Risk Analysis process. (Client Report CR0127. Australian Senate Rural and Regional Affairs and Transport Committee). Wellington, NZ. Risk Management Ltd. 2013.

[10] THOMAS, P., BRATVOLD, R. B., BICKEL, J. E.: The Risk of Using Risk Matrices. SPE Economics & Management, April 2014.

[11] ELMONSTRI, M.: Review of the strengths and weaknesses of risk matrices. Journal of Risk Analysis and Crisis Response, Vol. 4, No. 1 (March 2014), 49-57.

[12] DUIJM, N. J.: Recommendations on the use and design of risk matrices. Safety Science, 76, 21–31. 2015.

[13] ZAMBON et al.: Model-based qualitative risk assessment for availability of it infrastructures. Softw. Syst. Model., 10(4):553–580, October 2011.

[14] World Economic Forum, The Global Competitiveness and Risks Team: The Global Risks Report 2016, 11th Edition. World Economic Forum. 2016.

[15] SENSOR – South-East Neighbourhood Safe Road projekt, South-South-East Europe Road Risk Maps (http://sensorproject.eu/see.html) 2016.05.30.

MEGYERI Lajos: A Magyar Honvédség nyílt és a polgári elektronikus információs rendszerek működtetésének azonos és eltérő szabályai

Absztrakt

Az információk ismerete, továbbítása az ősidőktől kezdve fontos szerepet játszott az emberek életében. A XXI században az informatikai és kommunikációs eszközök fejlődésével az emberek által megismerhető információk mennyisége és kezelésének sebessége ugrásszerűen megnőtt. Kiemelt fontosságú, hogy az információt kezelő elektronikai rendszerek tervezését, használatát üzemeltetését egységes elvek alapján, szabályozottan tegyük. Jelen dolgozatban a szerző bemutatja a katonai elektronikus adatkezelő rendszerek felhasználói szintű üzemeltetéséhez jogszabály által előírt szabályzat felépítését, tartalmát, esetenként összehasonlítva polgári elektronikus adatkezelő rendszerek működését szabályozó okmányainak azonos és eltérő elemeire.

***Kulcsszavak**: Információ - Information , továbbítás – transmission, biztonság – security, védelem – protection, rendszabályok – rules, üzemeltetés - operations*

Bevezető

Az állandó vezetékes kommunikációs hálózat története Magyarországon 1881.-ben kezdődött, ekkor helyezték üzembe az első telefonközpontot Budapesten. A telefonközpontok, hálózatok folyamatosan fejlődtek, újabb átviteli elvek és a technikai eszközök alkalmazásával használatuk a mai napig folyamatos.

A telefon használatának kezdetben csak etikettszerű szabályai voltak, mint pl. bemutatkozás, később a készülékek hivatali használatba vételekor hivatalos szabályrendszert alkottak arra vonatkozólag, hogy kinek milyen jogosultsága van a

különböző hívások kezdeményezésekor. Nagyon szigorú előírások voltak a telefonon bonyolítható beszélgetések jellegével kapcsolatban is. A telefon lehallgatás szinte egyidős magával a telefon megjelenésével, és igen hamar rájöttek a felhasználók, hogy titkaik nincsenek biztonságban a vezetékes vonalak teljes hosszában. Ezért fontos információkat „titkokat" csak meghatározott technikai megoldások vagy más rejtjelző technikák alkalmazásával továbbítottak telefonon. Az így kialakított biztonsági alapelvek a mai napig érvényesek.

Az 1960.-as évek végén a már világméretű telefonhálózati rendszer szolgáltatásait egy addig ismeretlen kihívás elé állították. A számítógép feltalálása és folyamatos fejlesztése során ugyanis megszületett az igény azok összekapcsolására. Kézenfekvő volt a lehetőség, hogy ezt a meglévő telefonvonal hálózaton tegyék. Az USA védelmi minisztérium kutatóintézete (ARPA)[1] kifejlesztette az általam ismert első számítógépes hálózatot, melynek célja a számítógépek közötti közvetlen adatcsere kapcsolat megteremtése volt. A hálózat működtetése és fejlesztése teremtette meg a ma használatos internet alapjait.

Az informatika fejlődésével annak árnyoldalai is egyre inkább előtérbe kerültek. A szakképzetlenség mellett elterjedt bizonyos programok, kódok rosszindulatú vagy anyagi hasznon szerzés szándékával történő terjesztése. Az informatikai rendszerek védelmében védelmi eszközöket és eljárásrendeket kell alkalmazni.

A távközlési szolgáltató szervezetek fejlődésével különböző célú hálózatok épültek, mint pl. magáncélú, vagy közcélú elkülönített hálózat. A hálózatok használatának szabályai értelemszerűen erősen függnek attól, hogy milyen bizalmassági fokú

[1] ARPA - *Advanced Research Project Agency*

információt dolgoznak fel, és hogy milyen szervezet használja azokat. Az adatok elektronikus kezelését törvények, rendeletek, utasítások is meghatározzák.

Jelen dolgozatomban a szabályozás felhasználói szintjét kívánom vizsgálni. Az elektronikus adatkezelő rendszerek végpontjainál betartandó rendszabályok a különböző szakterületeken mások, mégis azonos elvek szerint, hasonló keretek között kerültek kialakításra.

A Magyar Honvédség (MH) állandó hírrendszere biztosítja a béke elhelyezési körletben települt szervezetek részére a kiképzéshez, magasabb készenlétbe helyezéshez, napi feladatok ellátásához szükséges híradó,- informatikai átviteli utakat.

A hírrendszer elemei hagyományosan két nagy csoportra oszthatóak:

Hang továbbítás és adat továbbítás: A továbbiakban az adat továbbítás kérdéskörét tárgyalom részletesen. Az adat továbbítás egyik alapvető módszere az informatikai eszközök összekötésével létrehozott informatikai hálózat szolgáltatásainak az igénybevétele.

Az informatikai hálózat szolgáltatásai messze túlmutatnak az információ továbbításon. Az informatikai hálózatban megvalósítható az információ létrehozása, átalakítása, tárolása, megosztása, továbbítása, törlése is. A funkciók bővülése nagyban megkönnyíti a felhasználók napi munkáját. Gyorsabb, kulturáltabb feladat kidolgozást tesz lehetővé, nagy lehetőségeket nyújt a párhuzamos munkavégzés, az információk azonnali megosztása terén. A gyorsabb feladat kidolgozási eljárásrendnek azonban vannak veszélyei is. Az adatok véletlen vagy szándékos jogosulatlan törlése, másolása, továbbítása, adatokhoz illetéktelen személy

hozzáférésének lehetősége nem zárható ki. Ezért nagy szükség van egy minden releváns részterületre kiterjedő szabályozásra, mely megszabja az informatikai rendszer használatának szabályait, a felhasználók és a menedzsment személyzet jogait és kötelességeit.

Szabványok és szabályozások

Az információs rendszerek életciklusa[2] során az alábbi szabályok az irányadók:

Nem minősített adatok elektronikus úton történő továbbítása esetén a polgári szabályozás alapját az MSZ/ISO 27000 szabvány képezte. Ezt a szabványcsaládot a Brit 7799 szabványcsalád alapján készítették.

Legmagasabb szintű jogi szabályozás a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, [1] mely szerint:

"*13. § (1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.*

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

[2] Információs rendszer életciklusa: tervezés,szervezés,kivitelezés, üzemeltetés,módosítás,kivonás

b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,]*"*

A törvény tehát az állami és önkormányzati szervek részére informatikai biztonsági szabályzat készítését írja elő.

Az elektronikus információtovábbítás katonai környezetben lényegében követi az MSZ/ISO 27000 szabványcsaládban foglaltakat, HM HVK[3] intézkedések, HM utasítások és MH ÖHP[4] PK parancsok formájában.

A 3/2012. (I. 13.) HM utasítás [2] pontosította a védelmi intézkedéseket, és előírta, hogy *„a biztonsági követelményeket meghatározott védelmi rendszabályokon és kialakított eljárásokon keresztül kell érvényesíteni, amelyeket Elektronikus Információbiztonsági Szabályzat (a továbbiakban: EIBSZ) formájában kell megfogalmazni, jóváhagyatni és alkalmazni*"

Mindezek alapján a nem minősített adatokat feldolgozó informatikai rendszerekkel szemben is elvárásokat támaszt, követelményeket határoz meg, ennek alapján működik például a Magyar Honvédség zárt informatikai rendszere is. Az EIBSZ az adatok megfelelő bizalmasságának, sértetlenségének és rendelkezésre állását biztosító helyi szabályozást részletesen tartalmazza. A szabályzatot a rendszer valamennyi felhasználójának ismernie kell, és évente legalább egy alkalommal foglalkozás keretében frissíteni az ismereteket.

[3] Honvédelmi Minisztérium Honvéd Vezérkar
[4] Magyar Honvédség Összhaderőnemi Parancsnokság

Minden egyes informatikai rendszernek rendelkeznie kell minden helyszínen egy helyi EIBSZ szabályzattal.

A téma egyik avatott ismerője, Kassai Károly írta:

„kiegészítő feladat, hogy a központilag meghatározott, a honvédelmi szervezeteknél készítendő Elektronikus Információbiztonsági Szabályzatra (EIBSZ) vonatkozó követelményt4 ki kell egészíteni az új jogszabályban meghatározott védelmi rendszabályokkal. [3

Elektronikus Információbiztonsági Szabályzat (EIBSZ) [4]

Az EIBSZ első fejezetében fel kell sorolni az okmány kidolgozása során alkalmazott hatályos jogszabályok és rendelkezések jegyékét. Az üzemeltetés során a szabályzatban foglaltak időszerűségét rendszeresen át kell gondolni, különös tekintettel a hatályos jogszabályok jegyzékére. Meg kell határozni a szabályzat hatályát. Meg kell nevezni azokat az informatikai és egyéb információs rendszereket (pl. rádióhálók, irányok) amelyekre a szabályzat hatálya kiterjed. A minősített adatkezelő rendszereket csak felsorolásszerűen kell megjeleníteni, azoknak a rendszereknek a használatához, üzemeltetéséhez külön okmányrendszert kell alkalmazni[5].

Meghatározásra kerül, mely szervezetekre, személyekre terjed ki a szabályzat hatálya és az elkészült okmányt olyan szintű elöljáróval kell jóváhagyatni, aki állományilletékes a szabályzatban foglalt szervezetekre, személyekre nézve. Definiálni kell az alapfogalmakat, mint például adat, hozzáférés, bizalmasság,

[5] Rendszer Biztonsági Követelmények (RBK), Üzemeltetésbiztonsági Szabályzat (ÜBSZ)

informatikai rendszer, stb. Ez fontos, mert a rendszer valamennyi használójának egy szakmai nyelvet kell beszélnie a félreértések elkerüléséért.

Részletesen meg kell határozni a felügyelő és üzemeltető szervezet megnevezését, feladatait. A feladatokat úgy kell elosztani, hogy se átfedés, se kimaradt tevékenységi terület ne legyen a végrehajtási és ellenőrzési rendszerben.

Azonosítani kell a vagyontárgyakat, melyek elsősorban számítástechnikai eszközök és programok. Különösen lényeges az azonosítás, ha más katonai szervezet az üzemeltető, mint a rendszer használója. Ez jelenleg a teljes Magyar Honvédségre jellemző állapot. Általánosságban az MH ÖHP[6] alárendelt alakulatainál az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred szakállománya végzi az üzemeltetői feladatokat az alakulatok személyi állománya felé. Ezért fontos meghatározni, melyik hálózati vagy végponti eszköz kinek a nyilvántartásában szerepel, ki felel a tárolt adatok meglétéért, az adatkezelési lépések szabályos végrehajtásáért.

A szabályzat megnevezi az informatikai rendszer szabályos működtetéséért felelős személyek nevét, beosztását, megszabja felelősségi körüket, végrehajtandó feladataikat.

A szabályzat külön fejezetben tárgyalja az MH INTRANET mint különcélú elkülönített informatikai hálózat üzemeltetésének szabályait. Nem túlzás azt állítani, hogy ez a leghangsúlyosabb része az EIBSZ.-nek, mert az MH INTRANET hálózat az MH legnagyobb és legtöbb felhasználó által napi szinten használt informatikai rendszere, ami napjainkra szinte nélkülözhetetlenné vált az alakulatok napi és béke

[6] Magyar Honvédség Összhaderőnemi Parancsnokság

kiképzési feladatainak végrehajtásához, elsősorban a mindenoldalú biztosítás és támogatás érdekében. Személyes tapasztalatom, hogy amikor néhány óra hosszára megszakadt a hálózat elérhetősége, az alakulat törzs munka intenzitása töredékére esett. .Az üzemeltetéshez szükséges okmányrendszer mintáit nem az EIBSZ tartalmazza, ezt az MH ÖHP külön intézkedésben adta ki [5]

A rendszer folyamatos és megbízható működése tehát minden katonai szervezet létérdeke, annak ellenére, hogy minősített adatfeldolgozás a vonatkozó, minősített adatok védelméről szóló törvény értelmében tilos.

A megbízható működés érdekében szigorú szabályok vannak új felhasználók felvételnél, jelszóházirend alkalmazásánál, hogy az esetlegesen bekövetkező incidens esetén visszakövethető legyen az egyes felhasználók tevékenysége a hálózaton. A felhasználók lehetőségei csak a meglévő szoftverkörnyezet használatára terjednek ki, nem telepíthetnek programokat, hardver eszközöket a hálózati végpontokra. A hordozható adathordozók (pendrive,mobil merevlemez) használatát a szabályzat elvben korlátozza, de sem szoftver sem hardver védelem nincs kiépítve a végpontokon, ami nagy veszélyt jelent a hálózat működésére. Az MH INTRANET használata során szinte csak olyan incidensek fordultak elő, melyek a hordozható adathordozók által a rendszerbe jutott rosszindulatú programok miatt alakultak ki.

A védelem lehetőségei a felhasználói és rendszer adatok rendszeres mentése külső adathordozóra és a vírusvédelmi rendszer adatbázisainak folyamatos frissítése, mely tevékenységek az EIBSZ.-ben részletesen meg vannak határozva.

Saját tulajdonú informatikai eszközök használatát az állományilletékes parancsnokok a szabályzatban szabályozhatják, általános elv, hogy ne használjunk saját eszközt katonai tevékenységre, az ettől való eltérés veszélyes, nem javasolt.

Az EIBSZ a külső szolgáltató tulajdonában lévő számítástechnikai eszköz katonai objektumba történő behozatalát, a honvédségi tulajdont képző számítástechnikai eszköz bázis objektumából történő kiviteli engedélyezését, valamint az MH tulajdonú számítástechnikai eszköz katonai objektumba történő bevitelét más alegység állományába tartozó személy részére - is részletesen szabályozza.

A szabályzat rendelkezik a szervezet internet végpontok kialakításának, üzemeltetésének, használatának a szabályairól. A munkaállomásokon (annak merevlemezén, vagy bármilyen típusú adathordozóján) az MH-ra vonatkozó és a szolgálati tevékenységgel összefüggő – nyílt, illetve belső használatra készült nem nyilvános adatok tárolása, feldolgozása és továbbítása tilos. Az INTERNET hálózatra tilos olyan számítógép rákapcsolása, amely olyan lokális hálózat tagjaként üzemel, amelynek szerverén vagy más munkaállomásain szolgálati tevékenységgel összefüggő adatokat tárolnak. Az INTERNET igénybevételére fizikailag elkülönített számítógépet vagy lokális hálózatot kell használni. Az INTERNET szolgáltatást, mint minden munkahelyen, csak a munkavégzéshez szükséges információcsere végrehajtására szabad igénybe venni, kivéve gyakorlat vagy missziós feladatok végrehajtása idején a hazai kapcsolattartás céljából telepített INTERNET végpontokat.

Az EIBSZ rendelkezik a minősített információtovábbítás és tárolás lehetőségeiről, szabályairól, beleértve a rádió csatornák zárt üzemmódban történő működtetésének lehetőségét és feltételeit is. Részletesen leírja a teendőket

felhasználó ideiglenes vagy végleges távozásakor. Rendelkezik az eseti és előre tervezett oktatások, továbbképzések lebonyolításának, okmányolásának rendjéről.

Rendelkezik a felhasználók és a rendszert üzemeltetők által végrehajtandó teendőkről bármelyik, az MH INTRANET rendszerhez csatlakoztatott eszköz meghibásodása, vagy bármely egyéb incidens esetén. Leírja a teendőket tűz vagy elemi csapás esetre.

A szabályzat név szerint meghatározza az MH INTRANET helyi rendszeradminisztrátorait és részletesen meghatározza feladataikat is. Nagy részletességgel tárgyalja a vírusvédelmi programok alkalmazását, frissítését, teendőket rosszindulatú program működésének észlelése vagy annak gyanúja esetén.

Az EIBSZ leírja a biztonsági mentésekkel, vészhelyzeti és helyreállítási tevékenységekkel kapcsolatos részfeladatokat. Rendelkezik a mobil adathordozók védelméről, selejtezésének rendjéről. Szabályozza a szervezetek közötti adatcsere végrehajtásának módját, lehetőségeit, meghatároz tűzvédelmi, munka és érintésvédelmi szabályokat is.

A záró rendelkezésekben intézkedik a szabályzat aláírója a hatálybaléptetés időpontjáról, a megelőző hasonló szabályozás hatályon kívül léptetéséről.

A szabályzatot minden katonai szervezet valamennyi önálló telephelyére, kihelyezett részlegére vagy csoportjára el kell készíteni, a helyi sajátosságok figyelembevételével. A katonai szervezet elkészítheti a szabályzatot egyben, valamennyi települési helyre érvényes módon, csak akkor telephelyenként külön kell választani a végrehajtandó feladatokat. Ez nem célszerű, mert az okmány

hosszú, nehezen olvasható lesz, esetleg félreérthető, hogy mely feladatok mely telephelyekhez tartoznak. Végül pedig olyan információkat oszt meg a szervezet teljes állományával, ami csak egyes részeire tartozik. Mindezek figyelembevételével javasolt a telephelyenként kiadott EIBSZ használata.

Összegzés

A címben vállalt feladat a civil és MH által üzemeltetett elektronikus információs rendszerek közötti különbség vizsgálata. Jelen dolgozatomban a katonai elektronikus adatfeldolgozó rendszerek alapvető szabályozó okmányát, EIBSZ.-t vizsgáltam részletesen.

A katonai és civil információbiztonsági menedzsment közötti különbségről írta Kerti András és Farkasné Hronyecz Erika:

„A különbséget a menedzsment megközelítésében látom. Addig, amíg a „civil" cég saját maga határozhatja meg az információvédelem megvalósításának módszerét például a COBBIT, ISO 27001 vagy teljesen saját módszer szerint, a közfeladatot ellátó szervezeteknek jogszabályok és az ezeket alátámasztó államirányítás egyéb jogi eszközei kötelező jelleggel határozzák meg a feladataikat." [6]

A megállapítás helyes, de részleteiben megvizsgálva megállapítottam, hogy a civil szabályozás számos elemében erősen hasonlít a katonai előírásokhoz. Ennek okát abban látom, hogy azonos törvényi szabályozásból indulnak ki.

Összehasonlításul átolvastam a BM Nemzetközi oktatási Központ, a Kecskemét Megyei Jogú Város Önkormányzati Hivatala és a Szent István Egyetem Elektronikus Információbiztonsági Szabályzatát.

Valamennyi okmányról elmondható, hogy csak nyílt információkat tartalmaznak, a civil szabályzatok az interneten is elérhetőek. Éppen ezért részletes hálózat topológia, IP címzések, valós felhasználói nevek nem szerepelnek a dokumentumokban, ezeket a szabályzat mellékleteként vagy külön okmányként dolgozták ki, és nem tették nyilvánosan elérhetővé. Ez így helyes, mert megnehezíti a nyílt forrású információk gyűjtésével és feldolgozásával próbálkozó rosszindulatú felhasználók dolgát. [7]

Továbbiakban a katonai és civil szabályzatok hasonló felépítésűek és tartalmúak annak köszönhetően, hogy közös alapokból, az Informatikai Tárcaközi Bizottság Ajánlásaiból (IBT) és az MSZ ISO/IEC 27001:2006 szabványból indultak ki.

A katonai szabályozás kénytelen foglalkozni minősített hálózatokkal is. Jó megoldásnak tartom, hogy a minősített elektronikus információkezelő rendszereket nem tárgyalja részletesen. Egyrészt a szabályzat mérete jelentősen megnövekedne, megnehezítve ezzel a szabályzat felhasználóktól megkövetelt rendszeres átolvasását. Másrészt a szabályzatba minősített információk kerülhetnének, ami szűkítené azoknak a körét, akik jogosultak elolvasni. A minősített adatkezelő rendszerek leírására, üzemeltetésének és használatának a szabályaira külön, általában minősítéssel védett szabályzat használatát határozták meg.

Számomra további egyetlen észrevehető különbség volt a katonai és civil szabályozás között, nevezetesen, hogy a katonai szabályozás precízebb, minden részletre a végletekig kitérő, nincsenek benne általánosságok, minden feladatot azonosítható személyhez rendel a jogok és felelősségek egyértelmű meghatározásával. A szabályzat formai és tartalmi elemeit a különböző szintű

parancsnokságok megszabták, annak végrehajtását és az időszakos felülvizsgálat megtörténtét ellenőrzik. Ezért a szabályzat összefogott, egységes képet mutat.

A civil szabályzat tartalma erősen függ az elkészítő szakmai felkészültségétől, a ráfordított munkaórák minőségétől és mennyiségétől. Összességében azonban elmondható, hogy a katonai és civil szabályozás között számottevő különbség nincs, bármelyik civil szervezet szabályzata egy szakmai revízió utáni minimális átdolgozással hasonló minőségűvé válhatna, mint a katonai szabályozás.

Az EIBSZ kiváló lehetőség arra, hogy az üzemeltető szakállomány a szakma és a jogszabályok által előírtak szerint megkövetelje az informatikai rendszerek előírásszerű használatát a civil vagy katonai szervezet minden tagjától. Egyértelműen megszabja a menedzsment, üzemeltető és felhasználói csoport tagjainak a jogait és kötelességeit. A szabályzat pontjainak betartása garancia az informatikai hálózatok megbízható és biztonságos működtetésére.

Irodalomjegyzék

[1] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[2] 3/2012. (I. 13.) HM utasítás.

[3] Kassai Károly: Az elektronikus információvédelmi rendszabályok katonai specifikációjának kialakítása, a civil önkéntes támogatás megvalósításának fontosabb kérdései. Hadmérnök,IX évfolyam 1. szám 9.oldal.

[4] MH 34. Bercsényi László Különlegs Műveleti Zászlóalj Elektronikus Információvédelmi Szabályzata.(2013)

[5] MH ÖHP 11/2011 számú intézkedése az MH ÖHP és alárendelt szervezeteinek állandó jellegű távközlő, informatikai hálózatának békeidejű üzemeltetési, felügyeleti és működési rendjének szabályozására.

[6] Kerti András – Farkasné Hronyecz Erika: A közfeladatot ellátó szervezetek információs rendszereinek személyi biztonsága. Hírvillám,2015.1. szám, 37. oldal

[7] Kendernay Zsolt , Pándi Erik ,Tóth András: A készenléti szervek informatikai rendszereinek helyzete, várható fejlesztési irányai, HÍRVILLÁM = SIGNAL BADGE 2010:(1) pp. 178-188., 2010

[8] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi Szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal, HU ISSN 2060-0437);

[9] Négyesi Imre: Az információgyűjtés jövőképe (Hadtudományi Szemle on-line, I. évfolyam (2008) 3. szám, 95-100. oldal, HU ISSN 2060-0437);

.

Bozsó Zoltán: A rendőrségi tevékenység-irányítás fejlesztésének lehetőségei

Absztrakt

Rengeteg olyan helyzet volt a munkám során, hogy szükség lett volna a témában kidolgozott tanulmányra, esettanulmányokra, melyek segítették volna a döntések és a helyzetfelismerés, a tevékenységirányítás hatékonyságának fokozását. Eddigi tapasztalataimat és a témával kapcsolatos kutatásaimat kívánom összefoglalni, további segítséget és ajánlást tenni a jövőre vonatkoztatva.

Kulcsszavak: *kommunikációs platform, WiMAX, WiFi, VLAN, NLOS*

Új típusú kommunikációs platformok

„Csak az tud biztonságot szolgáltatni, aki maga is biztonságban él.”[1]

Az elmúlt évtizedekben kiemelt figyelmet kaptak a különböző rendezvények biztosításának végrehajtása, valamint a biztonság kérdése. A 90-es évek előtti időszakban kevés alkalommal kellett komoly és összetett rendőri vezetést igénylő feladatokat végrehajtani, de a 90-es évek közepétől egészen 2006-ig több fontos eseményt kellett biztosítani, melyek kialakítottak egyfajta vezetési stílust és módszert (pl.: pápa-látogatások, nemzetközi sportesemények, stb.).

A 2006-ban történt események rávilágítottak a rendőri tevékenység-irányítás szervezeti-szervezési, vezetési és technikai hiányosságokra ezért szükségessé vált a vezetés rendjének új alapokra helyezése, valamint a technikai és szervezeti fejlesztésekre az új típusú kihívásoknak való megfelelés érdekében. [1]

[1] Salgó László: A magyar rendőrség jelene, jövője, kilátásai. Kriminológiai Közlemények 2004.

A jelenleg működő szervezeti rend és technikai háttér támogatottság már nem felel meg minden tekintetben a 21. század követelményeinek ezért szükségessé vált egy újfajta, átgondoltabb, új alapokon nyugvó rendszer kialakítása. Ehhez a korábbi alapok és a bázis megfelelő, de újfajta rendszerek, eljárások és lehetőségek bevezetésével a kor színvonalának megfelelő helyzetbe hozhatóak azok az egységek és vezetőik, akik felelnek a rendezvények biztonságáért és biztosításáért, a tevékenység-irányítás korszerűsödhet.

A tevékenység-irányítás új, a korábbi években ritkán használt elemei kerültek előtérbe 2006 októberétől, amikor Budapest közterületein a jelentős tömegrendezvényeken, tüntetéseken tömegoszlatás történt. Az akciócsoportok parancsnokai kezdetben kis tapasztalattal rendelkeztek, a tömegoszlatási feladatok gyakorlatlanok voltak, több esetben pedig kommunikációs problémák léptek fel az akciócsoport parancsnokok és a tevékenységüket irányító bevetés-irányítási központ között. [2]

A WiMAX technológia alkalmazhatóságának alapjai

Az új típusú tevékenység-irányítás rendszeréhez olyan környezeti eszközökkel biztosított kommunikációs rendszerre van szükség, mely biztosítja a kiemelten kezelendő problémákat és a kommunikáció egyéb követelményeit is. Erre dolgoztam ki megoldási javaslataimat is, melyeket e fejezetben kívánok bemutatni.

A WiMAX[2] gyökerei az informatika, azon belül is a hálózatok robbanásszerű fejlődéséhez nyúlnak vissza. A személyi számítógépek széleskörű megjelenése az otthonokban is, valamint az Internet, mint mindennapi információs, szórakoztató, és nem utolsó sorban munkaeszköz egyre elterjedtebb használata rendre nagyobb és nagyobb adatforgalmat von maga után. A ezredforduló után a fordulópontot a szélessávú Internet-hozzáférés (DSL, kábel, stb.) jelentette, mely felváltotta az addigra elavult MODEM-es technológiát.

A mobiltelefonok tömeges elterjedésével egy időben ugrásszerűen megnőtt a hordozható, kis méretű eszközök (laptopok, PDA[3]-k, stb.) iránti kereslet – a kulcsszó a mobilitás lett. A megoldást egy vezeték nélküli, de a már meglévő hálózatokkal teljes mértékig kompatibilis hozzáférés jelentette. A TCP [4] /IP [5] protokoll felhasználásával, az Ethernet „továbbfejlesztésével" megszületett az IEEE[6] 802.11-es szabvány – közismertebb nevén WiFi[7] –, vagyis az első WLAN[8].

A WiFi alkalmas a vezetékes helyi hálózatok (LAN) kiváltására, de nem alkalmas nagy távolságú kapcsolatra, sem pedig egy gyalogos sebességénél gyorsabban mozgó eszközök kiszolgálására. Továbbra is kielégítetlen maradt tehát az igény a szélessávú, közepes távolságú vezeték nélküli hozzáférésre. A telekommunikáció és az informatika konvergenciája révén, a sávszélesség és a mobilitás iránti megnövekedett igényének következtében szükségessé vált egy új, szélessávú, közepes távolságú mobil adatátvitel rendszer. „A vezeték nélküli hozzáférési

[2] Worldwide Interoperability for Microwave Access – Világméretű Együttműködés a Mikrohullámú Hozzáférésért
[3] Personal Digital Assistent – Személyi digitális asszisztens
[4] Transfer Control Protocol – Átvitel-vezérlő protokoll
[5] Internet Protocol – internet protokoll
[6] Institute of Electrical and Electronics Engineers
[7] Wireless Fidelity
[8] Wireless Local Area Network – Vezeték nélküli helyi hálózat

hálózatok sokfélesége, arra késztette a világméretű kommunikációs, informatikai nagyvállalatokat, hogy összefogva közös, könnyen elterjeszthető, és elfogadtatható szabványt dolgozzanak ki. A mikrohullámú, vezeték nélküli szélessávú adatátvitel világméretű egységesítése, elterjesztése érdekében létrehozták a WiMAX Fórumot, melynek napjainkra már több mint 350 tagja van, szolgáltatók és gyártók egyaránt. Munkacsoportjai különböző ajánlásokat (WiMAX profilok) dolgoztak ki, olyan átfogó szabvány megalkotása érdekében, mely elősegíti a szélessávú vezeték nélküli hálózatok és technológiák gyors elterjedését.

„A vezeték nélküli mikrohullámú adatátviteli hálózatokkal két szabványosítási szervezet is foglalkozik, a IEEE[9], és a ETSI[10] különböző szabványokban. Az IEEE 802.16 és az ETSI HiperMAN[11] szabványok közös metszete, a 256FFT[12] OFDM[13] (opcionális UL[14], FFT2048 OFDMA[15]) technológia a különböző WiMAX profilok alapja. Az IEEE 802.16 szabályozza az állandóhelyi vezeték nélküli szélessávú kapcsolatok levegő interfész kialakítását. Széles frekvenciasávot támogat (10-66 GHz-ig), változatos csatorna sávszélességek alkalmazásával (1,25 MHz-től 20 MHz-ig), pont-pont összeköttetések megvalósítása esetén. A technológia 2003. évi 802.16a jelű módosítása már tartalmazza az NLOS[16], illetve PMP[17] kapcsolatok kialakításának lehetőségét, mint állandóhelyi szélessávú felhasználói hozzáférést, melyet a 2004. évi, 16d jelű (802.16-2004) átdolgozás egészít ki, és meghatározza a

[9] Institute of Electrical and Electronics Engineer – Villamosmérnökök Intézete
[10] European Telecommunications Standards Institute – Európai Távközlési Szabványintézet
[11] High Performance Radio Metropolitan Area Network – nagyteljesítményű rádiós városi hálózat
[12] Fast Fourier Transform – gyors Fourier átvitel (tulajdonképpen az OFDM vivők száma)
[13] Orthogonal Frequency Division Multiplexing – ortogonális frekvenciaosztásos multiplexálás
[14] Uplink – adatátviteli irány, felhasználói eszköztől a központi állomás felé
[15] Orthogonal Frequency Division Multiplexing Access – ortogonális frekvenciaosztásos multiplexálási hozzáférés
[16] Non Line of Sight – közvetlen rálátás nélküli
[17] Point to Multipoint – Egy bázisállomás-több felhasználói állomás topológia

WiMAX rendszer profilokat, a 2-11 GHz-es sávban. A 2005. novemberben elfogadott 802.16e kiegészítés a mobil (gyalogos-, illetve gépjármű sebességű) megvalósítást szabályozza a 6 GHz alatti frekvenciatartományban, lehetővé téve a hordozható felhasználói eszközök vándorlását a szolgáltatási területen belül, illetve között."

A világméretű együttműködés érdekében külön-külön meghatározták az alkalmazni kívánt frekvencia tartományokat, valamint megjelöltek lehetséges frekvenciákat is, a későbbi bővítésre. Európában, így Magyarországon is a 3.5 GHz-es illetve az 5.8GHz-es (de lehetséges a 2.3 és a 2.5GHz) sávok alkalmazhatók, a nemzeti frekvenciagazdálkodási jellegzetességek figyelembevételével. Hazánkban a Nemzeti Hírközlési Hatóság és a Kormányzati Frekvenciagazdálkodási Hatóság szabályozza e sávok használatát. A jelenlegi szabályok alapján a 2.3, a 2,5 és a 3,8 GHz sáv egyedi engedélyezés köteles, míg mentességet csak az 5.8 GHz-es tartomány élvez. (A katonai célokra fenntartott – *ún. NATO IV sáv, mely névlegesen az 5 GHz-es tartomány, ami a valóságban 4.5–5.0 GHz-et jelent* – elvi síkon lehetőséget ad külön frekvenciahasználati engedély nélkül eszközök és rendszerek telepítésére és alkalmazására.

Az átviteli csatorna sávszélessége 1,25 MHz-től 20 MHz-ig különböző diszkrét értéket vehet fel. A 802.16-2004 WiMAX profil által ajánlott sávszélességeket és a duplexitás biztosításának módjai az alkalmazott frekvenciasáv függvényében eltérőek lehetnek.

Frekvencia sáv	Duplexitás	Csatorna sávszélesség
2.5GHz	TDD[18]	5 MHz
	FDD[19]	5 MHz
3.5GHz	TDD	3.5 MHz
		7 MHz
	FDD	3.5 MHz
		7 MHz
5.8GHz	TDD	10 MHz

A mobil WiMAX profil a fentiektől eltérően 5MHz, 7MHz, 8.75MHz, 10MHz szélességű csatornákat javasol a 2.5GHz-es, és a 3.5GHz-es frekvenciasávokhoz, bár a SOFDMA[20] alkalmazásával ez dinamikusan változtatható 1.25MHz-től egészen 20MHz-ig.[21][3]

Ha a csatornát egyetlen vivővel szeretnénk átvinni, az nem lenne elég hatékony, mivel a sáv alsó és felső tartományában más-más csillapítási jellemzők, interferencia jelenségek, stb. jelenhetnek meg. Ezt még adaptív szintszabályozással sem lehet kiküszöbölni, ezért megoldást az OFDM technológia – *melyet eredetileg a 802.11a szabványhoz fejlesztettek ki* – kínál, mely egy úttal kiküszöböli a több utas terjedésből adódó terjedési-idő szórást és a szimbólumok közti interferencia problémákat is, így nagyobb lesz a sáv átviteli kapacitása. Az OFDM lényege, hogy a csatornát több, kisebb sávszélességű jelfolyamra osztja, melyek mindegyike külön vivőfrekvenciával rendelkezik, majd ezeket az alvivőket ortogonálisan modulálja és összegzi. Ezzel a módszerrel elérhető, hogy a csatornát egyenletesen használjuk ki, így jobb jel/zaj viszonyt érünk el. Ha spektrális zavar áll fenn, akkor lehetőség van az

[18] Time Division Duplex – időosztásos duplex
[19] Frequency Division Duplex – frekvenciaosztásos duplex
[20] Scalable Orthogonal Frequency Division Multiple Access – skálázható ortogonális frekvenciaosztásos többszörös hozzáférés
[21] (Forrás: Vass Zoltán szds. – A WiMAX hálózat jellemzői, gyakorlati alkalmazhatósága a Magyar Honvédség hírrendszerében – ZMNE, 2006)

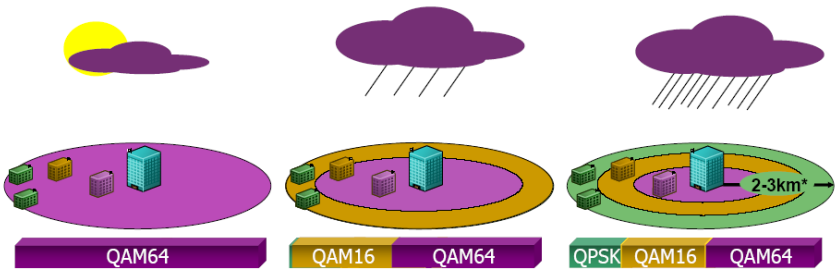
egyes alvivők modulációjának egyszerűsítésére, vagy az adatátvitel leállítására, míg a többi alvivőn ugyanúgy folyhat a kommunikáció. Az SOFDMA ennek a továbbfejlesztése, melyben az alkalmazási viszonyoknak megfelelően, rugalmasan változtatható a csatorna sávszélessége. Az alvivők száma megválasztható (128, 256, 512, 1024, vagy 2048), miközben a szimbólum időtartam és az alvivők közti frekvenciakülönbség fix. Mivel azonban az OFDMA és az SOFDMA különböző modulációs technikán alapszik, az SOFDMA nem kompatibilis az OFDM-mel.

A fejlett fizikai réteg technológiák egy olyan gyűjtőfogalmat alkotnak, melybe azokat a megoldásokat soroljuk, melyek a szűkre szabott spektrum nagyobb kihasználásához segítenek hozzá. Ide tartoznak a különböző modulációs eljárások, hibajavító kódok, fejlett antenna-megoldások, stb. A WiMAX esetén számos ilyen technológiát alkalmaznak, melyek műszaki leírása több ezer oldalra rúg, ezért csak a legjelentősebbeket emeltem ki.

Első az adaptív moduláció, mely rugalmasan ötvözi a QPSK[22], QAM16[23] és QAM64 technológiákat, a vételi viszonyoknak megfelelően. Amennyiben a bázisállomás és a felhasználói terminál között LOS [24] kapcsolat van, elméletileg zavartalan a kommunikáció, és a leghatékonyabb (és egyben „legsűrűbb") modulációt alkalmazhatjuk. Gyakorlatilag viszont számolni kell a légköri csillapítással, amit az időjárási jelenségek jelentősen befolyásolnak – számít a páratartalom, a csapadék, a köd, stb. A mindenhol az elérhető leghatékonyabb átviteli kapacitás elérése érdekében dolgozták ki az adaptív modulációt, melynek lényege, hogy a távolság növekedésével és a vétel romlásával arányosan, vagyis a jel-zaj viszony (SNR[25])

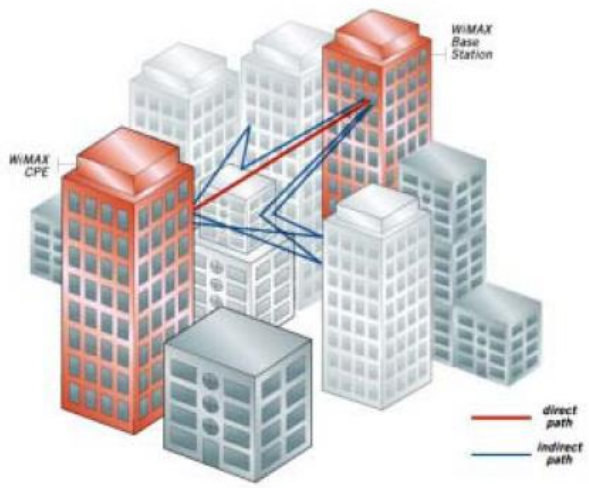
[22] Quadrature Phase Shift Keying – Kvadratúra fázisbillentyűzés
[23] Quadrature Amplitude Modulation – Kvadratúra amplitúdó moduláció
[24] Line of Sight – közvetlen optikai rálátás
[25] Sound-to-Noise-Rate – Jel-zaj viszony

függvényében egyre egyszerűbb (kisebb kapacitású), ám jobban fogható modulációt alkalmaz.



1. ábra: Adaptív moduláció (Forrás: Reza Goslhan – Fixed and Mobile WiMAX OVerview – http://www.fujitsu.com/downloads/MICRO/fma/pdf/esc_wimax06.pdf)

A második technológiai megoldásnak NLOS környezetben van jelentősége. Ez lehet városi környezet, vagy akár hegyes-erdős, erősen átszegdelt terep is. Ilyen körülmények között a kisugárzott visszavert jelek különböző utakat futnak be, más-más idő alatt. A technológia lényege, hogy a több utas terjedésből fakadó zavarokat, interferenciákat kiküszöbölje.[4]



2. ábra: Több utas terjedés (Forrás: WiMAX's technology for LOS and NLOS environments – www.wimaxforum.org)

A megoldásra a MIMO[26] antennarendszer használata látszik jó megoldásnak. Ez azt jelenti, hogy több antennát használunk egyszerre, és az adó és vételi oldalon az egyes antenna-párok között mintha külön-külön csatorna lenne. Ezek a csatornák azonban nem különbözőek a rajtuk átvitt információ szempontjából, az csak más-más úton, eltérő terjedési idővel halad át rajtuk. A zavarok és interferencia kiszűrésére speciális eljárást alkalmaznak, melyet *space-time* kódolásnak nevezünk. „A space-time kódolást 1998-ban Tarokh, Seshadri és Calderbank [TSC] fejlesztettek ki MIMO rendszerekre. Lényege, hogy térbeli és időbeli kapcsolatot teremtsen a különböző antennákból különböző időpontokban sugárzott jelek között. Ezt a kapcsolatot arra használjuk, hogy minimalizáljuk a dekódolási hibákat a vevőnél. A space-time kódolás adó diversity-t és teljesítménynyereséget jelent a sávszélesség feláldozása nélkül."

[26] *Multiple Input Multiple Output* – Több bement, több kimenet

Következtetések

A Rendőrség korszerű, perspektivikus infokommunikációs [5] rendszerének kialakítása, a meglévő technikai lehetőségeink jobb kihasználása és a pénzügyi források hatékonyabb felhasználása érdekében javaslom a következő szempontok figyelembevételét:

- Az infokommunikáció minden területén törekedni kell a legkorszerűbb adatvédelmi eljárások rendszertechnikai megvalósítására;
- A tevékenység-irányítási rendszer struktúráját javaslom WiMAX alapra helyezni, ahol a szoftveresen programozható, gyors (VoIP képes) bázisállomások beszerzése javasolt a mikrohullámú gerincek és a területlefedő megoldásokra is;
- A megjelenő rádióképességek integrálása a WiMAX rendszerrel növeli a rendszer megbízhatóságát;
- Feladat végrehajtásakor egységeink megóvása érdekében a távoltelepült WiMAX csomópontok a kapcsolat tartására alkalmasak. Ebben az esetben a WiMAX terület lefedő üzemmódban dolgozik;
- Rendszereink a digitalizáció növekedésével egyre inkább támadhatóvá válnak távoli hozzáféréssel is – ezért mindent meg kell tenni a kockázati tényezők csökkentése érdekében.

A fenti szempontok szerinti ajánlások, javaslatok figyelembe vétele – megítélésem szerint – nagymértékben elősegítheti a Rendőrség modernizációját, fejlesztési ütemének felgyorsítását.

Felhasznált Irodalom

[1]. Salgó László: A magyar rendőrség jelene, jövője, kilátásai. Kriminológiai Közlemények 2004.

[2]. Vizsgálati Jelentés 2006 Szeptember-Október Fővárosi Eseményeiről

http://www.parlament.hu/biz39/emb/albiz/jelentes.pdf 2010 Budapest

[3]. Vass Zoltán szds. – A WiMAX hálózat jellemzői, gyakorlati alkalmazhatósága a Magyar Honvédség hírrendszerében – ZMNE, 2006

[4]. Tóth András: A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében, PhD disszertáció, Nemzeti Közszolgálati Egyetem, Budapest, 2015

[5]. Németh Gyula: A Rendőrség Logisztikai támogatásának átalakítása, PhD. értekezés – ZMNE, Budapest 2011

[6]. Négyesi Imre: COTS rendszerek alkalmazási lehetőségeinek vizsgálata (Hadtudományi szemle on-line, IV. évfolyam (2011) 4. szám, 111-116. oldal, HU ISSN 2060-0437)

[7]. Négyesi Imre: DIE ÜBERPRÜFUNG DER VORAUSSETZUNGEN VON COTS SYSTEMEN (COTS RENDSZEREK KÖVETELMÉNYEINEK VIZSGÁLATA) (Hadmérnök on-line, VII. évfolyam (2012) 2. szám, 371-376. oldal, ISSN 1788-1919).

Lányi Márton: A szállítmányozó értéke

Absztrakt

Az új évezred új kihívások elé állítja a szállítmányozó szakmát. A keresett információ egyre jobb internetes elérhetősége, a térinformatikai megoldások, az okos telefonok, a közösségi hálók rendszere, valamint az ezekre épülő alkalmazások, számítástechnikai megoldások alapjaiban kérdőjelezik meg a szállítmányozó szerepét a logisztikai rendszerekben. Időszerű a kérdés, vajon milyen értéket képviselt a múltban, a jelenben és vajon milyen értéket fog képviselni a szállítmányozó a jövőben? Miért és milyen esetekben válasszunk szállítmányozót egy eszközzel rendelkező fuvarozóval szemben? A cikk választ ad a felvetésekre új megvilágításba helyezve a szállítmányozót.

Kulcsszavak: *szállítmányozó, innováció, hozzáadott érték, értékteremtés*

Bevezető

A cikk célja, hogy bemutassa, hogyan változott és változik korunkban is a szállítmányozás, miért alkalmaztak szállítmányozót a múltban és a jelenben egyes kereskedelmi ügyletek lebonyolításához. A téma minden eddiginél időszerűbb, hiszen az új, innovatív technológiák megjelenésével a szállítmányozás léte kérdőjeleződhez meg. A szállítmányozásban érdekelt vállalatok felsőbb vezetői a munkájuk részeként több évtizedre előre tekintve foglalkoznak stratégiai tervezéssel. A kirajzolódó jövőkép aggasztóan fest a hagyományos szállítmányozásra nézve. Egyre több startup vállalat foglalkozik a szállítmányozás közösségivé formálásával, digitalizálásával. A közösségi logisztika vagy szállítmányozás már jelen van, bár még nem terjedt el széles körűen. Hogy néhány

példát említsek, megjelent az amerikai piacon a Shipster, a Shipstr (Fleet) és a Postmates nevű szolgáltatás. Ez utóbbi az Uber teherszállításra szakosodott kistestvére. Bárki lehet fuvarozó, akinek van hely az autója csomagtartójában és bárki megrendelhet tőlük egy belföldi szállítást egy mobiltelefonos alkalmazáson keresztül. A postmates ez esetben teljesen kikapcsolja szállítmányozót, de a hagyományos fuvarozókat is. Az üzleti modell lényege az útirányonként meglévő helyek kihasználásában van. Ez tehát a közösségi logisztika előszobája. A hasonló nevű Shipstr (Fleet) és Shipster két olyan startup [1], amely kifejezetten a szállítmányozás kikapcsolására törekszik, gyakorlatilag egy logisztikai IKEA [2] szolgáltatás, ahol a vásárló nem igényli, hogy a szolgáltatást egységbe szervezve kapja meg, hanem az egyes elemek összeillesztését maga vállalja.

A szállítmányozás értékválság előtt áll. A jelen vezetőinek feladata a vállalatukat ezen az értékválságon átvezetni. Az egyik lehetséges mód a szállítmányozó értékének definiálása és egy ezen alapuló stratégia kidolgozása.

A cikk nem összpontosít a szállítmányozás technikai részleteinek a pontos kifejtésére, viszont képet ad a szállítmányozó vállalatok múltbeli, jelenlegi és várható jövőbeli hozzáadott értékéről.

Történelmi áttekintés, a szállítmányozás kialakulásának alapvető kérdései

A múlt feldolgozásához Dr. Magyary István kéziratát hívtam segítségül, aki megfelelő rálátással elemzi a közlekedés, a fuvarozás és a szállítmányozás kialakulását, működésének alapvető mozgatórugóit. A kézirat megállapításait

[1] startup: angol kifejezés, újonnan alapított, nagy növekedési potenciállal rendelkező, induló vállalkozásokat jelenti, melyet többnyire termék- vagy üzleti modell innováció jellemez.
[2] IKEA: svéd lakberendezési áruház, általános jellemzője, hogy a vevő maga végzi a termékek végösszeszerelését

kiegészítem a saját tapasztalatommal, amelyet az szakmában töltött 20 év alatt szereztem.

A szállítmányozás kialakulása a történelem folyamán a 17. századra vezethető vissza. A kereskedők számára egyre fontosabb lett, hogy áruinak továbbításához mindig elegendő fuvareszköz álljon rendelkezésére. A fuvarozónak pedig az volt az érdeke, hogy folyamatosan kapjon fuvarozási megbízásokat. E feladat megoldására jöttek létre a fuvarozási ügynökségek, melyek egy-egy körzetben számon tartották a fuvarozásra váró árukat, és rakománnyal látták el a fuvarért jelentkező fuvarosokat. Közvetítő szerepet töltöttek be a fuvarosok és a fuvaroztatók között. Saját fuvareszközük nem volt, mások járműveivel továbbították mások áruit. A fuvaroztatókkal kötött megállapodásukban arra vállalkoztak, hogy díjazás ellenében gondoskodnak az elszállításra váró áruk továbbításáról. A velük szerződéses viszonyban levő fuvarosokkal szemben arra kötelezték magukat, hogy díj ellenében fuvart szereznek a számukra. A 17. század végére Európa minden jelentősebb kereskedelmi és közlekedési gócpontjában működtek már fuvarozási ügynökségek, melyek egymás között is fuvarozták a küldeményeket. A fuvarozási megbízások közvetítésén kívül az áruk helyváltoztatásával járó valamennyi feladatot is elvégezték. Egyeztették az árukat a fuvarlevél adataival, megszervezték a be- és kirakodást, az átrakodást. Házhoz fuvarozták a küldeményeket, kiszámították az árut terhelő illetékeket, beszedték, ill. kifizették a fuvardíjat. A szárazföldi fuvarozás ügynökségeivel egy időben megalakultak a hajózási ügynökségek is, melyek gondoskodtak a tengeri kikötőbe érkező áruk továbbításáról és a hajótér megszervezéséről. A tengeren érkezett árukat szerződéses fuvarozókkal szállították tovább. Közvetítő szerepük volt az árutulajdonosok, a hajózási vállalkozók és a szárazföldi fuvarosok között. Elvégezték a rakodási feladatokat, raktáraikban

átmenetileg tárolták az árut, kiállították a tengerhajózási okmányokat, megkötötték a biztosítási szerződéseket. A kereskedők az áru átvételéről kiállított ügynöki elismervények alapján fizették ki egymásnak a vételárakat. [1]

A gőzgép feltalálása korszakalkotó változást jelentett a közlekedéstechnikában is. A 19. században létrejöttek az első vasútvonalak, és rövid idő alatt hálózattá terebélyesedve kapcsolták össze az ipari, mezőgazdasági és kereskedelmi körzeteket. Egyre több szakértelemre volt szükség annak eldöntéséhez, hogy milyen fuvareszközzel, melyik útvonalon továbbítsák az árukat. A helyes választás idő- és pénzmegtakarítást jelentett. Ebben siettek a megbízók segítségére a szállítmányozók. Azokat a vállalkozókat, akik megbízójuk helyett megszervezték az áruk továbbítását, a 19. század végétől speditőröknek, azaz szállítmányozóknak, munkájukat pedig spedíciónak, azaz szállítmányozásnak nevezik. [1]

A szállítmányozási gyakorlat a közelmúltban

Egy szállítmányozó munkavégzése a 90-es években abból állt, hogy a beérkező megbízásokat a saját alvállalkozói kapcsolatrendszerén belül igyekezett megszervezni. Ez azt jelentette, hogy a szállítmányozónak birtokában kellett lennie annak a tudásnak, hogy melyik fuvarozó melyik viszonylatban fuvarozik, mikor és hol lesz elérhető kapacitása. Természetesen a fuvarozóknak egy rangsora is létezett, mely sorba állítja őket szaktudás, minőség, ár és a kapcsolat minősége szempontjából. A szállítmányozó a fentiek alapján kezdte el keresni a feladathoz legjobban illő fuvarozót. A megbízó felé ugyanakkor szakmai, szakértői segítséget is nyújtott, legyen az útvonal vagy egyéb, már említett szervezésbeli kérdés.

A fentieknek az alternatívája a fuvaroztató szempontjából csak az lehetett, ha kinyitja a szaknévsort vagy a telefonkönyvet a fuvarozóknál és sorban elkezdi

felvenni velük a kapcsolatot. Nem kizárt, hogy így is lehet sikeres üzletet kötni, de könnyen belátható a szállítmányozó értéke ebben a folyamatban, amely megjelenik idő, energia ráfordításban és egyéb biztonsági kockázatok csökkentésében. A szállítmányozó alapvető hozzáadott értéke a kapcsolati hálója volt és a szállítmányozás technikai know-how[3]-ja.

A szállítmányozó és a fuvarozó érdekének összehasonlítása

Ezen a ponton azért érdemes tisztázni a fuvarozás és a szállítmányozás alapfogalmait, mert a szállítmányozói szolgáltatások igénybevételének a helyettesítő terméke a fuvarozóval kötött közvetlen megállapodás lehet.

A fuvarozás az a művelet, amelyet az áru helyváltoztatása érdekében kell elvégezni. A helyváltoztatás kezdőpontja rendszerint a termelési vagy tárolási hely (gyár, üzem, bánya, termőhely, raktár), célpontja a felhasználás, illetve a rendeltetés helye. Az e célra szerveződött és szakosodott vállalkozók, a fuvarozók: vasutak, közúti fuvarozócégek, hajótársaságok, légitársaságok végzik.

A fuvarozásnál bővebb szolgáltatást foglal magában a szállítmányozás. A szállítmányozó köteles a küldemény továbbításához szükséges fuvarozási és egyéb szerződéseket megkötni, valamint az árutovábbításával kapcsolatos egyéb teendőket elvégezni pl. a csomagolást, az árudarabok megjelölését, a hatósági vizsgálatok lebonyolítását, a raktározást. [1]

A szállítmányozó egyébként szükségszerűen fuvaroztató, mert megbízásából származóan elvállalta azt a kötelezettséget, hogy megköti a fuvarozóval a

[3] know-how: szellemi alkotás vagy vagyoni értékű gazdasági, műszaki, szervezési ismeret, tapasztalat

fuvarozási szerződést. A fuvarozó szempontjából közömbös, hogy ki a fuvaroztató, számára csak a megbízás elnyerése fontos. A szállítmányozó és a fuvarozó érdekközösséget alkot, amely a rájuk bízott küldemény maradéktalan, sérülésmentes, időbeli célba juttatása, a megbízás teljesítése. Alapjaiban azonban a fuvarozó érdekrendszere különbözik a szállítmányozóétól.

A fuvarozó elsődleges érdeke:

- a fuvareszköz kihasználtságának a növelése,
- a megtett, rakott távolság maximalizálása,
- az állásidők csökkentése, a hasznos idő növelése,
- a fuvarozási sebesség maximalizálása a legnagyobb költséghatékonyság elérése,
- karbantartási és finanszírozási költségek leszorítása,
- a lehető legmagasabb fuvardíj elérése.

A szállítmányozó elsődleges érdeke:

- a megbízói igények maximális kielégítése,
- a küldemény éppen időben célba juttatása,
- a nyereség maximalizálása, amely több módon elérhető:
    - lehető legalacsonyabb alvállalkozói díjak elérésével,
    - bevételeinek növelésével,
    - hatékonyság növeléssel,
    - gyűjtőszállítmányozással.

A szállítmányozó alapvető érdeke egybe esik a megbízó érdekével. A fuvarozónak csak a saját eszközének a kihasználtsága az elemi érdeke. A fuvaroztató és a szállítmány csak a rendszernek bizonyos elemei. A szállítmányozó esetében a gondolkodása középpontjában a megbízó áll, tetteit, napi munkáját ez vezérli.

A szállítmányozó hozzáadott értéke a múltban

A szállítmányozó eltérően a fuvarozótól tehát, a szállítási tevékenységek megszervezése során, az ügyfél megbízottjaként, annak érdekeit képviselve lép fel a szakmai ismereteit felhasználva. Tekinthetünk a szállítmányozóra úgy, mint a vállalat kiszervezett tudásközpontjára. Fuvarozó alkalmazása esetén, a vállalaton belüli szaktudás elengedhetetlen. Analógiaként azt említhetném, amikor az egyénnek hitel felvételére van szüksége. A helyzet egyszerű abból a szempontból, hogy a hitelt egy bank fogja nyújtani, a hirdetményben szereplő kondícióval. De vajon mindenki érti-e, hogy a kondíciók, hivatkozások pontosan mit is jelentenek? Azon túlmenően, vajon az összes bank, összes ajánlatát összevetették-e? Az összevetés egyszerű-e annyira, hogy csak néhány számot (kamat, fuvardíj) egybevetünk? A válasz egyértelműen nem, hacsak az egyén nem képzett szakember, akinek belefér az idejébe, hogy az összes ajánlatot megvizsgálja és lehetőleg a saját keresleti mennyiségénél fogva engedményeket is érjen el. A szállítmányozás világa hasonlóképpen működik, mint a bankvilág. Ha valamihez nincs szakértelmünk, nincs időnk vagy képességünk rá, akkor szakemberhez fordulunk. A szállítmányozás múltbeli elsődleges hozzáadott értéke tehát az, hogy a szaktudást nem kellett megszerezniük és állandóan rendelkezésre tartaniuk az egyes vállalatoknak, hanem azok tranzakciós alapon is elérhetőek voltak.

Összefoglalóan, a szállítmányozóval szemben alapvetően kétféle elvárása volt a megbízónak, amennyiben ezeket teljesíti, hozzáadott értéket képvisel:

- értsen ahhoz, hogyan lehet az árukat eljuttatni egyik földrajzi pontról a másikra,
- tudja kikkel kell szerződést kötni, milyen okmányok és hatósági kezelések szükségesek,
- mindezt csinálja olcsóbban, mint a megbízó.

A szállítmányozó múltbeli értékteremtését tekinthetjük a hagyományos szállítmányozás értékének is, a mai szállítmányozás alapjának. Ezen értékek a felsorolás szerűen a következőkből álltak:

- Hajózási és a fuvarozási ügynökségek nélkül lehetetlen lett volna a gazdasági szükségletek kielégítése.
- Szakértőként a megbízó érdekeit úgy tudta képviselni, hogy az hasznot hozzon.
- Csökkentek a szállítási költségek.
- Összegyűjtötték a kisebb tételekből álló küldeményeket.
- Rakománnyal látták el az üresen közlekedő járműveket.
- Raktárak fenntartásával tették egyenletesebbé a fuvarozást.
- A rakodás gyorsításával segítették a fordulóidő csökkentését.
- A fuvarozó és a szállítmányozó között így a legszorosabb együttműködés alakult ki, ezért javult az árutovábbítás minősége.
- Az áruhoz az adott körülményekhez a legmegfelelőbb csomagolást és fuvareszközt tudta hozzárendelni.

- Gondoskodni tudott a legbiztonságosabb, a fuvardíj alakulás szempontjából legkedvezőbb elrendezésről a fuvareszközben.
- Ezzel csökkenthető az áru egységére jutó fuvardíj, a rakodási költség, valamint a hibás csomagolásból adódó átcsomagolási költség.
- Nagy volumenű megrendeléssel és fuvarpiaci tapasztalattal kedvező fuvardíjakat és fizetési feltételeket értek el.
- Biztosította a lehető leggazdaságosabb és legbiztonságosabb útvonal kiválasztását. [1]

A szállítmányozó tehát elsősorban szellemi tőkéjét értékesítette, amikor megbízói részére az árufuvarozás megszervezését bizományosként vállalta, s elvégezte mindazokat a teendőket, amelyek a megbízó feladatai lennének. [2]

Érték a jelenben

A szállítmányozás virágzó üzletággá vált. A speditőrök száma gyorsan növekedett. A fuvarpiacon előnyösebb helyzetben voltak a nagy szállítmányozási cégek. Az általuk diktált versenyfeltételeket a kisvállalkozók nem tudták teljesíteni, fokozatosan tönkrementek vagy beolvadtak a nagyvállalatokba. Európában szállítmányozási világcégek alakultak ki. A kombinált fuvarozás jelentős fejlesztése is megkövetelte, hogy a szállítmányozók kapcsolódjanak be a szállítási folyamatok lebonyolításába.

A globális logisztikai piacot jelenleg nem több mint egy tucat multinacionális vállalat dominálja, őket több kisebb cég követi, amelyek száma összesen ötven alatti. A teljes globális kereskedelem ezen vállalatok közreműködésével zajlik. A piac vezető szereplők a DHL, Kühne+Nagel, Schenker, UPS, Geodis, Expeditors, Agility, Ceva, Hellman stb. [3]

Az elmúlt két évtizedben lezajlott a piac koncentrációja, összeolvadások és felvásárlások történtek annak érdekében, hogy az egyes vállalatok globális hálózatra, és ezzel együtt multinacionális státuszra tegyenek szert.

A legtöbb piaci szereplő hagyományos szállítmányozóként működött, fő tevékenysége a szállítmányok könyvelése volt, ezt a feladó- és a célállomásokon nyújtott szolgáltatásokkal egészítette ki. Amint a globális üzleti gyakorlat megváltozott és az ellátási lánc menedzsment került előtérbe, a vállalatok felfedezték az üzleti potenciált abban, hogy egyszerre többféle szolgáltatást nyújtsanak ügyfeleiknek egyablakos rendszerben. A cél érdekében saját beruházásként, felvásárlásokkal létrehozták a szükséges raktár és szerződéses logisztikai kapacitásokat. [3]

A legtöbb ellátási láncban a 3PL[4] szolgáltatók további kiszervezéssel maguk is alvállalkoztatnak, több helyi szolgáltató bevonásával. . Felmerül a kérdés, hogy miért is ne lehetne a 3PL szolgáltatót kihagyni az alvállalkoztatási láncolatból. Globális megoldásoknál ez azonban több okból sem lehetséges jelenleg. [3]

A 3PL szolgáltató egységes eljárási rendet és folyamatokat tud biztosítani minden helyszínen és országban. Amennyiben a termelő, kereskedő vállalat azonos 3PL szolgáltatóval dolgozik Európában, Ázsiában és Amerikában, minden iroda ugyanazon okmányokkal, eljárásokkal és folyamatokkal fog találkozni. Továbbá, a 3PL szolgáltató ismeri a helyi szokásokat és jogi környezetet, ezért a folyamatait könnyebben igazítja ezekhez. A megbízó nem feltétlenül van abban a helyzetben, hogy a helyi törvényeknek, vámszabályoknak vagy engedélyezési környezetnek teljesen megfeleljen, ezért jobb egy 3PL szolgáltatót használni. A 3PL szolgáltatók

[4] 3PL: third-party logistics provider

méretüknél fogva kiépítették az egyes tevékenységekhez kötődő alap kompetenciákat és kapacitásokat. Ezen tevékenységek általában a fuvarozás, vámkezelés és a szerződéses logisztika. A szolgáltatásukat egy fejlett technológiájú IT háttér támogatja, amely képes bármikor azonnali átláthatóságot adni a tevékenység részleteiről. A 3PL szolgáltatók manapság már nem csak specializált leltár menedzsment és raktár operációt tudnak nyújtani. Közvetlen vevői megrendelések kezelése, egyszerűbb összeszerelések vagy, egy kisebb piac igényeire alapozva, az ún. integrált logisztikai szolgáltatás további hozzáadott értékű szolgáltatásként jelenik meg. [3]

A 3PL szolgáltatók napjainkban egyre többet fektetnek épületekbe és disztribúciós szolgáltatások kialakításába, hogy az ügyfeleik igényeit ki tudják elégíteni. Ezen felül egyre jobban specializálódnak az egyes iparágak kiszolgálására, ilyen ágazatok például az autóipar, a repülőgép ipar, a gyógyászati vagy a környezettudatossághoz kapcsolódó logisztika. Ezen területekre külön, nagy tapasztalattal rendelkező szakértőket alkalmaznak.

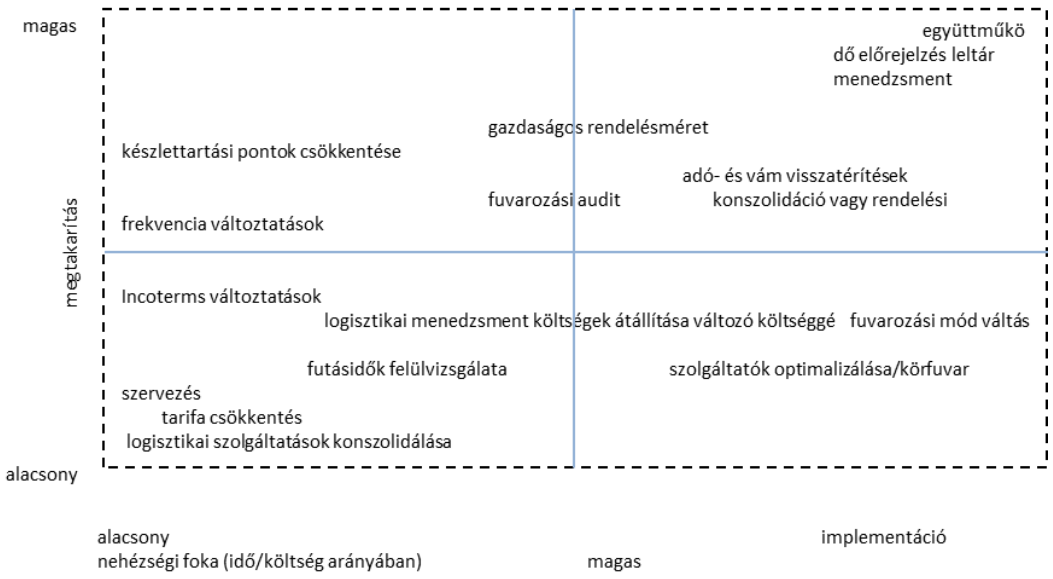
A vállaltok mai ellátási lánc menedzsment stratégiájának részeként a logisztikai költségeket tisztán változó, tranzakciós költségekre próbálják konvertálni. Ez esetben nem lenne lehetséges, hogy maguk beruházzanak és irányítsák a logisztikai tevékenységüket. A legjobb, ha ezt egy logisztikai szolgáltatóra hagyják és annak szinergiáit kihasználva érjék el szakmai vagy költség céljaikat. [3]

A jelenkor szállítmányozója előlépett globális logisztikai szolgáltatóvá. A szolgáltatások alapját még mindig a hagyományos, múltbeli értékek adják, de megjelenik egy azokra épülő iparág. A 3PL szolgáltató túllép az A-ból B-be áruszállítás kérdéskörén és egy ellátási láncra vetített optimalizációt hajt végre. A

saját kapacitásait is e szerint fejleszti és már nem csak hagyományos szállítmányozás, hanem egyre gyakrabban a szerződéses logisztika is része. A 3PL szolgáltató mellett megjelent a 4PL[5] szolgáltató is. A 4PL szolgáltatás a megbízó komplett logisztikai tevékenységét tervezi, szervezi, kivitelezi. Az üzleti modell lényege, hogy a megbízó oldalán egyáltalán nem marad logisztikai szakember, vagy legfeljebb csak a szervezet vezetője. Ebben az esetben, a 4PL szolgáltató további 3PL szolgáltatókat bíz meg, amelyek lehetnek akár a közvetlen versenytársai is, hiszen a cél, hogy úgy válasszon 3PL szolgáltatót, ahogy azt az ügyfél maga is tenné. Nem cél az egy hálózathoz, világcéghez tartozás. Ebben a megoldásban már megjelenik a modularitás és esetenként a világhálózatok versenyeztetése. Adott esetben, akár egy viszonylatban is lehet több versenytárs megoldásait alkalmazni, amennyiben azok eltérő szolgáltatási szintet jelentenek. A termelő vállalatnak gazdasági hasznot jelent a 4PL szolgáltató alkalmazása, mert az csak a fő tevékenységének az elvégzésére koncentrál, míg a megtakarítási és folyamatfejlesztési célokat a 4PL szolgáltató általában szerződésben garantálja.

A következő ábra néhány értékteremtő szolgáltatást helyez el azok bevezetésének idő és költségbeli függvényében úgy, hogy a megtakarítási potenciál mértékét is mutatja. Látható, hogy a hagyományos szállítmányozási megoldások, ebben a koordináta rendszerben a gyorsan implementálható[6], de relatív alacsony megtérülésű negyedben vannak, ahhoz, hogy magasabb megtakarítást érjenek el már egy komolyabb együttműködésre van szükség. Ebben az együttműködésben a szolgáltató a megbízó szervezetének része, együtt terveznek, szerveznek. Az ilyen együttműködés csak fejlett infokommunikációs eszközök összekapcsolásával és harmonizálásával lehetséges.

[5] 4PL: fourth-party logistics provider
[6] rövid idő alatt, alacsony költség mellett bevezethető intézkedések



1. ábra: A logisztikai szolgáltató értékteremtése az idő és költség arányában (Forrás: saját szerkesztés a Kühne+Nagel AG bemutatója alapján)

Összefoglalóan, a jelenkori szállítmányozó komplex rendszerlogisztikai szolgáltatóvá vált. A globalizálódó világban vele szemben támasztott elvárások már megkövetelik a versenytársak szolgáltatásainak ismeretét és bizonyos esetekben, az üzletbe kapcsolását, valamint az ügyfél infokommunikációs rendszereinek támogatását.

Érték a jövőben

Vizsgálatom tárgya, hogy miután sorba vettük a múlt és a jelen szállítmányozói értékeit, nézzük meg, milyen létező vagy várható fejlesztések befolyásolhatják a jövő szállítmányozási iparát. A továbbiakhoz elengedhetetlen összesíteni, hogy az innovációnak milyen megjelenési formái lehetnek és azok közül melyik gyakorolhat

hatást a szállítmányozásra. A téma tárgyalása igen fontos, hiszen az elmélet megfelelő alkalmazása elengedhetetlen ahhoz, hogy annak előnyeit realizálni, veszélyeit pedig felmérni lehessen. Például, kisebb versenytársakat, akik az adott vállalat fő bevételi forrásának számító üzletének a perifériáján dolgoznak, nagyobb valószínűséggel hagynak figyelmen kívül, amíg tevékenységükkel nem jelentenek fenyegetést a vállalat számára. A szállítmányozásban többfajta fejlesztési irányt lehet megfigyelni. Vajon melyik lehet ténylegesen romboló hatású és melyik jelent innovációt, vagy csupán technológiai továbblépést?

Schumpeter az innováción szakmai fejlődést értett. Elmélete szerint a kapitalizmus lényege az innováció lehetőségeinek keresése, melynek során az innováció az egyensúly agresszív lerombolására törekvést jelenti. A környezet nem adott, hanem állandó harcot és mozgást: „kreatív rombolást" fejez ki, ezzel is egy dinamikus, érzékeny szelekciós folyamatot hozva létre. Az innovatív vállalkozó az innováció motorja, aki tevékenysége során módosítja a helyzeteket. Tanulmányában az innovációnak öt alapesetét írja le:

- új javak eladása, vagy régi javak újszerű előállítása;
- új szállítási módszerek bevezetése;
- új piacok feltárása;
- új termelési anyagok (nyersanyagok vagy félkész áruk) használata;
- új piaci helyzet kialakítása (pl. új monopolhelyzet megteremtése, illetve régi megszüntetése). [4]

Clayton M. Christensen és Joseph Bower közgazdászok 1995-ben jelentették meg a *disruptive innovation* elnevezésű elméletüket. Az angol kifejezés szó szerinti fordítása: romboló innováció. Olyan innovációt vagy fejlesztést nevezünk

rombolónak, amely azzal, hogy létrehoz egy új érték hálózatot és piacot, lerombol egy meglévőt, helyettesítve a jelenlegi piaci szereplőket. [5]

Az elmélet az innováció egy meghatározott formájára használja a disruptive innovation kifejezést. Ezekben az esetekben egy kisebb piaci szereplő, amely lehet egy akár éppen piacra lépő startup vállalkozás, jellemzően kevés erőforrással, képes az adott piacon régebb óta jelen lévő szereplőktől piaci részesedést elhódítani. Az elméletben a piaci részesedés megszerzésének a technikája mindig ugyanaz. A piaci szereplők arra összpontosítanak, hogy a szolgáltatásaikat és termékeiket a legigényesebb és ezáltal általában a legnagyobb nyereséget termelő ügyfeleik elvárásai szerint fejlesszék. Ezáltal a piacnak csak egy szeletére koncentrálnak, míg mások elvárásai háttérbe szorulnak. Az új piacra lépő sikeresen fejleszt ennek a szegmensnek olyan üzleti megoldásokat, melyek az ő igényeiket elégíti ki. Ezen megoldások jellemzően olcsóbbak, hiszen a termékkel, szolgáltatással kapcsolatos elvárások is alacsonyabbak. A piaci szereplői nem reagálnak az új szereplő belépésére, mert számukra kevésbé vagy egyáltalán nem nyereséges üzletrészt céloz meg. Az új piacra lépő később megcélozza a piac felsőbb szegmensét, melyben a jelenlegi piaci szereplők tevékenykednek. Megtartják a sikerük alapját képező eredeti fejlesztést, de már képesek a magasabb elvárásoknak is megfelelni. Amikor a piaci szereplők elkezdik elveszíteni a legjobb ügyfeleiket, a rombolás már megtörtént. [6]

Nem minden innováció romboló, akkor sem, ha az forradalmi. Például, az automobil feltalálása nem volt romboló hatású a lovas kocsikra nézve, mert az autók történelmük első 30 évében luxuscikknek számítottak. Az alacsony árfekvésű Ford T-Model 1908-ban megkezdett tömeggyártása viszont rombolónak bizonyult, mert megváltoztatta az egész közlekedést.

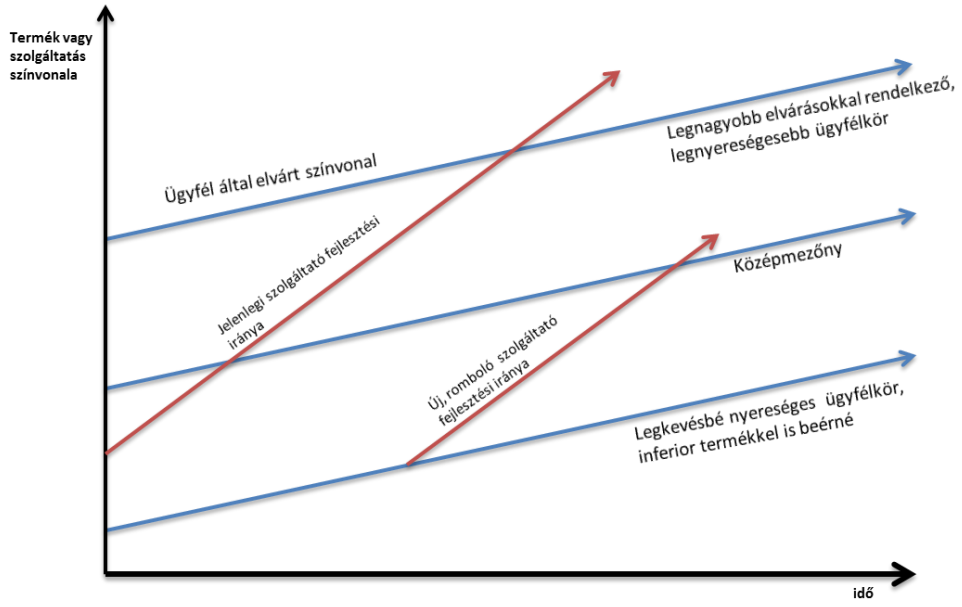
Christensen különbséget tesz *low-end disruption* és a *new-market disruption* között. A *low-end disruption*, vagyis az alacsonyabb elvárásokkal rendelkező ügyfélkörben történő rombolásról akkor beszélünk, amikor a termék vagy szolgáltatás tulajdonságai túltesznek a vásárló elvárásain. A többlet minőségért pedig csak egy inferior[7] termék hiánya miatt hajlandó magasabb árat fizetni. A romboló vállalkozás éppen egy ilyen inferior termékkel lép a piacra, melynek minősége még éppen elég jó, hogy a vásárlók ezen szegmense átpártoljon. [7]

Az úgynevezett *new market disruption*, vagyis rombolás új piacok megnyitása által, pedig olyan új vagy fejlődő piaci szegmensekre összpontosít, amelyeket a jelenlegi piaci szereplők nem szolgálnak ki. Egyszerűen kifejezve nem-fogyasztókat fogyasztóvá tesz. Vegyük példaként a kezdeti fénymásolási technológiát. A Xerox célfogyasztói köre óriás vállalatokból állt, akiknek magas áron tudták értékesíteni a termékeiket az elvárt teljesítményért cserébe. Kisebb mennyiségekkel rendelkezőknek maradt az indigó vagy a stenciles sokszorosítógép, mivel ők a piaci árakat nem tudták megfizetni. A 70-es évek végén megjelent a személyi nyomtató, mely egy új piacot hozott létre, mivel elérhető megoldást nyújtott egyéneknek és kisebb szervezeteknek is. A személyi nyomtatók ebből a kezdetben moderált piaci jelenlétből veszélyeztették később a Xerox fő fénymásoló piacát is. [6]

Az üzleti rombolással kapcsolatos elmélet megkülönbözteti a romboló innovációt az úgynevezett *sustaining innovation*, vagyis fenntartó innovációtól. Ez utóbbi a fogyasztó számára jónak vélt terméket tesz mégjobbá: ötödik penge a borotván, tisztább TV képminőség, jobb mobiltelefon hálózat lefedettség. Ezek a fejlesztések

[7] inferior: alárendelt vagy alsóbbrendű javaknak nevezik a mikroökonómiai fogyasztáselméletben azokat a javakat, amelyek a fogyasztó vagy fogyasztók jövedelmének változására keresletük ellenkező előjelű változásával reagálnak

lehetnek pótlólagos előnyök vagy jelentős áttörések, de mindnek az a célja, hogy többet értékesítsen a vállalat a már meglévő, nyereséget termelő ügyfeleinek. [6]



2. ábra: A romboló innováció (Forrás: saját szerkesztés Clayton M. Christensen munkája alapján)

A mai modern információ- és tudás alapú technológiáknak a célja és módszertana egységes:

- integrálják a feladatokat, a munkaerőt, a tudást,
- túlmutatnak az elméleti és adminisztratív tevékenységek klasszikus szétválasztásán,
- növelik a rendszerszemléletű látásmódot,

- előtérbe helyezik az önbizalmat, az önkiszolgálást, az innovációt és a kreativitást.

Ezzel szemben a hagyományos technológia, függetlenül attól, hogy mennyire új, komplex, vagy haladó, még mindig igényli:

- a feladatok, a munkaerő és a tudás megosztását,
- növeli a specializációt,
- előtérbe helyezi a felosztást és függőséget,
- fenntart közvetítőket,
- csökkenti a kezdeményezést.

A technológiai fejlesztések iránya visszatükrözi azt, ahogy a tudás dominanciája felülmúlja a tőkét, munkaerőt és nyersanyagot, mint közgazdasági erőforrásokat. A technológiák gyorsan változnak a központi hierarchiáktól a szétosztott hálózatok irányába. Manapság a tudás nem egy szuperagyban, szuperkönyvben vagy szuperadatbázisban van, hanem hálózatok komplex viszonyrendszerében, mely elősegíti a feladatok egyéni megoldását.

Vegyük az Ubert, a mindenki által jól ismert személyszállítási vállalatot, amely egy mobil applikáción keresztül összeköt olyanokat, akik utazni szeretnének, olyanokkal, akik el akarják vinni őket. A vállalatot 2009-ben hozták létre és fantasztikus növekedésen ment keresztül (több mint 100 városban van jelen, 60 országban és folyamatosan bővül). A vállalkozás a pénzügyi jelentések alapján hatalmas siker (a vállalat értéke jelenleg meghaladja az 50 milliárd USD-t). Az Uber ténylegesen megváltoztatja a taxizás üzleti környezetét. A fenti elméletek szerint

viszont nem számít romboló innovációnak. Habár az Uberre többen romboló innovátorként tekintenek, csupán a pénzügyi és stratégiai eredményei ezt nem igazolják. Romboló innovációnak csak azt az innovációt nevezzük, mely vagy új piacot hoz létre (személyi nyomtatók) vagy egy inferior termékkel lép a piacra (Ford T-modell). Az Uberről egyiket sem mondhatjuk el. Nehéz lenne azt állítani, hogy a vállalat egy inferior terméket kínál: ez azt jelentené, hogy a taxi társaságok túlzásba estek a szükségletek területén, tehát a taxi túl szép vagy túl könnyű használni. Azt sem állíthatjuk, hogy az Uber olyan célközönséget céloz, akik eredetileg nem használtak volna taxi szolgáltatást. Az Uber fogyasztói éppen ellenkezőleg, jellemzően olyanok, akik taxival szeretnének utazni. [6]

Az Uber meglehetősen vitatható módon növelte a teljes keresletet, amely várhatóan megtörténik, ha egy jobb, olcsóbb megoldást fejleszt egy vállalkozás egy széles körben használt szolgáltatásra. Ezért azt mondhatjuk az Uberre illő elmélet a fenntartó innováció. Több eleme is erre utal, de a leglátványosabb, hogy az ilyen típusú innovációra érzékenyen és azonnal reagálnak a piaci szereplő: új versenyképes technológiát vezetnek be, mint a saját applikációk és tiltakoznak az Uber szolgáltatás elemeinek illegalitása miatt. Ahogy az Uber esete mutatja, az igazi romboló innováció felismerése egy bonyolult feladat. Ugyanakkor elkerülhetetlen a megfelelő stratégiai döntések meghozatalakor.

Fejlesztések a szállítmányozásban

A korunkban elérhető innovációs kezdeményezések jellemzően a szállítmányozás átláthatóságára törekszenek. A digitalizáció megváltozatja az üzleti modelleket, ezáltal új értéket és bevételi forrást is teremt. Az eszközök közötti kommunikáció, okos megoldások és az internet egyre jobb elérhetősége és felhasználása

tönkreteszi a hagyományos értékláncokat, növeli az árak átláthatóságát, ezáltal megváltoztatja magát az árazást is. Esetünkben a fuvarozók fenntartó innovációja a szállítmányozóra hathat rombolóként, hiszen az esetek nagy többségében a szállítmányozás inferior terméke a fuvarozás. A fuvarozó szempontjából a fejlesztések többsége csupán a verseny elengedhetetlen részeként jelen lévő fenntartó innovációként jelenik meg, amellyel nekik lépést kell tartaniuk. A szállítmányozás viszont nem csak a fuvarozó közvetítéséből áll, ezért egy komplexebb szállítmányozási ügyletet nézve a szállítmányozás alternatívája egy csináld magad logisztika, melyhez egyre jobb terepet nyújtanak az újkori fejlesztések. A fejlesztések révén egy logisztikai IKEA világa jön létre, ahol a kellő mennyiségű nyersanyag és szerszám rendelkezésre áll, de az összeszerelés már a fogyasztó dolga. Ilyen innovációnak minősül a Shipster, a Fleet, melyek a szállítmányozó kiváltását célozzák; a Timocom és egyéb fuvarbörzék vagy a Colo21[8] a gyűjtőszállítmányozás világában. Ez az innováció rombolja a szállítmányozást, de nem minden esetben. A Colo21 például gyűjtőszállítmányozási rendszereket kapcsol össze, úgy hogy a fogyasztó maga választhatja melyik területen melyik szállítmányozóval szeretne együttműködni. Így hát a rendszer alapja maga a szállítmányozás, viszont az egyes központosított hierarchiákat rombolhatja a jövőben. Érvényesül a modern tudásalapú technológiák módszertana a hagyományossal szemben. Az átláthatóság miatt, a Colo21 világában elemi szinten kell lépést tartani a versenytársakkal.

A jövő ugyanis ebbe az irányba tart, az egyre átláthatóbb, hálózat vagy közösség alapú rendszerekben a verseny az egyes részfeladatok szintjén jelenik meg. Amennyiben nem tetszik az egyik szereplő által nyújtott részszolgáltatás ára,

[8] Colo21: német startup vállalat

hatékonysága vagy a piaci értékelése, akkor az könnyen cserélhető lesz. Egy webes applikáció segítségével egyszerűen lecseréljük a szolgáltatót. A logisztikai IKEA alapú technológiáknak vannak hátulütői is: feltétlenül hisznek a piac szabályozó szerepében, elsősorban a minőség értékelésénél, vagy egyfajta uralom nélküli rend víziójaként. A piac önszabályozó hatása valóban lehet reális feltevés, de az alaptalan, ellenőrizhetetlen kritikák könnyen tönkre is tehetnek egy vállalkozást. Gondoljunk csak arra: hányan reklamálnak a legjobb éttermekben is. Elégedetlenkedők mindenhol vannak, a kérdés, hogy annak a célja, hogy felhívja a figyelmet egy rossz szolgáltatásra vagy termékre, vagy javítson a színvonalon vagy egyszerűen csak tudatosan reklamál, hogy árengedményt érjen el? Ezek a rendszerek alapesetként csak az első esetet veszik alapul. Képzeljük el, hogy a weben keresztül összekötünk 2 ismeretlenen felet, amelyek egyikének nincs semmilyen szakmai képzettsége, következésképpen azt sem tudja, mit várhat el a szolgáltatótól. A skála nagyon széles: több szolgáltatást, jobb elbánást, alacsonyabb árat.

Következtetésképpen elmondhatjuk, hogy a jelenleg látható szállítmányozási innovációk kockázati költsége igen magas. Ezen innovációk akkor működhetnek, ha az ügyfél maga is járatos a szállítmányozásban és tisztában van a helyi szokásokkal, üzleti környezettel, továbbá az üzletvitelére nem hat zavarólag a különféle eljárásokból adódó extra munkateher.

A jövő szállítmányozása feltétlenül egy digitalizált, JIT infokommunikáción alapuló decentralizált, esetenként közösségi megoldásokkal kiegészített, moduláris, elemi szinten versenyeztetett tevékenység lesz. A várható áttörést ugyanakkor nem a digitalizáció fogja meghozni, amely a fenntartó fejlesztés eszköze, hanem egy új piacot nyitó innovatív megoldás. Az új piacra lépőknek képesnek kell lenniük

árutovábbításra biztonságosan, darabáron, jó költséghatékonyság és átláthatóság mellett. A szállítmányozás hozzáadott értéke a jövőben egyfelől tehát a biztonság: az információé, az üzleti érdeké, az árué-, a szolgáltatásé és a minőségé. Másfelől a hálózatok kialakításával és folytonos versenyeztetésével elért költséghatékonyság, mellyel a megbízók változó költségre vonatkozó igényét is ki lehet elégíteni. Harmadrészt, a szállítmányozó maga vállalkozhat az egyes piaci szereplők transzparens értékelésére, ezáltal a logisztikai IKEA egyik szereplőjévé is válhat, melynek következtében a megbízók képesek lesznek eldönteni, melyik alvállalkozóval, milyen minőségi szinten akar együttműködni. Ez a tevékenység viszont korlátozódni fog a hagyományos, nagy volumenű szállítmányozási formákra, mint a komplett rakományos szállítmányozás a kapacitással jól lefedett viszonylatokban. A szállítmányozóra továbbra is szükség lesz egzotikusabb, kihívásokat rejtő feladatoknál, ahol a szállítmányozó know-how-jára van szükség.

Összefoglaló

A cikkben bemutattam a szállítmányozás kialakulásának történeti okait, valamint jelentőségét az egyes korszakokban. A szállítmányozás jelentősége a hozzáadott értékében rejlik, de ez a hozzáadott érték folyamatosan változik, ahogy a szállítmányozásnak is szükséges megújulnia. A cikkben három időszakot különböztettem meg, részletesen bemutatva a változó piaci körülményeket és a szállítmányozás kihívásokra adott válaszát. A kérdés, hogy a szállítmányozó hozzáadott értéke változik-e a jövőben a digitalizáció és az innovatív technológiák gyorsuló ütemű megjelenésével, eldőlt. A jelenleg számba vehető fejlesztések iránya az átláthatóság és a közösségi megoldások alapjain nyugszik. Ezen megoldások piaci elterjedése a szállítmányozó alap know-how-jának tekintett kapcsolati rendszert értéktelenné teszi. A szállítmányozási szakma új értékeket

kénytelen keresni, a fennmaradása érdekében. Ezen értékek legfontosabbika a biztonság, amely lehet szolgáltatási, ellátási vagy műszaki jellegű.

Felhasznált irodalom

[1] I. Dr.Magyary, „Szállítmányozási Ismeretek," Gyöngyös, Károly Róbert Főiskola.

[2] KOTK, A külkereskedelem technikája, I-IV., Budapest, 2005.

[3] H. Obiri-Yeboah és E. E. T. Ghansah, „Role of Freight Forwarding & Logistics Firms in Supply Chain," *Dama International Journal of Researchers,* pp. 40-47, 1 április 2016.

[4] J. A. Schumpeter, „The Theory of Economic Development: An inquiry into profits, capital, credit, interest and business cycle," 1911.

[5] C. M. Christensen, The innovator's dilemma: when new technologies cause great firms to fail, Boston: Harward Business School Press, 1997.

[6] C. M. Christensen, M. E. Raynor és R. McDonald, „What is Disruptive Innovation?," *Harward Business Review,* december 2015.

[7] Wikipedia, „Wikipedia," [Online]. Available: https://en.wikipedia.org /wiki/Disruptive_innovation. [Hozzáférés dátuma: április 2016].

[8] Kühne+Nagel, „Integrated Logistics ppt. bemutató," 2016.

[9] Négyesi Imre: DIE ÜBERPRÜFUNG DER VORAUSSETZUNGEN VON COTS SYSTEMEN (COTS RENDSZEREK KÖVETELMÉNYEINEK VIZSGÁLATA) (Hadmérnök on-line, VII. évfolyam (2012) 2. szám, 371-376. oldal, ISSN 1788-1919).

Paráda István – Bodnár István: Jelszó ellopás social engineering, e-mail spoofing és fake url segítségével

Absztrakt

A mai információs társadalom, és a folyamatosan fejlődő technikai megoldások világában jelentős szerepet tölt be az információ, illetve informatikai biztonság. A kérdéskör vizsgálatánál egyedi megközelítést ad, ha az ellentétes oldalról próbálunk betekintést nyerni. A biztonságot fenyegető megoldások száma rengeteg és kivitelezési módjai is különbözőek, így a cikkben vizsgált gyakorlat kellő rávilágítást ad ezek fontosságára, valamint komplexitására.

Kulcsszavak *Social Engineering, Fake URL, E-mail spoofing, Hack, Linux, Site klónozás, Jelszó*

Bevezetés

„A valós ***információ*** létfontosságú, a téves ***információ*** sajnálatos és káros, de a jól irányzott hamis ***információ*** halálos.”

Frederick Forsyth

Napjainkban rengeteg cikket lehet olvasni, vagy hírt hallani arról, hogy „hackerek” törtek fel különböző intézményi adatbázisokat, és ennek útján olyan információkhoz jutottak, amelyeket valamilyen formában felhasználhattak. Az ilyen jellegű támadásokra számos példát fel lehet mutatni. Az elektronikai, informatikai információhalmazok elleni támadások rendkívül széles skálán mozognak, a személyes, céges adatoktól kezdődően akár a pacemakerek hackeléséig, melyek már közvetlenül az emberi élet kioltására is irányulhatnak. Ehhez ismét nem kell más, mint, adott információ birtokában felülírni egy

szabályozó programot. Az információk meghatározzák, befolyásolják lehetőségeinket, így ebből kifolyólag életünket, az ehhez kapcsolódó igényeket és anyagi erőforrásokat is. [1]

Ahhoz hogy, biztonságban tudjuk adatainkat, meg kell ismerni az ellenük irányuló támadásokat. Tehát meg kell érteni az ellenség gondolkodásmódját, továbbá a kárt okozók szemszögéből kell megvizsgálni saját erőforrásaink biztonságát, biztonsági réseit. Amennyiben megvizsgáljuk és megértjük az ellenünk irányuló információs támadásokat, úgy e folyamatokat a megelőzés folyamatával képesek leszünk elhárítani, megakadályozni. Közhellyel élve az ellenség fejével kell gondolkodnunk. [2]

Cél meghatározása

Általában különféle indíttatásokból kifolyólag, keletkezik egy igény, amely felhasználónév és jelszó jogosulatlan hozzáféréshez csatlakozik. Rengeteg feltört telefont, számítógépet, valamint postafiókot láthatunk főleg közismert emberek körében melyekből a felhasználónév és jelszó páros segítségével nem nyílt, sokszor kompromittáló információkat nyertek illetve szivárogtattak ki.

Vizsgáljuk meg a helyzetet műszaki szempontból. Felkérnek egy ilyen postafiók vagy akár facebook profil feltörésére. Felvetődik a kérdés, hogy milyen metódussal közelítsük meg a megvalósítást illetve mi a célunk vele?

A cél egyértelműen valamilyen rendszerbe történő bejutás, más jogosultságával. Ezáltal személyes információk birtokába jutni. A metódus az egyszerűség elvét követi. Természetesen szubjektív fogalom, hogy kinek mi a legegyszerűbb. Létrehoztunk egy gyakorlatot, amelyben magamból indultam ki és ily módon

választottam meg a támadási mechanizmusokat, azaz amely nekem a legegyszerűbb módszernek látszott.

Megvan a célom és a hogyant is megválaszoltuk. Következő lépés a tervkészítés, és információszerzés. Fiktív felkérésünkben a facebook feltörést valósítottunk, meg amit gyakorlatban is kipróbáltunk. Itt természetesen volt valamilyen indokunk kiválasztani az adott célszemélyt, például olyan beosztást tölt be ahol akár facebookon keresztül is értékes információkat szerezhetünk be a cégéről, kollegáiról stb. Valamint akár bosszú, vagy csak szakmai tudásunk fitogtatásának indokán is választhatunk egy profilt. Erről az emberről minél több információt kell gyűjteni. Mivel az Internet világában élünk ez már viszonylag könnyen megvalósítható. Facebook, google, stb.

A támadás végrehajtásánál fel kell ismernünk korlátainkat is. Olyan módszert választunk, ami vezeték nélküli hálózaton valósítható meg. Ehhez szükségük van arra, hogy az áldozattal egy wifi routeren csatlakoznunk az Internetre. Ez is többféleképpen valósítható meg vagy leinformálódunk az otthoni hálózatáról és akár WPA2 jelszófeltöréssel csatlakozunk rá, vagy csak kivárjuk, amíg egy nyílt hálózatra csatlakozik valamilyen közösségi helyen.

Támadás végrehajtása

A konkrét letesztelt támadásnál Kali Linux operációs rendszert használtunk. Előnye hogy rengeteg informatikai biztonságot veszélyeztető programmal rendelkezik, így ennek telepítése már nem szükséges. Ezen kívül egy vezeték nélküli Wi-fi routerre és egy áldozat webes tartalmat megnyitni képes informatikai eszközre.

Kali linux:

Ez a backtrack5 továbbfejlesztett változata, debian alapokon. Elvileg pentest, és biztonsági tesztekre használható. A kaliban megtalálható szinte mindegyik program,ami a backtrackben is volt, hálózati biztonsági tesztelő programok,kezdve,a proxy, fuzzer, crawler, minden ami kellhet a biztonsági rések teszteléséhez hackeléshez. A BackTrack egy Debian Linux alapú, számítógépek sebezhetőségével foglalkozó, teljesen ingyenes operációs rendszer. Nevét a backtrackingkereső algoritmus után kapta. Hackerek és biztonsági szakemberek körében nagyon népszerű. Operációs rendszerek (jellemzően Microsoft Windows) sebezhetőségeinek felderítésére és kihasználására alkalmas. Rengeteg sikeres betörést hajtottak vele végre szerte a világon.[3]

1. ábra Kali Linux

Mit is tartalmaz a Kali?

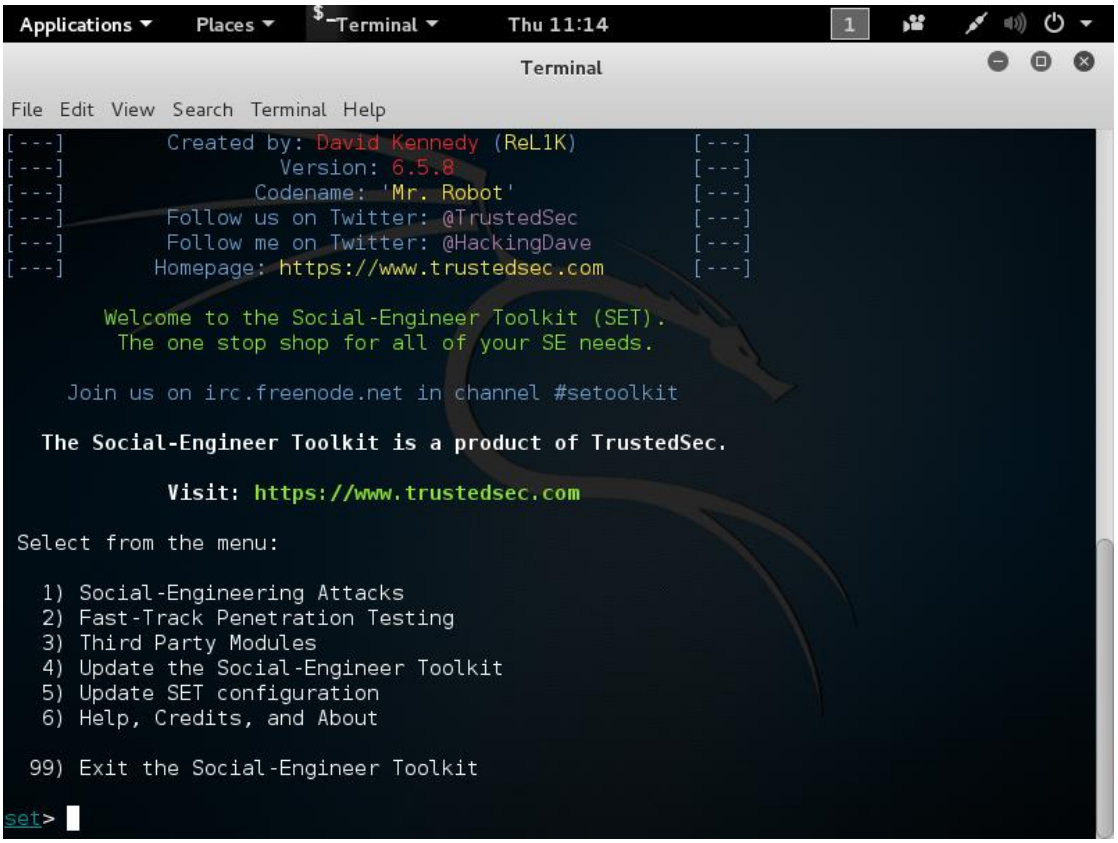
- Metasploit integráció
- RFMON Injekció képes WiFi driverek
- Aircrack-ng

- Gerix Wifi Cracker
- Kismet (szoftver)
- Nmap
- Ophcrack
- Ettercap
- Wireshark (korábban Ethereal néven volt ismert)
- BeEF (Browser Exploitation Framework)
- Hydra
- OWASP Mantra Security Framework hacker eszközök készlete, add-onok Firefoxhoz
- Cisco OCS Mass Scanner Egy nagyon megbízható és gyors szkenner Cisco routerekhez.
- Nagy számú exploit gyűjtemény [4]

Támadás

A kali-ban található setoolkit segítségével a kiválasztott weboldal leklónozása. A gyakorlat esetében ez a www.facebook.com

- 1. Social-Engineering Attacks
- 2. Website Attack Vectors
- 3. Credential Harvester Attack Method
- 2. Site Cloner



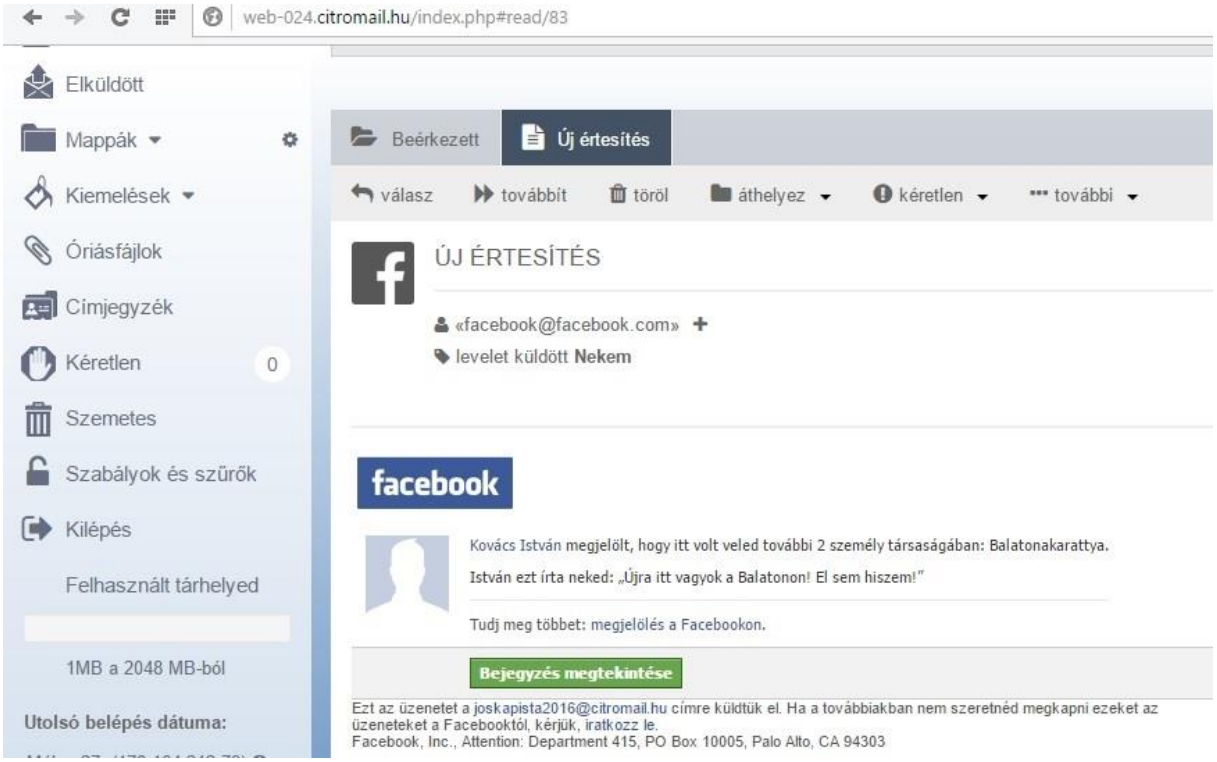
2. ábra Setoolkit

A fenti menüpontok megadása után a program kér egy IP-címet amelyet a támadó gép IP címére kell beállítani. Továbbá a klónozott oldal URL címét kéri (Ebben az esetben facebook.com). A program elindít a támadó számítógépen egy Apache szerverszolgáltatást. Azaz a gép egy webszerver szerepét játssza, amely IP címét beírva a böngészőbe, olyan webalapú szolgáltatást biztosít, mint az eredeti oldal. Természetesen fellép pár különbség az eredeti és a „fake” oldal között, az előnyös, hogy a felhasználónév és jelszó begépelésekor a támadó most már szerver gép egy text fájlba menti az adatokat, így hozzáférési adatokat biztosítva a célszemély adatlapjához, másrészt egy hátrányos különbség is mutatkozik, hisz az URL

mezőben az IP cím látszik. Ezt a hibát számos Interneten feltalálható oldallal maszkolni lehet. (Például http://bit.ly/).

A támadás folyamán, amikor a hitelesítési információk mentésre kerültek, az oldal automatikusan átirányítja az áldozatot az eredeti oldalra, így csökkentve annak esélyét, hogy a célszemély felismeri magát a biztonsági eseményt.

Ezen folyamatok során felmerül a kérdés, hogyan érjük el, hogy az áldozat a Fake URL címre jelentkezzen be. E-mail spoofing segítségével, olyan levelet küldünk neki, amely alapoz a Social Engineering-re, hisz megbízható forrást sugall. Ehhez lemásoltuk a facebook által kiküldött egyik általános üzenet html kódját. A lenti ábra mutatja a végeredményt.



3. ábra E-mail spoofing

A találó és csalogató szöveg után a „bejegyzés megtekintése” gombra kattintva, az áldozat a támadó Fake oldalára kerül, ahol felhasználóneve és jelszava mentésre kerül.

A megbízhatóság látszatát keltve, a e-mail header-t is átírjuk, így olyan emberek nevében is küldhetünk e-mailt, akikben az áldozat bízik.

Összegzés

Ezek alapján a Social Engineering, a Fake URL és az E-mail spoofing segítségével viszonylag könnyen hozzájuthatunk célszemélyek adataihoz, mérgezhetjük meg postafiókjukat különféle e-mailekkel. Természetesen a fenti támadási folyamatban

vannak korlátok, mint a kritériuma annak, hogy a támadó és az áldozat egy Wi-fi hálózatra csatlakozzanak, mégis az ilyen támadások véghezvitele felhívja a figyelmünket a megfelelő biztonságtudatra. Valamint arra, hogy kellően megalapozott háttértudással és minimális szoftver illetve html ismeretekkel mennyire egyszerű végrehajtani egy jelszó ellopására irányuló támadást. A gyakorlat végrehajtásra került 2016. májusában Balatonkenesén NKE HHK KÜI Híradó Tanszék Információvédelmi Konferenciáján. [5]

Hivatkozások

[1] Tóth András: A felhőinformatika alapjai, HÍRVILLÁM = SIGNAL BADGE 2:(1, pp. 85-90., 2011

[2] Paráda István - A hálózatbiztonság vizsgálata a hálózati eszközöket érintő támadások gyakorlati szimulációin keresztül 2013

[3] https://www.kali.org

[4] http://www.gamechannel.hu/cikk/blog/kali_a_backtrack_ujjaszuletese 2016.07.06

[5] Saját gyakorlat végrehajtás 2016. május Balatonkenese NKE HHK KÜI Híradó Tanszék Információvédelmi Konferencia

Szerzőink figyelmébe

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás nélkül* - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni

és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Felelős kiadó: Dr. Fekete Károly mk. alezredes
Megjelent az NKE HHK Híradó Tanszék gondozásában, 10 példányban, illetve elektronikusan:

www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-407 mellék)
hhk_hirado_szakcsoport@uni-nke.hu