

HADTUDOMÁNY

A MAGYAR HADTUDOMÁNYI TÁRSASÁG ÉS
AZ MTA HADTUDOMÁNYI BIZOTTSÁG FOLYÓIRATA



XXIX. évfolyam
2019/3.

A TARTALOMBÓL

A magyar királyi honvédség szervezése és lehetőségei 1920–1938 között

Térbe írt (had)történet

A hadtörténelem helyéről és szerepéről félévszázada folytatott diskurzus máig ható tapasztalatai

Gerilla-ellenes műveletek az egykori indokínai térségben: a LEA-hadművelet

Mesterséges intelligencia és a hadseregek

Adalékok a közigazgatás információ-biztonságához

A szervezeti kultúra fejlesztésének időszerű kérdései a honvédségben

A magyar védelmi ipar fejlesztésének esélyei a Zrínyi 2026 program tükrében

A Hadtudomány a Magyar Tudományos Akadémia támogatásával jelenik meg. A folyóiratot az MTMT indexeli és a REAL archíválja.

A lapszám szerzői:

Dr. Andaházi Szeghy Viktor őrnagy, PhD,
a HM Oktatási, Tudományszervező és
Kulturális Főosztály kiemelt főtisztje

Beláz Annamária, az Óbudai Egyetem doktorandusza

Dr. Boda Mihály PhD,
a NKE HHK egyetemi docense

Budavári Krisztina államháztartási gazdálkodás és
ellenőrzés szakértő, nemzetközi biztonság- és
védelempolitikai szakértő,
a ROTEC-Rockwell Technologies Kft.
ügyvezető igazgatója

Dr. Forgács Balázs őrnagy, PhD,
a NKE HHK egyetemi docense

Harangi-Tóth Zoltán százados,
NKE HHK egyetemi tanársegédje

Dr. Hausner Gábor alezredes, PhD,
a NKE főmunkatársa

Dr. Hegedűs Henrik ny. alezredes, PhD,
a Magyar Hadtudományi Társaság alelnöke,
Hadtudomány Szerkesztőbizottságának
elnöke, 2019-től

Dr. Király László CSc,
a Hadtudomány Szerkesztőbizottságának
2010 és 2019 közötti elnöke

Krizbai Diána Daniella, az MTI újságírója

Dr. Krizbai János ny. ezredes, CSc,
az MHTT Humánforrás-fejlesztési
Szakosztályának elnöke

Dr. Négyesi Imre mk. alezredes, PhD,
NKE HHK tanszékvezető egyetemi docense

Tulipán Éva, a HM HIM Tudományos főmunkatársa

Vánczi Dániel, az Óbudai Egyetem doktorandusza

Zsigri Ferenc, a Szent István Egyetem doktorandusza

Rövidítések jegyzéke:

HM – Honvédelmi Minisztérium
NKE – Nemzeti Közzolgálati Egyetem
HHK – Hadtudományi és Honvédtisztképző Kar
MTI – Magyar Távirati Iroda
MHTT – Magyar Hadtudományi Társaság
HIM – Hadtörténeti Intézet és Múzeum

A Magyar Hadtudományi Társaság és az MTA Hadtudományi Bizottság lektorált folyóirata

Felelős kiadó:

Szenes Zoltán, az MHTT elnöke

A folyóirat szerkesztőbizottsága:

Elnök:

Hegedűs Henrik, az MHTT alelnöke

Elnökhelyettes:

Bertalan György főszerkesztő

Rovatvezető (angol nyelvű közlemények):

Panajotu Kosztasz

A bizottság tagjai:

Balla Tibor,

Forgács Balázs,

Haig Zsolt,

Hausner Gábor,

Horváth Attila,

Kátai–Urbán Lajos,

Lakner Zoltán

Palik Mátyás,

Siposné Kecskeméthy Klára,

Ujházy László.

Szerkesztőbizottság és kiadó:

Budapest X.,

Hungária krt. 9–11.

Tel.: 432-9000/29-684 mellék

(A mellék HM-vonalon
közvetlenül hívható.)

Levélcím:

1581 Budapest, Pf. 15.

E-mail cím:

hadtudomany@freemail.hu

Honlap:

www.mhtt.eu/?page=ht_archiv

Nyomtatott kiadásváltozat:

ISSN 1215-4121

Nyomdai előkészítés:

BAUSZ Stúdió

Nyomtatta:

Prime Rate Kft.

Online kiadásváltozat:

ISSN 1588-0605

Webmester: Jelencsics Imre

HADTUDOMÁNY

A MAGYAR HADTUDOMÁNYI TÁRSASÁG ÉS
AZ MTA HADTUDOMÁNYI BIZOTTSÁG FOLYÓIRATA

XXIX. évfolyam

3. szám

2019. SZEPTEMBER

Tartalomjegyzék

HADTUDOMÁNY – HADÜGY

- Forgács Balázs Abraham Guillén és a városi gerilla-hadviselés 3
- Andaházi Szeghy Viktor
Trianontól Bledig: a magyar királyi honvédség
szervezése és lehetőségei 1920–1938 között 15
- Boda Mihály Az alapvető katonai erények mibenléte és helyük
a hosszú 19. századi magyar
hadtudományos gondolkodásban
5. rész – A magyar hadtudományos irodalom 24
- Tulipán Éva Térbe írt (had)történet. Elméleti és módszertani vázlat . . 33
- Hausner Gábor Egy félévszázados diskurzus
a hadtörténelem helyéről és szerepéről.
Perjés Géza hozzászólása
a magyar hadtörténetírásról zajló vitához 1956 nyarán . . 43

KATONAI MŰVELETEK

- Harangi-Tóth Zoltán A LEA-hadművelet 59

HADITECHNIKA

- Négyesi Imre A mesterséges intelligencia és a hadseregek 71
- Váczai Dániel Az emberi tényező kockázatainak modellezési
lehetősége Fuzzy-logikával a vasútnál,
mint kritikus infrastruktúrában 80

Beláz Annamária	A közigazgatás információbiztonsága: megjósolhatók az incidensek?	92
-----------------	--	----

HUMÁNPOLITIKAI SZAKTEVÉKENYSÉGEK

Zsigri Ferenc	Döntési elméletek (szakirodalmi áttekintés)	105
Krizbai János	A szervezeti kultúra fejlesztésének kérdései a honvédségben	118
Krizbai Diána Daniella	Álhírek és a biztonságunk	128

VÉDELEMGAZDASÁG ÉS LOGISZTIKA

Budavári Krisztina	A Zrínyi 2026 program. Korlátozott lehetőségek a magyar védelmi ipar fejlesztésére	142
--------------------	---	-----

FÓRUM

Király László	Tíz év mérlege (a szerkesztőbizottság elnöki tisztségéből)	160
Hegedűs Henrik	Az Olvasó köszöntése	162

ABSTRACT	163
--------------------	-----

Közlemény	169
---------------------	-----

Beláz Annamária

A közigazgatás információbiztonsága: megjósolhatók az incidensek?¹

DOI 10.17047/HADTUD.2019.29.3.92



Az állami feladatok hatékony, eredményes és gazdaságos ellátását a modern, digitális közigazgatási szolgáltatások segítik. A közigazgatási rendszerekben tárolt, feldolgozott és továbbított adatok védelmének, biztonságának mindenkor prioritást kell élveznie. Jelen tanulmány bemutatja, hogyan használhatóak fel a valószínűségszámítás és a statisztikai elemzés módszerei a biztonsági incidensek előrejelzésében és elhárításában.

Az internet, a hálózat alapú rendszerek egyre inkább nélkülözhetetlen részei a mindennapjainknak. Nem okoz ennél fogva különösebb meglepetést az, hogy az átlagos polgárok – a híroldalak és közösségi média platformok böngészésén túl, – egyre gyakrabban mobilkészülékeiken, okos eszközeiken keresztül intézik közigazgatási hatósági ügyeiket. A közigazgatás modernizációjával, digitalizálódásával azonban együtt kell járnia annak, hogy növeljük az információs rendszerek megbízhatóságát és az információbiztonsági események elleni védekező képességét.

Az információbiztonsági incidensek száma minden évre egyre nagyobb méreteket ölt, ezen incidensek egyre jelentősebb anyagi károkat okoznak. Az incidensek alól a közigazgatás, a közszeaktor sem képez kivételt. „A statisztikai adatok alapján a 2017-es év első felében globálisan közel kétmilliárd adatrekord került illetéktelen eltulajdonításra, milliós károkat okozva ezzel a köz- és magánszeaktorok egyaránt. Az eltulajdonított adatok huszonegy százaléka (404.244.346 adatrekord) a közszeaktorból származik.² Az illegális adatszerzés mellett számos más típusú információbiztonsági támadásnak vannak kitéve a közszeaktor szervezetei, többek között: szolgáltatásmegtagadással járó támadás, weblaprongálás, káros szoftverek, adathalászat, kéretlen levelek és jogosulatlan hozzáférés.” (Beláz 2018)

1 A kutatás a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet támogatásával a Belügyminisztérium és a Belügyi Tudományos Tanács által meghirdetett kutatási gyakorlati program keretében készült. Elismeréssel és köszönettel tartozom Doroszi Zoltánnak, aki a téma iránti szeretettel és elkötelezettséggel irányította a szakmai munkát.

2 Gemalto Breach level index: *Findings from the first half of 2017*;
<http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf>

Jogos kérdést fogalmaz meg a témával kapcsolatban Csutak Zsolt (2018, 172.) „... ki vagy mi képes felügyelni, irányítani, illetve biztonságos, emberbarát működést biztosítani... a milliárdnyi okoseszköz számára egy olyan fékezhetetlenül fejlődő, számítógépek uralta világban, ahol a webalapú bűncselekmények és visszaélések száma 2015-ben az Amerikai Egyesült Államokban és az Egyesült Királyságban már letaszította trónjáról a szervezett bűnözést és a kábítószer-kereskedelmet?”

Annak érdekében, hogy a közigazgatási rendszer hosszú távon működőképes maradjon, valamint a rendszerekben előállított, tárolt, feldolgozott és továbbított adatok védelme biztosított legyen, az államnak kiemelkedő feladata az információbiztonság szervezése és az információbiztonsági szemléletmód kialakítása, fenntartása. Ennek érdekében szükséges, hogy az információbiztonsági feladatok és programok jogi és stratégiai szinten is megjelenjenek, azok szerves részét alkossák a kockázatelemzési és értékelési folyamatok, megoldások, továbbá a prediktív, előrejelző funkciók.

A közigazgatás szervezetrendszerének és infrastruktúrájának védelme különösen azért indokolt, mert az állami alapfeladatok végrehajtásáért a közigazgatás felel, így amikor közigazgatási feladatokról és funkciókról beszélünk, akkor tulajdonképpen a feladatok mögött meghúzódó, azok létrehozását indokló általános állami érdekeket vizsgáljuk. A közigazgatás öt alapvető területe (külügyi-, rendészeti-, hadügyi-, igazságügyi és pénzügyi igazgatás) az állam állami mivoltából, azaz a közhatalomgyakorlásból fakad. Az állam és a közigazgatás modernizációjával ez az öt alapvető funkció nem tűnik el, hanem folyamatosan kiegészül és differenciálódik.³ Vitathatatlan, hogy a közigazgatás, valamint az azt támogató infrastruktúra védelme kiemelkedően fontos terület minden állam számára.

Jelen tanulmány témájának szempontjából elkerülhetetlen a kérdés: mit értünk a *biztonság* fogalma alatt? A legtöbb ember számára a biztonság nem más, mint egy nyugodt, fenyegetésektől mentes állapot. Ugyanakkor el kell ismernünk, hogy ez a meghatározás meglehetősen felszínes, hiszen a biztonság fogalmához számos elmélet és eltérő tudományos megközelítés kapcsolódik. A biztonság körülírására szolgáló meghatározások vizsgálatát követően Gábris Máté (2010, 112.) tanulmányában a következő megállapítást tette: „... összességében elmondható, hogy a biztonság fogalma valamiféle fenyegetés köré épül, mely fenyegetésnek van egy forrása és egy alanya. A fenyegetés meghatározása lehet objektív és szubjektív. Előbbi a tradicionális vonulatra, míg az utóbbi az újszerű gondolkodásra jellemző. A fenyegetéshez kapcsolódóan a biztonság jelentheti a fenyegetés hiányát, vagy a fenyegetés korlátozására, visszaszorítására alkalmazható eszközök meglétét.”

A biztonságot kutató szakemberek közül Ole Waever az újszerű gondolkodók közé tartozik. Meglátása szerint a biztonság egy olyan állapot, ahol fenyegetések léteznek, de képesek vagyunk ellenlépések megtételére. Úgy gondolom, ez a megfogalmazás jól alkalmazható jelen tanulmány kereteiben is, hiszen a kibertérből érkező információbiztonsági fenyegetések folyamatosan jelen vannak, azaz léteznek, de az állam a biztonsági feladatának ellátása keretében képes a biztonsági események ellen való védekezésre, továbbá a meglévő képességek fejlesztésére törekszik.

3 A feladatrendszer ezen változásának történeti áttekintését Lőrincz Lajos akadémikus foglalja össze tanulmányában. (Lőrincz 2009)

A közigazgatás információbiztonságát szolgáló jogi és szervezeti kérdések fejtegetését számos kutató (többek között Muha Lajos, Munk Sándor, Kassai Károly, Kovács László, Krasznay Csaba, Simon László, Magyar Sándor, Kelemen Roland, Farkas Ádám) megtette tanulmányaiban, monográfiáiban. Jelen kutatás keretében e területek részletes kifejtésétől eltekintek, azokat csak a témakör áttekintéséhez szükséges mértékben mutatom be.

Dolgozatomban egy olyan modellezési metódussal kívánok a közigazgatás információbiztonságának komplex kérdésére megoldást keresni, amely dinamikusan változik, az egyenletbe kerülő elemek hatására. A közigazgatási rendszerek információbiztonsági intézkedési stratégiájának, akciótervének elkészítéséhez a statisztikai modellezés és a valószínűségszámítás módszertana alapot szolgáltat, függetlenül a biztonsági veszély forrásától és kiterjedésétől. Az általam felvázolt modell előnye, hogy független a szervezetrendszer méretétől, ennél fogva a megoldás a rendelkezésre álló adatok alapján ugyanolyan hatékonysággal alkalmazható egyetlen szervezet vizsgálatára, valamint az egész országra kiterjedő közigazgatási szervezetrendszerre is.

A tanulmány következő részében, a figyelem fókuszában az a kérdés áll, hogy milyen a közigazgatás működését veszélyeztető biztonsági fenyegetések vannak és mely biztonságtechnikai, szervezetrányítási megoldások segítenek ezek elhárításában.

A közigazgatás információbiztonságának védelme

A közigazgatás számára kiemelkedően fontos feladat a biztonság garantálása az offline és az online életben egyaránt. A közigazgatási feladatok folyamatosan változnak, sőt a feladatok skálája növekszik,⁴ azonban a feladatok mennyiségi változásán túl, a tudományos diskurzus során kiemelkedők az olyan szakaszok, ahol a közigazgatás lényegi tevékenysége sajátos karakterisztikát mutat. Ilyen egyedülálló szerepet tölt be a szolgáltató állam modell.

„Todd Ramsey A szolgáltató állam című művében kifejti, hogy a szolgáltató állam, szemben a korábbi modellekkel (pl. éjjeliőr állam, jóléti állam), alapvetően proaktív, az ügyfél elvárásainak megfelelő, igény szerinti szolgáltatásokat nyújt, miközben gyakran támaszkodik a partnerekre, beszállítókra. Ramsey a szerint határozza meg a szolgáltató államot, hogy a közigazgatási modernizáció mely ismérvek mentén zajlik. Hat egymással összefüggő ismérvet állapított meg, melyek a következők:

- | | |
|------------------------|---------------------------------|
| 1) koncepció, | 4) technológiai infrastruktúra, |
| 2) szervezeti kultúra, | 5) átalakítási menetrend és |
| 3) működési modell, | 6) távlatos gondolkodás. |

4 Berényi Sándor meglátása szerint a közigazgatás alapvetően vagy döntést hoz, vagy előkészíti mások döntéseit. Ezzel szemben Magyar Zoltán az állami feladatok komplex megközelítését írta le, kiemelkedő feladatként azonosította a következőket: községi szervezet biztosítása, közlekedés biztosítása, foglalkoztatás, társadalombiztosítás, gazdasági élet irányítása, alapvető szociális szükségletek biztosítása (élelem, lakhatás), közegészségügy, tudomány-oktatás, rendészet, azaz biztonság. (Berényi: A közigazgatás rendeltetése In: Fazekas-Ficzere (szerk.): Magyar közigazgatási jog, 42. o. (vö: Magyar: A magyar közigazgatás, 1942)

A közigazgatást érő elsősorban információbiztonsági kihívásokkal kapcsolatban a legfontosabb ismérvek a szolgáltató állam működési modellje és a technológiai infrastruktúra.” (Beláz 2018, 58.) Budai Balázs (2009) könyvében kifejti, miszerint a szolgáltató modell fejlesztési csapdája lehet, hogy az egyes lényegi (core) folyamatok, tevékenységek vagy feladatok modernizációja háttérbe szorul a kiegészítő tevékenységek (non-core) fejlesztése miatt. Ez a fajta hozzáállás egy látszólag jól működő, de a valóságban instabil szervezet, rendszer kiépítéséhez vezet. A gyakorlatban ez azt jelenti, hogy a közigazgatási szervezetek kitettsége az információbiztonsági incidenseknek növekszik, mivel az alapvető (ugyanakkor időigényes és költséges) folyamat, az információbiztonság fejlesztésének jelentősége csökkent valamely más tevékenység miatt.

Az incidensek

De melyek azok az incidensek, amelyek a közigazgatási rendszert érhetik? A 2013. évi L. törvény 1.§ 9. pontja következőképpen írja le a biztonsági esemény fogalmát: *„... nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmasága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül”*. Az információbiztonsági incidensek, jellegük szerint lehetnek fenyegetések, sérülékenységek vagy támadások. A kutatás során az alább incidens-típusokat vizsgáltam meg: adathalászat, káros szoftver, robothálózat, kéretlen levél, túlterheléses támadás, jogosulatlan hozzáférés, sérülékeny szolgáltatások, célzott támadás, honlap rongálás.

Hogyan zajlik, és milyen hatása lehet egy információbiztonsági incidensnek a közigazgatáson belül? Az információbiztonság lényegi folyamatának háttérbe szorítását a honlap-rongálás (defacement) eklatáns példáján keresztül lehet bemutatni. A kutatás által vizsgált időtartam (2017. január 1. – 2018. augusztus 31.) alatt 361 alkalommal került sor állami, közigazgatási honlapok rongálásával összefüggő incidensekre. A Nemzeti Kibervédelmi Intézet munkatársai az ellenőrzések keretében számos validációs hibát tártak fel. A kritikus találatok alapján elmondható, hogy az alkalmazásfejlesztők főként a működésre koncentrálnak munkájuk során, a biztonságos szoftverfejlesztés területén még kihívásokkal küzdenek. Egy defacement incidens esetén a hibajavítási munkák több napon át is eltarthatnak, de az idő ráfordításon túl, a valódi veszteséget, az állampolgárok megbízható közigazgatásba vetett bizalmának elvesztése jelenti.

A szervezetrendszer

Ezen incidensek elhárításához szükséges, hogy nemzeti szinten létre jöjjön egy hatékony reagálási képesség. Ahogyan Horváth és társai megfogalmazzák tanulmányukban (Horváth – Erdősi – Kiss 2016, 114.), *„... ez gyakran különböző nemzeti hálózatbiztonsági csoportok formájában valósul meg. A felállított szervezetek, csoportok feladatai többek között a fenyegetések megértése, értelmezése és prezentálása a döntéshozók számára... a megoldási*

javaslatok publikációja, az IT-biztonság oktatás és a legjobb gyakorlatok terjesztése, a veszélyforrások érzékelése, beazonosítása, és kezelése, az incidensek elemzése, a reaktív intézkedések megszervezése... valamint az ellenálló képességet növelő intézkedések promóciója.”

Akkor lehet sikeres egy szervezet, ha minél teljesebb mértékben éri el a szervezeti stratégiában megfogalmazott célokat. A célok eléréséhez egyrészt nélkülözhetetlen azok világos megfogalmazása, az akciók mérhető, követhető végrehajtása. Másrésztől azonban elengedhetetlen, hogy a stratégia végrehajtói, a vezetők jó döntéseket hozzanak, minimalizálva a kudarc lehetőségét. Ezzel összefüggésben a közigazgatás, mint szervezetrendszer sikere az információbiztonság területén függ az információbiztonsági kockázatok egyértelmű felmérésére, kezelésére létrehozott szabályzatok, valamint az azokhoz kapcsolódó eljárások minőségétől. (Michelberger – Lábodi 2012, 243. és Kerti – Nyikes 2015, 327.)

Az az információbiztonsági rendszer kiépítéséhez és a kapcsolódó kockázatmenedzsment feladatok végrehajtásához érdemes követni a Nemzetközi Szabványügyi Testület (ISO) egységes iránymutatásait.⁵ Az ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek című szabvány tartalmazza a kockázatmenedzsment⁶ alapelveit, valamint a kockázatfelmérés, kockázatértékelés és kockázatkezelés lépéseit. A szabványban felsorolt alapelvek közül a témánk szempontjából az alábbi négy alapelvet tartom kiemelkedően fontosnak. Ezek a következők:

1. A kockázatmenedzsment *feladata az értékek létrehozása és védelme*. A kockázatkezelés hozzájárul a célok kimutatható eléréséhez és a teljesítmény javításához a szervezet számos területén.
2. A kockázatmenedzsment *központi feladata a bizonytalanság fogalmának értelmezése*, természetének explicit módon történő megfogalmazása.
3. A kockázatmenedzsment az elérhető *legpontosabb tényeken, információkon alapul*, többek között: korábbi adatok, tapasztalat, érdekelt felek visszajelzései, megfigyelései, előrejelzései és szakértői vélemények.
4. A kockázatmenedzsment *szervezetre szabott*, igazodik az egyéni igényekhez. A szervezet külső és belső környezetével, valamint a kockázati profiljával összhangban kell megalkotni.

A felsorolt alapelvek közül a második a bizonytalanság fogalmának értelmezése, feladata. Ez az alapelv el is vezet minket a valószínűségszámítás és a statisztikai elemzés területére, mely területek az incidens előrejelzési modell alapjául szolgálnak.

5 ISO 31000-es szabványcsoport, magyar nyelvű címekkel:
 – MSZ 13073:2014 Kockázatfelmérés és -kezelés. Szakszótár,
 – MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek,
 – MSZ EN 31010:2010 Kockázatkezelés. Kockázat-felmérési eljárások.

6 A kockázatmenedzsment/kockázatkezelés (Risk Management) nem más, mint „egy szervezet kockázatokkal kapcsolatos összehangolt irányítási és felügyeleti tevékenységei.”

Az incidensek előrejelzése

A valószínűségszámítás tárgya a végtelen tömegjelenségek vizsgálata. Témánk szempontjából azt fontos feltárni, hogy egy adott „X” esemény, azaz információbiztonsági incidens bekövetkezésének mekkora a valószínűsége, valamint az esemény bekövetkezése milyen kapcsolatban van más információbiztonsági incidensekkel, valamint milyen hatásokat vált ki a közigazgatás informatikai hálózatában (azaz milyen kapcsolatban van a „Y” eseménnyel). Amennyiben elfogadjuk a definíciót, mely szerint „... a kockázat a bizonytalanság hatása a célokra”, az információbiztonsági rendszerek és folyamatok tervezésekor elsődleges helyet foglal el a bizonytalanság csökkentése.

Egy rendszer védelmének tervezésekor első lépés a követelmények rögzítése, melyet szorosan követ a védelmi mechanizmusok kialakítása. Széles körben elfogadott és használt védelem-tervezési módszer a PreDeCo elv, mely három egymásra épülő és egymást kiegészítő részre, kontrollra bontja a védelmet:

- *Preventív/Megelőző* kontroll: egy incidens bekövetkezési valószínűségét csökkentő intézkedések. Nem egyenlő a védelmi intézkedések számának irracionális fokozásával.
- *Detektív/Felismerő* kontroll: egy adott incidens bekövetkezését észlelő folyamat.
- *Korrektív/Elhárító* kontroll: egy adott incidens, rendellenes esemény megakadályozása, a károk kiküszöbölésének és a normál állapot visszaállításának céljából.

A fenti védelem-tervezési módszer kiegészíthető, s véleményem szerint kiegészítendő egy további elemmel, a korai előrejelzéssel (Early Warning System – EWS) (Apel és társai 2010), más néven predikcióval. Prediktív kontroll alatt értem a korábban) bekövetkezett biztonsági események elemzését; az események közötti összefüggések vizsgálatát, összefüggés-mintázatok feltárását; s ezen mintázatok alapján történő jövőbeli előrejelzéseket.⁷ Az előrejelző rendszer képes valós időben észlelni és elemezni az Interneten keresztül érkező támadások adatait. Az adatok feldolgozása során, az előre beállított riasztási szabályok szerint a rendszer jelentést készít, mely tartalmazza a biztonsági események kockázati szintjét, trendjét, valamint jelzi az átlagos trendektől való eltérést. Az előrejelző rendszer adatbázisaiban a nemzeti információbiztonsági szervezet által gyűjtött adatok, valamint nemzeti és nemzetközi állami és üzleti partner szervezetek adatai kerülnek raktározásra (erről az információcsere folyamatról ír részletesen Munk Sándor (2018) tanulmányában). Egy ilyen rendszer segítségével egy információbiztonsági esemény bekövetkezése előre „megjósolható” lenne, így a megvalósulás pillanatában lehetőség lenne az incidens forrásának

7 A közigazgatási szervezetek jogszabályi előírás alapján jelenleg is rendelkeznek éves kockázatelemeléssel és kockázatértékeléssel, gondoskodnak az elektronikus információs rendszer eseményeinek nyomon követhetőségéről, továbbá az információs rendszer biztonságáért felelős személy az elektronikus információs rendszert érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni kötelesek a kormányzati eseménykezelő központot (Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, korábban NKI GovCERT). 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 13–14. §.

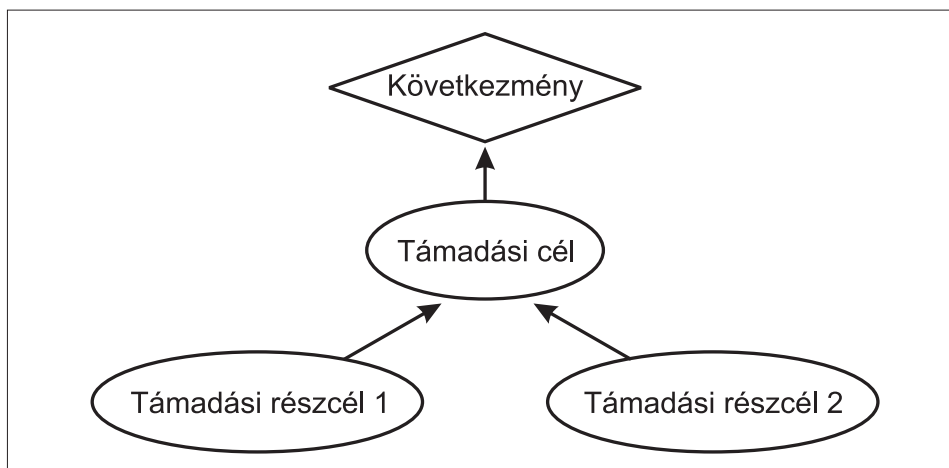
beazonosítására, valamint a károk azonnali elhárítására. De hogyan alakítható ki egy ilyen előrejelző rendszer?

A támadási és a védekezési fa modell

Ahhoz, hogy egy korai előrejelző rendszer fel tudja ismerni a különböző típusú támadásokat, szükség van azok egyedi jellemzőinek feltárására. Ebben nyújt segítséget a fenyegetés-elemzés, valamint annak eszközei: a támadási és a védekezési fa modellek.

A fenyegetés-elemzés egy módszer, mely során egy adott rendszer (lehet az szoftver, weboldal, vagy egy komplex szervezeti struktúra) felépítését vizsgáljuk abból a célból, hogy a lehetséges támadási felületeket, hibákat feltárjuk. A modellezés azt szolgálja, hogy az adott rendszert komplex módon, ne csupán részleteiben lássuk. Egy jó modell segítséget nyújt abban, a fenyegetések csoportosításában, továbbá a látszólag egymástól elkülönülő, de a valóságban összetartozó fenyegetések közötti kapcsolatok feltárásában.

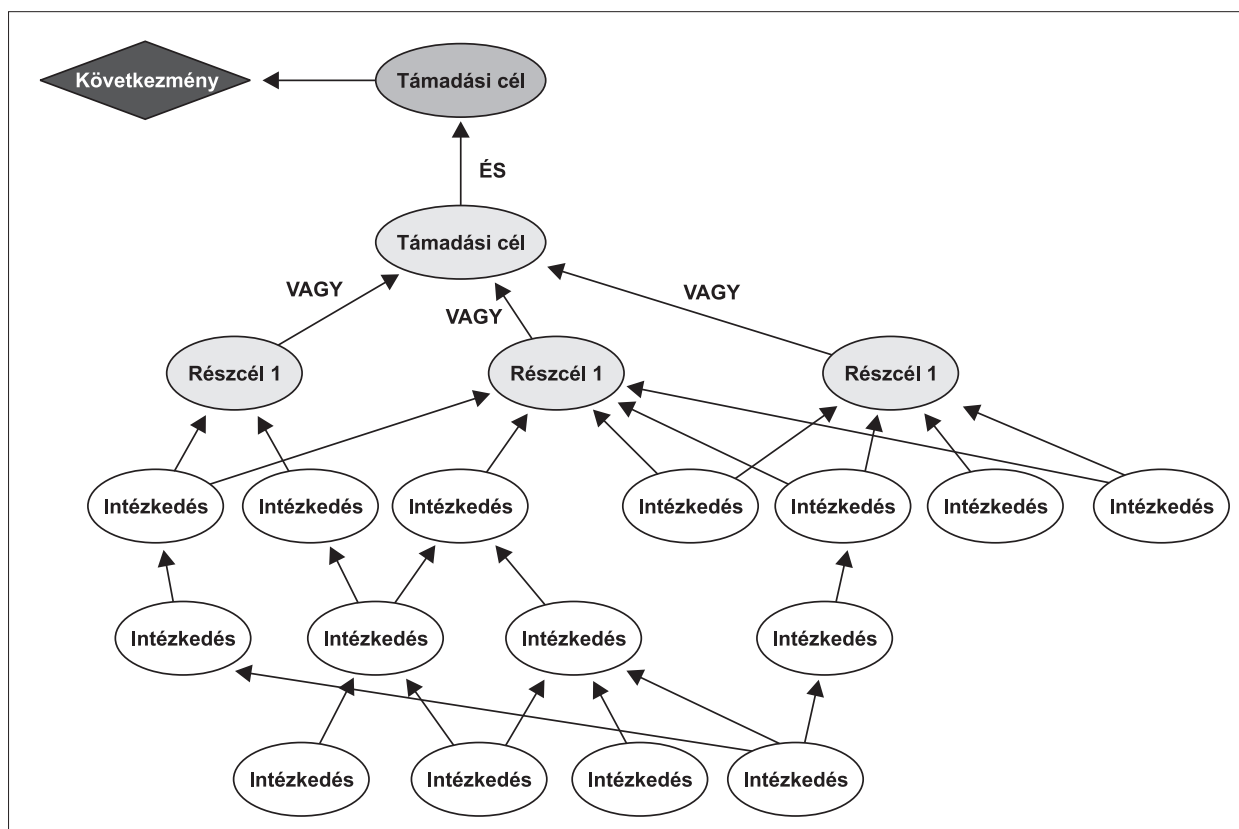
A támadási fák olyan gráfok, melyek megmutatják, hogy egy adott rendszerben a támadó milyen utak segítségével képes elérni célját. A fa-szerkezetű modell gyökerében a támadó konkrét célja áll, mely apró lépésekre, részcélokra kerül lebontásra, amíg egy végrehajtható támadáshoz nem jutunk. A részcélok egymással ÉS, illetve VAGY kapcsolatban állva vezetnek a cél eléréséhez. A támadási fa csúcspontjait a részcélok alkotják, melyekhez különböző értékek rendelhetők, mint például bekövetkezési valószínűség vagy a ráfordítás mértéke. Az egymásra épülő, egymással összefüggő részcélok összeköthetők, így ezek a kapcsolatok alkotják a gráf éleit, ahogyan az 1. ábrán látható. (Munk 2010)



1. ábra.
Támadási fa koncepció
(Saját szerkesztés)

Jóllehet, jellemzően nehéz előre kitalálni, hogy a támadók milyen lépéseket választanak, valamint milyen gyakorisággal próbálkoznak egy-egy biztonsági incidens végrehajtására, azok sikeressége a megfelelő ellenintézkedések alkalmazásával csökkenthető. Egy szándékos támadásnál a támadó fél célja, hogy a lehető legnagyobb

csapást mérje a hálózatra, így az megállíthatatlanul összeomlik, megsemmisül. Legegyszerűbben ezt úgy lehet megtenni, ha a támadó sorban eltávolítja az összekötőket. Ehhez ismernie kell a hálózat felépítését, valamint tudnia kell, hogyan támadható meg a kiemelkedő fontosságú csomópontok. Ugyanakkor logikus, ha a támadást részcélokra fel lehet osztani, akkor hasonlóképpen az elhárító tevékenység a részcélokhoz kapcsolódó ellenintézkedési akciókra bontható. Az ellenintézkedéseknek a támadási modellbe történő kapcsolása létrehozza a védekezési fa modellt, melyet a 2. ábra mutat be. (Sommetstad és társai 2009)



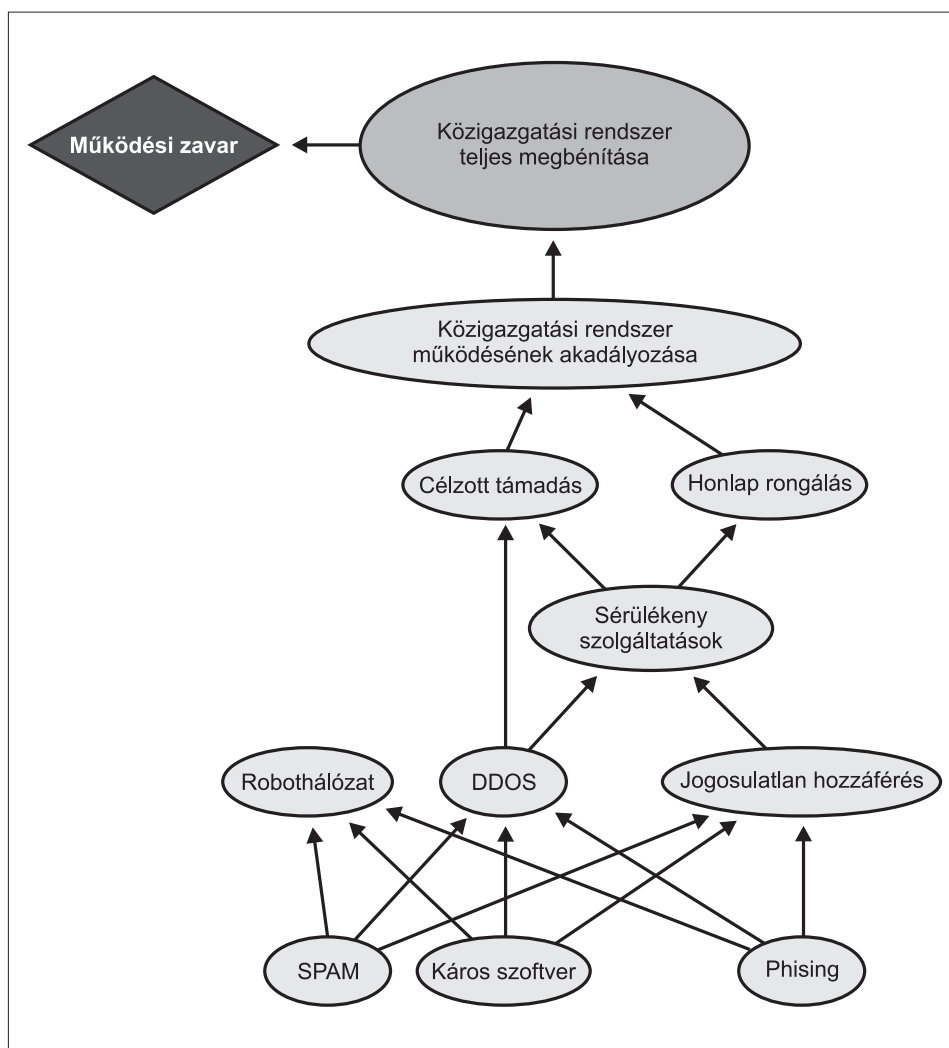
2. ábra.
Védekezési fa modell koncepciója
(Saját szerkesztés)

Feltételezésem szerint a közigazgatás szervezetrendszerét érő támadások valamilyen formában kapcsolatban állnak egymással. Ennélfogva adott incidens bekövetkezéséről következtetni lehet az azzal kapcsolatban álló incidens bekövetkezési idejére, az incidens volumenének mértékére. A rendelkezésre álló adatok alapján ennek a hipotézisnek a vizsgálatát végeztem el matematikai eszközökkel.

Ahogy a támadási fák, úgy a védekezési fák is gráfok. A védekezési fa modell koncepciójának felállítása után a kutatás célja az volt, hogy a rendelkezésre álló adatok alapján teszteljem annak működőképességét. Ehhez a valószínűségszámítás és statisztikai matematika módszereit alkalmaztam. A Bayes-hálózatok módszere megfelelő eszköz, mert alkalmas különböző fogalmak kombinálására és az értékelésekben lévő bizonytalanság kezelésére.

A Bayes-háló nem más, mint egy irányított gráf, melyben irányított élek egy halma összeköt bizonyos csomópontpárokat. A háló topológiája megadja a fennálló feltételes függetlenségi kapcsolatokat. Egy helyesen létrehozott hálóban az X csomópontot az Y csomóponttal összekötő nyíl tehát azt jelenti, hogy X-nek közvetlen befolyása van Y-ra.

A modell teszteléséhez első lépésben szükség van a használandó támadási-védekezési fa modell elkészítésére. A szakirodalom, az ismert támadási modellek, valamint korábbi incidensekről készült leírások alapján elkészítettem egy támadási fa modellt (szcenáriót), melyben a csomópontokat a vizsgált incidens típusok alkották (adathalászat, káros szoftver, robothálózat, kéretlen levél, túlterheléses támadás, jogosulatlan hozzáférés, sérülékeny szolgáltatások, célzott támadás, honlap rongálás). A támadó célja ebben a modellben a közigazgatási informatikai rendszer működésének ideiglenes, vagy akár tartós akadályozása (teljes hálózat megbénítása). A 3. ábra mutatja be, hogy az általam felvázolt támadási fa modellben hogyan kapcsolódnak egymáshoz a különböző biztonsági incidensek.



3. ábra.

A közigazgatási rendszer működésének megbénítását célzó támadási fa
(Saját szerkesztés)

Ebben a modellben természetesen a fenti forrásokat alapul véve, ugyanakkor szubjektív módon az általam feltételezett kapcsolatok kerültek felvázolásra. Ahhoz, hogy a már bekövetkezett incidensek alapján előre képesek legyünk megállapítani, hogy egy következő tetszőleges incidens (például káros szoftverek használata) bekövetkezése esetén mekkora valószínűséggel áll fenn egy másik incidens (például DDOS-támadás) bekövetkezésének az esélye, szükséges meggyőződni arról, hogy az incidensek (vagyis csomópontok) között valóban létezik kapcsolat.

A kapcsolatok feltérképezéséhez a korrelációelemzés módszerét használtam. Előzetes feltételezésem az volt, hogy a közigazgatást érő információbiztonsági incidensek között egyértelmű összefüggés van. A korreláció (r) két tetszőleges érték (A és B) közötti lineáris kapcsolat nagyságát és irányát mutatja meg. Erőteljes negatív korreláció ($R \approx -1$) és erőteljes pozitív korreláció ($0,7 \leq R$) vagy ($R \approx 1$) esetén a két érték között egyértelmű kapcsolat van, míg nincs kapcsolat, ha a korreláció értéke nulla, vagy ahhoz közelít ($R \approx 0$).

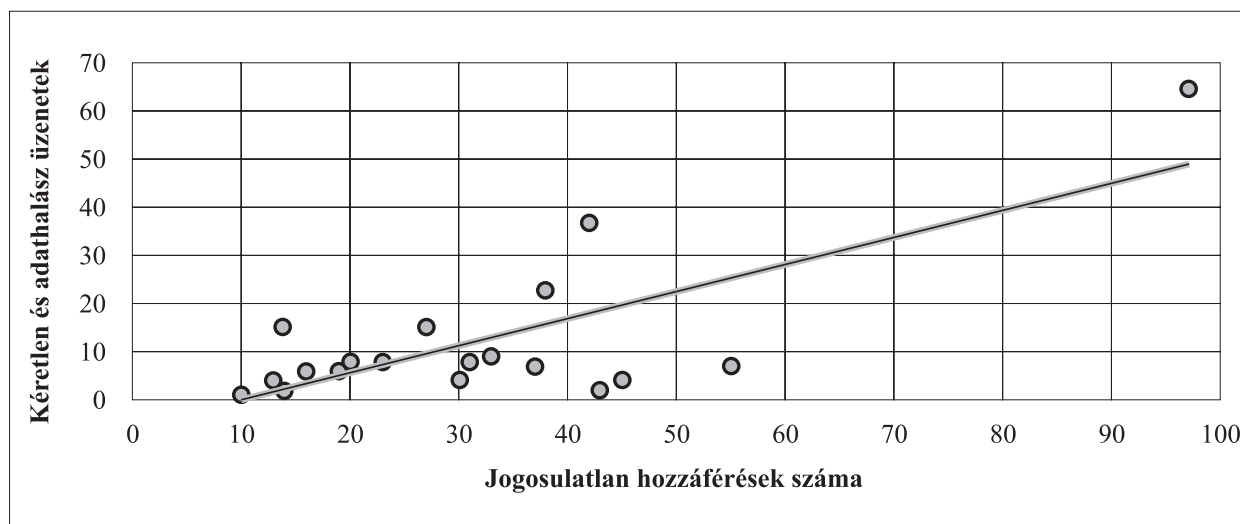
A rendelkezésemre álló statisztikai adatok vizsgálata során egy esetben sikerült egyértelműen pozitív összefüggést kimutatni a biztonsági események között. Az alábbi táblázat bemutatja az adathalász és spam üzenetek, valamint a jogosulatlan hozzáférések számának változását 2017. január 1. és 2018. augusztus 31. között.

1. táblázat.

**Kéretlen és adathalász levelek és a jogosulatlan hozzáférések száma
2017 január–2018 augusztus**

(Forrás: NBSZ, saját szerkesztés)

Időpont	Spam, phishing (darab)	Jogosulatlan hozzáférések (darab)
2017. január	13	4
2017. február	20	8
2017. március	23	8
2017. április	19	6
2017. május	33	9
2017. június	55	7
2017. július	14	15
2017. augusztus	31	8
2017. szeptember	14	2
2017. október	45	4
2017. november	43	2
2017. december	38	23
2018. január	42	37
2018. február	97	65
2018. március	37	7
2018. április	19	6
2018. május	16	6
2018. június	10	1
2018. július	27	15
2018. augusztus	30	4



4. ábra.

*Kéretlen és adathalász levelek és a jogosulatlan hozzáférések közötti korreláció
2017. január – 2018. augusztus közötti adatok alapján*

(Forrás: NBSZ, saját szerkesztés)

A korrelációs számítás eredménye szerint a spamek és adathalász üzenetek, valamint a jogosulatlan hozzáférések között a korreláció mértéke $R \approx 0,75$. Az alábbi diagrammon látható az összefüggés trendje, valamint az értékek szóródása.

Az incidensek között fennálló egyértelmű kapcsolat meglepte nem meglepő, hiszen a Nemzeti Kibervédelmi Intézet munkatársai rendszeresen kapnak értesítéseket megtévesztő levelekkel kapcsolatban, amelyek kártékony csatolmányt vagy kártékony kódra mutató hivatkozást tartalmaznak. Ezen megtévesztő levelek gyakran adott körbe tartozó intézményeket céloznak. A további csomópontpárok vizsgálata során azonban nem sikerült az incidensek közötti egyértelmű kapcsolat, összefüggés fennállását bizonyítani. Ez többek között az alábbi két fő okra vezethető vissza:

1. Egyrészt lehetséges, hogy a vizsgált időintervallum alatt az incidensekről gyűjtött adatbázis nem volt teljes. Ennek indoka, hogy:
 - 1.1. voltak olyan incidensek, amelyeket nem sikerült felismerni, vagy
 - 1.2. egyes incidensekről nem érkezett bejelentés a hatóság felé a közigazgatási szerv (vagy az adott szolgáltatás üzemeltetője) felől.
2. Másrészt lehetséges, hogy a kutatás során használt incidens-kategóriák túlságosan szélesek, szükségszerű lenne kisebb lépésekre bontani őket és ezen kisebb lépések alapján egy új támadási fa modellt készíteni. Ilyen kisebb lépések lehetnek például a jogosulatlan hozzáférés esetén: jelszó feltörése brute-force módszerrel, jelszó megszerzése sikeres social-engineering által, jelszó megszerzése adatszivárgás következtében nyilvánosságra jutott jelszó listából, logikai kontroll kikerülése (további példákért lásd Sommestad és társai 2009; Abraham&Nair 2015).

Úgy gondolom, hogy egy részletesebben kidolgozott támadási fa koncepció elkészítése nagyban hozzájárulna a rendelkezésre álló adatok pontosabb feldolgozásához, és az incidensek között feltételezett kapcsolatok létének bizonyításához. Amennyiben

az incidensek közötti kapcsolatok kimutathatóvá válnak, lehetőség nyílik az incidensek előrejelzésére használatos módszer részletes kidolgozására.

Ugyanakkor fontos megjegyezni, hogy a korreláció mértéke az incidensek közötti összefüggések elemzésének csak egy módszere. A korrelációs számítás a különböző események számosságán alapul, azonban figyelmen kívül hagyja azok hatását. Például, bár az adathalász üzenetek és a célzott támadások között a számadatok alapján igen gyenge a korreláció mértéke, csupán egy sikeres támadás is igen kritikus eredményekkel járhat a közigazgatás működésére nézve.

Következtetések

Az állam egészének biztonsága, így a közigazgatás alrendszerének offline és online térben történő háborítatlan működése kiemelkedő fontosságú terület. Napról, napra számtalan információbiztonsági incidens bekövetkezése fenyegeti a köz- és magánsektort egyaránt, ezért az információbiztonság jogi, szervezeti és technikai rendszerének fejlesztése nélkülözhetetlen feladat.

Dolgozatomban egy olyan modell elkészítésére kívántam javaslatot tenni, amely a korábban bekövetkezett biztonsági események vizsgálatával, valamint az események közötti összefüggések feltárásával képes valós időben észlelni és elemezni az érkező információbiztonsági incidensek adatait, megállapítani azok kockázati szintjét, trendjét. Egy ilyen rendszer segítségével egy információbiztonsági esemény bekövetkezése előre „megjósolható” lenne, így a megvalósulás pillanatában lehetőség lenne az incidens forrásának beazonosítására, valamint a károk azonnali elhárítására.

A modell elkészítéséhez a kutatás során a közigazgatás szervezetrendszerére ellen irányult, 2017. január 1. és 2018. augusztus 31. közötti időintervallumban bekövetkezett incidenseket vizsgáltam statisztikai és valószínűség számítási módszerek segítségével. Jelen kutatás során sor került a korai előrejelző rendszer elméleti modelljének felvázolására, valamint az incidensek közötti összefüggések vizsgálatára. Mivel a kutatás során felhasznált adatok egy meghatározott körre és időintervallumra vonatkoztak, így csak korlátozott eredmények születtek. Egyrészt az adatok a Nemzeti Kibervédelmi Intézet adatállományából kerültek felhasználásra, ez korlátozza a megállapítások általánosíthatóságát, ugyanakkor a kutatás központi megállapításai összhangban vannak korábbi, a jelent tanulmányban is idézett kutatásokkal.

Másodszor, csupán egy esetben sikerült erőteljes korrelációt kimutatni az incidensek között, ennek az oka, hogy az egyéb incidens típusok viszonylag alacsony számúak voltak. Egy kiterjedtebb adatkör nagy valószínűséggel az összefüggések között erőteljesebb korrelációt mutatna.

Harmadszor, a kutatás során minden egyes incidens típust egyenértékűként kezelttem, vagyis nem vettem figyelembe az incidensek hatásai közötti különbségeket (például az érintett számítógépek és/vagy hálózatok száma; a biztonsági és gazdasági intézkedésekre gyakorolt hatások, mint például az adatvesztés és az idő). Az incidens súlya és annak időzítése összefügghet. A közelmúltban végzett kutatások azt mutatják, hogy adatszivárgás, adatrekordok eltulajdonítása esetén a támadások között eltelt idő és a támadások súlyossága jelentősen összefügg egymással.

Negyedszer, a vizsgálat nem terjedt ki az egyes incidensekről szóló jelentések vizsgálatára (például az incidens észlelésének módjára, kártékony szoftverek esetén azok konkrét típusára) csupán az incidensek havi bontásban készült idősoros elemzésére. A részletes jelentések számos érzékeny információt tartalmaznak, hiszen feltárják, hogy a gyakorlatban hogyan működik a közigazgatási rendszerek információbiztonsági ellenőrzése és védelme. Bár jelen kutatás keretei között ezt nem tudtam megtenni, az összefüggések vizsgálatának alapjául szolgáló matematikai változók beépítése ezen rendszerekbe javíthatja az előrejelzés minőségét, és segítheti a konkrét támadások szempontjából releváns tényezők azonosítását is.

IRODALOM

- Abraham, Subil – Nair, Suku (2015): *Predictive Cyber-security Analytics Framework: A non-homogenous Markov model for Security Quantification*. Natarajan Meghanathan et al. (Eds): NeTCoM, CSIT, GRAPH-HOC, ŠPTM – 2014. pp. 195–209, 2014.
- Apel, Martin – Biskup, Joachim – Flegel, Ulrich – Meier, Michael (2010): *Towards Early Warning Systems – Challenges, Technologies and Architecture*. In: Rome E., Bloomfield R. (eds) *Critical Information Infrastructures Security*. CRITIS 2009. Lecture Notes in Computer Science, vol 6027. Springer, Berlin, Heidelberg.
- Beláz Annamária (2018): A digitális állam információbiztonsága: kockázatmenedzsment elvek megjelenése a stratégiai dokumentumokban. *Bánki Közlemények* 1(3), 56–60.
- Budai Balázs Benjámin (2009): *Az E-közigazgatás elmélete*. Budapest. Akadémiai Kiadó, 2009.
- Buzan, Barry – Weaver, Ole – De Wilde, Jaap (1998): *Security – A new framework for analysis*. Lynne Rienner Publishers.
- Csutak Zsolt (2018): Szép új világ, avagy a kibertér és a mesterséges intelligencia korának új kihívásai. *Felderítő Szemle*, 17(1), 170–186.
- Gábri Máté (2010): Biztonsági komplexumok az információs korban. *Hadmérnök*, V. évfolyam, 4. szám, pp. 110–121.
- Horváth Attila – Erdősi Péter Máté – Kiss Ferenc (2016): Az informatikai sérülékenységek gazdasági összefüggései. Budapest, *INFOTA* 2016. 109–135.
- Kerti András – Nyikes Zoltán (2015): Overview of Hungary Information Security. The Issues of the National Electronic Classified Material of Transmission. In: Szakál, A. (ed.) *10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI 2015)*, Budapest, Óbudai Egyetem, 2015. pp. 327–333.
- Lőrincz Lajos (2009): *A modern állam feladatai – kiemelten a közigazgatásban*. In Halm – Vadász (szerk.): *A modern állam feladatai*. Magyar Közgazdasági Társaság – Gazdasági és Szociális Tanács, Budapest.
- Michelberger Pál – Lábodi, Csaba (2012): *Vállalati információbiztonság szervezése*. In: Nagy Imre Zoltán (ed.): *Vállalkozásfejlesztés a XXI. században II*. Budapest, pp. 241–302.
- Munk Sándor (2010): A biztonság kérdéseinek dekompozíciója. *Hadmérnök*, V. évfolyam, 2. szám.
- Munk Sándor (2018): Kiberbiztonsági szervezetek közötti információcsere. *Hadmérnök*, 13. évfolyam, 4. szám.
- Pokorádi László (2016): Modellek a műszaki biztonság tudományban. *Gradus* Vol 3, No 2. pp. 92–100.
- Sasith M. Rajasooriya – Chris. P. Tsokos – Pubudu Kalpani Kaluarachchi (2017): Cyber Security: Nonlinear Stochastic Models for Predicting the Exploitability. *Journal of Information Security*, 8, pp. 125–140.
- Sommestad, Teodor – Ekstedt, Mathias – Johnson, Pontus (2009): *Cyber security risks assessment with bayesian defense graphs and architectural models*. In: 2009 42nd Hawaii International Conference on System Sciences. IEEE, 2009. pp. 1–10.