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 valószínûségszámítás és a statisztikai elemzés módszerei a biztonsági incidensek elõrejelzésében 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 védekezõ képességét.

Az információbiztonsági incidensek száma minden évre egyre nagyobb méreteket ölt, ezen incidensek egyre jelentõsebb anyagi károkat okoznak. Az incidensek alól a közigazgatás, a közszektor sem képez kivételt. „*A statisztikai adatok alapján a 2017-es év elsõ felében globálisan közel kétmilliárd adatrekord került illetéktelen eltulajdonításra, milliós károkat okozva ezzel a köz- és magánszektornak egyaránt. Az eltulajdonított adatok huszonegy százaléka (404.244.346 adatrekord) a közszektorból származik.*[2] *Az illegális adatszerzés mellett számos más típusú információbiztonsági támadásnak vannak kitéve a közszféra 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 gyakornoki 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 mûködést biztosítani... a milliárdnyi okoseszköz számára egy olyan fékezhetetlenül fejlõdõ, számítógépek uralta világban, ahol a webalapú bûncselekmények és visszaélések száma 2015-ben az Amerikai Egyesült Államokban és az Egyesült Királyságban már letaszította trónjáról a szervezett bûnözést és a kábítószer-kereskedelmet?"*

Annak érdekében, hogy a közigazgatási rendszer hosszú távon mûködõképes maradjon, valamint a rendszerekben elõállított, tárolt, feldolgozott és továbbított adatok védelme biztosított legyen, az államnak kiemelkedõ 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, elõrejelzõ funkciók.

A közigazgatás szervezetrendszerének és infrastruktúrájának védelme különösképpen 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 alapvetõ 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 alapvetõ funkció nem tûnik el, hanem folyamatosan kiegészül és differenciálódik.[3] Vitathatatlan, hogy a közigazgatás, valamint az azt támogató infrastruktúra védelme kiemelkedõen 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, fenyegetésektõl mentes állapot. Ugyanakkor el kell ismernünk, hogy ez a meghatározás meglehetõsen felszínes, hiszen a biztonság fogalmához számos elmélet és eltérõ tudományos megközelítés kapcsolódik. A biztonság körülírására szolgáló meghatározások vizsgálatát követõen Gábri Máté (2010, 112.) tanulmányában a következõ 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. Elõbbi a tradicionális vonulatra, míg az utóbbi az újszerû gondolkodásra jellemzõ. 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 újszerû 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 kibertérbõl érkezõ információbiztonsági fenyegetések folyamatosan jelen vannak, azaz léteznek, de az állam a biztonsági feladatának ellátása keretében képes a biztonsági események ellen való védekezésre, továbbá a meglevõ képességek fejlesztésére törekszik.

3 A feladatrendszer ezen változásának történeti áttekintését Lõrincz Lajos akadémikus foglalja össze tanulmányában. (Lõrincz 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 kifejtésétõl 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 kerülõ elemek hatására. A közigazgatási rendszerek információbiztonsági intézkedési stratégiájának, akciótervének elkészítéséhez a statisztikai modellezés és a valószínûségszámítás módszertana alapot szolgáltathat, függetlenül a biztonsági veszély forrásától és kiterjedésétõl. Az általam felvázolt modell elõnye, hogy független a szervezetrendszer méretétõl, ennél fogva a megoldás a rendelkezésre álló adatok alapján ugyanolyan hatékonysággal alkalmazható egyetlen szervezet vizsgálatára, valamint az egész országra kiterjedõ közigazgatási szervezetrendszerre is.

A tanulmány következõ részében, a figyelem fókuszában az a kérdés áll, hogy milyen a közigazgatás mûködését veszélyeztetõ biztonsági fenyegetések vannak és mely biztonságtechnikai, szervezetirányítási megoldások segítenek ezek elhárításában.

A közigazgatás információbiztonságának védelme

A közigazgatás számára kiemelkedõen fontos feladat a biztonság garantálása az offline és az online életben egyaránt. A közigazgatási feladatok folyamatosan változnak, sõt a feladatok skálája növekszik,[4] azonban a feladatok mennyiségi változásán túl, a tudományos diskurzus során kiemelkedõk 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 címû mûvében kifejti, hogy a szolgáltató állam, szemben a korábbi modellekkel (pl. éjjeliõr állam, jóléti állam), alapvetõen proaktív, az ügyfél elvárásainak megfelelõ, 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 összefüggõ ismérvet állapított meg, melyek a következõk:

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

4 Berényi Sándor meglátása szerint a közigazgatás alapvetõen vagy döntést hoz, vagy elõkészíti mások döntéseit. Ezzel szemben Magyary Zoltán az állami feladatok komplex megközelítését írta le, kiemelkedõ feladatként azonosította a következõket: községi szervezet biztosítása, közlekedés biztosítása, foglalkoztatás, társadalombiztosítás, gazdasági élet irányítása, alapvetõ 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: Magyary: A magyar közigazgatás, 1942)

A közigazgatást érõ elsõsorban információbiztonsági kihívásokkal kapcsolatban a legfontosabb ismérvek a szolgáltató állam mûködési 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 kiegészítõ tevékenységek (non-core) fejlesztése miatt. Ez a fajta hozzáállás egy látszólag jól mûködõ, de a valóságban instabil szervezet, rendszer kiépítéséhez vezet. A gyakorlatban ez azt jelenti, hogy a közigazgatási szervezetek kitettsége az információbiztonsági incidenseknek növekszik, mivel az alapvetõ (ugyanakkor idõigényes és költséges) folyamat, az információbiztonság fejlesztésének jelentõsége 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 következõképpen írja le a biztonsági esemény fogalmát: *„… nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezõtlen változást vagy egy elõzõleg ismeretlen helyzetet idéz elõ, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, 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 szorulását a honlap-rongálás (defacement) eklatáns példáján keresztül lehet bemutatni. A kutatás által vizsgált idõtartam (2017. január 1. – 2018. augusztus 31.) alatt 361 alkalommal került sor állami, közigazgatási honlapok rongálásával összefüggõ incidensekre. A Nemzeti Kibervédelmi Intézet munkatársai az ellenõrzések keretében számos validációs hibát tártak fel. A kritikus találatok alapján elmondható, hogy az alkalmazásfejlesztõk fõként a mûködésre koncentrálnak munkájuk során, a biztonságos szoftverfejlesztés területén még kihívásokkal küzdenek. Egy defacement incidens esetén a hibajavítási munkák több napon át is eltarthatnak, de az idõ 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 – Erdõsi – Kiss 2016, 114.), *„… ez gyakran különbözõ 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 növelõ 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 mérhetõ, követhetõ végrehajtása. Másrészrõl azonban elengedhetetlen, hogy a stratégia végrehajtói, a vezetõk jó döntéseket hozzanak, minimalizálva a kudarc lehetõségét. Ezzel összefüggésben a közigazgatás, mint szervezetrendszer sikere az információbiztonság területén függ az információbiztonsági kockázatok egyértelmû felmérésére, kezelésére létrehozott szabályzatok, valamint az azokhoz kapcsolódó eljárások minõségétõl. (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 címû szabvány tartalmazza a kockázatmenedzsment[6] alapelveit, valamint a kockázatfelmérés, kockázatértékelés és kockázatkezelés lépéseit. A szabványban felsorolt alapelvek közül a témánk szempontjából az alábbi négy alapelvet tartom kiemelkedõen fontosnak. Ezek a következõk:

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 történõ megfogalmazása.
3. A kockázatmenedzsment az elérhetõ *legpontosabb tényeken, információkon alapul*, többek között: korábbi adatok, tapasztalat, érdekelt felek visszajelzései, megfigyelései, elõrejelzései és szakértõi vélemények.
4. A kockázatmenedzsment *szervezetre szabott*, igazodik az egyéni igényekhez. A szervezet külsõ és belsõ környezetével, valamit 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 valószínûségszámítás és a statisztikai elemzés területére, mely területek az incidens elõrejelzési modell alapjául szolgálnak.

5 ISO 31000-es szabványcsoport, magyar nyelvû 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 elõrejelzése

A valószínûségszámítás tárgya a végtelen tömegjelenségek vizsgálata. Témánk szempontjából azt fontos feltárni, hogy egy adott „X" esemény, azaz információbiztonsági incidens bekövetkezésének mekkora a valószínûsége, 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 elsõdleges helyet foglal el a bizonytalanság csökkentése.*

Egy rendszer védelmének tervezésekor elsõ 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 épülõ és egymást kiegészítõ részre, kontrollra bontja a védelmet:

- *Preventív*/Megelõzõ kontroll: egy incidens bekövetkezési valószínûségét csökkentõ intézkedések. Nem egyenlõ a védelmi intézkedések számának irracionális fokozásával.
- *Detektív*/Felismerõ kontroll: egy adott incidens bekövetkezését észlelõ folyamat.
- *Korrektív*/Elhárító kontroll: egy adott incidens, rendellenes esemény megakadályozása, a károk kiküszöbölésének és a normál állapot visszaállításának céljából.

A fenti védelem-tervezési módszer kiegészíthetõ, s véleményem szerint kiegészítendõ egy további elemmel, a korai elõrejelzéssel (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 történõ jövõbeli elõrejelzéseket.[7] Az elõrejelzõ rendszer képes valós idõben észlelni és elemezni az Interneten keresztül érkezõ támadások adatait. Az adatok feldolgozása során, az elõre beállított riasztási szabályok szerint a rendszer jelentést készít, mely tartalmazza a biztonsági események kockázati szintjét, trendjét, valamint jelzi az átlagos trendektõl való eltérést. Az elõrejelzõ rendszer adatbázisaiban a nemzeti információbiztonsági szervezet által gyûjtött adatok, valamint nemzeti és nemzetközi állami és üzleti partner szervezetek adatai kerülnek raktározásra (errõl az információcsere folyamatról ír részletesen Munk Sándor (2018) tanulmányában). Egy ilyen rendszer segítségével egy információbiztonsági esemény bekövetkezése elõre „megjósolható" lenne, így a megvalósulás pillanatában lehetõség lenne az incidens forrásának

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

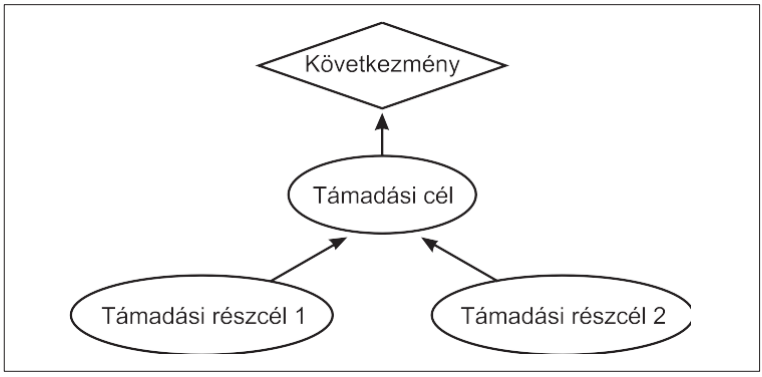
beazonosítására, valamint a károk azonnali elhárítására. De hogyan alakítható ki egy ilyen elõrejelzõ rendszer?

A támadási és a védekezési fa modell

Ahhoz, hogy egy korai elõrejelzõ rendszer fel tudja ismerni a különbözõ típusú támadásokat, szükség van azok egyedi jellemzõinek 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 elkülönülõ, de a valóságban összetartozó fenyegetések közötti kapcsolatok feltárásában.

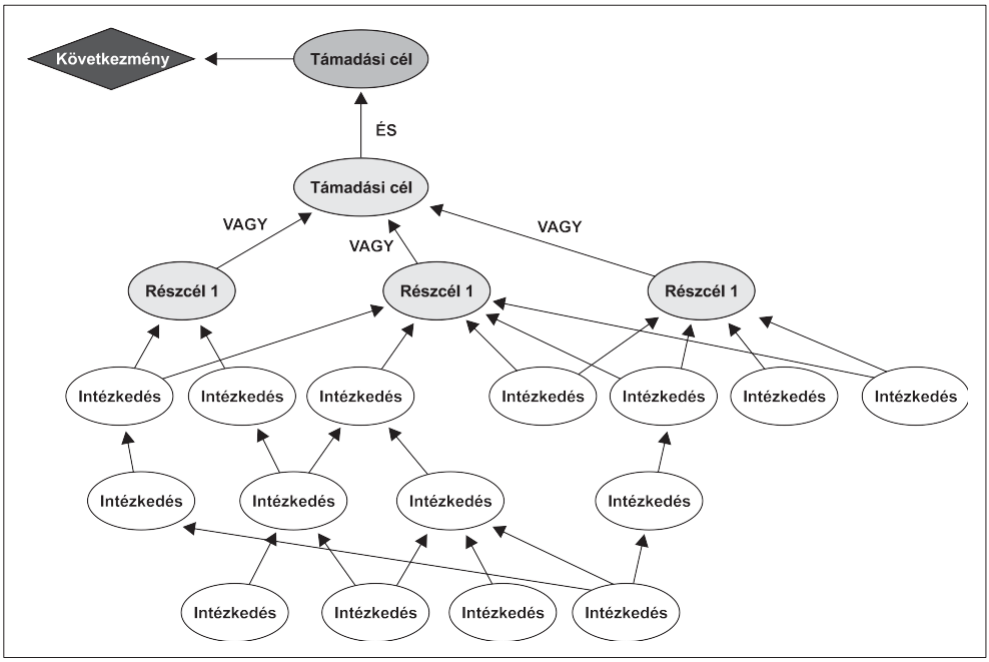
A támadási fák olyan gráfok, melyek megmutatják, hogy egy adott rendszerben a támadó milyen utak segítségével képes elérni célját. A fa-szerkezetû modell gyökerében a támadó konkrét célja áll, mely apró lépésekre, részcélokra kerül lebontásra, amíg egy végrehajtható támadáshoz nem jutunk. A részcélok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



1. ábra.
Támadási fa koncepció
(Saját szerkesztés)

Jóllehet, jellemzõen nehéz elõre kitalálni, hogy a támadók milyen lépéseket választanak, valamint milyen gyakorisággal próbálkoznak egy-egy biztonsági incidens végrehajtására, azok sikeressége a megfelelõ ellenintézkedések alkalmazásával csökkenthetõ. Egy szándékos támadásnál a támadó fél célja, hogy a lehetõ legnagyobb

csapást mérje a hálózatra, így az megállíthatatlanul összeomlik, megsemmisül. Legegyszerûbben ezt úgy lehet megtenni, ha a támadó sorban eltávolítja az összekötõket. Ehhez ismernie kell a hálózat felépítését, valamint tudnia kell, hogyan támadhatók meg a kiemelkedõ 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 történõ kapcsolása létrehozza a védekezési fa modellt, melyet a 2. ábra mutat be. (Sommestad és társai 2009)



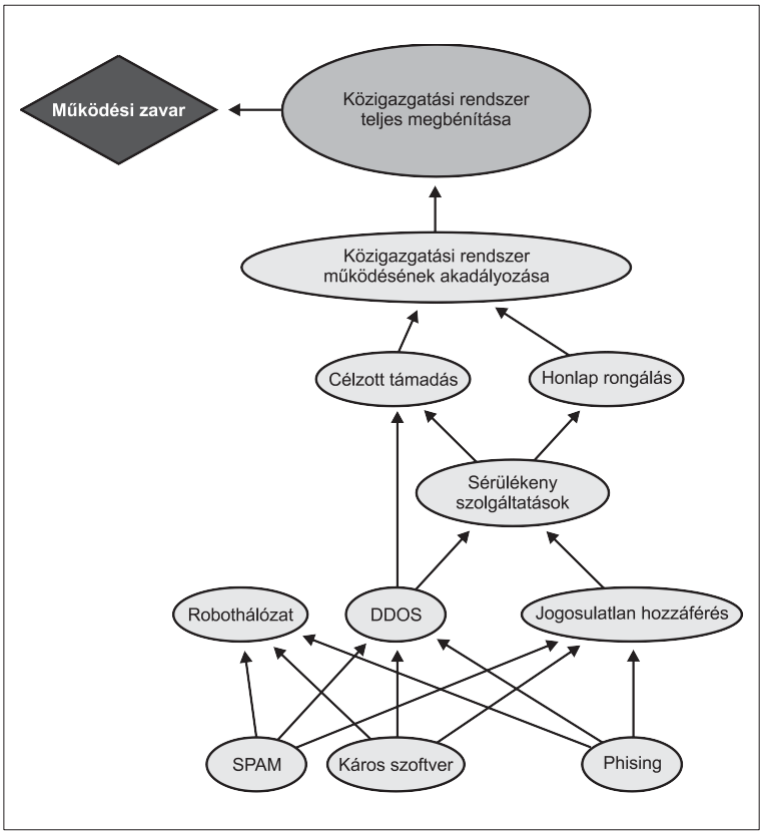
2. ábra.
Védekezési fa modell koncepciója
(Saját szerkesztés)

Feltételezésem szerint a közigazgatás szervezetrendszerét érõ támadások valamilyen formában kapcsolatban állnak egymással. Ennélfogva adott incidens bekövetkezésérõl 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.

Ahogyan 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 mûködõképességét. Ehhez a valószínûségszámítás és statisztikai matematika módszereit alkalmaztam. A Bayes-hálózatok módszere megfelelõ eszköz, mert alkalmas különbözõ fogalmak kombinálására és az értékelésekben lévõ bizonytalanság kezelésére.

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

A modell teszteléséhez elsõ lépésben szükség van a használandó támadási–védekezési fa modell elkészítésére. A szakirodalom, az ismert támadási modellek, valamint korábbi incidensekrõl 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 mûködésének ideiglenes, vagy akár tartós akadályozása (teljes hálózat megbénítása). A 3. ábra mutatja be, hogy az általam felvázolt támadási fa modellben hogyan kapcsolódnak egymáshoz a különbözõ biztonsági incidensek.



3. ábra.
A közigazgatási rendszer mûködésének 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 elõre képesek legyünk megállapítani, hogy egy következõ tetszõleges incidens (például káros szoftverek használata) bekövetkezése esetén mekkora valószínûséggel áll fenn egy másik incidens (például DDOS-támadás) bekövetkezésének az esélye, szükséges meggyõzõdni arról, hogy az incidensek (vagyis csomópontok) között valóban létezik kapcsolat.

A kapcsolatok feltérképezéséhez a korrelációelemzés módszerét használtam. Elõzetes feltételezésem az volt, hogy a közigazgatást érõ információbiztonsági incidensek között egyértelmû összefüggés van. A korreláció (r) két tetszõleges érték (*A* és *B*) közötti lineáris kapcsolat nagyságát és irányát mutatja meg. Erõteljes negatív korreláció ($R \to -1$) és erõteljes pozitív korreláció ($0{,}7 < R$) *vagy* ($R \to 1$) esetén a két érték kö- zött egyértelmû kapcsolat van, míg nincs kapcsolat, ha a korreláció értéke nulla, vagy ahhoz közelít ($R \to 0$).

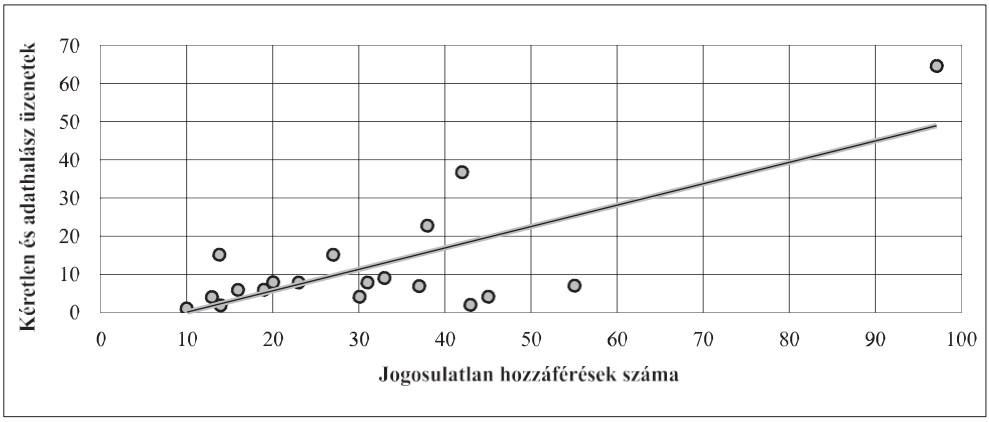
A rendelkezésemre álló statisztikai adatok vizsgálata során egy esetben sikerült egyértelmûen pozitív összefüggést kimutatni a biztonsági események között. Az alábbi táblázat bemutatja az adathalász és spam üzenetek, valamint a jogosulatlan hozzáférések számának változását 2017. január 1. és 2018. augusztus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

1. táblázat.

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

(Forrás: NBSZ, saját szerkesztés)

Idõpont	Spam, phising (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 korrelációszámítás eredménye szerint a spamek és adathalász üzenetek, valamint a jogosulatlan hozzáférések között a korreláció mértéke $R \approx 0{,}75$. Az alábbi dia- grammon látható az összefüggés trendje, valamint az értékek szóródása.

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

1. Egyrészt lehetséges, hogy a vizsgált idõintervallum alatt az incidensekrõl gyûjtött adatbázis nem volt teljes. Ennek indoka, hogy:
   1.1. voltak olyan incidensek, amelyeket nem sikerült felismerni, vagy
   1.2. egyes incidensekrõl nem érkezett bejelentés a hatóság felé a közigazgatási szerv (vagy az adott szolgáltatás üzemeltetõje) felõl.
2. Másrészt lehetséges, hogy a kutatás során használt incidens-kategóriák túlságosan szélesek, szükségszerû lenne kisebb lépésekre bontani õket 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, lehetõség nyílik az incidensek elõrejelzésére használatos módszer részletes kidolgozására.

Ugyanakkor fontos megjegyezni, hogy a korreláció mértéke az incidensek közötti összefüggések elemzésének csak egy módszere. A korrelációszámítás a különbözõ 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 mûködésére nézve.

Következtetések

Az állam egészének biztonsága, így a közigazgatás alrendszerének offline és online térben történõ háborítatlan mûködése kiemelkedõ fontosságú terület. Napról, napra számtalan információbiztonsági incidens bekövetkezése fenyegeti a köz- és magánszektort 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 idõben észlelni és elemezni az érkezõ információbiztonsági incidensek adatait, megállapítani azok kockázati szintjét, trendjét. Egy ilyen rendszer segítségével egy információbiztonsági esemény bekövetkezése elõre „megjósolható" lenne, így a megvalósulás pillanatában lehetõség lenne az incidens forrásának beazonosítására, valamint a károk azonnali elhárítására.

A modell elkészítéséhez a kutatás során a közigazgatás szervezetrendszere ellen irányult, 2017. január 1. és 2018. augusztus 31. közötti idõintervallumban bekövetkezett incidenseket vizsgáltamstatisztikai és valószínûségszámítási módszerek segítségével. Jelen kutatás során sor került a korai elõrejelzõ rendszer elméleti modelljének felvázolására, valamint az incidensek közötti összefüggések vizsgálatára. Mivel a kutatás során felhasznált adatok egy meghatározott körre és idõintervallumra vonatkoztak, így csak korlátozott eredmények születtek. Egyrészrõl 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 erõteljes korrelációt kimutatni az incidensek között, ennek az oka, hogy az egyéb incidens típusok viszonylag alacsony számúak voltak. Egy kiterjedtebb adatkör nagy valószínûséggel az összefüggések között erõteljesebb korrelációt mutatna.

Harmadszor, a kutatás során minden egyes incidens típust egyenértékûként kezeltem, 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 idõ). Az incidens súlya és annak idõzítése összefügghet. A közelmúltban végzett kutatások azt mutatják, hogy adatszivárgás, adatrekordok eltulajdonítása esetén a támadások között eltelt idõ és a támadások súlyossága jelentõsen összefügg egymással.

Negyedszer, a vizsgálat nem terjedt ki az egyes incidensekrõl szóló jelentések vizsgálatára (például az incidens észlelésének módjára, kártékony szoftverek esetén azok konkrét típusára) csupán az incidensek havi bontásban készült idõsoros elem- zésére. A részletes jelentések számos érzékeny információt tartalmaznak, hiszen fel- tárják, hogy a gyakorlatban hogyan mûködik a közigazgatási rendszerek információ- biztonsági ellenõrzése és védelme. Bár jelen kutatás keretei között ezt nem tudtam megtenni, az összefüggések vizsgálatának alapjául szolgáló matematikai változók beépítése ezen rendszerekbe javíthatja az elõrejelzés minõségét, és segítheti a konk- rét támadások szempontjából releváns tényezõk 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, SPTM – 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. *Felderítõ Szemle*, 17(1), 170–186.

Gábri Máté (2010): Biztonsági komplexumok az információs korban. *Hadmérnök,* V. évfolyam, 4. szám, pp. 110–121.

Horváth Attila – Erdõsi Péter Máté – Kiss Ferenc (2016): Az informatikai sérülékenységek gazdasági össze- függései. 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.

Lõrincz 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 információbiztons*ág 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 mûszaki biztonságtudományban. *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.