Rosszindulatú számítógépes fertőződés vizsgálatának lehetséges kérdései és indokai a közigazgatásban

Dr. Horváth Attila

Vezető kutató
Információs Társadalomért Alapítvány
e-mail: horvath.attila@infota.org

Erdősi Péter Máté

PhD hallgató
Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola
e-mail: erdosi.peter.kdi@office.uni-nke.hu

Absztrakt

A közigazgatás számítógépesedésével, az elektronikus információs rendszerek térnyerésével megjelentek a biztonságuk ellen ható informatikai tényezők is, melyek a papír alapú közigazgatásban ismeretlenek voltak. Az e-közigazgatás és a közigazgatási informatika mellett azonban ma már nincsenek reális – ugyanilyen hatékonysággal és eredményességgel működő – alternatívák, a közigazgatással szemben támasztott elvárásokat csak magas szintű számítógépesítéssel és információ-feldolgozással lehetséges teljesíteni. Az informatika-függőség felveti az eredményesség elérését célzó fejlesztési, innovációs kérdések vizsgálata mellett a rosszindulatú károkozó programok hatásának vizsgálatát is. A kérdések feltevéséhez érdemes megvizsgálni a potenciális terjedési mechanizmusokat és szinteket, illetőleg a jelenlegi és a jövőbeli trendek, technológiák sem hagyhatók figyelmen kívül egy proaktív megközelítésnél. A cikk célja olyan kérdésekre ráirányítani a figyelmet, melyek megválaszolásával az elektronikus közszolgáltatások biztonsága fenntartható és tovább növelhető.

Kulcsszavak: *e-közigazgatás, informatikai biztonság, rosszindulatú programok, fertőződés, vizsgálat*

Bevezetés

A közigazgatás számítógépesedésével, az elektronikus információs rendszerek térnyerésével megjelentek a biztonságuk ellen ható informatikai tényezők is, melyek a papír alapú közigazgatásban ismeretlenek voltak. Az e-közigazgatás mellett azonban ma már nincsenek reális – ugyanilyen hatékonysággal és eredményességgel működő – alternatívák, a közigazgatással szemben támasztott elvárásokat csak magas szintű számítógépesítéssel és

információ-feldolgozással lehetséges teljesíteni. Nem véletlenül jelent meg a közigazgatási informatika fogalma és készült el 2009-ben az e-közigazgatás elméletéről szóló könyv is, melynek második kiadása 2014-ben készült el [2], már öt évvel az első kiadást követően. Az informatika-függőség felveti az eredményesség elérését célzó fejlesztési, innovációs kérdések vizsgálata mellett a rosszindulatú károkozó programok hatásának vizsgálatát is, annak eldöntési igénye nélkül, hogy ez rossz vagy jó. Neumann János szavaival élve annyit lehetséges mondani, nem valamilyen különleges felfedezés különlegesen romboló mivolta okozza a veszélyt, mert a technikai hatékonyság kétarcú vívmány, aminek a veszélye a lényegéből fakad. A technikai rendszerek ugyanakkor hallatlan életerőt rejtenek magukban, így a visszaszorításukra irányuló tanácsok már Neumann János idejében sem látszottak elfogadhatónak [22].

Az informatika-függés azonnal feltételezi az energia-függést is, hiszen a szilícium-alapú számítástechnikai eszközök állandó működéséhez folyamatos külső energia-betáplálás szükséges (az állandó saját energiaforrás kifejlesztéséig). A magyar közigazgatás számára ez nem túl jó hír, és előbb vagy utóbb – de inkább előbb – szorosan összekapcsolódik a villamosenergia-ellátó rendszerek állapotával is (mivel a szünetmentes áramforrások egy idő után kimerülnek és a generátorok üzemanyag-ellátási lánca is megszakadhat). A magyar villamosenergia-ellátó rendszer állapotáról Bárdosi Zoltán így írt 2009-es cikkében [1]:

„A villamosenergia-piaci kereskedelem révén a határkeresztező szállítások mennyisége és távolsága megnőtt; továbbá, a pontosan előre nem jelezhető, időszakosan működő villamos energiatermelés (szélerőmű, kiserőművek) gyors térhódítása figyelhető meg. Ezek az Európát átszelő, egyre növekvő nagyságú áramlásokat idéznek elő, melyeket a rendszer kezdeti tervezésénél nem vettek figyelembe. A megváltozott körülmények miatt a rendszert a biztonsági határokhoz közel üzemeltetik, ami miatt a napi hálózatüzemeltetés sokkal kihívóbb feladattá vált."

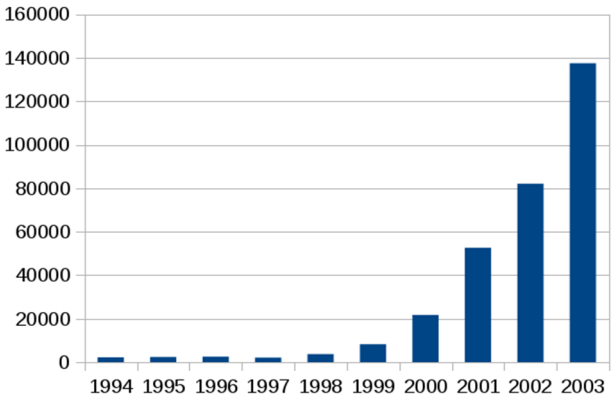
A villamosenergia-ellátó rendszer biztonsági határokhoz közelebbi üzemeltetése miatt az incidensek valószínűsége természetes következményként megnövekszik, mivel kisebb lehetőségei vannak a rendszernek a jövőbeli kiugró helyzetek elviselésére. Az energia-ellátásnak a számítógépes biztonsághoz való kapcsolódását egyébként a SCADA[1] rendszerek teremtik meg, amelyekkel az energia-ellátási folyamatokat vezérlik. Ennek távoli (logikai) támadásával közvetlenül lehet hatást gyakorolni az energia-ellátó rendszerekre az informatikai rendszereken keresztül, a vezetékek és elosztóközpontok (fizikai) támadásán túl, ahogyan erre Kovács László és Krasznay Csaba is rávilágított 2010-

[1] SCADA: Supervisory Control And Data Aquisition, felügyeleti ellenőrző és adatbegyűjtő számítógép által vezérelt/felügyelt ipari vezérlő rendszer

es elhíresült tanulmányukban (Digitális Mohács) [15]. Az üzemeltetési szempontok a szakértelem centralizálódásával együtt szükségessé tették az irányítási rendszerek távoli elérhetőségének biztosítását, aminek legegyszerűbb és legkézenfekvőbb módja az internetes védett kapcsolódás kialakítása – de ez újabb veszélyforrásokat teremtett a rendszer számára és ezzel ez a terület is összekapcsolódott az internetes fenyegetésekkel.

Fenyegetés, malware, botnet

Az interneten a mindennapos szolgáltatások (böngészés, web2 alkalmazások, e-mail, csevegő szobák, közösségi oldalak, játékok stb.) mellett folyamatosan jelen vannak a rosszindulatú támadások is. Kezdetben a CERT közzétette a bejelentett incidensek számát (mely 1997-2003 között exponenciális növekedést mutatott) [4], amit a következő ábra szemléltet.



1. ábra: CERT incidensek száma 1994-2003 között

A CERT egy idő után abbahagyta az incidensek számának mérését és közzétételét azzal az indoklással, hogy az incidensek számának növekedése már nem jelent hozzáadott értéket, gyakorlatilag majdnem mindegy, hogy 100e, 1, 10 vagy 100 M incidens következik-e be egy adott hónapban. Ezzel implicit módon ekkor kimondták azt, hogy a fenyegetettség folyamatos, a sérülékenységek kihasználására nap mint nap számtalan próbálkozás történik az internetes világban. Más szóval a 2010-es évektől kezdődően elérkeztünk a folyamatos fenyegetettség korszakába, ahogyan ezt Gyebrovszky Tamás 2014-es cikkében is olvashatjuk [8], az Advanced Persistent Threat (APT) – Folyamatosan Fennálló Fejlett Fenyegetés (4F) Gyebrovszky szerinti definíciójával együtt:

„Informatikai rendszerekbe észrevétlenül, célzott módon, adatszerzés és/vagy rombolás céljából bejuttatott különleges képességű folyamatok, melyek külső kapcsolat segítségével,

távolról kiadott vezérlőparancsok végrehajtásával folyamatosan működve fejtik ki jogszerűtlen tevékenységüket."

A témakör definícióinak egyeztetése és konszenzuson nyugvó használata alapvető fontosságú az eredmények széles körben való elterjedéséhez, hiszen a sokrétűség fogalomzavarhoz és meg nem értéshez vezethet, sőt, talán már vezetett is, amint ezt Bukovics István és Vavrik Antal is megjegyzi [3]:

„Túl sok ember használ túl sok rosszul definiált kifejezést ahhoz, hogy úgy a hazai, mint nemzetközi biztonsági szakemberek közösségével megfelelően kommunikálni tudjon."

Figyelemre méltó – és Neumann Jánosnak a kétarcú technikai veszélyekről szóló véleményét támasztja alá Gyebrovszkynak az a megállapítása, hogy 2003-ban felfedeztek egy olyan féreg kódot (Welchia [Nachi]), mely a rosszindulatú és nagy károkat okozó Blaster féreg által kihasznált sérülékenységet javította, a Blaster férget törölte, majd önmagát is megsemmisítette. Vagyis ezzel bebizonyosodott, hogy lehetséges a féreg terjedési mechanizmusát a féreg irtására felhasználni, természetesen megfelelő óvintézkedéssel (önmegsemmisítés).

A folyamatos fenyegetettség vizualizálására több honlap is vállalkozott (pl. [6], [23]), és az aktuális adatok ábrázolásával – éppen folyó támadások adatainak megjelenítésével – mutatja be azt, hogy a világhálón minden pillanatban realizálódik valamilyen támadás. Ma már minden pillanatban lehetséges támadás bekövetkezése az internetre csatlakozott csomópontok esetében.

A kezdeti boot-vírusok és a mostani APT-fenyegetések között jelentős technológiai evolúció, lényeges fejlődés fedezhető fel, ami rávilágít az informatika egyik problémájára, mégpedig arra, hogy a fenyegetések technológiája is fejlődik. A kvantum-számítógép fogalmának megjelenését követően magától értetődő módon vetődik fel a kérdés, hogy vajon kvantum-számítógépre írt vírus létezhet-e elméletileg? Erre ad egy nem túl megnyugtató, de nem is meglepő választ Lian-Ao Wu és Daniel A. Lidar 2006-os cikke [18], mely szerint semmilyen nehézségbe nem ütközik kvantum-malware[2] létrehozása, teljes mértékben elképzelhető, hogy ilyen malware továbbítódhat egy kvantum információs hálózaton, tárolódik egy vagy több kvantum hálózati csomóponton és ott (valószínűségi) programokat futtathat. A szerzők szerint bármelyik esemény bekövetkezése katasztrofális következményekkel jár az ott tárolt adatokra (teljes megsemmisülés). Felmerül a kérdés

[2] malware: a malicious software, a rosszindulatú szoftver szóösszetétel általánosan elfogadott rövidülése

tehát – de a megválaszolása a jövőbe mutat, hogy vajon hogyan fognak kinézni a kvantum-vírusirtók?

A jelenbe visszatérve, a Neumann-elvű számítógépeken sem egyszerű ma már a rosszindulatú programkódok felderítése, hiszen a fejlett rosszindulatú kód megbújhat csak a memóriában vagy elrejtőzhet a háttértárolókon – sőt, azok firmware-programjában – is, mindenféle aktivitás nélkül. Emiatt a memóriában nem kereső vagy a csak rosszindulatú hálózati aktivitás felismerésére, netán csak egy előre rögzített minta keresésére programozott védelmi szoftverek jelentős hátrányban vannak az aktuális fejlett támadásokkal szemben. Nem adnak okot a bizakodásra Luís Mendonça és Henrique Santos 2012-es cikkében [19] foglaltak sem, mely szerint ha a hálózati forgalomban keresünk anomáliákat egy botnet szoftver lehetséges működésére, egyrészről magas lehet a hamis riasztások száma, másrészről virtuálisan lehetetlen megkülönböztetni egy normál működést szimuláló botnet szoftvert egy valódi számítógéptől:

„In the end, it will be virtually impossible to detect a botnet whose bots mimic normal host behavior. But a bot behaving as normal host can't be that malicious.„

Biztonsági aspektusból meglátásom szerint nem elfogadható a szerzők azon véleménye, hogy egy normál működést szimuláló botnet szoftver nem is látszik annyira veszélyesnek, hiszen a védelmi képességet nemcsak a látható, hanem a rejtett képességek (alvó ügynök probléma) ellen is ki kell fejlesztenie a közigazgatási információs rendszereknek. Ez behozza a bizalom fogalmát a rendszerbe, mivel a látens fenyegetésekkel szemben csak a bizalom működik, hiszen kénytelenek vagyunk bízni abban, hogy a rendszer jól működik ebben az esetben is. Bizalom nélkül nem működhet elektronikus információs rendszer (a bizalmatlansági dilemma nem feloldható infokommunikációs környezetben sem [9]), általánosítva ez azt jelenti, hogy a bizalmi elv nélkül nem működhetnek az információs rendszerek. A látens fenyegetés feltételezésével az elvárt biztonságot így nyilvánvaló módon már nem lehetséges a malware programok feltelepülését követően megteremteni – bármit is csinálnak vagy nem csinálnak azok az adott pillanatban – mindaddig, amíg a rendszer védelmi képességei nem nyújtanak védelmet az alvó ügynökök jövőbeli káros tevékenységei ellen is. A botnet példánál maradva Gyebrovszky megjegyzi, hogy itt már nem új támadási formák megjelenéséről van szó, hanem ismert támadások szorosan egymásba fonódó, vagyis gyakorlatilag egymástól elkülöníthetetlen végrehajtásáról. Kiegészítő kérdésként felvethető, hogy vajon az emberiség létszámával (növekedésével) arányos (arányosan növekedett-e) a károkozókat gyártó hackerek száma? A hacktivizmus létrejötte és a számítógépes bűncselekmények jövedelmezőségi rátája mindenesetre nem ad túlzott bizalomra okot.

A botnetek fertőzési folyamatát megvizsgálva a dán Aalborg Egyetem kutatói megállapították, hogy a folyamat három szakaszra osztható fel [29]:

1. fázis: kezdeti fertőződés, amit követ egy másodlagos fertőződés (amely során a malware további elemei kerülnek be a megfertőzött gépre),
2. fázis: kapcsolódás (a parancsközponthoz), illetve karbantartás, update,
3. fázis: a rosszindulatú tevékenység végzése vagy a botnet propagálása.

Nagyon érdekes eredménynek gondolom ebből a technikai riportból, hogy a botnetek detektálására 20 különböző módszert vizsgált meg és kivétel nélkül mindegyik módszer a botnetek fertőzési fázisaiból csak a 2-es és 3-as szakaszban vált hatékonnyá, az 1-es szakaszban egyik módszer sem volt képes felismerni a megfertőződést. Érdekes kérdés lehet statisztikai szempontból megvizsgálni az egyes fázisok bekövetkezési valószínűségét, különböző feltételezések vagy tapasztalati értékek mentén.

A számítógépek megfertőződéséhez

Alapvető kérdés az egyes nem kívánt események – mint például a számítógépek megfertőződése – valószínűségének becslése vagy idősorok alapján történő kiszámítása. Ebből lehet ugyanis számítani az esemény kockázatait. A várható érték alapú kockázat-számítási módszer (kárkövetkezmény szorozva a bekövetkezési valószínűséggel) tömegjelenségekre kiválóan működik, de vannak olyan események, amelyekre nem tudjuk megadni ezt az értéket, tipikusan olyan események ezek, melyek a gyakorlatban még ezelőtt sohasem következtek be (pl. 9/11, invázió az űrből, globális epidemiológiai járvány gyógyszer-rezisztens kórokozókkal). Mivel ezeknek az eseményeknek nincs előfordulási valószínűségük, így érdemben statisztikailag sem vizsgálhatók (egyszeri események vagy be nem következett hipotézisek). Ebből adódóan módszertanilag különböző módon kell vizsgálni a tömegjelenségeket és az extrém (egyszeri) jelenségeket. Amíg van értelme valószínűségekkel dolgozni, addig természetesen lehet számolni velük, legfeljebb meg kell változtatni a súlyozást. Erre azért van szükség, mivel nagyon nagy kárérték nagyon kis valószínűségekkel megszorozva már adhat kockázati értéket, holott az esemény nem felfogható értékekkel rendelkezik a gyakorlatban és a reprezentációs skálán is marginalizálódik. A valószínűségeket emiatt oly módon kell transzformálni, ami követi a kockázathoz fűzött érzetet, így biztosítva azt, hogy fel tudja fogni az értelmezője. Benedikt, Kun és Szász kutatásai szerint célszerű logaritmikus transzformációt választani (nagyon kicsi és nagyon nagy értékek együttes reprezentálása esetében) [26], továbbá ez megfelel a pszichofizikai érzékelési törvényeknek is. Harmadik módszer, amikor valószínűségeknek nincs értelme, egyedi események léteznek, akkor csak a hibafa-elemzés alkalmazható. A körülmények, a vizsgálandó események paraméterei határolják be, hogy melyik modellt

lehet adott esetben alkalmazni. Például nem valószínűségi alapon megközelíthető esemény lehet önmagában az, ha a teljes internet (számítógépek, okostelefonok, útválasztók, IoD[3], IoT[4], konzolok stb. mindegyike) megfertőződik egy még nem ismert károkozó szoftverrel. Megjegyezzük, hogy kiinduló gócról sok esetben nincs értelme beszélni, a fertőzés ebből következően feltételezésünk szerint véletlenszerűen jelenik meg. A csomóponti vizsgálat során lehetséges a nagyon nagy kapcsolati számossággal rendelkező csomópontok fertőzésének (pl. Microsoft Update webhely) hatását gócpontként vizsgálni, vagyis a legmagasabb kapcsolati osztályba sorolt elemek fertőzésének hatása eltér a véletlenszerűen feltételezett fertőzés megjelenésétől. Figyelemmel kell lenni arra a tapasztalati tényre, hogy általában a védelem a professzionális csomópontoknál magasabb szintű, így ez befolyásolja a terjedés csomóponti hatékonyságát is.

Trendszámításokhoz érdekes kérdés lehet például sokéves átlagban vizsgálni azt, ami egy éves távban nem értelmezhető – amennyiben így lehet az egyedi jelenségeket tömegjelenségekké átalakítani azáltal, hogy hosszabb időszakban vizsgáljuk. A hosszabb időtáv következménye az, hogy felléphet a károsszegek nominálértékeinek a jelentős különbsége, az időtáv alatti infláció függvényében. A kárkövetkezmények számításában ebben az esetben alkalmazható a jelenérték-számítás az időtávlatokban szemlélt kárértékek összehasonlíthatóságának biztosítása miatt, aminek létezik jól kiforrott matematikai apparátusa.

Érdekes és relevanciával rendelkező kérdés lehet az, hogy vajon mekkora botnet-hálózat lehetséges elvileg? A gyakorlatban több tízmilliós esetekről tudunk idáig. A kérdés egyszerűnek tűnhet abban az esetben, ha csupán az asztali és mobil számítógépekre koncentrálunk – esetleg kiegészítve a szuperszámítógépekkel, de egy kicsit bonyolultabbá válik akkor, ha az okostelefonokat, a játékkonzolokat és minden Neumann-elvű eszközt (IoD, IoT) is figyelembe kívánunk venni, mint potenciális botnet-hordozó. A figyelembe vétel az eszközök egymáshoz viszonyított logikai távolságainak meghatározásakor történhet meg, amikor is szomszédosnak tekintünk két eszközt akkor, ha a második eszköz egy lépésben megfertőződhet az első eszköz fertőzöttsége esetében – és ha a lépéseket diszkretizáltuk (folyamatos fertőzés feltételezése helyett, a kapcsolati szám [σ] bevezetésével). A fertőzés leírását az átviteli függvény meghatározása jelenti ebben az esetben. Más szóval a szomszédság-probléma így metrikai problémává tehető, vagyis logikai probléma lesz, nem pedig fizikai (euklideszi) távolság. Így lehetővé válik az, hogy egy többszintű hálózatban bármelyik alhálózati szinten legyen a legfelső szintű

[3] IoD = Internet of Devices, az eszközök internete
[4] IoT = Internet of Things, a dolgok internete

csomópontnak szomszédja – logikai szomszédság, ez megfelel például a nyilvános weboldalak böngészésének a belső hálózatról. Könnyen belátható egyébként, hogy ebben az esetben elméletileg végtelen rekurzív halmazzal van dolgunk, hiszen minden egyes IP-címmel rendelkező hálózati csomópont mögé elvileg el lehet helyezni egy újabb hálózatot, amire a címfordítás (Network Address Translation, NAT) ad lehetőséget. A lépések egymásutánisága pedig ebben az esetben sejtautomata modellel modellezhető. Meg kell itt jegyezni, hogy az első szintű hálózat csomópontjainak száma a teljes IP címtartományt felöleli (kivéve a belső IP-címtartományokat), míg a második és minden további alhálózat csomópontjainak száma a belső IP címtartomány számosságával egyezhet meg az elvi maximális érték kihasználása esetében (ez IPv4, mint alsó elvi korlát esetében is 254^4 = 4 162 314 300 – a 0 és a 255 foglalt címek). Egy ilyen struktúrában vajon milyen gépi utasítás-végrehajtási kapacitással (MIPS[5]) rendelkezhet az a hacker, aki 100e, 1M, 10M, 100M, 1Mrd gépből álló botnetet birtokol átlagos processzorkapacitás feltételezése mellett? Az időtényezőt és a Moore-törvényt is figyelembe véve ez a kérdés a jövőbe is extrapolálható, habár a nem Neumann-elvű számítógépek elterjedése vagy egy technológiai miniatürizálási korlát nyilvánvaló módon befolyásolhatja az extrapoláció érvényességét.

A jövőbeli extrapolációnál figyelembe lehet venni a frissen feltárt fenyegetések arányát a már ismertekhez képest, amely során feltételezzük, hogy véletlenszerű folyamat lesz a fenyegetések felbukkanása, ekkor az időtényező diszkretizálásával a felbukkanás valószínűségét meg lehet határozni az egyes diszkrét időpontokra.

További érdekes kérdés, hogy mekkora annak a valószínűsége, hogy ez a botnet-hálózat a fenti számosságokkal a valóságban is realizálódik? Ennek vizsgálatakor tömegjelenségként kell kezelni a hálózatba való bevonást. Lehetséges, hogy releváns kérdés az is, hogy a botnet-hálózat kiépítésének technológiai ismeretével kik rendelkeznek? Nyilván földrajzilag függetlennek kell feltételezni a támadó elhelyezkedését, hiszen az internetezők gépparkját egységes egésznek tekintve bárkinek ugyanolyan esélye van arra, hogy hozzáfér ehhez a „gép”-hez, ha a a technológiát ismeri. Az idézőjelet a virtuális jellemzői miatt kapta a „gép” szó, hiszen a botnet vezérlőközpontjából látszólag egy „gép” számára adhatók utasítások, amit az sok-sok részletre bontva „többprocesszoros rendszer”-ként hajt végre. A realizálódást két tényező befolyásolhatja erőteljesen, a terjedési képesség és ennek másik oldala, a védelmi mechanizmusok. A terjedési képesség a még ismeretlen sérülékenységekkel van összefüggésben (Zero Day Attack, Nulladik Napi Támadás), hiszen a védelmi szoftverek a sérülékenység kihasználhatóságnak kiderülése és a védelem megjelenése között gyakorlatilag teljesen védtelenek a támadással szemben. Alapvető

[5] MIPS a Million Instruction Per Secundum, a másodpercenkénti egymillió (gépi) utasítás mértékegységének a rövidítése

biztonsági érdek, hogy ez az időszak a lehető legrövidebb legyen. A fertőzés megakadályozása technikai jellegű, kérdés lehet az is, hogy a már megfertőződött hoszt be tudja-e vonni a következő számítógépet a botnet-hálózatba (bevonási valószínűség). A bevonást ebben az esetben az teszi lehetővé vagy akadályozza meg, hogy a megtámadott számítógép tartalmazza-e a bevonáshoz szükséges sérülékenységet vagy sem. Ha a gépeket egymástól függetlennek tekintjük, akkor a bevonási valószínűséget megszorozva a fertőzés célpopulációjának számosságával meg lehet kapni a botnet feltételezhető méretét.

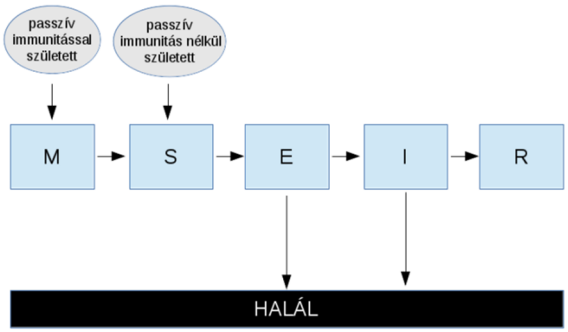
Ezt a vizsgálatot lehet finomítani a védelemmel ellátott számítógépek védelmi képességével hiszen ha védett a számítógép, valamennyivel kisebb a bevonódás valószínűsége ahhoz képest, ha nulla védelmet feltételezünk. Meg kell jegyezni, hogy itt a védelem nem egy általános célú funkciót jelent és nem is a védelem létezését (kifejlesztését), hanem a fertőződéshez szükséges sérülékenységnek a megtámadott számítógépen való megtalálhatóságát. Nyilván egy 'A' módszerrel támadó botnet ellen nem nyújt védelmet a 'B' módszer ellen védő specializált szoftver – a generikus védelmi algoritmusokat tartalmazó megoldásokat (heurisztika, entrópia-vizsgálat) is figyelembe véve. Lehetséges mutálódást modellezni, hogy egy bizonyos modellidő után másik malware (mutáns) terjedését is lehetséges vizsgálni, kérdés, hogy a mutáció és egy új malware között van-e lényeges különbség a terjedést illetően. További finomítást jelent a fenti vizsgálatra nézve az időtényező bevezetése, vagyis az egyes csomópontok támadhatóságának és védelmi képességének időbeli változásait is vizsgáló modell kialakítása.

A rosszindulatú programkódok terjedési mechanizmusait tekintve egy adott halmazból építkeznek, az elnevezések különbségei a kódok egyes jellemzőiből fakad. Például a 'vírus' elnevezést – hasonlóan a biológiai vírusokkal – azokat a rosszindulatú programkódokat jelöli, melyek képesek önmagukat megsokszorozni, de önmagukban életképtelenek, szükséges egy másik fájlhoz csatlakozniuk a működőképességük fenntartása érekében. A vírusok absztrakt modelljének korai leírását már Leonard M. Adleman is megadta 1988-ban [17], amiben a vírusok tevékenységét a sérülések okozása, a fertőzés és az imitáció hármasban jelölte meg. Az imitáció abból a szempontból érdekes, hogy ez akkor következik be, ha a vírus nem talál tevékenységére alkalmas környezetet és fertőzésre alkalmas fájlt sem. Ez esetben a megtámadott számítógép gyakorlatilag védett a támadás ellen, annak ellenére, hogy a rendszer integritása a vírusnak a memóriába történő bekerülésével már – ha ideiglenesen is, de – sérült. Valóban lehetséges ezt üzemeltetési szempontból megbízható működésnek tekinteni, de tény, hogy az erőforrások biztonságát (integritását) sértő esemény ebben az esetben is bekövetkezett és a bekövetkezés kockázata nem eliminálható. A vírus egyébként a fertőzést követően – ha talál fertőzhető fájt, végrehajtja annak eredeti programját, majd – átprogramozza a megfertőzött fájl működését, a biológiai analógia tehát ebben is tetten érhető. A terjedési mechanizmusok mindazonáltal külön vizsgálandók a malware céljától. Meg kell jegyezni, hogy az integritás nem jelenik

meg hangsúlyosan az infokommunikációs projektek eredményei között és kommunikációjában sem, ahogyan erre Aranyossi Márta, Nemeslaki András és Fekó Adrienn rámutatott a magyar ICT projektek vizsgálatánál [20].

Megvizsgálva a biológiai vírusok terjedésénél használt matematikai apparátust [24], fontos elemként jelenik meg az elsődleges reprodukciós arány (Basic Reproduction Ratio, R_0), mely azt mondja meg, hogy egy fertőzött egyed a fertőzési időszak teljes időtartama alatt hány egyedet fertőz meg tipikus terjedéssel másodlagosan. A Kermack-McKendrick küszöbfeltétel kimondja, hogy ha $R_0 < 1$, akkor a fertőző ágens nem tud elterjedni a tiszta populáció fertőzésre érzékeny tagjain, míg ha $R_0 > 1$, akkor pedig igen. Ebben a definícióban implicit módon benne foglaltatik az az állítás is, hogy a populációnak (P) vannak olyan tagjai (I), akik eredendő módon immunisak az adott fertőzés ellen, nyilván ennek két szélsőértéke az, ha $I = P$ (ez esetben semmilyen fertőzés nem történik), illetve $I = 0$ (ha minden egyed védtelen a fertőzéssel szemben). További vizsgálandó fogalom a fertőzés virulenciája, ami az érzékeny egyedek megfertőződésének egységnyi idő alatti valószínűségét jelenti, amitől nyilvánvaló módon függ a fertőzés elterjedésének sebessége. Ezt követően a vírusterjedés dinamikájának vizsgálata következhet, amire matematikai modellezési eszközök léteznek, és sok modellben ezeket már meg is vizsgálták (pl. MSEIR).

Ezek után lehetséges vizsgálni és modellezni a számítógépes vírusok terjedését. A vizsgálatban véleményem szerint felhasználhatók a biológiai vírusok terjedésére alkalmazott módszertanok is, azzal az eltéréssel, hogy a biológiai populációnál megjelenő természetes immunitás automatikusan nem jelenik meg a számítógépes rendszerek esetében, ez minden esetben emberi beavatkozás eredménye lehet csak – akár telepítési, akár védelmi tevékenység eredményezi azt.



2. ábra: A fertőzések általános állapotváltozási modellje (készült [10] 1. ábrája alapján)

Az ábrán használt nagybetűk a populáció hasonló tulajdonságú elemeit jelölik, a következő módon:

- M: passzív immunitással rendelkező gyermek, vagyis olyan utód, aki már nem fogékony a fertőzésre (passively immune infant)
- S: fogékonyak (susceptible)
- E: lappangó periódusban fertőzésnek kitett egyedek (exposured in latent)
- I: fertőzöttek (infectives)
- R: immunitással rendelkező meggyógyultak (recovered)

Az eredeti ábrán a halál, mint esemény megjelent a passzívan immunis, a fogékony és a rezisztens állapotnál is, azonban számítástechnikai értelemben ezek nem vezethetnek a számítógépes szolgáltatások rendelkezésre állásának megszűnéséhez, csak a lappangás és az aktív fertőződési szakaszban van lehetősége a rosszindulatú programkódnak erre (annak figyelembe vételével, hogy egy bizonyos módszer ellen immunis gép egy másik módon sebezhető lehet), így emiatt az eredeti ábra módosítása indokolttá vált. Természetesen fertőzésen kívüli események ugyan vezethetnek a számítógép leállásához, azonban ennek vizsgálata nem lehet célja egy ilyen modellnek. A fenti ábrán látható általános modellt MSEIR néven hivatkozzák, de számos más modell is vizsgáltak már a vírusok terjedése kapcsán, pl. MSEIRS, SEIR [21], SEIRS, SIR, SIRS, SEI, SEIS, SI vagy SIS.

A vírus propagációjának vizsgálatában egyensúlyi helyzeteket is kerestek a fertőzött és nem fertőzött populációk között, melyeknek léteznek feltételei, amit 2014-ben közzé is tettek [5].

A vírusok terjedésének modellezése véletlen vagy skálafüggetlen (csomópontokon keresztül terjedő) szempontú is lehet. A szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ) elterjedése és az ICT szempontból is centralizált közszolgáltatások létrejötte indokolja a csomóponti szemléletet. A kettő közötti különbséget az egyedek kapcsolatainak számával, illetve annak inhomogenitásával lehetséges kezelni (vagyis vannak olyan egyedek, akik kevesebb, míg mások több kapcsolattal rendelkeznek). Praktikusnak tűnik emiatt az egyedeket a kapcsolataik száma szerinti osztályokba besorolni a vizsgálat folyamán, ahelyett, hogy minden csomópontot egy fix kapcsolati számmal jellemeznénk. Ha azonban a modellt egyszerűsíteni kívánjuk, akkor a csomóponti támadások azok egyedisége miatt inkább logikai elemzéssel vizsgálhatók. Az óvintézkedések pedig működhetnek úgy, mint egy véletlen hálózat. Kérdés ez esetben, hogy a már megfertőződött, de még nem aktív és az aktivizálódott számítógépek közötti különbséget (lappangás) hogyan lehetséges kezelni? A terjedési módszer kihat ennek a vizsgálatára is, ha az idődimenzió is eleme a modellnek, hiszen a háttértárolóra feltelepült malware lappangási ideje valószínűleg hosszabb, mint a kizárólag a memóriában létező rosszindulatú programkódok esetében mérhető lappangási idő.

A vírusterjedési módok figyelembe vételére a „technológiai hálózat" (technological network) vizsgálatát veti fel 2004-ben Justin Balthrop szerzőtársaival együtt [12]. A cikk négy jól ábrázolható technológiai hálózatot ad meg, melyek sérülékenyek a támadásokkal szemben:

A. az Internet Protocol (IP) használó csomópontok közötti lehetséges kapcsolódások
B. a felhasználói (desktop) számítógépeken megosztott távoli adminisztrátori accountok hálózata
C. az e-mail címjegyzékek (address book) hálózata
D. a felhasználói e-mailek hálózata (e-mail messages)

Kritikaként felvethető, hogy mind az adminisztrátori, mind a felhasználói e-mailek hálózata IP-címek és portok használatával érhető el, ebből a szempontból a címjegyzékek tartoznak csupán másik kategóriába, mivel ezek egy fájlként helyezkednek el a felhasználói számítógépeken. A „technológiai hálózatok" szemüvegén keresztül felvetődik a kérdés, hogy vajon hány ilyen hálózat létezik? Az joggal feltételezhető, hogy nincs értelme az egyes technológiai hálózatokat egymástól függetlenül vizsgálni, mivel ismert az is, hogy léteznek olyan malware programok, melyek nem egy, hanem több (3-4) terjedési módszert is felhasználnak a fertőzések kivitelezéséhez. Ez – plasztikusan ábrázolva – az egymásra tett technológiai hálózatok eredőjének vizsgálatát teszi szükségessé, annak ismeretében, hogy általában a malware az első sikeres módon terjed (okos fertőződés), nem pedig *mindegyik módon (*buta fertőződés*)* – de volt már példa ismétlődő fertőzésekre megtámadott és sikeresen megfertőződött rendszerek esetében is. Az alkalmazott terjedési módszer sok esetben jellemző a támadó személyiségére, aki különböző okokból követheti

el tetteit [30], így kereshetnek a számítógépes bűncselekményeket vizsgáló nyomozók az elkövetőre jellemző nyomokat is a rendszerekben (pl. exploitálási mód, log-lenyomat, egó bizonyítási vágy stb.)

Ha a támadók személyiségi jegyei felől közelítjük meg a kérdést, akkor felmerül az, hogy mi lehet a támadó célkitűzése a malware megírásával? Visszakövetkeztetve a fenyegetések kétféle típusából (általánosan – véletlenszerűen – terjedő, korlátok között terjedő célzott támadás), a támadó szándékát is ebből adódóan általános célú károkozás (hírnév) vagy célzott támadás (anyagi előny, sértődöttség, düh) motiválhatja. Ebben az esetben a támadó személyiségtípusokon keresztüli elemzése adhat arra választ, hogy mit kell a védelemben figyelembe venni az akadályok felépítésében. Kovács Judit a doktori disszertációjában [14] átfogó jelleggel összefoglalta az emberi kockázatok mérésére alkalmas metodológiákat. Kérdés, hogy melyik modell lehet a célravezető akkor, ha a valószínűsíthető támadói alkat például leptoszóm? Milyen sorrendben és nehézségi fokban kell az akadályokat (körkörös védelmet) kiépíteni, elöl alacsonyak, egyszerűek, hátul nagyok, magasak vagy fordítva? Nem szabad figyelmen kívül hagyni azonban azt sem, hogy ha egy támadó rendelkezik a támadáshoz szükséges *konkrét* tudással, azzal már potenciális fenyegetést képezhet. Másrészről annak is tudatában kell lenni, hogy a támadások egy része véletlenszerű próbálkozással történik az internet felől.

Az internet-használók nem mind egységesen használják az internetet, van aki jobban, van aki kevésbé. Hullám István és Muha Lajos arra figyelmeztet 2010-ben, hogy az internetfüggőség magasabb kockázati tényezőt jelent az információs társadalom biztonságát tekintve [11], így felmerül a kérdés, hogy vajon a vírus-propagációban is kihasználható-e ez a tulajdonság az internet-használók egyre növekvő internetfüggő táborában.

Lehetséges kutatási kérdések megfogalmazása

A fentiek alapján a rosszindulatú kódok terjedésének modellezésére az alábbi területek kutatását tartom relevánsnak a fentiek alapján:

- bevonási modell kidolgozása minden terjedési módszer figyelembe vételével (többszintű technológiai hálózati modellben). A terjedési módszereket a támadó aktivitása szerint vélhetően csoportosítani is lehet (pl. az internetbiztonsági taxonómia alapján)
- ki kell számítani (vagy meg kell becsülni) a botnet-hálózatba bevonódás valószínűségét (megfelelő források alapján), amihez feltételként meg kell határozni az érintett számítógépek számát, kiegészítve a processzorral rendelkező eszközökkel – ideértve az IoT, IoD eszközöket is, valamint a botnetekről szóló becsléseket is fel lehet ezekhez használni. Jó kérdés, hogy a hálózati topológiát mélységében is tekintve

a feltételezett alhálózatok (szintek) száma és mérete hogyan befolyásolja ezt a valószínűséget, IPv4 és IPv6 esetében.

- védelem hatásának meghatározása a fertőződésre (felhasználható a biológiai vírusok fertőzési és lecsengési adatai és számítási módszerei)
- a modell finomítása többszintű védelem feltételezésével (itt a fertőzés ténye lesz vélhetően az érdekes, nem pedig a védelem feltörésének módja). Emiatt a többszörös védelmi intézkedések hatására a védelem arányosan növelhető, nincsen szükség feltételes valószínűség-számításra. Figyelembe kell venni azt, hogy habár a többszintű védelem feltörésénél az egyes védelmi intézkedések feltörése logikailag egymás után történik, de statisztikai szempontból a feltörés valószínűsége nem függ az előző feltörésének valószínűségétől, legfeljebb kauzális viszony lehet közöttük, de statisztikai nem.
- a modell érvényességének validálása valós adatokon, vagyis annak vizsgálata, hogy a modell működése összhangban van-e a tapasztalt eseményekkel? Létező probléma a modell ellenőrzése is, vagyis hogyan tudunk kísérleteket végezni a modell ellenőrzésére? Szükséges-e ehhez egy „dummy" vírus elterjedését vizsgálni, vagy lehetséges egy valódi eseményt figyelemmel kísérni? Ez utóbbihoz az érintett szervezetek biztonsági tudatossága és együttműködési képessége elengedhetetlen, az információ-áramlás biztosítása érdekében. Az együttműködésről tényéről vita nem lehetséges, hiszen a 2013. évi L. törvény ezt előírja az információbiztonsági felelősök tevékenységei között.

Összefoglalás

Az infokommunikációs technológia fejlődése eddig nem küszöbölte ki a sérülékenységek megjelenésének lehetőségét. Az új technológiák is rendelkeznek befogadóképességgel a szoftverek sérülékenységeit kihasználó rosszindulatú programkódokat tekintve (pl. trójai, backdoor, vírus). A globálisan működtetett vírusvédelmi rendszereknek természetes módon van egy reakcióideje, mely nem csökkenthető minden határon túl, mert a reakciók előállításához időre van szüksége a gyártóknak, vagyis a reakcióidő alulról korlátosnak tételezhető fel. Emiatt a védelem létrejötte nem lehet exponenciális. A védelem megjelenésének vizsgálatához adódik a lehetséges időpontok következő négy mérföldköve: nulladik napi támadás megjelenése, fenyegetettségi intervallum, védelem létrejötte, védelem elterjedése. A fertőződések elterjedésének vizsgálata alapvető fontosságú a védelmi prioritások meghatározásánál és a rendelkezésre állási paraméterek folyamatosságának biztosíthatóságában.

A sérülékenységek közzététele a javítások megjelenését követően tűnik praktikusnak, hiszen addig az információ terjedése korlátozottan mehet csupán végbe, ami csökkentheti a fenyegetettségi intervallumban bekövetkező incidensek számát. A védelem létrejötte és

elterjedése szakaszok szétválasztását az indokolja, hogy számos esetben hiába dolgoznak ki a gyártók védelmi megoldásokat az egyes sérülékenységekre, az üzemeltetésért felelősök nem telepítik azt, így egy ismert sérülékenységből adódó fenyegetettség akár évekig is fennmaradhat. Ehhez hozzátartozik az is, hogy a gyártók hiába javítják a sérülékenységeket egyes szoftverekben vagy fejlesztői környezetekben, ha a programfejlesztők nem frissítik azokat tervezett módon, akkor az elavult program használhatóságának fenntartása érdekében kell működésben tartani a régebbi sérülékeny környezetet, a rendelkezésre állás biztosításának kényszeréből adódóan. A biztonság fenntartása tehát nem egy szereplőn – nem csak a felhasználón – múlik ilyen esetekben.

A közigazgatásban az ügyfelek elégedettségének egyik mérőszáma a hozzáférési index – amire Orbán Anna is rámutatott [25], amit értelemszerűen befolyásol egy rosszindulatú programkód sikeres támadása, ahogyan ez a múltban is előfordult (DDoS támadások, zsaroló programok). Krasznay Csaba felveti a polgárok védelmét egy kiberkonfliktusban [16], ami arra utal, hogy noha kevés az ilyen események számossága napjainkban, azonban a védelem megteremtésekor gondolni szükséges erre is. A helyzetet árnyalja, hogy az új technológiák elterjedésével együtt fog élni sok esetben a régi és az új, amelyek használatához bátorság szükséges, ahogyan erre Som Zoltán rámutatott:

„Sok szempontból hiánypótlás történt, hiszen végre megtörtént a jogalap kimondása egy esetleges közigazgatási felhő létrehozásához, bátor jelentkezőket vár ez a lehetőség. Általánosítva pedig az új technológiák bevezetésének lehetőségét is megteremteni a törvény." [28]

A felhőalapú számítástechnika elterjedését nagymértékben akadályozta a biztonságosságába vetett negatív hit, a kiszolgáltatottságtól való félelem, ahogyan azt Sasvári Péter László empirikusan is alátámasztotta a magyar vállalkozások vizsgálatában [27].

Kiss Attila és Beláz Annamária megállapította [13], hogy *„A közigazgatásban is egyre nagyobb az igény a gyorsabb és biztonságosabb ügyintézés iránt, az okostelefonokhoz és az intelligens online szolgáltatásokhoz szokott ügyfelek elvárásai mellett a hatékonyság növelése és az átlátható közigazgatási szolgáltatások érdekében is szükséges a telekommunikációs és széles sávú fejlesztések mielőbbi megkezdése, az e-közigazgatás előtérbe helyezése."* Mindez természetesen a normatív közigazgatásban jogszabály-alkotást kell, hogy eredményezzen, de ezt annak tudatában kell majd figyelni, hogy végső soron a közigazgatási jog nem kodifikálható [7], heterogenitása miatt.

Összegezve, a megfelelő információbiztonsági védelem kialakításához a támadások elterjedési paramétereit és mechanizmusait alapvető fontosságú megismerni, ideértve a támadások realizálhatóságát eredményező veszélyforrások vizsgálatát is, az optimális, azaz

zárt, folytonos, teljes és kockázatarányos védelem minden időpontban való fenntarthatóságáért, amíg az ICT eszközöktől való függősége a társadalmainknak fennáll.

Köszönetnyilvánítás

Jelen tanulmány elkészítését a PD-109740 számú „IT és hálózati sérülékenységek tovagyűrűző társadalmi-gazdasági hatásai" című projekt támogatta a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal – NKFIH finanszírozásával.

Irodalomjegyzék

[1] Bárdos Zoltán. 2009. A villamosenergia-ellátás biztonságáról. *Bolyai Szemle* XVIII(1): 77-84.

[2] Budai Balázs Benjámin. 2009. *Az e-közigazgatás elmélete (Második, átdolgozott kiadás)*. Budapest: Akadémiai Kiadó Zrt.

[3] Bukovics István, Vavrik Antal. 2006. Infrastruktúrák kockázata és biztonsága: Kritikai problémaelemzés. *Hadmérnök*, I(3): 32-40.

[4] CERT Annual Reports 1994-2003. http://www.cert.org/historical/annual_rpts/ (2016. július 1.)

[5] Chenquan Gan, Xiaofan Yang, Qingyi Zhu. 2014. Global Stability of a Computer Virus Propagation Model with Two Kinds of Generic Nonlinear Probabilities. Research Article. *Abstract and Applied Analysis*, 2014(Article ID 735327): 1–7.

[6] Cyberthreat Real-Time Map, http://cybermap.kaspersky.com/ (2016. július 1.)

[7] Gellén Márton, Patyi András, Péterfalvi Attila, Révész Balázs, Szalai András, Takács Albert, Temesi István. 2013. *A közigazgatás funkciói és működése*. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt.

[8] Gyebrovszky Tamás. 2014. Folyamatos fenyegetések a kibertérben. *Hadmérnök* IX(3): 137-153.

[9] Hámori Balázs. 2004. Bizalom, jóhírnév és identitás az elektronikus piacokon. *Közgazdasági Szemle*, LI(2004. szeptember): 832–848.

[10] Herbert W. Hethcote. 2000. The Mathematics of Infectious Diseases. 2000. *Society for Industrial and Applied Mathematics (SIAM) Review* 42(4): 599–653.

[11] Hullám István, Muha Lajos. 2010. Új típusú függőségek az információs társadalomban és azok hatása az informatikai biztonságra. *Hadtudományi Szemle* 3(2): 70-76.

[12] Justin Balthrop, Stephanie Forrest, M. E. J. Newman, Matthew M. Williamson. 2004. *Technological networks and the spread of computer viruses*. http://arxiv.org/pdf/cs/0407048.pdf (2016. július 1.)

[13] Kiss Attila – Beláz Annamária. 2015. Szabályozás és egységesítési törekvések az IKT és a távközlés világában. Beszámoló az ITU 2015 konferencia eredményeiről és annak hátteréről. *Pro Publico Bono,* 2015 (4): 146-157.

[14] Kovács Judit. 2011. *Az emberi tényező matematikai modellezésének lehetőségei a katasztrófavédelmi kockázatértékelés és kockázatkezelés területén. Doktori PhD értekezés.* Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, Bolyai János Katonai Műszaki Kar, Katonai Műszaki Doktori Iskola.

[15] Kovács László – Krasznay Csaba. 2010. Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság* 2010. január: 44-56.

[16] Krasznay Csaba. 2012. A polgárok védelme egy kiberkonfliktusban. *Hadmérnök*. VII (4): 142-151.

[17] Leonard M. Adleman. 1988. *An Abstract Theory Of Computer Viruses*. http://www.cin.ufpe.br/~ruy/crypto/virus/ala01.pdf. (2016. július 1.)

[18] Lian-Ao Wu and Daniel A. Lidar. 2006. Quantum Malware. *Quantum Information Processing* 5(2): 69-81.

[19] Luís Mendonça, Henrique Santos: Botnets: a heuristic-based detection framework. *SIN'12 Proceedings of the Fifth International Conference on Security of Information and Networks, 2012, Jaipur, India*. New York: ACM.

[20] Márta Aranyossi, András Nemeslaki, Adrienn Fekó. 2014. Empirical Analyis of Public ICT Development Project Objectives in Hungary. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 5(12): 45-54.

[21] Michael Y. Li, Hal L. Smith, Liancheng Wang. 2001. Global Dynamics Of An SEIR Epidemic Model With Vertical Transmission. *Society for Industrial and Applied Mathematics (SIAM) Review* 62 (1): 58–69.

[22] Neumann János. 2005. *Túlélhetjük-e a technikát? (Can we survive technology? Fortune, June 1955)* In: Neumann János Válogatott írásai. Válogatta és az előszót írta: Ropolyi László. Budapest: TYPOTEX Kft. Elektronikus Kiadó.

[23] NORSE. http://map.norsecorp.com/ (2016. július 1.)

[24] O. Diekmann. 1996. *Mathematical Epidemiology of Infectious Diseases. Images of SMC Research.* http://oai.cwi.nl/oai/asset/13562/13562A.pdf. (2016. július 1.)

[25] Orbán Anna. 2015. Ügyfél-elégedettség mint a hatékonyság egyik dimenziója. *Pro Publico Bono*, 2015 (4): 51-59.

[26] S. Benedikt, I. Kun, G. Szász. 2004. Individual and Collective Risk Perception in Decision Criteria. CYBERNETICS AND SYSTEMS 2004. VOLUME I. *Proceedings of the Seventeenth European Meeting on Cybernetics and Systems Research, organized by the Austrian Society for Cybernetic Studies, held at the University of Vienna, Austria, 13-16 April 2004*. 321-325.

[27] Sasvári Péter László. 2015. *A felhőalapú számítástechnika elterjedésének empirikus vizsgálata a magyar vállalkozások körében.* In: Fejlődő jogrendszer és gazdasági környezet a változó társadalomban. Komárno: International Research Institute.

[28] Som Zoltán. 2013. A közigazgatási informatikai felelősök oktatásának kérdései. *Hadmérnök*, VIII.(4): 223-237.

[29] Stevanovic, Matija; Pedersen, Jens Myrup. 2013. *Machine learning for identifying botnet network traffic*. http://vbn.aau.dk/files/75720938/paper.pdf (2016. július 1.)

[30] Vasvári György. 2009. *A társadalmi és szervezeti (vállalati) biztonsági kultúra.* Budapest, Ad Librum Kft.