Kiss Dávid – Váczi Dániel

A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján

DOI 10.17047/HADTUD.2018.28.1.151

A szerzők célja, hogy elméleti oldalról megközelítve feltárják a kritikus infrastruktúra-elemek humánveszélyeit és a hálózatelemzés segítségével a kockázati faktor csökkentésének lehetőségét vizsgálják meg a terjedési mechanizmus modellezésére, illetve megállítására használt ún. vírusfertőzés és az immunizálás módszerével.

Korunk egyik legnagyobb civil és katonai kihívását jelenti a különböző elektronikai, virtuális és más ellátó rendszerek (gazdasági, társadalmi, szociális stb.) működésének folyamatos fenntartása és ez által a meghibásodás vagy a célzott támadás rizikófaktorának redukálása. A támadások, meghibásodások okának feltárása, vizsgálata és az azokra való preventív felkészülés már nem elegendő, szükséges a kapcsolatban álló rendszereket is figyelembe venni. Az elmúlt két évtizedben az állami működés szempontjából kiemelt rendszereket és azok elemeit a nemzetállamok elkezdték specifikusan a saját működésük alapján meghatározni, és részben erre alapozni a békeidőszaki és védelmi intézkedéseiket, stratégiájukat.

A kritikus infrastruktúra fogalmának megszületése szorosan összekapcsolható az Amerikai Egyesült Államokat ért sajnálatos 2001. szeptember 11-ei terrortámadással. Bár annak elméleti alapjait már 1998-ban lefektették egy elnöki direktívában,[1] az mégis csak a terrortámadást követően emelkedett törvényi hatályba.[2] Már itt megjelenik az interdependencia, vagyis a kölcsönös függőség kérdésköre.

1 PPD 63 – 1998. május 22. Protecting America's critical infrastructures https://fas.org/irp/offdocs/pdd/pdd-63.htm (Letöltés ideje: 2017. 10. 04.)

2 Egyesült Államok, Uniting and Strengthening America, by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001-es 107-56-os törvény, 1016-os szekció, másnevén a Kritikus Infrastruktúrák védelméről szóló 2001-es törvény https://www.selectagents.gov/resources/USApatriotAct.pdf (Letöltés ideje: 2017. 10. 04.)

A kritikus infrastruktúra a következőképpen értelmezhető e törvénybe iktatott megfogalmazás szerint: *„… mindazon fizikai vagy virtuális rendszerek és berendezések, amelyek oly létfontosságúak az Amerikai Egyesült Államok számára, hogy azok korlátozása vagy megsemmisülése meggyengítő hatással lenne a nemzetbiztonságra és a nemzetgazdaság biztonságára, a közegészségre, közbiztonságra vagy ezek bármely kombinációjára".*[2] A rendszerek kombinációja az, ami utal a kölcsönös kapcsolatra. Az elmúlt évek alatt a nemzetállamok és közösségek ezt a megfogalmazást vették alapul, majd alakították saját specifikus helyzetüknek megfelelően, mérlegelve a különböző ellátó rendszerek fontosságát, összefüggéseit és relevanciáját.

A rendszerek összefonódása egy olyan új kihívást jelent a társadalom, a kormányzás, a gazdaság és a védelmi szféra számára, ami a korábbi szemléletmódokkal már nem megoldható. A rendszerszintű védelem már nem opcionális, hanem létkövetelmény. A történelem folyamán ugyan találunk egymással kölcsönösen összefüggő rendszerelemeket, de az internet és a technológia segítségével ezek a rendszerek eddig soha nem látott szoros kapcsolatba kerültek.

A XXI. század egyik legnagyobb vívmánya az Internet és annak világméretű elterjedése. Bár a technológia alapjait már a 1900-as évek közepén lefektették, az ún. internetboom mégis csak a XXI. századra tehető, amikor már világszerte évről évre több millió újabb háztartás és felhasználó csatlakozott a hálózathoz. A Kleiner Pirkins gondozásában megjelent, Mary Meeker által az internetes trendekről publikált tanulmányából kiderül,[3] hogy 2009 óta megduplázódott az internetfelhasználók száma (1,5 milliárdról közel 3,5 milliárdra nőtt), az okostelefonok száma, amik a telefonálás és az internet segítségével tovább csökkentik a távolságot a társadalom szereplői között, 300 millióról közel 3 milliárdra nőtt. Külön érdemes megemlítenünk az ún. Internet of Things[4] megjelenését is. A hálózatba kapcsolás során már nem elég a számítógépeket, okostelefonokat figyelembe vennünk, hanem egyre több passzív és aktív (okos) eszközt csatlakoztatnak a világhálóra (hűtő, mosógép, ipari eszközök stb.), ami tovább növeli a támadási felületet és a befolyásolható eszközök számát.

A rendszerek közötti kapcsolatok kialakulásának fokozódása miatt elengedhetetlen volt új, matematikai és más elemzési módszerek kifejlesztése annak érdekében, hogy a rendszerbe álló elemeket minél hatékonyabban tudják vizsgálni, azok sajátosságait még pontosabban tudják meghatározni.

Hálózatelemzés

Az elmúlt évtizedek fejlődése és a már említett hálózatok összetettségének fokozódása életre hívott egy, mára már külön tudományágazatként, aposztrofált módszertant, a hálózatelemzést. A gráfelméleti alapokra támaszkodó hálózatelemzés története viszont jóval korábbra helyezhető.

---

3 Mary Meeker, Internet Trends 2017 – Code Conference http://dq756f9pzlyr3.cloudfront.net/file/Internet+Trends+2017+Report.pdf (Letöltés dátuma: 2017. 10. 04.)

4 Buyya, Rajkumar et al.: Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, Volume 29, Issue 7, September 2013, pp. 1645–1660 http://www.sciencedirect.com/science/article/pii/S0167739X13000241 (Letöltés ideje: 2017. 10. 09.)

Stanley Milgram, 1967-os kutatása jelenti a hálózatelemzés egyik alapkövét.[5] Milgram úgy juttatott el csomagokat az Egyesült Államok különböző pontjaira, hogy azokat csak személyesen lehetett továbbadni egy a postázó által ismert személy által. A kísérlet arra hivatott választ keresni, hogy van-e univerzális szabályrendszere a társadalom kapcsolati hálójának. Vagyis Milgram egy általános igazságot keresett, ami jellemző az Egyesült Államok társadalmi kapcsolataira. A kísérlet eredményeképp bebizonyosodott, hogy az Államokban együttesen átlagosan mindenki ismer mindenkit 5-6 ismerős közbeiktatásával. Ez a szociális munka megalapozta az ún. *kisvilág* elméletet,[6] amelyet később kiterjesztettek az Internetre és más szociális, kapcsolati hálóra, ahol egy hasonló nagyságú értékre bukkantak. A kisvilág elmélet lényege, hogy egy sok pontból álló hálózat esetén is az átlagos távolság[7] meglepően kicsi.

A hálózatelemzés fejlődésének következő állomásaként kell megemlítenünk két, igazán fontos tanulmányt, amelyek a hálózatok általános szabályszerűségeire, tulajdonságaira összpontosítottak. Az Erdős–Rényi modell[8] rámutatott egy, a világunkban általánosan fellelhető jelenségre, a véletlen gráfokra és így a véletlen hálózatok kialakulásának módjára. Ezen modell alaptézise szerint a modellbe belépő új pontok ugyanakkora valószínűséggel csatlakoznak a hálózat bármely pontjához, ezáltal fokszám-eloszlásuk[9] normál vagy más néven Gauss görbét követ majd.

Visszautalva Milgram kisvilág elméletére meg kell említenünk, hogy a legtöbb véletlen gráf is rendelkezik ezzel a tulajdonsággal, hogy az új (véletlenszerű) pontok (például személyek), élek (például a személyek közti kapcsolatok) kapcsolódása esetén az átlagos távolság az elemszámot tekintve viszonylag alacsony. A hálózatok általános tulajdonságait tekintve a véletlen gráf elmélete sok, valóságban is megjelenő hálózat tulajdonságát is leképezte. Viszont azokra a hálózatokra, amelyeknél az új pontok belépése nem véletlenszerű jelleget, hanem szabályszerűséget mutatott, egy új fogalmat és új szabályrendszert kellett kialakítani.

Barabási Albert László szerzőtársaival 2000-ben publikált[10] tanulmányában bevezette a skálafüggetlenség fogalmát. Barabásiék bizonyították, hogy egyes hálózatban a nagy fokszámmal rendelkező pontok nagyobb vonzással rendelkeznek, mint a hálózat kevés kapcsolattal ellátott pontjai. A belépő elem ez által nagyobb valószínűséggel csatlakozik azokhoz a pontokhoz, amik a hálózat jelentősebb, központibb pontjainak nevezhetőek. Ennek eredménye, hogy ahogy növeljük egy ilyen hálózat esetén az elemszámot, annál szebben kirajzolódik, hogy a hálózat fokszám-eloszlása

5 Milgram, Stanley: The Small World Problem. Psychology Today, vol. 1, no. 1, May 1967, pp. 61–67.

6 Barabási Albert László: Behálózva. Budapest, Helikon Kiadó, 2013.

7 A hálózat pontjai közötti távolság számtani átlaga. Két pont közötti távolság, ha összeköttetésben állnak, akkor értéke 1, ha közvetlen kapcsolat nincs a két pont között, a távolság megegyezik a közbeiktatott csúcsok száma +1 értékével.

8 Erdős Péter, Rényi Alfréd: On The Evolution of Random Graphs. Magyar Tudományos Akadémia Matematikai Kutató Intézet Közlöny 5, 1960, pp. 17–61.

9 Fokszám: egy csúcsba befutó élek száma (jelen tanulmány keretében az élek iránya nem releváns) Fokszám-eloszlás: a hálózatban szereplő pontok fokszámainak eloszlás függvénye

10 Barabási Albert László et al.: The large-scaleorganization of metabolic networks. Nature 407, 2000, pp. 651–654.

egy negatív hatvány függvényt fog követni, és nem a véletlen gráfoknál ismert normál eloszlást.

A skálafüggetlenség fogalmának megjelenése jelentősen befolyásolta a hálózatelemzés addigi képét. A véletlen gráfok, bár alkalmasak voltak korlátozottan hálózatok modellezésére, de a hétköznapokban fellelhető rendszerekre sokkal inkább jellemző a skálafüggetlenség. Ezt a tulajdonságot figyelhetjük meg a gazdasági kapcsolatrendszerekben, a társadalmi és szociális hálókban, a különböző digitális hálózatok feltérképezése során, sőt, még az agyban fellelhető idegrendszerek esetében is.

A XXI. századhoz érkezve már új tudományként tekinthetünk a hálózatelemzésre, aminek módszertana a gráfelméletben gyökeredzik, de olyan jellegű összefüggéseket vizsgál és olyan jelentős mértékű rendszerszemlélet szükséges hozzá, amit a gráfelmélet már nem tud önmagában kielégíteni. Szükséges volt természetesen a hálózatelemzés felszínre töréséhez a technológiai fejlődés is. A nagy, komplex hálók[11] elemzéséhez szükséges infrastruktúrákat (hardware – számoló kapacitás, nagy mennyiségű adattárolás) és elemző programokat (software) csak az utóbbi évtized technológiai fejlődése tudta biztosítani a kutatók számára.

Az IT-biztonság és a vállalati kapcsolatrendszer összefüggései

A védekezés

Az információbiztonság területén a védekezésnek több különböző dimenzióját különböztethetjük meg. A küzdelem a szándékos vagy véletlen károkozás ellen megvalósulhat többféle módon. A különböző adminisztratív, fizikai és technikai[12] kontrollok megfelelő bevezetésével a biztonsági kockázatok nagy részére megoldást adhatunk.

Az adminisztratív kontrollok előírások és eljárások formájában járulnak hozzá a magasabb biztonsági szint eléréséhez. A fizikai védelem a különböző eszközökhöz és objektumokhoz történő illetéktelen hozzáférés megnehezítését hivatott elősegíteni. A logikai védelmi intézkedések segítségével a különböző technikai eszközökön keresztül történő elérhetőséget tudjuk korlátozni. Manapság sem egy versenyszférában tevékenykedő vállalat, sem egy közszférában működő állami szervezet nem teheti meg azt, hogy ezeket a gátakat nem építi be a saját védelmi infrastruktúrájába. A megfelelő kialakításra különböző szabványok, ajánlások, jó gyakorlatok[13] léteznek. Ezek segítik a biztonsági szakemberek munkáját abban, hogy kockázatarányos védekezést tudjanak kialakítani, majd azt gazdaságos módon működtetni és fenntartani.

---

11 Komplex hálózatoknak nevezzük azokat a hálózatokat, amelyek elemeinek ismeretében se tudunk pontos vagy egyszerű leírást adni a rendszer egészének működésére. Például egy gazdasági hálózat tagjainak ismeretében nem következtethetünk feltétlenül a gazdasági tevékenységük alakulására.

12 Fleiner Rita-Munk Sándor: Informatikai biztonsági útmutatók, kontrollok és szerepük az adatbázis-biztonság megvalósításában. Hadmérnök, VI (3), 2011, pp. 100–116. http://hadmernok.hu/2011_3_fleiner_munk.pdf (Letöltés ideje: 2017. 10. 08.)

13 Szádeczky Tamás: Információbiztonsági szabványok. Budapest, Nemzeti Közszolgálati Egyetem, 2014.

A védekezésben elkülönített területek	*A védekezés eszközei*
Adminisztratív kontroll	előírások és eljárások
Fizikai védelem	eszközökhöz, objektumokhoz kiépített vagyonvédelmi rendszer
Logikai védelem	technikai (informatikai) eszközökön keresztül kialakított védelem

Békeidőben a vállalatok elsődleges veszélyforrásai nem a (más nemzet és/vagy belső forradalmi) fegyveres erők támadásából eredő károk. A vállalat védelmét és védelmi rendszereit más jellegű támadások ellen, más szempontok szerint építik fel és alakítják ki. A védelmi rendszerek kialakítása jelentősen függ a vállalat és/vagy rendszer, objektum felépítésétől, működési mechanizmusától és rendeltetésétől. A támadások jelentős része azonban egy új dimenzión, a kibertéren keresztül érkezik a különböző informatikai rendszerek felhasználásával.

A támadás

Lehet szó célzott vagy halászó (nem konkrét személy/csoport ellen irányuló) tevékenységről. A csoportosítás és a védelemre való felkészülést jelentős mértékben befolyásolhatja, hogy a kártékony kódok milyen szándék mentén íródnak;

- Egyes kártevők arra hívatottak, hogy egyszerűen blokkolják valamilyen módon a rendszerek működését. Ilyenek lehetnek például a különböző titkosító, zsaroló (ransomware) vírusok, de az elkövetők túlterheléses támadással (DoS/DDoS)[14] bizonyos szolgáltatások elérhetetlenségét is előidézhetik.
- Lehet cél a felhasználók bosszantása, esetleg különböző kéretlen hirdetések megjelenítése a felhasználók számára. Előfordulhat, hogy a kártékony kód segítségével olyan portokat nyitnak meg, amelyek közreműködésével bot-hálózat[15] részeivé válhatnak az áldozatok, hogy így engedély nélkül használják ki a fertőzött számítógépek kapacitását, akár bűncselekmények végrehajtására is.
- Egyik legkártékonyabb támadási típus az, amikor információkat szivárogtatnak ki a megtámadott eszközről vagy hálózatról. Az így kinyert adatokat nyilvánosságra hozhatják, árulhatják például a dark-weben,[16] ipari kémkedés során felhasználhatják, esetleg országok egymás védett titkaihoz is hozzáférhetnek ily módon.

14 Olyan támadás, mely ismert sérülékenységek vagy kommunikációs protokollok sajátos gyengeségeit kihasználva teljesen vagy részlegesen meggátol vagy ellehetetlenít egy informatikai szolgáltatás.

15 Hálózatba kötött számítógépek, melyek egy fertőzést követően a tulajdonosok akaratán kívül végeznek műveleteket.

16 A világháló azon része, melyet nem indexelnek a különböző keresőmotorok. Ezt kihasználva a számítógépes bűnözők könnyebben tudnak tevékenykedni a felfedhetésüket, így minimalizálva.

A kártékony kódok különböző rendszerekbe történő bejuttatásának csak a készítőik fantáziája (és a rendelkezésükre álló erőforrás) szab határt. Megtörténhet, hogy különböző ismert vagy még nem publikált (zero-day[17]) sérülékenységeket használnak ki. Az is lehetséges, hogy az emberek figyelmetlenségén, tudatlanságán alapuló támadás kivitelezése vezet célra. Ilyen például egy adathalász (phishing[18]) támadás vagy elektronikus levelek fertőzött csatolmányainak letöltésén keresztül történő támadás.

A malware-ek[19] célzott eljuttatásának módja több úton is elképzelhető, amennyiben egy adott céget kívánnak megtámadni. Lehet dömpingszerűen mindenkinek direkt módon fertőzött elektronikus levélként kiküldve, azonban az ilyen tömeges támadásokat a különböző határvédelmi megoldások általában könnyen tudják azonosítani. Ennél ma már sokkal kifinomultabb kódok vannak, melyek operációs rendszertől, hardvertől, hálózattól vagy akár védelmi eszközök meglététől függően is másként viselkednek. Az ilyen jellegű eszközök mögött valószínűsíthetően a rendelkezésre álló erőforrások (anyagi, humán) messze túlmutatnak egy scriptkiddie[20] által összeállított gyenge kódon. Azt érdemes megvizsgálni, hogy amennyiben nem áll rendelkezésre megfelelő mennyiségű erőforrás, akkor vajon egy gyengébb kód eljuthat-e ugyanolyan valószínűséggel egy potenciális célponthoz, mint bárki máshoz. Ha pedig még a megfelelő háttér is rendelkezésre áll, vajon milyen hatékonysággal fertőzhető meg valaki.

A vállalati kapcsolatrendszer és annak támadási felületei

Érdemes megvizsgálni egy nagy hierarchikus szervezet általános felépítését. Legfelül áll a tulajdonos/tulajdonosok, akik általában kevésbé folynak bele a munkavégzésbe, de még a közvetlen irányításába is csak ritkán. Általában van egy megbízott személy, aki az irányításért felel mint ügyvezető igazgató. Amennyiben több telephellyel rendelkezik a cég, lesznek a különböző helyi irányítók, akik napi szinten vannak kapcsolatban valamilyen dedikált feladattal megbízott helyetteseikkel. Őket a beosztottakkal a különböző közép- és alsóvezetők kötik össze. Elméletben lefektethető az a szabály, hogy a tulajdonost a munkavállaló csak sok áttéten keresztül tudja csak elérni. (1. ábra)

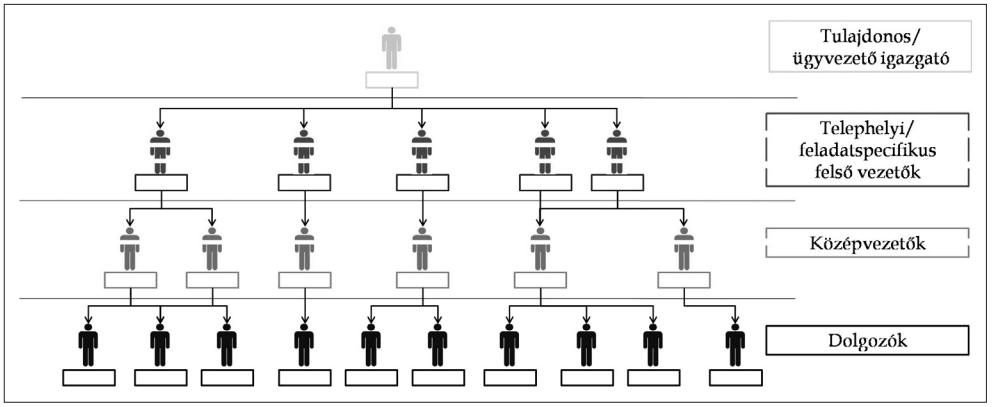
Azonban, ha alaposabban megvizsgálunk egy céget, rá kell jönnünk, hogy ez a valóságot nem tükrözi. Az informális és nemcsak hierarchikus kapcsolatokat is figyelembe véve a kapcsolati háló egy vállalaton belül sokkal összetettebb és bonyolultabb. A munkavállalók akár beosztotti szinttől, munkaterülettől, nemtől, kortól függetlenül is kapcsolatba kerülhetnek egymással, ami előidézi az információáramlás hatékonyságának növekedését. A 2. ábrában egy elméleti esetet vázoltunk fel, amely a legtöbb esetben tükrözi a vállalati struktúra kapcsolati rendszerét. Az ábra szereplői

17 Zero-day = nulladik napi támadás: olyan támadás mely egy rendszer olyan sérülékenységét használja ki, amit még nem publikáltak.

18 Phishing = adathalász: Az a támadási forma, amikor a támadó úgy kívánja begyűjteni az áldozatok (személyes) adatait, hogy megtévesztés képen legitim tartalomnak tünteti fel az adatkérést.

19 Malicious software = rosszindulatú szoftver: a különböző rosszindulatú kódok összefoglaló neve.

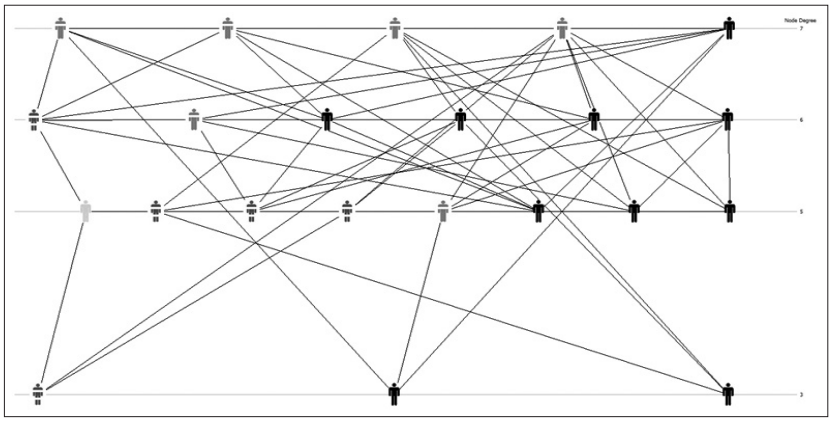
20 Olyan szaktudással nem rendelkező személy, aki mások által megírt programok, eljárásokat használ károkozás céljából.



1. ábra
A vállalati hierarchia egy elméleti hálója
(saját szerkesztés)

az 1. ábrának megfelelőek (1 tulajdonos, 5 felsővezető, 6 közép és alsóvezető és 10 dolgozó), viszont a hierarchiát most nem a munkahelyi értelemben vett alá-fölé rendeltség alapján alakítottuk ki, hanem az adott személy kapcsolati rendszerén alapulva. A kapcsolatoknál a formális (1. ábrában szereplő) kapcsolatok mellé további informális (személyes- és munkaviszonyon alapuló) kapcsolatokat rendeltünk véletlenszerűen. A háló összesített fokszámát így az 1. ábrában lévő 25 helyett 60-ra növeltük. A 2. ábrában legalulra kerültek a háló azon szereplői, akik a legkevesebb informális és/vagy formális kapcsolattal rendelkeznek, és hasonló elv alapján a legfelül helyezkednek el a vállalat azon szereplői, akik viszont a legtöbbel. Vagyis a 2. ábra az új, kapcsolati hálóban szereplő csúcspontok fokszám eloszlását mutatja.

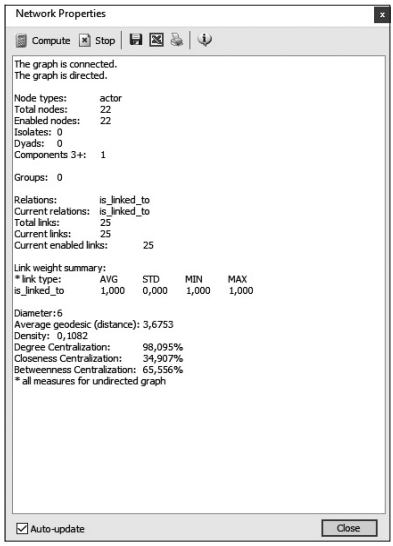
Látható, hogy ebben az esetben a tulajdonos/ügyvezető csak a hierarchia középszintjén helyezkedik el, míg a legfelső szintekre a közép- és alsóvezetők, valamint maguk a dolgozók kerültek.



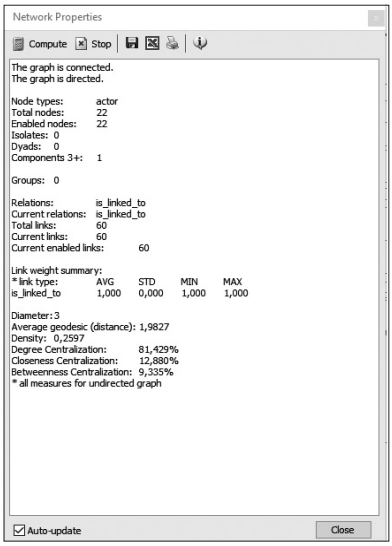
2. ábra
A vállalati hierarchia egy elméleti kapcsolati hálója
(saját szerkesztés)

Ez közvetlen hatással van az információk terjedésére is. Egy információ így az egyik végponttól bármelyik másikig sokkal gyorsabban eljut a 2. ábrában felvázolt hálón keresztül, mint az 1. ábrában. Ezt igazolja, hogy az 1. ábrán szereplő háló átmérője[21] 6 és átlagos távolsága 3,6753, míg a 2. ábrán szereplő hálóban ezek az értékek jelentősen kevesebbek (átmérő: 3, átlagos távolság 1,9827). (3. és 4. ábra) Ezen kívül sajátosságként említhető meg az is, hogy az információ nemcsak vertikálisan, hanem horizontálisan is terjed a hálózatban.

Az úgynevezett informális hálózatok segítségével tehát gyorsabban és intenzívebben terjednek az információk. Ennek oka, hogy nemcsak a közvetlen főnökeinkkel és kollégáinkkal vagyunk kapcsolatban, hanem a cégnél lehetnek más magánjellegű vagy hivatalos kapcsolataink.



3. ábra
A 1. ábra vállalati hierarchia hálózatának tulajdonságai
(saját szerkesztés)



4. ábra
A 2. ábra vállalati hierarchia kapcsolati hálójának tulajdonságai
(saját szerkesztés)

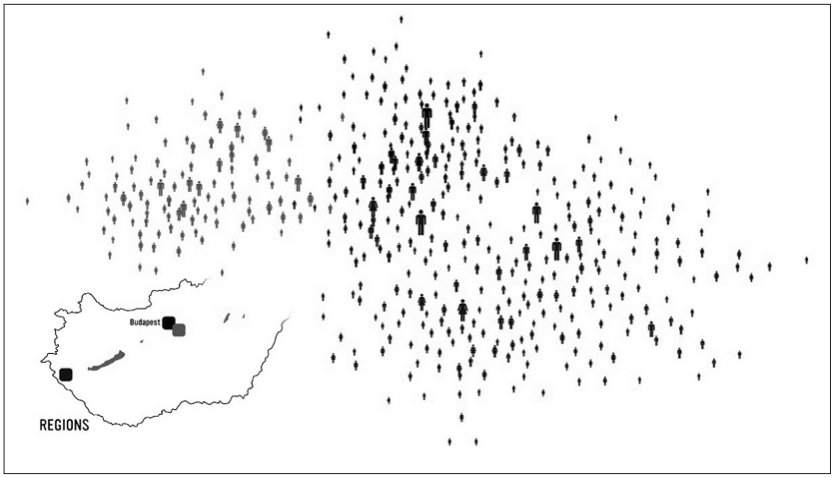
Ha növeljük a csomópontok számát a hálózatban (egyre nagyobb vállalatot veszünk alapul), akkor a kapcsolati háló skálafüggetlen jelleget fog felvenni. A fokszám-eloszlás ennek függvényében pár kulcsfontosságú szereplő vezető szerepét (kapcsolati és nem munkahelyi hierarchia szempontjából) fogja mutatni, míg a szereplők jelentős része jóval kevesebb fokszámmal fog csak rendelkezni. Emellett a skálafüggetlenség azon tulajdonsága is megfigyelhetővé válik, hogy egy új pont belépése esetén a pont nagyobb valószínűséggel kerül kapcsolatba azon szereplőkkel, akik már eleve sok kapcsolattal rendelkeztek korábban.

21 A hálózat pontjai közötti távolság legnagyobb értéke.

Új kutatások[22] szerint egy pozíciót betöltő személy hatékonysága attól is függ, hogy egy ilyen hálózatban milyen szerepet tölt be (hány fokszámmal rendelkezik). Ez a felismerés újabban sok különböző szervezetfejlesztés alapját is szolgálja a vállalatokon belül, azonban számos más aspektusban is figyelembe vehető.

Itt kell kitérnünk a kapcsolati struktúra által generált veszélyekre. Egy számítógépes fertőzés szétterjesztéséhez egy vállalatnál, amely különböző üzleti titkok kiszivárogtatása céljából backdoorokat[23] nyit a hálózaton, egy ilyen kapcsolati struktúrát mutató hálózatban a célzott támadás lehet a megfelelő módszer. Amennyiben a támadónak nem áll rendelkezésére jelentős mennyiségű erőforrás egy kifinomult eszköz fejlesztéséhez, megvásárlásához elég lehet egy baiting[24] támadással egy fertőzött pendrive-ot a kiemelt szereplők (magas fokszámmal rendelkező csomópontok) egyikéhez eljuttatnia, és így hatványozni tudja a károk valószínűségét és intenzitását. Ha a munkavállalók ismeretségét véletlen hálózatnak tekintjük, akkor a fertőzött adathordozót bárhol elhelyezheti a támadó. Abban az esetben azonban, ha egy valós, csomópontokkal rendelkező hálózatként tekintünk rá, akkor könnyen beláthatjuk, hogy nem mindegy a terjesztő személye.

Barabási Albert László *A hálózatok tudománya* című művében[25] egy olyan magyarországi vállalat elemezését mutatja be, mely 3 telephellyel rendelkezik.



5. ábra
Egy magyarországi vállalat humán erőforrás térképe[26]

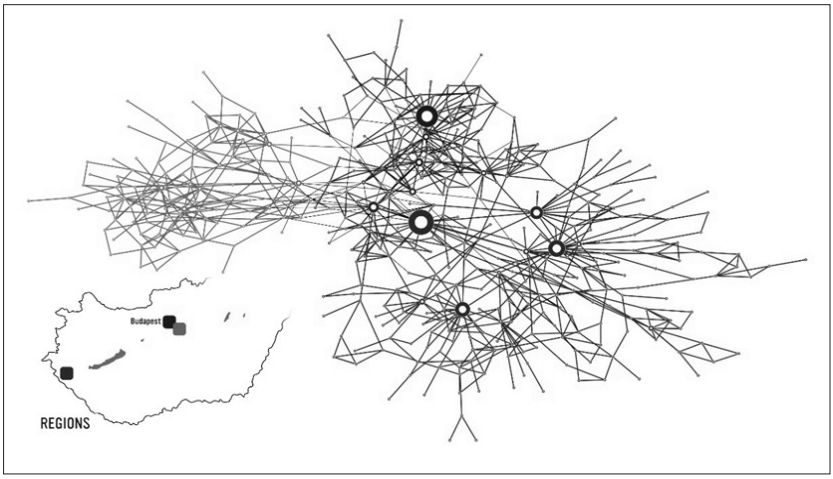
22 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. pp. 47–50.

23 Egy olyan program részlet, mely segítségével a támadó szolgáltatásokat tud futtatni a megtámadott eszközön, a tulajdonos tudta nélkül.

24 Fertőzött hordozható eszközök célzott elhelyezése, úgy hogy az azt megtaláló személy nagy valószínűséggel csatlakoztassa egy informatikai eszközbe.

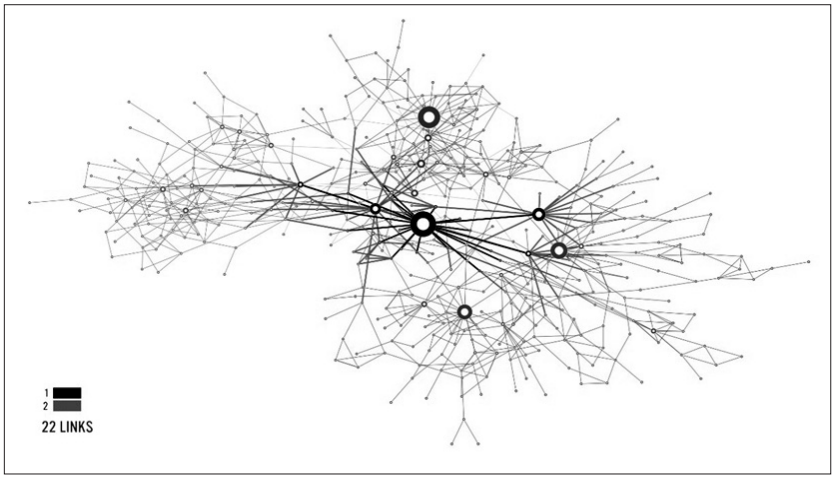
25 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. pp. 47–50.

26 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. pp. 48–49. 1.7. ábra



6. ábra
Egy magyarországi vállalat kapcsolati hálója[26]

Az 5. ábrán láthatók a telephelyeken dolgozó személyek, akiknek kapcsolati hálóját a 6. ábra hálózata szemlélteti. A 7. ábrában fokszám-eloszlás alapján súlyozásra kerültek a hálózatban szereplő elemek és látható, ahogy a sötétebb színnel kiemelkednek a több kapcsolattal rendelkező és elhalványodnak a perifériára kerülő pontok.



7. ábra
A magyarországi vállalat kapcsolati hálója kontrasztba helyezve a legtöbb kapcsolattal rendelkező elemeket (fokszám szerinti hierarchiában)[26]

Az elemzés során a leírás kiemeli, hogy a legtöbb kapcsolattal rendelkező csomópont (7. ábra közepén látható fekete kör) a munka- és környezetvédelmi felelős. Ő gyakorlatilag mindenkivel kapcsolatban áll. Ha belegondolunk, az is világossá válik számunkra, hogy nagy eséllyel ő fog a különböző telephelyekre egy pendrive-al érkezni, hogy megtarthassa a kötelező oktatásokat. Tehát vírusterjesztési szempontból egy hasonló beosztású személy környezetében kellően előkészített baiting pendrive nagyobb eséllyel éri el a várt hatást, mint ha véletlenszerűen helyeznénk el azt.

Védelmi szempontból meg kell tehát vizsgálnunk egy vállalatnál, hogy melyek azok a pozíciók, ahol a legtöbb formális és informális kapcsolat alakulhat ki a munkavégzés során. Ez nemcsak a belső védelem szempontjából fontos. Arra is gondolni kell, hogy kik azok, akik a vállalat partnereivel állnak szorosabb vagy akár mindennapos kapcsolatban. Vezetői szempontból fontos szem előtt tartani a már meglévő üzleti kapcsolatokat és azok fenntartását, így az összekötő munkatársak és azok képzése kiemelt figyelmet érdemel, hiszen egy meghatározó üzleti együttműködés megromlását eredményezheti egy tőlünk eredő vírusfertőzés.

Amennyiben kockázatarányosan szeretnénk egy védelmi struktúrát kialakítani, nem szabad elvakultan az általánosan elfogadott kritikus pozíciókra fókuszálnunk. A fenti példából is látszik, hogy bizonyos pozíciót betöltő emberek egy célzott támadáskor veszélyeztetettebbek lehetnek, mint például egy felsővezető. Érdemes az ő biztonsági továbbképzésükre külön figyelmet fordítani és bevezetni olyan technikai kontrollokat, melyek csökkentik az őket fenyegethető támadások sikerességét. Ily módon a védelmi szakemberek közelebb kerülnek a 20–80[27] (30–70) aránypárként emlegetett kockázatarányos védekezéshez.

Ez a fajta védekezési stratégia alkalmazása egy létfontosságú rendszerelem (kritikus infrastruktúra) esetén még hangsúlyosabbak lehetnek, hiszen a veszélyek kockázata is nagyobb.

A terjedési, vírusfertőzési modell védelmi aspektusai

Abban az esetben, ha egy célzott támadás sikerrel jár és a fertőzés sikeresen megvalósul, figyelembe kell vennünk annak terjedését. Barabási Albert László A Hálózatok Tudománya c. kötetében részletesen leírja, hogy a különböző hálózati modellekben hogyan terjedhetnek a vírusok.[28] A szerző itt elsősorban az orvosi értelemben vett vírusok terjedését elemzi, azonban kitér arra is, hogy ez más tudományterületeken – mint például az informatikában[29] – is hasonló módon történik. Tételezzük fel, hogy a kártékony kód kétféleképpen terjedhet. Egyik módja az, hogy a fertőzött pendrive csatlakoztatásakor a háttérben automatikusan lefut, így megtelepszik a gazdaszámítógépen. A másik módja pedig az, hogy a hálózaton keresztül terjed. Lehetséges tehát, hogy ha a vírushordozó személy több helyen (például telephelyen) is csatlakoztatja

27 Barabási Albert László: Behálózva. Budapest, Helikon Kiadó, 2013. pp. 74–89.

28 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. pp. 397–402.

29 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. p. 396. 10.1 ábra / p. 412.

az eszközt, több irányból tud elkezdeni terjedni a kártékony kód. Gyakorlatilag a két hálózat: a szociális és az informatikai hálózat[30] összeforr. Feltehetően a kettő egy cégnél nagyban hasonlít, de mégis lehetnek eltérések.

A vírus terjedését Barabási 3 típusú (SI, SIS, SIR) járványmodellezés alapján vizsgálja.

- A SI (Susceptible-Infected[31]) modellben (8.a ábra) kétféle állapotot vehetnek fel az érintettek: lehetnek fogékonyak és fertőzöttek. Itt a vírus élethosszát aszerint vizsgálja, hogy a kezdeti időpontban mindenki fogékony, majd amint elkezdődik a fertőzés,a fertőzöttek száma exponenciálisan nőni kezd. Mivel a fertőzött emberek száma nő és egyre kevesebb fogékony pont van a rendszerben, a terjedési sebesség csökkeni fog.
- A SIS (Susceptible-Infected-Susceptible) modell (8.b ábra) annyiban tér el az előzőtől, hogy miután valaki a fertőzést elkapta, abból ki is gyógyulhat, ami után ismét fogékonnyá válik.
- A 3. modell (8.c ábra) a SIR (Susceptible-Infected-Removed[32]), melyben egy új állapot található meg, ez a gyógyult. Miután egy fertőzött egyén megkapja az ellenszert, vagy magától meggyógyul, nem válik ismét fogékonnyá, mivel a szervezetében az ellenanyag már megtalálható.

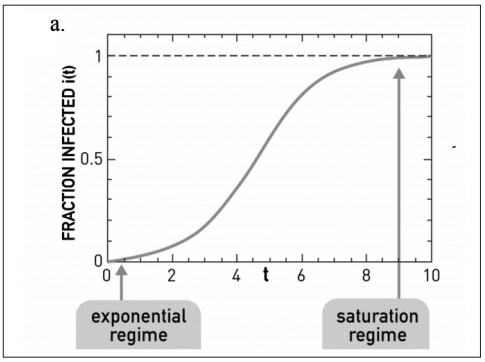
A három modell terjedési hatékonyságát és lefolyását a 8. a-c ábrákon lévő diagramok szemléltetik. A SI és a SIS modell közötti szignifikáns különbség a fertőzött populáció mértékében keresendő. A SI modell esetében a teljes populáció megfertőződik egy idő lefolyása után, itt nem veszi figyelembe a gyógyulást, mint ahogy a SIS modell esetében. A fertőzés mértéke exponenciálisan nő, majd a fogékony alanyok csökkenésével a fertőzés üteme is csökkeni fog. A SIS modell esetében a fertőzés nem terjed ki az egész populációra, a kigyógyulás okozta redundancia miatt. A kigyógyulás és a fertőzés mértékének aránya adja a populáció egészséges hányadát a fertőzés kiteljesedésekor. A SIR modell esetében több szempontot is figyelembe kell vennünk. A fogékony egyedek drasztikus csökkenése (s függvény) és a fertőzöttség növekedése (i függvény) mellett megjelennek az immunis, vagy a vizsgált populáció esetében az elhunyt egyedek (r függvény) számának változása. Látható az, hogy egy vírusfertőzés esetén a modellek alkalmazása nem szubjektív, hanem objektív módon történik. A vizsgált populáció reakciója (lesz-e immunis egyed vagy nem) kiemelten fontos a modellek bevezetésénél.

A károkozók számítógépen történő terjedésénél az első modellt akkor lehet értelmezni, ha nincs biztonsági kontroll, tehát senki nem foglalkozik a kártékony kód eltávolításával. Manapság azonban a nagy cégeknél, illetve a létfontosságú rendszerelemek jelentős részénél elvárt az informatikai biztonság kialakítása, így a védekezés is. A kártékony kódok terjedése ebben az esetben egyfajta hibrid modellt fog képezni. A SIR modellt lehet alapul venni, hiszen általában egy kártékony kód elleni

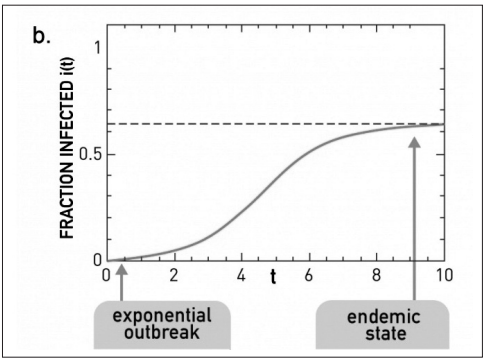
30 Birher Nándor – Bertalan Péter: Hálózatokban. Veszprém, Okter-Nobus Kiadó, 2014, pp. 60–62.

31 Susceptible = Fogékony – Infected = fertőzött

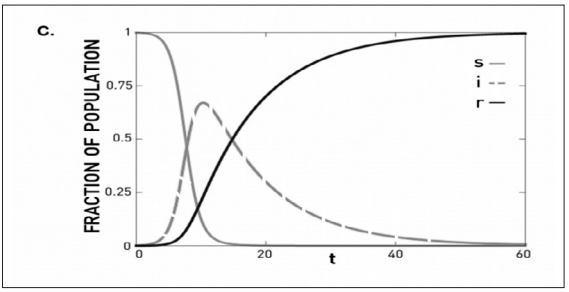
32 Removed = eltávolított (ebben az aspektusban az immunis vagy elhunyt személyekre vonatkozó tulajdonság)



8.a ábra
A SI modell[33]



8.b ábra
A SIS modell[34]



8.c ábra
A SIR modell[35]

védekezés a kód által kihasznált sérülékenység megszüntetésével történik. Így tehát nemcsak, hogy a fertőzött gépek kerülnek gyógyult állapotba, de ha rendszerszinten kezelik a problémát, így a többi eszköz megfertőződését megakadályozzuk.

Figyelembe kell venni azonban azt, hogy egy szofisztikált kód terjedése nemcsak egyféleképpen történhet meg. Abban az esetben, ha több sérülékenységet is ki tud használni, és nem mind lett kezelve (egyáltalán felfedezve), akkor nem teljes a fertőzés megállítása. Előfordulhat tehát, hogy egy adott sérülékenységet javítottak, de a kártékony kód többféleképen is tud terjedni, így a rendszer továbbra is fertőzött marad. Ilyenkor a SIS modellt lehet ötvözni a SIR-rel, hiszen egy adott eszköz újra megfertőződhet egyazon vírussal annak ellenére, hogy már kezelve lett.

33 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. p. 399. 10.4. ábra

34 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. p. 400. 10.5. ábra

35 Barabási Albert László: A hálózatok tudománya. Budapest, Libri Könyvkiadó Kft., 2016. p. 401. 10.6. ábra

Amennyiben egy támadás romboló célú és a lefutása sikeres, olyan központi csomópontok kiesését is okozhatja, amely megszűnésével akár több működési folyamata is megállhat. Ilyen esetekre érdemes preventív módon különböző terveket (BCP,[36] DRP[37]) készíteni, amelyek egy rendszer kiesésekor útmutatást adnak a kritikus folyamatok működtetéséhez.

A preventív védelmi felkészülés és a kritikus infrastruktúrák kérdésköre

Az elmúlt évek, évtizedek technológiai fejlődése nemcsak a vállalati szektornak jelent újabb kihívásokat a védelem területén, de az államok számára is. A kritikus infrastruktúrák még inkább ki vannak téve a támadásoknak, és a bennük okozott károk még inkább kihatással vannak a társadalomra és annak működésére. Az internet és az információs technológia fejlődésével a kapcsolat mértéke ezek között a rendszerek között hatványozottan fokozódott.

A XXI. század egyik jelensége egy új típusú hidegháború kialakulása. Amellett, hogy az Észak-Koreában folyó atomkísérletek és a fegyverkezés eddig nem látott mértéket ölt,[38] sokkal aggasztóbbak lehetnek azok az államilag finanszírozott kiberbiztonsági kutatások, kísérletek, amelyek a háttérben zajlanak, és amelynek célja egy új típusú fegyver kidolgozása. Az elmúlt évek során több olyan esemény is történt, amely erre enged következtetni. Csak a nagyobb eseményeket figyelembe véve érdemes górcső alá venni az Iráni atomdúsító elleni Stuxnet esetét, az amerikai szivárogtatások kapcsán napvilágot látott különböző kibertámadásokra vonatkozó információkat, vagy az Oroszországgal összefüggésbe hozott Észtország[39] ellen indított túlterheléses támadást, az orosz–grúz kiberháborút.

Ezen kívül elengedhetetlen az információs hadviselés[40] megemlítése is, amelynek során jelen kontextusban az államok célja az, hogy más államok működését rejtett módon befolyásolják. Erre példaként említhető a közelmúltban történt 2016-os amerikai elnökválasztás esete. Sok feltételezés született azzal kapcsolatban, miszerint Donald John Trump elnök azért nyerhetett Hillary Clinton ellen, mert különböző módszerekkel befolyásolták a szavazókat.[41]

Észre kell venni tehát, hogy a kibertér egyre több lehetőséget biztosít a bűnözőkön kívül a nemzetállamok számára is az egymás ellenvívott csatározásra. Az ilyen jellegű

---

36 Business Continuity Plan = Üzletmenet folytonosság terv

37 Disaster Recovery Plan = Katasztrófa helyreállítási terv

38 http://index.hu/kulfold/2017/09/04/soha_ennyire_nem_allt_kozel_a_haboruhoz_eszak-korea_mint_most/ (Letöltés dátuma: 2017. 10.09.)

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

40 Szabó András: Az információs hadviselés és a hadtudomány. Hadtudomány VIII. évfolyam 4. szám (1998. december)

41 Kovács László – Krasznay Csaba: Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. Stratégiai Védelmi Kutató Központ (elemzések) / Center for Strategic and Defense Studies Analyses, 2017 (9), pp. 1–11.

támadások kapcsán meghatározni a támadó „személyét" szinte lehetetlen, ennek ellenére tényként kell kezelnünk azt, hogy az államok „kiber-fegyverkezésbe" kezdtek.

Vannak módszerek, amelyek segítik a víruskutatókat abban, hogy valószínűsítsék a támadó személyét egy kód kapcsán, azonban biztos módszer ennek meghatározására egyelőre nem ismert. A probléma kezelése kapcsán történnek előrelépések, de azok egyelőre se regionális, se nemzetközi szinten nem jelentenek megoldást. Ilyen kisebb mérföldkőnek tekinthető például a NATO által hozott döntés, aminek értelmében a kiberteret is hadszíntérnek nyilvánították, azonban ez a helyzet továbbra sem tisztázott. A nemzetközi jog[42] területe is további kívánnivalókat hagy maga után, ahol továbbra sem definiálták a kiberháború fogalmát és annak eseteit. De a jog kérdése mellett jelen tanulmány részeként egy másik kontextust kell megvizsgálnunk: a védekezés és a támadás lehetőségeit, a károkozások mértékét és valószínűségét.

A kritikus infrastruktúrák meghatározásánál minden nemzetállam vagy közösség törekedett arra, hogy megállapítsák, melyek nélkülözhetetlenek a társadalom, a kormányzás, a gazdaság stb. számára, illetve melyek tekinthetők kritikusnak működésük szempontjából, így külön figyelmet vagy védelmet érdemelnek. Magyarországon a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény mellékleteiben található táblázatok tartalmazzák általánosságban ezeket a rendszereket. Az energiaszektor mellett feltűnik a közlekedés, az agrárgazdaság, az egészségügy, a pénzügyi szektor, az infokommunikációs technológiák, a vízzel kapcsolatos infrastruktúrák, a kormányzat, a rendvédelem és a honvédelem, mint különböző ágazatok.

Vizsgálatunk szempontjából triviálisnak tekinthető, hogy hálózati kapcsolatrendszere ezeknek az ágazatoknak (egymástól való függőség tekintetében) majdnem teljes gráfot[43] alkot. Az energiaszektor által felügyelt üzemanyag és áramellátás biztosítása bármelyik másik ágazat szempontjából elengedhetetlen. Ezt a relációt ugyanúgy felállíthatjuk a többi ágazat kapcsán, amelyek legalább közvetett módon hatást gyakorolnak bármelyik másik ágazatra. Ezért ennek külön vizsgálatára nincs szükség, hiszen a logikai kapcsolatrendszer elfogadása után könnyen belátható, hogy egyik infrastruktúra kiiktatása kapcsán több másik elem működésében hibák keletkezhetnek, és a dominó elv alapján ez többszörös kárt indukál egy nemzetállam vagy közösség életében.

Sajnos a gyakorlatban a legtöbb nemzetállam esetében még a pontos kritikus infrastruktúra-hálózat vagy egyszerűen a hálózat elemeinek azonosítása sem történt meg. A preventív védekezés viszont drasztikusan csökkentheti a hálózatban okozott károkat. A fenti összefüggések felismerése tovább növeli a kritikus infrastruktúrák fontosságát és a védelmükre fordított erőforrás-igényeket.

A tárgyalt hálózatelemzési és IT-biztonsági kérdések legfőbb elemeként adoptálható a terjedések és betörések valószínűségének csökkentése. Ha egy kritikus infrastruktúrát

42 Lattmann Tamás: A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén https://www.academia.edu/8028014/A_nemzetközi_jog_lehetséges_szerepe_az_informatikai_hadviselés_területén (Letöltés dátuma: 2017. 10. 10.)

43 Olyan egyszerű gráf, ahol a pontok minden más ponttal kapcsolatban állnak.

támadás ér, olyan mértékű károkat okozhat, amelyek a preventív és rendszerszintű szemléletmód nélkül, akár helyrehozhatatlanokká is válhatnak. Ezért fontos, hogy egy ágazatra, mint hálózatra tudjunk tekinteni, mert ebben az esetben meghatározhatjuk azokat a gyenge pontokat, amelyek elvételével végzetesen meggyengül a hálózat, vagyis maga az ágazat működése és ezáltal a rendeltetésszerű feladat ellátásának folyamatossága. Példaként véve egy ország energia ellátását: a 2003 augusztusában bekövetkezett „nagy észak-amerikai" áramszünet[44] kapcsán bebizonyosodott, hogy milyen mérhetetlen károkat tud okozni egy közel 50 millió lakost érintő energetikai meghibásodás. A szakértők megállapítása szerint az áramellátó rendszer összeomlása külső támadás nélkül, dominóelv-szerűen következett be, aminek egyik jelentős oka az Egyesült Államok áramszolgáltatásának liberális voltából eredeztethető. A szövetségi államok szabályozásai egymástól függetlenek voltak, és ezáltal az együttműködés és preventív védelmi felkészülés sem volt megvalósítható az eltérő szolgáltatók esetében. Megállapították a szakértők azt is, hogy egy egységes szabályrendszer és katasztrófa-forgatókönyv segítségével a 4 napos visszaállási idő jelentősen csökkenthető, sőt, az áramkimaradás is elkerülhető lett volna. Ha hasonló példát keresünk magyarországi viszonylatban, akkor elengedhetetlen megemlítenünk Krasznay Csaba és Kovács László Digitális Mohács tanulmányát,[45] ahol bizonyítást nyer, hogy viszonylag kis erőforrás befektetésével célzott legfőképp kibertámadások segítségével mekkora károk okozhatók a kritikus infrastruktúrák rendszerében. A tanulmány fontos elemeként aposztrofálható a védekezés rendszerszintű szükségességére való felhívás.

Összefoglalás

A fent említett példák is bizonyítják azt, hogy a hálózatszintű szemléletmód elengedhetetlen. A jövőbe tekintve emellett egyértelmű, hogy a békeidőszaki klasszikus preventív védelmi felkészülés mellett foglalkoznunk kell azzal, hogy egy háborúban a fegyveres hadviselés mellett a kibertérben elkövetett műveletek is fontos szerepet fognak kapni.

Tanulmányunk fókuszában egy olyan, hálózatokra ható tényező állt, amely jelentősen befolyásolhatja mind a támadási, mind a védekezési stratégiákat. A hálózati vírusfertőzés egy új támadási mechanizmus esetét vázolja fel, amely magában hordozza az immunizálás védelmi lehetőségeit is. Egy univerzális biztonsági eljárás vagy stratégia megfogalmazására nincs lehetőség a hálózatok összetettségéből következően, de a téma elméleti körüljárása a felvetett kérdések egzakt megválaszolása helyett megmutatja az esetlegesen követendő irányvonalat, és rávilágít ezeknek a mechanizmusoknak a működésére.

---

44 Körmendi Krisztina – Solymosi József: A villamosenergia-ellátás zavarának kialakulása és okai a 2003. augusztusi „nagy észak-amerikai" áramszünet példáján. Hadmérnök, III (1), 2008, pp. 39–50.

45 Kovács László – Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság: Biztonságpolitikai Szemle, 2010 (1), pp. 44–56.

Bár általános védelmi rendszer megfogalmazására lehetőség nincs, az IT-biztonság emberi kockázatának csökkentése jelentősen elősegíti a védelmi stratégiák kialakítását. Egy vállalati vagy akár kritikus infrastruktúra kapcsolathálójának feltérképezése az egyik kulcsot jelentheti az IT-biztonság fokozására.

Figyelembe véve a kritikus infrastruktúrák összefonódását, fel kell térképeznünk azokat a rendszereket és az azokra vonatkozó biztonsági intézkedések összességét, amik lehetővé teszik, hogy a hálózatba rendeződött elemek kiesése során is a rendeltetésszerű működés és a szolgáltatások ellátása zavartalanul működhessen, vagy a helyreállítás ideje a lehető legrövidebbre redukálódjon. Ennek egyik legfőbb eleme az emberi tényezőből fakadó rizikófaktor csökkentése, ami a történelem által is igazoltan egészen addig a legnagyobb kockázatot fogja jelenteni, amíg a különböző vállalatok és infrastruktúrák teljesen nem függetlenednek tőlük, hiszen az emberi természet sosem lesz annyira kiszámítható, mint a szabályokra épülő gépek, programok, rendszerek működése.

FELHASZNÁLT IRODALOM

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

Barabási Albert László: Behálózva. Budapest, Helikon Kiadó, 2013.

Barabási Albert László: A hálózatok tudománya.Budapest, Libri Könyvkiadó Kft., 2016.

Barabási Albert László et al.: The large-scaleorganization of metabolicnetworks. Nature 407, 2000, pp. 651–654.

Birher Nándor – Bertalan Péter: Hálózatokban. Veszprém, Okter-Nobus Kiadó, 2014, pp. 60–62.

Buyya, Rajkumar et al.: Internet of Things (IoT): A vision, architecturalelements, and futuredirections. FutureGeneration Computer Systems, Volume 29, Issue 7, September 2013, pp. 1645–1660.

Erdős Péter – Rényi Alfréd: On The Evolution of Random Graphs. Magyar Tudományos Akadémia Matematikai Kutató Intézet Közlöny 5, 1960, pp. 17–61.

Fleiner Rita – Munk Sándor: Informatikai biztonsági útmutatók, kontrollok és szerepük az adatbázis-biztonság megvalósításában. Hadmérnök, VI (3), 2011, pp. 100–116.

Kovács László – Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság: Biztonságpolitikai Szemle, 2010 (1), pp. 44–56.

Kovács László – Krasznay Csaba: Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. Stratégiai Védelmi Kutató Központ (elemzések) / Center forStrategic and DefenseStudiesAnalyses, 2017 (9), pp. 1–11.

Körmendi Krisztina – Solymosi József: A villamosenergia-ellátás zavarának kialakulása és okai a 2003. augusztusi „nagy észak-amerikai" áramszünet példáján. Hadmérnök, III (1), 2008, pp. 39–50.

Lattmann Tamás: A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén https://www.academia.edu/8028014/A_nemzetközi_jog_lehetséges_szerepe_az_informatikai_hadviselés_területén (Letöltés dátuma: 2017. 10. 10.)

Mary Meeker, Internet Trends 2017 – CodeConference http://dq756f9pzlyr3.cloudfront.net/file/Internet+Trends+2017+Report.pdf (Letöltés dátuma: 2017. 10. 04.)

Milgram, Stanley: The Small-World Problem. PsychologyToday, vol. 1, no. 1, May 1967, pp. 61–67.

Szabó András: Az információs hadviselés és a hadtudomány. Hadtudomány, VIII. évfolyam 4. szám (1998. december).

Szádeczky Tamás: Információbiztonsági szabványok. Budapest, Nemzeti Közszolgálati Egyetem, 2014.

INTERNETES HIVATKOZÁSOK

http://index.hu/kulfold/2017/09/04/soha_ennyire_nem_allt_kozel_a_haboruhoz_eszak-korea_mint_most/ (Letöltés dátuma: 2017.10.09.)

JOGSZABÁLYOK

PPD 63 – 1998. május 22. Protecting America's criticalinfrastructures https://fas.org/irp/offdocs/pdd/pdd-63.htm (Letöltés ideje: 2017. 10. 04.)

Egyesült Államok, Uniting and Strengthening America, by Providing Appropriate Tools Requiredto Intercept and Obstruct TerrorismAct, 2001-es 107-56-os törvény, 1016-os szekció, más nevén a Kritikus Infrastruktúrák védelméről szóló 2001-es törvény https://www.selectagents.gov/resources/USApatriotAct.pdf (Letöltés ideje: 2017. 10. 04.)