Kovács László – Krasznay Csaba

Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint[1]

Életünk, legyen szó politikáról, gazdaságról vagy éppen kultúráról, nagyban függ azoktól az információs rendszerektől, amelyek sokszor láthatatlanul vannak jelen mindennapjainkban. Ugyanakkor egy-egy informatikai vagy kommunikációs rendszer kiesése, részleges vagy teljes működésképtelensége azonnal ráirányítja a figyelmet ezekre az infrastruktúrákra. 2009-ben Digitális Mohács címmel egy elképzelt forgatókönyvet vázoltunk fel annak bizonyítására, hogy szándékos támadások sorozatával valóban lehetséges-e komoly károkozás egy olyan, viszonylag fejlett infrastruktúrával rendelkező ország esetében, mint hazánk. Az azóta eltelt időben egy sor kormányzati lépés és számos jogszabály született, amelyek infrastruktúráink védelmének jogi és szervezeti alapjait hivatottak megteremteni. Ezért itt az idő, hogy megvizsgáljuk, ma mi a véleményük a szakembereknek, elegendők-e az eddigi lépések a védelem megteremtése érdekében. Így egy új forgatókönyvet vázoltunk fel, amelynek egyes lépéseit a szakemberek elé tártuk, és megkérdeztük, mit tennének az adott támadások esetén.

Kulcsszavak: *információ, infrastruktúra, kiber, támadás, védelem*

Kovács László – Krasznay Csaba: Digital Mohács 2.0: Expert Opinions on Cyberattacks and Cyberdefence

Our everyday life highly depends on information infrastructures which are invisibly present in our politics, economy or cultural life. However, partial or complete inoperability of communication systems and the loss of information immediately draw attention to those infrastructures. In 2009 a hypothetical scenario was outlined entitled Digital Mohács. The main idea of this scenario was to prove whether a series of deliberate attacks could cause serious damages in case of a country with a relatively developed infrastructure as Hungary. Since this scenario was issued, a series of governmental steps and several legislative acts has been made designed to ensure the legal and organizational basis for protection of critical infrastructures. Therefore, it is the time to examine what the opinion of experts is; whether the steps taken so far are sufficient for creating real and effective protection. That is why we have drawn up a new script and we asked experts what they would do in case of specific cyberattacks.

Keywords: *information, infrastructure, cyber, offense, defense*

1 A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Bevezetés

Közel nyolc évvel ezelőtt jelent meg a Digitális Mohács című forgatókönyv.[2] Ez a szcenário egy olyan elképzelt, egymással párhuzamosan elkövetett támadások sorozatát írta le, amelynek során azt vizsgálták a szerzők, hogy Magyarország kritikus infrastruktúrái, valamint kritikus információs infrastruktúrái milyen módszerekkel támadhatók, illetve ezeknek a támadásoknak milyen következményei lehetnek az ország különböző területeire, valamint az ott lévő alapvető szolgáltatásokra.

A forgatókönyv megalkotásának az egyik legfontosabb motivációját az adta, hogy 2009-ig, azaz a forgatókönyv felvázolásáig nem történt komoly előrelépés a kritikus infrastruktúra, illetve a kritikus információs infrastruktúra, vagy akár azok egyes elemei, mint például az infokommunikációs rendszerek védelmének érdekében. Született ugyan egy kormányhatározat a kritikus infrastruktúrák védelméről 2008-ban,[3] de a teljesen konkrét, részletekbe menő, a koordinált védekezést meghatározó, annak szervezeti és törvényi hátterét egyaránt megteremtő jogszabályok együttese még váratott magára.[4]

Ugyanakkor a világban számos helyről érkeztek negatív és egyben nagyon komoly figyelmeztető jelzések, hogy ezek a rendszerek igen nagy sérülékenységeket hordoznak magukban, és adott esetben, mint például 2007 tavaszán Észtországban, ezeket a sérülékenységeket egyes gazdasági vagy politikai csoportok, vagy akár egy ellenséges másik ország ki tudja használni. Így ezeken a sérülékenységeken keresztül egy teljes ország, sőt akár egy egész régió is támadható, beleértve a gazdasági, pénzügyi vagy akár a közigazgatási rendszereken át a védelmi szférát is, az ott működő rendszerek hosszabb vagy rövidebb ideig részben vagy teljes egészében működésképtelenné tehetők.

A Digitális Mohács-forgatókönyvhöz az alapinformációkat az interneten elérhető nyílt forrásokra támaszkodva gyűjtöttük össze. (Ez azt is jelenti, hogy ilyen információgyűjtést bárki el tud végezni, így ez magában hordozza az ártó szándékú potenciális elkövetők információhoz való hozzájutásának lehetőségét is.) A forgatókönyv egy olyan elképzelt támadássorozatot írt le, amelyben logikailag egymásra épülő pszichológiai műveletekkel, informatikai, valamint korlátozott fizikai támadásokkal hazánk infrastruktúráit, infrastrukturális elemeit korlátoztuk, illetve működésükben akadályoztuk. Elsőként egy pszichológiai műveletsort vázolt fel a forgatókönyv, amelyek negatív vagy álhíreken keresztül a lakosság széles rétegeihez eljuttatva – például az elektronikus médiumok informatikai támadásával, azokban valótlan híreket megjelentetve – befolyásolni lehet az embereket. Ezt követően a földfelszíni műsorszórás ellehetetlenítésével az egyre inkább manipulált internetes médiumok felé terelve a figyelmet, még nagyobb befolyásolást feltételezett a szcenário. Ezek a negatív hírek a pénzügyi és bankrendszer közelgő összeomlását vetítették előre, amelyekkel párhuzamosan a bankrendszer támadhatóságát, illetve kitettségét

2 Kovács László, Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság – Biztonságpolitikai Szemle,* 2010/1, 44–56. o.

3 *2080/2008. (VI. 30.) Korm. h. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról.*

4 Ugyanakkor meg kell jegyezni, hogy ez a 2008-as kormányhatározat volt az első, amely a kritikus infrastruktúra védelméről hazánkban ilyen magas szintű jogszabályként rendelkezett. Maga a kormányhatározat egy rendkívül hosszú és alapos közigazgatási egyeztetésen esett át, és egyik legnagyobb erényének a kritikus infrastruktúrák ágazatokba és alágazatokba való sorolása tekinthető.

vizsgáltuk. A következő támadási fázis az infokommunikációs szolgáltatások, ezen belül is az internet támadása volt. Ezt követte a közlekedés, elsősorban a budapesti tömegközlekedés, valamint a légi közlekedés támadása, illetve ezek támadhatóságának vizsgálata. Az olyan egyéb rendszerek támadásán kívül, mint például az egészségügyi információs rendszerek, megvizsgáltuk, hogy van-e realitása az energiaellátási rendszerek, ezen belül is a villamosenergia-rendszer támadásának. Az eredmény meglepő volt. Arra a következtetésre jutottunk, hogy önmagában informatikai támadásokkal nem, vagy csak részben lehet támadni a villamosenergia-szolgáltatást, viszont az internetről szerzett „ötletekkel" nagyon kis energiabefektetéssel, viszonylag kicsi, de nagyon jó helyen elkövetett fizikai támadásokkal a magyarországi villamosenergia-rendszer is megbénítható. Ugyanakkor pont ezek a támadások okozhatják a legnagyobb és legveszélyesebb rendszerkieséseket, amely a szolgáltatások összekapcsolása, valamint azok országhatárokon átívelő kiépítése miatt nemcsak Magyarországon, hanem nagy bizonyossággal az egész régióban beláthatatlan következményekkel járó áramkimaradásokat okozhatnak.

A forgatókönyv több szakmai fórumon bemutatásra került, majd tudományos publikáció formájában a *Nemzet és Biztonság* folyóiratban jelent meg. Mind a különböző helyeken és különböző hallgatóságnak megtartott nagyszámú előadásnak, mind a lap hasábjain megjelent tudományos cikknek komoly szakmai és médiavisszhangja volt. A szcenáriót, illetve egyes elemeinek összefüggéseiben történő magyarázatait, az azokból levonható következtetéseket az egyetemi oktatásban is megjelenítettük.

Jelen írás arra a keresi a választ, hogy egy a Digitális Mohács-forgatókönyvhöz hasonló, alapvetően elképzelt, de mégis viszonylag reális forgatókönyv egyes lépései esetén a terület szakemberei milyen válaszokat adnának, azaz elegendőek-e a korábban említett jogszabályi és szervezeti háttér kialakítása és működtetése során eddig tapasztalt védelmi megoldások.

A hazai kibervédelem fejlődése

A Digitális Mohács-forgatókönyv megjelenése óta eltelt időszakban hazánkban komoly jogszabályi és szervezeti változások történtek a kibervédelem területén.

A 2009-től eltelt közel nyolc év alatt a kormányzat és a jogalkotó is felismerte a kritikus infrastruktúrák és a kibertér fontosságát. Számos stratégia, törvény és alacsonyabb szintű jogszabály született az elmúlt időszakban, amelyek ma már megteremtik azt a szervezeti hátteret, amelyek garantálhatják a kritikus infrastruktúrák, a kritikus információs infrastruktúrák, valamint a kibertér biztonságát hazánkban.

Ennek megfelelően célszerű nagyon röviden ezeket számba venni és értékelni, mielőtt az új forgatókönyv egyes lépéseit, valamint az azokra adott szakértői válaszokat elemeznénk.

A kritikus infrastruktúrák védelmére irányuló kormányzati elgondolás első jogszabályban is rögzített lépése a már említett 2080/2008. (VI.30.) Korm. határozat volt, amely a Kritikus Infrastruktúra Védelem Nemzeti Programja címet viselte. Ebben a határozatban célozta meg a magyar kormány a legalapvetőbb teendőket és a felkészülés alapvetéseit a kritikus infrastruktúrák védelmének területén. Ne feledjük, hogy ezt megelőzően nem

született átfogó jogszabály erre a területre, pedig az infrastruktúráinkkal szemben már akkor is komoly kitettséggel rendelkeztünk. Ekkor született meg a kritikus infrastruktúra hazai hivatalos fogalmának meghatározása. A jogszabály, ahogy utaltunk rá, részletesen felsorolja és osztályozza a kritikus infrastrukturális ágazatokat és alágazatokat. A védelem konkrét és részletes, felelősöket is megjelölő feladatainak leírása azonban nem történt meg.[5]

2012-es év áttörést hozott Magyarországon azzal, hogy a Nemzeti Biztonsági Stratégiába kiemelt helyen mint veszélyforrás került be a kiberkihívások jelentette problémakör. Az új Nemzeti Biztonsági Stratégia rendkívül előremutató még ma is, hiszen államilag elfogadott, a nemzet biztonságát meghatározó stratégiai elvekben először találkozhattunk e terület ilyen szintű és kiemelt helyen történő kezelésével hazánkban. A stratégia lefekteti annak alapjait, hogy a nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására a koordinált védelem kialakítását, valamint az ezeken a területeken történő védelmi célú felkészülést meg kell kezdeni.[6] Ennek érdekében a stratégia megjelöli a kibertérben jelentkező, már meglévő és potenciálisan a jövőben jelentkező fenyegetések és kockázatok rendszeres felmérését és priorizálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködési lehetőségek kiaknázását.[7]

Szintén 2012-ben jelent meg a köztudatba röviden csak kritikusinfrastruktúra-törvény néven a bevonult jogszabály,[8] amely a terület egyik legjobban várt jogforrása volt. Ez a törvény egyrészt nagyon világos képet ad a kritikus infrastruktúrák ágazati és alágazati besorolásával kapcsolatosan, ugyanakkor csak utalásokat tartalmaz a kibertér különböző – nyilvánvalóan a kritikus infrastruktúrákra vonatkozó – területein megteendő védelmi lépésekről.[9]

Ezt követően a kormány 2013 elején fogadta el a Nemzeti Kiberbiztonsági Stratégiát.[10] Erre a stratégiára építve készült el az úgynevezett információbiztonsági törvény[11] szintén 2012-ban. Ez a törvény az egyik legfontosabb jogszabály a hazai kibervédelem (információbiztonság) területén, hiszen a közigazgatás és az állami szféra szereplőinek ez biztosítja az információbiztonsághoz, valamint a kibervédelemhez az egyik legfontosabb jogszabályi alapot. A törvény megalkotása után azonban a hazai kibervédelmi szervezetek meglehetősen heterogén módon, sokszor egymást átfedő feladat- és felelősségi körökkel dolgoztak. Így szükségessé vált a szervezeti struktúra világossá, átláthatóvá és nem utolsósorban hatékonyabbá tétele. Ennek megfelelően az Országgyűlés 2015 júliusában mó-

5 Kovács László: Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései. In: Nemeslaki András (szerk.): *E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek*. NKE, Budapest, 2014.

6 Kovács: *Az e-közszolgálat-fejlesztés…, i. m.*

7 *1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.*

8 *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.*

9 Meg kell jegyezni, hogy az Országgyűlés 2016-ban módosította a törvényt az egyes belügyi tárgyú törvények módosításáról szóló 2016. évi CXVI. törvénnyel, amely 2017. január 1-én lépett hatályba, és amely módosítás némileg érintette a kritikus ágazatok és alágazatok besorolását.

10 *1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.*

11 *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.*

dosította a törvényt. Ennek köszönhetően jött létre például az állami szféra informatikai incidens kezeléséért felelős Nemzeti Kibervédelmi Intézet (NKI) is.

Összefoglalva a hazai kibervédelem fejlődését, megállapíthatjuk, hogy nemcsak beértük Európát, hanem sok tekintetben meg is előztük azokat az intézkedéseket, illetve szervezeti kiépítést, amelyet az Európai Unió is csak a 2016 júliusában elfogadott úgynevezett NIS-irányelvekben határozott meg.[12]

Digitális Mohács 2.0: új támadások

2016 szeptemberében a Hétpecsét információbiztonsági egyesület szakmai fórumán került bemutatásra a Digitális Mohács 2.0 előadás.[13] Az előadásban felvázolt forgatókönyv az úgynevezett Table Top Exercise (TTX)[14] mintáját követte. A forgatókönyvben egy, napjainkban reális és sajnos teljesen elképzelhető politikai válság eszkalációs folyamatát, illetve annak egyes lépései, például a külföldről érkező informatikai támadások közül mutattuk be néhányat.

A felvázolt forgatókönyvben nem tértünk ki arra, hogy milyen stratégiai cél érdekében történnek a támadások. Ugyanakkor tudományos módszerekkel kívántuk mérni, hogy az elsősorban az információbiztonsággal és a kibervédelemmel foglalkozó szakemberek mit gondolnak egyrészt magáról a forgatókönyvről, másrészt a forgatókönyv egyes lépéseinek megvalósíthatóságáról, valamint mindezek tükrében a kritikus infrastruktúra-, illetőleg a kibertérvédelem hazai állapotáról. Ezért azt kértük a szakértőktől, hogy az előre összeállított és a számukra kiadott űrlapon jelezzék, hogy az általunk meghatározott válaszok közül melyiket választanák. Jelen tanulmány a kapott válaszokat elemzi.

A forgatókönyv

A Digitális Mohács 2.0 forgatókönyv egyes lépéseinek alapjául az a tény szolgált, hogy a 2009-ben felvázolt eredeti Digitális Mohács-szcenárióban leírt informatikai támadások mindegyikére volt nemzetközi példa az elmúlt közel egy évtizedben. Azt is tényként kezeltük, hogy a fegyveres konfliktusok, valamint a terrortámadások jelentős részénél megfigyelhető, hogy a kibertér, valamint az ott működő eszközök és rendszerek ma már természetes módon kerülnek felhasználásra a támadások során. Mindezeken túl a politikai küzdelmek jelentős részénél szintén markánsan megjelennek a kibertéri eszközök, legyen szó hamis hírekről, lejáratásról vagy egyszerű ellehetetlenítésről. Azt is megfigyelhetjük, hogy a kiberhadviselés egyre inkább szervezetszerű lesz, és, párhuzamosan a fizikai dimenzióban vívott fegyveres – kinetikus energián alapuló – küzdelmekkel, egyre nagyobb teret és szerepet kap. Ma már kiberhadviselési stratégiák jelennek meg a különböző országokban a katonai stratégiák mellett vagy azok részeként, mintegy bizonyítva a terület egyre inkább fokozódó jelentőségét.

12 *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.* (NIS-irányelvek). Ugyanakkor a NIS-irányelvek számos helyen érintik a hazai kibervédelem szervezeti és jogszabályi hátterét. Ezeknek a teljesítésére a következő két évben kell felkészülnie hazánknak is.

13 Lásd: Információvédelem menedzselése LXXIII. Szakmai fórum [online] 2016. 11. 16. Budapest. [2017. 02. 26.].

14 Table Top Exercise: elképzelt forgatókönyvre épülő realisztikus gyakorlat.

A forgatókönyvet négy egymásra hatással lévő, de mégis jól elkülöníthető fázisra (felvonásra) osztottuk.

Az 1. fázisban – a korábbi Digitális Mohács-szcenárióhoz hasonlóan – *pszichológiai műveleteket* vázoltunk fel. Ennek első részében, amelyet a *sejtetés* időszakának neveztünk, azt feltételeztük, hogy egy gyaníthatóan külföldi titkosszolgálat által támogatott blogon olyan hírek jelennek meg, amelyek a magyar kibervédelem állítólagos gyengeségéről tudósítanak. Ezt követően a blogon megjelenő hír a közösségi oldalakon is megjelenik, így a korábbi kedvelések miatt tízezrek látják, azaz ez a *terjesztési* fázis. A közösségi médiumok működési elveinek megfelelően következik a *megosztási* fázis, amely során az ellenérdekelt titkosszolgálat szakértői által létrehozott álprofilokon keresztüli megosztások miatt egyre több hírfolyamban jelenik meg a hír, amelyet folyamatosan osztanak tovább a közösségi oldalak felhasználói. Ezt a *kiemelés* fázisa követi, amely alatt a nagy megosztásszám miatt a bulvársajtó is elkezd a témával foglalkozni, így a mérvadó lapoknál is témává válik az „eredeti" hír, miszerint a kibervédelmi szervezetek nem képesek ellátni feladatukat Magyarországon.

A 2. fázisban *látványos informatikai támadásokat* feltételeztünk, amelyek – építve az 1. fázis pszichológiai műveleteinek közvetlen vagy közvetett hatásaira a technikai következményeken túl – erősítik az 1. fázis lélektani hatásait. Elsőként olyan *DDoS-támadásokat*[15] feltételeztünk, amelyek során bizonyos kormányzati weboldalak és az NTG[16] ellen túlterheléses támadások indulnak. A túlterheléses támadások következtében egyes szolgáltatások órákra elérhetetlenné válnak. Ezeket *defacement*[17] támadások követik, amelyek során önkormányzati és háttérintézményi weboldalakat törnek fel meg nem határozható elkövetők, és a kezdőlapokon Magyarországot fenyegető üzeneteket jelenítenek meg. Ezután tömeges adatszivárgás történik. Olyan adatbázisok jelennek meg az interneten, melyek az azokat közzétevők állítása szerint több tízezer magyar állampolgár személyes adatait tartalmazzák.

A 3. fázis *a politika befolyásolás*ának fázisa. Az elképzelt forgatókönyv szerint ekkor a Wikileaks, építve az első két fázis során megjelenő hírekre, magyar kormányzati e-maileket hoz nyilvánosságra, ráadásul #HunLeaks címmel a nemzetközi sajtó ráveti magát ezekre a hivatalosnak tűnő elektronikus levelekre. Sorra jelennek meg az ezeket az e-maileket elemző írások a nemzetközi sajtóorgánumokban. Ezt követően feltűnik a „magyar Snowden", aki jelentős mennyiségű minősített dokumentumot ad át egy oknyomozó újságírónak. Ezt a csomagot már erre az ügyre elkülönített speciális nemzetközi újságírócsapat elemzi. Mindezek után egy olyan *APT*[18] támadásra derül fény, amely egy létfontosságú rendszert üzemeltető cég számítógépeit támadja. A korábbi támadások hatására elrendelt

15 DDoS támadások: Distributed Denial of Service, azaz elosztott túlterheléses támadások. Ezek során olyan sok számítógép olyan sok helyről intéz lekérdezést a cél, azaz a megtámadott számítógép felé, amelyet az már kapacitás hiányában nem tud teljesíteni, így működése akadozni fog, majd leállnak a szolgáltatásai.

16 Nemzeti Távközlési Gerinchálózat. Az NTG-t a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. üzemelteti és fejleszti. Fő feladata a közigazgatás és az állami infrastruktúra hatékony, nagy teljesítményű infokommunikációs támogatása.

17 Honlap jogosulatlan átalakítása, azon sok esetben sértő, lejáró tartalomnak nem az üzemeltető vagy tulajdonos engedélyével történő elhelyezése.

18 APT: Advanced Persistent Threat: kifinomult, folyamatosan fennálló támadás.

vizsgálat egy kifinomult malware-t[19] talál egy közműszolgáltatónál, amelynek az elemzésekor kiderül, hogy ennek a malware-nek a célja komoly mennyiségű adatszerzés lehetett, és a vizsgálat azt is kideríti, hogy már legalább 2 éve fut ez a program a közműszolgáltató különböző gépein.

A 4. fázis az *infrastruktúratámadások* fázisa. Elsőként a telekommunikációs szolgáltatásokat támadják. A mobil- és VoIP[20]-szolgáltatások elleni támadások egyre nagyobb mértéket öltenek, így ezeknek a szolgáltatásoknak a többsége elérhetetlenné válik. Akadozik a kormányzat kommunikációja is. A védelem koordinálása lelassul, megakad. Ezt *pénzintézetek elleni támadások* követik. Az online bankolás szünetel a legnagyobb bankoknál, ahogy szünetelnek a nemzetközi pénzügyi tranzakciók is. Ezt követően újabb nagyarányú infrastrukturális támadások következnek be: elkezdődnek az *áramszolgáltatók elleni támadások*. Lokális (kerületi szintű) áramkimaradások lépnek fel, amelyek egyre nagyobb területen és egyre nagyobb számban érintik a lakosságot és a közintézményeket is.

E négy fázis tehát egy teljes támadási életciklust ír le, ugyanakkor természetesen ezeken kívül számos egyéb támadás is elképzelhető lenne.

A forgatókönyvünkben hangsúlyozni kívántuk, hogy – ellentétben az eredeti Digitális Mohács-forgatókönyvvel – elsősorban nem a támadások esetleges (elvi) következményeit kívántuk felmérni, hanem a szakemberek (támadási események által kiváltott) véleményeinek felmérésére koncentráltunk.

A felmérés módszertana és alapvetései

Vizsgálatunk módszertanául a kérdőíves felmérést választottuk. Közel 100 kérdőívet osztottunk ki a már említett szakmai fórumon. A kiosztott papíralapú kérdőívek közül 70 darabot töltöttek ki és juttattak el a résztvevők a fórum szervezőihez, akik ezeket elektronikusan rögzítették és adták át a számunkra.[21] A kérdőívek kitöltését természetesen név és pontos beosztás nélkül kértük. A kötelezően elvárt – a kitöltő szakemberre vonatkozó – adatok a következők voltak:

– szektor, ahol dolgozik: magán/állami;
– Ibtv.[22] alá tartozik-e: igen/nem;
– életkor;
– végzettség;
– szakvizsga;
– IT-felelős: igen/nem.

A válaszadók életkori megoszlása az 1. ábrán látható. Ezek az adatok jellemzők lehetnek a forgatókönyv egyes fázisánál feltett kérdésekre adott válaszok elemzésénél. Az világosan

19 Malware: malicious software, azaz rosszindulatú program.

20 VoIP: Voice over the Internet Protocol, azaz internetalapú telefonszolgáltatás.

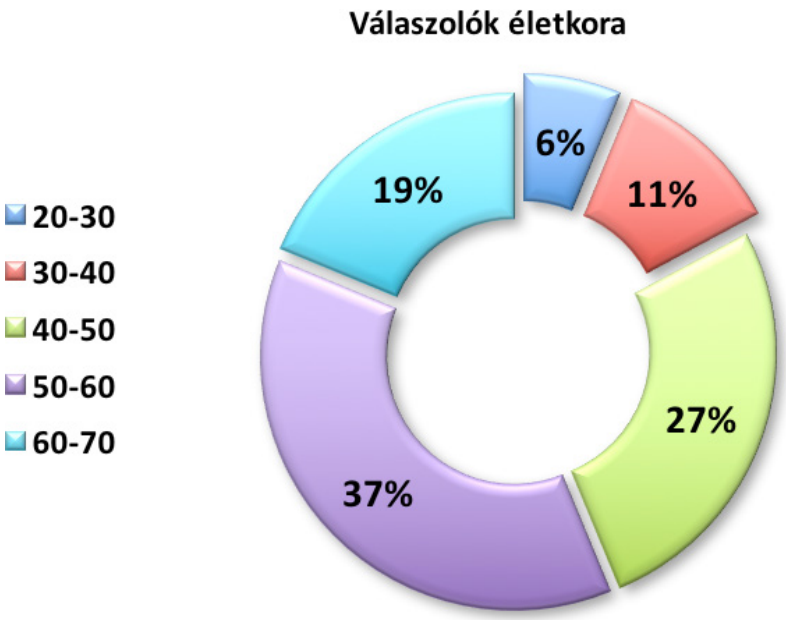
21 Természetesen tisztában vagyunk azzal, hogy a felmérés nem reprezentatív, és nem is felel meg teljesen sem a statisztikai, sem a tudományos kutatások módszertani követelményeinek. Ugyanakkor a beérkezett – szakmai közönség által – kitöltött kérdőívek elemzése, a kapott eredmények reményeink szerint választ adhatnak azokra a markáns kérdésekre, amely egy-egy informatikai alapú támadás során a védelem megalapozásának, illetve minőségének javításához szükségeltetnek.

22 Ibtv.: *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*.

látszik, hogy – bár, ahogy említettük, nem reprezentatív a felmérés – az információbiztonsági szakemberek jelentős része 40 év felett van. Ennek több oka lehet, amely a szakmai tapasztalat megszerzésének hosszú idejében, másrészt ezt megelőzően vagy ezzel párhuzamosan a megfelelő iskolai, szakmai és egyéb tanfolyami végzettség megszerzésében keresendő. Ugyanakkor az életkor meghatározhatja a szakértők biztonságról alkotott véleményét vagy akár a biztonságpercepciójukat is, valamint szakmai és élettapasztalataik alapján egészen más válaszokat adhatnak egyes kérdésekre, mint a lényegesebb fiatalabb generáció tagjai.

A válaszolók szektor szerinti eloszlása – azaz, hogy IT-felelős-e vagy sem az adott válaszoló – közel 50–50%-os arányt mutatott.

1. ábra: A válaszadók életkor szerinti eloszlása

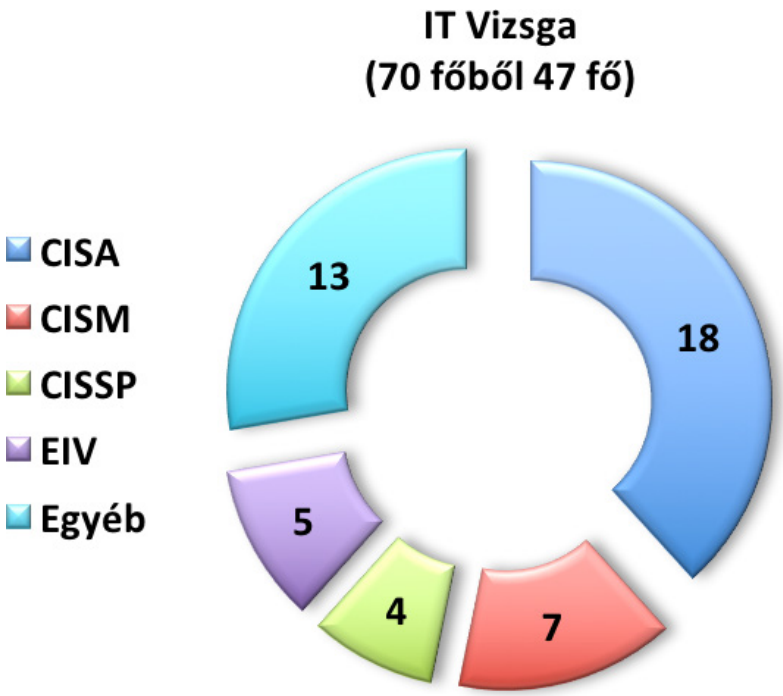


A szerzők saját szerkesztése

A kérdőívet kitöltőket arról is megkérdeztük, hogy rendelkeznek-e valamilyen információbiztonsági minősítéssel vagy vizsgával. Az erre a kérdésre adott válaszokat a 2. ábra mutatja be. A beérkezett válaszok alapján a szakértők közel kétharmada, azaz a 70 főből 47 fő rendelkezett valamilyen információbiztonsági vizsgával. Ezek megoszlása: CISA[23] vizsgával 18 fő, CISM[24] vizsgával 7 fő, CISSP[25] vizsgával 4-en, EIV[26] tanfolyami végzettséggel 4 fő, egyéb minősítő vizsgával pedig 13 fő rendelkezett.

23 CISA: Certified Information System Auditor, azaz minősített informatikai rendszer auditor.
24 CISM: Certified Information Security Manager, azaz minősített informatikai biztonsági menedzser.
25 CISPP: Certified Information Systems Security Professional, azaz minősített informatikai rendszerbiztonsági vezető.
26 EIV: elektronikus információbiztonsági vezető.

2. ábra. A válaszadók IT minősítései



A szerzők saját szerkesztése

A Digitális Mohács 2.0 forgatókönyv egyes fázisaira adott szakmai válaszok

Az 1. fázis, azaz a pszichológiai műveletek – sejtetés, terjesztés, kiemelés – esetén a következő válaszlehetőségeket biztosítottuk a felmérésben résztvevő számára:

a) Ilyen mendemondákkal nem kell törődni, semmilyen válaszlépést nem tennék.
b) A kormánnyal szimpatizáló blogokon és internetezőkön keresztül hasonló módszerekkel élő ellenkampányba kezdenék.
c) A Nemzeti Kibervédelmi Intézet nevében kiadnék egy közleményt, melyben cáfolnám az állításokat.
d) A magyar kormány nevében cáfolnám a híresztelést, egyben diplomáciai úton jelezném a gyanús nagyhatalom felé ellenérzéseimet.

A 3. ábra mutatja be a pszichológiai műveletek fázisában az egyes megoldásokat választók számarányát. A válaszadók jelentős része a „c" választ részesítette előnyben, azaz a Nemzeti Kibervédelmi Intézetben látja a megoldás kulcsát a pszichológiai műveletek kezelésére. Ugyanakkor a második legtöbbet választott megoldás az internetes ellenkampány, amelynek során a szakértők az internetezők segítségét is felhasználnák.

3. ábra. 1. felvonás: Pszichológiai műveletek

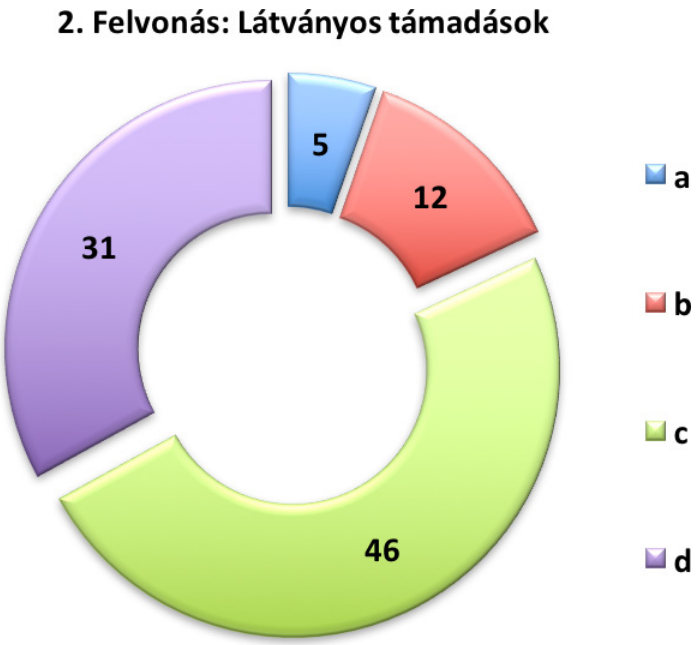
A szerzők saját szerkesztése

A 2. fázis, azaz a látványos támadások – DDoS-támadások, defacement-támadások, tömeges adatszivárgás – során a következő válaszlehetőségeket adtuk meg:

a) Ezek jelentéktelen támadások, hatásuk ideiglenes, így semmilyen különleges intézkedést nem hoznék. A sajtóval nem foglalkoznék.
b) Decentralizáltan, a támadások által érintett szervezetekre fókuszálva elkezdeném az elhárító munkálatokat. A sajtót az érintett szervezetek kezelik.
c) A Nemzeti Kibervédelmi Intézet vezetésével végezném az elhárítást, egyben bizonyos műszaki intézkedések mentén kiterjedtebben kezdenék el a további potenciális támadásokra figyelni. A sajtót az NKI kezeli.
d) Összehívnám a Nemzetbiztonsági Kabinetet, ahol egy műveleti törzset állítanék fel, így a műszaki intézkedések mellett egyéb hírszerzési és belbiztonsági tevékenység folytatása is lehetővé válik. A sajtót a kormányszóvivőre bíznám, egyben megnevezném a gyanítható elkövető országot.

A 2. fázis során lehetséges megoldásokat választók szám szerinti eloszlását mutatja a 4. ábra. Világosan látszik, hogy hasonlóan az 1. fázishoz, azaz a pszichológiai műveletek kezeléséhez, a látványos – alapvetően informatikai – támadások során is a Nemzeti Kibervédelmi Intézetben látják a megoldást a válaszadó szakemberek. Ennek során az NKI műszaki intézkedéseket (informatikai védelmi megoldások), valamint a sajtón keresztül a lakosság megnyugtatását is végzi.

4. ábra. 2. felvonás: Látványos támadások



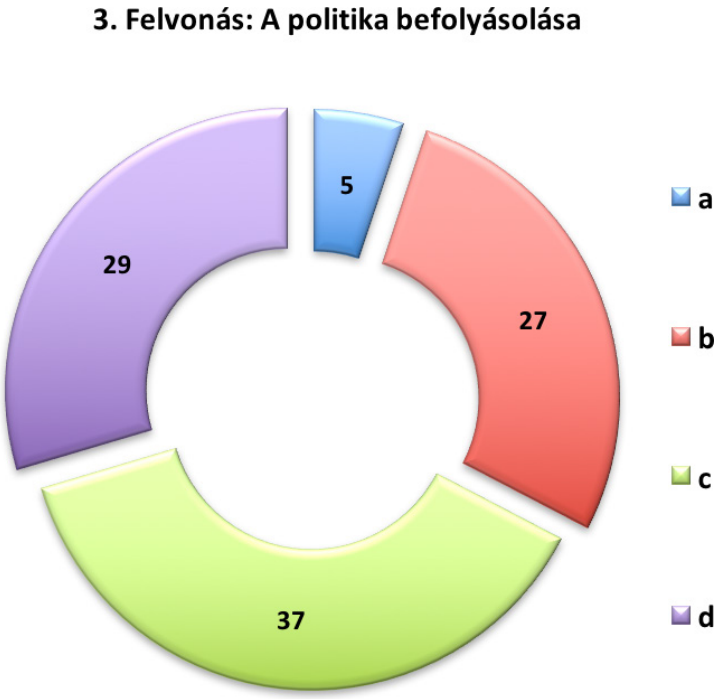
A szerzők saját szerkesztése

A 3. fázis, azaz a politika befolyásolása során – Wikileaks-szivárogtatás, a „magyar Snowden" megjelenése, APT-támadás egy létfontosságú rendszerelemnél – a következő válaszok közül választhattak a szakértők:

a) Mivel az incidensek valószínűleg egymástól függetlenek, egyedi, testreszabott választ adnék rájuk.
b) Az esetek valószínűleg összefüggnek, titkosszolgálati tevékenységgel próbálnám megoldani a kialakult helyzetet. A sajtó kezelését a szakértőkre és az NKI-re bíznám.
c) Mivel az esetek egyértelműen összefüggnek, a Nemzetbiztonsági Kabineten belül működő operatív törzs hangolja össze a válaszlépéseket. A sajtóban nevesíteném az elkövető államot.
d) Mivel jelen támadássorozat aláássa Magyarország biztonságát, az Európai Unió és a NATO diplomáciai és szakértői segítségét kérném!

Az 5. ábrán látható a 3. felvonásra adott válaszok megoszlása. A válaszokból kitűnik, hogy a szakértők egyre komolyabb és egyre hangsúlyosabb válaszokat kívánnak adni, ahogy nő a támadások intenzitása és volumene. Mivel ebben a fázisban már komoly informatikai támadásokat feltételeztünk, amelyek következményei politikai síkon is megjelennek, ráadásul nagy valószínűséggel nemcsak Magyarországon, hanem szövetségesi – Európai Unió-, illetve NATO-szinten is, a szakértők válaszai arra engednek következtetni, hogy már nem elegendő a probléma helyi kezelése, hanem szükség van kormányzati (például Nemzetbiztonsági Kabinet), illetve EU-s megoldásra.

5. ábra. 3. felvonás: A politika befolyásolása

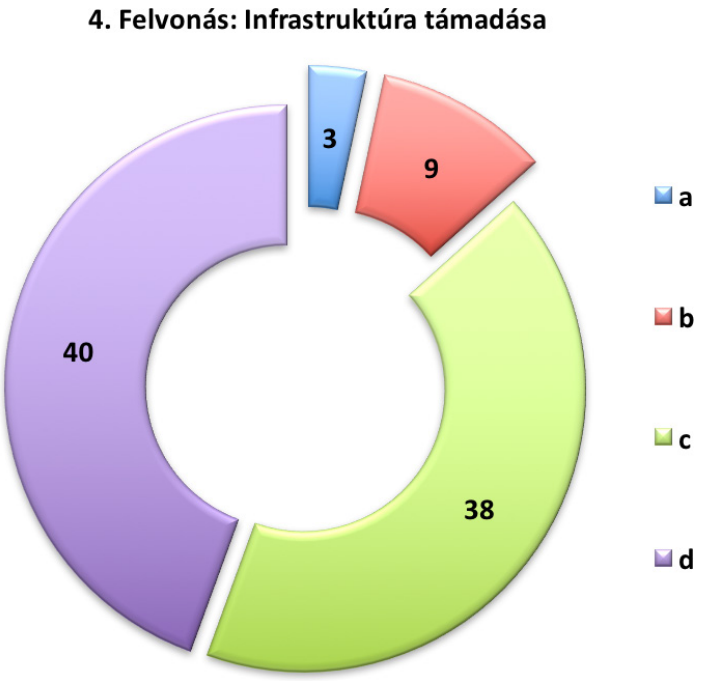


A szerzők saját szerkesztése

A 4. fázisban, azaz az infrastruktúra támadásának fázisában, ahol a telekommunikációs szolgáltatások, a pénzintézetek, valamint az áramszolgáltatók támadása is bekövetkezik, a következő lehetőségek közül kértük a szakértők választását:

a) Ezek elszigetelt támadások, de lehet, hogy csak a rendszerek egymástól független, véletlen meghibásodásai, hatásuk ideiglenes és csak korlátozott lehet, így semmilyen különleges intézkedést nem hoznék.
b) Decentralizáltan, a támadások által érintett szervezetekre fókuszálva elkezdeném az elhárító munkálatokat és a szolgáltatások minimális szintű visszaállítását. A sajtót az érintett szervezetek kezelik.
c) Mivel egyértelmű, hogy a korábban talált malware-hez kapcsolódó, célzott támadásokat látunk, a Nemzeti Kibervédelmi Intézet vezetésével végezném az elhárítást, egyben bizonyos műszaki intézkedések mentén kiterjedtebben kezdenék el a további potenciális támadásokra figyelni. A sajtót az NKI kezeli.
d) A Nemzetbiztonsági Kabineten belül működő műveleti törzs kezelné a helyzetet, így a műszaki intézkedések mellett egyéb hírszerzési és belbiztonsági tevékenység folytatása is lehetővé válik. A sajtót a kormányszóvivőre bíznám. EU és NATO segítséget kérnék diplomáciai és szakértői szinten.

6. ábra. 4. felvonás: Infrastruktúra támadása



A szerzők saját szerkesztése

A 6. ábrán látható a 4. fázisra, azaz az infrastruktúra-támadási fázisra adott válaszok megoszlása. A kapott válaszokból kitűnik, hogy a szakértők ebben a támadási fázisban is kiemelt szerepet szánnak a Nemzeti Kibervédelmi Intézetnek. Mivel azonban az olyan infrastruktúrát is támadás éri, mint például a villamosenergia-ellátás, amely támadásnak nemcsak hazai, hanem regionális következményei is vannak, ezért szükséges a nemzetközi együttműködésben végzett és koordinált védelmi megoldások szervezése és végrehajtása.

Összefoglalás, következtetések

2009 óta, azaz a Digitális Mohács eredeti forgatókönyvének elkészítése és megjelenése óta hazánk hatalmas lépéseket tett az információbiztonság, a kibervédelem, illetve a kritikus infrastruktúra és a kritikus információs infrastruktúra védelem különböző területein. Számos, ezeket a területeket meghatározó védelmi stratégia és jogszabály született. Kialakult az a szervezeti háttér, amely a kibertér biztonságát hivatott ellátni mind a közigazgatás, mind a kritikus infrastruktúrák területén, mind pedig a védelmi szférában. Megszülettek azok az alapvető szabályzók, amelyek hiánya 2009-ben még forgatókönyvünk megalkotásának egyik fő mozgatórugója volt.

Az elmúlt közel egy évtizedben a terület mind a kutatók mind a politika figyelmének középpontjába került. Amíg korábban a kibertér, az ott folyó tevékenységek, és még inkább az olyan kifejezések, mint például a kiberhadviselés, nagyon futurisztikusnak tűntek, addig ma ezek egyre inkább a mindennapjaink részévé válnak.

A mindennapi védelmi munka során a nemzetközi kapcsolatok kiépítése megkezdődött, hiszen ahogy forgatókönyvünk egyes lépéseinél a szakértők által adott válaszokból is kitűnik, nemzetközi kapcsolatrendszer nélkül nem lehetséges hatékony kibervédelem.

Ugyanakkor továbbra is komoly a függőségünk az infrastruktúráinktól. Ennek pedig az a sajnálatos velejárója, hogy amíg azok nem 100%-ban biztonságosak, addig egy jól felépített, összehangolt támadássorozattal szemben nem vagyunk teljesen biztonságban mi magunk sem. Ezt látványosan támasztja alá a leírt vizsgálatunk is, mert a Digitális Mohács 2.0 forgatókönyvben szereplő támadások a szakemberek szerint reálisak, potenciálisan bekövetkezhetnek.

Mindezeknek megfelelően olyan, az elmúlt években már számos alkalommal elhangzott, de sajnos továbbra is érvényes általános, a védelmet növelő, de eltérő módszereket kell hangsúlyoznunk, mint például az információbiztonsági tudatosság növelése, amelyet az egyébként szintén fejleszteni szükséges kibervédelmi szervezetek feladatául is kell szabni. További védelmi megoldást kell jelenteniük – függetlenül a gazdaságossági megfontolásoktól – az alternatív, vészhelyzetben is működő infrastruktúráknak, vagy legalábbis ezek egyes elemei kiépítésének, fenntartásának.

Mindezeken túl továbbra is hangsúlyoznunk kell a koordinált, centralizált védelem eszközrendszerének erősítésére tett megoldásokat. Ezt igazolja az az eredményünk, mely szerint a felvázolt forgatókönyvben szereplő támadások intenzitásával növekszik a szakemberek igénye a központi (állami) incidenskezelésre, mely során a különböző támadások kezelésében a szakma a Nemzeti Kibervédelmi Intézet szerepét kiemelt jelentőségűnek látja.

Ugyanakkor a szervezetrendszer erősítése megköveteli, hogy a közigazgatás, a piaci szereplők, valamint az akadémiai szféra a már megkezdett – a kiberteret és az ott elvárt biztonságot fő kérdésként tárgyaló – párbeszéde folytatódjék.

FELHASZNÁLT IRODALOM

1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

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

2080/2008. (VI. 30.) Korm. h. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Kovács László, Krasznay Csaba: Digitális Mohács: egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság – Biztonságpolitikai Szemle,* 2010/1. 44–56. o.

Kovács László: Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései. In: Nemeslaki András (szerk.): *E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek.* NKE, Budapest, 2014.