NB10_01_bel.qxd 2010.02.15 12:22 du. Page 44

Kovács László – Krasznay Csaba

Digitális Mohács

Egy kibertámadási forgatókönyv Magyarország ellen

Jelen tanulmány azokat a rendszereket kívánja bemutatni, amelyek a leginkább támadhatók és a leginkább sérülékenyek egy összehangolt információs támadás esetén hazánkban. Szerzőinek az a célja, hogy felhívják a figyelmet: hazánk is komoly veszélyben van, amelyet nem lehet túlértékelni.

Az elmúlt években folyamatosan kapunk híreket arról, hogy egy-egy informatikai rendszer kiesése milyen károkat okozott egy adott ország normális működésében. A komoly had-, biztonság- és informatikai kultúrával rendelkező országok éppen ezért a 21. század elejének egyik legkomolyabb kihívásaként kezelik a kritikus információs infrastruktúrák védelmének vagy éppen támadásának kérdését. Tanulmányok sora elemzi, hogy milyen láncreakciót válthat ki egy kritikus információs rendszereket érintő átfogó – informatikai és fizikai támadásokat is magába foglaló – cselekménysorozat. Magyarországon ilyen elemzések eddig nem láttak még napvilágot, noha a kockázatok hasonlóak, mint minden fejlett vagy akár fejlődő ország esetén.

Az alábbiakban megkíséreljük felvázolni egy olyan kritikus információs infrastruktúrákat érő támadás forgatókönyvét, mellyel akár napokig tartó működési zavarok kelthetők hazánkban. A szcenárió az utóbbi években különböző országokban végrehajtott valós támadások elemzésével alakul ki. A végrehajtáshoz szükséges információk mindegyike nyílt forrásból származik, amely mindenki számára rendelkezésre állhat. A támadások mindegyike aránylag kis költséggel, kevés ember bevonásával végrehajtható. Ugyanakkor ezen akciók legnagyobb kockázata pontosan ebben áll.

Tanulmányunknak nem célja a tippadás vagy ötletek gyártása, csupán megjelenítünk egy olyan lehetséges folyamatot, mely akár meg is történhet. Ennek megfelelően nem konkrét támadási recepteket mutatunk be, hanem azoatk a kritikus rendszereket vagy ezek egyes pontjait, amelyek hazánkban információs módszerekkel támadhatók és sebezhetők.

Kitekintés

1526. augusztus 26-án Magyarország taktikai, stratégiai, információszerzési és nem utolsósorban belső csatározások miatt gyakorlatilag másfél óra alatt elesett. Ez az esemény hazánk történelmi emlékezetében tragédiaként él mind a mai napig.

Napjainkban az észak-atlanti szövetség és az Európai Unió tagjaként ilyen történelmi korokon is átnyúló tragédia nem fordulhat elő még egyszer, hiszen maga a szövetségi rendszer nagyfokú védelmet és ezzel együtt szilárd alapokon nyugvó biztonságot jelent.

Addig azonban, amíg a hagyományos támadások és konfliktusok tekintetében nagy

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 45

bizonyossággal kijelenthető a védelem és a biztonság, addig a kibertérről, ami főleg, de nem kizárólag az internetet jelenti, még nem mondható el ugyanez. A kibertér ma hazánkban, hasonlóan a legtöbb fejlett infrastruktúrával rendelkező országhoz, védtelennek tekinthető. Bár léteznek nagyon jó védelmi intézkedések, amelyek az egyes önálló kritikus infrastruktúrákat kielégítően védik, a határtalan és korlátlan hálózatok kölcsönös függéseket alakítottak ki, melyek hatásait nem vagy nem kellően vizsgálták még. Emiatt a mohácsi tragédia újra megismétlődhet a virtuális térben. Bár pusztán az informatikai rendszerek támadásával emberéletekben nem vagy csekély kár eshet (közvetett hatásként), de a gazdasági és ennek következményeként a politikai károk felbecsülhetetlenek.

A kritikus infrastruktúra fogalma a 2080/2008. kormányhatározat szerint a következő: „Kritikus infrastruktúra alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúraelemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.” A kritikus információs infrastruktúrák az Európai Unió Zöld Könyve szerint „azon infokommunikációs rendszerek, melyek magukban kritikus infrastruktúrák, vagy ilyenek működéséhez elengedhetetlenül szükségesek”.

A kormányhatározat tíz ágazat 43 alágazatát sorolja a kritikus infrastruktúrák közé, melyek mindegyike, kivétel nélkül, kisebb vagy nagyobb mértékben függ az információs rendszerektől. Ezek az információs rendszerek célpontjai lehetnek az információs hadviselésnek (katonai terminológiával élve: információs műveleteknek), amely magába foglalja az elektronikai hadviselést, a számítógép-hálózati műveleteket, a pszichológiai műveleteket, a megtévesztést és a műveleti biztonságot. Az alábbi megtörtént események ezek mindegyikét felvonultatták.

2007. április 27-én Észtország kritikus információs infrastruktúráit érte külső, elsősorban elosztott túlterheléses *(Distributed Denial of Service – DDoS)* támadás, melyet tömeges levélküldés *(spam)* és weboldalak megváltoztatása *(deface)* egészített ki. A kiváltó ok egy szovjet hősi emlékmű eltávolítása volt. A főbb célpontok az észt parlament gépei, bankok, minisztériumok, napilapok és elektronikus hírközlő szervezetek voltak. A támadás elkövetését 2009-ben egy orosz hazafias csoport vállalta magára. Az akció mind Észtországot, mind a NATO-t felkészületlenül érte, pedig kivitelezéséhez csekély erőforrásokra volt szükség. Egyes feltételezések szerint a támadás azért ért véget, mert a támadók pénze elfogyott, és nem tudták tovább bérelni a feketepiacon elérhető informatikai erőforrásokat *(botneteket).* Ez az esemény vezetett oda, hogy ma már komolyan veszik a számítógéppel, interneten végrehajtott támadásokat, hiszen egy hasonló méretű provokáció például az USA-ban hatványozottabban nagyobb károkat okozott volna.

2008 augusztusában a pekingi olimpia alatt tört ki az grúz-orosz–grúz háború. A háború során mindkét fél intenzív információs csatát vívott, bevetve az internetet is. Ez azért meglepetés, mert mindkét ország arányaiban szegényes internetes hálózati infrastruktúrával rendelkezik. Az elsődleges célpontok az internetes hírforrások voltak. A grúz kormány blokkolta az

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 46

orosz weboldalakat Grúziában, így téve lehetetlenné az orosz hírforrások elérését. Válaszként az orosz fél ellehetetlenítette a grúz féltől érkező tájékoztatást a világ többi része felé. Ezt egészítették ki folyamatos hackertámadások orosz, grúz, dél-oszét és azeri weboldalak ellen. A konfliktus tanulsága, hogy mindkét fél bevetette a számítógépes támadásokat egy valódi háború során. Ennek alapján kijelenthető, hogy a hagyományos hadviselés részeként számolni kell az internetes hadviseléssel is.

2009 áprilisában informatikai kémek több terrabyte-nyi tervezési adatot loptak el az Egyesült Államok legdrágább fegyverrendszerével, a 300 milliárd dollár költségvetésű *Joint Strike Fighterrel* kapcsolatban. Hasonló adatlopást észleltek a légierő légiforgalmi irányítási rendszeréből is. A támadások 2007-ben kezdődtek, és 2008-ig folytatódtak. A kémek titkosították az ellopott adatokat, így nehezítve meg a nyomozók – a lopás pontos mértékének megállapítására irányuló – munkáját. Azt a tényt, hogy a vadászgéppel kapcsolatos adatok kémekhez kerültek, először Joel Brenner, az USA akkori kémelhárítási vezetője *(National Counterintelligence Executive)* árulta el. Brenner aggályait fejezte ki azzal kapcsolatban, hogy ha a kémek átvehetik az irányítást a légiforgalmi irányítási rendszerekben, „a vadászgépek pilótái többet nem bízhatnak a radarokban". A behatolás mögött Kínát sejtik, mely 2003 óta bizonyíthatóan folyamatosan betöréseket követ el az USA kormányzati rendszereibe. A betörések többsége azonban felderítetlen marad. Gyaníthatóan Kína (és más országok) folyamatosan élnek ezzel a fegyverrel, feltételezhetően Magyarország ellen is. A támadások célja az információgyűjtés, esetleges konfliktus esetén a rombolás és az információs rendszerek működésének ellehetetlenítése.

2009 júliusában dél-koreai magán- és kormányzati oldalakat ért DDoS-támadás. A célpontok között megtalálhatók voltak a már hagyományosnak mondható bankok, az elnök weblapja, a Koreában állomásozó amerikai csapatok honlapjai, és hírportálok, de ezek mellett például online aukciós portált is célba vettek a támadók. Az akció során amerikai weblapok is célkeresztben voltak, de ezekre már nem jutott elég kapacitás. A feltételezések szerint észak-koreai vagy velük szimpatizáló csoportok követték el a támadásokat. Ez azért aggasztó fejlemény, mert bizonyítja, hogy néhány ember, különösebb hadászati tudás nélkül, akár egy informatikailag fejletlen államból is képes fennakadásokat okozni egy másik, informatikailag fejlett országban.

Az incidensek sorát hosszan lehetne folytatni, szinte minden hétre jut egy olyan esemény, mely egy kritikus információs infrastruktúrát érint. Magyarországon egyelőre nem került napvilágra olyan incidens, mely külső támadás eredménye lett volna, de 2009-ben több olyan informatikai hiba is bekövetkezett, mely az adott kritikus információs infrastruktúra működését megakasztotta. Ez emberek tíz- és százezreinek okozott nehézséget, a sajtó kiemelten foglalkozott velük, és jelentős presztízsveszteséget jelentett az üzemeltető intézménynek. Magyarországnak is van tehát keserű tapasztalata az IT-rendszerek leállásának következményeivel kapcsolatban, de a direkt, összehangolt támadások hatása – egyelőre – elképzelhetetlen.

Amerikai forgatókönyv

2002-ben a Gartner tanácsadó cég és a US Naval War College felkérte négy iparág (elektromos hálózat, telekommunikáció, pénzügyi szolgáltatások, internet) szakem-

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 47

bereit, hogy tervezzenek olyan forgatókönyveket, melyekkel a saját iparáguk működése ellehetetleníthető. A feladat szerint terroristatámadást kellett szimulálni a kor technológiai eszközeinek felhasználásával. A támadó csapatok maximum öt főből állhattak. Fizikai támadásokat csak minimálisan lehetett felhasználni. A támadásra iparáganként 50 millió dollárt biztosítottak virtuálisan a gyakorlat szervezői. A csapatoknak először a stratégiai tervezést kellett végrehajtani, melyet a felkészülés és a felderítés követett, majd a támadás és ellentevékenység megszervezése volt a feladat, végül felül kellett vizsgálni az eredményeket.

A forgatókönyv hatásai megdöbbentőek voltak. A szakemberek olyan irányokat vázoltak fel, melyekkel mind a négy iparág, és rajtuk keresztül az USA gazdasága is jelentős veszteségeket szenvedhetne. A villamosenergia-ellátásban távoli támadásokkal helyi kiesések okozhatók, teljes kimaradás nem. Viszont néhány jól célzott hagyományos robbantással, melyek nagyfeszültségű vezetékek ellen irányulnak, valamint az emberi hiszékenységet alapul vevő *social engineering* támadásokkal, melyekkel hozzá tudnak férkőzni a kritikus IT-rendszerekhez, akár nagyobb területek is áram nélkül maradhatnak. Az ipari irányító rendszerek (SCADA-rendszerek) különösen védtelennek tűnnek informatikai szempontból. A pénzügyi rendszereknél ezek heterogén felépítése miatt a tömeges károkozás kockázata kicsi, de ha mégis sikerül, akkor az USA teljes gazdasága megbénulhat. Az internetes infrastruktúra támadásához a szakértők olyan megoldást találtak, melyek kísértetiesen hasonlítanak napjaink botnet hálózataihoz, melyeket az előzőleg felsorolt támadások mindegyikénél igénybe vettek. A távközlési hálózatok szakértői pedig már a szimuláció megkezdése előtt tudták, hogy rendszerük sérülékeny és teljes mértékben megbénítható. Az iparág ugyanis sok egyéni megoldást használ biztonsági megoldások nélkül.

Magyarországi kibertámadási forgatókönyv

Az események láncolatának bemutatása előtt hangsúlyoznunk kell, hogy informatikai eszközökkel végrehajtott támadásokkal már ma is komoly károk okozhatók, azonban ezek az ország egész lakosságára és gazdaságára vonatkoztatva feltételezhetően rövid ideig tartó, részleges fennakadásokat jelentenének csak. Akkor azonban, ha az informatikai támadásokat kiegészítik az információs rendszerek egyes – jól megválasztott – elemei ellen végrehajtott fizikai támadások, akkor a kár óriási lesz. Ebben az esetben a megtámadott rendszerek, és közvetett módon, azok egymástól való kölcsönös függősége miatt számos más rendszer működésképtelenné válik néhány óráig vagy akár több napig, több hétig is. Ebben az esetben a probléma már nemcsak hazai vonatkozású lesz, hanem nemzetközivé is válik, hiszen nagyon kevés rendszertől eltekintve ezek országhatárokon átnyúló felépítésű hálózatok, amelyek ráadásul nemcsak egymás fizikai működésétől függnek, hanem szolgáltatásaikban is nagyban egymásra vannak utalva.

Számos bekövetkezett támadás elemzésével és értékelésével, valamint a vázolt amerikai szcenárió tapasztalatainak felhasználásával a Digitális Mohács-támadás lehetséges forgatókönyvét három egymást követő részre osztottuk.

Az első rész a felderítés és az információszerzés. A támadásokat megelőzően a majdani támadóknak szükséges a sebez-

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 48

hető és sérülékeny pontok behatárolása. Tapasztalataink szerint ez az információgyűjtés elvégezhető kizárólag nyílt források felhasználására támaszkodva is. Forgatókönyvünk összeállításakor a nyílt források közül is csak az internetet, illetve annak e célra történő felhasználhatóságát vizsgáltuk. Véleményünk szerint egy – az információs rendszerek elleni – támadáshoz, illetve támadássorozathoz megfelelő mennyiségű és minőségű adatok szerezhetők az internet segítségével anélkül, hogy bármilyen titkos vagy védett rendszerbe informatikai betörést kellene végrehajtani.

A második részben – a felderítést követően – pszichológiai műveletek végrehajtására kerülhet sor, amelyek jól tetten érhetők a legtöbb terrorista jellegű támadás elsődleges céljai között. Bár jelen forgatókönyv nem nevez meg konkrét elkövetőket vagy elkövetői csoportokat, ezek számára a támadások pszichológiai hatásai figyelemre méltóak lehetnek. Már ekkor is jelen lehetnek információs támadások – például hamis hírek elhelyezés online hírportálokon –, amelyek felhívják a figyelmet a közelgő támadásokra. Ennek komoly jelentősége van, hiszen naponta tapasztaljuk, hogy a médiában bemutatni egy-egy informatikai támadást igen nehéz feladat, ennek következtében számos alkalommal még a sikeres támadásokat és azok következményeit is elhallgatják a megtámadott rendszerek üzemeltetői. Ebben élen járnak a bankok, bár egy-egy ilyen támadás az ő esetükben (is) komoly anyagi veszteséget okozhat – akár közvetett módon, például bizalomvesztés következtében. Így többékevésbé érthető, ha nem vagy nem szívesen ismertetik az ilyen eseteiket. Ugyanakkor azt is el kell mondani, hogy a kritikus ágazatok közül éppen a pénzügyi szektor, ezen belül is a bankok azok, amelyek a lehető legtöbb figyelmet fordítják a fizikai védelem mellett az információs rendszereik védelmére.

A harmadik, egyben a legfontosabb fázis a kritikus információs infrastruktúrák komplex támadásának megtervezése és végrehajtása a megszerzett adatok és információk alapján. Mindezeknek megfelelően a Digitális Mohács-forgatókönyv a következő sorrendben határozza meg a megtámadni kívánt célokat:

– elektronikus média;
– műsorszórás;
– internetes média;
– pénzügy;
– közlekedés;
– telekommunikáció;
– internet;
– villamos-energiaszolgáltatás.

Elektronikus média

Első támadási célpont tehát az elektronikus média. A különböző kereskedelmi és közszolgálati médiumok természetesen ma már számítógépeket alkalmaznak a műsorok szerkesztésére és a műsormenet biztosítására. Ezek támadhatóak informatikai eszközökkel, ráadásul ezek a médiumok internetes oldalai is komoly látogatottsággal bírnak. Az adásmenetbe való beavatkozás jelentheti az adás teljes leállítását is, de például a képernyőkön lévő információcsíkok hamis hírekkel történő megjelenítése sem elképzelhetetlen. Ugyanebben az időben az adott médium weboldalán elhelyezett – szintén hamis – hírek már komoly hatást gyakorolhatnak a nézőkre, hiszen máris két – bár ebben az esetben egymástól egyáltalán nem független – hírforrás mondja ugyanazt. A pszichológiai hadviselés tehát elkezdődik, amely tovább fokozható, amennyiben elérjük, hogy ne le-

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 49

gyen földfelszíni műsorsugárzás. A hazai földfelszíni műsorsugárzás nagyban függ a budapesti Széchenyi-hegyen található adótól. A bárki által elérhető Google Earth szolgáltatás segítségével nagyon világosan látszik, hogy ez az adó és átjátszókomplexum a környező utakon szabadon – néhány tízméteres – távolságra megközelíthető. Ez a távolság már bőven elegendő, hogy a támadó a közelben egy elektromágneses impulzusbombát elhelyezzen. Ennek receptje az internetet nem túl hosszas kutakodás után szintén elérhető. Ez a bomba nem a hagyományos kinetikus energiával, hanem egy óriási, nagyon rövid ideig tartó elektromágneses energiaimpulzussal pusztít. Amennyiben ez az akár több gigawattnyi energia félvezetőket, elektronikus áramköröket tartalmazó berendezésekre jut, akkor azok ideiglenesen vagy véglegesen használhatatlanná válnak. Esetünkben ez azt jelenti, hogy ha a Széchenyi-hegyi adótorony közvetlen közelében egy ilyen jól irányított elektromágneses impulzusbomba működésbe lép, akkor hazánk jelentős területén megszűnik a földfelszíni műsorsugárzás.

Tapasztalataink szerint, amennyiben nincs tévé-, illetve rádióműsor, akkor az emberek jelentős része az internetes médiumok felé fordul hírekért.

Internetes hírportálok

Hazánkban megközelítőleg 1,5 millió ember látogat meg legalább egy internetes hírportált naponta. Ez a szám már önmagában is jelentős, de abban az esetben, ha nincs elérhető tévé és rádió, akkor nagy valószínűséggel ez a szám eléri vagy akár meg is haladja a 2,5–3 milliót. Ekkor már komoly befolyásoló tényezőként számolhatunk ezekkel a hírportálokkal a lakosság egészét tekintve. Itt következik a pszichológiai hadviselés következő fázisa. Ha nem is könnyű feladat, mégis lehetséges hamis híreket elhelyezni a különböző hírportálokon, azok meglévő és többször bizonyított sebezhetősége és sérülékenysége miatt. Amennyiben ezek a hamis hírek egymással összefüggnek, illetve a különböző blogokon is megjelennek, már komoly mértékű pánikot is okozhatnak. Ilyen hamis hír lehet többek között egy pénzügyi válságra utaló figyelmeztetés. Az események ezután már igen gyorsan – látszólag egymással összefüggésben – követik egymást.

Pénzügy, banki rendszer

A hamis hírekkel párhuzamosan a pénzügyi rendszer informatikai hálózatait is támadások érik. A közigazgatás pénzügyi működését tekintve hazánkban a legnagyobb kárt természetesen a Magyar Államkincstár elleni támadással lehetne okozni. Véleményünk szerint azonban ez mind fizikailag, mind informatikailag megfelelően védve van. Ugyanakkor, a social engineering, azaz az emberi hiszékenységet kihasználó támadások itt sem zárhatók ki teljes mértékben. További támadási felület lehet az önkormányzatok informatikai kapcsolata az államkincstárral. Itt külön meg kell említeni azt a tényt, hogy egy-egy önkormányzat rendkívül sebezhető a nem egységesen és számos helyen nem megfelelő szinten védett saját informatikai hálózata miatt. Az ezek sebezhetőségére vonatkozó tanulmányok – a hálózatok támadható pontjainak meglehetős részletességgel történő bemutatásával – szintén elérhetők az interneten.

A pénzügyi szektor további szereplői a különböző bankok, melyek, illetve köz-

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 50

pontjaik két-három nagyobb centrumban helyezkednek el Budapest belvárosában. Korábban már utaltunk rá, hogy informatikai támadást intézni közvetlenül a bankok ellen nagyon nehéz, hiszen kimagaslóan jó védelemmel rendelkeznek ezen a téren. Ennek ellenére, éppen centralizált fizikai elhelyezkedésük miatt a kommunikációs rendszereik – telefon-, fax-, internetkapcsolat – fizikai elérése, majd azok működésképtelenné tétele egyszerre több bankot is megfoszthat a létfontosságú infrastruktúrától. Itt nem kell hatalmas dolgokra gondolni: néhány utcai kábelalagút szerelőnyílásának leemelése után hozzáférhetővé válnak azok a hagyományos és optikai kábelek, amelyek a gerincét jelentik az említett infrastruktúráknak.

Közlekedés

A pénzügyi terület támadása után következhet a közlekedés támadása. Forgatókönyvünkben csak a budapesti metró és a BKV forgalomirányításának zavarásáról, illetve Budapest három-négy frekventált helyén lévő közlekedési jelzőlámpa működésébe történő beavatkozásról ejtünk szót.

A budapesti 3-as metróvonal csúcsidőben 26–27 ezer utast szállít irányonként minden órában. A metró biztonsági, valamint forgalomirányítási megoldásai nagyon részletes technikai leírásokkal, képekkel és ábrákkal nyíltan hozzáférhetőek az interneten. Alapszintű elektronikai és informatikai ismeretekkel, valamint némi helyismeret birtokában, a metró alagútjaiban ezek megtalálhatók és manipulálhatók. Az alagútba való bejutás sem megoldhatatlan feladat, hiszen a budapesti metró esetében még a közelmúltban is láthattunk különböző videómegosztó portálokon olyan amatőr videókat, amelyeket fiatalok készítettek a metrókocsik ütközőin történt „utazásaikról".

Ha egy szerelvény leáll a metróalagútban két állomás között, akkor több száz ember rekedhet ott. Amennyiben a biztosító berendezések meghibásodása miatt nem csak egy szerelvényt kell leállítani, akkor akár több ezer ember is az alagutakban reked hosszabb-rövidebb ideig. A pszichológiai hatás itt is komoly mértékű lesz, főleg akkor, ha ezeket a leállásokat előre – akár néhány perccel azok bekövetkezése előtt – az online médiumokon bejelentik a támadók.

A másik „találomra" kiválasztott cél a BKV forgalomirányítása, illetve ezen belül is az elektronikus járműkövető rendszer. Ez az interneten nyilvánosan elérhető információk szerint egy olyan elektronikus és informatikai megoldásokat közösen tartalmazó rendszer, amely néhány helyen vezeték nélküli internettechnológiát (WLAN) is használ. Abban az esetben, ha ezen a WLAN-on keresztül a támadók be tudnak hatolni a vállalat rendszerébe, akkor annak működése befolyásolható vagy akár le is állítható. Ha a budapesti tömegközlekedési járművek közül csak a belvárosban közlekedők, illetve a főbb közlekedési csomópontok – például autópályák bevezető szakaszai, hidak – környékén lévő járatok járművei esetében sikerül azt elérni, hogy a diszpécserek nem vagy csak késve kapjanak információt a járművek pillanatnyi helyzetéről, akkor az nagy valószínűséggel rövid időn belül komoly torlódásokhoz vezet. Jól megválasztva az egyébként is csúcsforgalmat jelentő napszakot, valamint a közlekedés szempontjából a hétköznapokon is neuralgikus pontokat, olyan mértékű torlódás okozható, amely már Budapest határain is túl fog nyúlni. Számos – az autópályák bevezető szakaszai mellett található – logisztikai központ csak nehe-

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 51

zen vagy egyáltalán nem lesz megközelíthető, a mentők és tűzoltók közlekedése szintén nehézkessé válik, és alapvető ellátási problémák is felléphetnek nagyon rövid időn belül. A közlekedési nehézségeket tovább fokozva egyszerű fizikai rombolással – néhány kulcsfontosságú helyen lévő – forgalomirányító jelzőlámpa működésének megakadályozása következik. Ez összességében csak a megfelelő helyek előzetes kiválasztásában jelenthet némi nehézséget, mivel fizikailag – és tegyük hozzá, informatikailag – ezek az eszközök csak minimális mértékben vannak védve. Ráadásul nyitott szemmel járva a városban a „forgalomirányítás" felirat messziről szembeszökik azokon a kapcsolószekrényeken, amelyek gyakorlatilag minden forgalomirányító jelzőlámpával ellátott kereszteződés közelében megtalálhatók.

Kommunikáció és internetszolgáltatás

A következő célpont a telekommunikáció, valamint az internetszolgáltatás.

Közigazgatásunk és gazdaságunk is jelentős mértékben függ a különböző telekommunikációs szolgáltatásoktól és az internet alapú megoldásoktól. A tőzsdétől kezdve a már említett bankokon keresztül számos gazdasági társaság és vállalat, illetve maga a közigazgatás is csak nehezen vagy egyáltalán nem működik e szolgáltatások nélkül. Az informatikai támadások ezeken a területeken csak részleges károkat okozhatnak, mivel a védelem itt a legfelkészültebb. Ugyanakkor e rendszerek fizikai infrastruktúrái közel sem ilyen jól védettek. A közelmúltból is emlékezetesek lehetnek azok a példák, amikor véletlenül (például talajmunkák végzése során) vagy szándékos módon (például kábellopások) kommunikációs gerincvezetékeket vágtak el. Egy-egy ilyen esetben több ezer ügyfél nem jutott napokig telefon- és internetszolgáltatáshoz. Az egyik nagy telekommunikációs cégünk gerincvezetékének véletlen elvágása pedig – más, ezzel egy időben, de e kábelvágás közvetett hatására bekövetkezett műszaki hiba miatt – azt okozta, hogy Magyarország internetes adatforgalma közel a tizedére esett vissza több órán keresztül. Az egyik legnagyobb hazai mobiltelefon szolgáltató rendszerében a közelmúltban bekövetkezett rendszerhiba miatt több millió ügyfél közel fél napig csak akadozva tudta használni a GSM-hálózatot. Ezek persze jelentős részben műszaki meghibásodások, de ott az intő jel, ami nagyon komolyan felhívja figyelmünket e rendszerek sérülékenységére.

Villamosenergia-szolgáltatás

A teljes káosz a villamosenergia-szolgáltatás bénításával érhető el. Ma már közhely, hogy áram nélkül nincs semmi. Az eddig felsorolt rendszerek mindegyike, csakúgy, mint az összes infrastruktúra-elem, függ a villamos-energiától. Ennek megfelelően az egész országra kiterjedő igazi és nagymértékű kár a villamosenergia-rendszer bénításával, esetleges pusztításával érhető el.

Gyakran felteszik a kérdést: villamosenergia-rendszer működésképtelenné tételéhez az erőműveket, ezen belül is az atomerőművet kell-e támadni? A válasz egyértelmű: nem. A villamosenergia-szolgáltatás biztosításában és koordinációjában a rendszerirányító a központi elem. Ezért nem az erőművek, hanem a rendszerirányító lesz a célpont, kiegészítve néhány kulcsfontosságú helyen lévő távvezetékkel. Az informatikai támadás ebben az esetben kevés szerepet kap, hiszen a rendszerirányító többszörö-

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 52

sen védett, fizikailag is leválasztott informatikai hálózatokat használ. Ugyanakkor többek között a SCADA felügyeleti és adatgyűjtő rendszer alkalmazása magában rejti a támadhatóság veszélyét.

A támadást megelőzően az információszerzésben itt is szerepet kap az információtechnológia, hiszen az interneten csak néhány kattintás, és elénk tárul a rendszerirányító pontos címe, és térképen még az épület pontos elhelyezkedését is láthatjuk. Hasonlóan a földfelszíni műsorszórás hazai központi adótornyának épületéhez, a villamos energia rendszerirányító budapesti épülete is nagyon könnyen megközelíthető. Ez egy elektromágneses impulzusbomba alkalmazása esetén azt eredményezheti, hogy az épületben használt számítógépek és elektromos berendezések üzemképtelenné válnak. A támadó eszköz egy – az épület közvetlen közelében – parkoló autóban akár távirányítással is működésbe hozható, amely a későbbi felderítést majdhogynem lehetetlenné teszi, hiszen a jármű utána egyszerűen el fog hajtani, hiszen fizikai kár nem keletkezett benne, sőt még elektromos sem.

Nem úgy a rendszerirányító számítógépekre alapozott információs rendszereiben. Még abban az esetben is komoly fennakadás feltételezhető a villamosenergia-ellátás koordinációjában és ezáltal az ország villamosenergia-ellátásában, ha bizonyos rendszerek az elektromágneses impulzusok ellen megfelelő szintű védelemmel rendelkeznek.

A támadás következő fázisa néhány kulcsfontosságú nagyfeszültségű távvezeték fizikai rombolása. Ezek a már említett Google Earth segítségével nagyon pontosan meghatározhatóak, hiszen a műholdas fényképeken kitűnően látszanak. Maga a rombolás pedig ezen információk birtokában már sokkal könnyebben végrehajtható.

Védelmi lehetőségek

Digitális Mohács-forgatókönyvünkben nem foglalkoztunk az elkövetők személyével. Ugyanakkor a támadások mind terrorista jellegű cselekmények, mind az országok közötti konfliktusok esetén bekövetkezhetnek. Ezek valószínűsége azonban eltérő. A tapasztalatok szerint a független csoportok, az úgynevezett hacktivisták által elkövetett incidensek előfordulási lehetősége nagy. Különösen igaz ez Magyarország esetében, hiszen a konfliktusokkal teli szomszédságpolitika bármikor elérheti azt a hatást, hogy a kormányoktól független szélsőséges csoportosulások néhány tízezer dollárnyi befektetéssel, mely akár nacionalista vállalkozói rétegtől vagy az alvilágtól is származhat, sikeresen zavarják meg hazánk mindennapos működését. Az országok közötti hasonló konfliktusok bekövetkezési valószínűsége kicsi, ám az informatikai kémkedés valószínűleg mindennapos, így a kritikus információs infrastruktúrák védelme mindenképpen kiemelt fontosságú.

A nemzeti kibervédelemben más országokhoz hasonlóan be lehet vonni a helyi hackerközösséget is. Ehhez viszont valamilyen párbeszédet kell kialakítani a védelmi szervek és a közösség tagjai között. Több országban ez informális szinten, az USA-ban formálisan is megtörtént. Magyarországon azonban ez nem jellemző, pedig ez a közösség a legfőbb forrása az informatikai védelemért felelős személyeknek, akár állami, akár magánszervezet esetén. Valamilyen módon ezért érdemes megtudni, hogy mit gondolnak ezek a szakemberek a nemzetvédelemről. Reprezentatív felmérés a közösség rejtőzködő volta miatt nem lehetséges, ám az egy-kétezer főre tehető csoport bizonyos csatornákon elérhető. Jelen tanulmány egyik szerzője, Krasznay Csaba a Hacktivity hackerkonferencia

NB10_01_bel.qxd 2010.02.15 12:22 du. Page 53

levelezőlistáját választotta a kérdőív kiküldéséhez, mely 600 címet tartalmazott. A címzettek majdnem 20%-a, 187 megkérdezett válaszolt a kérdésekre.

Összesen négy kérdésre keresett választ a felmérés.

Olyan helyzet alakul ki az országban, amikor szükség van a hackerekre. Mit teszel?

Az IT-biztonság melyik motivációját érzed leginkább magadénak?

Hova sorolnád be magadat?

Mi a véleményed a Magyar Honvédségről?

Ezekkel a kérdésekkel a válaszadók hazafiságának mértékét kívánta felmérni, valamint a hackerek lehetséges szerepét a nemzetvédelemben, helyüket a munkaerőpiacon, valamint a védelmi szervekről alkotott véleményüket.

Az első kérdésre adott három lehetséges válasz a következő volt.

Ha hív a haza, kötelességem segíteni.

Van az a pénz, amiért segítek.

Hagyjanak békén engem ilyen hülyeségekkel!

Előzetes feltételezésként megfogalmazódott, hogy a válaszadók szeretik a hazájukat, és készen állnak egy krízishelyzetben ingyen segíteni. Ezt a válaszok megerősítették.

A kibervédelem elsősorban az infrastruktúrákat üzemeltetők és a megfelelő állami szervek feladata, nem a hackereké. Ők viszont birtokában vannak annak a tudásnak, amellyel támadni tudnak vagy támadást szimulálni, esetleg külső támadás után visszavágni.

A második kérdésre – *Az IT- biztonság melyik motivációját érzed leginkább magadénak?* – adott lehetséges válaszok a következők voltak.

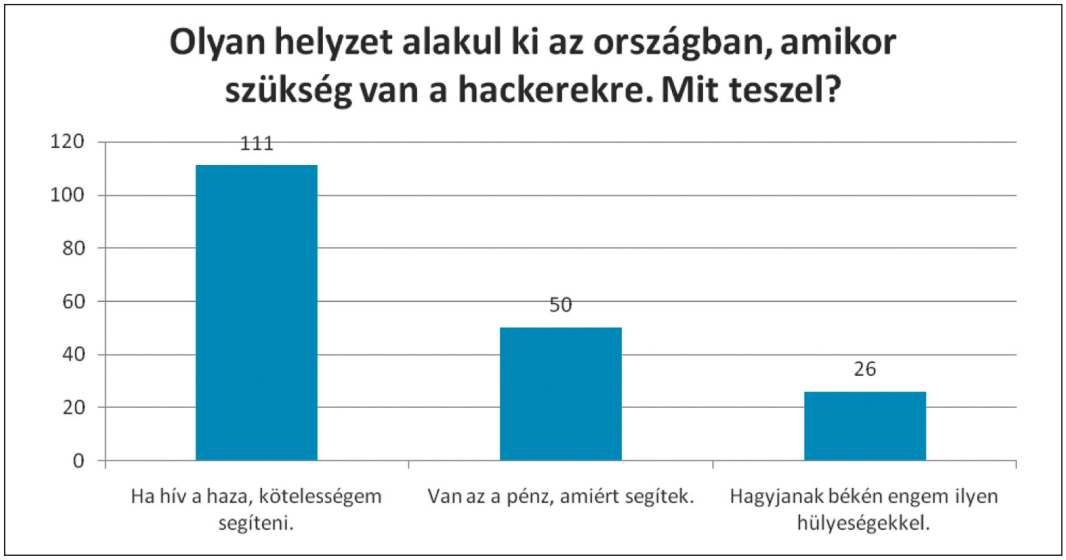
Támadok.

Védekezni tudok a legjobban.

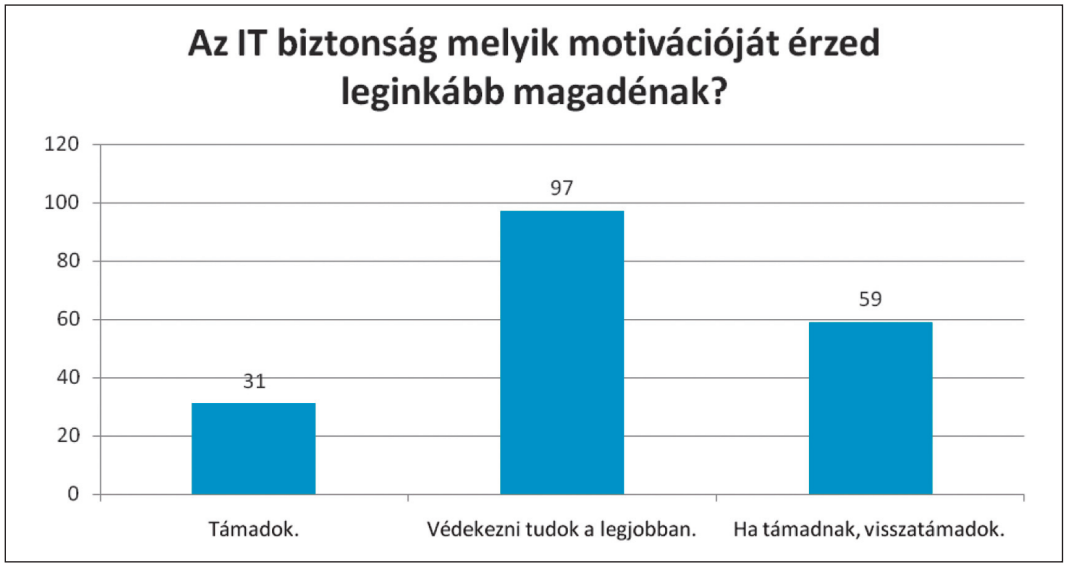
Ha támadnak, visszatámadok.

Az előzetes várakozások azt mutatták, hogy a válaszolók többsége a támadást fogja a fő motivációnak megnevezni. Ez azonban nem igazolódott.

A harmadik kérdés – *Hova sorolnád be magadat?* – célja annak mérése volt, lehetnek-e a hackerek egy esetleges kiberszázad alkotói. Az országban ugyanis van néhány hivatásos etikus hacker, és van sok



NB10_01_bel.qxd 2010.02.15 12:22 du. Page 54



olyan egyetemista, aki azzá válhat. Mellettük pedig van sok olyan szakemberünk, akik számára a hackelés hobbi, más jelenti nekik a megélhetést. A lehetséges válaszok erre a kérdésre a következők voltak.

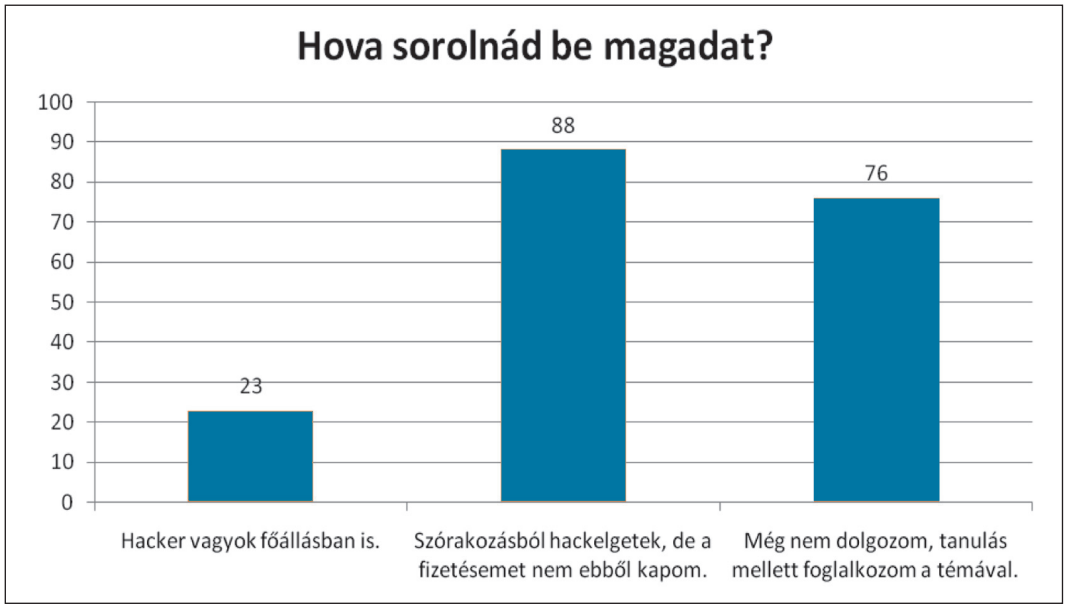
Hacker vagyok főállásban is.

Szórakozásból hackelgetek, de a fizetésemet nem ebből kapom.

Még nem dolgozom, tanulás mellett foglalkozom a témával.

Előzetesen arra számítottunk, hogy néhány hivatásos hacker mellett a hackertársadalom erős felsőoktatási háttérrel rendelkezik. Ez beigazolódott.

A közösség és a hivatalos szervek közötti együttműködés elengedhetetlen fel-



NB10_01_bel.qxd 2010.02.15 12:22 du. Page 55

tétele, hogy mindkét fél megbízzon valamennyire a másikban. Ehhez viszont pozitív képet kell kialakítania magáról annak a szervnek, amely az együttműködést kezdeményezi. A kérdés a Magyar Honvédségre vonatkozott – *Mi a véleményed a Magyar Honvédségről?* –, de a honvédség talán tetszőlegesen helyettesíthető más védelmi szervezettel is. A kérdés mérte továbbá azt is, hogy a válaszadók hogyan viszonyulnak a hadviseléshez. A három válasz a következő.

A Magyar Köztársaság fontos, elismert intézménye.

Operetthadsereg, bezzeg külföldön...

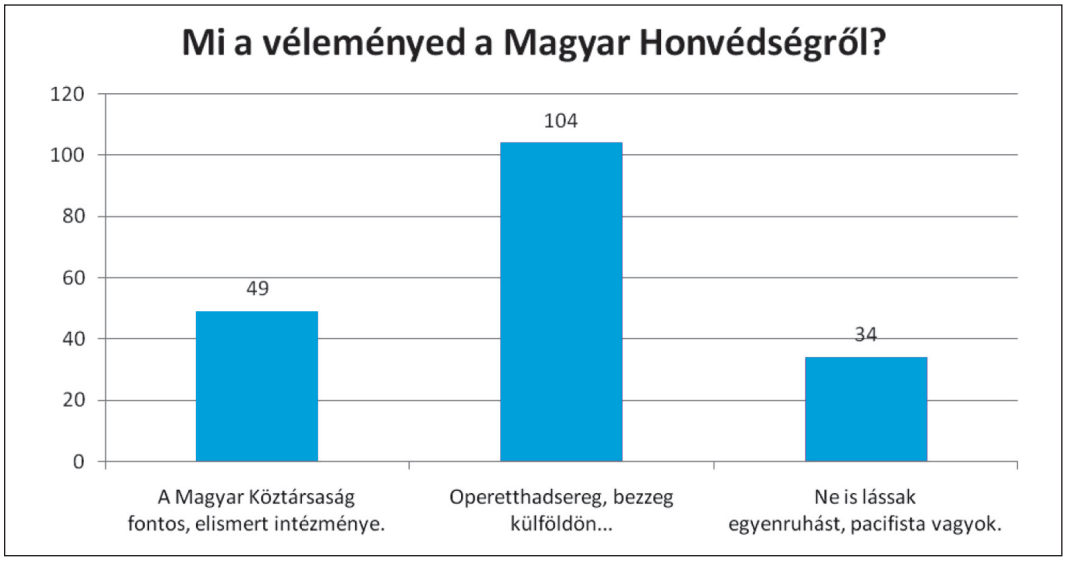
Ne is lássak egyenruhást, pacifista vagyok.

Előzetesen azt vártuk, hogy a válaszadók többsége nem pacifista, de meglehetősen negatív képe van a Magyar Honvédségről. Ez be is igazolódott.

A válaszok alapján tehát a hackerközösség szereti az országot, és kész megvédeni a maga eszközeivel. A válaszadók fele kész támadni vagy visszatámadni egy esetleges konfliktus során. Magyarországon van néhány hivatásos hacker, és hatalmas utánpótlás van az egyetemeken, amellyel érdemes számolni, illetve valamilyen módon támogatni az ilyen képzéseket. A Magyar Honvédségnek viszont sokkal pozitívabb képet kell kialakítania.

Néhány érdekes összefüggésre is fény derült. A hivatásos hackerek fele pénzért, másik felük ingyen segítene. Az etikus hackereknek nincs jó véleményük a Magyar Honvédségről, ugyanakkor a hobbihackereknek van a legjobb benyomásuk a testületről. A hazafiak nem pacifisták. A hobbihackerek készen állnak támadni és visszatámadni. Ami pedig talán a legjobb hír a tanulmány szempontjából, hogy a diákok hazafiak és nem pacifisták.

Ezt a közösséget tehát érdemes figyelembe venni a kibervédelem tervezésénél. Ehhez aktívan részt kell venni a hackerkonferenciákon, pozitív képet kell építeni a Honvédségről, esetleg támogatást kell szerezni egy kibergyakorlathoz, melybe be lehetne vonni a hazafias hackereket is. De mindenekelőtt el kell kezdeni a stratégiai gondolkodást ezen a téren is.



NB10_01_bel.qxd 2010.02.15 12:22 du. Page 56

Következtetések

Tanulmányunk célja az volt, hogy ráirányítsuk a figyelmet a kibertérből érkező, hazánkat is fenyegető veszélyekre. Azok a kritikus információs infrastruktúráink, amelyek működése annyira természetes, hogy gyakran észre sem vesszük őket, sérülékenyek és sebezhetőek. Ugyanakkor ezek a rendszerek mindennapjaink meghatározó tényezői. Ezek nélkül nem képzelhető el olyan szintű társadalmi és gazdasági élet, mint amelyet a 21. század elején megszoktunk, és amely mindenképpen szükséges az ország normális működéséhez.

Természetesen a különböző infrastruktúrákat üzemeltetők bizonyos szintig fel vannak készülve az esetleges támadásokra, illetve ezek kezelésére. Abban az esetben azonban, ha az ország több kritikus információs infrastruktúráját éri egyszerre, párhuzamosan komplex – tehát egyidőben jelentkező informatikai és fizikai – támadás is, akkor koordináció hiányában nem biztosítható megfelelő szintű védelem.

Mindezeknek megfelelően a védelem területén egy átfogó – a kritikus információs infrastruktúrák komplex védelmére vonatkozó – védelmi stratégia kidolgozása az első lépés, amelyet meg kell tenni. Ebben rögzíteni kell a védelemért felelős koordinátor személyét és annak szervezetét, illetve e szervezet feladatát. A stratégiában meg kell határozni a kritikus információs infrastruktúrák üzemeltetői számára azokat a szükséges feladatokat, lehetőségeket és megoldásokat, amelyekkel biztosítható egy vészhelyzetben az együttműködés az állami szervekkel. Ez komoly előzetes egyeztető munkát is igényel, hiszen a kritikus információs rendszerek jelentős részben nem állami, hanem magántulajdonban vagy magáncégek üzemeltetésében vannak.

Gyakran elhangzó vélemény jelen tanulmány szerzőitől is: nem az a kérdés, hogy egy ilyen támadássorozat bekövetkezik-e, hanem az, hogy mikor fog bekövetkezni.

Bízunk benne, ha szerény mértékben is, és ha mással nem is, de a figyelemfelkeltés erejével hozzájárulunk ahhoz, hogy ez a *mikor* minél később és úgy következik be, hogy arra már megfelelő védelemmel felkészültünk. ■

Irodalom

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

Krasznay Csaba: Hackers in the national cyber security, Cyber Terrorism and Crime Conference CYTER 2009, Prague, June 24, 2009.

Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17. 11. 2005. COM (2005) 576 final.

Kovács László: Possible methodology for protection of critical information infrastructures. *Hadmérnök,* 2009. 3. szám, 310–322. o. http://www.hadmernok.hu/2009_3_kovacsl.pdf.

Ghosh, Sumit – Malek, Manu – Stohr, Edward A. : *Guarding your business: A management Approach to Security.* Chapter 4: Digital Pearl Harbor: Case Study in Industry Vulnerability to Cyber Attack. New York, 2004, Kluwer Academic/Plenum Publishers.