Vállalkozásfejlesztés a XXI. században
Budapest, 2017.

Információbiztonság az Y generáció körében

Ali Beáta

Hallgató, Óbudai Egyetem Keleti Károly Gazdasági Kar

alibea56@gmail.com

Szikora Péter

Egyetemi adjunktus, Óbudai Egyetem Keleti Károly Gazdasági Kar

szikora.peter@kgk.uni-obuda.hu

Abztract A 21. század tudásalapú társadalmának, az infokommunikációs eszközök által egyre több lehetősége van arra, hogy információkat gyűjtsön és osszon meg másokkal. Mindezek mellett számos tevékenységet bonyolíthat le online, ami több előnnyel is jár, azonban gondolni kell a hátrányokra is.
Az társadalom tagjai aktívan részt vesznek az online közösségi életben, ezzel digitális lábnyomot hagyva maguk után. Tovább rontja a biztonságtudatos viselkedést az, hogy okostelefon révén akkor is fel tudnak csatlakozni a világhálóra, amikor épp nincsenek is otthon. Ezek az eszközök nélkülözhetetlenné váltak az egyének számára, így a dolgozat célja, hogy felhívja a figyelmet a különböző veszélyekre, az adatok fontosságára és a magánszféra védelmére, mellyel növelné a biztonságtudatos gondolkodást.

Kulcsszavak:biztonság, információbiztonság, malware, biztonsági mentés, vírusirtó szoftver

1 Bevezetés

Korunk új típusú társadalma jellemzően függőségben szenved. Ez jelentheti azt, hogy az alkohol, cigaretta, kábítószer rabja, de jelenthet információ, számítógép, okostelefon, internet függőséget is. Míg az előbbieknek az emberi szervezetre, az egészségre van kártékony hatása, az utóbbi példák talán még veszélyesebbek lehetnek.
Az ember természetéből adódóan rendkívül kíváncsi, tehát minden új információt azonnal tudni szeretne. Ehhez segítségül szolgál az infokommunikációs technológia rohamos fejlődése, hiszen akár otthon, akár az utcán pillanatok alatt elérhetővé válik számunkra az internet. Azonban ennek az előrelépésnek is megvan a maga árnyoldala, ugyanis a rendszerek sebezhetősége is ezzel egyenes arányban

növekszik. Így szinte elengedhetetlen, hogy a számítógépeken, illetve az okostelefonokon biztonsági alkalmazásokat futtassunk, ha nem szeretnénk, hogy különböző veszélyeknek legyünk kitéve. Komoly problémát jelent, hogy ezek a támadások egyre kifinomultabbak, nehezebben érzékelhetők és kezelhetők, így a magánszférát, illetve a vállalati és kormányzati szektort is egyaránt fenyegetik.
Annak ellenére, hogy különböző biztonsági programmal próbáljuk megvédeni az eszközeinket, sajnos a teljes biztonságot akkor sem tudjuk biztosítani a készülékeink, illetve saját magunk számára. Az életben vannak bizonyos kockázatok[1] és általában kompromisszumra is szükség van. Néha le kell mondanunk bizonyos dolgokról, mint például kényelemről, lehetőségekről, időről, ahhoz, hogy védelem alatt érezhessük magunkat. Ezeket az egyezségeket tudatosan vállaljuk, viszont olyan helyzetek is kialakulhatnak, amikor öntudatlanul kötjük meg őket. Azonban azt tudni kell, hogy a technológia módosíthatja ezeket; van, amit gyorsabbá tesz és van, amit időigényesebbé. A technológia fejlődése valamikor a támadást könnyíti meg és van, amikor a védekezést. Így a rohamosan változó technológiai világunkban fontos, hogy felfigyeljünk az új biztonsági egyensúlyhiányokra. [1]

2 A biztonság és az információbiztonság kapcsolata

2.1. A biztonság

A magyar köztudatban a „biztonság”, valamint a „védelem” szavak jelentése összemosódik, tulajdonképpen egymás szinonima szavai. Azonban mindkét szó viszonylag jól körülhatárolhatóan definiálható.
A Magyar Értelmező Kéziszótár a „védelem” kifejezést úgy definiálja, hogy „az a cselekvés, tény, hogy valakit, valamit védenek, oltalmaznak”.
Ezzel szemben a „biztonság” kifejezés a Magyar Értelmező Kéziszótár szerint egy „veszélyektől vagy bánásmódtól mentes (zavartalan) állapot”.
Ebből a két meghatározásból kitűnik, hogy a magyar értelmezés a védelemre, mint tevékenységre, a biztonságra pedig, mint állapotra gondol. Munk Sándor viszonyításában „a biztonság egy olyan állapot, amelyben valaki/valami a lehetséges fenyegető hatások ellen a megkívánt mértékben védett. A védelem pedig ebben az értelemben a fenyegetések elleni, a biztonság (mint megkívánt állapot) megteremtésére és fenntartására irányuló tevékenységek, rendszabályok összessége.”[2]

[1] A kockázat tulajdonképpen egy olyan lehetséges esemény, ami kárt, vagy veszteséget tud okozni, vagy hatással lehet a kitűzött célok elérésére. A kockázatot a veszély valószínűségével, az eszköz veszéllyel szembeni sebezhetőségével és a bekövetkezés esetén fellépő hatással mérik.

Összegezve tehát elmondható, hogy a biztonságtól elvárt követelmény az, hogy a fenyegetések bekövetkezésének lehetősége, illetve egy esetlegesen bekövetkezett fenyegetés által okozott kár a lehető legkisebb legyen. Ahhoz pedig, hogy a biztonság teljes körűvé válhasson, szükséges, hogy minden valós fenyegetésre valamilyen védelmi megoldást nyújtson, nélkülözhetetlen, hogy minden támadható ponton biztosítson valamilyen akadályt a támadó számára, valamint létfontosságú, hogy fenntartható legyen.

2.1.1. A biztonság dimenziói

A biztonságnak számos meghatározása létezik, attól függően, hogy ki milyen nézőpontból vizsgálja. Mást jelent az egyén számára, mást a társadalom egészére, valamint más értelmezése van egy nemzet biztonságának. Egy megközelítés szerint a biztonság egy olyan sajátos, fenyegetettség nélküli, kockázatmentes helyzet, amikor az elméleti veszélytényezők aktivizálódása nem várható és ezáltal nincs szükség különböző ellenintézkedések megtételére sem egyéni, sem társadalmi, sem pedig állami szinten. Míg a korábbi biztonságfelfogás szerint egy csoport védelmét csak a természeti csapások, illetve a katasztrófa-, és háborús helyzetek fenyegethették, ma már ennél jóval komplexebb támadásokra kell számítani. Így a klasszikus biztonságpolitikai felfogás szerint a biztonságnak jellemzően öt dimenzióját különítjük el, melyek között igen szoros a kapcsolat, hiszen egyik hathat a másikra.
Ezt úgy kell értelmezni, hogy ha az egyes területeken jelentkező veszélyekre adott ellenintézkedések nem megfelelőek, akkor ezek a fenyegetések más dimenziók biztonságára is károsan hathatnak. Ez az öt dimenzió a következő:

- politikai biztonság,
- katonai biztonság,
- társadalmi biztonság,
- gazdasági biztonság és
- környezeti biztonság.

A politikai dimenzió esetén ezeknek az új típusú veszélyforrásoknak, valamint egy sikeresen végrehajtott támadásnak főként a belpolitikában lenne számottevő negatív vonzata, hiszen az állami és közintézmények, illetve a kritikus infrastruktúrák leállnának, továbbá a szolgáltatások is akadoznának. Ezek a leállások, valamint az elektronikus kormányzati és közigazgatási rendszerek működésképtelensége pedig közvetve a politikai intézményrendszer instabilitását eredményezhetik. Ugyanakkor a politikai szektorban jelentkező problémák, borúlátóan hatnak ki a többi szektorra is.
A következő, a társadalmi dimenzió, ami szorosan kapcsolódik a politikai dimenzióhoz, ugyanis a belpolitikában bekövetkező kritikus állapot, túlnyomórészt a társadalomra fejti ki negatív hatásait. Az információs támadások által leállhat, illetve akadozhat a bankrendszer, az áramellátás, a vízszolgáltatás, az élelmiszer-ellátás, valamint a közlekedés is. Nem kizárható, hogy a távközlési hálózat is

megszűnhet, a televízió és a rádióállomások is csak zavarral, vagy nagyon rossz minőségben foghatók, melynek következtében a tömegtájékoztatás szinte megvalósíthatatlanná válhat. Továbbá fontos megemlíteni, hogy a kórházakban is rengeteg ember életébe kerülne az áramkimaradás, hiszen az életfunkciókat biztosító orvosi műszerek csak időközönként működnének, ami megnehezíti a súlyos sérültek ellátását. Ilyen esetekben a társadalom tüntetésekkel reagálna és követelné a kormánytól, hogy minél előbb kezelje a kialakult válsághelyzetet. Mindemellett a bűncselekmények száma is drasztikusan megnövekedhet, melynek következtében az emberek társadalmába vetett bizalma és hite rendülne meg.

A biztonság katonai dimenziója szoros kapcsolatban áll a már említett politikai dimenzióval. Ebben a dimenzióban jut érvényre leginkább, hogy az információnak mekkora értéke van és ez az, amit leginkább védeni kell, hiszen a jelen háborúinak már nélkülözhetetlen összetevői a támadó, illetve a védelmi információs műveletek. Főleg a kibertérben[2] folytatott támadó és védelmi folyamatok kapnak hangsúlyos szerepet. A megtámadott nemzet kritikus infrastruktúráit – főként az adatgyűjtést, vezérlést, kommunikációt biztosító infokommunikációs hálózatokat – érik az első fizikai és információs csapások, majd a konfliktus továbbterjedése esetén a katonai fronton folytatódnak ezek a tevékenységek. Aki jobban tud érvényesülni az információs környezetben, annak jelentős fölénye származik a másik féllel szemben és ez kihathat a fegyveres konfliktus végső eredményére is.

Bár a biztonság katonai dimenziójában is jelentős szerepet kap az információ védelme, a gazdasági dimenzióban érintheti az ország legérzékenyebb pontját egy-egy információs támadás. Tudniillik, hogy a gazdaság állapota határozza meg egy ország teljesítőképességét, egy régióban betöltött szerepét, katonai erejét, valamint az életszínvonal mértékét. Ha a banki és pénzügyi szektort éri a támadás, akkor az emberek nem tudnak hozzáférni a pénzükhöz, nem tudnak pénzügyi tranzakciókat folytatni. Huzamosabb elakadás esetén a teljes pénzügyi infrastruktúrát, a bankrendszert érintheti, a bankok közötti átutalások megszűnhetnek, illetve az önkormányzatok gazdasági működőképessége is korlátozottá válhat. Ha a támadás az üzemanyag-, az áram-, a gáz- és a vízszolgáltatásra, illetve a szállításra terjed ki, akkor az alapvető szolgáltatások, valamint a nyersanyagok nem jutnak el az egyéni és a nagyüzemű fogyasztókhoz. Ennek következtében az ipari és mezőgazdasági termelés is visszaeshet, a szolgáltatóipar pedig teljesen le is állhat. Ez azért rendkívül veszélyes, mert ha a konfliktus háborús helyzetet szül, akkor az ellátást biztosító iparágak nem tudják kielégíteni sem a katonai, sem pedig a civil szféra élelmezését, illetve a hadi felszerelések utánpótlását.

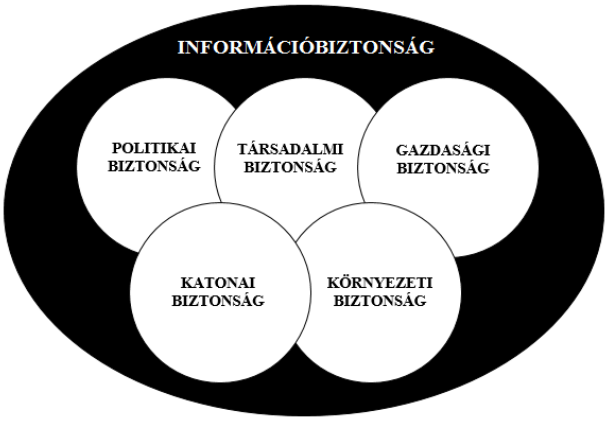
Végül ezek a támadások hatással lehetnek a biztonság környezeti dimenziójára is, hiszen egy ország infrastruktúráinak megrongálódása esetén nem csak a gazdasági teljesítménye csökken, hanem jelentős környezeti katasztrófa is bekövetkezhet. Például egy atomerőmű vezérlő rendszerében keltett rongálás akár nukleáris

[2] „Globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.” (Magyarország Nemzeti Kiberbiztonsági Stratégiája)

balesetet is vonhat maga után, aminek következtében radioaktív anyagok kerülhetnek a környezetbe. Egy gátrendszer, illetőleg egy vízerőmű irányító rendszere elleni támadás eredményeképp pedig árvizek keletkezhetnek, amelyhez hazánk területi elhelyezkedése is kedvez. [3] [4]
Összességében megállapíthatjuk, hogy a „biztonság" szó mára sokkal komplexebb értelmezést nyert és nem elég, ha a saját testi épségünket próbáljuk megóvni, hiszen a rólunk és általunk kezelt információk sokkal többet árulnak el rólunk. Már minden a kibertérben történik, ott tároljuk az adatainkat, online kommunikálunk és vásárolunk, így egyre több bűnöző és terrorszervezet támad a virtuális téren keresztül és okoz hatalmas katasztrófát mind az egyén, mind a nemzet számára. Így a „biztonság" szó szoros összefüggésbe került az „információbiztonság" szóval.

2.2. Az információbiztonság

A biztonság dimenziói már rámutattak arra, hogy mindennek köze van az információhoz, méghozzá olyan mértékig nőtte ki magát, hogy már önálló kockázati tényezőként is kell kezelni. Az információfüggőség és az információs infrastruktúra integrációjának jelenlegi szintje miatt, az infokommunikációs rendszereket, valamint az általuk tárolt információkat és az azokból jelentkező kockázati tényezőket tulajdonképpen egyfajta hatodik dimenzióként kell értelmezni. Azonban a modern biztonságfelfogás szerint az információbiztonságot nem egy különálló dimenzióként, hanem az öt dimenziót körülölelő dimenziónak kell tekinteni, hiszen integrációja révén jelentős hatást gyakorol rájuk. [5]



1. ábra
A biztonság dimenziói és az információbiztonság

Így, hogy az információnak ekkora jelentőséget tulajdonítottak, különböző követelményeket fogalmaztak meg annak érdekében, hogy az információ megfelelően védve legyen. Ezek a követelmények a következők:

- confidentiality – bizalmasság,

- availability – rendelkezésre állás,
- integrity – sértetlenség és ezen belül
  - hitelesség és
  - letagadhatatlanság.

A bizalmasság egy olyan biztonság tulajdonság, amely az információt védi az illetéktelen hozzáféréstől, tehát az információ a jogosulatlanok számára nem elérhető.
A rendelkezésre állás követelménye mind az információkra, mind az IT erőforrásokra elérhetőséget biztosít az arra feljogosított embernek, vagy gépi folyamatnak. Ennek elvesztése azt jelenti, hogy az információhoz, vagy az infokommunikációs rendszerhez való hozzáférés korlátozottá válik, esetleg adott időtartamra vagy akár teljes mértékben megszűnik.
A sértetlenség biztosítja, hogy az információt vagy a programot csak az arra jogosultak változtathassák meg, valamint, hogy észrevétlenül ne módosuljanak, törlődjenek, illetve semmisüljenek meg. Eme tulajdonság igazolja, hogy az információ és a program fizikailag, valamint logikailag is teljes. Fontos, hogy ez a követelmény magába foglalja az információk hitelességét, illetve letagadhatatlanságát is.
A hitelesség olyan biztonsági tulajdonság, amely igazolja, hogy az információ bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. Egy információ akkor tekinthető hitelesnek, ha mind tartalmának, mind a létrehozójának (küldőjének) sértetlensége bizonyítható.
Végül a letagadhatatlanság egy olyan tulajdonság, amely elegendő bizonyítékkal szolgál az infokommunikációs rendszerben elkövetett tevékenységek későbbi ellenőrzéséhez. [2]
A különböző szervezeteknél kiemelkedően fontos, hogy ezek a követelmények biztosítva legyenek, hiszen ha nem gondoskodnak az információ megbízhatóságáról és biztonságáról, akkor az könnyen befolyásolhatja a vállalat működési folyamatát, szolgáltatásainak elérhetőségét, illetve a termékeinek a minőségét.

2.3. Számítógép-hálózati támadások

A komplex információs fenyegetés témakörénél már említésre került a számítógép-hálózat általi sebezhetőségünk, ám ezeknek a támadásoknak a fajtáiról, módszereiről és eszközeiről itt térek ki részletesen.
Fajtáját tekintve megkülönbözetünk aktív, valamint passzív támadásokat. Utóbbi esetén a hálózat felderítésére kerül sor, ami tulajdonképpen behatolást jelent a számítógépes rendszerekbe, hálózatokba. Így teszi lehetővé az adatbázisokban tárolt adatokhoz, információkhoz való hozzáférést és saját célra való felhasználását.
A felderítés során tehát lehetőség nyílik a számítógépes-hálózatok felépítésének meghatározására, a működési sajátosságaik feltárására, a hálózaton keresztüli adatáramlás regisztrálására, valamint az adatbázisban tárolt adatok megszerzésére, azok saját célú felhasználására.

Megállapíthatjuk, hogy passzív támadás esetén a rendszer nem sérül és a benne tárolt adatok sem módosulnak vagy törlődnek, viszont mivel azok illetéktelen kezekbe kerülnek, jelentős veszteséget okozhatnak a támadás áldozatának. Következtetésképp láthatjuk, hogy ennél az esetnél a tárolt adatok bizalmassága sérül. Azonban a passzív támadás semmivel sem különb, mint az aktív támadás, mivel a megszerzett adatok birtokában a rendszer sokkal könnyebben támadható, tehát épp olyan veszélyforrás, mint a tényleges kárt okozó támadás.
Az aktív hálózati támadás a nevéből adódóan olyan tényleges és egyértelmű észlelhető kárt okozó behatolást jelent a másik fél számítógépes rendszereibe, illetve hálózataiba, amelynek eredményeképp tönkretehetők, módosíthatók, manipulálhatók vagy hozzáférhetetlenné tehetők az adatbázisban tárolt adatok, információk.
Az is előfordulhat, hogy a támadás következtében maga a rendszer vagy a hálózat sérül. Ebből adódóan levonható, hogy a rendszerben tárolt adatok sérülékenysége nő, a szolgáltatások elérhetősége csökken. [6]
Az ismertetett kettős célú számítógépes-hálózati támadások az információs dimenzióban közvetlen, valamint közvetett formában valósulhatnak meg. Közvetlen támadás során a támadó fél egyrészt bejut a számítógép-hálózatokba, hozzáfér a különböző adatbázisokhoz és ezáltal számára hasznosítható információkhoz jut; másrészt megtévesztő információk, rosszindulatú szoftverek bejuttatásával tönkreteszi, módosítja, törli az áldozat számára fontos adatokat. Ezzel szemben közvetett támadás alkalmával a támadó fél hozzáférhetővé teszi egy másik fél számára a saját megtévesztő információit, vagy félrevezető hálózati tevékenységet folytat, ami által befolyásolja az adat- és információfeldolgozást, illetve hamis adatokkal túlterheli a rendszert, aminek eredményeképp a hálózati hozzáférés akadályozott lesz. [7]
A számítógép-hálózati támadás eszközei a malware-ek, amelyek rosszindulatú, kártékony programok. Minden olyan rendszer vagy hálózat, mely nem rendeltetésszerűen működik, valószínűleg rosszindulatú szoftver befolyása alatt áll. A malware-ek közös jellemzője, hogy a felhasználó engedélye nélkül jutnak a rendszerbe és így megzavarhatják a rendszer működését, adatokat lophatnak, vagy akár a rendszer feletti vezérlést is átvehetik.
A „malware” kifejezés több rosszindulatú programot takar, többek között a köznyelven elterjedt vírus is csak egy fajtája a malware-eknek. Napjainkban ezeknek a szoftvereknek a köre folyamatosan bővül, így elég nehéz őket kategorizálni.
Ám egyfajta csoportosításként két osztályt különböztetünk meg, méghozzá a program típusú malware-eket és a szöveg típusú malware-eket. [8] [9]

A program típusú malware-ekhez a következőket sorolhatjuk:

- A számítógépvírusok olyan rosszindulatú programok, amelyek saját programkódjukat egy másik programhoz hozzáfűzik és így szaporodnak. A kapcsolódás módja sokféle lehet, például a vírus saját programkódját beleírja a gazdaprogram kódjába, azaz módosítja azt. Az egyik

legveszélyesebb fajtája a makrovírus, amelynek célpontjai a dokumentumfájlok, ezeken keresztül érkeznek, illetve szaporodnak.

- A programférgek (worms) nem igényelnek gazdaprogramot, önállóan futnak és képesek saját maguk megsokszorosítására. Másolataikat egyrészt a megtámadott számítógép merevlemezén készítik el, másrészt pedig a hálózaton keresztül juttatják el.
- A trójai programok tulajdonképpen hasznos funkciókat látnak el, de emellett adatvesztéssel járó műveleteket is végrehajtanak. Egyik speciális fajtájának tekinthetők a dropperek, azonban itt legyártanak kettő vagy több operációs rendszer által futtatható vírust, majd elindítják azokat. Mivel ezek új programot állítanak elő, nem pedig saját magát másolják, ezért nem sorolhatók a klasszikus víruskategóriába.
- A backdoor programok eredetileg a rendszeradminisztrátorok vagy rendszerfelügyeleti jogokkal rendelkező személyek számára nyitnak arra lehetőséget, hogy a kívánt számítógépet távolról is elérjék és így végezzenek azokon különböző javításokat, illetve beállításokat. Ezzel szemben a rosszindulatú backdoor programok jogosulatlanul próbálnak meg „hátsó ajtókat" nyitni a rendszerhez, melyek többsége e-mail mellékletként, vagy egyéb letöltés „mellékleteként" érkeznek. A backdoor programokkal lehetőség adódik a rendszeradminisztrációs jogok megszerzésére.
- A spyware-ek, magyarul kémprogramok a rendszerbe jutva és ott elrejtőzve, a háttérből figyelik a rendszer eseményeit, adatokat gyűjtenek, majd küldenek a rendszeren kívülre a számítógépen futó szoftverekről, beállításokról, felhasználói adatokról, azonosítókról, jelszavakról és egyéb bizalmas információkról.
- A keyloggerek a háttérben a billentyűleütéseket figyelik és rögzítik, mellyel akár jelszavakat, bankkártya-számokat, azonosítókat is kijuttathatnak a hálózaton keresztül. [10]

Másik csoport volt a szöveg típusú malware-ek osztálya, amelyek szöveges formában jelentenek veszélyt a rendszerre és a felhasználóra. Ebbe a kategóriába az alábbiakat sorolhatjuk:

- A spam, vagyis kéretlen levél nagyon gyakran érkezik, néha egészen nagy számban, tehát sávszélességet és tárhelyet foglal. Ezen levelek témája igen változatos, kiválogatásuk a többi és várt levél közül idő- és energiaigényes.
- A hoaxok, vagy álhírek a spamek speciális csoportjai, amelyek vagy valamilyen veszélyre (vírus, spam) hívják fel a figyelmet, vagy valamilyen nyereményt (szerencsét) helyeznek kilátásba, ha több példányban, akkor több helyre továbbítjuk őket. Amennyiben több helyre továbbítjuk ezeket, akkor sávszélességet és tárhelyet foglalunk le, így a hoaxok akadályozzák a hálózati hozzáférést.
- A phising, vagyis az adathalászat az emberek hiszékenységét használja ki, méghozzá egy eléggé megtévesztő eljárással. Látszólag a bankunktól kapunk egy e-mailt, melyben arra kérnek, hogy a banki átalakítás után

egyeztessük az adatainkat. Ehhez megadnak egy linket, melyre rákattintva a belépési nevünket, a banki azonosítónkat és a jelszavunkat kell megadni. Amennyiben ennek eleget teszünk, máris a csalók birtokában lesznek az adataink és ezeket felhasználva saját célra fordítják, mint például online vásárlás, vagy pénzátutalás.

- A pharming szintén adathalászati megoldás, viszont ebben az esetben a számítógépen található hosts fájlba írja bele a meghamisított banki oldalak címét. Ennek értelmében a megtámadott számítógép felhasználója hiába írja be a böngésző címsorába a bankja URL[3] címét, a hosts fájlban átírt banki oldalon fog kikötni, ahol gyanútanul megadja az adatait. [10]

A támadás különböző módszerei és eszközei lehetővé teszik a hálózatba való behatolást, működésének akadályozását, megbontását, valamint az adatokhoz való hozzáférést. Ennek azonban rengeteg módja létezik. Viszont, ha a támadó rendelkezik a megfelelő szekértelemmel, akkor a támadás eszközeit remekül tudja kombinálni a megfelelő eljárásokkal. A legelterjedtebb eljárás a Denial of Service (DoS) – „szolgáltatás megtagadásos", vagy magyarul „túlterheléses támadás", amely során a támadó célja, hogy megakadályozza a hálózat megfelelő működését, melyet úgy ér el, hogy a szervert hamis kérésekkel terheli túl és így a szerver a más forrásból érkező valós kéréseket már nem tudja kiszolgálni. [11]
Ezeket a támadásokat az alábbiak szerint osztályozhatjuk:

- adatkapcsolati rétegben kivitelezett támadás, melyet csak a hálózat határain belül lehet elvégezni;
- hálózati rétegben kivitelezett támadás a célponthoz vezető informatikai hálózat erőforrásait (sávszélességét) terheli túl;
- alkalmazási rétegben kivitelezett támadást végrehajtó a szolgáltatást nyújtó eszköz (kiszolgáló) erőforrásait (memória, háttértároló kapacitás, számítási teljesítmény) terheli túl. [12]

A DoS támadások többnyire elosztott túlterheléses támadások (Distributed DoS - DDoS), ahol több támadó egy időben több végpontról, együttesen próbálja a rendszert felborítani. Ebben az esetben a támadók a támadás idejére átveszik a támadásra szolgáló számítógépek felett az irányítást és egy automatizált alkalmazás segítségével felderítik az interneten lévő sebezhető számítógépeket. Ha ez megvan, akkor automatikusan vagy elektronikus levelekben küldött, esetleg egyes honlapok látogatásakor „összeszedett" vírusokkal és trójaiakkal feltelepítenek rá egy rejtett támadóprogramot, mellyel a kiszemelt gépet „zombivá" teszik. Ez azt jelenti, hogy azokat egy „mester-gép" távolról vezérli, utasítja a kiválasztott honlap elleni támadás megkezdésére. Az ilyen számítógépek hálózatba szervezhetők, amelyekkel veszélyes támadásokat lehet kezdeményezni. [13]
Ezeket a zombi számítógépekből álló hálózatokat hívjuk botneteknek, melynek részei a botnet irányítója, a botnet irányítására szolgáló vezérlő számítógép, a botnet tagjai, a fertőzött számítógépek és a vezérlő számítógép közötti irányító csatorna,

[3] Uniform Resource Locator – egységes forrásazonosító, az interneten lévő bizonyos források szabványosított címe

valamint egy „drop server” néven ismert külső adattároló szerver, amit a botnet tagjai a begyűjtött adatok feltöltésére és a kliensprogramok frissítéseinek letöltésére használnak. [12]

2.4. Kutatás

Az információbiztonság kérdése egyre fontosabbá válik napjainkban, hiszen a technológiai fejlődés eredményeképp, számos lehetőség adódik arra, hogy megfigyeljenek minket és számunkra fontos, esetleg titkos adatokat lopjanak tőlünk. A különböző generációk más-más szokásokat mutatnak a számítógépeken, illetve a mobiltelefonokon, melynél az utóbbit azért emelném ki, mert mára a mobiltelefon tulajdonképpen egy „hordozható jegyzetfüzetté” vált. Mindenki számára kényelmesebb, mert kis helyen is elfér, nem kell különböző naptárakat és füzeteket magunkkal vinni egy-egy találkozó, vagy megbeszélés alkalmával. Ezek a telefonok ugyanis rendelkeznek naptárral, jegyzettel, telefonkönyvvel, „okos” tulajdonsága miatt pedig minden digitális lábnyommal, amiket magunk után hagyunk. Éppen ezért fontos lehet a gyakori biztonsági mentések végzése, telefonunk vírusirtóval és egyéb lehetőségekkel védett állapota, de legfőképp az, hogy semmiképp ne adjuk meg azoknak a lehetőséget, akik illetéktelenül szeretnének hozzáférni mobiltelefonjainkhoz és az azokon tárolt információkhoz. Legjobb megoldás az volna ebből a szempontból, ha jelszavakat, banki adatokat, illetve személyes dolgokat nem, vagy csak minimális ideig tárolnánk ezen eszközökön.

Felmérésemben arra keresem a választ, hogy a társadalom tagjai mennyire viselkednek biztonságtudatosan mobiltelefonjaikon. Ehhez egy kérdőívet készítettem, melyben azt vizsgáltam, hogy a két felállított hipotézisem mennyire helytálló. Az első feltételezésem, hogy azok, akik fontos adatokat tárolnak, gyakrabban végeznek biztonsági mentést, hiszen nem kockáztatják meg azt, hogy számukra nélkülözhetetlen, esetleg titkos információ szivárogjon ki a külvilág felé, például egy illetéktelen hozzáférés által, illetve ha mégis elvesznének ezek az adatok, akkor könnyebben tudják pótolni azokat. A következő elméletem szerint, akik online végeznek különböző tevékenységeket, azok használnak vírusirtó szoftvereket, mert egy-egy letöltés, vagy vásárlás alkalmával könnyen megtámadhatja mobiltelefonjukat valamilyen nem kívánt hatás.

3 Eredmények

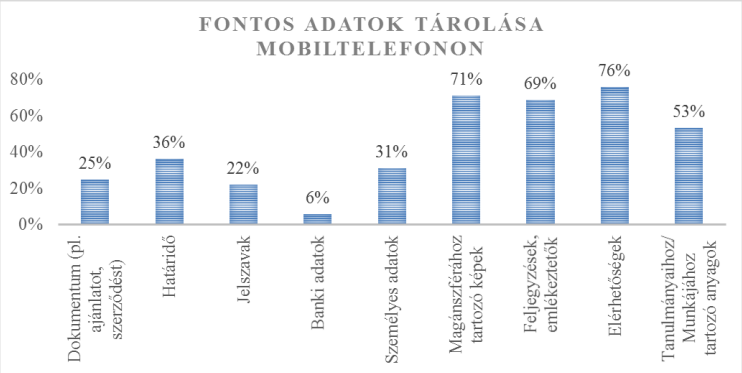
3.1. A minta bemutatása

A kérdőívet 120 nő, illetve 70 férfi töltötte ki, így összesen 190 választ vizsgáltam. A válaszadók többsége (58,4%) budapesti lakos, viszont akadt olyan is, aki kisebb

község tagja (15 fő). A kitöltők mobiltelefonnal átlagosan 15 éves koruk óta rendelkeznek és a többség egy eszközt birtokol, azonban egész gyakori két mobiltelefon is. A legnépszerűbb mobiltelefonok közé elsőként a Samsung tartozik, hiszen a megkérdezettek 35,8%-a ilyen eszközzel rendelkezik. Nem meglepő, hogy a második helyezett az Apple lett 22,1%-kal. Megnyugtató számomra, hogy a válaszadók általában kétévente, vagy annál ritkábban cserélik le mobiltelefonjukat főként azért, mert eszközük elromlott, vagy azért, mert az új gyorsabb. A kitöltők többsége rendelkezik mobilinternettel (86,3%), ami ahhoz is köthető, hogy főként előfizetéses telefonjuk van, tehát lehetséges, hogy a csomag tartalmazza azt.
Véleményem szerint saját mobilinternettel rendelkezni rendkívül előnyös, hiszen így nem szükséges felcsatlakozni a különböző nyílt Wi-Fi hálózatokra azért, hogy böngésszünk egy kicsit az interneten. Hátránya azonban, hogy korlátozott az adatforgalom, ezért sokan mégis a Wi-Fi-t választják, amennyiben olyan helyen vannak, ahol lehetőségük van felcsatlakozni rá (például kávézó, pláza). Így telefonjukat könnyedén érheti valamilyen nem kívánt hatás, amit csak különböző védelmi előkészületekkel enyhíthetnek, illetve „semmisíthetnek meg".

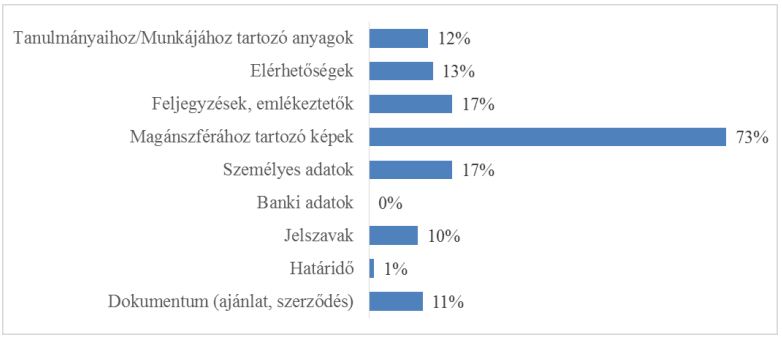
3.2. Azok, akik telefonjukon tárolnak fontos adatokat, gyakrabban végeznek biztonsági mentést

Az első feltételezésem szerint azok, akik fontos adatokat tárolnak, gyakrabban végeznek biztonsági mentést, hiszen nem kockáztatják meg azt, hogy számukra nélkülözhetetlen, esetleg titkos információ szivárogjon ki a külvilág felé, például egy illetéktelen hozzáférés által, illetve ha mégis elvesznének ezek az adatok, akkor könnyebben tudják pótolni azokat. Gyanítottam, hogy nincs olyan ember manapság, aki valamilyen fontosabb adatot ne tárolna mobiltelefonján, hiszen mint azt már említettem, a telefonunk lett a legfőbb társunk és jegyzetfüzetünk. Így a válaszadó 190 fő mindegyike azt jelezte vissza felém, hogy tárolnak fontos információkat eszközükön, melyek a következőképp oszlanak meg:



2. ábra
A válaszadók mobiltelefonon tárolt adatai

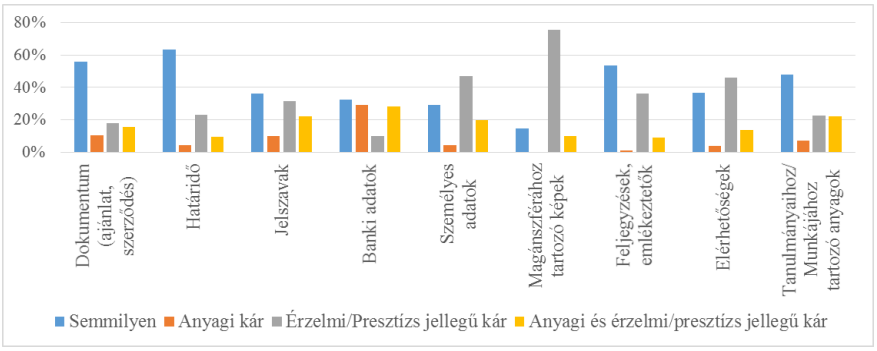
Ebben az esetben mindenkinél elvárható, hogy biztonsági mentést készítsen, hiszen a felmérésem alapján többüknek is pótolhatatlan adat rejlik telefonjában. Ezt az arányt a 3. ábra mutatja meg.



3. ábra

Adatok pótolhatatlansága illetéktelen hozzáférés esetén

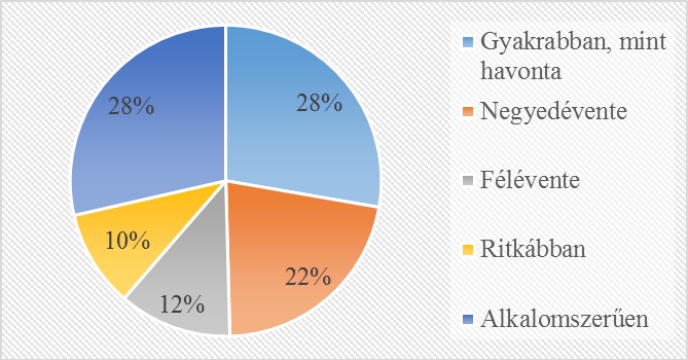
Természetesen amellett, hogy pótolhatatlan adatokról lehet szó, egyáltalán nem elhanyagolható annak ténye sem, hogy némelyik adat elvesztése igen nagy kárt is okozhat számunkra. Ilyen lehet például banki adat, illetve jelszó esetén anyagi kár, fényképek esetén érzelmi/presztízs jellegű kár, de az is lehet, hogy valakinek egyszerre mindkét részét is sérti. Ezért felmértem, hogy egy-egy adat elvesztése, milyen kárt okoz egy személynek. Ezt a 4. ábra mutatja:



4. ábra

Adatok vesztesége illetéktelen hozzáférés esetén

A fenti ábrák alapján elvárható lenne, az adatok biztonsági mentésének elvégzése, ennek ellenére a kérdőívemben feltett kérdésre mindössze 113 fő (60%) válaszolta azt, hogy valamilyen formában menti adatait. Továbbá azok, akik így cselekednek, azoknak a többsége is inkább csak alkalomszerűen végeznek biztonsági mentést. Ezt az alábbi ábra igazolja:

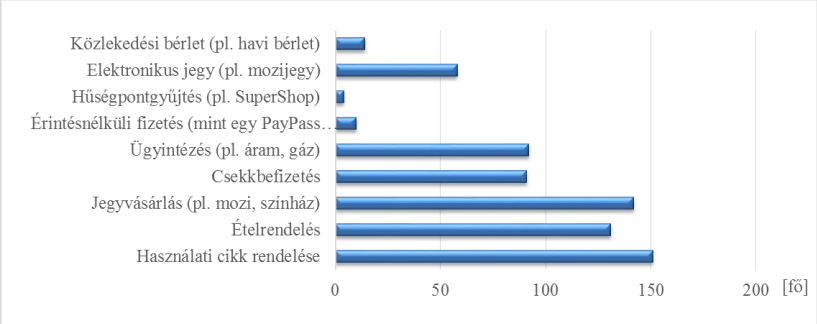


5. ábra
A biztonsági mentést végzők adatmentéseinek gyakorisága

Összegezve láthatóvá válik, hogy annak ellenére, hogy a válaszadók mindegyike tárol valamilyen fontos adatot, 50%-ban nem végeznek túl sűrűn biztonsági mentést, továbbá 37%-uk egyáltalán nem is cselekszik így. Következtetésképpen a megkérdezettek 87%-a nem tartja fontosnak azt, hogy adatait elveszítheti egy-egy illetéktelen hozzáférés során, még ha az valamilyen kárt, illetve pótolhatatlanságot okoz számára.

3.3. Azok, akik online végeznek különböző tevékenységeket, használnak telefonjukon vírusirtó szoftvereket

A következő elméletem szerint, akik online végeznek különböző tevékenységeket, azok használnak vírusirtó szoftvereket, mert egy-egy letöltés, vagy vásárlás alkalmával könnyen megtámadhatja mobiltelefonjukat valamilyen nem kívánt hatás. A felmérésem alapján mindenki azt válaszolta, hogy legalább egy tevékenységet online végez. Ennek eloszlását a következő ábra mutatja:



6. ábra
Különböző tevékenységet végzők

Ennek következtében úgy gondoltam, hogy azok, akik online végeznek különböző tevékenységeket, azoknak minimum a 90%-a használ vírusirtó szoftvert mobiltelefonján. A vizsgálat során statisztikai próba segítségével állapítottam meg az állításom helyességét. Jelen esetben egymintás aránytesztet számoltam, ahol véletlenszerűen 50 főnél megnéztem, hogy ki az, aki vírusirtóval rendelkezik okostelefonján és ebből 34 fő volt az, aki igennel reagál. A megoldásom azomban 5%-os szignifikanciaszinten az elfogadási tartományon kívül esett, így ez a feltételezésem hamisnak bizonyul.

Fontos eleme a biztonságtudatosságnak, hogy nem csatlakozhatunk fel minden nyílt Wi-Fi hálózatra, amit a mobiltelefonunk talál, hiszen ilyenkor az adataink legtöbb esetben nem titkosított csatornán mennek, így nagy kockázatnak vagyunk kitéve. Ennek ellenére az 1. táblázat alapján, melyet a kérdőívemre kapott válaszok szerint állítottam össze, egész mást mutat:

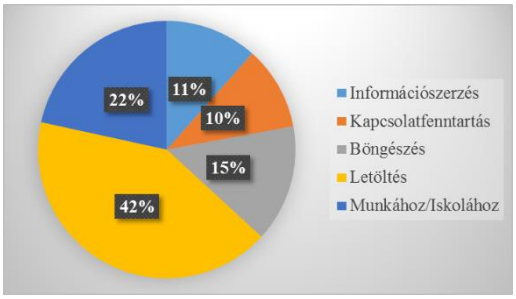
Wi-Fi hálózatra kapcsolódás, vírusirtó szoftvert használók között	
Igen, bármilyen nyílt Wi-Fi hálózathoz kapcsolódni szoktam	61 fő
Csak olyan Wi-Fi hálózatokhoz kapcsolódom, amit megbízhatónak tartok	61 fő
Csak olyan Wi-Fi hálózatokhoz kapcsolódom, amit én magam, vagy olyan ember kezel, akit ismerek és megbízok benne	24 fő
Bár képes lenne csatlakozni a telefonom Wi-Fi-vel, nem használom	3 fő
Nem Wi-Fi képes a telefonom	3 fő

1. táblázat
Vírusirtó szoftverrel rendelkezők Wi-Fi-re csatlakozási szokásai

Ezt azért vizsgáltam meg a vírusirtó szoftverrel rendelkezők körében, mert úgy gondolom, hogy azok, akik bármilyen nyílt hálózatra felkapcsolódnak, azoknak a 80%-a naponta, vagy legalább heti egy-két alkalommal végeznek vizsgálatot annak segítségével. Ezt a feltételezést szintén egymintás aránytesztet segítségével vizsgáltam meg. Véletlenszerűen kiválasztottam 20 főt, ebből 12 fő válaszolta azt, hogy naponta vagy legalább heti egy-két alkalommal vizsgálja át telefonját vírusirtó

igénybevételével. Az eredmény 5%-os szignifikanciaszinten az elfogadási tartományon belül esik, ami azt jelenti, hogy a vírusirtót használók közül, azok, akik bármilyen nyílt Wi-Fi hálózatra felkapcsolódnak, 80%-uk naponta vagy legalább egy-két alkalommal vizsgálatot végez ezen szoftver segítségével.

A kérdőívemben megkértem a válaszadókat, hogy rangsorolják azt, hogy főként mire használják az internetet, melynek eredményét a következő ábra mutatja:



7. ábra
Internethasználat rangsora

Láthatjuk, hogy a válaszadók többsége főként letöltésre alkalmazza az internetet, mely alapján elvárható, hogy azok, akik első helyre sorolták a letöltést, 90%-uk használ vírusirtó alkalmazást. Hasonlóan jártam el, mint az előbbi feltételezések esetén, hiszen véletlenszerűen kiválasztottam 20 főt azok közül, akik elsőként jelölték meg a letöltést, ebből pedig 16 fő válaszolta azt, hogy használ vírusirtó alkalmazást. A megoldásom azomban 5%-os szignifikanciaszinten az elfogadási tartományon kívül esett, így ez a feltételezésem hamisnak bizonyul.

Mindent összevetve láthatóvá vált számunkra, hogy ez az állításom is megdőlt, hiszen az előbbi példák eredményei inkább azt szemléltetik, hogy a társadalom tagjai nem mutatnak biztonságtudatos viselkedést mobiltelefonjukon, mert több tevékenységet is online végeznek, mégis sokan nem használnak vírusirtó alkalmazást.

4 Következtetés

Összegezve az eddigieket, elmondható, hogy a biztonság egy kulcsfontosságú kérdés az életünkben, hiszen a technológiai fejlődés, valamint a tudásalapú társadalom eredményeképp rengeteg veszély fenyeget bennünket. Az offline térben történő személyes érintkezés révén történő bántalmazás is egyfajta veszély, viszont az online térben történő fenyegetettség sokkal nagyobb, hiszen átverhetnek, adatokat lophatnak tőlünk, amiket fel is használhatnak ellenünk. Bármit is cselekszünk akár offline, akár online, mindig valamilyen kockázatot vállalunk. Ezzel kijelenthető, hogy az emberi tényező jelenti a legnagyobb veszélyt a

biztonságtechnika, valamint az információbiztonság területén is. A jóindulatú emberek hiszékenyek, a rosszindulatú emberek pedig ezt kihasználják, és ahol tudnak, ott támadnak.
A kérdőívemből kiderült, hogy nagyon sokan tárolnak mobiltelefonjukon fontos adatokat, amelyek elvesztése valamilyen kárt von maga után és emellett még lehet, hogy pótolhatatlan is. Ezért fontos, hogy biztonsági mentéseket készítsünk, hiszen nem egy szerencsés helyzet, ha valaki illetéktelenül fér hozzá például a banki adatainkhoz. Emellett nagyon fontos, hogy a hagyományos védelmek mellett, alkalmazzunk okostelefonjainkon vírusirtó szoftvereket, mert minél több tevékenységet végünk ezen az eszközön, annál nagyobb a valószínűsége, hogy valamilyen nem kívánt hatás éri mobilunkat.
Ennek nagyobb az esélye akkor, ha meggondolatlanul felcsatlakozunk minden nyílt Wi-Fi hálózatra, amit az eszközünk talál. Legyünk megfontoltabbak és csak olyan hálózatra kapcsolódjunk, amit biztosan tudunk, hogy megbízható. Mindezek mellett az a legfontosabb, hogy bármit cselekszünk az online térben, digitális lábnyomokat hagyunk magunk után. Így válunk lekövethetővé, azzal pedig segítjük a bűnözőket, hogy a magánéletünket teregetjük ki a különböző közösségi oldalakon és blogokon. A már ismertetett „IoT" megjelenésével pedig csak bonyolódik a helyzet, hiszen azáltal, hogy a különböző háztartási eszközeinket hálózatra kapcsoljuk, még több bizalmas információt adunk magunkról.

Irodalomjegyzék

[1] eNET – Telekom (2013): Már okostelefon-felhasználó a magyar lakosság több mint ¼-e
http://www.enet.hu/hirek/mar-okostelefon-felhasznalo-a-magyar-lakossag-tobb-mint-%C2%BC-e/ (Utolsó letöltés: 2017.03.19. – 16:50)

[2] Haig, Zs.: Információ - Társadalom - Biztonság. NKE Szolgáltató Kft., Budapest 2015. pp. 169-177. ISBN 978-615-5527-08-1

[3] Geri, P.: Számítógépes hálózatok védelme az információs műveletek eszköz- és eljárásrendszerében. Diplomamunka, ZMNE, 2009.

[4] Fehér-Polgár, P. – Németh, Zs.: Safety Consciousness of the Mobile Phone Users In: Szakál Anikó (szerk.) Proceedings of the11th IEEE International Symposium on Applied Computational Intelligence and Informatics SACI 2016. 412 p. Konferencia helye, ideje: Timisoara, Románia, 2016.05.12-2016.05.14. Budapest: IEEE, 2016. pp. 345-348. ISBN: 978-1-5090-2379-0

[5] Gábri, M.: Az információ hatása a XXI. század biztonságára. Diplomamunka, ZMNE 2008.

[6] Haig, Zs.: Az információs társadalmat fenyegető információalapú veszélyforrások. In: Hadtudomány XVII. évf. 3. sz. 2007. pp. 37-56. ISSN 1215-4121

[7] Waltz, E.: Information Warfare Principles and Operaions. Artech House, Inc. Boston, London. 1998. ISBN 0-89006-511-X.

[8] Dr. Nagy, G.: Phishing, pharming – mi jöhet még?
https://itcafe.hu/cikk/phishing_pharming_mi_johet_meg/kartevok_celkereszt jeben.html (Utolsó letöltés: 2017.03.04. – 15:33)

[9] Protalinski, E. (2014): Android accounted for 97% of all mobile malware in 2013, but only 0.1% of those were on Google Play
http://thenextweb.com/google/2014/03/04/f-secure-android-accounted-97-mobile-malware-2013-0-1-google-play (Utolsó letöltés: 2017.03.19. – 16:55)

[10] Kovács, L.: Az információs terrorizmus eszköztára. In: Hadmérnök, Robothadviselés 6 Különszám. 2006. november 22. Konferencia
http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/kovacs_rw6.html (Utolsó letöltés: 2017.03.04. – 15:36)

[11] Előházi, J.: Internetbiztonság. Robothadviselés 5. Tudományos szakmai konferencia, Bolyai Szemle 2006. 1. sz. ZMNE, Budapest, pp. 160-178. ISSN 1416-1443

[12] Kovács, L. (szerk.): Számítógép-hálózati hadviselés: veszélyek és a védelem lehetséges megoldásai Magyarországon. Tanulmány, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest 2012.

[13] Gyányi, S.: DDoS támadások veszélyei és az ellenük való védekezés. In: Hadmérnök, Robothadviselés 7 tudományos szakmai konferencia különszám. 2007. november 27.
http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/gyanyi_rw7.html (Utolsó letöltés: 2017.03.04. – 15:46)