VI. évfolyam 1.

R E N D V É D E L E M

2017/1. SZÁM

B U D A P E S T

– 2017 –

A BELÜGYI TUDOMÁNYOS TANÁCS

ONLINE FOLYÓIRATA

Felelős szerkesztő:

Dr. Dános Valér CSc/PhD

ny. r. vőrgy.

ügyvezető alelnök

TARTALOM

Szerkesztői előszó

A Belügyi Tudományos Tanács 2016. áprilisában pályázatot hirdetett meg a *„Kiberbiztonság kihívásai Európában és Magyarországon”* címmel, *„Kiberbiztonság – az információs társadalmi környezet kockázatai”*, valamint a *„Kibertér bűnügyi és nemzetbiztonsági kihívásai”* témákban.
Jelen számunkban a beérkezett pályamunkák közül – a bírálóbizottság döntése alapján díjazott – öt tanulmány válik elérhetővé a téma iránt érdeklődők számára.

A Belügyi Tudományos Tanács 2016. áprilisában publikációs pályázatot hirdetett továbbá *„Biztonsági kihívások és válaszok a 21. században”* címmel. A beérkezett pályaművek közül egyet szintén közreadunk Olvasóink számára.

Az értékes tanulmányokhoz hasznos olvasást kívánunk!

Déri Attila

Informatikai eszközeink sebezhetősége, támadása, védelme

1. Bevezetés

A számítógépes eszközeink ellen irányuló támadások napjaink része. Ezek a támadások érinthetnek állami és magáncégeket, bankokat és otthoni felhasználókat egyaránt. A támadásokat és azok hatásait meg lehet közelíteni jogi, információ-technológiai, szociológiai stb. irányból. Én az információ-technológiai irányt választottam. A támadások módjai közül mutatok be néhányat a teljesség igénye nélkül.

Rövid történeti áttekintés után betekintést nyújtok néhány érdekes támadásba. Részletesen kifejtem azokat a támadási formákat, melyek az átlagos felhasználót érintheti. A támadások több formáját is bemutatom, de a támadási lehetőségek nagy száma miatt nem törekedhettem a teljességre. Röviden szólok az okos eszközök sérülékenységéről. A támadások elleni lehetséges védekezésekről is írok, majd legvégül a szakemberképzést mutatom be. A pályázati anyagomat több, személyes példával is színesítem.

Mielőtt rátérnék a részletes leírásra, néhány fogalmat szeretnék tisztázni. A legtöbb helyen kártékony, károkozó programnak hívom a károkozásra, az adatok megszerzésére, számítógépbe történő behatolásra írt programokat, vírusokat, trójaiakat, spam-eket, exploitokat[1], stb. Azokat az embereket hackereknek hívom, akik ezeket a programokat írják, károkozásra, adatok megszerzésére, bűnös célból történő behatolásra használják. Ez a fogalom kicsit bővebb a hétköznapi szóhasználatnál, mert ott általában csak a számítógépekbe

[1] 1.Vírus: önmagát másolni tudó károkozó program, trójai: olyan károkozó program, mely „jóindulatú programnak álcázza magát, a fogadók által nem kért elektronikus levél, exploit: olyan program, mely alkalmas egy szoftver vagy egy hardver biztonsági résének kihasználására.

behatoló embereket nevezik hackereknek. A hackerek céljaik érdekében gyakran több módszert is ötvöznek. Az internet alatt a számítógépek közötti tcp/ip protokollt használó összeköttetéseket és az összekötött informatikai eszközöket (szerver, router, stb.) értem. A word wide web (www, világháló) alatt az interneten hyperlinkekkel összekötött dokumentumok összeségét értem.

Több olyan dologról írok, amit az informatikabiztonsági szakemberek úgy gondolnak, hogy a többi informatikus is ismer. Sajnos a tapasztalatok azt mutatják, hogy az informatikusok között a biztonsági ismeretek szintje messze nem egyenletes. Vannak, akik kiválóan képzettek, míg mások egyáltalán nem. A BSC képzés első évfolyamán oktatott informatikai és matematikai ismereteket tudottnak feltételezem, azok magyarázatára, bizonyítására külön nem térek ki. Szintén ismertnek gondolom az alapvető titkosítási eljárások ismeretét is.

2. Rövid történeti áttekintés

Az elmúlt 15-20 évben az informatikai eszközök mindennapjaink részévé váltak. Ma már szinte minden háztartásban megtalálható a számítógép és az internet. Egyre több eszközünk csatlakozik az internetre, válik „okos” eszközzé. Az informatika fejlődésével megjelentek azok a programok, melyeket károkozásra, számítógépek működésének megakadályozására fejlesztettek ki. Ezek a programok kezdetben nem önálló programként léteztek, hanem más programokhoz kapcsolódtak, illetve a rendszerlemezek boot szektoraiba másolódtak be. A hordozó program indítása, illetve rendszerindítás után a számítógép memóriájában maradtak és képesek voltak önmagukat másolni másik programokhoz, illetve másik rendszerlemezt megfertőzni. Ezeknek a programoknak az írása kezdetben ártatlan játéknak tűnt. Azonban az idő múlásával, a technika fejlődésével a bűnözők is felismerték ezekben a programokban rejlő lehetőségeket.

A 90-es évek elején Magyarországon is megjelentek azok a hardvereszközök, melyekkel csalást követtek el. Itt említeném meg a végtelenített telefonkártyákkal elkövetett csalásokat, valamint a 450 MHz-en működő mobiltelefonok sérülékenységét. A mobiltelefonokban lévő epromot át lehetett programozni oly módon, hogy a hívásokat ne a mobiltelefon használójának, hanem másnak számlázza a szolgáltató.

Az internet fejlődésének, elterjedésének nagy lökést adott a word wide web (www, web) megalkotása. A web tette lehetővé, hogy a hétköznapi ember is könnyen hozzáférjen a szervereken tárolt adatokhoz. Kijelenthetjük, hogy a web-technológia vitte be a háztartásokba az internetet. Az internet kapcsolat kiépítéséhez először telefonhálózatra kapcsolt modemet használtak. Később a kapcsolt vonalat használó modemet felváltotta az állandó on-line kapcsolat, adsl illetve optikai összeköttetés. Az internetes kapcsolat új sérülékenységet is jelentett, amit a vírusírók ki is használtak. Az állandóan on-line kapcsolatban lévő számítógépek folyamatosan a fertőzések kereszttüzében állnak. Ezt a vírusírtó programokat készítő cégek is felismerték és állandóan futó víruskereső programokat készítenek. A víruskereső programok a vírusokkal egyidejűleg jelentek meg. A működésük során a kártékony programok kódjainak mintáit keresik a számítógép adathordozóin lévő állományokban. A víruskereső programok megtévesztésére a hackerek a vírusok több változatát hozták létre oly módon, hogy kis mértékben megváltoztatták a vírus kódját. A kód átírása a vírus működésében nem okozott jelentős változást, de a víruskeresők dolgát megnehezítette. A vírusok kódjainak megváltoztatásával kialakultak a polimorfikus víruscsaládok.

Az internet elterjedésével megjelentek azok az informatikai eszközök is, melyeket az internetre kapcsolva az életünket tovább könnyítik (pl.: programozható, távvezérelhető termosztát stb.). Sajnos ezzel megteremtettük ezeknek az eszközöknek a támadhatóságát is.

Az utóbbi években a támadások jelentőségét a kormányok is felismerték. Megjelentek azok a támadások, melyek mögött kormányokat, vagy kormányzati megrendeléseket lehet sejteni. A védekezésre történő felkészülés fontossága is megnőtt, ezért is tartanak évente NATO kibervédelmi gyakorlatot. A legutóbbi tavaly Észtországban volt (http://www.honvedelem.hu/cikk/54201_nato_kibervedelmi_gyakorlat_esztorszagban).

3. Néhány támadás bemutatása

A mai napig bekövetkezett támadások széles spektrumot fognak át. A pályázati anyagomban csak néhánnyal foglalkozok részletesen, de a támadások más dimenzióit is szeretném érzékeltetni a teljesség igénye nélkül:

Elsőként a túlterheléses támadásokról, más néven Dos/Ddos támadásokról írok. Ezek a támadások több lépcsőben zajlanak. A hackerek első lépésben általában vírussal vagy trójai programmal fertőznek meg számítógépeket. A vírus rejtett támadóprogramot telepít, ezeket a fertőzött számítógépeket hívják zombiknak. A fertőzött számítógépek a víruskészítő utasítására egyidejűleg az interneten küldött adatcsomagokkal bombázzák az utasításban meghatározott számítógépet, szervert. A támadás során a támadó gépek egyenként kis mennyiségű adattal dolgoznak, viszont mivel egy ilyen támadás során sok támadó gép lehet, ezért a megtámadott gép próbálja feldolgozni az interneten kapott nagy mennyiségű adatot, ezért működése akadozhat, vagy le is állhat.

A túlterheléses támadás jellegéből adódik, hogy sok, akár a háztartásokban lévő számítógépeket fertőznek meg és alakítanak zombi gépekké. Az ilyen gépekből alakított hálózatot nevezzük botnet hálózatnak. A támadás célpontja egy kiemelt jelentőségű gép, sok esetben szerver.

Az internet topológiájából adódik, hogy a routerek kapacitásának eloszlása hatványfüggvényhez[2] hasonló (Dr. Barabási Albert László Behálózva c. előadása, Szeged Ifjúsági Ház 2016. 10. 04.). Abban az esetben, ha valamilyen – esetleg túlterheléses – támadással sikerül a legnagyobb forgalmú routerek működését gátolni, akkor az internet megbénulhat. Az internet routereinek kapacitását nem ismerem, ezért nem tudom, hogy a legnagyobb kapacitású routerek közül hányat kell működésképtelenné tenni, hogy a többi router kapacitása elégtelen legyen az adatforgalom lebonyolítására. Elméletben lehetséges egy olyan nagyméretű támadás, amely az internet fizikai széteséséhez is vezethet.

[2] Hatványfüggvény: $f(x) = x^a$ alakú függvény, ahol a konstans

Nem a túlterheléses támadás témakörébe tartozik, de itt említem meg az internet topológiájának egy másik sérülékenységét. A routerek közötti összeköttetések kapacitásának eloszlása is hatványfüggvényhez hasonló. A legnagyobb kapacitású összeköttetések megbénításával jelentős csapást lehet mérni az internetre. A többi összeköttetés túlterhelődhet és ez az internet lassulásához vezethet.

Egy másik figyelemre méltó támadás volt az iráni atomcentrifugák elleni támadás. Ez nemcsak a technikai, hanem politikai vetülete miatt is érdekes, előre vetíti a kiberháborúk lehetőségét is. Közismert, hogy a nagyhatalmakon kívül több ország is rendelkezik atomfegyverrel, illetve törekszik előállításukra. Ezek közé tartozott az Iráni Iszlám Köztársaság. Az atomfegyverben az egyik legyakrabban használt hasadó anyag az urán 235 tömegszámú izotópja. Az urán – mint minden más kémiai elem – izotópjainak kémiai tulajdonságai azonosak, ezért az izotópok eltérő tömegét használják fel azok szétválasztására. Az elkülönítés egyik módszere az atomok centrifugában történő szétválasztása. Az iráni atomprogramban használt centrifugák működésének megakadályozására készült a Stuxnet nevű vírus. Ez a vírus a Siemens SCADA nevű ipari szoftverének sebezhetőségét használta ki. A vírus a szoftver által vezérelt frekvenciaváltókat kereste. Ezekkel a frekvenciaváltókkal[3] vezérelték a centrifugák motorjait. A vírus a frekvenciaváltóknak adott utasítással a motorok forgási sebességét változtatta meg, ezzel akadályozva a dúsított urán gyártását. A vírusnak sikerült több éven keresztül észrevétlen maradnia, így hosszú időn keresztül akadályozta az urándúsítást. (http://www.origo.hu/techbazis/20101116-az-urandusitok-ellen-irtak-a-stuxnet-virust-a-symantec-szerint.html)

Szintén figyelemre méltó volt az RSA Security informatikabiztonsági cég elleni támadás. A támadás azért nagy jelentőségű, mert világszerte több millió felhasználó, számos vállalat és kormány használja az RSA SecurID tokenjét. A SecurID token egy kisméretű hardver eszköz. Az eszköz 60 másodpercenként generál egy 6 jegyű számot. Ezt a számot, mint jelszót tudjuk használni programokba történő belépéshez. Az RSA cég elleni sikeres támadás során megszerzett kódok más cégek biztonságát is veszélyeztetik. Nem tudni pontosan, hogy a támadók milyen adatot loptak az RSA-tól, de a cég lecserélte az összes SecurID tokent. A nyilvánosságra hozott adatok szerint a támadók közösségi oldalon választották ki az áldozataikat, akiknek e-maileket küldtek. Az e-mailekhez csatoltak egy Excel állományt. A

[3] Frekvenciaváltó: az iparban használatos készülék, a hálózati áramból állít elő tetszőleges frekvenciájú áramot

csatolt Excel állomány megnyitáskor az Adobe Flash program akkor még meglévő sebezhetőségét kihasználva hátsó ajtót, un. backdoort telepített a gépre. A hackerek lépésről lépésre jutottak közelebb a céljukig, végül sikerült az adatokat eltulajdonítaniuk (http://www.hwsw.hu/hirek/46444/rsa-securid-biztonsag-adobe-flash.html, http://www.hwsw.hu/hirek/46832/rsa-securid-token-lockheed-martin-biztonsag.html). A így megszerzett adatokkal a támadók több haditechnikai céghez próbáltak betörni.

4. Sérülékenységek, támadási lehetőségek

A számítógépes károkozók sokszor a számítógépre telepített programok sérülékenységeit használják ki. Ezek a sérülékenységek adódhatnak csak a kártékony program írója által ismert programhibákból, a gyártó cég által is ismert, de ki nem javított program hibából, régebbi programverziók használatából, a felhasználó gondatlanságából. Több esetben a hackerek kihasználják képzetlenségünket, jó indulatunkat. Az alábbiakban ezeket a sérülékenységeket, valamint a különböző támadásokat, támadási technikákat és az ellenük történő védekezést részletezem.

4.1 Frissítések szükségessége

A programok készítésekor előfordulnak kisebb-nagyobb hibák, amiket a tesztelés folyamán nem vesznek észre. A kártékony programok írói is igyekeznek felderíteni ezeket a hibákat, hogy ezeket kihasználva juttassák be a kódjukat az adott gépre, illetve a programjaik minél nagyobb kárt tudjanak okozni. A felderített és még nem publikált hibákat nulladik napi hibáknak, illetve ezeket a hibákat kihasználó támadást nulladik napi támadásnak is hívjuk. Sok nulladik hibát jó indulatú hackerek (etikus hackerek) fedeznek fel és közlik a program írójával.

A programok írói igyekeznek a felderített hibákat javítani, és a javított kódot eljuttatni a felhasználókhoz. A javított kódot idegen szóval pach-nek hívjuk. A pach-eket nem mindegyik felhasználó futtatja le, így nem frissül a szoftvere. Sok hacker ezt ki is használja, mert a patch-ek visszafejtéséből igyekszik megismerni azokat a sérülékenységeket, melyeket éppen az adott patch-el javítanak. Ezekre a sérülékenységekre írt támadó kóddal próbálnak kárt okozni azokon a gépeken, melyeken nem futtaták le az adott pach-t. A programok frissítése maga után vonhatja más programok frissítését, illetve újabb verziók megvásárlását is. Példaként

említeném a java futtató környezet frissítését. A java népszerű nyelv a programozók körében. Sok programot írnak ezen a nyelven. A nyelv népszerűségéből is ered, hogy a java futtató környezet sérülékenységére sokan figyelnek. A java frissítésével jelentősen csökkenteni tudjuk számítógépünk sérülékenységét. Sajnos előfordulhat, hogy a régebbi verziójú java nyelven írt program már nem fut a frissített futtató környezetben. Ilyenkor csak a program frissítése, vagy az újabb verziója a segítség. Előfordulhat, hogy át kell térni másik gyártó programjára, ami sok kellemetlenséggel (pl.: adatvesztéssel) járhat.

Az információs technika gyors fejlődése nem kíméli az operációs rendszereket sem. Az operációs rendszerek írói is újabb verziókkal igyekeznek követni a technika fejlődését, új hardvereszközök megjelenését. Megfigyelhetjük, hogy a felhasználók jelentős része nehezen cseréli le megszokott operációs rendszerét. Ennek oka lehet a megszokás, az operációs rendszer ára, valamint az, hogy sokszor az új operációs rendszer csak erősebb hardveren fut, ezért a számítógép cseréje, bővítése is szükséges. Példaként említeném meg, hogy a Windows-XP a mai napig népszerű operációs rendszer annak ellenére, hogy támogatása véget ért. Az XP-t jelenleg is sok gépen használják. Az XP felváltására is több operációs rendszert készített a Microsoft, ezek között voltak sikeresek és kevésbé sikeresek. A Microsoft az XP támogatásának, azaz a javítások kiadásának végső határidejét több alkalommal is kitolta, végül 2014. április 8-a lett a végleges határidő. A Windows-XP operációs rendszerre ezután nem lettek kiadva javítások, annak használata már nem biztonságos. Fennáll a lehetősége, hogy az újabb Windows operációs rendszerek javításait visszafejtve az XP sérülékenységére is fény derül, és erre a sérülékenységre készül támadó program. Mivel az XP-re már nem készül javítás, ezért ezek a sérülékenységek javítás nélkül maradnak. Érdekessége miatt említeném meg, hogy az XP javításokat minden hónap első keddjén az un. patch kedden jelentette meg a Microsoft.

4.2 Középre állás

Középre állás technikának nevezik azt a technikát, amikor a támadók a számítógépünk internetes adatforgalmát eltérítik a saját gépükre, és azt rögzítik. A titkosított kapcsolatok (SSL/TLS adatátviteli protokoll) sem lehetnek akadályai az ilyen támadásoknak. Több weboldal (pl.: banki oldalak) csak titkosított kapcsolatokon keresztül érhető el. A titkosított kapcsolatot több böngésző külön is jelzi, de abból is láthatjuk, hogy a weboldal címében nem http, hanem https jelölés van. Az ilyen kapcsolathoz használt titkosítási kulcs hitelesített tanúsítvánnyal van ellátva. A tanúsítvány azt jelenti, hogy az adott titkosítási kulcs biztonságos. Sajnos nem minden webszolgáltató használ hitelesített tanúsítvánnyal rendelkező

titkosítási kulcsot. Az ilyen kulccsal titkosított kapcsolat esetén a böngésző hibaüzenettel jelzi, hogy a webszerverrel a kapcsolat annak ellenére nem biztonságos, hogy az adatátvitel titkosított csatornán történik. Ennek az esetek többségében nincs is biztonsági kockázata.
Középre állás technikával lehetőség van a titkosított csatornán folyó adatforgalmat rögzíteni. Abban az esetben, ha az adatforgalom titkosított, akkor azt a középre állás technikát alkalmazó rögzítő program felismeri, a szerver oldali titkosítást feloldja, a felhasználó felé az adatokat újra titkosítja, de ez a titkosítás már nincs hitelesített tanúsítvánnyal ellátva. A felhasználó számítógépén a böngésző jelzi, hogy a titkosítás nincs ellátva hitelesített tanúsítvánnyal. Abban az esetben, ha olyan weboldalt nézünk, ami eddig hitelesített tanúsítvánnyal ellátott kulccsal volt titkosítva, és most kiírja a böngésző program, hogy a titkosítási kódnak nem hiteles a tanúsítványa, akkor érdemes ezt az oldalt megnézni másik számítógépen is, ami a szomszédban, munkahelyünkön, stb. van. Ha akkor is jelez a böngésző, hogy a tanúsítvány nem hiteles, akkor megnyugodhatunk, mert nem valószínű, hogy heckerek vannak a háttérben.

4.3 Jelszavaink megválasztása

A számítógépek sérülékenységéhez szervesen nem kapcsolódó, viszont a biztonságunk miatt fontos téma a különféle jelszavak helyes megválasztása. A szakfolyóiratok is több alkalommal foglalkoznak a számítógép operációs rendszerébe, valamint a különféle alkalmazásokba, programokba történő belépésre jogosító jelszavak helyes megválasztásával. A jelszóval védett programjainkat, alkalmazásainkat a leggyakoribb jelszavakat tartalmazó szótárral próbálják feltörni a hackerek. A leggyakoribb jelszavakról sok szótár van a világhálón. A legnagyobb szótárak több millió jelszót is tartalmaznak. A 25 leggyakoribb jelszóról az F-Secure informatikai biztonsági cég honlapján is olvashatunk (http://www.antivirushaz.hu/a-25-leggyakoribb-jelszo-es-pin-kod-az-one-kozte-van).
A téma fontosságát mutatja, hogy jelentős informatikabiztonsági cégek is belefoglalják előadásaikba a jelszavak helyes megválasztását. A HWSW informatikai portál által szervezett 2016. június 23-i rendezvényen Peter Košinár az ESET informatikabiztonsági cég képviseletében beszélt jelszavaink fontosságáról. Megemlítette, hogy sokan csak kis mértékben térnek el a leggyakoribb jelszavaktól pl.: 12345 helyett 12346-ot választanak. Természetesen ez a jelszóválasztás nem növeli meg a védelmet megbízható mértékben. Célszerű minél hosszabb jelszót kitalálni. A szakemberek jelenleg a minimum 8 karakter hosszúságú jelszót tartják biztonságosnak. Fontos, hogy legyen benne nagy és kis betű, valamint szám is, és ne kapcsolódjon hozzánk semmilyen formában. Gondolok itt

keresztnevekre, születési dátumokra stb. A jelszavak rendszeres cseréje növeli a biztonságot, mert ha a jelszavunk kitudódik, akkor is csak rövid ideig tudják illetéktelenül használni. Ha cseréljük a jelszóinkat, akkor mindig olyan jelszót találjunk ki, amire az előző jelszavakból nem jöhetnek rá. Rossz lehet például a jelszo01, jelszo02, jelszo03, … jelszavak választása. Természetesen a hosszú, bonyolult, önmagukban értelmetlen jelszavak megjegyzése nehezebb, de ezek jelentik a nagyobb biztonságot. A jelszavak megjegyzését nehezíti, hogy egyre több dolgot intézünk on-line és mindegyik rendszerhez külön jelszó ajánlott.

Itt írnék egy személyes történetről. Az említett HWSW előadás után néhány nappal az egyik mobiltelefon-szolgáltatónál kötöttem új szerződést. Az új szerződéshez 5 számból álló jelszót (pin kódot) kellett választanom. Néhány jelszót (pl.: 12345) nem lehetett választani. Az eladót megkérdeztem az 12346 jelszó választásáról. Azt mondta, hogy ezt a jelszót a rendszer már elfogadja. Az előadáson hallottak alapján arra gondoltam, hogy könnyen lehetséges nem biztonságos jelszót választani.

Az interneten lévő alkalmazások közül sokat csak úgy lehet használni, ha regisztráljuk magunkat az adott programban. Lehetnek olyan alkalmazások, melyekhez a regisztrációkor nem kell megadni jelszót. A regisztrációt követően egy alap jelszóval tudunk belépni és magában az alkalmazásban kell jelszót változtatni. Ilyen helyzet a jelszó elfelejtésekor kért új jelszó is. Abban az esetben, ha ilyen alkalmazásba regisztráltunk, illetve valami miatt új jelszót kaptunk, javaslom, hogy a lehető legrövidebb időn belül cseréljünk jelszót. A cserét akkor is végezzük el, ha az adott időszakban nem akarjuk használni az alkalmazást.

A routerek esetében a gyártás során beállítanak az admin felhasználónak egy alap jelszót, amivel be tudunk lépni, és konfigurálni tudjuk a routert. Javaslom, hogy ezt a jelszót a konfigurálás első belépésekor cseréljük le egyedi jelszóra.

A témához szervesen nem kapcsolódik, de itt említeném meg, hogy az F-Secure fenti honlapján megtalálható a leggyakoribb 25 PIN kód listája is. A honlap szerint az első 10 adja az összes PIN kód 15 %-át. Ez azt jelenti, hogy valaki 10 próbálkozással minden 7. PIN kóddal védett alkalmazást, ajtózárat, stb. fel tudja törni. A bankjegykiadó automatákat a PIN kódokkal történő próbálkozások ellen úgy védik, hogy három elrontott kód után az automata bevonja a kártyát.

4.4 Illegális behatolás a számítógépekbe

A számítógépen futó programok sérülékenységei lehetőségeket adnak arra, hogy a számítógépbe az internetkapcsolat segítségével kívülről hackerek lépjenek be. A programok

feltárt sérülékenységeiről adatbázisokat állítottak össze a világhálón. Ezek az adatbázisok az adott sérülékenységre írt támadó programot is tartalmazzák.

Rendelkezésre állnak programok, melyek fel tudják térképezni az internetre kapcsolódó számítógépeket. Akár a gépeken futó operációs rendszer gyártójáról és verziójáról is tudnak információt adni. A sérülékenységi adatbázisból keresni lehet megfelelő támadó programot az adott operációs rendszerre. Abban az esetben, ha létezik támadó program, a heckerek megpróbálhatják a belépést a számítógépre. A behatoláskor használhatják a világhálón lévő szótárakból letölthető jelszavakat is.

A hackerek rendszergazdai jog megszerzésére törekszenek, hogy átvegyék a teljes felügyeletet a megtámadott számítógép felett. Lehet, hogy ezt a jogot nem sikerül sikeres elsőre megszerezni. Ekkor további sérülékenyéget keresnek céljaik eléréséhez.

4.5 Levelekkel terjedő kártékony programok

A vírusok voltak a legrégebbi támadó programok. Sajnos napjainkban naponta születnek újabb és újabb vírusok. A víruskereső programokat készítő vállalkozások versenyt futnak a víruskészítőkkel. A vírusok gyakran az e-mailekhez kapcsolt állományokkal terjednek, illetve kihasználják az operációs rendszer még ki nem javított sérülékenységét.

A levelekkel terjedő kártékony programok sok esetben a felhasználók hiszékenységét, képzetlenségét használják ki. A levelek csatolmányaként elküldött Word dokumentumok, Excel táblák, képek, PDF állományok tartalmazhatnak kártékony kódot. Ezek a kódok önállóan is kárt okozhatnak, de sok esetben csak arra szolgálnak, hogy az interneten keresztül letöltsenek más kártékony kódokat. A kártékony kódok lehetnek zsaroló vírusok, billentyűzetnaplózó programok (keylog), hátsó ajtót (backdoor) nyitó programok, kiolvashatnak különböző adatokat (pl.: e-mail címeket) a gépről stb.

A másik gyakorta alkalmazott módszer, hogy a levélben linket küldenek és igyekeznek rávenni a levél olvasóját, hogy a linkre kattintson. A letöltődő weboldal tartalmazhat kártékony kódot. Egy példán mutatom be az ilyen károkozást. A napokban két munkatársam is megkapta az alábbi angol nyelvű levelet:

Tárgy: MICROSOFT FINAL WARNING

Levél tartalma:

MICROSOFT OUTLOOK NOTIFICATION

Your email box account needs to be verify immediately due to irregularities found in your mail box account. Failure to do this your email box account will be suspended now.

Microsoft Outlook © 2016

Copyright Inc. All rights reserved.

Első ránézésre a levél eredeti Microsoft által írt levélnek tűnik. Még megnyitás előtt érdemes megnézni a feladót, és rögtön gyanússá válik a levél, ugyanis a feladónak vietnami e-mail címe van. Az is gyanús lehet, hogy angol nyelvű a tárgya, mert a Microsoftnak van magyarországi képviselete. A levelet kinyitva azt olvashatjuk, hogy ellenőrizzük le az e-mail fiókunkat, mert szabálytalanságot találtak. Abban az esetben, ha nem ellenőrizzük le, az e-mail fiókunk felfüggesztésre kerül. A levél írója az ellenőrzéshez segítséget is nyújt, mert a levélben a verify szó egy hyperlink. Az egérmutatót rámozgatva a verify szóra, elolvastam, melyik weboldal jelenne meg a böngészőben, ha rákattintok a szóra. Azt találtam, hogy nem a Microsoft weboldalára mutat a hyperlink. További vizsgálatokat ezzel az e-maillel nem végeztem.

A feladó címéből és a levél tartalmából elképzelhetőnek tartom, hogy a levél károkozó kódot tölt le a számítógépre. Abból, hogy egyidejűleg két munkatársam is megkapta a levelet, feltételezem, hogy a károkozó kód a fertőzött számítógép levelező programjából kiolvassa a partnerek e-mail címeit, és interneten elküldi a szerverre. A szerver az így megszerzett új címekre is kiküldi a levelet.

A levél mellékleteként terjedő kártékony programok elterjedésének megfékezésére nem csak technikai lehetőségeink vannak. A járványmatematika és a hálózatkutatás eredményeit is felhasználhatjuk. Például a munkahelyeken a külső partnerekkel kapcsolatot tartó emberek jelenthetnek nagyobb veszélyt. A legtöbb e-mail kapcsolattal rendelkező emberek is veszélyt jelenthetnek, gócpontjai lehetnek egy lehetséges fertőzésnek.

4.6 Zsaroló vírus

A károkozó programok egy újabb formája a zsaroló vírus. A vírusok veszélyességét, illetve az általuk okozott károkozás súlyosságát jelzi, hogy napjaink konferenciáin több előadás is ezzel a témával foglalkozik. A Kapsersky Lab informatikabiztonsági cég jelentése alapján 2015 áprilisa és 2016 májusa között közel egymillió felhasználó vált a zsaroló vírusok áldozatává (http://www.origo.hu/techbazis/20160726-itt-keressen-megoldast-ha-zsarolovirus-aldozata-lett.html). A fertőzések számának gyarapodása mellett, a víruscsaládok száma is ugrásszerűen növekszik.

A vírusok a fertőzött számítógépeken található állományokat erős aszimmetrikus kriptográfiával titkosítják, és a program írói, illetve terjesztői pénzt kérnek az állományok visszakódolásáért. A vírus terjedési formája sokféle. A megfigyelések szerint leginkább netezéssel, e-mailek csatolmányaként (pl.: Word dokumentumban, Excel táblázatban lévő macro program tartalmazza a vírus kódját) terjed. Abban az esetben, ha fertőzött csatolmányt nyitunk meg, a vírus a merevlemezen található állományokat titkosítja erős, az esetek többségében 4096 bites RSA titkosítással. A felhasználó ekkor csak azt veszi észre, hogy a program folyamatosan írja, olvassa a gép merevlemezét. A titkosítás kiterjedhet a dokumentumokra, Excel táblákra, kép-, filmállományokra. A vírus a felhasználónak jelzi, hogy az állományai titkosítva lettek, és egy meghatározott időn belül fizessen bitcointal[4] egy jelentős összeget. A vírus szerzői lehetőséget biztosítanak néhány állomány visszakódolására, ezzel jelezve, hogy birtokukban van a titkosítás magánkulcsa. A vírus elküldi a kiválasztott állományokat a szervernek, majd onnan letölti visszakódolva. A vírus készítői vigyáznak arra, hogy az aszimmetrikus titkosítás magánkulcsa ne kerüljön ki a szerverről a pénz megfizetése előtt. Mindegyik támadáshoz más titkosítási kulcspárt használnak.

A zsaroló vírusok ellen a merevlemezen található állományok mentése biztosít megfelelő védelmet. A mentésre többféle eszközt is lehet vásárolni. A legegyszerűbb megoldás a külső merevlemez, amit USB csatlakozóval tudunk a számítógépünkhöz kapcsolni. Ennél a mentési módnál csak a mentés idejére van a gépünk összekapcsolva a külső merevlemezzel, ezért ez a legbiztonságosabb. A fontosabb állományokról ajánlott több mentést is végezni.

[4] Bitcoin: nyilt forráskódú digitális fizetőeszköz. Tranzakcióknál a felek csak a bitcoincímükkel jelennek meg, amik a tulajdonoshoz nyilvános adattal nem köthetők.

A másik mentési lehetőség a NAS (Network Attached Storage, hálózati adattároló eszköz). A NAS egy speciális hardver eszköz, melyet eredetileg hálózati adattároló eszköznek fejlesztettek ki. Napjainkban a NAS-t az adattároláson kívül használhatjuk adatbázis szervernek, média szervernek, FTP szervernek, nyomtató szervernek stb.

4.7 Billentyűleütéseket naplózó programok

A károkozó programok másik fajtája a billentyűleütéseket rögzíti és továbbítja az interneten keresztül. A vírus írói így próbálnak jelszavakat, és más fontos adatokat megszerezni. A banki rendszerek esetében a szerződés megkötésekor lehetőség van biztonsági belépésikód-szolgáltatást kérni. Ebben az esetben minden alkalommal, mikor belépünk a banki oldalra, SMS-ben kapunk egy plusz, egyszerhasználatos belépési kódot. A biztonsági kód megnehezíti az illegális belépést. Az okos mobiltelefonok terjedésével a mobilon is tudjuk a banki weboldalakat nézni, banki ügyeinket on-line intézni. A hackerek is felfigyeltek erre a fejlődésre és olyan kártékony programokat készítenek mobilokra, melyek a billentyűleütések mellett az SMS üzenetek tartalmát is elküldik az interneten. Így lehetővé válik az illegális belépés a biztonsági kóddal védett oldalakra is. A banki ügyek intézéséhez javaslom, hogy mindig másik eszközről jelentkezzünk be, mint amire a biztonsági SMS kódot kapjuk.

A károkozó programok elleni védelmet a programok frissítésein kívül víruskereső program telepítésével növelhetjük. Sokat segíthet, ha nem rendszergazdai jogokkal rendelkező felhasználóként használjuk a gépet, csak a legszükségesebb esetben jelentkezünk be rendszergazdaként.

Kritikus alkalmazások (pl.: banki oldalak, pornó oldalak stb.) felkeresésekor nagyobb figyelmet kell fordítani a biztonságra. Javaslom, hogy ilyenkor Linux operációs rendszert használjunk. A Linuxra lényegesen kevesebb támadó program készül, mint a Windowsra. A Linux operációs rendszert rá lehet másolni CD-re vagy pendrive-ra oly módon, hogy erről lehessen indítani a számítógépet (live Linux). A live Linux használata közben nem fut semmilyen vírusvédelmi program és így támadhatóvá válik a merevlemez. A live Linux használata előtt javasolt a merevlemez eltávolítása a számítógépből. Természetesen időnként a Linux lemezt is frissíteni kell.

A kritikus alkalmazások és más oldalak olvasásakor használhatunk virtuális gépet. Abban az esetben, ha virtuális gépre telepített operációs rendszert és böngészőt használunk, megvédjük

a gépünket az esetleges támadástól. Ha böngészés során mégis elszenvedünk egy támadást, akkor nem sérül a virtuális gépen kívüli környezet.

4.8 Mobiltelefonok sérülékenysége és támadásuk

A mobiltelefonok elterjedéséről, sérülékenységéről a banki adatok megszerzésekor már írtam. Most megpróbálok néhány összefüggésre, további sérülékenységre rávilágítani.

Sajnos a mobiltelefonok többségén és a táblagépeken futó Android operációs rendszer is népszerű a vírusírók között. Sok vírus készül Androidra. A vírusok a hagyományos károkozás mellett képesek kiolvasni és az interneten továbbítani a telefonunk telefonkönyvét, az SMS-eket, a tartózkodási adatainkat a cellainformációk alapján vagy a beépített GPS vevő bekapcsolásával.

Az Android operációs rendszer sérülékenységeit is kihasználják a hackerek. A Nemzeti Kibervédelmi Intézet honlapján (http://neih.gov.hu/stagefright) olvasható az Android egyik sérülékenységére írt támadás. A támadóknak elég egy speciálisan összeállított videót elküldeni MMS-ben. A támadás sikeres végrehajtásához felhasználói interakció sem szükséges. A támadással a kiválasztott telefonon távoli kódfuttatás válik lehetővé, amin keresztül képesek lehetnek átvenni az irányítást a fertőzött eszköz felett.

Manapság rendelkezésre állnak víruskereső alkalmazások, melyeket a mobiltelefonokon tudunk használni. Ezekkel az alkalmazásokkal tudjuk megvédeni mobilunkat a nem kívánatos támadástól.

Itt térek ki a 2014. évi Ethical Hacking konferencián elhangzott Kovács Zsombor „Egy kínai androidos mobil vizsgálata” című előadására (https://www.youtube.com/watch?v=UGL6Huo4ay0). Az előadás Kínában belső piacra szánt mobiltelefon teszteléséről szólt. Elhangzott, hogy a telefont nem boltban vásárolták. Bemutatták az Androidos alkalmazások elemzésének módjait, magát a telefonnak a vizsgálatát. A vizsgálat alatt a telefon adatforgalmát routeren keresztül bonyolították le, így lehetőség nyílt az adatforgalom naplózására és elemzésére. Az adatok elemzése során megállapítást nyert, hogy a telefonon lévő kártékony alkalmazások az interneten keresztül

elküldték az összes telepített alkalmazás adatait, GPS adatokat, IMSI, IMEI[5], MAC számokat, híváslistákat, SMS-eket. A leírtakból látszik, hogy az ismeretlen forrásból vásárolt mobil telefonon keresztül mennyire sebezhetőek vagyunk.

4.9 WiFi törése, lehallgatása

Napjainkban is megfigyelhető, hogy a WiFi hálózatok jelentős része kódolatlan, annak ellenére, hogy egyre több hálózaton állítanak be titkosítást. A kódolatlan WiFi hálózatra kívülről rá lehet csatlakozni és ingyen lehet használni, ami a hálózat sebességét csökkenti. Valószínűleg az ilyen jellegű, illegális belépések fordulnak elő a legtöbb esetben, hiszen a külső használónak nem kell díjat fizetni az internet használatáért. Sokan úgy gondolják, hogy az ingyenes használat megelőzése miatt kell beállítani a titkosítást a WiFi routeren. Azonban az ingyenes WiFi hálózat használata másoknak lehetőséget biztosít az adatforgalmunk lehallgatására, továbbá arra, hogy a hackerek a WiFi hálózatot használják fel bűncselekmények végrehajtására. Véleményem szerint az internet illegális használatából a tulajdonos számára jelentkező kényelmetlenség (sávszélesség csökkenése) eltörpülhet, a lehallgatásból eredő veszteség mellett.

A WiFi routeren az adatforgalom titkosítására több féle mód is beállítható. A WEP és a WPA titkosítás nem biztonságos, rövid idő alatt feltörhető. Javasolt a WPA2 titkosítás beállítása.

Évekkel ezelőtt a titkosítatlan WiFi hálózatok számának nagymértékű növekedését eredményezte, hogy a laptopok elterjedésével sok, nem informatikával foglalkozó felhasználó vásárolt otthonába WiFi routert. Ők azok beállításával nem voltak tisztában. Az informatikai boltok nagy hányada rendelkezik szerviz háttérrel és kérésre konfigurálják is a routereket. A konfigurálás ára a router árához képest azonban jelentős. Ezért megfigyelhető, hogy sok felhasználó családtagját, ismerősét kéri meg routerének beállításához, ez is oka lehet a sok titkosítatlan hálózatnak. Szerencsére az utóbbi években előtérbe került a biztonság, így a konfigurálásnál egyre jobban ügyelnek a titkosított kapcsolat beállítására is.

A WiFi eszközzel ellátott számítógép, általában laptop segítségével fel tudjuk deríteni a fogható WiFi hálózatokat. Erre több program is lehetőséget biztosít. A programok kiírják a

[5] A mobiltelefon nemzetközi szabvány szerinti azonosító számai

hálózatok adatait, köztük a titkosítás típusát. Rendelkezésre állnak olyan USB csatlakozású WiFi eszközök un. WiFi stick-ek, melyek külső antennával, vagy antenna csatlakozóval rendelkeznek. Ezekkel az eszközökkel a vételi hatótávolságot tudjuk növelni.

A felderített WiFi hálózat forgalmát több programmal is ki tudjuk fürkészni. Gyakorlatilag a nem titkosított adatforgalmazást teljes egészében fel lehet deríteni. Itt nemcsak a web használatára gondolok, hanem FTP, telnet, e-mail stb. programok (protokollok) forgalmára is. Az így szerzett adatokat, jelszavakat, e-mailek tartalmát fel lehet használni bűnös szándékkal is. Az ingyenes (free) WiFi szolgáltatással rendelkező vendéglők, szállodák, közlekedési eszközök is sok esetben kódolatlan WiFi hálózatot kínálnak. Ilyenkor az adatainkat csak úgy tudjuk védeni, ha titkosított kapcsolatot használó weboldalhoz csatlakozunk (SSL/TLS protokollt használó weboldal).

4.10 RFID sérülékenysége

Jelenleg még a nagyközönség által kevésbé ismert sérülékenység a rádiójelekkel automatikus azonosítást, adatközlést végző eszközök az un. RFID tag-ek illegális olvasása, és az így szerzett adatok felhasználása. Az RFID áramkörök megtalálhatóak hétköznapi eszközeinkben, pl. az érintéses fizetésre alkalmas bankkártyákban, az e-személyiben, útlevelekben, bolti lopásgátlókban, Londonban a közlekedési bérletekben is.

Az RFID eszközök rádiós frekvenciás adatátvitellel olvashatóak, írhatóak. Mindegyik tartalmaz speciális egy chipre integrált számítógépet. Több, különböző RFID tag-et készítenek. Az áramellátás szempontjából megkülönböztetünk aktív és passzív tag-et. A passzív tag nem tartalmaz saját áramforrást, a működéshez szükséges áramot indukcióval nyeri a külső elektromágneses mezőből. Röviden leírnám a működését: A tag-et elektromágneses mezőbe helyezve, a tag-ben lévő tekercsben áram indukálódik, a tag ekkor feléled, idegen szóval bebootol és a chip programjában lévő műveleteket elvégzi. A passzív tag-ek is lehetnek többfélék, az egyszerűbbek csak egy számsor tárolására és rádiófrekvenciás továbbítására alkalmasak, a bonyolultabbak kétirányú kommunikációra, programok futtatására is képesek.

A témához látszólag nem kapcsolódik, hogy a bűnözők a bolti lopásoknál felismerték a rendszer egyik hiányosságát. A boltokban a kijáratnál elhelyezett olvasók a termékeken lévő tag-eket olvassák. Abban az esetben, ha a tag-et a pénztárban nem olvasták le, akkor a

kijáratnál lévő olvasó riasztja a bolt személyzetét. A bűnözők ezért belülről árnyékolt táskákkal tulajdonítják el a termékeket.

Az utóbbi időben elterjedőben vannak az RFID chipet tartalmazó bankkártyák (paypass kártyák). A pár éve megjelent mini számítógépekre (pl.: Raspberry pi számítógép) épülő eszközökkel is lehetséges az ilyen bankkártyák olvasása. A mini számítógép méretéből adódóan elrejthető a felső ruházat alatt. Az elkövetők pl. zsúfolt közlekedési eszközön rejtett módon tudják a bankkártya adatokat kiolvasni. Az adatok kiolvasása után könnyen készíthető klón kártya. Ennek elkerülése érdekében lehetőségünk van a bankkártyánk árnyékolására, és így az adatok leolvasásának megakadályozására. Árnyékoló bankkártyatok a világhálón több cégtől is rendelhető. Az ilyen tok ugyanazt a technikát alkalmazza, amivel a bolti riasztók működését is kijátsszák.

Az útlevelekben is RFID chipen tárolják a személyes adatainkat elektronikusan. Ezek az adatok is kiolvashatók, és visszafejthetők (Tomcsányi Domonkos „E-útlevelek biztonsága" Ethical Hacking konferencia 2011.). Az igazolványokban, útiokmányokban tárolt adatok védelmét megnehezíti az okmányok – az információs technológia fejlődési üteméhez képest – hosszú, akár 10 éves érvényességi ideje.

4.11 Dolgok internete, azaz okos eszközeink

Az otthonainkban egyre több eszköz kapcsolódik az internethez, ezeket az eszközöket hívják okos eszközöknek is. Ezek az eszközök önállóan is kommunikálhatnak egymással, illetve másik számítógéppel, szerverrel. Az okos eszközök lehetnek tv, hűtő, kazán stb. Az okos eszközök az internetre kapcsolódása szórakoztatásunk, életünk megkönnyítésére szolgál. A tv esetében el tudjuk érni a különféle közösségi médiákat, hálózati adattároló eszközeinket (NAS), felhőben tárolt fotóinkat stb. A kazán, illetve okos otthon esetében hálózaton keresztül tudjuk a hőmérsékletet, világítást stb. szabályozni.

A hálózatra kapcsolt eszközeink informatikai kapacitása (pl.: processzor sebessége, RAM nagysága, stb.) nem bővíthető. Az eszközökre nem készül, illetve csak korlátozott ideig készül frissítés. Előfordulhat, hogy a weboldalak fejlődése is lehetetlenné teszi egyes funkciók használatát.

Szeretném a következőkben saját tapasztalatomat megosztani. 6 évvel ezelőtt cseréltem le a televíziómat egy akkor modern típusra. Az új tv-t bekötöttük az internetre és tudtuk nézni a közösségi média oldalakat. Az idő múlásával a közösségi média weboldalát fejlesztették. A tv beépített szoftverét próbáltuk frissíteni a gyártó által közzétett programokkal, de a közösségi média weboldalát továbbra sem tudjuk nézni. A tv alap funkciója továbbra is működik, így modernebb készülék vásárlásában nem gondolkozunk. A személyes példából is látszik, hogy az internet gyors fejlődését az eszközök frissítésével nem mindig tudjuk követni.

Kártevő programoknak, illetve hacker támadásoknak is ki lehetnek téve okos eszközeink. Az okos eszközök nagy része speciális hardverrel rendelkezik. Ezekre a hardverekre nem készül víruskereső program. A hardver kapacitása sem elég a védelem biztosításához szükséges programok futtatására. Megfelelő védelmet biztosítana, ha a helyi hálózatban lenne egy biztonsági szűrő. Gondolok olyan routerre, ami alkalmas víruskereső program futtatására.

Abban az esetben, ha eszközeink jelszóval védettek, akkor a jelszavakat is tartsuk karban. Az admin felhasználónak a jelszavát minden esetben cseréljük le. Ha az okos eszköz jellegéből fakadóan lehetséges, akkor hozzunk létre új felhasználót, aminek nincs admin joga. Az admin felhasználót csak a legszükségesebb esetben használjuk.

4.12 Adathalászat

Nem technikai jellegű támadások közé tartozik az adathalászat. Ennek egy tipikus esetét mutatom be:

A bűnözők e-mailt küldenek a bank nevében, különféle okra hivatkozva kérik, hogy adjuk meg az adatainkat. A levélben található link segítségével rögtön a bűnözők által elkészített, a bank oldalára megtévesztésig hasonló weboldalra mehetünk. A linkben található URL nagyon hasonló, illetve látszólag teljes mértékben megegyezik a bank weboldalának címével. Az ilyen URL-ben sok esetben található olyan karakter is, amit a böngésző, illetve a levelező program nem jelenít meg.

A bűnözők a bank weboldalával összetévesztésig hasonló oldalon bekérik banki adatainkat, számlaszámunkat, bankkártyánk számát stb. Ezek az adatok a bűnözők adatbázisába kerülnek. Az adatok felhasználásával lehetőségük van a bankszámlánk megcsapolására. Előfordul, hogy

az adatokat bekérő oldal nem használ titkosított kapcsolatot (SSL/TLS protokoll). Ilyenkor mások is láthatják adatainkat.

Sajnos az adathalász levelek sok embert tévesztettek meg. Azokat a leveleket mindig fogadjuk fenntartással, melyekben banki, vagy más védendő adatot kérnek tőlünk. A bankok soha nem kérnek e-mail-ben, interneten adatokat. Ha ilyen levelet kapunk, érdeklődjünk személyesen vagy telefonon bankunknál.

5. Védekezés

A leírtakból látszik, hogy a támadások elleni védekezés a felhasználó, rendszergazdák feladata. Az informatikabiztonság témakörében kevésbé jártas felhasználók jelentős része nincs tudatában annak, hogy támadás célpontja lehet. Nem ismerik sem a támadás, sem a védekezés módjait. Eddig sajnos nem találkoztam a lakosság informatikabiztonsági ismereteit bővítő széleskörű programmal.

A támadás lehetőségének csökkentése érdekében az alábbi lépéseket javaslom:

- Operációs rendszer és a programok megfelelő frissítése. A már nem támogatott programokról áttérés a támogatott verzióra.
- Jelszavak beállítása, a felhasználói fiókok, jogosultságok karbantartása, a nem használt felhasználói fiókok törlése. Ez nemcsak az operációs rendszer felhasználói fiókjainkra, hanem a programjainkra és az internetes accountjainkra (levelezőprogram, közösségi megosztó programok stb.) is vonatkozik. A jelszavak beállítását hajtsuk végre a routerünkön és az okos eszközeinken is.
- Megfelelő vírusvédelmi program kiválasztása. A programok között akad ingyenes és megvásárolható. A hazai szaklapok rendszeresen összehasonlítják a különböző programokat. A vírusvédelmi programok nevükkel ellentétben nemcsak a vírusokat szűrik ki internetezés, külső adathordozó (pl.: pendrive) használata során, hanem védenek az internetes támadásoktól is. Az állandó védelem mellett a programok különféle vizsgálati lehetőséget (gyors vizsgálat, teljes vizsgálat,stb.) is biztosítanak. A vizsgálatok során a merevlemezek és egyéb adathordozók teljes, illetve részleges

átvizsgálásával keresnek támadó programokat. A vizsgálatokat rendszeres időközönként le kell futtatni.

- Figyeljünk oda bejövő elektronikus leveleinkre. A levelek feladói, tárgyai támpontot adhatnak. Ismeretlentől kapott levelet fenntartással fogadjuk. A levelek mellékletét csak akkor nyissuk meg, ha biztosak vagyunk benne, hogy megbízható személy küldte. Ha a melléklet neve gyanús, megnyitás előtt inkább érdeklődjünk a feladónál.

A védelem megteremtésén túl meg kell oldani a rendszeres adatmentés technikai lehetőségét is. A mentéseket megfelelő időközönként javasolt elvégezni. A számítógép használata közben oda kell figyelni a gyanús eseményekre. Abban az esetben, ha gyanús dolgot tapasztalunk, kapcsoljuk ki a számítógépet, és forduljunk szakemberhez. Ilyen gyanús dolog lehet például a képernyő rendszeres elsötétedése.

A web használatának is vannak fontos biztonsági szabályai. A SSL/TLS protokoll használatáról már írtam. A különböző bankoknál, szolgáltatóknál, közösségi oldalakon, levelező rendszerekben lehetnek felhasználói fiókjaink, amiket a weben tudunk elérni. Abban az esetben, ha valamelyik felhasználói fiókunkban a munkánkat befejeztük, akkor mindig szabályosan lépjünk ki a felhasználói fiókunkból és utána zárjuk be a böngészőt. Egy másik számítógépről ugyanis lehetőség van a nyitott fiókot elérni, és az ott tárolt leveleinket, adatainkat elolvasni, nevünkben műveleteket végezni. Abban az esetben, ha web böngészés alatt a böngésző újra kéri a jelszavunkat, mindig nézzünk meg, hogy az adott weboldalhoz tartozik-e időkorlát és az lejárt-e. Ha nincs időkorlát, vagy nem járt le, okkal gyanakodhatunk támadásra.

6. Képzések

A tapasztalatok azt mutatják, hogy sok informatikai szakember sincs tisztában az informatikabiztonsággal, a rendszerek sérülékenységével. Azt is tapasztaljuk, hogy a támadás, károkozás bekövetkezése után sem térnek el a régi, hibás gyakorlattól.

A megfelelő védelem kulcsa a szakemberek képzettsége. A felsőoktatásban az informatikai szakokon van informatikabiztonsági tantárgy. Sajnos azonban tudok olyan egyetemről, ahol

az informatikabiztonsági kurzust csak a közelmúltban vezették be. Az egyetemek lehetőséget biztosítanak a téma iránt érdeklődő hallgatóknak a mélyebb ismeretek elsajátítására is. Itt emelném ki a Budapesti Műszaki és Gazdaságtudományi Egyetem CrySys „!SpamAndHex" nevű hacker csapatát. Elmondható, hogy ők Magyarország legeredményesebb csapata. A csapat az idén másodszorra jutott a DefCon elnevezésű konferencia hackerverseny döntőjébe, amit az amerikai Las Vegasban tartottak meg (https://www.bme.hu/hirek/20160826/Muegyetemi_hackerek_sikere_a_Capture_the_Flag_viadalon). A nemzetközi versenyek mellett a különböző hazai egyetemek is szerveznek versenyeket, ahol a hallgatók mérhetik fel tudásukat.

Érdekesség képpen a BME által szervezett tavalyi Security Challenge versenyről bemutatok egy feladatot.

A feladatban szereplő python programozási nyelven írt program generál egy 1024 bites RSA kulcspárt, ahol e=17. A program a titkos kulccsal dekódolást végez egy 1000 bites véletlenszámon. A generált véletlenszámot jelöljük a-val, az a szám dekódolásának eredményét jelöljük b-vel. Az eredeti véletlenszámot megjeleníti a program. A program ezek után ciklusban bekér egy számot a billentyűzetről. A bekért számnak különböznie kell az a számtól. Ha azonos, akkor leáll a program futása. Ha a szám eredmény megegyezik a b-vel, akkor a program gratulál és futása leáll. Egyéb esetben a program titkos kulccsal titkosítja a beírt számot és kiírja a titkosítás eredményét, majd visszatér a ciklus elejére. A ciklus tízszer fut le. A feladat az, hogy a program segítségével a számból meghatározzuk a b számot.

A feladatnak két megoldását ismertetem. Mind a két megoldás során első lépésként az n-t kell meghatározni. Indítsuk el a programot. A program kiírja a véletlenszám titkosítását, jelöljük ezt b-vel. A program a ciklusba belépve kéri az inputot. Egy tetszőleges természetes számot adjunk meg inputként. A beírt szám kettes alapú logaritmusa legyen kisebb 1024-nél. Jelöljük ezt a számot c-vel. A beírt számot a program titkos kulccsal titkosítja, és az eredményt kiírja. A titkosított számnak vegyük a 17. hatványát. A kapott szám és c szám azonos maradékosztályban vannak modulo n, azaz két szám különbsége az n többszöröse. Jelöljük a különbséget n_1-gyel. Ezután válasszunk 3 egymástól és a c számtól is különböző természetes számot, melyeknek a kettes alapú logaritmusa kisebb 1024-nél. A számokat rendre írjuk be a programba, majd az outputként kapott számokon végezzük el a leírt számolást. Az eredményt jelöljük n_2, n_3, n_4 betűkkel. Az n számot megkapjuk, ha az n_1 n_2, n_3, n_4 számoknak vesszük a legnagyobb közös osztóját.

A két megoldás ettől a lépéstől elkülönül egymástól. Az első megoldás: számoljuk ki a b számnak a multiplikatív inverzét. Az így kapott számot már beírhatjuk a programba és titkosíthatjuk. A titkosítás eredménye a feladatban keresett szám multiplikatív inverze. A másik megoldás: a b számot szorozzuk 131072-vel (2 17. hatványával). A kapott számot titkosítsuk a programmal. Abban az esetben, ha a titkosítás eredménye páros szám, akkor a kapott számnak fele a keresett szám. Abban az esetben, ha páratlan szám a titkosítás eredménye, akkor adjunk hozzá n-t és az összege osztva 2-vel megkapjuk a keresett számot.

A versenyek nagy lehetőséget adnak az informatikabiztonsági cégeknek szakemberek toborzására. A versenyek mellett az egyetemi tananyagtól elkülönülő képzések köre is egyre szélesebb. Az Óbudai Egyetem a hallgatóknak meghirdetett kurzusoktól teljesen elkülönülő, szélesebb kör által látogatható informatikabiztonsági képzést is szervez. A képzés fizetős és más egyetem hallgatói is elvégezhetik. A képzés ára messze nem olyan magas, mint az üzleti alapon szerveződőknek. Az egyetemi képzések mellett megjelentek az üzleti alapon szerveződő képzések is. Ezeket a képzéseket vállalkozások (Kürt KFT, NetAcademia Oktatóközpont stb.) szervezték és szervezik a mai napig. A képzések alatt az informatikabiztonság alapjai mellett olyan információkat is átadnak, amik a sérülékenységek felderítéséhez, etikus hacker munkakörök betöltéséhez is elegendőek. Itt emelném ki a témában rendszeresen tartott konferenciákat (pl. Budapesten évente megtartott Hacktivity konferencia), ahol az aktuális ismeretetekre is szert lehet tenni.

Az elmúlt években az informatikabiztonság egyre fontosabbá vált. Ez a törvényeinkben is megjelent. A régi bűntető törvénykönyvbe (1978. évi IV. törvény) a 1994. évi IX. törvénnyel emelték be a számítógépes csalás tényállását. Természetesen az új büntető törvénykönyvben (2012. évi C. törvény) is szerepelnek a számítógépben tárolt, feldolgozott adatok védelmét szolgáló tényállások. A cselekmények büntethetőségének törvénybe emelésével egyidőben nem született törvény a megfelelő védelem megteremtéséről. Az Országgyűlés az állami és önkormányzati szervek elektronikus információbiztonságáról csak 2013-ban hozott törvényt (2013. évi L. törvény (Ibtv.)). A szakemberek képzését a törvény 23. § szabályozza, a Nemzeti Közszolgálati Egyetemet (NKE) jelöli ki a képzés kidolgozására, valamint a képzés megszervezésére, tartására. A törvényben szereplő felhatalmazások alapján megalkotott alacsonyabb szintű jogszabályok közül kiemelném a 26/2013. (X. 21.) Közigazgatási és Igazságügyi Miniszteri rendeletet. A rendelet az Ibtv. által meghatározott vezetők képzését és az elektronikus információs rendszer biztonságáért felelős személyek képzését szabályozza. A

rendelet háromféle oktatást ír elő: képzés, továbbképzés, éves továbbképzés, melyeket az NKE tart. A képzés a legmagasabb szintű, 2 féléves. A képzésre felsőfokú végzettséggel és alapfokú angol nyelvvizsgával lehet jelentkezni. Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában résztvevő személyek és az elektronikus információs rendszer védelméért felelős vezetők részére továbbképzést szervez az NKE. Ez alacsonyabb szintű a képzésnél, időtartama 50 óra. Az NKE kötelező jelleggel éves továbbképzést tart a jogszabály által meghatározott személyek részére.

Az Ibtv. gondoskodik az állami és önkormányzati szervek információ biztonságáról. Ugyanakkor elmondható, hogy a versenyszférára nem vonatkozik törvény. Itt csak a szakemberek felkészültsége adhat megfelelő védelmet. Mindenképpen örvendetes a felsőoktatási képzés kiszélesedése ebben az irányban, valamint a versenyek és a konferenciák szervezése.

7. Összefoglalás

Az eltelt évtizedekben az informatikai eszközöket ért támadások a gyermeki csínytevésből, laboratóriumi kísérletezésből, komoly, minden felhasználó számára veszélyt jelentő cselekményekké nőték ki magukat. A kormányok is felfigyeltek a támadásokban rejlő lehetőségekre és a védekezés fontosságára. Kijelenthetjük, hogy napjainkra az internet is hadszíntéré vált.

A támadások jelentős száma és súlyossága miatt napjaink egyik fontos feladata lett az informatikai eszközeink védelme. Látható, hogy az informatikai eszközeink állandó támadásnak vannak kitéve. A támadások nagyon sokfélék lehetnek, ezekbe próbáltam bevezetni az olvasót. Számba vettem a támadások elleni védekezési lehetőségeket is.

A leírtakból kitűnik, hogy a teljes biztonság nehezen vagy egyáltalán nem érhető el. A biztonságunk megteremtése, illetve fenntartása kellemetlenségbe, időráfordításba és nem utolsó sorban pénzbe kerül. Sokunknak kényelmetlenség lehet a biztonsági szabályok betartása, amivel csökkenteni tudjuk támadhatóságunkat. Meg kell fizetni a mentésekre használt eszközeinket, víruskereső programokat, a verziófrissítésből eredő kényszerű

hardverbővítéseket. Sajnos ezek a költségek sok esetben nem megkerülhetők, viszont körültekintéssel csökkenthetők. A költségek mérlegelésekor megállapíthatjuk, hogy a hackerek az adatok ellopásával, jelszavaink megszerzésével, zsaroló vírusokkal, sokkal nagyobb kárt okozhatnak, mint amibe a biztonságunk kerül.

Megállapítható, hogy a felsőoktatásban megjelentek az informatikabiztonsági kurzusok. Az órarendben beépített képzés mellett, az érdeklődő hallgatóknak lehetőségük van az ismeretek mélyebb elsajátítására. A versenyek is jó próbatételt biztosítanak a hallgatóknak. A posztgraduális képzések is megjelentek, amivel a korábban megszerzett ismereteinket frissíteni tudjuk. Itt említeném meg a különféle konferenciákat is. Ellenben az is látható, hogy régebben a szakemberképzésben ez a terület elmaradt a szükségestől. Sok esetben a régebben végzet szakemberek az informatika más területeiben mélyedtek el, illetve nem érdeklődtek az informatikabiztonság iránt. Ez jelentős veszélyt rejthet, hiszen az általuk felügyelt rendszerek sebezhetősége így nagyobb.

A közszférát érintő törvényi szabályozás nagymértékben növeli a biztonságot azáltal, hogy többek között kötelező képzést ír elő.

Sajnos a mindennapi életben azt tapasztalom, hogy az átlagos felhasználók nincsenek tudatában a rájuk leselkedő veszélyekkel, nem ismerik a védekezés lehetőségeit. A széleskörű felvilágosítás, a könnyen elérhető képzések jelentősen csökkentenék a sebezhetőségüket.

Irodalomjegyzék:

1. A Flash sebezhetőségét használták ki az RSA támadói, Forrás: http://www.hwsw.hu/hirek/46444/rsa-securid-biztonsag-adobe-flash.html
2. A leggyakoribb jelszavak és PIN kódok, Forrás:http://www.antivirushaz.hu/a-25-leggyakoribb-jelszo-es-pin-kod-az-one-kozte-van
3. Az urándúsítók ellen írták a Stuxnet vírust a Symantec szerint, Forrás: http://www.origo.hu/techbazis/20101116-az-urandusitok-ellen-irtak-a-stuxnet-virust-a-symantec-szerint.html

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

5. Itt kaphat segítséget, ha zsarolóvírus áldozata lett Forrás: http://www.origo.hu/techbazis/20160726-itt-keressen-megoldast-ha-zsarolovirus-aldozata-lett.html

6. Kovács Zsombor: Egy kínai androidos mobil vizsgálata Ethical Hacking konferencia 2014., Forrás: https://www.youtube.com/watch?v=UGL6Huo4ay0

7. NATO kibervédelmi gyakorlatot Észtországban, Forrás:http://www.honvedelem.hu/cikk/54201_nato_kibervedelmi_gyakorlat_esztorszagban

8. Műegyetemi hackerek sikere a Capture the Flag viadalon, Forrás: https://www.bme.hu/hirek/20160826/Muegyetemi_hackerek_sikere_a_Capture_the_Flag_viadalon

9. Tomcsányi Domonkos: E-útlevelek biztonsága Ethical Hacking konferencia 2011 Forrás: https://www.youtube.com/watch?v=vTmY0mN3WF8

10. RSA kicseréli az összes SecuriID tokent, Forrás: http://www.hwsw.hu/hirek/46832/rsa-securid-token-lockheed-martin-biztonsag.html

11. Stagefright sérülékenység (Android), Forrás: http://neih.gov.hu/stagefright

Jogszabályok:

1. 1978 évi IV törvény a Büntető Törvénykönyvről

2. 1994. évi IX. törvény a büntető jogszabályok módosításáról

3. 2012 évi C törvény a Büntető Törvénykönyvről

4. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

5. 26/2013. (X. 21.) Közigazgatási és Igazságügyi Miniszteri rendeletet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

Brehel József

Kiberbiztonság – az információs társadalmi környezet kockázatai

Kiberbiztonsági helyzetkép, kockázatelemzés és kockázatértékelés.

1. Bevezetés, hazai és Európai helyzetkép

A hazai és az európai kiberbiztonsági helyzetkép összefoglaló ismertetése érdekében néhány idézettel kezdem, amelyek az elektronikus, illetve írott sajtóban jelentek meg a témában. Egy előadás is ide kívánkozik a teljesség érdekében:

„Rajnai Zoltán, Magyarország kiberkoordinátora előadást tartott – Velem vagy mellettem? címmel a ITBN budapesti IT- és Kiberbiztonsági konferencián. „

Az előadás alcíme: „A magyarországi kormányzati kiberkoordináció helyzete, az állami és piaci szereplők együttműködésének formái”[14] volt.

Ennek kapcsán fogalmazódott meg néhány gondolat és készültek innovációs lehetőséget is tartalmazó javaslatok, melyeket a hazai kibervédelmi körképet követően ismertetünk.

IDÉZETEK:

„Kezdjük mindjárt a jó hírrel:

Az elmúlt időszakban nem történt nagy veszteséget okozó kár a kormányzati hálózatokban. – mondta még az előadása elején Rajnai Zoltán, Magyarország kiberkoordinátora..”

Megjegyzés: Ez persze nem jelenti azt, hogy nem is történik ilyen a jövőben.

KÉRDÉS: Felkészültünk-e erre? És ha igen akkor milyen mértékben?

Az ezt biztosító magyar kibervédelem gyakorlati oldala éppen egy évvel ezelőtt alakult át és vette fel a mai formáját, középpontban a Nemzeti Kibervédelmi Intézettel.

2. HAZAI HELYZETKÉP

2.1 „Egy kézben a magyar kibervédelem[9]

„Központosított a kormányzat, de ez egyáltalán nem biztos, hogy jó. Van olyan eset, amikor több hivatal helyett nem biztos, hogy jobb a kevesebb, a kibervédelem összetett kérdése pont ilyen lehet. A NATO jelentése[9] egyelőre csak bemutatja az új helyzetet." Rajnai erről ezúttal nem beszélt, inkább a jogalkotói oldalt mutatta be.

A lényeg röviden: 2013-ban a parlament elfogadta a Nemzeti Kiberbiztonsági Stratégiát.[10]

Ugyanebben az évben megszületett a ma is érvényben lévő infótörvény[11] ennek a stratégiának a megvalósítására.

A kormány egy rendelettel[12] létrehozta a Nemzeti Kiberbiztonsági Koordinációs Tanácsot és a Kiberbiztonsági Fórumot, hogy ezt a törvényt konkrét feladatokra bontsák és azokat végre is hajtsák. Olajozottan hangzik, igaz? A gyakorlatban persze ennél kicsit döcögősebb a történet:

2.2 A kormány biztonságot akar, a cégek eladni?

A tanácsnak viszont csak tanácsadási, javaslattételi jogköre van, még hat munkacsoportostól is. Konkrét technikai tanácsot nem adnak, hiszen;

Miniszterek, államtitkárok, valljuk be őszintén, talán a legkevesebbet fognak érteni ahhoz, hogy technikailag milyen megoldásokat lehet alkalmazni.

Ezért hozta létre az a bizonyos kormányrendelet a tanács mellett a Kibervédelmi Fórumot is. Itt keresik a technikai megoldásokat a problémákra, de itt már nem a kormányzati oldal, hanem a magánszektor, a szakma tesz javaslatokat a konkrét technikai megvalósításokra. A kiberkoordinátor, vagyis most Rajnai feladata pedig éppen a két oldal: a politikai és a piaci szereplők közötti közvetítés. Ha önnek ez kicsit lassúnak hangzik, akkor nem egyedül gondolja ezt, hanem Rajnai Zoltánnal együtt:

„Már most elkéstünk, amikor a legújabb kibervédelmi módszereket kell a támadások ellen kidolgozni” – mondta a kiberkoordinátor.

Rajnai szerint a vállalati szféra elsősorban abban érdekelt, hogy legyen minél könnyebben használható, így minél eladhatóbb ez a védelem, vagyis a hozzáférés az elektronikus adatokhoz. "Sajnos néha a cégek szándékosan gyengítik azt az információbiztonsági szintet, ami jogszabályi oldalról elvárt lenne" – mondta a cégek képviselői előtt állva. Két éve épp az ITBN zárásaként hangzott el, hogy ha nem történik valami nagy változás,

„Magyarország a személyes adatai kétharmadát nem fogja tudni megvédeni.

Minden 4 adatból 3 felfedésre, eltulajdonításra kerül.”

Újabb pontban érthetünk egyet a kiberkoordinátorral, ha ön is azt gondolja, hogy ez óriási probléma. Rajnai szerint ha nem tudjuk megvédeni az adatainkat, úgy járhatunk, mint az Egyesült Államok, ahol tavaly sok millió társadalombiztosítási adatot tudtak ellopni a hekkerek. De említhette volna éppen a több amerikai állam választói adatbázisa elleni támadásokat is, amelyekből legalább az egyik bevallottan sikeres volt. Abba most ne is gondoljunk bele, hogy mi lenne velünk, ha a magyar adatokat övezné olyan érdeklődés, mint az amerikaiakat.

2.3 Az ITBN CONF EXPO 2016

A konferencián Rajnai beszélt még arról is, hogy szintén nagyon fontos a kritikus infrastruktúrák kibervédelme. Ezt elsősorban az Országos Katasztrófavédelmi Főigazgatóság látja el, de a kiberkoordinátor szerint nem szabad magára hagyni ebben a katasztrófavédelmet, mert ott nincs meg az a szakmai tudás, ami önmagában elég lenne a szükséges védelem biztosításához.

Szintén fontos még az információmegosztás, ami Rajnai szerint az amerikai kibervédelem első számú pillére, itthon viszont még van hova előre lépni ebben. Kell is hova, hiszen a hálózati és információs rendszerek biztonságáról szóló NIS-irányelvet a közelmúltban fogadta el az Európai Unió, és ennek az elemeit 2018-ig át kell ültetni a hazai kibervédelembe is.

3. EURÓPAI HELYZETKÉP

3.1 Európa felkészül a kiberháborúra

„Életbe lépett az első uniós kiberbiztonsági szabályozás. Ideje volt, mert egyre több a veszély. Itthon egész jól állunk, de azért van még teendő.”

Ezzel az idézettel még találkozni fogunk.

Az Európai Unió már évek óta dolgozik azon, hogy megerősítse a kontinens kiberbiztonságát. Van is miért, évről évre egyre több a fenyegetés, egyre gyakoribbak a támadások. A személyes adataink védelmére hozott közelmúltbeli rendelet után most újabb kirakósdarab, a legfontosabb európai szolgáltatások védelmére hivatott NIS-irányelv is hatályba lép. Az EU-ra jellemző komótos tempóban, de lassan összeáll a 21. századhoz igazított kibervédelem. Na és Magyarországra milyen feladatok várnak?

Miközben a társadalmunk egyre elképzelhetetlenebb internet vagy mobileszközök nélkül, és a gazdaság is egyre nagyobb részben támaszkodik digitális infrastruktúrákra, ez a rengeteg pozitívummal járó átalakulás egyben beláthatatlan biztonsági kockázatot is hozott.

3.2 A hekkerek, akik 17 millió forintot kerestek több százmillió jelszón

Ez viszont csak az az összeg, amit az adatok eladásából szereztek. Valószínűleg évekig saját célra használták ezeket, és jó eséllyel az ön jelszava is a neten kering. Lépésről lépésre bemutatjuk, hogyan védheti meg magát.

Szinte hetente derül fény újabb és újabb durva adatlopásokra, azt pedig mi magunk is teszteltük, hogy még a privát wifihálózatok sincsenek biztonságban. Az utóbbi években viszont az egy-egy céget vagy a felhasználók adatait érintő veszélyek mellett megszaporodtak a kritikus infrastruktúra elleni támadások is. 2007-ben például Észtországot érte átfogó kibertámadás, a kórházakat sorban fertőzik meg a zsarolóvírusok, és tavaly történt az ukrán elektromos hálózat addig példátlan meghekkelése is. Oroszországgal szemben pedig gyakorlatilag jelenleg is folyik a kiberháború.

3.3. Javában zajlik a kiberháború Oroszországgal

Az észak-európai országok nem csak az online hadviseléstől tartanak, az információs hadviselésben pedig a V4-ek is célpontok.

A példákat persze lehetne még sorolni: egy felmérés szerint 2015-ben 38 százalékkal több kiberbiztonsági incidenst jelentettek globálisan, mint egy évvel korábban. Ezért egyre nagyobb szükség van összehangolt stratégiára és a gyakorlatban is hasznos szabályozásra. Már csak azért is indokolt a közös EU-s fellépés, mert nemcsak a szolgáltatások nyúlnak át ma már rutinszerűen az országhatárokon, de egy-egy hálózat- vagy információbiztonsági incidens is kihathat az egész Unióra.

3.4 Az EU kiterjeszti a biztonságot. Ennek egyik pillére a GDPR

Ebben a helyzetben nem csoda, hogy az EU a maga bürokratikus megfontoltságával, de sorban fogadja el a biztonságosabb digitális mindennapok megteremtésére hivatott szabályozásokat. Korábban leginkább csak a távközlési és az internetszolgáltatók voltak kénytelenek foglalkozni a kiberbiztonsággal, mert csak rájuk vonatkoztak az EU által 2012-ben bevezetett hálózatbiztonsági, adatvédelmi és incidens bejelentési kötelezettségek. Az új szabályozások egyik célja éppen ennek a kiterjesztése a távközlési piacon túlra is.

Az EU új információbiztonsági rendje két fő pillérre épül. Az egyik a tagországok adatkezelését közös nevezőre hozó általános adatvédelmi rendelet, a **GDPR**. Ez az európai állampolgárok személyes adatait védi minden eddiginél alaposabban, és egységes működési keretet biztosít az ezeket az adatokat kezelő cégeknek.

3.5 Sosem látott szigor jön az adatvédelemben

Hatályba lépett az új EU-s adatvédelmi rendelet, amely nagyobb felhasználói kontrollt és egységes szabályozást ígér. De mi változik, hogyan és miként érinti ez a felhasználókat?

3.6 A második pillér a NIS

A másik pillér pedig az augusztus elején frissen életbe lépett, a hálózati és információs rendszerek biztonságáról szóló irányelv, vagyis a **NIS**. Ez az első uniós szintű kiberbiztonsági szabályozás, amely az EU szerint segíthet megelőzni az európai infrastruktúra elleni kibertámadásokat. Július 6-án hagyta jóvá az Európai Parlament (EP), és augusztus 8-án lép hatályba. Célja közös nevezőre hozni a tagállamok kibervédelmét, meghatározni egy közös biztonsági minimumot, és ehhez közös eszköztárat – intézményi rendszert, szabályozást – adni a kezükbe.

Az irányelv legfontosabb jellemzői dióhéjban:

- Két csoportra vonatkozik: az alapvető szolgáltatást nyújtó szolgáltatókra (vagyis a kritikus infrastruktúrára) és a digitális szolgáltatókra.
- Komolyabb biztonságot követel meg, és kötelező incidens bejelentést ír elő kibertámadások esetén.

- A tagállamoktól saját kiberstratégia és felügyeleti intézmények létrehozását várja el, illetve lefekteti a tagállamok közötti kötelező együttműködés kereteit.

4. Az európai infrastruktúra védelme

„A NIS nem általános szabályozás, hanem két konkrét csoportra vonatkozik, azokra, amelyeknek a megtámadása a legérzékenyebben érinti a társadalmat. Az egyik ilyen halmaz az alapvető szolgáltatást nyújtó szolgáltatóké: digitális infrastruktúrák, energiacégek, ivóvízellátók, közlekedési vállalatok, egészségügyi szolgáltatók, banki szolgáltatások, pénzügyi piaci infrastruktúrák tartoznak bele. Az ide sorolandók pontos körét a tagállamok maguk határozzák meg az alapján, hogy az adott szervezet szolgáltatása alapvető-e a társadalom vagy a gazdaság számára, ennek a szolgáltatásnak a biztosítása függ-e hálózati és információs rendszerektől, illetve egy kiberbiztonsági incidens jelentős zavart okozna-e a szolgáltatásban.”

"Ezeken az ágazatokon belül sem mindenre és mindenkire vonatkozik, hanem csak azokra a konkrét szolgáltatásokra, amelyeknek a kiesése komoly társadalmi vagy gazdasági károkat okozna. Ha egy kibertámadás nagyobb fennakadást okoz egy ország áramellátásában, az ide tartozik. Ha a támadás viszont csak az adott áramszolgáltató marketingrészlegét lövi le két-három napra, akkor nem biztos. Az első esetben ugyanis a kritikus infrastruktúra védelme és a lakosság alapvető áramellátása közvetlenül sérülnek, a másodikban viszont csak az adott szolgáltató szenved el némi üzleti kellemetlenséget." – magyarázta az Indexnek Précsényi Zoltán, aki a Symantec biztonsági cég brüsszeli kormányzati kapcsolati menedzsereként részt vett az új szabályozások előkészítésében.

A másik érintett csoportba azok a digitális szolgáltatásokat nyújtó szolgáltatók tartoznak, amelyek ugyan nem nélkülözhetetlen, de fontos társadalmi hatású szolgáltatásokat kínálnak: az online piacterek, a keresőszolgáltatások és a felhőszolgáltatók. (Az irányelv korábbi tervezetében a közösségi oldalak is szerepeltek, de a végleges változatból kikerültek – vagyis kimondatott, hogy Facebook nélkül is van élet.) Fontos, hogy azokra a szolgáltatókra is vonatkozik a NIS, amelyek az EU-n kívüliek, de itt is szolgáltatnak, tehát például az amerikai Amazonra vagy Google-re. Ugyanígy, a brexit ellenére a brit cégeknek is meg kell felelniük az irányelvnek, ha az EU-n belül működni akarnak.

4.1 Nagyobb szigor, kötelező jelentések

Nagyobb a szigor, náluk a tagállamok hatóságai ellenőrizhetik, hogy milyen biztonsági lépéseket terveznek, és hogy ezeket a gyakorlatba is megfelelően átültetik-e.
Jelentős átfedés van a két új szabályozás, a GDPR és NIS rendelkezései között, hiszen mindkettő meghatároz biztonsági előírásokat és incidens bejelentési kötelezettséget.

A két jogszabály két különböző aspektusból és két különböző cél érdekében támaszt egyébként eléggé hasonló elvárásokat.

Teljesen más irányból közelít viszont a két szabályozás, és más típusú incidensekre vonatkoznak:

- A GDPR célja a személyes adatok és a magánszféra védelme, ezért a központjában a felhasználó áll. A NIS-ben a hálózatvédelmen van a hangsúly, és a szolgáltatókra hegyezték ki.

- A GDPR minden cégre vonatkozik, amelyik európai állampolgárok személyes adatait kezeli, a NIS hatásköre jóval szűkebb, csak a legfontosabb szolgáltatásokra összpontosít.

- A GDPR szerint akkor kell bejelenteni egy biztonsági incidenst, ha személyes adat forog kockán, a NIS alatt akkor, ha az adott szolgáltatás kerül veszélybe.

- Ha személyes adat kompromittálódik, a GDPR értelmében az adott cég köteles az adat tulajdonosát, vagyis a felhasználót is értesíteni, a NIS hatálya alá tartozó cégeknek elég a felügyelő hatóságnak bejelentést tenni "jelentős hatású" hálózati incidens esetén.

Hogy mennyire számít jelentős hatásúnak egy biztonsági esemény, attól függ, hány embert érint a szolgáltatás-kimaradás, mennyi ideig tart, és földrajzilag mennyire kiterjedt; illetve a digitális szolgáltatók esetében még attól is, hogy milyen mértékű zavart okoz a szolgáltatásban, és mekkora hatást gyakorol az adott szolgáltatásra épülő gazdasági és társadalmi tevékenységekre. A tagállamoknak e szempontok szerint kell majd pontosan meghatározniuk a feltételeket, amikor átültetik az irányelvet a maguk nemzeti jogrendjébe.

Mindkét csoport számára két fontos változást hoz az irányelv. Egyrészt a kockázatokkal arányos mértékű hálózat- és rendszerbiztonságot kell garantálniuk, másrészt be kell jelenteniük az illetékes nemzeti hatóságnak, ha mégis valamilyen jelentős biztonsági incidens éri őket. Az alapvető szolgáltatások esetében viszont

4.2 Szorosabb európai együttműködés

„A kibertámadások gyakran egyszerre több tagállamot érintenek, a szétforgácsolt védelem sebezhetővé tesz minket.”

– mondta Andreas Schwab, az Európai Parlament illetékes jelentéstevője a NIS elfogadásakor, amelynek éppen az a fő célja, hogy szorosabbra fűzze az együttműködést. Ehhez a tagállamoknak több feladatuk is van az irányelv élesedéséig hátralévő 21 hónapos türelmi időben. A főbb feladatok:

- A NIS alapján ki kell dolgozniuk egy nemzeti hálózat- és információbiztonsági stratégiát.
- Ki kell jelölniük egy nemzeti hatóságot, amely felügyeli a NIS átültetését és végrehajtását.
- Ki kell jelölniük egy vagy több gyors reagálású kibervédelmi csapatot, ezek az úgynevezett CSIRT-ek (Computer Security Incident Response Team) vagy CERT-ek (Computer Emergency Response Team). (A kettő ma már szinonimának számít, az EU a CSIRT kifejezést használja, Magyarországon inkább a CERT-et preferálják a hatóságok.)
- Szektoronként meg kell határozni, pontosan milyen kritériumok alapján számít egy-egy cég az irányelv hatálya alá, és ezután a konkrét cégeket is ki kell jelölni. Erre a 21 hónapos átültetés után még további 6 hónapja lesz a hatóságnak.
- EU szinten pedig létre kell hozni a kiberbiztonsági csapatok együttműködését koordináló CSIRT-hálózat, illetve a nemzeti hatóságok együttműködését segítő Együttműködési Csoportot is. Mindkét szervezet felállítására fél éve van az EU-nak – vagyis a tagállamoknak közösen –, de érezhetően gyorsan akarnak haladni, ezért ezeket már el is kezdték előkészíteni.

A szabályozás részleteinek a kidolgozására az Európai Bizottság létrehozott egy szakértői csoportot még májusban. Ennek magyar részről a Nemzeti Kibervédelmi Intézet (NKI) a

tagja, és általában is az egész kiberbiztonsági szervezkedésben ők képviselnek minket, ezért őket kérdeztük arról, milyen feladatok állnak még Magyarország előtt, és mit várnak az új irányelvtől. Itt volt már az ideje

A GDPR-t 2018 májusától kezdik alkalmazni (közvetlenül, hiszen az egy rendelet), és a NIS-t is ugyaneddig kell átültetni a nemzeti jogrendekbe (mivel az csak irányelv). Vagyis alkalmazni a gyakorlatban.

5. 2018-ra áll össze az új európai kiberpáncélzat.

Annyi biztos, hogy már épp ideje is lesz, mert a kiberbiztonság gyorsan változó terület, az EU malmai viszont lassan őrölnek: a GDPR-t 2012-ben kezdték kidolgozni, a NIS első tervezete 2013-as, vagyis mire életbe lépnek, már 5-6 évesek lesznek.
"Az eredeti javaslatok évekkel ezelőtti beterjesztése óta végeláthatatlan viták zajlottak Brüsszelben arról, hogy azok életképesek, indokoltak, arányosak-e." – mondja Précsényi. Egyesek sokkal nagyobb szigort követeltek, mások már így is túlszabályozással riogattak. Viszont amikor tavaly decemberben már látszott, hogy milyen lesz a végleges változatuk, akkor a szakmán belül a vitát felváltotta a verseny: ki milyen gyorsan, milyen ügyesen lesz képes alkalmazkodni az új szabályokhoz, és milyen hatékonyan fog élni a bennük rejlő új lehetőségekkel. 2018-ig a legfontosabb itthoni tennivaló, hogy meg kell ismertetni az új szabályokat az érintett ágazatok szereplőivel, és együtt kidolgozni a megvalósítás részleteit. Ki kell jelölni a azokat a cégeket is, amelyekre konkrétan vonatkozni fognak itthon az új előírások. Mindeközben a részletek EU-s szintű kidolgozásában is részt kell venni: az Együttműködési Csoport beindításában, illetve az incidensek bejelentése pontos menetének meghatározásában.

6. A Kiberbiztonsági kockázatok elemzése és kezelése

6.1 Kiberbiztonsági állapotfelmérést és helyzetelemzést, kockázatelemzést és akcióterv kidolgozását támogató megoldás

IDÉZET: *„Életbe lépett az első uniós kiberbiztonsági szabályozás. Ideje volt, mert egyre több a veszély. Itthon egész jól állunk, de azért van még teendő.”*

Kezdjük ezzel az idézettel és ennek kapcsán gondoljuk végig, hogy hogy is és hol is állunk (merre haladunk) ma Magyarországon a kibervédelem, kiberbiztonság terén (hazai helyzetkép, helyzetfelmérés) és milyen teendőink vannak ebből a helyzetből adódóan, továbbá az EU-s jogszabályi megfelelés tekintetében az elkövetkezendő években.

Az idézet: - amely a sajtóban megjelent fenti „Európa felkészül a kiberháborúra” c. cikkből származik, még egyszer tehát:

„Életbe lépett az első uniós kiberbiztonsági szabályozás. Ideje volt, mert egyre több a veszély. Itthon egész jól állunk, de azért van még teendő.” Ennek kapcsán néhány kérdés és gondolat merül fel:

Mit is jelent pontosan az, hogy „egész jól állunk”? – mire alapozza ezt a kijelentést a tisztelt cikkíró? A mérnökben az alábbi kérdések merülnek fel:

Volt felmérés ebben a témában? Ha igen, milyen körben? Milyen módszertannal?

Ezek ismeretében és eredményeképpen kijelenthetjük-e, hogy egész jól állunk?

NEM HISZEM. EZ CSAK EGY BECSLÉS LEHET, AMI VAGY IGAZ, VAGY NEM. AZ ÁLLÍTÁST MILYEN SZÁMOKKAL ÉS TÉNYEKKEL - BIZONYÍTÉKOKKAL TUDJUK ALÁTÁMASZTANI?

ÉN ÚGY GONDOLOM, HOGY NEM TUDOM, NEM TUDJUK PONTOSAN, HOGY IS ÁLLUNK VALÓJÁBAN! DE MEGTUDHATJUK.

HOGYAN?

6.2 A javaslat:

VÉGEZZÜNK EGZAKT TUDOMÁNYOS ALAPOKON NYUGVÓ FELMÉRÉST, (ÖNÉRTÉKELÉST) ÉS AZ EREDMÉNYEK ÉRTÉKELÉSE, ELEMZÉSE ALAPJÁN ADJUNK PONTOS HELYZETKÉPET. EHHEZ A MÓDSZERTAN ÉS AZ ESZKÖZ IS ADOTT.

6.3 A módszertan és az eszköz:

A JAVASOLT FELMÉRÉSI ESZKÖZ: A NIST – (National Institute of Standards and Technology, továbbiakban: NIST) Cyber Security Excellence Builder Toolkit (Draft/Tervezet) dokumentuma. Ennek az eszköznek, mint papíralapú kérdőívnek a későbbiekben - várhatóan és vélhetően a jövő év, 2017 elején - új elektronikus verziója is lesz (Excel vagy egyéb program támogatás). Ezért célszerű az alábbi linken is megtalálható (CEBEREYE) Blog és/vagy a NIST Institute weblapok figyelemmel kísérése.

A cikk angol nyelvű linkje:

- **NIST offers cyber self-assessment tool, updates email security guidance**

A NIST kiadott egy biztonsági felmérést és értékelést támogató új eszközt, amely segítségével a szervezetek jobban megérthetik, felmérhetik, pontosabb ismeretek birtokába juthatnak saját kiberbiztonságuk és annak menedzselésével kapcsolatos helyzetük, erőfeszítéseik és előre haladásuk tekintetében.

A NIST által javasolt Kiberbiztonsági önértékelési eszköz (Tervezet, 2016 Szeptember)

Az eszköz elsősorban a versenyszféra képviselőire került kifejlesztésre, de értelemszerűen elvei és gyakorlata jól alkalmazhatók az állami, kormányzati szektorban is. Minél szélesebb a felmérés köre, annál pontosabb képet kaphatunk arról, hogyan is állunk valójában és melyek a teendőink a jövőben.

7. Kibervédelmi kiválóság fejlesztési és állapot felmérési eszköz (angol verzió, tervezet).

Baldrige Cybersecurity Excellence Builder

Key questions for improving your organization's cybersecurity performance
Draft September 2016

National Institute of Standards and Technology (www.nist.gov)

7.1 Az eszköz összefoglaló ismertetése

Az új eszköz - USA Nemzeti Szabványügyi és Technológiai Intézete (a NIST) szerint – az általuk bevezetett és alkalmazott folyamat segítségével a felhasználó szervezetek felmérhetik a Kiberbiztonsági helyzetüket, - Kiberbiztonsági karakterisztika és szükséges stratégiai lépések, valamint képesek lesznek az alábbiakra:

- **Meghatározhatók azok a kiberbiztonsággal kapcsolatos tevékenységek, amelyek fontosak az üzleti, ügymeneti stratégia és a kritikus szolgáltatások biztosítása szempontjából.**

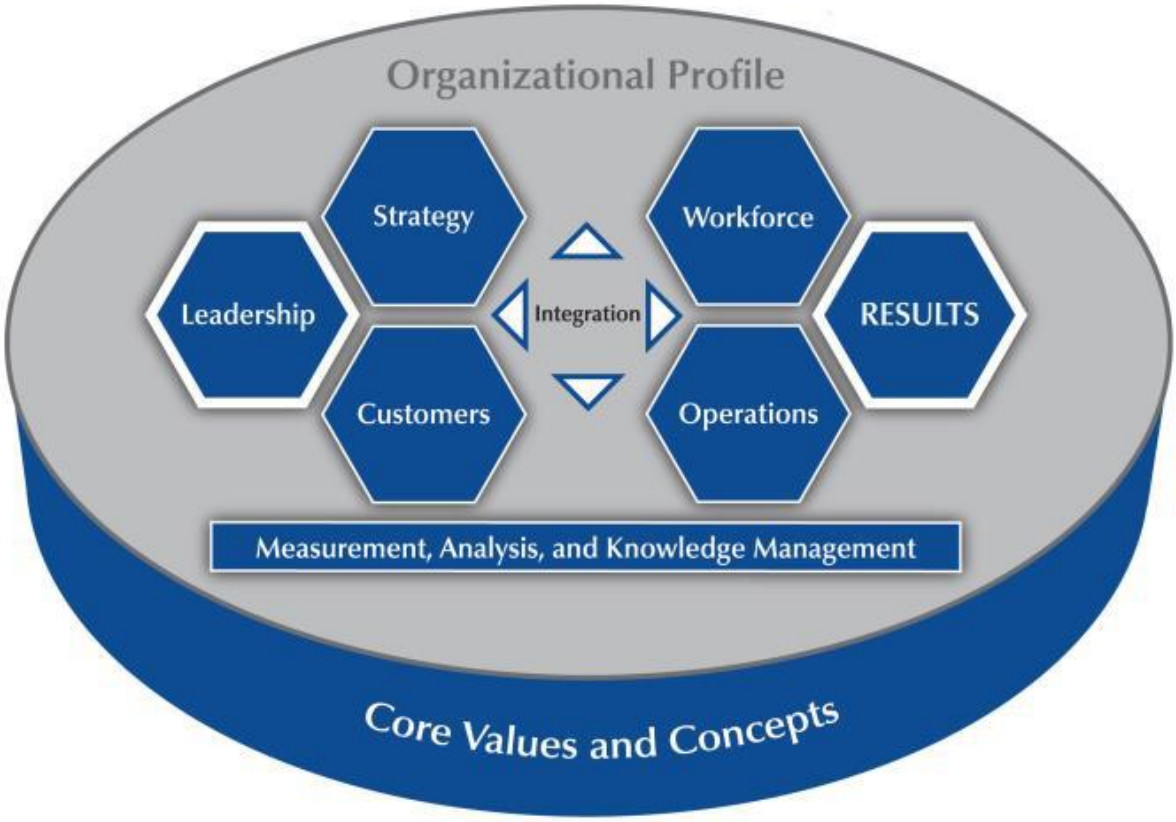
- **Priorizálhatók, rangsorolhatók a kiberbiztonsági kockázatkezelési intézkedések és kiadások, beruházások.**
- **Felmérhetők az alkalmazott kibervédelemmel kapcsolatos alkalmazott szabványok, irányelvek és gyakorlati megoldások hatékonysága és eredményessége.**
- **Felmérhetők a kiberbiztonsági eredmények**
- **Azonosíthatók és rangsorolhatók a szükséges továbbfejlesztések.**

A felmérés, önértékelés eredményeként az adott szervezet Fejlettségi/Érettségi besorolást kap – melynek szintjei lehetnek: reaktív/reagáló, korai, fejlett, vagy szerep alapú modell – és ennek ismeretében minden szervezet kidolgozhatja saját fejlesztési intézkedési tervét és megalapozott döntéseket hozhat a kiberbiztonság javítása, szükséges szintjének emelése érdekében. **Fentiek miatt javasoljuk és tekintjük a tanulmány fő tárgyának az említett eszközt.**

A továbbiakban az alkalmazással, az eszköz használatának módjával, a kérdésekkel és a várható gyakorlati eredményekkel foglalkozunk.

7.1.1 Az (ön-)értékelés elemei és folyamata

Szervezeti profil és kontextus – (Az 1. sz. ábra: A „Baldrige Excellence Framework” alapján)



1. sz. ábra: A szervezeti profil kiberbiztonsági vonatkozású összetevői, komponensei. Forrás: NIST, Baldrige Cybersecurity Excellence Builder, DRAFT.

(Framework for Improving Critical Infrastructure Cybersecurity, by NIST) – Keretrendszer szempontjai alapján és elemeinek figyelembe vételével került kidolgozásra a NIST által.

7.2 Kik a potenciális felhasználói az eszköznek?

- Az Igazgatótanács és az igazgatók, végrehajtó menedzserek, vezetők
- Az Informatikai igazgató (CIO)
- Az információbiztonsági vezető (CISO)
- Az IT folyamatgazdák és folyamat menedzserek
- KOCKÁZATKEZELÉSI SZERVEZETÍEK ÉS –SZAKEMBEREK, AUDITOROK

- Jogi megfelelőségi (Compliance) szervezetek és menedzserek
- Alkalmazottak, munkatársak

7.3 Hogyan használhatják a szervek, szervezetek az eszköz t a kiberbiztonsági kockázatok menedzselésének felmérésének és fejlesztésének érdekében?

Alapvetően 17 tétel (plusz 2 a „Szervezeti környezet"-témakörben), mindegyik elem területi fókusszal. Ezek az elemek három csoportra oszthatók az információk típusától függően, amelyekre vonatkozóan kérdéseket fogalmaznak meg:

7.3.1 Szervezeti környezet (C) amely a kiberbiztonsági kockázatkezeléssel kapcsolatos szervezeti információk és annak környezete.

7.3.2 Folyamat elemek (1-6 kategória), a kérdések a szervezet kiberbiztonsági folyamatokra irányulnak.

1. Vezetés, Leadership
2. Stratégia, Strategy
3. Ügyfelek, Customers
4. Mérés, Elemzés és Tudásmenedzsment
5. Munkaerő
6. Működés, Operations

7.3.3 Eredmény elemek (7. kategória) kérdései a szervezet kiberbiztonsági folyamataival kapcsolatos eredmények jelentéseire irányulnak.

7.3.4 Az Értékelő fejezet (az eredeti dokumentum 25. oldalán található) segít értékelni a kiberbiztonsági folyamatok hatékonyságát és eredményességét – csakúgy, mint a Kiberbiztonsággal kapcsolatos elért eredmények minőségét és ezek összességét – azaz hogyan működnek ezek rendszerként.

7.4 Az eszköz „Használati Utasítása” – Hogyan használhatjuk, melyek a lépései a kiberbiztonsággal kapcsolatos erőfeszítések értékelési folyamatának?

7.4.1 A felmérés hatókörének megállapítása: mi képezi a vizsgálat tárgyát?

A *Baldrige Cybersecurity Excellence Builder – a legértékesebb önértékelési eszköz egy teljes szervezet kiberbiztonsági kockázat menedzsment programjának értékelésére, de alkalmas* és hasznos lehet egy szervezeti egység, vagy több szervezeti egységből álló csoport, szervezeti részek felmérésére is.

7.4.2 A szervezeti környezet meghatározása, a kérdések megválaszolása

A szervezeti környezet c. fejezet kritikus fontosságú az alábbi okokból:

- Segít azonosítani az esetleges eltéréseket a kulcs információk és a kulcs kiberbiztonsági teljesítőképességi követelmények és eredmények között.
- ***Használhatjuk kezdeti/első felmérés eszközekénz is (baseline – alapvonal). A kérdések megválaszolása során felmerülő esetleges ellentmondásos területek, vagy kiderülő hibák, illetve hiányosságok (információk vagy megoldások hiánya) azonosítása segítségével akcióterv alkotható ezek megszüntetésére, fejlesztésre, előre lépésre.***
- Meghatározza a kontextust és lehetővé teszi, hogy feltárjuk az adott szervezet speciális, egyedi vonásait, kiberbiztonsággal kapcsolatos igényeit, a többi Baldrige Cybersecurity Excellence Builder kérdésre adott válasz segítségével.

7.4.3 - A 7.3.2 pont Az 1-6. kategória kérdéseinek megválaszolása

Sok kérdés „Hogyan”-nal kezdődik. Ezeknek a hogyanoknak a megválaszolása során fontos információkat adunk az adott szervezet kiberbiztonsággal kapcsolatos *kulcs folyamatairól:* ***(M-H-TK-I)***

- ***Megközelítés*** *(Approach): Hogyan történik a szervezet kiberbiztonsággal kapcsolatos feladatainak végrehajtása? Mennyire szisztematikusak (rendszeresek, módszeresek) a meglévő kulcsfolyamatok?*
- ***Használat, elterjesztés*** *(Deployment): Mennyire következetesen használják a kiberbiztonsággal kapcsolatos kulcsfolyamatokat a szervezet releváns szervezeti egységei?*

- ***Tanulás és kommunikáció*** *(Learning): Értékelték és továbbfejlesztették az adott szervezet* kiberbiztonsággal kapcsolatos *kulcsfolyamatait?* Az eredményeket megosztották a szervezeten belül?
- ***Integráció*** *(Integration): Mennyire fedi le a kiberbiztonsággal kapcsolatos folyamatok kezelése a jelenlegi és jövőbeli szervezeti igényeket, követelményeket?*

A 7.4.4 – A 7.3.3 pont – a 7. kategória kérdéseinek megválaszolása

Ezekben az elemekben információt adunk a kérdések megválaszolásával azokról a Kiberbiztonsággal kapcsolatos eredményekről, amelyek a legfontosabbak szervezet sikeressége szempontjából: **(SZTÖI)**

- ***SZINTEK****/(Levels): Melyek a kulcs mutatói, mérőszámai a kiberbiztonsággal kapcsolatos folyamatok hatékonyságnak és eredményességének, mi a kiberbiztonsági teljesítmény, teljesítőképesség aktuális szintje?*
- ***TRENDEK****/(Trends): Az eredmények fejlődő, stagnáló vagy hanyatló, visszaeső tendenciát mutatnak?*
- ***ÖSSZEHASONLÍTÁSOK****/(Comparisons): Milyen a szervezet helyzete, eredményei kiberbiztonság tekintetében más szervezetekhez, versenytársakhoz képest, vagy Összemérés (Banchmarking) tekintetében?*
- ***INTERGRÁCIÓ****/(Integration): A kiberbiztonsággal kapcsolatos - a szervezet szempontjából fontos eredményeket monitorozzák és rögzítik? Figyelembe veszik a tulajdonosok és a kulcs személyes igényeit, elvárásait? Figyelembe veszik aza eredményeket a döntéshozatali folyamatokban?*

7.4.5 Alkalmazzunk egy LEÍRÓT minden egyes kérdés elemre adott válasz során

Az eredeti dokumentumban a 25. 26. oldalon lévő folyamat és az eredmények fejezetek használatával rendeljünk hozzá egy leírót, amely lehet: - **Reaktív, Korai, Fejlett vagy Szerep modell** - leíró társítása minden válaszhoz.

7.4.6 Priorizáljunk, rangsoroljunk minden tevékenységet

Jelezzük a fontosságot is (Magas, Közepes, Alacsony) minden egyes elemre, kérdésre adott válasz során a sikeres kiberbiztonsági menedzsment érdekében.

A kiberbiztonsági kockázatkezelési program erősségeire alapozva, fejlesszük tovább az elért eredményeket. Ezeknek az erősségeknek és eredményeknek a többi szervezeti egységgel való megosztása révén felgyorsíthatjuk a fejlesztés folyamatát.
Állítsuk rangsorba a lehetőségeket, a kiberbiztonsági folyamatok és eredmények fejlesztendő területeit is: mivel lépésenként haladhatunk csak, nem tudunk mindent egyszerre végrehajtani. Gondoljuk meg melyek a szervezet szempontjából legfontosabbak jelenleg. Teremtsünk egyensúly a tulajdonosi, vezetői igények és elvárások és a lehetséges erőforrásokkal elérhető elvárható eredmények között és döntsük el a végrehajtási sorrendet, mit hajtsunk végre először.

8. Dolgozzunk ki akciótervet, valósítsuk meg, mérjük és értékeljük az előrehaladást

Ahogy reagálunk a kérdésekre és felmérjük a válaszokat az adott fejezetben, akkor kezdjük beazonosítani az erősségeket és gyenge pontokat, először a kategóriákon belül, majd azok között is. Hangoljuk össze, koordináljuk a legfontosabb folyamatok közötti kapcsolatokat, továbbá a folyamatok és az eredmények közötti összefüggéseket, ezek vezethetnek el javítási ciklusokhoz.
Az eszköz további folyamatos használata során egyre többet és többet tudhatunk meg szervezetünkről és meghatározhatjuk az erősségekre építés, az eltérések megszüntetésének és az innováció legjobb módját.
Ennek az önértékelésnek a teljesítésével megtehetjük az első lépést, megfelelve és eleget téve a *Cybersecurity Framework,* section 3.0 pontjában javasoltaknak: (“How to Use the Framework” – Hogyan használjuk a keretrendszert):

8.2 A kiberbiztonsági folyamatok alapvető felmérése, áttekintése

Az önértékelési eszköz kérdéseire adott válaszok során szerzett információkat hasonlítsuk össze az aktuális tevékenységeinket azokkal a kiberbiztonsági tevékenységekkel, amelyek a „*Cybersecurity Framework* Core” dokumentumban szerepelnek.

8.3 Kiberbiztonsági program létrehozása vagy továbbfejlesztése

Használjuk a válaszokat, amelyeket az önértékelési kérdésekre adtunk, hogy tájékoztassuk a hét lépés létrehozásában vagy bővítésében a kiberbiztonság program tekintetében. (lásd a mellékletet).

8.4 A kiberbiztonsági követelmények kommunikációja a tulajdonosokkal, vezetőkkel

A kérdésekre adott válaszok segítségünkre lehetnek egy „Célprofil" létrehozásában és az egyeztetésben a menedzserekkel, vezetőkkel, tulajdonosokkal, döntéshozókkal a kiberbiztonsági kockázatkezelési követelményrendszer tekintetében.

9. SZK – Szervezeti környezet („C" – as Context in original document)

SZK.1 A szervezet leírása: Melyek a szervezet kulcs karakterisztikái?

a. Szervezeti környezet

(1) TERMÉKEK ÉS SZOLGÁLTATÁSOK

(2) KÜLDETÉS, JÖVŐKÉP ÉS ÉRTÉKEK

(3) MUNKAERŐ PROFIL

(4) VAGYONTÁRGYAK, ESZKÖZÖK

(5) JOGI ÉS SZABÁLYZATI KÖVETELMÉNYEK

b. Szervezeti kapcsolatok

(1) Szervezeti Struktúra

(2) Ügyfelek és érdekeltek

(3) Szállítók és Partnerek

TÁBLÁZATOK ÉS MUNKALAPOK [16]

Értékelési kategóriák (1-6.) Folyamatok [16]

Process (Categories 1–6)

Maturity Level	Evaluation Factor			
	Approach	Deployment	Learning	Integration
Reactive	CYBERSECURITY-related policies/operations are characterized by activities rather than by PROCESSES.	DEPLOYMENT of CYBERSECURITY-related APPROACHES to appropriate organizational units, and to CUSTOMERS, PARTNERS, and suppliers, as appropriate, is lacking.	Improvement in CYBERSECURITY-related policies/operations is achieved mainly in reaction to immediate needs or problems.	CYBERSECURITY-related goals are poorly defined; individual units within the CYBERSECURITY operations function independently of each other. There is no coordination between CYBERSECURITY-related policies/operations and those of the rest of the organization.
Early	CYBERSECURITY-related policies/operations are beginning to be carried out with SYSTEMATIC APPROACHES.	KEY CYBERSECURITY-related APPROACHES are beginning to be DEPLOYED to appropriate organizational units and to CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are beginning to be SYSTEMATICALLY evaluated and improved.	CYBERSECURITY-related strategy and quantitative GOALS are being defined. There is some early alignment among CYBERSECURITY operational units and, as appropriate, between CYBERSECURITY policies/operations and the rest of the organization.
Mature	Most elements of CYBERSECURITY-related policies/operations are characterized by SYSTEMATIC APPROACHES.	KEY CYBERSECURITY-related APPROACHES are well DEPLOYED to appropriate organizational units and to CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are SYSTEMATICALLY evaluated for improvement, and learnings are shared, with some INNOVATION evident.	CYBERSECURITY-related APPROACHES address KEY strategies and GOALS. There is alignment among CYBERSECURITY operational units and, as appropriate, between CYBERSECURITY policies/operations and the rest of the organization.
Role Model	Many to all elements of CYBERSECURITY-related policies/operations are characterized by SYSTEMATIC APPROACHES.	KEY CYBERSECURITY-related APPROACHES are fully DEPLOYED to appropriate organizational units and to CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations seek and achieve efficiencies through ANALYSIS, INNOVATION, and the sharing of CYBERSECURITY information and knowledge, including with the rest of the organization.	CYBERSECURITY-related policies/operations are INTEGRATED with current and future organizational needs defined by the organization; these policies/operations are well INTEGRATED with those of the rest of the organization.

Értékelési kategória (7. Eredmények) [16]

Results (Category 7)

Maturity Level	Evaluation Factor			
	Levels	Trends	Comparisons	Integration
Reactive	CYBERSECURITY-related RESULTS are missing, not used, or randomly reported.	TREND data are not reported or show mainly adverse TRENDS.	Available comparative information is not tracked.	CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are not tracked.
Early	The organization tracks some CYBERSECURITY-related RESULTS, and they show early good performance LEVELS.	Some TREND data are tracked, and some show improvement over time.	Some available, mainly internal, comparative information is tracked.	Some CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are tracked.
Mature	The organization tracks many CYBERSECURITY-related RESULTS, and they show good-to-excellent performance LEVELS.	Many CYBERSECURITY-related RESULTS show improvement or sustained high PERFORMANCE over time.	Results show good CYBERSECURITY-related PERFORMANCE relative to available information on competitors, other relevant organizations, or BENCHMARKS.	Many CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are tracked. RESULTS are beginning to be used in decision making.
Role Model	The full array of CYBERSECURITY-related RESULTS is tracked, indicating top performance.	The full array of CYBERSECURITY-related RESULTS is TRENDED over time, indicating improvement or sustained high PERFORMANCE.	Results indicate top CYBERSECURITY-related PERFORMANCE relative to available information on other organizations or BENCHMARKS.	All CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are tracked. The RESULTS are used in decision making.

Az önértékelési táblázatok [16]

Self-Analysis Worksheet

[Note: In its final form, this worksheet may be an Excel file with drop-down boxes and/or another type of non-paper-based tool.]

Process (Categories 1–6)	Reactive, Early, Mature, or Role Model?				High, Medium, or Low?
	Approach	Deployment	Learning	Integration	Importance
1 Leadership					
1.1 Senior and Cybersecurity Leadership: How do your senior and cybersecurity leaders lead your cybersecurity policies and operations?					
1.2 Governance and Societal Responsibilities: How do you govern your cybersecurity policies and operations and fulfill your organization's societal responsibilities?					
2 Strategy					
2.1 Strategy Development: How do you develop your cybersecurity strategy?					
2.2 Strategy Implementation: How do you implement your cybersecurity strategy?					
3 Customers					
3.1 Voice of the Customer: How do you obtain information from your customers?					
3.2 Customer Engagement: How do you engage customers by serving their needs and building relationships?					
4 Measurement, Analysis, and Knowledge Management					
4.1 Measurement, Analysis, and Improvement of Performance: How do you measure, analyze, and then improve cybersecurity-related performance?					
4.2 Knowledge Management: How do you manage your organization's cybersecurity-related knowledge assets?					
5 Workforce					
5.1 Workforce Environment: How do you build an effective and supportive workforce environment to achieve your cybersecurity goals?					
5.2 Workforce Engagement: How do you engage your workforce to achieve a high-performance work environment in support of cybersecurity policies and operations?					
6 Operations					
6.1 Work Processes: How do you design, manage, and improve your key cybersecurity work processes?					
6.2 Operational Effectiveness: How do you ensure effective management of your cybersecurity operations?					

Results (Category 7)	Reactive, Early, Mature, or Role Model?				High, Medium, or Low?
	Levels	Trends	Comparisons	Integration	Importance
7 Results					
7.1 Cybersecurity Process Results: What are your cybersecurity performance and process effectiveness results?					
7.2 Customer Results: What are your customer-focused cybersecurity performance results?					
7.3 Workforce Results: What are your workforce-focused cybersecurity performance results?					
7.4 Leadership and Governance Results: What are your cybersecurity leadership and governance results?					
7.5 Financial Results: What are your financial performance results for your cybersecurity operations?					

Evaluating Your Responses

1. **For each item (e.g., 1.1, 1.2) in categories 1–7 of the *Baldrige Cybersecurity Excellence Builder*, use the process and results rubrics on pages 24–25 to assign a descriptor (Reactive, Early, Mature, or Role Model) for each evaluation factor.**

For processes (categories 1–6), the evaluation factors are approach, deployment, learning, and integration (ADLI):

- *Approach* consists of the methods used to carry out a process, the degree to which your approach is systematic (i.e., repeatable and based on reliable data and information), the appropriateness of these methods to the item questions and your operating environment, and the effectiveness of your use of the methods.
- *Deployment* is the extent to which your approach is applied consistently and the extent to which it is used by all appropriate work units.
- *Learning* is the refinement of your approach through cycles of evaluation and improvement, the encouragement of breakthrough change to your approach through innovation, and the sharing of refinements and innovations with other relevant work units and processes in your organization.
- *Integration* is the extent to which your approach is aligned with the organizational needs identified in the Organizational Context section and in other process items. Integration also includes the extent to which your measures, information, and improvement systems are complementary across processes and work units; and the extent to which your plans, processes, results, analyses, learning, and actions are harmonized across processes and work units to support organization-wide goals.

For results (category 7), the evaluation factors are levels, trends, comparisons, and integration (LeTCI; "let's see").

- *Levels* are your current performance on a meaningful measurement scale.
- *Trends* are your rate of performance improvement or continuation of good performance in areas of importance (i.e., the slope of data points over time).
- *Comparisons* are your performance relative to that of other, appropriate organizations, such as competitors or organizations similar to yours, and your performance relative to industry leaders or relevant benchmarks.
- *Integration* is the extent to which your results address important performance requirements relating to customers, products/services, markets, processes, and action plans identified in the Organizational Context section and in the process items (categories 1–6). It also includes the extent to which your results reflect harmonization across your processes and work units to support organization-wide goals.

2. **Indicate the importance (high, medium, or low) of each item to the successful management of cybersecurity within your organization.**
3. **Prioritize your actions.**

Celebrate your strengths of your cybersecurity risk management program, and build on them to improve what you do well. Sharing the things you do well with the rest of your organization can speed improvement.

Prioritize your opportunities for improvement; you cannot do everything at once. Think about what is most important for your organization as a whole at this time, balancing the differing needs and expectations of your stakeholders, and decide what to work on first. Look at the next level in the rubric for how you might improve. Develop an action plan, implement it, and measure your progress.

Függelék a Baldrige Cybersecurity Excellence Builderhez [16]

Táblázat: Az eszköz és a Cybersecurity Framework kapcsolata, összefüggései

Cybersecurity Excellence Builder Categories and Items	Related Sections in the *Cybersecurity Framework*		
	2.4, Figure 2: Notional Information and Decision Flows	3.2, Establishing or Improving a Cybersecurity Program	Appendix A: Framework Core Categories and Functions[1]
C Organizational Context			
C.1 Organizational Description	Executive Level	Step 1: Prioritize and Scope; Step 2: Orient	ID-AM, ID-BE
C.2 Organizational Situation	Executive Level; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient	ID-BE, ID-RM
1 Leadership			
1.1 Senior and Cybersecurity Leadership	Executive Level	Step 1: Prioritize and Scope; Step 2: Orient	ID-BE, RC-CO
1.2 Governance and Societal Responsibilities	Executive Level	Step 2: Orient	ID-GV, RS-CO
2 Strategy			
2.1 Strategy Development	Business/Process Level; Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient; Step 4: Conduct a Risk Assessment; Step 5: Create a Target Profile Step 6: Determine, Analyze, and Prioritize Gaps	ID-BE, ID-GV, ID-RA, ID-RM
2.2 Strategy Implementation	Business/Process Level; Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient; Step 5, Create a Target Profile; Step 7: Implement Action Plan	ID-BE, ID-GV, ID-RA, ID-RM
3 Customers			
3.1 Voice of the Customer	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	ID-BE
3.2 Customer Engagement	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	ID-AM, PR-AT, RS-CO, RC-CO
4 Measurement, Analysis, and Knowledge Management			
4.1 Measurement, Analysis, and Improvement of Performance	Implementation Progress	Step 6: Determine, Analyze, and Prioritize Gaps	DE-AE, DE-DP, RS-IM, RC-IM
4.2 Knowledge Management	Business/Process Management; Implementation/Operations Level	Step 6: Determine, Analyze, and Prioritize Gaps	ID-RA, DE-AE, RS-CO
5 Workforce			
5.1 Workforce Environment	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	ID-AM, ID-GV, PR-IP, DE-DP, RS-CO
5.2 Workforce Engagement	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	PR-AT, PR-IP, RS-CO

6	**Operations**			
	6.1 Work Processes	Implementation/Operations Level	Step 2: Orient; Step 3: Create a Current Profile; Step 4, Conduct a Risk Assessment; Step 5, Create a Target Profile	PR-AC, PR-DS, PR-IP, PR-MA, DE-AE, DE-CM, DE-DP, RS-RP, RS-AN, RS-IM, RS-MI, RC-RP, RC-IM
	6.2 Operational Effectiveness	Implementation/Operations Level	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-AM, ID-BE, PR-AT, PR-IP
7	**Results**			
	7.1 Process Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	PR-AC, PR-DS, PR-IP, PR-MA, DE-AE, DE-CM, DE-DP, RS-RP, RS-AN, RS-IM, RS-MI, RC-RP, RC-IM
	7.2 Customer Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-BE, ID-AM, PR-AT, RS-CO, RC-CO
	7.3 Workforce Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-AM, ID-GV, PR-IP, DE-DP, RS-CO, PR-AT, PR-IP, RS-CO
	7.4 Leadership and Governance Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-BE, ID-GV, ID-RA, ID-RM, RC-CO
	7.5 Financial Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-BE

[1]The *Cybersecurity Framework* functions are Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). For an explanation of the categories within these functions, see the *Cybersecurity Framework*.

10. Forrásmunkák, linkek, referenciák:

Internetes források:

1. NIST Cybersecurity Excellence builder tool:
https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf

2. NIST Cybersecurity Framework
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

3. NIST Cybersecurity Framework (CSF) **CORE** Reference Tool

- NIST Cybersecurity Framework (CSF) Reference Tool
nist.gov/cyberframework/csf_reference_tool.cfm

The NIST CSF reference tool is a FileMaker runtime database solution. It represents the FrameworkCore which is a set of cybersecurity activities etc.

4. Published more than 40 different standards and guidelines to help protect non-national security IT systems from cyber threats.

A kiberfenyegetések elleni védelem NIST által kiadott több mint 40 szabványa és irányelve:
https://www.nist.gov/cybersecurity-1

5. NIST Special Publication (Second draft) 800-150 34 35 36 Guide to Cyber Threat Information Sharing. A kiberfenyegetésekkel kapcsolatos információk megosztása:
http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf

6. NIST - Computer Security Resource Center – Az USA Nemzeti Szabványügyi Hivatalának linkje:

http://csrc.nist.gov/

7. CYBEREYE Blog archive link:
https://gcn.com/blogs/cybereye/2016/09/nist-cyber-self-assessment.aspx?s=gcntech_300916&mkt_tok=eyJpIjoiTWpVNU9EbGpNV1ZoWTJRdyIsInQiOiJ1YnNWZVFBclg5ZXZ2NHRHYWErQjVwN1ZBYitEUzUrWmZoMUJSaGtTTWk3emZuNzlFUUlTTlIxVUhEMXRGMjJFK3lOSnJmYVhmY0pRTFNVYlZOOUNDRlpzT3ZPMFFoemZrRVI2aVM1TzdXbz0ifQ%3D%3D

8. Index.hu cikk: Az Európai Unió Hálózatbiztonsági irányelve (NIS):
http://index.hu/tech/2016/08/08/europa_kiberbiztonsag_halozatvedelem_nis_iranyelv/

9. NATO Tanulmány a magyar kiberbiztonsági helyzetről
https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf

10. Index.hu cikk: Egy kézben a magyar kibervédelem
http://index.hu/tech/2015/11/03/egy_kezben_a_magyar_kibervedelem/

11. Magyarország kibervédelmi stratégiája:
http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845

12. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323157

13. 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
http://njt.hu/cgi_bin/njt_doc.cgi?docid=165583.269327

14. Index.hu cikk: Munkacsoportok? Megvannak. Biztonság? Dolgozunk rajta
http://index.hu/tech/2016/09/29/munkacsoportok_megvannak_biztonsag_dolgozunk_rajta/

A magyarországi kormányzati kiberkoordináció helyzete, az állami és piaci szereplők együttműködésének formái.

15. Index.hu cikk: Európa felkészül a kiberháborúra;
http://index.hu/tech/2016/08/08/europa_kiberbiztonsag_halozatvedelem_nis_iranyelv/

16. A Baldridge Excellence Framework – A Baldrige Kiválósági Keretrendszer
https://www.nist.gov/baldrige/publications/baldrige-excellence-framework

17. A Baldridge Excellence Builder Tool
https://www.nist.gov/sites/default/files/documents/baldrige/publications/Baldrige_Excellence_Builder.pdf

MELLÉKLET:

Minősített adatokat (is) kezelő szervezetek és rendszerek kiberbiztonsági szempontú kockázatelemzését, fejlettségi szintjének felmérését támogató modell és módszertani segédeszköz.

Egy Excel alapú táblázatos pontozásos vegyes (kvalitatív-kvantitatív) kockázatelemzési módszertanon alapuló megoldás. A „CD RISKMAN" – CYBER DEFENCE RIKS ASSESSMENT AND MANAGEMENT TOOLSET. Egy elsősorban de nem kizárólag - minősített adatokat kezelő szervezetek és rendszerek kiberbiztonsági szempontú kockázatelemzését, fejlettségi szintjének felmérését támogató modell és módszertani segédeszköz.

1. A SZERVEZETI KIBERKOCKÁZATI PROFIL – A KOCKÁZATI KITETTSÉG MÉRTÉKE ÉS MÉRÉSE

Egy szervezetet és annak komplex kiberbiztonsági és (minősített) adatkezelési szempontú kockázati kitettségét ezzel a jellemzővel határozhatjuk meg. Ezt KIBERBIZTONSÁGI KOCKÁZATI PROFILNAK (KP), vagy röviden kiberkockázati profilnak nevezzük. Ez a kiberkockázati profil jellemző az adott szervre, szervezetre, telephelyre, adatkezelő környezetre, rendszerre, annak komplex kiberkockázati szintjére.

A modell jelenleg és jellemzően 5 kategóriából, és ezeken belül a kockázatot befolyásoló tényezőkből áll össze, melyek bármelyikének megváltozása befolyásolja (módosítja!) az adott szervezet kiberbiztonsági kockázati profilját. A szervezeti kiberkockázati kitettség mértéke egy számszerűsített jellemző, amely jellemző az adott szervezet és rendszer minősített adatkezelési szempontú kiberbiztonsági kockázat nagyságára a fenyegetettségekkel és a sebezhetőségekkel arányosan. **Ez lehet Minimális, Alacsony, Közepes, vagy Magas, illetve MAXIMÁLIS/IGEN MAGAS.**

2. KIBERBIZTONSÁGI SZEMPONTÚ SZERVEZETI-RENDSZER KOCKÁZATI SZINTEK MEGHATÁROZÁSA

2.1 Az összesített kiberbiztonsági kockázati profil szintjei

2.1.1 Minimális szintű kiberbiztonsági kockázati profil

Egy szervezet esetén ez a szint nagyon korlátozott IT/technológiahasználatot jelent. Alacsony komplexitású és igen kisszámú informatikai (IT) rendszerrel, berendezéssel rendelkeznek (1-2). Minimális a számítógépek, az alkalmazások és az eszközök száma. A kezelt minősített adatok érzékenységi szintje igen alacsony (Korlátozott Terjesztésű vagy alacsonyabb). Kevés alkalmazott (max. 1-2 fő) fér hozzá minősített adatokhoz és a kezelt minősített dokumentumok száma is minimális (<5 dokumentum/hónap) . A szervezet geográfiai „lábnyoma" és digitális lenyomata is elenyésző.

2.1.2 Alacsony szintű kiberbiztonsági kockázati profil

Ezen a szinten lévő szervezetek korlátozott komplexitású és viszonylag kisszámú IT rendszerrel, berendezéssel, minősített adatot kezelő berendezéssel, eszközzel rendelkeznek (n>2). A kezelt minősített adatok érzékenységi szintje és kritikussága viszonylag alacsony (Bizalmas vagy alacsonyabb). A kezelt minősített dokumentumok száma <15/hónap. Viszonylag kevesen férnek hozzá minősített adatokhoz (2-5 fő). A szervezet geográfiai és digitális lábnyoma alacsony mértékű.

2.1.3 Közepes szintű kiberbiztonsági kockázati profil

Ezen a szinten lévő szervezetek közepes komplexitású és közepes számú IT rendszerrel, berendezéssel, minősített adatot kezelő berendezéssel, eszközzel rendelkeznek (2>n>5). A kezelt minősített adatok érzékenységi szintje és kritikussága közepes (TITKOS vagy alacsonyabb). A kezelt minősített dokumentumok száma <25/hó. Viszonylag kevesen férnek hozzá minősített adatokhoz (5-8 fő). A szervezet geográfiai és digitális lábnyoma közepes mértékű.

2.1.4 MAGAS kiberbiztonsági kockázati profil

Ezen a szinten lévő szervezetek jelentős komplexitású és számú rendszerrel, berendezéssel, minősített adatot kezelő eszközzel/rendszerrel rendelkeznek (5>n<10 az eszközök száma). A kezelt minősített adatok érzékenységi szintje és kritikussága közepes (TITKOS vagy magasabb). A kezelt

minősített dokumentumok száma: n<50/hó. Viszonylag kevesen férnek hozzá minősített adatokhoz (n<10 fő). A szervezet geográfiai és digitális lábnyoma jelentős mértékű.

2.1.5 Maximális, IGEN MAGAS szintű kiberbiztonsági kockázati profil

Ezen a szinten lévő (nagy és/vagy kiemelt fontosságú, kritikus, létfontosságú) szervezetek nagy komplexitású és számú rendszerrel, berendezéssel, minősített adatot kezelő rendszerrel és eszközzel rendelkeznek (n>10). A kezelt minősített adatok érzékenységi szintje és kritikussága igen magas (SZIGORÚAN TITKOS). A kezelt minősített dokumentumok száma >50/hó. Viszonylag sokan férnek hozzá minősített adatokhoz (n>10 fő). A szervezet geográfiai és digitális lábnyoma nagymértékű.

3. A MÓDSZERTAN ÉS AZ ESZKÖZ – „CD-RISKMAN" átfogó ismertetése

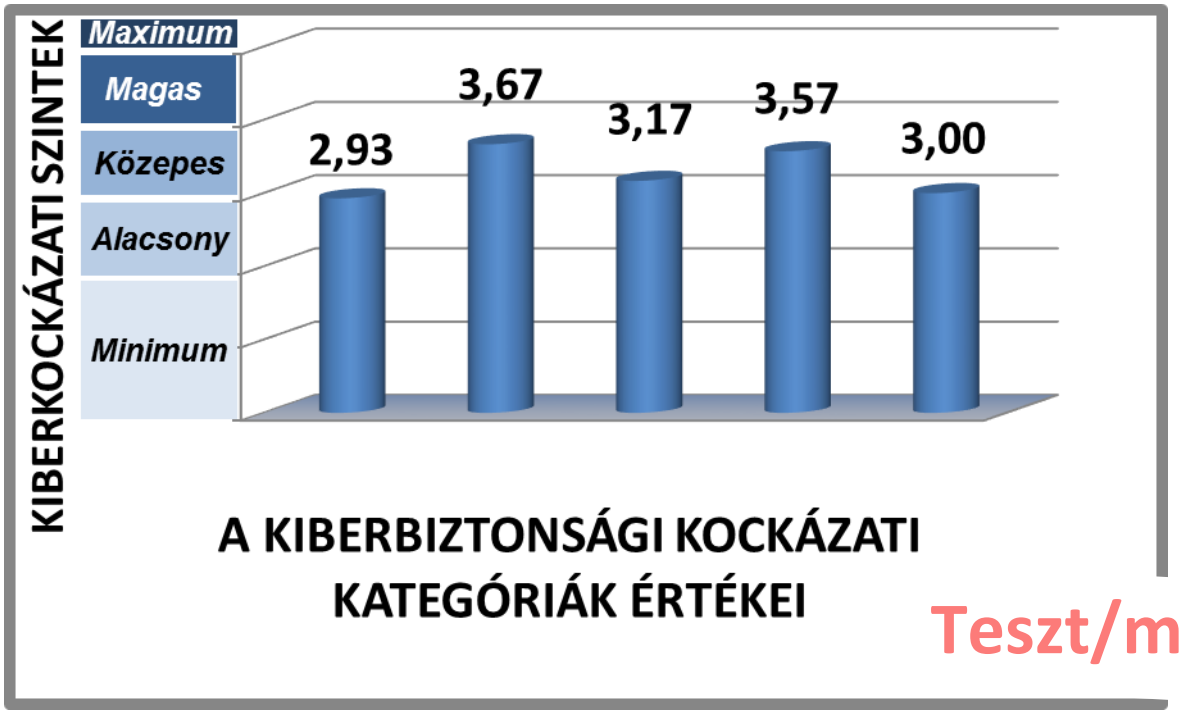
Minősített adatkezelő rendszerek és szervezetek kiberbiztonsági szempontú kockázatelemzése és fejlettségének értékelése.

3.1 A kockázati szintek és kategóriák összefoglaló ábrázolás

RENDSZERKOCKÁZAT Profil (Kategória szerint)	RENDSZER-KOCKÁZATI SZINT	Normalizált Kockázat Pontszám	Kockázat Pontszám	A tényezők száma #
1. LÉTESÍTMÉNY-, KÖRNYEZETI- ÉS RENDSZERJELLEMZŐK	*Közepes*	2,93	*41*	14
2. (MINŐSÍTETT) ADATOK ÉS ADATHORDOZÓK	*Magas*	3,67	11	3
3. (MINŐSÍTETT) ADATFELDOLGOZÓ RENDSZEREK KÖVETELMÉNYEK ÉS ELEMEK	*Közepes*	3,17	38	12
4. SZERVEZET, EMBEREK ÉS KAPCSOLATOK	*Magas*	3,57	25	9
5. FENYEGETETTSÉGEK, SEBEZHETŐSÉGEK	*MAXIMUM*	4,50	6	3
KIBERBIZTONSÁGI ÖSSZKOCKÁZATI SZINT	*KÖZEPES*	*3*	121	41

KIBERBIZTONSÁGI FEJLETTSÉGI SZINTEK		KÍVÁNT SZINTEK		
Fejlődő	MINIMUM SZINT			
Közepes	OPTIMUM SZINT			
Magas	MAXIMUM SZINT			

3.2 A kiberbiztonsági kockázati szintek és értékeik



3.3 A kiberbiztonsági kockázati kategóriák

1.LÉTESÍTMÉNY, KÖRNYEZETI ÉS RENDSZERJELLEMZŐK
2. (MINŐSÍTETT) ADATOK ÉS ADATHORDOZÓK
3. (MINŐSÍTETT) ADATFELDOLGOZÓ RENDSZEREK, KÖVETELMÉNYEK ÉS ELEMEK
4. SZERVEZET, EMBEREK ÉS KAPCSOLATOK
5. FENYEGETETTSÉGEK, SEBEZHETŐSÉGEK

4. FEJLETTSÉGI MODELL SZINTEK

A fejlettségi modell szintek az alábbiak

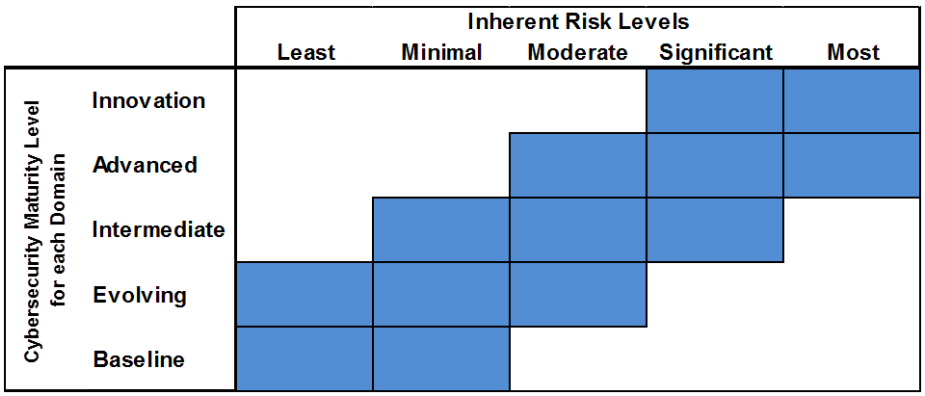
Baseline - ALAPVONAL

Evolving - Fejlődő

Intermediate - Közepes

Advanced – Magas

Innovation – Innovatív



Az ábra az FFIEC Cyberrisk Management Maturity Modellje alapján került másolásra és alkalmazásra

SAJÁT Táblázat:

4.1 A fejlettségi kategóriák és értékelési faktoraik

FEJLETTSÉGI KATEGÓRIA	Értékelési Faktorok	Kívánt Érettségi szint Kategóriánként
K1: KOCKÁZAT KEZELÉS & IRÁNYÍTÁS	1: VEZETŐI IRÁNYÍTÁS	**Evolving - Fejlődő**
	2: KOCKÁZATKEZELÉS	
	3: ERŐFORRÁSOK	
	4: Képzés & Kultúra	
K2: Fenyegetettség-Veszélyelemzés	1: Fenyegetettségelemzés	**Advanced - Magas**
	2: Veszélyelemzés	
	3: Információ szerzés és megosztás	
K3: Biztonsági kontrollok	1: Preventiv Kontrollok	**Intermediate - Közepes**
	2: Detectív Kontrollok	
	3: Korrectív Kontrollok	
K4: Külső függőség Menedzsment	1: KAPCSOLATOK	**Evolving - Fejlődő**
	2: Ralációmenedzsment	
K5: Incidens Menedzsment	1: Incidenskezelés Tervezés és Stratégia	**Evolving - Fejlődő**
	2: Detektálás, Válaszadás és Hatáscsökkentés	
	3: Eszkalálás és Jelentés	

SAJÁT TÁBLÁZAT:

4.2 A FEJLETTSÉGI KATEGÓRIÁK ELEMEI

K1: KOCKÁZATKEZELÉS & IRÁNYÍTÁS
1: VEZETŐI IRÁNYÍTÁS
2: KOCKÁZATKEZELÉS
3: ERŐFORRÁSOK
4: Képzés & Kultúra
K2: Fenyegetettség- Sebezhetőségelemzés
1: Fenyegetettségelemzés, veszélyelemzés és veszélykezelés
2: Sebezhetőségelemzés és kezelés
3: Információszerzés és megosztás
K3: Biztonsági kontrollok – kockázatkezelő intézkedések
1: Preventiv Kontrollok
2: Detectív Kontrollok
3: Korrectív Kontrollok
K4: Külső függőség menedzsment
1: KAPCSOLATOK
2: Ralációmenedzsment
K5: Incidens Menedzsment
1: Incidenskezelés Tervezés és Stratégia
2: Detektálás, Válaszadás és Hatáscsökkentés
3: Eszkalálás és Jelentés

5. A KOCKÁZATI KITETTSÉG SZINTJEI

A FENTI KATEGÓRIÁK SZERINTI JELLEMZŐKET AZ ALÁBBI 5 SZINTNEK MEGFELELŐEN KELL PONTOZNI A MEGHATÁROZOTT KRITÉRIUMOK ALAPJÁN.
A MÓDSZERTAN jelenlegi verziója 5 kockázati szintet különböztet meg, a finom felbontás érdekében ezeket pontszámokkal jellemezzük, súlyozzuk és pontozzuk.
A komplex kiberkockázati kitettséget - azaz a Szervezet és rendszereinek Kiberbiztonsági szempontú kockázati Profilját - ezek összegzésével és normalizált, súlyozott értékeinek számításával és kategorizálásával képezhetjük és jellemezzük.
A SZERVEZETRE JELLEMZŐ TELJES KIBERKOCKÁZATI PROFIL IS BESOROLHATÓ 5 KATEGÓRIÁBA AZ ÖSSZETEVŐK, A SÚLYTÉNYEZŐK (RELATÍV PREFERENCIA, FONTOSSÁGI SORREND) ÉS A HATÁRÉRTÉKEK ISMERETÉBEN, AZOK FÜGGVÉNYÉBEN.

A SZINTEK A KÖVETKEZŐK:

0 – Nem létező (Nem kitöltött az érték)
1 – Minimális kockázat (1 pont)
2 – Alacsony kockázat (2 pont)
3 – Közepes kockázat (3 pont)
4 – Magas, jelentős kockázat (4 pont)
5 – Maximális, igen magas kockázat (5 pont)

Az értékhatárok, a Kiberkockázati küszöbértékek az alábbiak.
Ezek a pontozásos értékelést követő számítás alapján a besorolás határértékei.

5.1 AZ ÉRTÉKHATÁROK

1.) **Minimális n < 1.5**
2.) **Alacsony: 1.5 < n <2.5**
3.) **Közepes: 2.5 < n < 3.5**
4.) **Szignifikáns: 3.5 ≤ n < 4.5**
5.) **Maximális n ≥ 4.5**

Ahol „n” a normalizált számított kiberkockázati érték.

6. KIBERBIZTONSÁGI KOCKÁZATKEZELÉS ÉS KOCKÁZAT-MENEDZSMENT

A vegyes kvantitatív-kvalitatív modell és módszertan alkalmazásával egy pontozásos és súlyozott normalizált kiberbiztonsági kockázati kitettség érték számításán alapuló megoldással pontos helyzetképet kaphatunk a kiberbiztonsági kockázatokról. Az Excel táblázatban kategóriánként strukturáltan szereplő és kitöltendő tényezők értékei az ún. Inherent Riskek, a technológia alkalmazásából adódó és a környezeti, szervezeti tényezők, valamint a(z) (minősített) adatok mennyisége és kezelésük módja, minősége által meghatározott és ezekből adódó komplex kiberbiztonsági kockázat meghatározásához szükséges kérdések és értékelésük, besorolásuk. (kockázati kritériumok).

A válaszok megadásával és ezek pontozásával, súlyozott értékük, valamint a küszöbértékek figyelembevételével – amelyeket statisztikai adatok és tapasztalati értékek, valamint a KIPA módszeren alapuló súlytényezők szakértői meghatározása alapján állítottunk össze – elvégezhető az EU-s és NATO-s és NEMZETI minősített adatok kezelése esetén kötelezően előírt – minősített adatok feldolgozásának kibervédelmi kockázatelemzése és értékelése. Ez lehet a kiberbiztonsági kockázatkezelés alapja.

A módszertan alkalmazásával automatizált módon – tehát a szubjektivitás és a hibalehetőségek, az emberi tényező kiküszöbölésével, illetve ezek minimálisra csökkentésével – szervezetenként összehasonlítható kiberkockázati kitettség értékek, ún „Kiberkockázati Profil”-ok (KP-k) határozhatók meg és az adott szervezet a jogszabály által meghatározott szintekbe sorolható. (3 szinten: Alacsony, Közepes vagy Magas, vagy a fenti 5 szintnek megfelelően: 1. Minimális, 2. Alacsony 3. Közepes. 4. Magas. 5. Maximális / IGEN MAGAS.

Az eszköz tartalmaz egy Fejlettségi szintet meghatározó lehetőséget is (Maturity Model) – amely az adott szervezet kibervédelmi fejlettségi szintjére jellemző. A kibervédelmi kockázati kitettség és a Fejlettségi szint között szoros összefüggés van, amely az eszköz alkalmazásával meghatározható, a kívánt mértékre beállítható – és az eredmények alapján Kiberbiztonsági kockázatkezelési akcióterv készíthető.

Ennek az eszköznek a segítségével eleget teszünk a nemzetközi követelményeknek és a kiberkockázati szempontú biztonsági szinteket átláthatóvá, kimutathatóvá, a kiberbiztonsági kockázatokat számszerűsíthetővé és összemérhetővé, kezelhetővé tesszük.

Nézetünk és törekvésünk szerint ez egy jelentős előrelépést jelenthet a hazai információ- és kiberbiztonsági szakmai színvonal emelése és a kockázati szempontú szemléletmód elterjesztése, fejlesztése terén is.

Horváth Dávid

A kiberbiztonság kihívásai Európában és Magyarországon
Dark Net: az érem két oldala

Tartalomjegyzék

1. Bevezető

Dolgozatom témája a Dark Net, melyre egységes definíció a szerző ismeretei szerint jelenleg nem áll rendelkezésre. Hogy megértsük, fontos ismerni, de legalábbis elképzelni az Internetet, ami nem más, mint olyat hálózatok hálózata, amely emberek milliárdjai által elérhető egy közös szabvány által (Internet Protocol – IP). A gyakorlatban ez úgy néz ki, hogy egy adott Internet szolgáltató (Internet Service Provider – ISP, pl. Telekom, Digi, UPC stb..) elérést biztosít a hálózathoz a felhasználónak, amit leggyakrabban egy böngészőn keresztül ér el (80-as illetve 443-as portokat használva). Modern felhasználók többsége fejből ismer egy-két weboldalt, pontosabban azoknak az URL-ét (Uniform Resource Locator), de ahhoz, hogy teljes egészében böngéssze valaki az Internetet, szükséges egy keresőmotor (search engine) használata (pl. Google), amely segíthet megérteni a Dark Net-et. Itt szükséges bevezetni a kliens-szerver modellt, mely két csoportra bontja az Internet felhasználókat. Szemléltetés végett egy rövid példával fogom bemutatni:

Egy „x” hírportál üzemeltetője szerverként funkcionál, míg a weboldalról letöltött híreket elolvasó „y” egyén pedig a kliens. A keresőmotor nem csinál mást, mint a nyilvános IP tartományon végig menve megkeresi a tartalommal rendelkező weboldalakat, majd azokat indexeli a saját adatbázisában, amit felhasználva bárki képes böngészni az Interneten. A fenti példánál maradva, az „x” hírportálnak érdeke, hogy elérhető legyen a külvilág számára, ám vannak olyan szerverek, amelyek különböző technikákkal (melyeket majd részletesen kifejtek) szándékosan rejtve maradnak, és csak nem hagyományos módszerekkel érhetőek el.

1.1 Dark Net fogalma

Ezeknek a tartományoknak az összefoglaló neve a Dark Net. A terület annyira megfoghatatlan és tudományos téren kevéssé feldolgozott, hogy magával a fogalommal kapcsolatban is viták folynak. Sokan úgy vélik, hogy a fent kifejtett terület helyes elnevezése a Deep Web, és ezen belül annak illegális tevékenységet folytató része a Dark Net, vagy sok helyütt egybeírva Darknet, esetleg Dark Web.[i] A dolgozatkiírásnak megfelelően munkám során a Dark Net kifejezést fogom használni.

1.2. Dark Net elérése

A fenti bevezetőből kitűnik, hogy a Dark Net legfontosabb kritériuma, hogy hagyományos úton nem érthető el (pl. keresőszoftverrel). Továbbiakban bemutatok két eljárást, amivel elérhetőek az ilyen hálózatok.

1.2.1. Elérés Tor-on keresztül

Az utóbbi évek buzzword-jévé vált a Tor (The Onion Ring), különösen Snowden 2013-as kiszivárogtatásai után. A Tor-t legtöbben anonim böngészés céljából használják, de ami a téma szempontjából ennél is fontosabb, az ún. hidden service-ek üzemeltetésére.

A Tor működési elve az onion routing-on alapul, melynek lényege, hogy a csomagok relay-eken keresztül több rétegnyi titkosítással (mint a hagyma rétegei) mennek keresztül az Interneten, és mindegyik relay csak egy rétegnyi titkosítást tud visszafejteni, úgyhogy nem tudja kitől jött a csomag, csak hogy merre kell továbbítani. Ezáltal a felhasználó anonim módon böngészheti az Internetet.

Két módszer van a Tor-on keresztül böngészésnek. Egyrészt elérhető a Tor saját böngészője (Tor browser – a Firefox-nak egy módosított változata) minden operációs rendszerre. Kifinomultabb felhasználók maradhatnak a megszokott böngészőjüknél (pl. Chrome), csak futtatni kell a tor-t, mint programot (pl. Linuxon „*service tor start*” paranccsal), a böngészőnél pedig be kell állítani, hogy a 9050-es portot használja proxy-ként.

Visszatérve a hidden service-ekhez, a korábban említett szerver-kliens modellnél maradva, valaki dönthet úgy, hogy az általa üzemeltett szolgáltatás csak a Tor-on keresztül legyen elérhető. Ilyen esetben a felhasználó az alkalmazást telepítve rövid konfigurálás és minimális üzemeltetési ismeretekkel könnyedén beállíthat egy hidden service-t (két sor beírása a Tor konfigurációs fájljában). Ekkor a rendszer generál számára egy URL-t, melynek első tagja számok és az angol ABC betűiből álló random sorozat, míg a vége minden esetben -*.onion (pl. http://32rfckwuorlf4dlv.onion).

Innentől kezdve az adott szolgáltatás csak a Tor-on keresztül érhető el, ami biztosítja, hogy ne lehessen megállapítani honnan, és milyen IP címről üzemeltetik. Minden más szempontból ugyanolyan, mint bármilyen más szerver szolgáltatás, üzemeltethető az ismertebb rendszerekkel (pl. Apache2), csak fontos, hogy a Tor 9050-es portját fogja használni a szolgáltatás. Mivel egyedi *.onion URL-eket használ a rendszer, a keresőmotorok nem index-elik őket, a felhasználóknak ismerni kell a pontos URL-eket, hogy elérjenek szolgáltatásokat.

Itt jegyezném még, hogy vannak elérhető listák az *.onion címtartományról is, a szerző ismeretei szerint a legteljesebb a Pastebin oldalon közzétéve. [ii] Nagy különbség pl. egy

Google keresőmotorral szemben, hogy míg előbbinek az algoritmusa heti rendszerességgel az IP tartományt végigböngészi, addig a Pastebin-en közzétett és hasonló listák manuálisan vannak szerkesztve, semmiféleképpen sem teljesek vagy átfogóak, továbbá nem frissített (megfigyelhető, hogy sok link már nem él, vagy eleve nem is volt élő).

1.2.2. Elérés I2P-n keresztül

Az I2P (Invisible Internet Project) egy a Tor-hoz hasonló platform, amivel elérhető a Dark Net. Néhány különbség az I2P szempontjából a Tor-hoz képest:

- Kisebb hálózat, kevesebb felhasználó, kevésbé ismert és dokumentált
- Java-ban van megírva, ami kevésbé gépközeli, mint a C-ben megírt Tor
- Jobban van optimalizálva a hidden service-ekre, gyorsabban elérhetőek
- Teljesen megosztott a hálózat, semmilyen központi irányítása nincsen

Utolsó lényeges különbség pedig, hogy valós idejű rangsorolás van a peer-ek között, aszerint, hogy milyen valós adatátviteli kapcsolattal rendelkeznek. Tor relay esetén a felhasználó a konfigurációs fájlban megad egy adott sávszélességet (pl. 10 Mb/s), amit enged a rendszernek felhasználni, és ez automatikusan valid-nak van elfogadva, függetlenül attól, hogy ez a gyakorlatban megvalósul-e vagy sem.

2. Példák

2.1. Negatív példák

Mivel a Dark Net nehezen elérhető és lekövethető, sokan használják illegális tevékenységre (innen a Dark elnevezés, illetve a rosszhíre a kifejezésnek). A teljesség igénye nélkül az alábbi szolgáltatások érhetőek el különböző weboldalakon:

- Fegyverkereskedelem
- Kábítószer kereskedelem
- Lopott bankkártyák, hitelkártyák értékesítése
- Pénzmosás
- Bérgyilkos szolgáltatások
- Illegális szerencsejáték
- Hamis igazolványok, útlevelek készítése
- Hacker szolgáltatások bérbeadása
- Illegális pornográfia
- Szélsőséges gondolatok terjesztése
- Könyvek, folyóiratok illegális terjesztése

- Szervkereskedelem

A listában szándékosan említek kifejezetten ijesztő példákat (pl. bérgyilkos szolgáltatások), és morális szürke zónába tartozó példákat is (pl. könyvek, folyóiratok terjesztése).

2.2. Pozitív példák

Itthon, és a nyugati országokban természetesnek veszik az állampolgárok a szólásszabadság intézményét, de kevésbé demokratikus országokban (pl. Kínai Népköztársaság) mai napig erős cenzúra működik többek között az Interneten is (pl. a kínai cenzúrát „viccesen" csak *Chinese Great Firewall*-ként említik). Napjainkban is vitatott Julian Assange tevékenysége, mindenesetre az általa alapított WikiLeaks jelenleg üzemel hagyományosan elérhető URL-n (https://wikileaks.org), illetve vélhetőleg biztonsági okokból üzemeltet egy *.onion weblapot is (http://jwgkxry7xjeaeg5d.onion). Ezen kívül több ismert folyóirat is üzemeltet hidden service-t (Wired, New Yorker, Sun, Guardian, Washington Post), ahol whistleblower-ek, újságírók, állampolgárok szivárogtathatnak információkat (pl. a New Yorker által üzemeltett Project Strongbox, http://strngbxhwyuu37a3.onion).

Egy másik történet 2011-ben, az Arab Tavasz kezdetén bontakozott ki. Az egyiptomi tüntetések idején Mubarak elnök erős cenzúrát üzemeltett és rengeteg weboldalt elérhetetlenné tett országában (pl. a Twitter-t). Ezt megkerülve sok tüntető telepítette a Tor-t, mely egyrészt biztosította a felhasználó anonimitását, másrészről elérhetővé váltak az eddig elérhetetlen weboldalak.[iii]

Érdekességként egy harmadik példa: a népszerű social media, a Facebook is üzemeltet hidden service-t (https://facebookcorewwwi.onion/). Amennyiben valaki Tor böngészővel lépett be Facebook-ba, sokszor kapott figyelmeztetéseket, hogy felhasználófiókját esetleg feltörték, hiszen a Tor automatikusan 10 percenként változtatja az általa használt kilépőpontot. A gyakorlatban ez azt jelenti, hogy a Facebook rendszere észlel egy belépést pl. Norvégiából, fél órával később az USA-ból, egy óra múlva pedig Ausztráliából. Ilyenkor a log rendszere flag-gel jelzi a gyanús tevékenységet, ami rontja a felhasználói élményt. A *.onion oldalát látogatva ellenben megszűnik ez a kellemetlenség, továbbá a felhasználó anonim marad (legalábbis ami a kapcsolódást illeti, ellenben a Facebook az általa gyűjtött egyéb meta adatok és a böngészési stílus alapján nem kizárt, hogy továbbra is tudja deanonimizálni a felhasználót). Mindenképpen pozitív példával jár elől a Facebook, remélhetőleg más oldalak is követik, hogy teljes anonimitást biztosítsanak felhasználóinak.

2.3. Hidden service-ek megoszlása

Az előbbiekben bemutattam pozitív és negatív példákat is, most igyekszem konkrét adatokkal felmérni a hidden service-ek megoszlását. Pályamunkám megírása előtt nem sokkal jelent meg egy átfogó tanulmány, Daniel Moore és Thomas Rid közös munkája, *„Cryptopolitik and the Darknet”* címmel.[iv] A szerzők egy alapos vizsgálatot folytattak az elérhető *.onion weboldalakat, illetve az abból nyíló további weboldalakat felhasználva, hogy pontosan milyen arányban oszlanak meg a tartalmak. Felhívnám a figyelmet a cikk részletes tanulmányozására, mivel jelen műben csak a végeredményt mutatom be:

- Összesen üzemelő hidden service-ek száma: 5205
- Tartalommal rendelkező hidden service-ek száma: 2723
- Beazonosíthatatlan tartalommal rendelkező hidden service-ek száma: 155
- Legális tartalommal rendelkező hidden service-ek száma: 1021
- Illegális tartalommal rendelkező hidden service-ek száma: 1547

Fenti összesítés sajnos elég sötét képet fest: még optimistán feltételezve a beazonosíthatatlan oldalakról a legális tartalmat, akkor is messze nagyobb az illegális oldalak száma. Még valósabb lehetne kapni, ha elérhetőek lennének adatok az egyes szolgáltatások időben eloszló felhasználóinak számáról, de technikailag ez kivitelezhetetlen. Fontos kiemelnem, ahogy már korábban is említettem, nem lehetséges az összes hidden service-t áttekinteni, a szerzők is két nyilvánosan elérhető listát vettek alapul (továbbá az arról nyíló további oldalakat).

3. Gyakorlati megvalósulása a Dark Net-nek

3.1. Anonim fizetés

A negatív példáknál feltűnhet az olvasónak, hogy sok szolgáltatást biztosítanak, ahol felmerül az ellenszolgáltatás módja. Nyilván hagyományos bankszámlára utalva könnyen lekövethetővé válik bármilyen tranzakció és megszűnik a Tor nyújtotta anonimitás, a készpénz esetén pedig a személyes találkozó ténye miatt veszne el a felhasználók anonimitása. Ennek elkerülése végett használnak különböző cryptocurrency-ket (pl. Bitcoin, Litecoin, Faircoin, stb..). A rendszer lényege, hogy minden felhasználónak van egy anonim tárcája (wallet) ami teljesen egyedi, és amelynek segítségével tud utalni vagy fogadni másoktól utalásokat egy titkosított rendszeren keresztül. Kívülről annyi látszik, hogy két véletlenszerű azonosítóval rendelkező egyén között adott összegű tranzakció zajlott le. Bár

több szolgáltatás is épül az adott rendszerre, az első és mai napig legnépszerűbb a Bitcoin, így a továbbiakban ezt fogom említeni.

A rendszernek köszönhetően az üzemeltetőnek nincs más dolga, mint megadni a nyilvános azonosítóját és egy Bitcoin-ban megadott összeget, amit a szolgáltatásaiért cserébe vár, majd a Bitcoin-okat beváltva hagyományos valutába, anonim módon juthat hozzá pénzéhez. Ha figyeli is valaki a felhasználóhoz tartozó pénzmozgást, csak azt tudja megállapítani, hány alkalommal és mekkora összeget fizettek ki, de az kinyomozhatatlan, hogy ki(k)hez tartozik a tárca.

3.2. Anonim levelezés

Előfordulhat, hogy az anonim fizetés mellett felmerül az igény levelezésre is a Dark Net felhasználóinak. Ilyenkor két elterjedt lehetőség áll rendelkezésre

3.2.1. Eldobható e-mail címek

Az eldobható e-mailek rendszere arra épül, hogy a weblap megnyitásakor a felhasználónak generálódik egy e-mail cím (általában random karakterekből), amelyet egy bizonyos ideig (általában 1 óra) használhat, utána megszűnik. A fiók alkalmas e-mailek küldésére és fogadására, mint bármilyen más szolgáltatónál, viszont nem követel meg semmilyen regisztrációt vagy azonosítást, Tor hálózatról is elérhető. Legismertebb a GuerillaMail (http://www.guerillamail.com).

Érdekességként a Gmail szolgáltatás elérhető Tor-ról, ám ha új felhasználót akar valaki regisztrálni, és a Gmail észleli, hogy egy Tor kilépő pontról érkezett a kapcsolat, akkor megkövetel egy telefonszámot, aminek hitelességét egy SMS-ben érkező kód megadásával kell igazolni.

Fentihez hasonló rendszerek kijátszására (hasonlóan az eldobható e-mailekhez), egyes szolgáltatók üzemeltetnek nyilvános telefonszámokat SMS-ek fogadására, különböző országokban. A felhasználó regisztrációkor megad egy ilyen nyilvános telefonszámot, majd a szolgáltatás honlapján leolvassa az érkezett SMS-ben található kódot. A fenti Gmail esetében ez a rendszer nem működik, mivel a Google figyeli, ha több regisztrációkor használják ugyanazt a telefonszámot, viszont más szolgáltatóknak nincs mindig ilyen kifinomult védelmi rendszerük.

3.2.2. Titkosított levelezés

Az online levelezés (e-mail) 3 portot használ, a POP3 (port 110), az IMAP (port 143), és az SMTP (port 25) portokat. Az e-mailezés részletei nélkül annyit érdemes tudni, hogy mindhárom port alapjáraton titkosítatlan. Egyes szolgáltatók használják az SSL/TLS (Secure Sockets Layer/Transport Layer Security) technológiát (POP3S – port 995, IMAPS – port 993

és STMPS – port 465), amelynek segítségével a felhasználó és az e-mail kiszolgáló (pl. Gmail) között a kapcsolat titkosított lesz. Ez hasznos lehet, ha pl. a későbbiekben említett exit relay üzemeltetésével, vagy épp egy man-in-the-middle támadással akarja valaki a felhasználó e-mailjeit elolvasni, de fontos tudni, hogy az e-mail szolgáltatók között a világhálón titkosítatlanul megy át az üzenet. Köznapibb nyelven ez annyit tesz, hogy az e-mail szolgáltató belelát a felhasználó levelezéseibe. Kevesen tudják, de a Google 2014 óta nem titkolja, hogy beleolvas a felhasználó e-mailjeibe:

„Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."[v]

Ennek megoldására találta ki Philip R. Zimmermann 1991-ben a PGP-t (Pretty Good Privacy), egy számítógépes programot, amely alkalmas a titkosításra és a hitelesítésre. A rendszert és variánsait (OpenPGP, GPG) a mai napig használják, mivel a titkosításhoz használt kriptográfiai eljárás (RSA) a mai napig biztonságos és megbízható (megfelelő kulcsmérettel). A legnépszerűbb e-mail szolgáltatónál, a Gmail-nél, egy plugin segítségével (*Mymail-Crypt for Gmail*) érhető el a rendszer, míg Linuxon pl. gyárilag telepített a GNU Privacy Guard (GPG). Fontos, hogy a rendszer Nyilvános Kulcsú Infrastruktúrán (PKI) alapul, tehát minden felhasználó rendelkezik egy nyilvános-privát kulcspárral, és amennyiben valaki ismeri egy személy nyilvános kulcsát, úgy lehetősége van számára titkosított üzenet küldésére. A PGP rendszer mai napig biztonságosként van számon tartva, nincs ismert matematikai módszer, amellyel támadható volna, 1024 bites verzióját napjainkig nem sikerült még brute froce segítségével feltörni (bár egyes szakértők szerint éveken belül ez megtörténhet), míg 2048 bites verzióját még a pesszimistább kriptográfusok sem jósolják belátható időn belül.[vi]

Történet „érdekessége", hogy Zimmermann bíróság elé került, mivel a kriptográfiai eljárását a törvényszék „munition"-ként kezelte, így a vád hadianyag illegális exportja volt vele szemben. A pert végül ejtették és Zimmermannt felmentették, ezzel egy lépéssel közelebb kerültek az emberek a mindennapokban használható privacy-hez.

Napjainkban a legnépszerűbb platform a titkosított e-mail-ezéshez a Protonmail. Újítása abban rejlik, hogy automatikusan implementálja a PGP rendszerét, és amennyiben mind az üzenet küldője és fogadója is Protonmail-t használ, a levél automatikusan titkosítva megy át. Nagy előnye, hogy a felhasználójának nem kell ismernie a saját kulcsát, a titkosítási eljárást,

vagy akár a PGP-t magát se, egyszerűen használható, mint bármelyik másik nem titkosított levelező szolgáltatás.

4. Kihívások leküzdése

4.1. Dark Net felszámolása

A Dark Net esetleges felszámolása több okból is problémákhoz vezethet. Ahogy korábban is említettem, morális okokból is kérdéses, hiszen nem feltétlenül „rossz" a rendszer, csupán vannak, akik visszaélnek vele.

Az erkölcsi részétől eltekintve, gyakorlati problémák is felmerülnek. A hidden service-ek megszüntetéséhez a Tor-t magát is meg kellene szüntetni, ami körülményes, tekintve, hogy egy szabványról, egy protokollról beszélünk, és nem fizikai gépekről. A gyakorlatban ez úgy néz ki, hogy véges számú Tor relay-ek üzemelnek, amik közvetítik a titkosított kapcsolatot keresztül a világon, és ezáltal válik lekövethetetlenné a felhasználó. Ezeknek egy speciális fajtája az exit relay vagy exit node, a kilépési pont, amelyen keresztül a felhasználó eléri a látogatni kívánt weboldalt. Az exit relay-ek nyilvánosak, hiszen ez az utolsó stádiuma a kapcsolódásnak, ezek jellemzően önkéntesek gépén futó szolgáltatások, melyekről lehet tudni, hogy csak kilépési pontként szolgálnak (olyannyira, hogy a Google pl. detektálja, hogy a felhasználó Tor-on keresztül böngészik). Ezek a kilépő pontok könnyen beazonosíthatóak IP cím és szolgáltató által, viszont üzemeltetésük beszüntetése két szempontból is indifferens lenne.

Egyrészről egyből feltűnnének helyettük mások, akik saját gépükön folytatják a kilépőpont üzemeltetését. Egy Tor exit relay bekonfigurálása nem bonyolultabb a korábban már említett hidden service-nél, egy 1Mb/s-os Internet eléréssel stabil kilépőpontot lehet üzemeltetni. Érdemes megjegyezni, hogy napjainkban 1 Gb/s-os Internet előfizetési csomagokat kínálnak lakossági ügyfeleknek, a havi magyar átlagkereset ~5%-áért, vagyis elérhető áron.

Másrészről, aki érti a rendszer felépítését, az tudja, hogy a kilépési pont üzemeltetőjén keresztül se az esetleges illegális tevékenységet folytató egyént, se az azt igénybe vevő egyént nem lehetne elérni, tehát a valódi probléma megoldásához nem vezetne közelebb. Érdekességként az éppen aktuálisan üzemelő Tor kilépő pontok listája elérhető az alábbi weboldalon: https://torstatus.blutmagie.de/

4.2. Csapda állítása

A Dark Net felszámolása mellett alternatíva lehet az ott nyújtott illegális szolgáltatások igénybe vevőit csapdába csalni és beazonosítani.

Tételezzük fel, hogy az egyszeri „A” felhasználó kábítószert szeretne vásárolni online, és azt hallotta, hogy a Tor-on keresztül anonim módon tud böngészni. Ha egy jóindulatú „B” felhasználó szeretné beazonosítani „A” felhasználót, létrehozhat „csaliként” egy nem titkosított (80-as port-on futó) hagyományos HTTP weboldalt, mely illegális szolgáltatásokat hirdet magáról. Emellett „B” üzemeltet nagyobb mennyiségű kilépőpontot (mely se sávszélesség, se fizikai erőforrás szempontjából nem igényel különösebb eszközöket). Így van rá esélye, hogy az ő kilépő pontján keresztül csatlakozik „A” a weboldalra, és mivel nem titkosított a kapcsolata, az átmenő csomagokat könnyedén tudja szűrni és megvizsgálni (minél több kilépő pontot üzemeltet, annál nagyobb rá az esélye). Ebben az esetben „A” abban a hitben, hogy anonim a kapcsolata, megad személyes adatokat, elérhetőséget a weblapon (pl. telefonszám, postai cím, e-mail cím), mivel „B” úgy készítette el a weboldalát, hogy ezek megadása szükséges legyen. A csomagszűrést a tcpdump nevű programmal könnyedén végre lehet hajtani (Linuxon előre telepített), erre épül egyébként a népszerű és felhasználóbarát grafikus felülettel rendelkező Wireshark is (Windows-os felhasználók számára).

Amennyiben „B” sikeren „csapdába ejt” egy „A” felhasználót, az már elvezetheti egy hidden service-t üzemeltető egyénhez.

4.3. Csapda állítása 2.0

Az Interneten jelenleg is elérhető több olyan szoftver, amellyel a hidden service-ek elérhetőek a Tor böngésző használata nélkül. Példaként a Tor2web (https://tor2web.org/) használatához a *.onion site végére egy *.to domain nevet kell írni (pl. https://duskgytldkxiuqc6.onion.to/), és innentől kezdve a hagyományos böngészőn is elérhető a *.onion site.

Mivel nem Tor böngészővel irányul a felhasználó kérése a szolgáltatóhoz, ezért annak publikus IP címe ismert a szolgáltatónál. Az IP cím ezután egy adatbázisban összepárosítható a lekért *.onion site-tal. Innen már csak egy lépés, hogy a szolgáltató összeszedje a legnépszerűbb, illegális tevékenységet folytató Dark Net oldalak *.onion oldalát (Pl. a Silk Road-ét), és kiszűrje a rosszindulatú felhasználókat. Természetesen egy illegális szolgáltatást hirdető weboldal látogatása még önmagában nem illegális, de kiindulási pont lehet egy a potenciálisan illegális szolgáltatást használó egyének listája.

4.4. Deanonimizálás

Következő elképzelés egy kissé komplexebb eljárás, de elvben jó eséllyel jelenthet megoldást a kihívásokra. Adott a Dark Net, ahol a legnagyobb védelmet az anonimitás nyújtja. Ha az anonimitást nyújtó rendszert (Tor) nem is lehet megszüntetni, de az egyén anonimitását kompromittálva, egyénenként megszüntethető a fennálló helyzet.

Adott egy „A" egyén, aki valamilyen oknál fogva egy hidden service útján kezd el lopott bankkártyákat árulni egy *.onion-os weblapon keresztül, legyen ez „B". A probléma, hogy senki más nem tudja, hogy a „B" oldalt az „A" egyén üzemelteti, csak „A". A cél „A" azonosítása, anélkül, hogy bármi módon kompromittálódna a rendszer (Tor), amely összekapcsolja „A"-t a „B" weblaphoz. A deanonimizálási folyamatot a példánál maradva mutatom be.

Legyen „A"-nak egy nyilvános Facebook profilja is, „C", amely teljesen legitim és egyértelműen „A"-hoz köthető. Ha valamilyen módon sikerülne összefüggést felállítani „B" weboldal és „C" profil között, az egyértelműen igazolná, hogy „A" egyén áll a „B" weboldal mögött is. Ilyen összefüggés akkor állítható fel, ha feltételezzük, hogy mindannyiunk Internetes jelenléte olyan szinten egyéni, akár az aláírásunk.

A gyakorlatban ez úgy nézne ki, hogy egy megfelelő algoritmus végigmegy egy rendkívül nagyszámú bemeneti anyag (pl. az összes nyilvános Facebook profil) és az összes (elérhető) illegális weboldal között, és ahol összefüggést talál, azt visszadobja gyanús elemként.

Az elgondolást azért tartom megvalósíthatónak, mivel 2008-ban a University of Texas két kollégája publikált egy cikket „*Robust De-anonymization of Large Sparse Datasets*" címmel.[vii] Munkájuk során megvizsgáltak egy, a Netflix által kiadott, 500.000 felhasználójuk névtelen film értékelését tartalmazó adatbázisát. Ezt összevetették az Internet Movie Database (Imdb) adataival és sikerült beazonosítaniuk névtelen felhasználókat.

Véleményem szerint a fenti cikk csak a kezdet a témában. A problémának ketten álltak neki, különösebben kiemelkedő eszközök nélkül, ráadásul lassan tíz évvel ezelőtt. Ha pl. adott lenne egy kormányzati szerv, ahol korszerű software-ekkel és szuperszámítógépekkel felszerelt csapat tevékenykedne, jó eséllyel lehetne anonim személyeket beazonosítani.

4.4.1. DNS Leak

Amikor az Internetet böngészi a felhasználó, weboldalakat látogat meg, de ahhoz, hogy kapcsolódni tudjon a kiszolgálóhoz, ismernie kell a site-hoz tartozó URL-t (pl. www.google.com). A böngésző kapcsolódik egy Domain Name System-re (DNS), amely a kérésre visszaadja az URL-hez tartozó IP címet (pl. a Google esetén ez 216.58.217.110). Ez a

felhasználók számára észrevétlenül, általában az Internet szolgáltató saját DNS-ére kapcsolódva zajlik le. Ha a felhasználó a Tor saját böngészőjét használja, akkor automatikusan véletlenszerű DNS-ekhez kapcsolódik, ami megőrzi a felhasználó anonimitását. Ellenben, ha a felhasználó saját böngészőt használ Tor-hoz való kapcsolódáshoz, és nem megfelelően konfigurálta be a böngésző DNS beállításait, akkor a saját internetszolgáltatója DNS-éhez fog továbbra is kapcsolódni, innentől kezdve a felhasználó beazonosítható lesz.

4.4.2. Command Injection Vulnerability

Az előbbi eljárás a felhasználó módszereiben talált hibát használja ki, a következő pedig egy szerver oldali sérülékenységen alapul. Egy nem megfelelően konfigurált weblap alkalmazásnál el lehet érni, hogy bizonyos utasításokat hajtson végre. Az *Open Web Application Security Project* (OWASP) az alábbi példával szemlélteti a sérülékenységet:

http://sensitive/something.php?dir=%3Bcat%20/etc/shadow

A fenti példán látszik, hogy a rosszindulatú támadó egy lekérést hajtott végre, ami kiírja az */etc/shadow* tartalmát, ami a Linux jelszavak hash-ét tartalmazza. Ez már önmagában hasznos lehet egy hidden service deanonimizálásához, de a sérülékenységet kihasználva más parancsok is lefuttathatók. Egy egyszerű ping paranccsal bármilyen IP címre küldhető a szerverről egy csomag (megkerülve a Tor-t), pl. egy olyan címre, ahol tcpdump segítségével van figyelve a csomagforgalom. [viii]

4.5. A Silk Road története

Ahogy korábban bemutattam, rengeteg illegális tevékenység zajlik a Dark Net-en, és ahogy említettem, a Tor, mint rendszer nem szüntethető meg. Ellenben a Silk Road története talán alapot adhat jövőbeli tevékenységekhez az illegális szolgáltatások leküzdéséhez.

A Silk Road jól összegzi eddigi munkámat: Tor hidden service-t (*.onion weblapot) használva illegális szolgáltatásokat (főként kábítószer kereskedelmet) bonyolítottak le, cryptocurrency (Bitcoin) fizetőeszközzel. A Silk Road világszerte ismertté vált, de mégis lenyomozhatatlan maradt. Végleges megszüntetéséhez hagyományos módszereket kellett igénybe venni.

Az FBI azzal kezdte a nyomozást, hogy megkereste a legelső (nem Tor-on megosztott) bejegyzést, ami említi a Silk Road-ot:

„I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it.

I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at http://tydgccykixpbu6uz.onion.

Let me know what you think...”

Miután a poszt szerzőjének tevékenységét megfigyelték, kiderült, hogy az illető keresett egy Bitcoin technológiában jártas szakembert, és elérhetőségnek egy e-mail címet adott meg, mint később kiderült, a Silk Road tulajdonosának e-mail címét…

Az e-mail címhez tartozott egy Google+ fiók, amihez név és egyéb személyes adatok is tartoztak. Innentől a nyomozás részletei kissé homályosak, valószínűleg az FBI-nak nem érdeke minden részletet nyilvánosságra hozni, de a konklúzió egyértelmű: az emberi faktor szerepe. Bármennyire is tökéletes egy adott technológia (Tor), az emberi tényező mindig közrejátszik.

Érdemes megfigyelni a történet negatív oldalát is, egy hónappal a Silk Road bezárása után elindult a Silk Road 2.0, változatlan rendszer mellett, ugyanazokkal az üzemeltetőkkel, csak más vezető irányítása alatt. Egy év alatt azt is megszüntették, ellenben a Silk Road 3.0 a mai napig üzemel. A minta egyértelmű, ahogy azt már korábban a Tor exit relay-ek esetén is kifejtettem.

Jelenleg ami szükséges egy ilyen szolgáltatás üzemeltetéséhez egy rossz szándékú egyénnek, azt már mind kifejtettem írásomban:

- Minimális hardware igények a hidden service-hez
- Minimális sávszélesség igények a hidden service-hez
- A fenti követelmények megléte 24/7-ben
- Egy Bitcoin tárca (wallet), amely létrehozása 5 perces feladat
- … Maga az illegális tevékenység, ami felköltözne a Tor hálózatára

Amíg ezek a körülmények adottak, jó eséllyel nem szüntethetőek meg az illegális tevékenységek a Silk Road adott verziójának beszüntetésével, legfeljebb egy zuhanás érhető el a Bitcoin árfolyamában… (lásd 2013 október 2.)

5. Konklúzió

A szerzőnek nem feladata eldönteni, hogy a Dark Net létezése jogos továbbá etikus-e, ahogy azt sem, mi számít használatának, és mi visszaélésnek. Tény, hogy napról napra többen ismerik meg, használják, válik megbízhatóbbá, stabilabbá és elterjedtebbé a rendszer. Fentiekben igyekeztem bemutatni, hogy rengetegféleképpen lehet használni, visszaélni vele, továbbá azt is, hogy nem tökéletes és nem is teljesen lenyomozhatatlan.

A vita egyébként a Dark Net előtti időkre vezethető vissza. Kezdetben kormányok és szabadságjogi aktivisták között zajlott, a mérleg egyik oldalán a biztonság, a másik oldalán pedig a szabadság állt, mindkettő egyformán fontos része emberi életünknek. Napjainkban azonban az egyének szintjére is eljutott a debate, és elmondható, hogy az emberek megosztottak. Legelső nagyobb, nyilvánosság elé került ilyen esemény a Watergate ügy volt a 70-es években, majd Philip Zimmermann PGP-jével kapcsolatos court case kapcsán jött elő a kérdéskör, igaz, kevesebb nemzetközi visszhanggal. 2013-ban Snowden-nek hála megint napirendre került a téma, legutóbb pedig 2016 februárjában az *FBI-Apple Encryption Dispute* kapcsán vált ismét felkapottá. Ha valaki tehát meg akarja érteni a Dark Net körüli dilemmát, érdemes tanulmányozni a *Crypto Wars* néven elterjedt jelenséget, és annak történetét.

Véleményem szerint, bárki akar foglalkozni a Dark Net körül felmerülő biztonsági kihívásokkal, először magával a hálózatok működésének alapjaival, az Internet, a hálózatbiztonság és a sérülékenységek témakörében kell elmélyülnie, hogy reálisan felmérje az aktuálisan fennálló helyzetet. Ezek után van csak lehetőség az általam bemutatott gyakorlatban alkalmazható eljárások segítségével eredményeket elérni a témában.

6. Irodalomjegyzék

i. Daniel MIESSLER: The Internet, the Deep Web, and the Dark Web, 2016. Forrás: https://danielmiessler.com/study/internet-deep-dark-web/ (2016.08.25.)

ii. Over 5000 onion link 2016, Forrás: http://pastebin.com/hWyD5ZKP (2016.08.25.)

iii. Ingmar ZAHORSKY: Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum, 2011. Forrás: http://www.monitor.upeace.org/innerpg.cfm?id_article=816 (2016.08.25.)

iv. Daniel MOORE, Thomas RID: Cryptopolitik and the Darknet, Survival, 58:1, 7-38.

v. Google Terms of Service, Forrás: https://www.google.com/intl/en/policies/terms/ (2016.08.25.)

vi. Jeremy KIRK: Researcher: RSA 1024-bit Encryption not Enough, 2007. Forrás: http://www.pcworld.com/article/132184/article.html (2016.08.25.)

vii. Arvind NARAYANAN, Vitaly SHMATIKOV: Robust De-anonymization of Large Sparse Datasets, Oakland 2008. Forrás: http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (2016.08.29.)

viii. Testing for Command Injection (OTG-INPVAL-013), Forrás: https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013) (2016.08.29.)

Dr. Szabó Csaba – Horváth Alexandra – Nagy Bence

A KÖZÖSSÉGI MÉDIA BIZTONSÁGPOLITIKAI KÉRDÉSEI

A KÖZÖSSÉGI TARTALMAK RENDÉSZETI VONATKOZÁSAINAK VIZSGÁLATA

Tartalomjegyzék

Bevezetés

Jelen tanulmány egy olyan rendészeti szempontból meghatározó problémával foglalkozik, mint a közösségi szerepvállalások veszélyei az egyén részéről, valamint a rendőrség közösségi oldalakon történő jelenlétének viszonyrendszerei. Számos új és releváns biztonságpolitikai kérdés vár megoldásra, mind a kormányzatok, mind a rendészeti szervek és a nemzetbiztonsági szolgálatok részéről, amelyek negatív mértékben befolyásolják az egyén szubjektív biztonságérzetét. A kiberbűnözés megelőzése és az kibertérben elkövetett bűncselekmények realizálása nagyfokú szakértelmet és együttműködést igényel mind a rendvédelmi szervek, mind a jogkövető magatartást tanúsító állampolgárok részéről.

Kutatásunk a közösségi oldalakat és tartalmakat aktívan alkalmazó, valamint a közösségi média hírtartalmait rendszeresen „fogyasztó" személyek véleményére helyezi a hangsúlyt. A kutatás átfogóan bemutatja a közösségi oldalak történetét és jelenlegi helyzetét, kitekintéssel a rendészeti szervek közösségi oldalakon betöltött nemzetközi szerepvállalására. A közösségi oldalakkal összefüggésben elkövetett bűncselekmények a kibertér bűnügyi és nemzetbiztonsági kihívásai között előkelő helyet töltenek be. A közösségi tartalmak rendvédelmi vonatkozásai jelentős mértékben meghatározzák a közösségi oldalak felhasználóinak véleményét a rendőri szervek irányába. Szükséges megismerni a fiatal generáció véleményét a közösségi oldalak veszélyforrásaira vonatkozóan, valamint szükséges reflektálni ezekre a megfogalmazott veszélyekre a rendészeti szervek oldaláról.

A tanulmány bemutatja és elemzi a közelmúltban elkövetett egyes bűn- és terrorcselekményeket a közösségi média és a közösségi tájékoztatás szempontjából. Megvizsgálja azokat a lehetséges rendészeti eljárásokat és módszereket, amelyek alkalmazásával a közösségi tájékoztatás hatékonysága erősítésre kerülhet a lakosság biztonságérzetének növelése érdekében. Ajánlások kerülnek megfogalmazásra a rendőrség közösségi oldalakon és a közösségi médiában történő szerepvállalásának erősítése érdekében a hazai viszonyrendszerek figyelembevételével.

Kérdőíves kutatás kerül bemutatásra és elemzésre, amely a rendőrség és a közösségi tájékoztatás szerepének vizsgálatát kutatja.

I. A közösségi tartalmak rövid történeti áttekintése

Manapság a közösségi weboldalak, mint például Facebook és a Twitter szinte már-már kikerülhetetlen tényezői a modern életnek, különösen, ami a fiatal generációt illeti. Úgy tekintjük és használjuk a közösségi oldalakat, mintha azok mindig is az életünk részei lettek volna. Ma már egy fiatalnak elképzelhetetlen az élet internet és közösségi oldalak nélkül, ráadásul az okostelefonok világa elhozta a mobil internetezés lehetőségét, vagyis bárhol és bármikor csatlakozhatnak a világhálóra, és beszélgethetnek barátaikkal, megoszthatnak, illetve kedvelhetnek fényképeket és posztolhatnak egyéni tartalmakat. Azonban ez nem mindig volt így.

Első lépésben érdemes tisztázni mit is nevezünk *közösségi oldalnak,* vagy *közösségi hálózatnak*. A közösségi oldalak, vagy közösségi hálók azon az elven működnek, hogy a felhasználó az ismerősei segítségével találja meg más ismerőseit az adott oldalon. Az internet erre kiváló lehetőséget nyújt, mivel az online jelenlét könnyebbé teszi a hálózatok kiépítését. Ennek a piaci lehetőségét különböző csoportok és cégek kb. 10-15 éve ismerték fel. Közösségi hálózatnak nevezzük azokat az internetes portálokat, ahol a regisztrált tagok kapcsolatba léphetnek egymással. *Más megközelítésben közösséginek nevezhetünk egy hálózatot, ha az azt használók közösségi kapcsolatra képesek egymással*.[6] Általában az ismeretségre és a közös érdeklődési körre épít. Így a közösségi oldalak kategóriába beletartoznak a *fórumok,* a *videó megosztó portálok* is, és persze a klasszikus értelembe vett *közösségi oldalak*. Természetesen az előbb említett fogalmak között nagy különbségek is vannak. A történetiséget tekintve a következő fontos események kiemelése szükséges.

Az első klasszikus értelemben vett közösségi oldal 1995-ben tűnt fel az amerikai weben a *Classmates.com* oldalon, melynek segítségével megtalálhatták egymást az emberek, akár az óvodában, akár a gimnáziumban, akár a katonaságban ismerkedtek meg. Az oldal azóta folyamatosan működik, jelenleg a harmadik leglátogatottabb közösségi hálózat az

[6] Danah M. Boyd és Nicole B. Ellison: *Network Sites: Definition, History, and Scholarship,* Journaol of Computer-Mediated Communication. 2007/11. 20-22. A szerzők három szempontban határozták meg a közösségi hálózatokat: 1. Lehetővé teszi az egyéneknek hogy nyilvános, vagy félig nyilvános szakosított oldalt hozzanak létre egy behatárolt rendszerben. 2. Összekösse azokkal a felhasználókkal, akikkel kapcsolatban vannak. 3. Megnézhessék és áttekinthessék kapcsolataikat és mások kapcsolatait az adott rendszerben.

Egyesült Államokban.[7] Ezen az oldalon azonban tényleges profiloldalt még nem lehetett létrehozni és ismerőseink ismerősei között sem tudtunk böngészni. A már teljes értelemben vett közösségi oldal, ami már majdnem minden kritériumnak megfelelt, az 1997-ben létrejött *SixDegrees* volt. A sixdegrees a hat lépés távolságra utal. Ennek az elméletnek az a lényege, hogy a Föld minden lakója ismeri egymást, méghozzá a saját személyes ismerősein keresztül. Az ismerős és az ismeretlennek gondolt személy között pedig 5 elem van.[8] Ekkoriban az internetes közösségi oldalak funkciója csak az volt, hogy tárolta az ismerősöket, egy helyre gyűjtötte az adott felhasználó baráti körét.

Radikális változás csak a 21. századba lépve következett be, amikor megjelent a *virtuális közösség* fogalma. A fogalom értelmében a virtuális közösségek olyan társadalmi gyülekezetek, amelyek az Interneten tűnnek fel, ha ehhez elég ember a megfelelő emberi érzésekkel nyílt megbeszéléseket folytat, és személyes kapcsolatok hálóját alkotja a kibertérben. (Tapscott, 2001.) Ebben már a felhasználók közötti fórumozás, üzenetküldés, blogolás és képmegosztás vált a közösségek alkotójává. Az interaktivitás lehetősége rengeteg embert vonzott, a közösségi hálózatok egyre népszerűbbek lettek a felhasználók körében. 2005-ben már 200 ilyen portál közül válogathattak az internetezők, akkoriban ezek belül is a *MySpace* volt a leglátogatottabb. A közösségi oldalak megjelenése az online kapcsolatépítés újfajta eszköze lett, ez pedig egy újfajta piac kialakulását hozta magával. Nem meglepő tehát, hogy a világ legnagyobb internetes cégei, mint a Google, vagy a Yahoo is elindították saját hálózatukat. A következő években egyre több kisebb és nagyobb közösségi oldal jött létre.

Az online közösségeknek még nincs egy elfogadott definíciója, de *Preece* nyomán elmondható, hogy egy online közösség több összetevőből áll:

- *Emberek*, akik azért érintkeznek másokkal, hogy saját igényeiket kielégítsék, vagy valamilyen közösségi szerepet vállaljanak: vezetést, illetve moderálást
- *Közös szándék/cél*, mint például az azonos érdeklődés, információcsere igénye, vagy olyan szolgáltatás, mely a közösség létrejöttéhez nyújt alapot
- *Alapelvek* hallgatólagos feltevések, rituálék, szabályok és törvények formájában, amelyek az emberek interakcióit irányítják

[7]A közösségi hálózatok története. http://szocial.blogspot.hu/2008/05/kzssgi-hlzatok-trtnete.html, (letöltés ideje: 2016.10.03.)

[8]A közösségi oldalak: A közösségi oldalak története. http://felsofokon.hu/bolcseszettudomany/a-kozossegi-oldalalak-a-kozossegi-oldalak-tortenete/ (letöltés ideje: 2016.10.03.)

- *Számítógépes rendszerek*, melyek lehetővé teszik és közvetítik a szociális interakciókat és elősegítik az összetartozás érzését (Preece, 2000).

Továbbiakban a legnépszerűbb közösségi oldalak rövid átfogó történetének a bemutatására kerül sor.

I.1. A Facebook

Az egyik legnagyobb ismeretségi hálózat és egyben legnépszerűbb világszerte. 2004. február 4-én kezdte meg a működését Mark Zuckerberg révén, aki legjobb középiskolai barátjával létrehozott egy kezdetleges társasági oldalt az egyetemisták számára.[9] A Facemash nevű alkalmazás 2003-ban kezdte meg működését, amely nagyon hamar sikeres lett. Rengetegen kezdték el használni, használóinak a száma hamar elérte a százezret. Ennek hatására Mark Zuckerberg egy új programot kezdett el írni, a CourseMatch programot. A későbbiekben Mark néhány egyetemi társával egy új fejlesztésbe kezdett, melynek eredményeként megalapították a Facebookot. A munkáját segítette: Eduardo Saverin, Dustin Moskovitz és Chris Hughes. Az oldal kezdetleges szakaszában csak a Harvard egyetem hallgatói számára volt elérhető, csak később terjesztették ki az Ivy League-re és a Stanford Universityre. Ezután sorra követték egymást a fejlesztések mindaddig, míg minden 13 évesnél idősebb személy regisztrálhatott a Facebookra. Rengeteg munkával és támogatással elérték azt, hogy 2009-ben már a világ leggyakrabban használt szociális hálózatává vált, majd 2011 februárjára már több mint 637 millió regisztrált felhasználója volt. A következő mérföldkő 2012. október 4-e ugyanis ezen a napon elérte az 1 milliárd regisztrált felhasználót.[10]

A Facebook egy olyan közösségi oldal, ahol a felhasználók egy saját profiloldalt tudnak létrehozni maguknak, írhatnak üzenőfalukra, képeket tölthetnek fel és üzeneteket küldhetnek egymásnak. Az oldal jelenleg 207 országban és 37 különböző nyelven érhető el.[11]

Azonban, mint minden számítógépes rendszer, a Facebook is tartalmaz olyan elemeket, amelyek veszélyt jelentenek a felhasználóra. A biztonsági szoftverek megpróbálják kiszűrni ezeket, de valójában a felhasználó tudja a legjobban megvédeni magát, ha odafigyel ezekre az elemekre. Egy kimutatás szerint négy éven keresztül nem voltak védve adataink. A

[9] Carlson, Nicholas: *At Last — The Full Story Of How Facebook Was Founded*. Business Insider (online, 2010. március 5.)

[10] Schwartz, Bari: *Hot or Not? Website Briefly Judges Looks*. Harvard Crimson. (2009.)

[11] Facebook history. https://hu.wikipedia.org/wiki/Facebook. (letöltés ideje: 2016.10.04.)

Symantec 2011 májusában jelentette be, hogy egy olyan rés volt a Facebook rendszerében, ami 2007-től éveken át lehetővé tette, hogy a közösségi oldalakon jelen lévő harmadik felek (hirdetők, szolgáltatást kínálók stb.) hozzáférhessenek az összes felhasználó adataihoz (profil, képek, chatüzenetek stb.), akkor is, ha a fióktulajdonos ezt nem engedélyezte. A Symantec már korábban, április második hetében értesítette erről a Facebookot, akik megtették az első lépéseket a hiba kijavítására, és a köszönetnyilvánítás mellett hivatalosan is közölték, hogy vizsgálatuk semmiféle bizonyítékot nem talált arra, hogy bárki is kihasználta volna a lehetőséget adatgyűjtés céljából. A médiában ez után indult hatalmas hírverést követően a Facebook fejlesztői blogjában bejelentette, hogy a gondokat okozó régebbi autentikációs rendszerüket frissítik az OAuth 2.0 és a HTTPS bevezetésével.[12] Természetesen, ez nem azt jelenti, hogy innentől kezdve nincsenek veszélyek számunkra az oldalon.

I.2. A Twitter

A Facebook után a második legismertebb közösségi oldal. A Twitter 2006 márciusában jelent meg egy kutatási és fejlesztési projektként, amelyet az Odeonál Noah Glass és Jack Dorsay alapított. Októberben már létre is jött a Twitter rendszere a San Franciscó-i Obvious Corp. által. 2007-ben elérte, hogy elnyerte a South by Southwest (SXSW) Web díját, blog kategóriában. Ez egy olyan ismeretségi hálózat és mikroblog szolgáltatás, ahol egy azonnali üzenetküldő alkalmazáson, vagy webes szolgáltatáson keresztül, rövid bejegyzéseket vagy üzeneteket küldhetnek egymásnak a felhasználók rövid szöveges üzenet formájában.[13] A friss bejegyzések a felhasználó profilján jelennek meg, de azonnal láthatók az olyan felhasználók által is, akik feliratkoztak az adott felhasználó frissítéseire. Az üzenet küldője meghatározhatja, beállíthatja, hogy bejegyzéseit kik láthatják. Alapbeállításként mindenki láthatja, de ez szűkíthető saját baráti körre is. A Twitter ingyenes, de ha valaki rövid szöveges üzeneten keresztül kommunikál a rendszerrel, akkor a mobilszolgáltatónak az SMS-küldés díját meg kell fizetnie. Természetesen, mint a Facebook esetében, itt is volt biztonsági rés, mely problémát hamar sikerült orvosolni. A biztonsági rést 2007. április 7-én jelentette be Nitesg Dhanjani. A probléma oka az volt, hogy a Twitter az SMS-t küldő telefonszám által azonosította a felhasználót. Ez a rés csak akkor használható, ha a felhasználó telefonszáma ismert volt. Pár héten belül a Twitter bevezetett egy opcionális

[12] A Facebook 4 évig nem védte adatainkat. http://www.nyest.hu/hirek/a-facebook-4-evig-nem-vedte-adatainkat (letöltés ideje: 2016.10.04.)

[13] Levy, Steven: *Twitter: Is Brevity The Next Big Thing*? Newsweek. 2011.02.11. 15-16.

PIN kódot, amit a felhasználó határozhat meg, hogy biztosan azonosíthassák az SMS-üzenetek eredetét.[14]

I.3. Az Instagram

Nemrégiben lépett be a köztudatba egy kicsit másfajta közösségi oldal, amely fényképek és rövid videók megosztásán alapul. Csak okostelefonon érhető el, amelyen a felhasználók fényképeket, videókat készíthetnek, különböző művészi hatású effektekkel láthatják el, feliratozhatják, végül pedig megoszthatják ezt másokkal. A fényképen, videón megjelölheti a fénykép, videó készítésének helyét és megoszthatja név szerint azt az embert, akivel ezeken szerepel. A megosztás mehet az Instagramon belül és azon kívül több különböző közösségi hálózatban (Facebook, Twitter) és e-mailben is.[15] Ezeket a képeket a felhasználók kommentálhatják és kinyilváníthatják tetszésüket róla. 2010 októberében kezdte meg működését az Apple Inc. készülékein. Rohamos növekedés volt jellemző rá. Nagyon sokan megkedvelték az alkalmazást az egyszerűsége és a kreált fotók egyedisége miatt. 2010 decemberében már 1 millió felhasználó használta világszerte az alkalmazást, amely 2011 júniusára 5 millió felhasználóra bővült. Ekkor már közel 100 millió fotó volt elérhető benne. 2012 januárjában már 15 millió felhasználó használta az alkalmazást és ekkor már közel 400 millió fotót osztottak meg Instagramon. 2013-ban már 100 millió felhasználót tudhat magának az alkalmazás. 2012. április 12-én a Facebook megvásárolta az alkalmazást 1 milliárd dollárért, melyet készpénzben és részvényekben fizetett ki. Az eseményt Mark Zuckerberg, a Facebook alapítója egy Facebook bejegyzésben jelentette be.[16]

I.4. Magyarországi helyzet bemutatása

Ebben a fejezetben részletesebben kerül kifejtésre a közösségi oldalak Magyarországi helyzete és szerepe. Magyarországon elsőként 2002-ben találkozhattunk ilyen típusú hálózattal, ez nem más volt, mint a jelenlegi IWIW elődje, a WIW. A rövidítés a who-is-who kifejezésből ered, és egy baráti társaság ötlete alapján jött létre. Akkoriban azonban még csak szárnypróbálgatásnak indult, az igazi áttörést az jelentette, amikor 2005-ben a Telecom

---

[14] A Twitter. https://hu.wikipedia.org/wiki/Twitter (letöltés ideje:2016.10.04.)

[15]Tsukayama, Hayley: *Instagram adding ads boosts Facebook's outlook, analysts say*. The Washington Post. 2014.01.24. 25-26.

[16] Instagram. https://hu.wikipedia.org/wiki/Instagram. (letöltés ideje: 2016.10.05.)

csoport tulajdonába került az oldal. Ha már magyar közösségi portálokról beszélünk, akkor meg kell megemlíteni a MyVip, a BarátiKör.hu, és a MyBarát.hu elnevezésű oldalakat is. Mindegyik más felépítésű, lényegük mégis ugyan az: *közösséget kiépíteni*. Első lépés az oldalra történő regisztráció, amely megvalósulhat szabadon vagy meghívás útján. Minden felhasználó saját profillal rendelkezik, ahol személyes információkat oszthat meg magáról, képi és hanganyagot egyaránt feltölthet, csatlakozhat klubokhoz, csoportokhoz, internetes naplót vezethet, apróhirdetéseket adhat fel és élvezheti a különböző alkalmazások nyújtotta szórakozási lehetőségeket. Az egyéni kapcsolatok ápolásán túl alkalmasak üzleti, marketing célokra is, például a különböző cégek személyre szabott ajánlatokkal bombázhatják a felhasználókat. Ezek csak kisebb próbálkozások voltak, ugyanis a világ legnépszerűbb oldalai között ezek nem szerepelnek. Egy kimutatás alapján az első három legnépszerűbb közösségi oldal a Facebook, a Youtube és a Twitter.[17]

I.5. A közösségi oldalak szerepe a mai generáció szemével

A mai generációnál jól észrevehető az internet térhódítása. Ez alatt olyan dolgokat értek, mint például, hogy már egész fiatal korban úgy kezelik az okostelefonokat, laptopokat, tabletokat, mintha az mindig is életük része lett volna. Nagyon ritka az olyan fiatal, aki nincs regisztrálva valamilyen közösségi oldalon, vagy ne olvasna nap, mint nap híreket, vagy éppen ne írna blogokat. Az Internetnek a média világára gyakorolt hatásait tekintve három fontos tényezőt különböztethetünk meg: Az egyik az, hogy az Internetnek hála az emberek rengeteg információhoz férhetnek hozzá. A másik, hogy általa hétköznapi emberek kapnak lehetőséget arra, hogy véleményüket nyíltan kinyilvánítsak. A harmadik tényező, hogy segítségével csoportok szervezhetik meg tevékenységüket.

Azt már az elején érdemes leszögezni, hogy a mai generáció másként fogja fel a közösségi oldalak szerepét, mint az idősebb generáció. Míg a 18 éven aluliaknak, vagyis a Z-generáció tagjainak az a fontos, hogy minél több emberrel legyenek kapcsolatban, addig az Y (19-32 év) generációsok körében ez nem fontos.

Egy kétfázisos kutatás azt vizsgálta, hogy milyen hatást gyakorol a közösségi média az új generációkra és a fogyasztási szokásaikra. A kutatás megvizsgálta mindkét generációnál, hogy milyen szinten fontos számukra az úgynevezett *lájk*. A vélemények összegségéből az derült ki, hogy a 18 éven aluli fiataloknál az számít a legnépszerűbbnek, aki a legtöbb

[17]Top 15 Most Popular Social Networking Sites.http://www.ebizmba.com/articles/social-networking-websites. (letöltés ideje: 2016.10. 08.)

kedveléssel, ismerőssel rendelkezik. Ugyanez az időseknél szinte egyáltalán nem volt fontos. Egy másik szempont szerint arra az eredményre jutott a kutatás, hogy a 18 éven aluli fiatalok szokták retusálni és effektekkel ellátni képeiket mielőtt feltöltik azt, annak érdekében, hogy a közösségi oldalakon magukat minél jobb színben tüntessék fel. Ez az Y generációnál nem mondható el. A kutatás alapján beigazolódott az is, hogy a Z generációnak relatíve fontosabb a pozitív visszacsatolás a közösségi oldalakon, mint az Y generációnak, és hogy a közösségi média felerősíti a megfelelési kényszert az Y- és Z generáció tagjainál. Bebizonyosodott az is, hogy mindkét generáció tagjai pozitív énkép megjelenítésére törekednek a közösségi oldalakon.[18] A fiatal generációról elmondható, hogy sokkal több hajlandóságot mutatnak arra vonatkozóan, hogy megosszanak valamilyen internetes tartalmat - például képet, tartózkodási helyet, aktuális állapot, életérzést - annak ellenére, hogy mind a Z, mind pedig az Y generáció tagjai egyaránt napi rendszerességgel látogatják ezeket az oldalakat, általában kapcsolattartás céljából. Végül még egy meglepő eredmény, miszerint mindkét generáció egyaránt elégedetlen magával valamilyen téren, és mások véleményeire hagyatkozva ítélik meg magukat.

A vizsgálat második felében szükségszerű kitérni arra, hogy egyre több az a fiatal, akik már nem úgy látják ezeket az oldalakat, mint a fent említett idősebb generációk tagjai. Számtalan kutatás, felmérés jelent már meg arra vonatkozóan, hogy az egyes közösségi csatornákat milyen arányban használják a tizenévesek, de a korosztály tagjaitól származó vélemények, meglátások alapján alkothatunk igazán átfogó képet arról, mi áll ezeknek az adatsoroknak a hátterében, és mi határozza meg az ő esetükben a különböző felületekkel kapcsolatos preferenciákat. Egy tizenkilenc éves texasi fiatal vette sorra napjaink legnépszerűbb közösségi oldalait és mindegyiket a tizenévesek szemszögéből értékelte. Az tény, hogy elismeri benne, a vélemények még nem reprezentatívak, de a környezet véleményét hordozzák, amellyel érdemes foglalkozni.

Vizsgáljuk meg, minként vélekednek a legnépszerűbb közösségi oldalról, a Facebookról.

Számunkra a Facebook halott. A Facebook valami olyasmi, amit mindenki használt korábban, mert menő volt, de most már olyan, mint egy kínos családi vacsora, ahonnan nem

[18]Az ma a menő fiatal, akinek sok a lájkja a közösségi médiában. http://24.hu/media/2016/08/03/az-ma-a-meno-fiatal-akinek-sok-a-lajkja-a-kozossegi-mediaban/ (letöltés ideje:2016.10.10)

lehet lelépni.[19]- mondja a kutatásban résztvevő egyik személy. Gondol itt arra, hogy akármennyire is nem szeretne fenntartani profiloldalt, mégis az ismerősök, barátok általi nagy nyomás következtében nem tud kilépni ebből a világból. Az internetező fiatalok továbbá elmondták, hogy manapság csak annyira lépnek fel az oldalra, hogy megnézzék a friss híreket és informálódjanak. Negatív kritikát kapott az üzenőfalak minősége és a reklámok sokasága. A messenger részét viszont előszeretettel használják naponta többször is és elégedettek vele.

Következtetésként levonhatjuk, hogy bár a fiatalok nem szívesen használják a már elavultnak minősülő facebookot, az *internet word stats*[20] adatai szerint egyre több felhasználót számlál, a 3.6 milliárd internetezőből 1.1 milliárd rendelkezik facebook profillal. Ezt követi a második legnépszerűbb képmegosztó, a Twitter, mely 310 millió felhasználóval rendelkezik. A facebookkal ellentétben a kép- és videómegosztó programok, mint például a Twitter vagy az Instagram, sokkal közkedveltebbek. Egyszerűbbek, kezelhetőbbek, nincsenek zavaró reklámok. A Z generációnál már megemlített képretusálásra sokkal jobb lehetőségeket nyújtanak, a kép, videó és hanganyagok könnyebben megoszthatók, valamint ezen programok fő funkciója a lájkok gyűjtése, a képek kommentelése (értékelése, azokhoz megjegyzés fűzése), másodlagos funkcióként azonban jelen van az élő idős chat. Ezeken a megosztókon könnyedén találhatjuk meg ismerőseinket és vehetjük fel velük a kapcsolatot, ugyanakkor esélyt teremtenek olyan emberek megismerésére, akikkel addig nem még nem találkoztunk. A Twitter és Istangram programok nem igényelnek meghívót egy már aktív tagtól, a bejelentkezés teljesen szabad, így bárki számára elérhető. Folyamatosan frissülő tartalmuk egyre több és több filtert és képszerkesztő opciót tartalmaz, amely szintúgy csábító a Z generáció számára.

Összességben kijelenthető, hogy mind az Y, mind a Z generáció számára elengedhetetlen a mindennapi kapcsolattartás szempontjából a közösségi média, életük szerves részét képezi. Kapcsolatépítő és -fenntartó szerepük nem elhanyagolható, mindazonáltal rengeteg veszélyforrást hordoznak magukban a közösségi oldalak. Olyan bűncselekményi formák alakultak ki az idők folyamán a közösségi oldalakon, mint a személyes adatok megszerzése, rágalmazás, becsületsértés, zaklatás, pedofília, amely bűncselekmények elkövetői az esetek többségében rejtve tudnak tevékenykedni. A rendészeti szervek – kiemelten a rendőrség – szerepe elengedhetetlenül fontos, hogy kiemelt figyelmet

[19]Ezért halott a Facebook a fiatalok számára. http://bitport.hu/ezert-halott-a-facebook-a-fiatalok-szamara (letöltés ideje: 2016.10.11)

[20]Social Media Website Stats. http://www.internetworldstats.com/social.htm#world (Letöltés ideje: 2016.10.12)

fordítson a közösségi oldalakon zajló eseményekre, mivel a valós életben elkövetett bűncselekmények a virtuális térben is szedik áldozataikat. A virtuális térben élő személyek is igénylik a hatóságok védelmét és jelenlétét. A közösségi oldalak megkönnyítik a mindennapi kapcsolattartást és információcserét egymás között, azonban megannyi veszélyt is rejtenek magukban. A kiberbiztonság erősítése minden állam elsődleges feladata kell, hogy legyen, hiszen nem csak az állampolgárok szubjektív biztonságérzetét rontja, ha a közösségi oldalakon támadás éri őket, hanem a kritikus infrastruktúrák biztonságos működését is veszélyezteti a kiberbűnözők illegális tevékenysége.

II. A közösségi média szerepe a válsághelyzetekben

II.1. Franciaországi terrorcselekmények, rendőrgyilkosságok és terrorcselekmények az USA-ban

A brüsszeli terrorfenyegetettség erősödésének hatására a belga rendőrség számos különleges intézkedést vezetett be, amelyek között szerepelt az is, hogy megkérték a lakosságot, hogy a közösségi oldalakon keresztül ne tudósítsanak a rendőrök mozgásáról. A brüsszeli rendőrség okkal feltételezhette, hogy a lakosság által a közösségi oldalakon megosztott posztok a rendőri intézkedésekről, a rendőri jelenlétekről komoly kockázatot jelent az elkövető terrorista személyek felkutatása során. A lakosság által szolgáltatott - gyakorlatilag percre pontos - frissítésekből könnyen kikövetkeztethetővé vált a nyomozás aktuális státusza, a tervezett házkutatások, átvizsgálások.

Ennek elkerülése érdekében Steven Vandeput, a belga védelmi miniszter saját twitter oldalán felhívást tett közzé, melyben arra kérte a lakosságot, hogy segítsék a rendőrség munkáját azzal, hogy nem tesznek közzé rendőri akciókkal kapcsolatos állapotfrissítéseket.[21] A megszólítottak azonnal reagáltak a felhívásra, és macskás képeket kezdtek posztolni olyan leírásokkal, melyeknek a szövegei rendőrségi akciókról szóló jelentéseket utánoztak. A belga internetezők bár megtalálták a tragikus esemény humoros oldalát, azonban az eset nagyon jól jelképezi, mekkora hatalomra tett szert a közösségi média a különböző krízishelyzetekben és a rendőrségi akciók kezelésében.

[21] A közösségi média szerepe válsághelyzetekben. http://mtmi.hu/cikk/823/A_kozossegi_media_szerepe_valsaghelyzetekben. (letöltés ideje: 2016.10.02.)

A közösségi média a rendőrség szempontjából nézve kétélű fegyver. A házkutatásokról, lezárásokról, helyszínbiztosításokról és különböző akciókról történő valós idejű közvetítések, tudósítások, posztok könnyen a bűnelkövetők eszközévé válhatnak az igazságszolgáltatás elől való menekülés során, azonban a rendőrség is könnyedén a saját oldalára állíthatja ezt a hatalmas információáradatot kezelő hálózatot. Manapság nagyon sok információt osztunk meg önszántunkból ezeken az oldalakon, így a rendőrség is könnyebben felfedezheti és megfigyelheti az esetlegesen gyanúba keveredett személyeket.

Az ilyen közösségi médiákon történő információgyűjtést nevezzük *OSINT*-nak (open source intelligence). Ez az információszerzési lehetőség bárki számára elérhető, legális és gyakorlatilag napra kész adathalmaz. Ugyanakkor nem szabad megfeledkezni arról az oldaláról sem, hogy ezek az információk ellenőrizetlen, kétes források, melyek könnyedén félrevezethetnek akár nagy tömegeket is. Erre tökéletes példa a párizsi merényletet követő, kezdetben viccnek induló fotó, melynek elbírálása hamar éles fordulatot vett. Veerender Jubbal kanadai videójáték-blogger saját maga által közzétett képét valaki több helyen is módosította, melynek következtében a szikh vallású férfi ártatlan fürdőszobai szelfije rögtön terroristaképpé alakult át, és a közösségi oldalakon villámgyorsan elterjedt, mint a támadások egyik elkövetőjének akció előtti fotója.[22] A kép hihetetlen gyorsasággal ismertté vált az interneten, és hamar bekerült az újságokba is. Bármiféle ellenőrzés nélkül átvette Európa legnagyobb bulvárlapja, a német Bild, közzétette a Twitteren az olasz Sky TG24 tévéadó, a spanyol La Razón című újság még a címoldalára is kitette, egy az ISIS-hez közelálló Facebook-oldal pedig azzal az aláírással közölte, hogy a tudósítások szerint ő az egyik testvérünk, aki végrehajtotta a dicsőséges, Párizs elleni támadást.

Hasonló téves információk tucatjai kezdtek terjedni a közösségi oldalakon a lekapcsolt Eiffel-toronnyal, üres párizsi utcákkal, terrorista bevándorlókkal és más részletekkel kapcsolatban, melyekről azonban később mind kiderült, hogy csúsztatások vagy hamisítások. A közösségi oldalak egyik újítása a stream, vagyis az élő közvetítés. Ez az opció okolható az Amerikai Egyesült Államokban történt sorozatos rendőrgyilkosságokért.[23] Ugyanis élő közvetítésben került ki egy eset a világhálóra, amit napokon belül 4 millióan tekintettek meg

[22] Ashitha Nagesh: *Nice attack: Man wrongly identified as being behind Bastille Dayterror.* Metro UK. 2015.07.15.

[23] Fecebook live streaming of us police shooting of a black man leads. http://www.telegraph.co.uk/technology/2016/07/07/facebook-live-streaming-of-us-police-shooting-of-black-man-leads/ (letöltés ideje: 2016.10.12)

facebookon. Ezt követően a rendőrt megvádolták, hogy faji előítéletek miatt lőtt rá a gépkocsiban ülő férfira. Ez azonban nem derül ki a közétett videóból. Az esetet követően több rendőrre is rálőttek az utcán, melyeknek halálos kimenetele is volt. A közösségi médiák ellenőrizetlenül közzétett hírei befolyásolják a tömegeket és súlyos bűncselekmények kimenetelére adhatnak okot.

Mindazonáltal megállapítható, hogy pozitív hozadéka is van a közösségi médiának.

Több internetes portál beszámolt arról, hogy a párizsi terrortámadások során a közösségi média milyen jelentős segítséget nyújtott a párizsi lakosok számára. Kezdve onnan, hogy a facebook újonnan bevezetett funkciójának hála a felhasználók egyszerűen tudathatták ismerőseikkel, hogy biztonságban vannak, azon keresztül, hogy párizsi lakosok százai jelentkeztek twitteren, hogy befogadnak bárkit, aki nem tudott éppen biztonságban hazajutni aznap este egészen odáig, hogy az Airbnb is arra kérte a lakásokat kiadókat, hogy nyissák meg otthonaikat azok előtt, akiknek nem volt hova menniük. A bemutatott példák mind a pozitív mind a negatív oldalt jól bemutatják a közösségi média világának. A közösségi médiák krízishelyzetben való segítsége nem elhanyagolható tényező, beszéljünk akár arról, hogy az információáramlás egyik leggyorsabb módját képezik, beszéljünk akár az előre megírt programok (google person finder)[24], alkalmazások sokaságáról, amik ilyen helyzetben a bajbajutottak segítségére lehetnek, illetve a legkézenfekvőbb opciójukról, hogy a segítségre szorulók és a segíteni vágyók egy felületen tudnak kapcsolatba lépni egymással. Ugyanakkor azt is jól szemlélteti, hogy a médiák nem megfelelően ellenőrzik forrásaikat, és hogy ezek a közösségi médiák egész szervezeteket képesek pillanatok alatt a tömeg ellen fordítani. Ennek oka nem feltétlenül a szándékosság. Ezek a hírportálok próbálnak lépést tartani a közösségi oldalakon terjedő hatalmas információáradattal és minél nagyobb nézettséget/olvasóközösséget igyekeznek kiépíteni. Ennek okán mulasztják el a közzétett hírek forrásainak ellenőrzését.

Megállapíthatjuk tehát, hogy bár a közösségi média sokszor nehezíti a XXI. századi emberek életét, és olyan problémákat okoz, amelyek a régi korokban fel sem merültek, ugyanakkor katasztrófák, krízishelyzetek idején megfelelően használva, már-már közszolgálati segítség lehetősége rejlik benne, amely a korábbi időkben elképzelhetetlen lett

[24] Google person finder. https://google.org/personfinder/global/home.html (letöltés ideje: 2016.10.11)

Google person finder history. https://en.wikipedia.org/wiki/Google_Person_Finder (letöltés ideje: 2016.10.11)

volna.[25] Megfelelő célra használva, árnyoldalait is ismerve és azok ellen védekezve a közösségi médiák a XXI. század szerves részét képezve a krízishelyzetek megoldásának kulcsát képezhetik a jogkövető magatartást tanúsító lakosság aktív bevonásával az egész világon.

II.2. A magyar rendőrség szerepvállalásának kiszélesítése a közösségi oldalak vonatkozásában

Az internet számos lehetőséget nyújt az oktatás és a társadalom közösségi életének minden területén. Azonban nem hagyható figyelmen kívül, hogy a gyerekek ki vannak téve olyan veszélyeknek is, amelyek kortól és földrajzi helyzettől függetlenül jelen vannak az egész világon. A gyermekek jogait sértő képek, felnőtt tartalmak kerülnek fel az internetre; felnőtt internetes támadók szexuális irányultságú beszélgetésekbe vonják be a gyanútlan fiatalokat és internetes zaklatás teszi tönkre sok fiatal életét.[26] A regisztráció során gyakran nem veszik figyelembe a felhasználói licencszerződéseket, amelyekben le van írva mind a szerzői jogra vonatkozó tartalom, mind az adatvédelem módja. Az adatvédelmi beállításokkal könnyűszerrel kivédhető az adathalászati tevékenység egy jelentős része, azonban ezen beállításokkal rengeteg felhasználó nincs tisztában, a veszélyt nem érzékelik reálisnak. Ennek a valós veszélynek a megelőzéseként a magyar rendőrség már régebb óta tájékoztató előadásokat tart a fiataloknak és az idősebb korosztály számára, az internet és a közösségi oldalak veszélyeiről. A közösségi oldalakat használó fiatalok könnyen válhatnak bűncselekmények áldozatává, vagy akár elkövetőjévé úgy, hogy közben nem is érzékelik a valós problémát.

A prevenció érdekében a rendőrök a biztonságra nevelő iskolai programjaik végrehajtása során (D.A.D.A., Ellen-szer), az osztályfőnöki órák keretében, szülői és tantestületi értekezleteken tartott előadásaik mellett fontosnak tartják, hogy a gyerekek nevelésében közreműködő más munkatársak is kapjanak tájékoztatást a munkájukat segítő

[25]Közösségi média, mint remény katasztrófa idején. http://mtmi.hu/cikk/740/Kozossegi_media_mint_remeny_katasztrofa_idejen (letöltés ideje: 2016.10.12)

[26] A gyerekek online biztonsága.http://unicef.hu/a-gyerekek-online-biztonsaga/ (letöltés ideje: 2016.10.12)

információkról.[27] Kézenfekvő megoldás lenne, ha a rendőrség közvetlenebb módon lenne jelen a facebookon, valamint egyéb közösségi oldalakon, hogy a fiatalokat saját közegükben szólítsák meg. Elsődleges szempontként kijelenthetjük, hogy a tájékoztatás, a figyelemfelkeltés elengedhetetlen a már korábban megfogalmazott közösségi oldalakhoz kapcsolódó bűncselekmények elkerülése érdekében. Szükséges lenne egy olyan rendszer kiépítése, ahol a fiatal internetezők közvetlen módon tehetnék fel kérdéseiket a közösségi médiák használatával kapcsolatban a rendészeti szervek számára, és ezekre szakszerű, jól érthető, biztos forrásból származó válaszokat kapnának. Ez a megoldás kölcsönösen előnyös lenne, hiszen a közösségi rendőrség a public relation[28] (közönség kapcsolat) lényege a bizalom felkeltése, kialakítása, fenntartása, ez a kommunikáció tudatos kiépítése, melynek segítségével fokozható a szervezet ismertsége, elismertsége, elfogadottsága és megbecsültsége.

II.3. A közösségi tartalmak rendvédelmi vonatkozásai: Bűnfelderítés

A közösségi oldalak kétélű fegyverek. Az igazságszolgáltatás elől menekülők hasznára lehet a rendőrség elkerülése céljából, ugyanakkor a rendőrség számára is könnyen nyomravezető lehet egy-egy poszt, chat, vagy állapotfrissítés. Ennek kiaknázása hazánkban nem bizonyított, az Országos Rendőr-főkapitányság nem támasztja alá, hogy nyomozásai során használna bármilyen közösségi oldalt az elkövetők felkutatására. Ellentétben az Amerikai Egyesült Államokkal, ahol már megfigyelhető ez a tevékenység, olykor nem feltétlenül legális módon. Egy nemrég közzétett anyagból kiderül, hogy az FBI előszeretettel használja a közösségi oldalakat a nyomozáshoz, alibik igazolásához vagy cáfolatához és a bűncselekmények felderítéséhez. A dokumentumhoz az EFF szabadságjogi szervezet jutott hozzá, miután az információszabadságról szóló törvény nevében kikérte az adatokat az amerikai Igazságügyi Minisztériumtól.[29] Nemcsak az Amerikai Egyesült Államokban figyelhető meg a közösségi médiák bűnfelderítésre történő felhasználás. Az Open *Source Intelligence* (OSINT), vagyis a nyílt forrású információszerzés egy olyan, eddig alig

[27]Közösségi oldalak veszélyeiről.http://www.police.hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag/kozossegi-oldalak-veszelyeirol (letöltés ideje: 2016.10.12)

[28] A közösségi hálózatok és a közösségi rendőrség kapcsolata. (Mi keresni valója van a rendőrségnek a Facebookon?)
http://epa.oszk.hu/02500/02538/00008/pdf/EPA02538_nemzetbiztonsagi_szemle_2015_01_026-051.pdf

[29]Mit művelnek a rendőrök a facebookon. http://index.hu/tech/2010/03/30/mit_muvelnek_a_rendorok_a_facebookon/ (letöltés ideje: 2016.10.12)

kiaknázott lehetőséget nyúlt az igazságszolgáltatás számára, ami az online közösségi médiák előtt nem állt rendelkezésükre. Ez a nyílt forrású információszerzés lehet a kulcsa a hatékonyabb bűnfelderítésnek, bűnmegelőzésnek. A közösségi média további előnye a rendőrség szempontjából, hogy a lakosság érdekében elért eredményeket a lakosság számára is ismertté teheti. Ennek célja, hogy tudatosítsa a lakosságban: a rendőrség munkája értük van. Ez az úgynevezett bizalomépítő rendőrség (*reassurance policing*). A közösségi oldalak és egyéb közösségi médiák előnyeként vehető számba a nagy tömegek megmozgatása és a gyors hírközlés. Ezt használta ki az Országos Rendőr-főkapitányság a kormány augusztus 10-ei döntését követően, miszerint háromezer fővel bővítik ki a határvadászszázadok létszámát. Ez az illegális migrációs nyomás növekedése miatt vált szükségessé. Papp Károly országos rendőrfőkapitány sajtótájékoztatón jelentette be, hogy a rendőrség szeptember elsején kezd toborzást a többi közt a megyei és a járási kormányhivatalok, valamint a pályaorientációs iskolák bevonásával, de felhasználják a közösségi média nyújtotta lehetőségeket is.

A gyors toborzás érdekében elindult az Országos Rendőr-főkapitányság határvadász-toborzó facebook oldala,[30] melyen a Készenléti Rendőrség Határvadász Bevetési Osztályainak állományába járőrtárs beosztás betöltésére kínáltak lehetőséget. Ezen a facebook oldalon minden szükséges információ elérhető volt. Ez nagyon jól megmutatja, hogy a közösségi média mekkora erővel bír az emberek informálásával kapcsolatban.

Összesítve kijelenthetjük, hogy a közösségi médiák szükséges résztvevői a mindennapjainknak. A rendőrségi szerepvállalás tekintetében mind a felhasználók védelmének érdekében, mind a bűnmegelőzésben, mind a bűnfelderítésben nagy lehetőségeket nyújtanak ezek az oldalak. A lakosság gyors és biztos tájékoztatásának módját kínálják ezek az online felületek. Ezeknek a lehetőségeknek a kiaknázásával egy még hatékonyabb és közvetlenebb rendőrség építhető ki, amely a lakosság számára bizalmat sugároz, és közvetlenebb elérhetőséget nyújt rendkívüli helyzetek kialakulása esetén.

[30] Facebookon toboroz határvadászokat a rendőrség.http://24.hu/kozelet/2016/08/24/facebookon-toboroz-hatarvadaszokat-a-rendorseg/ (letöltés ideje: 2016.10.12)

Határvadász-képzés: Jelentkezz még ma! https://www.facebook.com/hatarvadaszkepzes/?fref=ts (letöltés ideje: 2016.10.12)

III. A közösségi tartalmak biztonságpolitikai kérdései

III.1. A közösségi média árnyoldala

Közösségi hálók igen nagy népszerűségnek örvendenek napjainkban. Ez azonban nem csupán a technológiai fejlődésnek, hanem a társadalmi szokásoknak, viselkedésnek és a szociális kapcsolatok átalakulásának is köszönhető. Az adatvédelem így nem csupán technológiai kérdéseket vet fel, hanem az emberi felelősséget is nagyban próbára teszi. Behálózott társadalmunkban, ahol életünk minden területét meghatározza, hogy fent vagyunk az interneten, számos új kockázat és kihívás jelenik meg: *hekkelés, szervertámadás* és egyéb technikai fejlettség okozta kockázatok. A közösségi oldalak kapcsán egyre többet lehet hallani a kockázatokról, a veszélyekről, és a visszaélésekről. A közösségi portálok, amelyeket mindennap használunk (Facebook, Twitter) a legdinamikusabban fejlődő webkettes szolgáltatások közé tartoznak. Hatalmas lehetőségek rejtőznek bennük és persze hatalmas kockázatok is. A következőkben a közösségi oldalakban rejlő veszélyforrások kerülnek bemutatásra.

Akármennyire is úgy tűnik, amiket ezekre a népszerű közösségi oldalakra posztolunk, legyen az csak egy fénykép, ártatlannak tűnnek, és nem jelentenek veszélyforrást, de sajnos ez nem minden esetben van így. Kikerülnek az ellenőrzésünk alól, ezáltal elérhető lesz a nyilvánosság számára. Észre sem vesszük, mennyi személyes adatot osztunk meg magunkról idegenekkel, amely hatalmas veszélynek teszi ki a szolgáltatásokat használók százmillióit. A rengeteg megosztott információ mágnesként vonzza a rosszindulatú kíváncsiskodókat, kémkedőket, számítógépes bűnözőket, sőt még a hatóságokat is, amelyek adatbányászati módszerekkel igyekeznek megelőzni a bűncselekményeket, illetve felderíteni a már megtörtént eseteket. Az évek teltével ugyan sokan visszafogták a közösségi tevékenységüket, odafigyelnek az adatvédelmi beállításokra és megfontolják, mit tesznek közzé, de még így is akadnak felelőtlen emberek. Nézzünk meg néhány példát, mit lehet kezdeni a nyilvánosságra hozott adatainkkal, milyen hatása lehet egy rosszul készült képnek.

A hackerek mindent megtesznek annak érdekében, hogy programkódot írjanak az okostelefonok feletti ellenőrzés megvalósítása érdekében, valamint különféle trükkökkel próbálják manipulálni az embereket. Tevékenységük olyan jól álcázott, hogy egy hétköznapi ember számára ezekből a cselekvésekből semmi sem tűnik fel. Amikor kiposztolunk valamit az oldalunkra vagy képet töltünk fel, azt akármelyik ismerősünk véletlenül vagy akár szándékosan nyilvánossá teheti. Innentől kezdve már mindenki számára elérhetővé válik.

Érdemes az adatvédelmi beállításokat úgy beállítani, hogy megosztott tartalmainkat csak ismerőseink, barátaink láthassák.

Sokan nem is gondolják, hogy egy megosztott képünkkel akár egy jól fizető állástól foszthatnak meg minket. Ugyanis már egyre több cégvezető nézi meg az álláshirdetésre jelentkezők Facebook profilját azzal a szándékkal, hogy kiszűrje esetleges szélsőséges tulajdonságaikat, cselekvésüket. Egy másik eset is egy teljesen hétköznapi példa. Egy barátunktól, közeli ismerősünktől akár egy rokontól kapott üzenet is rejthet veszélyeket. Ugyanis kaphatunk egy videót, melyről azt hisszük, hogy érdekes lehet számunkra, azonban az árnyoldalával már nem vagyunk tisztában. Az ilyen hivatkozások egy új szoftver letöltésére vagy lejátszónk frissítésére ösztönöznek minket, azonban, ha elindítjuk ennek letöltését, máris megfertőzzük gépünket. Ezzel sajnos itt még nincs vége. Innentől kezdve adatlapunk folyamatosan üzenetet küld ismerőseinknek ezzel a videóval, így a vírust terjesztjük is. Ezáltal a hackerek ezernyi gépet vonnak ellenőrzésük alá.[31] Sajnos ezek még mindig nem tartoznak a legveszélyesebb dolgok közzé. Egy megdöbbentő amerikai esettanulmány keretén belül kívánjuk bemutatni, hogy milyen további veszélyek várhatnak a gyanútlan személyekre: Alicia Kozakiewicz 13 évesen vált egy internetes ragadozó áldozatává. A 38 éves, perverz férfi markaiból négy nap elteltével szabadult az FBI segítségével. Alicia azóta idejének nagy részében iskolákban, fórumokon beszél megpróbáltatásairól és harcol azért, hogy a felnőttek (szülők, politikusok stb.) tegyenek meg mindent a gyermekek védelme érdekében. Alicia egy összetartó család tagjaként nevelkedett. Későbbi elrablójával egy internetes chat-fórumon ismerkedett meg. Annak ellenére, hogy félénk kislány volt, mégis beleegyezett, hogy találkozik az idegen férfival. Így 2002. január 1-ének éjszakáján kisétált házuk ajtaján és beszállt a férfi autójába, aki elvitte a lányt saját otthonába. A kislányra 4 nap földi pokol várt: a férfi, aki elrabolta verte, láncokkal megkötözte, árammal sokkolta, karjánál fogva felakasztotta és úgy ütötte, szexuálisan kizsákmányolta. A kislány életét az mentette meg, hogy elrablója barátainak hencegve, képeket töltött fel az internetre a kínzásokról, sőt online, webkamerával is közvetítette ezeket. A férfi egyik barátja, aki látta az újságokban a kislány fényképét, megijedt és bejelentést tett a rendőrségnek, így találta meg Alicia-t az FBI a férfi hálószobájában megkötözve, a nyakánál fogva a földhöz láncolva.[32] Ez az esettanulmány jól mutatja, hogy nem csak a felnőttek, de a

[31]Közösségi oldalak veszélyei - Csak óvatosan a megosztásokkal! http://pcworld.hu/kozosseg/kozossegi-oldalak-veszelyei-csak-ovatosan-a-megosztasokkal-152928.html (letöltés ideje: 2016.10.07.)

[32]A közösségi oldalak veszélyei. http://pecs.hit.hu/a-kozossegi-oldalak-veszelyei/ (letöltés ideje: 2016.10.07.)

fiatalabb generáció is hatalmas veszélynek van kitéve. Azt hinnénk, hogy csak a közösségi oldalak rejtenek veszélyeket. A közösségi médiának számos további veszélyforrása lehet.

A közösségi média számtalan lehetőséget kínál a kapcsolattartásra, a kommunikációra és a marketingre, hatása az élet minden területén érződik. Az internet és az erre épülő közösségi média állandó és azonnali információforrás. A közösségi média számtalan új lehetőséget teremt, ugyanakkor számtalan új kihívás elé is állítja a szervezeteket, amely rengeteg kockázatot hordoz magában. Az érintett felek ma már egyre inkább hajlanak arra, hogy saját kezükbe vegyék a kezdeményezést, és maguk járjanak utána az információknak. Mára az elsődleges információforrás a közösségi média lett. A közösségi média nem egyszerűen csak gyorsabb információs csatorna, hanem a legújabb és legmeghatározóbb médium, ami átírja a hagyományos média és a szervezetek szerepét, megváltoztatja a befolyásukat, miközben hatalommal ruházza fel az új aktivistákat, a közösségi média fogyasztókat – az otthoni monitor előtt ülő hétköznapi polgárokat. A közösségi médiában megjelent információnak sok különböző formája létezik, beleértve a fórumhozzászólásokat, a blogbejegyzéseket, kép-, videó-, és hanganyagokat és még sorolhatnánk. A közösségi média technológiák közé tartoznak többek között a blogok, a videóblogok, a kép- és videómegosztó oldalak, üzenőfalak, e-mail üzenetek, üzenetküldő szolgáltatások és programok, és a zenemegosztás is. A legújabb trend, hogy ezeket a technológiákat egyetlen felületbe integrálják, mint például a Ning vagy a Network.hu oldalak.[33]

A megalapozatlan pletykák, a hírek, az árfolyamok, az új kutatások eredményei mind azonnal felkerülnek az üzenőfalra, és elérhetővé vállnak a nyilvánosság számára. Ma már kevésnek bizonyul, ha a sajtóanyag egyszerűen csak felkerül a honlapra, a siker érdekében a webes tartalmak minél szélesebb eszközrendszerét kell alkalmazni: blog, podcast, RSS, videó, hasznos forrásokra mutató linkek. A közösségi média tökéletes platform a társadalmi mozgalmak szervezésére, vélemények megfogalmazására, érdekcsoportok kialakítására, együttműködésére. A társadalmi mozgalmak eszköztárában ma már a webcast, a Facebook profil, a vírusvideók, virtuális konferencia vagy több ezer olvasóval rendelkező blog szerepel. S ezek gyorsabban viszik előre ügyüket, mint bármi más médium.

A közösségi média az egyenlőség híve – az interneten minden információ és minden ember egyenlő. Senkinek nem kérdőjelezhető meg a hitelessége, és ilyen módon mindenki szakértő, a források pedig végtelenek. Mindenkiből lehet hiteles forrás anélkül, hogy a

[33]A közösségi média. https://hu.wikipedia.org/wiki/K%C3%B6z%C3%B6ss%C3%A9gi_m%C3%A9dia (letöltés ideje: 2016.10.09.)

felhasználónevén vagy nickjén kívül bármit is tudni lehetne róla. Az anonim felhasználók pedig fontos kockázati tényezők, hiszen bárki elindíthat egy pletykát úgy, hogy közben eltitkolja személyazonosságát. A felhasználók által megadott adatok olyanok kezébe kerülhetnek, akiknek ehhez nincs hozzáférési jogosultságuk. Az illetéktelen felhasználás pedig innen már csak egy lépés. A kiadott adatok felett nincs kontrollja sem a felhasználónak, és nem megfelelő védelmi rendszer esetén még az oldalak üzemeltetőinek sem. Jogosan merül fel a kérdés: ki a hibás, ha nem publikus megosztásra szánt adatok kerülnek nyilvánosságra, valamint ki a felelős azok illetéktelen használatáért?

III.2. A közösségi média és a közösségi oldalak összehasonlítása

Nehéz pontosan meghatározni a közösségi média fogalmát és elemeinek körét. Annyit azonban kijelenthetünk, hogy a közösségi média és a közösségi oldalak nem egymás ellentétei. A közösségi médiák összefoglaló elnevezése alá tartoznak a közösségi oldalak, mint például a Facebook és a Twitter. A közösségi oldalak csupán egyetlen pillérét képezik a közösségi médiáknak. Nem található egységes megfogalmazás a közösségi médiára. Szinte minden definíció más irányból közelíti meg a témát. A közösségi média egy rendkívül szerteágazó és dinamikusan fejlődő online tér. A közösségi média[34] kifejezés alatt azokra az online platformokra és eszközökre gondolunk, amelyek lehetővé teszik, hogy az emberek véleményüket megosszák másokkal. A közösségi média megjelenési formája változatos lehet. A hangsúly arra helyeződik, hogy ezeket a tartalmakat elsősorban emberek és nem szervezetek terjesztik. Következő lényeges jellemzőjük, hogy ezek a tartalmak ingyenesen, vagy minimális költséggel érhetők el.[35] Mindazon felület, ahol egy közösség tagjai kapcsolatot tudnak teremteni és tartani nem csak egymással, egymás közt, hanem a hálózat természetéből adódóan újabb tagok meghívásával, illetve csatlakozásával addig ismeretlen személyekkel, csoportokkal, vállalkozásokkal is. Általánosságban kimondhatjuk, hogy a közösségi média olyan internetalapú alkalmazásokból áll, amelyek a web 2.0-ra, mint technikai felületre építenek, és felhasználók által létrehozott tartalmak cseréjét teszik lehetővé. Ezek olyan új online információforrások, amelyeket a felhasználók hoznak létre,

[34] A közösségi média, mint online stratégiai eszköz. http://unipub.lib.uni-corvinus.hu/886/1/MKE_GM_mok2012.pdf (letöltés ideje: 2016.10.12)

[35] A közösségi média fogalma. http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e4_digitalis_marketing_scorm/a_kozossegi_media_fogalma_w0NOGk1cQOiR2A0n.html (letöltés ideje: 2016.10.12)

kezdeményeznek, áramoltatnak és formálnak. Ezen információk nagymennyiségű adatot képeznek, melyek szinte percre pontosak, azonban ennek áraként gyakran kétes információt képeznek, melyek ellenőrizetlen forrásokból származnak.

A közösségi oldalak olyan portálok, melyeken a felhasználók regisztráció után saját profilt hozhatnak létre, majd más felhasználókkal léphetnek kapcsolatba. Ezek az oldalak alkalmasak új és már meglévő kapcsolatok teremtésére és fenntartására. A résztvevők képesek személyes fényképeket, videókat, hangfájlokat vagy blogokat is létrehozni vagy megosztani mások által feltöltött híreket, tehát szinte bármilyen típusú információ közzétételére alkalmasak.

III.2.1. A közösségi média pillérei

- A blogok egy speciális típusai a mikroblogok (pl. Twitter), amelyek leginkább átmenetnek tekinthetők a blogok és a közösségi oldalak között, a felhasználók pedig képesek felületükön rövid üzeneteket küldeni és olvasni.
- A kollaboratív projektek (pl. Wikipedia) során a tartalmak előállítása több felhasználó által közösen történik és időben akár párhuzamosan is történhet, illetve itt a társszerzők egyben végfelhasználók is.
- A tartalommegosztók olyan közösségként írhatóak le, ahol a felhasználók megosztanak különböző médiatartalmakat.
- Megkülönböztethetünk videómegosztó (pl. YouTube) és
- képmegosztó (pl. Flickr) oldalakat.
- A közösségi híreket tartalmazó weboldalak lehetővé teszik bármilyen információ megosztását az internet bármelyik részéről.
- A virtuális világok olyan háromdimenziós környezetet biztosítanak, ahol a felhasználók személyre szabottan jelenhetnek meg virtuálisan, és a valós élethez hasonlóan kerülhetnek egymással kapcsolatba.

Megállapítható, hogy a közösségi oldalak jobban fókuszálnak a párbeszédekre, elsődleges szempontjuk a kapcsolatteremtés, építés, fenntartás. Közösségi oldalnak minősül minden olyan internetes felület, ahol kialakulhat valamilyen kommunikáció, interakció a felhasználók között. Ide sorolhatók a web áruházak, aukciós oldalak, fórumok, etc. minden olyan oldal, ahol van hozzászólási lehetőség, illetve valamilyen közösségi funkció.[36]

[36] Közösségi média. http://mediapedia.hu/kozossegi-media (letöltés ideje: 2016.10.11)

III.2.2. A közösségi média megjelenése

Magyarországon a közösségi média első érdemi állomásának 1996-ot tekinthetjük, amikor a Kulturális és Kommunikációs Központ Alapítvány Internet Műhelyében a látogatók, előzetes regisztráció után ingyenesen böngészhettek az interneten. Ugyan ebben az évben jelent meg a Heuréka, az első hazai keresőszolgáltatás. Majd az Internetto kezdeményezésével különböző közösségi szolgáltatások, fórumok, e-mail. Elsőként az elektronikus levelek kezelésére a nemzetközi Hotmail, majd 1997-ben a magyar fejlesztésű Freemail nyújtott ingyenes levelezésre lehetőséget. 1998-ban jelent meg a mai blogok elődje, a Freeweb. Itt a résztvevők személyes honlapokat hozhattak létre, ahol a látogatókat a megosztott szöveges tartalom mellett vendégkönyv várta, amelyben hozzá tudtak szólni a szerkesztők által megosztott tartalmakhoz. 1999-ben megalakult a Startlap, az első magyar internetes linkgyűjtemény. Ezzel párhuzamosan az internetezők száma is jelentősen megugrott. 2001-től indultak el az első igazi hazai blogok, amelyek ma már milliós nagyságú olvasóközönséggel bírnak.[37] A XXI. században a közösségi médiák használata mindennaposnak tekinthető. A világ teljes lakosságának több mint 49%-a használ napi rendszerességgel internetet, ez csaknem 3,6 milliárd fő. Ennek 76%-a használ valamilyen közösségi médiát (közösségi hálózathoz csatlakozik, blogot ír vagy olvas). Kiugróan magas adatot mutat a világ legnagyobb közösségi oldala, a Facebook, amely 1,1 milliárd regisztrált felhasználót számlál az Internet World Stats adatai[38] szerint. A legnépszerűbb mikroblog szolgáltatón, a Twitteren 310 millió aktív felhasználó van jelen, akik legalább naponta egy alkalommal bejelentkeznek az oldalra. Ezzel egy időben a YouTube video megosztó oldalon több, mint 24 órányi videó tartalmat töltenek fel minden percben.[39]

Megállapíthatjuk, hogy az internetfelhasználók száma egyre bővül, ezzel egy időben és egyenesen arányosan a közösségi médiákat látogatók, formálók száma is rohamosan növekszik. A közösségi média jelensége tagadhatatlanul hatással van mindennapi életünkre, hiszen ezen portálok a legfőbb információforrásaink. Következtetésként levonható, hogy a

---

[37]A közösségi média előzményei. http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e4_digitalis_marketing_scorm/a_kozossegi_media_elozmenyei_9kDI64BT8N14gbJn.html (letöltés ideje: 2016.10.12)

[38]Internet World Stats. Internet Users in Europe November 2015. http://www.internetworldstats.com/stats4.htm (letöltés ideje: 2016.10.12)

[39]Social Media Websites Stats. http://www.internetworldstats.com/social.htm#world (letöltés ideje: 2016.10.12)

közösségi oldalak a személyes kapcsolatok mindennapjainak szerves részét képezik. A közösségi médiák a hagyományos médiákkal szemben egyre jelentősebb szerepet töltenek be.[40] Naprakész, könnyen elérhető nagymennyiségű adattal szolgálnak, azonban ennek árnyoldalát képezik a megkérdőjelezhető források, szakszerűtlen portálok, téves információk.

IV. A rendőrség és a közösségi tájékoztatás szerepének kérdőíves kutatása

A tanulmány hipotéziseket fogalmazott meg a közösségi oldalak és a rendőrség kapcsolatrendszerére vonatkozóan. A közösségi oldalak szempontrendszereit vizsgálva a közösségi tájékoztatás viszonyrendszerének egyes elemei kerültek vizsgálat alá, kiemelten a rendőrség szerepvállalásának szempontjából.

A kérdésekre adott válaszok esetében az anonimitás biztosítva volt. A kérdőív tíz kérdést tartalmazott, amelyet online felületen keresztül lehetett elérni és terjeszteni. Az online kutatás 2016.08.28-tól, 2016. október 5-ig került végrehajtásra. A kérdőívet 111 személy töltötte ki. Férfi válaszadók száma: 47. Női válaszadók száma: 64. Életkori átlag: 24,1 év.

[40]Social Media Usage: 2005-2015. http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ (letöltés ideje: 2016.10.12)

Az első kérdés a közösségi oldalak használatára irányult. A válaszadók 93,7 %-a napi rendszerességgel használja a közösségi oldalakat. A kérdésekre adott válaszokból megállapítható, hogy a közösségi oldalak társadalmi jelentősége meghatározó tényező, ezért a számos vonatkozás mellett, rendvédelmi oldalról is szükséges vizsgálni, mind a megjelentetett tartalom, mind a felhasználók viktimológiai és bűnelkövetési magatartásának szempontjából.

A második kérdés egy személyesebb megközelítésre vonatkozó kérdést fogalmazott meg. A kérdés olyan egyéni kompetenciák közzétételére vonatkozott, mind a képek és a tartózkodási hely megadásának veszélye. Ebben az esetben a válaszadók döntő többsége ritkábban igaz, de mégis azáltal veszélynek teszi ki magát, hogy releváns egyéni információkat posztol ki, vagy ad meg a közösségi oldalakon.

A harmadik kérdés a második kérdés folytatása. A közösségi oldalakon már közzétett személyes és egyben releváns egyéni információk közzétételének az elérhetőségére kérdezett rá. Megállapítható, hogy a válaszadók meghatározott része körültekintően jár el az információk közzététele ügyében. Mindazonáltal megfigyelhető, hogy a válaszadók 16%-a mindenki számára elérhetővé tesz önmagáról fontos információkat és tartózkodási helyeket. Ezeknek az információknak a közzététele rendészeti és bűnmegelőzési szempontból aggályos, hiszen a bűnelkövető személyek nagyon könnyen és naprakészen tudnak tájékozódni az adott személy aktuális hollétéről, így könnyebben tudnak realizálni egy bűncselekményt akár vele, akár a tulajdonával szemben.

A negyedik kérdés a közösségi oldalak veszélyeinek az ismereteire kérdezett rá. A válaszadók több, mint 80%-a nyilatkozott úgy, hogy tisztában van a közösségi oldalak veszélyeivel, azonban megfigyelhető, hogy 12,7 % nem foglalkozik ezzel a problémával. A rendőrség szerepe ebben az esetben is fontos lehet, mivel a bűnmegelőzés területén a közösségi oldalakban rejlő jogsértések veszélyeire is fel kell hívni a felhasználók figyelmét, hogy ne váljanak áldozatokká.

Az ötödik kérdés az információszerzés egyes lehetőségeinek a használatával foglalkozik. A válaszadók 55,9 %-a az internetes portálokról, míg közel 20%-a a közösségi oldalakról szerzi be az aktuális napi híreket és információkat. A tanulmányban részletesen bemutatásra került esettanulmányokon keresztül a valótlan információk, vagy valós információk elferdítésének a veszélye.

A hatodik kérdés a rendőrség online jelenlétére, elsősorban a közösségi oldalakon való megjelenési formákra helyezte a hangsúlyt. A válaszadók 61%-a nincs tisztában azzal, hogy a rendőrség van-e, és ha igen, akkor milyen formában van jelen a közösségi oldalakon. Ennek az erősítése érdekében a tanulmányban kifejtésre került, hogy milyen releváns nemzetközi példák állnak a magyar hatóságok elé követendő példaként. A tanulmányban bemutatásra került a közösségi oldalakon történő rendőrhatósági jelenlétnek a közbiztonsági és bűnmegelőzési hatékonysága is.

A hetedik kérdés a rendőrség hatékonyságára volt kíváncsi. A válaszadók 53.2%-a elismeri a rendőrség munkáját, azonban megfigyelhető, hogy az elismertség mellett 11.7% az egyéni szubjektív biztonságérzet tekintetében meghatározónak érzi a rendőrség hatékonyságát. Továbbra is törekedni kell arra, hogy a rendőrség erősítse a lakosság biztonságérzetét, mivel megfigyelhető, hogy közel 30%-a a válaszadóknak nem érzi elfogadhatónak a rendőrség munkáját.

A nyolcadik kérdés a válaszadók és a rendőrség intézkedés központúságát helyezte előtérbe, megvizsgálva ezzel azt a hipotézist, hogy a válaszadók közvetlenül is szembesültek-e már a rendőri szervek munkájával, vagy csak más forrásokból tájékozódtak róla. Megállapítható, hogy a válaszadók 78.4%-a még nem volt rendőri intézkedés alá vonva.

A kilencedik kérdés esetében a válaszadók 93.7%-a mondta azt, hogy szükség van arra, hogy a rendőrség a közösségi oldalakon nyújtson tájékoztatást a lakosságnak a kialakult veszélyhelyzetekről. Azonban ennek a közvetlen tájékoztatásnak is van veszélye. Nem csak a segítséget igénylő állampolgárok, hanem a bűn- vagy terrorcselekményeket elkövetni szándékozó személyek is közvetlen módon juthatnak információhoz, közvetlenül a rendőri szervektől.

A tizedik kérdés szintén a rendőrség közösségi oldalakon betöltendő szerepét helyezte előtérbe. A válaszadók 60,4%-a nyilatkozott úgy, hogy erősödne az egyéni szubjektív biztonságérzete, amennyiben a rendőrség jelen lenne a közösségi oldalakon.

A kérdőíves kutatásból megállapítható, hogy a fiatal generáció (35 év alattiak), akik aktívan részt vesznek a közösségi oldalak nyújtotta felületek mindennapos életében, igénylik a rendőrség szerepvállalását a biztonságuk erősítése érdekében. A rendőrségnek nem szabad figyelmen kívül hagynia ezeket a kéréseket, hiszen a bűnelkövetési módszerek és magatartási metódusok egy jelentős része áttevődött a közösségi oldalakra. A bűnmegelőzés és a bűnfelderítés tekintetében meghatározó a jövőre nézve a rendőrség szerepvállalása.

Következtetés

A kiberbiztonság jelenlegi kihívásai úgy Magyarországon, mint Európában jelentős kockázati tényezőnek minősülnek. Ezek a veszélyek nagymértékben meghatározzák a rendvédelmi szervek és a nemzetbiztonsági szolgálatok stratégiai koncepcióját. Számos olyan *új típusú rendészeti kihívás* került be a rendészeti szervek feladatrendszerébe, mint az illegális migráció kezelése, a terrorcselekmények megelőzése és megakadályozása, valamint a kiberbűnözés.

A kiberbűnözésnek számos fajtáját különböztethetjük meg. Ezek a technológiai fegyverkezés, a hálózatok és személyközi kapcsolatok problémaköre, a kritikus információs infrastruktúrák, vagy a közösségi oldalak és a közösségi média rendvédelmi vonatkozásainak kihívásai.

Jelen tanulmány a közösségi oldalak és a közösségi média szempontjából, valamint ezen online tartalmak felhasználói szemszögéből fogalmazott meg hipotéziseket és releváns kérdéseket. Ezek a megfogalmazott kérdések elsősorban a rendőrség szerepvállalásával, jelenlétével, valamint bűnmegelőzési és bűnfelderítési hatékonyságával kapcsolatban kívántak tudományos szempontból használható válaszokat kapni. A tanulmány erőssége a kérdőíves kutatás, amely a közösségi oldalak felhasználói oldaláról vizsgálja a közösségi média egyes biztonságpolitikai kérdéseit. A válaszok elemzéséből jól kirajzolódik az az igény, hogy a rendőrség közösségi oldalakon történő szerepvállalásának igénye valós és időszerű. A tanulmányban röviden bemutatásra és elemzésre kerültek azok az európai és tengerentúli bűn- és terrorcselekmények, ahol a vizsgált országok rendvédelmi szervei a közösségi média segítségét igénybe véve tájékoztatták a lakosságot a kialakult veszélyhelyzetről.

Bizonyításra került, hogy a rendvédelmi szervek (kiemelten a rendőrség) bűnmegelőzési és bűnfelderítési, valamint terrorcselekmények megelőzése érdekében kifejtett munkamódszerei nagyobb hatékonyságot érnek el az eredményesség tekintetében, ha igénybe veszik a közösségi oldalak, valamint a közösségi média eszközrendszerét és a felhasználók segítségét. Mindazonáltal figyelemmel kell lenni azokra a tartalmakra és személyekre, akik szándékosan kívánják felhasználni a rendőrség online megosztott információit. További kutatások szükségesek e problémák feltárása és megoldására.

Felhasznált irodalom

- A Facebook 4 évig nem védte adatainkat. http://www.nyest.hu/hirek/a-facebook-4-evig-nem-vedte-adatainkat (letöltés ideje: 2016.10.04.)
- A gyerekek online biztonsága. http://unicef.hu/a-gyerekek-online-biztonsaga/ (letöltés ideje: 2016.10.12)
- A közösségi hálózatok és a közösségi rendőrség kapcsolata. (Mi keresni valója van a rendőrségnek Facebookon?) http://epa.oszk.hu/02500/02538/00008/pdf/EPA02538_nemzetbiztonsagi_szemle_2015_01_026-051.pdf
- A közösségi hálózatok története. http://szocial.blogspot.hu/2008/05/kzssgi-hlzatok-trtnete.html, (letöltés ideje: 2016.10.03.)
- A közösségi média előzményei. http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e4_digitalis_marketing_scorm/a_kozossegi_media_elozmenyei_9kDI64BT8N14gbJn.html (letöltés ideje: 2016.10.12)
- A közösségi média fogalma. http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e4_digitalis_marketing_scorm/a_kozossegi_media_fogalma_w0NOGk1cQOiR2A0n.html (letöltés ideje: 2016.10.12)
- A közösségi média szerepe válsághelyzetekben. http://mtmi.hu/cikk/823/A_kozossegi_media_szerepe_valsaghelyzetekben. (letöltés ideje: 2016.10.02.)
- A közösségi média, mint online stratégiai eszköz. http://unipub.lib.uni-corvinus.hu/886/1/MKE_GM_mok2012.pdf (letöltés ideje: 2016.10.12)
- A közösségi média. https://hu.wikipedia.org/wiki/K%C3%B6z%C3%B6ss%C3%A9gi_m%C3%A9dia (letöltés ideje: 2016.10.09.)
- A közösségi oldalak veszélyei. http://pecs.hit.hu/a-kozossegi-oldalak-veszelyei/ (letöltés ideje: 2016.10.07.)
- A közösségi oldalak: A közösségi oldalak története. http://felsofokon.hu/bolcseszettudomany/a-kozossegi-oldalalak-a-kozossegi-oldalak-tortenete/ (letöltés ideje: 2016.10.03.)
- A Twitter. https://hu.wikipedia.org/wiki/Twitter (letöltés ideje:2016.10.04.)

- Ashitha Nagesh: Nice attack: Man wrongly identified as being behind Bastille Day terror. Metro UK. 2015.07.15.
- Az ma a menő fiatal, akinek sok a lájkja a közösségi médiában. http://24.hu/media/2016/08/03/az-ma-a-meno-fiatal-akinek-sok-a-lajkja-a-kozossegi-mediaban/ (letöltés ideje:2016.10.10)
- Carlson, Nicholas: At Last — The Full Story Of How Facebook Was Founded. Business Insider (online, 2010. március 5.)
- Danah M. Boyd és Nicole B. Ellison: Network Sites: Definition, History, and Scholarship, Journaol of Computer-Mediated Communication. 2007/11. 20-22.
- Ezért halott a Facebook a fiatalok számára. http://bitport.hu/ezert-halott-a-facebook-a-fiatalok-szamara (letöltés ideje: 2016.10.11)
- Facebook history. https://hu.wikipedia.org/wiki/Facebook. (letöltés ideje: 2016.10.04.)
- Facebookon toboroz határvadászokat a rendőrség. http://24.hu/kozelet/2016/08/24/facebookon-toboroz-hatarvadaszokat-a-rendorseg/ (letöltés ideje: 2016.10.12)
- Fecebook live streaming of us police shooting of a black man leads. http://www.telegraph.co.uk/technology/2016/07/07/facebook-live-streaming-of-us-police-shooting-of-black-man-leads/ (letöltés ideje: 2016.10.12)
- Google person finder. https://google.org/personfinder/global/home.html (letöltés ideje: 2016.10.11)
- Határvadász-képzés: Jelentkezz még ma! https://www.facebook.com/hatarvadaszkepzes/?fref=ts (letöltés ideje: 2016.10.12)
- Instagram. https://hu.wikipedia.org/wiki/Instagram. (letöltés ideje: 2016.10.05.)
- Internet World Stats. Internet Users in Europe November 2015. http://www.internetworldstats.com/stats4.htm (letöltés ideje: 2016.10.12)
- Közösségi média, mint remény katasztrófa idején http://mtmi.hu/cikk/740/Kozossegi_media_mint_remeny_katasztrofa_idejen (letöltés ideje: 2016.10.12)
- Közösségi oldalak veszélyei - Csak óvatosan a megosztásokkal! http://pcworld.hu/kozosseg/kozossegi-oldalak-veszelyei-csak-ovatosan-a-megosztasokkal-152928.html (letöltés ideje: 2016.10.07.)
- Közösségi oldalak veszélyeiről. http://www.police.hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag/kozossegi-oldalak-veszelyeirol (letöltés ideje: 2016.10.12)

- Levy, Steven: Twitter: Is Brevity The Next Big Thing? Newsweek. 2011.02.11. 15-16.
- Mit művelnek a rendőrök a facebookon http://index.hu/tech/2010/03/30/mit_muvelnek_a_rendorok_a_facebookon/ (letöltés ideje: 2016.10.12)
- Schwartz, Bari: Hot or Not? Website Briefly Judges Looks. Harvard Crimson. (2009.)
- Social Media Usage: 2005-2015. http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ (letöltés ideje: 2016.10.12)
- Social Media Website Stats. http://www.internetworldstats.com/social.htm#world (Letöltés ideje: 2016.10.12)
- Social Media Websites Stats. http://www.internetworldstats.com/social.htm#world (letöltés ideje: 2016.10.12)
- Top 15 Most Popular Social Networking Sites. http://www.ebizmba.com/articles/social-networking-websites. (letöltés ideje: 2016.10. 08.)
- Tsukayama, Hayley: Instagram adding ads boosts Facebook's outlook, analysts say. The Washington Post. 2014.01.24. 25-26.

Dr. Nagy Terézia

A szélsőséges iszlamizmus térnyerése és a sebezhetőség hálózati szempontból

Téma: Kibertér bűnügyi és nemzetbiztonsági kihívásai

2016

Tartalomjegyzék

1 Bevezetés. A kibertér és a hálózat szerepe a nemzetközi terrorizmusban

Miközben a nemzetközi terrorizmus láthatósága, mindennapi percepciója folyamatosan erősödött az elmúlt években, a terrorizmus sajátságainál fogva számos dolog viszonylag rejtve marad a belső működésről, a hálózati tevékenyégéről, s részben a kibertér is egy olyan hely lett a nemzetközi terrorizmus számára, amelyben elrejtheti tevékenységét.

A kibertér biztonsági kérdései e témában nem érthetők meg a szélsőségre nyitott, iszlamista közösségek és közegek hálózati értelmezése nélkül. Ebbe beletartozik a sok kapcsolattal rendelkező központi szereplők és az izolált aktorok szerepeinek értelmezése is, a kapcsolatok hálózattudományi megközelítése és értelmezése. Azonban a szélsőséges iszlamizmus térnyerése és a hálózatok felszámolására irányuló tevékenységek komplex megközelítése sem ad mindenre választ. Tanulmányomban arra törekszem, hogy a hálózati sajátságokat, a résztvevő aktorok szerepein keresztül a szélsőséges eszmék terjedésére, a radikalizálódás folyamataira választ találjak és kínáljak. Elméleti megfontolásaimat hálózattudományi módszerrel kísérem – kisebb utalásokkal a területen alkalmazható big data és adatbányász módszerekre –, s célom az, hogy a közel-keleti, dél-ázsiai, maghrebi és szubszaharai diaszpórák és a wahabi muszlim közösségben végzett terepmunkám eredményeit a kapcsolatháló-elemzéssel kiegészítve implementáljam.

A tanulmányomban kitérek a hálózattudomány gyakorlati alkalmazhatóságára is, annak érdekében, hogy a tanulmányon keresztül végigvezetett hálózati sajátságok és empirikus eredmények összegzése hozzájáruljon a nemzetközi terrorizmus hálózatai elleni küzdelemhez.

2 A nemzetközi iszlám terrorizmus és a hálózati sajátságok

2.1 A szélsőséges eszmék terjedése – távolságok és közeliségek

A szélsőséges eszmék terjedése egy átlagos hálózatban több ponton akadályba ütközhet: vannak olyan szereplők, akik rezisztensek a szélsőséges megközelítésekre, a fundamentalista iszlámra, emellett számosan rezisztensek a kard dzsihádjára, ismét mások pedig a hálózat más aktorait tekintik vonatkoztatási pontnak. Az első kettő konzisztens együtt mozgását könnyen értelmezhetjük, ha azt tekintjük, hogy a fundamentalista iszlámnak részhalmazai a szélsőséges iszlamizmus és a dzsihád különböző megközelítései, s ezen belül helyezkedik el az a dzsihád halmaza is, amely erőszakkal is megvédi a vélt vagy valós támadásoktól az iszlámot és a muszlimokat, valamint aktív szerepet vállal a „hitetlenek" elleni küzdelemben, a félelem és a hatalom játszmáival, fegyverrel is hódít (vö. Elden, 2007).

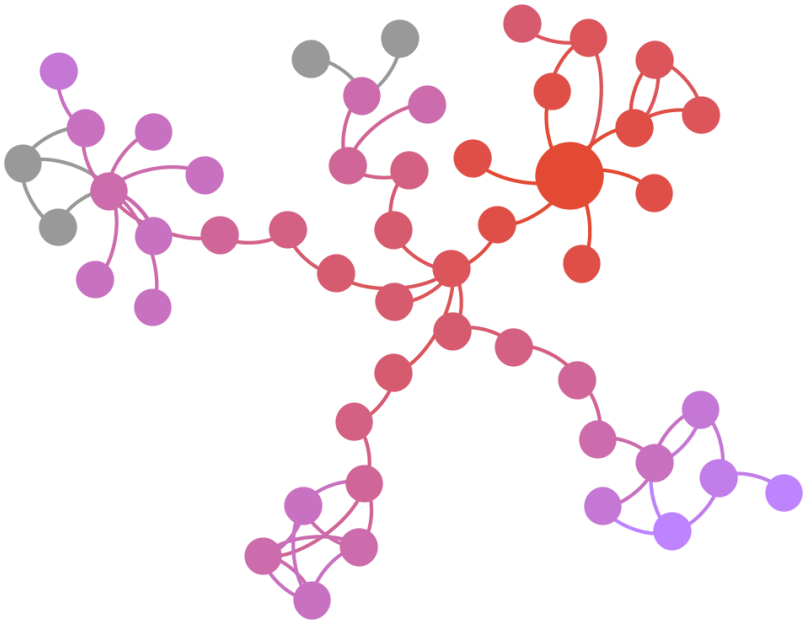
Az iszlám fundamentalizmus terjedésének feltételeit e tanulmányban hálózati megközelítésben kívánom értelmezni, így a továbbiakban a terjedés sajátságait e vonatkozásban vizsgálom.

Az iszlám fundamentalizmus terjedését a fogadópontok és a térítést, toborzást végzők hálózati aktivitása határozza meg – mind a valós, mind pedig az online térben. Miközben ezen aktivitások rejtettek, s éppen ezért erős és ellenálló a hálózatuk (vö. Krebs, 2002), van arra lehetőségünk, hogy az érkezési pontokat empirikusan is megvizsgáljuk. Az érkezési pontok megjelenését két analógiával ragadhatjuk meg:

1) a biológia rizóma fogalmával – a föld alatt korlátlan növekedésű gyökér rügyeiből a föld felett fejlődik ki a növény – az online világban, különösen a titkosított csatornákon keresztül történik a hálózatosítás, míg korábban elsősorban valós térben megvalósuló interperszonális kapcsolatokon keresztül.
2) a Lévy-repülés analógiájával – azaz a szélsőséges eszmék terjedése olyan szuperdiffúzióként írható le, melyben nagyobb távolságok megtétele után kisebb térben terjednek az eszmék és alakulnak a hálózatok, s ez a mintázat ismétlődhet.

A Lévy-repülés analógiája alkalmas arra, hogy megértsük a térben nagy távolságot bejáró szélsőséges eszmék terjedésének mintázatait (vö. Chaturapruek és mtsai, 2013). Az extrém iszlamizmus a dél-ázsiai vagy közel-keleti tanítóktól – általában brit vagy skandináv érkezési pontokon keresztül – érkezik Nyugat-Európába, ott, elsősorban személyes kapcsolatokon keresztül lokálisan terjed, illetve akadályokba ütközik, s ismét csak interperszonális kapcsolatokon keresztül terjed nagyobb távolságokra. Így érkezett és érkezik

Magyarországra is, ahol viszonylag szűk iszlám közösségen belül korlátozott térben tud terjedni az extremizmus. A nagy földrajzi távolságot bejárva kis területen lokalizálódik, majd tovább mozdul, ismét nagy távolságot megtéve. Ennek oka részben az, hogy (1) adott helyi szinten olyan akadályokba ütközik, amelyek gátat szabnak a terjedésnek – s így a potenciális résztvevők kiválasztásában, a toborzásban kénytelenek helyszínt váltani. De oka ennek az is, hogy az (2) elfogadottság hiánya és az (3) illegalitás mozgásban tartja a toborzókat, s szintén oka lehet az is, hogy (4) a toborzók nagyobb merítésből, az európai iszlám közösségekből és megtérőkből kell, hogy szelektáljanak ahhoz, hogy sikeres legyen a kiválasztás.



1. ábra. Információs elem terjedése. Saját szerkesztés

Az ábrán látható, hogy a nagy távolságok, melyek egy-egy kapcsolaton keresztül vagy személyes elmozduláson keresztül valósulnak meg, csillag alakú lokális terjedéssel és a csillag ágain láncok kialakulásával folytatódik a terjedés (1. ábra). Ez jelentősen különbözik a megközelítést megalapozó epidemológiai kutatásoktól, hiszen itt a terjedésnek erősen ellenálló rezisztens személyek jelenlétével is kell számolnunk, így bizalmas kapcsolatokon keresztül terjedhet.

A kibertérben a terjedés mechanizmusa hasonló, azonban kevesebb erőfeszítéssel, nagyobb attraktivitással és rövidebb idő alatt nagyobb hatékonysággal tudnak toborozni, új

kapcsolatokat építeni, illetve információt átadni. A hatékonyság megegyezik a Poisson-eloszlással, minthogy a hálózatok növekedése a kibertérben dinamikus, ámde a dinamikus fejlődés egy robusztus, nagy geodézikus távolságú, klaszterezett hálózatot hoz létre, s mivel folyamatosan akadályokba ütközik (amely szintén preferenciák mentén értelmezhető akadályokat jelent), a fejlődésnek és terjedésnek határa van. Ráadásul az online terek és felhasználóik attribútumait tekintve, s figyelembe véve más külső tényezőket (biztonság, támadhatóság/sebezhetőség), a hálózatnak elméletileg nagyon gyorsan kell kifejlődnie, intenzív kapcsolatokat ápolnia, mert az akadályokként azonosított preferenciák irányából ellenirányú folyamatok indulhatnak meg.

2.2 A kapcsolati mintázatok és az iszlamizmus fogadóterei

Az akadályok, melyek a szélsőséges eszmék terjedésének gátat szabnak, preferenciákat jelölnek, csakúgy, mint azok a fogadóterek, érkezési pontok, amelyek az iszlamizmust, a szélsőséges eszméket befogadják. Ezen utóbbi preferenciák részben az élettörténetben, részben az elkötelezettségekben, illetve kapcsolatokban gyökereznek. Azaz nemcsak a kudarcok jelölik ki az érkezési pontokat, hanem kapcsolati mintázatok és a kapcsolatokban megjelenő véleményvezető aktorok is (Nagy, 2009 és 2011).

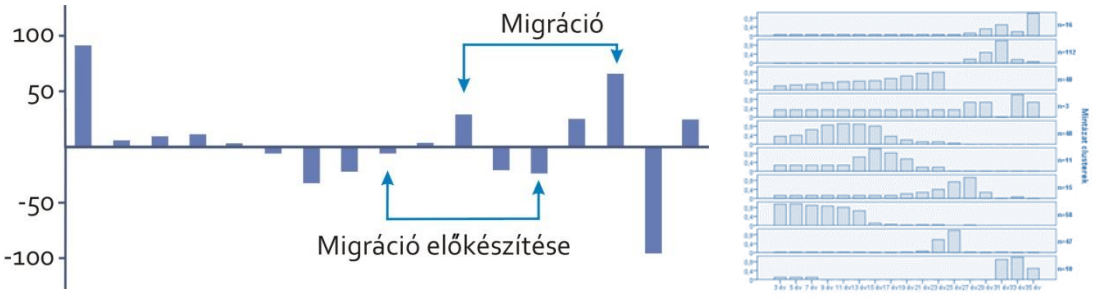
Távolabbról tekintve a problémára, hálózati szempontból periférikus szereplők válnak az extremizmusok érkezési pontjaivá. Ennek okai (vagy oksági láncolata):

1) az integráció foka (Brissette és mtsai, 2000) egzisztenciális kihívásokat jelent
2) a gazdasági tőke hiánya csökkenti a perspektivikus kilátásokat
3) a gazdasági, kapcsolati tőke hiánya a társadalmi és hálózati presztízst negatívan befolyásolja
4) az alacsony presztízs alacsony vonzerővel rendelkezik, így az izoláció fokozódik vagy állandósul.

A periférikus aktorok presztízsváltozásának (és így gazdasági-kapcsolati tőkéjének) kulcsa más, magasabb presztízsű aktorokhoz való kapcsolódás. Az izolációból, a legtöbb esetben, etnohomogén, azonos vallási közösségen alapuló kapcsolatokon keresztül próbálnak kitörni, s ez vagy egy erős klaszterhez vezet, vagy egy magasabb presztízsű aktorral patrónus-kliensi kapcsolatban (egyenlőtlen kapcsolatban) nyilvánul meg. Az így kialakuló mikroközösségek, részhálózatok középpontjában egy véleményvezető vagy tőke-gazdag aktor áll – e tőke lehet gazdasági, kapcsolati, társadalmi vagy kulturális tőke. Azonban még az izolált szereplők is aktívak a globális diaszpórahálózaton belül, s az online térben. Ezek

lehetőséget adnak az izoláltság csökkentésére, a társas kapcsolatok bővülésére és a kapcsolati tőke növekedésre. Ugyanakkor a periférikus szereplők, hálózati sajátságaiknál fogva, ki vannak téve a szélsőséges eszmék terjedésének: miközben véleményvezetőhöz kapcsolódnak vagy a kibertérben mozognak, a preferenciáikat a találkozásaik alakítják, de a valós térbeli hálózati gyengeségeik nem biztosítanak olyan vonatkoztatási pontokat vagy kontrollt, amely reflektálhat a szélsőséges gondolatokra.

A periférikus szereplők kiszolgáltatottsága az extremizmusok befogadására, hálózati mintázatokkal ragadható meg. A bevándorló vagy migráns hátterű aktorok jelentős kapcsolati veszteséggel jelennek meg a befogadó társadalomban: részben a migráció előkészítése során, részben a kivándorlás okaiként tételezett krízis vagy konfliktus okoz veszteségeket, ugyanakkor a befogadó társadalomban megjelenő szegregáló hatások is negatívan befolyásolják a bevándorlók és a migráns hátterű aktorok kapcsolati integrációját. Menedékkérők és nemzetközi védelemben részesített személyek esetében a migráció állomásai az ego-háló bővülésével, továbbvándorlás esetén ismételt szűkülés/veszteség és új kapcsolatok megjelenésével jár. Ezek jellemzően etnohomogén kapcsolatok, s a helyi diaszpórához, a diaszpóraközi térhez vagy a globális diaszpórahálózathoz köti őket (Safran, 1991; Nagy, 2009 és 2011). E kapcsolódások csak részben történnek valós térben (a helyi és a diaszpóraközi hálózatokban inkább jellemző), de nagy szerepe van a közösségi oldalaknak, az üzenetküldő szolgáltatásoknak és csak kisebb részben a titkosított csatornáknak és a Tor-nak.



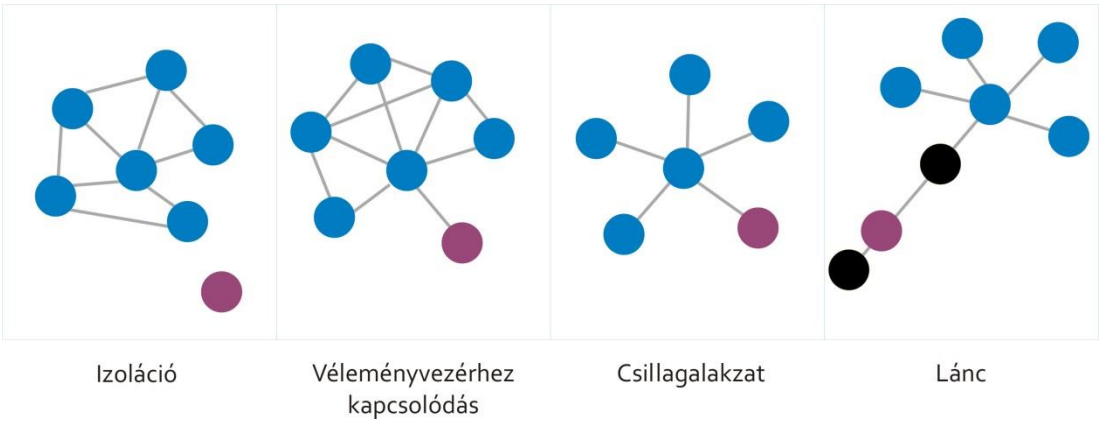
2. ábra. Kapcsolati mintázatok dinamikája - élettörténeti példa. Saját szerkesztés

Az egzisztenciális igények mellett fellépő társas igények predesztinálják a valós vagy online térben való ismerkedést, ezek ugyanis lehetővé teszik a diaszpórák erőforrásainak használatát, a kiépülő kapcsolati tőkék gazdasági tőkévé konvertálhatók, de támogatják a tranzitútvonalon való közlekedést, s később a diaszpórákhoz való kapcsolódást is (Nagy, 2011). A véleményvezetőhöz való kapcsolódás opcionális, de preferencia-vezérelt, s kétoldalú folyamat: a véleményvezetőnek és a periférikus szereplőnek is érdekeltnek kell lennie a

kapcsolat kialakulásában. A véleményvezetők többsége a diaszpóra magas presztízsű szereplője (hálózati szempontból: magas fokszámú hubja), ritkán a szalafita vagy a daesh ideológusa vagy toborzója. Rosszul kapcsolódó, periférikus szereplők esetében sok esetben az online térben jelenik meg, így közvetlenül nem jár egzisztenciális hatással.

Az extrémizmus fogadóterei tehát olyan periférikus szereplők, akik jellemzően kiestek az integráló közegből és újabbhoz nem tudnak kapcsolódni (készségei vagy szándékai is hiányoznak ehhez), sok esetben a valós térben korlátozott számú kapcsolatot épít és az online térben kevésbé instrumentális kapcsolatokból relatíve sokkal rendelkezik.

A jelzett kapcsolati mintázatok megközelítése jól prediktálja azt, hogy az izolált szereplő(k) külső véleményvezér érkezésével alkalmassá válhatnak az extremizmus befogadására, s az iszlamizmus, a szélsőséges eszmék érkezési pontjaivá válhatnak. A kapcsolati mintázatokban a drasztikus beszűkülést egy erős klaszterben megnyilvánuló kapcsolati bővülést, magas fokszámú véleményvezérhez, hubhoz való kapcsolódást követően a korábbi kapcsolatok maradványainak felszámolása követi, s végül egy, a véleményvezérhez kapcsolódó csillagalakzatban tömörülnek a szélsőséges eszmékre nyitott, befolyásolható, kevés vonatkoztatási ponttal és általában alacsony fokszámmal rendelkező izolált személyek. A csillagalakzat, más természetes hálózatokhoz képest, kisebb eséllyel növekszik, s amennyiben a szereplők kapcsolódnak is egymáshoz, a multilateralitás foka alacsony. Jellemzőbb ugyanakkor, hogy a csillagalakzat nem alakul át klaszterré, különösen nem a kibertérben kialakult kapcsolatok esetében. A csillagalakzat aktorai – kihasználva a diaszpóra-hálózatokat és az embercsempészetet –, nagyobb földrajzi távolságot megtéve jelennek meg: dawah-zóként (hitre hívóként), toborzóként vagy oktatható/aktivizálható operatív szereplőként. Ekkor a csillagalakzat hálózata „megnyúlik”, lánc-szerűvé válik, közbenső bizalmas szereplők jelennek meg.



3. ábra. Izolált szereplő integrációja iszlamista klaszterbe. Saját szerkesztés

2.3 A hubok és a hidak szerepe a terjedésben

A hálózatok fontos pontjai azok a jól, sokrétűen kapcsolódó szereplők, akik a hálózatban relatíve a legtöbb taggal kapcsolatban állnak, különböző minőségű kapcsolatot ápolnak. Ezen központi szereplőket nevezzük huboknak. A hubok mellett fontosak azon szereplők is, akik egy-egy részhálózatot kötnek össze – őket nevezzük híd szerepű szereplőknek. Az általam vizsgált diaszpórák, globális diaszpóra hálózatok illetve szélsőséges csoportok valós és kibertérbeli hálózatai esetében mindkettő kellően fontos pozíciót jelöl ki:

- a hubok magas presztízsüknél és a globális hálózatokba való bekapcsoltságuknál fogva jól transzferálják a konszenzuális értékeket, a szélsőséges ideológiákat vagy forrásokat (vö. Kitsak és mtsai, 2010);
- a hidak a hálózatok belső tagoltságát oldják, véleménybrókerként biztosítják a hálózaton belüli információáramlást és szelektálnak.

A probléma valójában az, hogy miközben a kapcsolatok jó részét birtokolják e központi szereplők, különösen a hubok (ld. még skálafüggetlen hálózatok), a hálózatközi tőkeáramlást is biztosítják, s minthogy az ideológusok és toborzók válnak hubokká, meghatározó szerepük van a tudásátadásban, értelmezésben (Edgar, 2011) és az alacsony fokszámú aktorok megtartásában. Sajátos szerepük okozza a hálózat instabilitását is: a hubok elmozdításával a hálózatok szétesnek.

A hálózat több tagja, de különösen a hubok, több dimenzióban rendelkeznek kapcsolatokkal a diaszpórán belül, a helyi diaszpórák között, a befogadó társadalom felé és a globális diaszpórahálózatban – s e dimenziókban a valós és kibertérben is. Minden irányban számosságában és minőségében is felülmúlják a hálózat többi szereplőjének átlagos kapcsolatszámát. Ennek eredményeképp a társas kötéseket (vagy más megközelítésben: kapcsolati tőkét) gazdasági tőkére képesek konvertálni, ezt részben megosztják a hálózat alacsonyabb rangú szereplőivel, többek között annak érdekében, hogy ezzel presztízshez vagy más potenciálhoz férjenek hozzá.

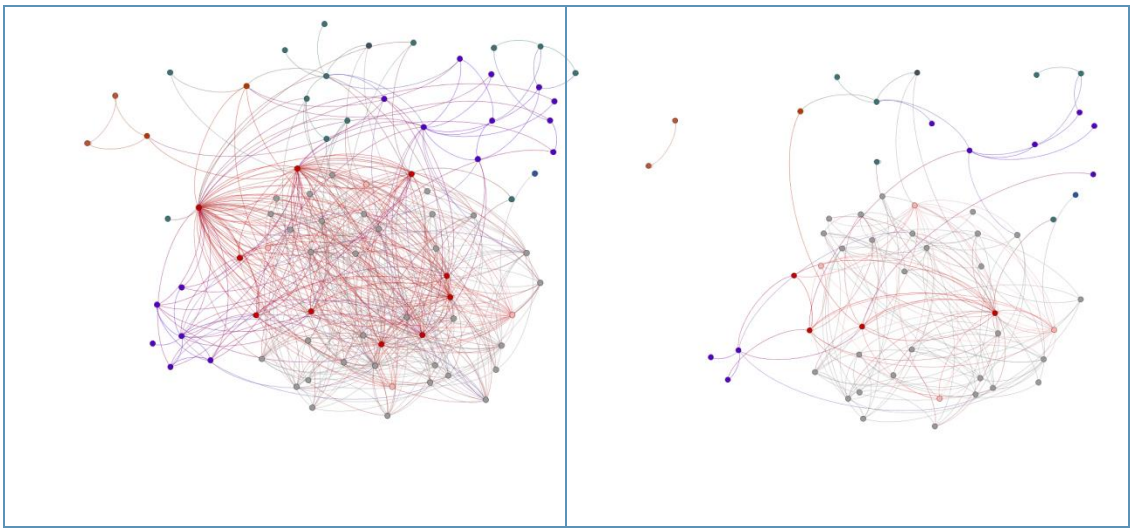
A hubok preferenciális választások (Barabási, 2016. 238-241) miatt dinamikus növekedésnek indulnak, s ennek gátat a hálózat robusztusságát is meghatározó kritikus értékek szabnak. Miközben a hálózat legtöbb aktora kevés kapcsolattal rendelkezik, a hubokhoz nagyobb valószínűséggel kapcsolódnak az újabb aktorok. A hubok így referenciális pontként is meghatározhatóak, s mint ilyenek, számos bizalmas kapcsolat révén a velük

közvetlenül kapcsolatban nem álló szereplőket is elérik. A hubok között találjuk azokat az imámokat és toborzókat, akik a szélsőséges eszméket közvetítik, illetve pragmatikus feladatokat bíznak más aktorokra. Ezen szereplők – funkcióiknál fogva is, s már meglévő kapcsolataikra épülő preferenciális kapcsolódások révén is – a kibertérben tudatosan felépített tevékenységet folytatnak, melyek egy része attraktív, nyitott, hozzáférhető és a tudásátadás folyamata jellemzően didaktikus, más része azonban csak a bizalmas, személyes kapcsolatokon keresztül – ajánlások által – hozzáférhető titkos csoportokban, fórumokban vagy a kibertérből kilépve privát területeken történik. A hubok szerepe, hogy olyan hatást fejtsenek ki, amelyek a hálózat kvázi határain túli növekedést is lehetővé teszik, így a megfelelő embereket tudják bevonzani.

Tevékenységük sok időráfordítást, s alkalmasint financiális ráfordítást kíván. Ugyanakkor az is fontos, hogy a hubok:

1) a diaszpórákon, illetve hálózatokon belül, presztízsüknél és kvázi-hatalmuknál fogva befolyásolni tudják a diaszpóra normáit, megközelítéseit, külső kapcsolatait és belső narratíváit, így befolyásolják a befogadó társadalom felé irányuló kapcsolatokat is,
2) a diaszpórák tagjainak többsége elsősorban rajtuk keresztül éri el a gazdasági-társadalmi erőforrásokat, illetve számukra perspektívákat kínálnak (mártíromság, jótett, ösztöndíj, új család, feleség, jövedelem, részesedés és túlvilági értékek),
3) a globális hálózaton belül is jelentős közvetlen és közvetett kapcsolatot ápolnak, de attraktivitásuk további kapcsolati potenciált jelenthet,
4) jellemzően vallási homogén, etnohomogén kapcsolatokat ápolnak, így a befogadó ország társadalma helyett a diaszpórához kapcsolódnak helyi szinten, s így az általuk tranzitált kapcsolatok is oda kötik.

Mivel a hubok számos potens kapcsolattal rendelkeznek, a globális hálózatban is képesek elmozdulni, akár azért, hogy további (és távolabbi) részhálózatokat fejlesszenek, akár azért, hogy elköltözzenek. Ha a hubok távoznak vagy beavatkozás következtében kikerülnek a hálózatból, a hálózat morfológiája és topológiája megváltozik (ld. 4. ábra): a strukturális hiányokat nem, az összekapcsoltságot pedig csak idővel tudják pótolni.



4. ábra. Komplex, multilaterális hálózat és ugyanazon hálózat néhány hub távozása után. Saját szerkesztés

A preferenciális kapcsolódásokkal növekvő hubok szerepe a hálózatok fenntartásában, működtetésben, a láncok integrálásában és az ideológiai közösségekkel való kapcsolattartásban ragadható meg, de hálózati szempontból kiemelten fontos, hogy megértsük azt a potenciált, amelyet egy-egy imám, mint hub, vagy egy-egy toborzó, aki alacsonyabb fokszámmal, de erősebb kapcsolatokkal rendelkezik, ki tud fejteni.

2.4 Láncok és átfedések a hálózatokban

A csillagalakzatból kiváló és sokszor térbeli mozgást végző lánc (ld. 3. ábra) szerepe rendkívül érdekes: miközben alacsony fokszámú aktorok összekapcsoltságát észleljük a hálózatban, ahol az információk áramlása N~L útvonalon halad, rendkívül fontos a valós térbeli és a kibertérbeli mozgás és információterjesztés vonatkozásában, hiszen magas bizalmi szinttel, a kapcsolatok multilaterális jellegével erős kapcsolatokból alakul ki. A láncok elemeiben új, tudatosan elhelyezett szereplők jelennek meg, amelyek mögött egy másik hálózat tevékenysége bújik meg. Valójában a láncok kapcsán vissza kell térnünk a rizóma megközelítéséhez: egy alternatív hálózat a felszíni pontjait kapcsolja egymáshoz, a vizsgált térben azonban csak a láncolat látszik. A lánc kapcsoltsága tehát már önmagában indikátora egy másik térben – valós térben, a kibertér más szegmensében – fejlődő hálózatnak, illetve a hálózatok átfedettségének (ld. Kovács és mtsai, 2010). (Igen izgalmas elemzés Krebsé (2002), aki a 9/11-es gépeltérítők találkozási pontjait és kapcsolódásait vizsgálta.)

A láncokban megjelenő aktorok a bizalmas kapcsolataik révén, a kapcsolataik potenciálját és változatos IKT-k használatával, szállítanak és fogadnak információkat, forrásokat. A fizikai térben a láncszemek egymástól távol is állhatnak, térbeli mozgással vagy

IKT eszközökkel e távolságokon keresztül is képesek közvetíteni úgy, hogy más számára nem hozzáférhetőek forrásaik és információik. A láncok gyakran közvetítők révén két hub között feszülnek ki, így a kódolt üzenetváltások mellett a források és eszközök tranzitálásában játszanak szerepet, de aktív alakítóivá is válhatnak a folyamatoknak: a csillagalakzatról leváló aktor az „ideológiai érettségét" elérve kaphat szerepet egy új területen, mint toborzó vagy eszmei vezető. Abban az esetben, amikor a láncolat két végpontja hubhoz kapcsolódik, a két szélső láncszem feltételezésem szerint az alternatív hálózatban van jelen, így közvetlen kapcsolódás nem, csak a strukturális hiány által következtetett aktor-hely információja áll rendelkezésünkre.

A láncok vizsgálata meghatározó a különböző hálózatok átfedésének vizsgálatában és megkívánja, hogy más adatforrások vizsgálatával térképezzük fel a láncok kapcsolódásait. E vizsgálatok elsősorban a big data és az adatbányász módszerek beépítésének lehetőségét jelentik, azaz a meglévő adatállományok, pénzügyi mozgások, információáramlások együttmozgása által kijelölt területek szenzitív vizsgálatát kijelölő algoritmusok alkalmazását. Érdemes a műveleteket a közösségi oldalak, a titkosított kommunikációt alkalmazó applikációk felszíni megjelenéseit a modellbe bevonni.

A „felszíni" hálózatok átfedettsége ismert, a munka és a magánélet világa sokszor összeér, a diaszpóra hálózatai és a munka világa komplementer hálózati részeket is tartalmaznak. Miközben a különböző etnikai, vallási hálózatok, a munka és a megélhetés hálózatai többszörösen átfedésben vannak, az extremizmus – éppen illegalitásánál fogva – kevés tranzitivitást mutat. Azaz az ismerősök, melyek csillagalakzatokat és láncokat képeznek, nehezen kapcsolódnak össze, hiszen erősen kötődnek a bizalom és az intimitás (szövetség/titok) által meghatározott diád- és triád-jellegű kapcsolatokhoz, azaz kettő, illetve három fős mikroközösségekből állnak, melyeket

- a híd szerepű aktorok szerveznek láncokká
- a híd szerepű aktor a fentebb jelzett átfedésben lévő hálózatok között is közvetíthet, elősegítheti a rizómák felbukkanását
- a lánc szereplői egyikének közvetlen kapcsolódása a hubokhoz: jelzi az extremitás tereibe való bekapcsoltságukat.

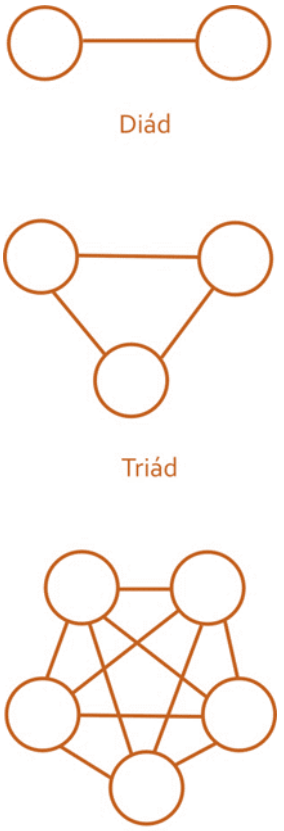
Ez azt is jelenti, hogy a láncban megjelenő aktorok fokszáma jellemzően alacsony, miközben néhány magas fokszámú hubhoz is kapcsolódhat a lánc egyik vége. A hub szereplő birtokolja a kapcsolatok túlnyomó hányadát, így a kapcsolatok eloszlása balra dőlő ferdeségű ($\beta<0$). Az összefüggő komponensek (aktorok és diádok közötti kapcsolatok alapján)

viszonylag stabilak, különösen a hubok eszmei környezetében kialakuló struktúrák stabilitása képes hónapokon, éveken át fennmaradni. Azonban a célorientált kapcsolatokat feltételező akciók esetében a lánc távolabbi pontja (toborzó, képző, operatív vezető) ugyan stabil, a többi résztvevő funkcionálisan gyorsan össze- majd szétkapcsolódik.

Külön figyelmet érdemelnek a diádok és triádok, amelyeknek az állandósága magas, éppen a bizalmasságuknál fogva (ld. Kapcsolati modulok és szélsőséges terek c. fejezet).

2.5 Kapcsolati modulok és szélsőséges terek

A diádok és triádok, azaz a két vagy három egyén közötti kapcsolatok stabilak, egymást támogatják, s elvi szinten képesek egymás számára további kapcsolatokat biztosítani és bekapcsolni a közösségeikbe társaikat. Alkalmasak az egzisztenciális, emocionális támogatásra, s egymás vonatkoztatási pontjaiként is értelmezhetjük őket. Éppen ezen utóbbi jellegzetesség alapozza meg azt, hogy együtt tudnak cselekedni, vagy épp elköteleződni egy tevékenység, munka, eszme iránt: egyik aktor, mint kvázi-vezető elköteleződése társas támogatására találhat, s kölcsönös megerősítést tudnak biztosítani egymás számára. Ha a belső bizalom nagyobb, mint a diádon/triádon kifelé mutató, akkor a megerősítés ellenpontja hiányozhat, s ez az, amely miatt az Európából kiképzésre, IS-taggal való házasságra induló másodgenerációs bevándorlók vagy megtértek általában ketten indulnak el. Vagyis miközben egy, akár valós, akár online térben megjelenő vonatkoztatási pont befolyása alá kerülnek, a külső, ellenirányú nyomás ellenében megerősítik összetartozásukat. A külső környezet ellenségesnek tűnik fel a narratíváikban, hitetlenként, komfort-keresőként, amellyel szemben egy erős ideológia és annak „utántöltése”, valamint a kapcsolati modul szereplőinek társas támogatása áll. Mindehhez az kell, hogy a magas belső bizalmi szinttel működő izolált mikrocsoport, a triád vagy a diád, ritkább esetben a néhány fős klikk, az izoláció ellenére gyenge kapcsolaton keresztül kapcsolódjon egy magas fokszámú szereplőhöz (hub-hoz), aki az információáramlásban vagy az integráció irányában segíthet. Vizsgált területünkön ez jellemzően az előbbit jelenti, de az információáramlás azonban nem csak egzisztenciális információkat hordoz, hanem – ahogy fentebb is utaltunk rá –, az eszmei támogatás, ideológiai utánpótlás forrása a hub.



5. ábra. Diád, triád, klikk

Miközben a kapcsolati modulok jellemzően a valós térben jelennek meg (ott kapcsolódtak egymáshoz vagy a későbbiekben találkoznak), az ideológiai véleményvezetők többsége az online térben jelenik meg: kihasználva a közösségi oldalakat, az audiovizuális lehetőségeket, a vallási tanítók, térítők, az IS-ideológusai, ahogy az al-Kaida vagy az al-Shabab ideológusai is, a valós térhez kapcsolódó távolságokat és határokat leküzdve, rendszeres, ütemezett tanításokat, illetve a politikai, vallási kérdésekre adott reflexiókat osztanak meg.

Miután e komplex jellegzetességeket áttekintettük, érdemes megvizsgálni a valós tér és a kibertér szerepét, a valós és kibertérbeli profilok, avatarok szerepét. A következő változatokban fordul elő a tér és szereplő jelenléte a valós és kibertérben:

Aktor	Hub
Dawah kapcsán a valós térben ismerkedik meg az aktor és a hub, a bizalmas kapcsolat e területen belül jön létre.	Nagy földrajzi távolságot bejáró térítők, toborzók, illetve a diaszpórában letelepedett tanítók, imámok
Online oktatás, toborzás területén jelenik meg az aktor, aki épp válaszokat keres	Online oktatást, térítést folytat

1. táblázat. Valós és kibertér. Saját szerkesztés

Folyamatában a valós és kibertér közötti átjárás adott, így a hubok mindkét térben aktivizálják magukat, kapcsolatokat ápolnak, jelentős időráfordítással érik el a kapcsolati tőke konvertálhatóságát. Az aktorok ehhez hasonlóan be- és kilépnek a kibertérből, jellemzően kezdetben saját néven, majd a szülők által választott név helyett saját muszlim nevet, beszélő nevet választanak, s a terület sajátságai miatt e néven követnek tudástranszferáló közösségeket, imámokat, magas alternatív presztízsű szereplőket. A diaszpórában megtalálható kapcsolatok közül a hasonló kötődésűek maradnak fenn, mások megfogyatkoznak (ld. kapcsolati mintázatok), s a hasonló érdeklődésűekből diádok, esetleg triádok formálódnak. Az online kapcsolatok többsége azonban nagy fizikai távolságot jelent, így kevesebb az esélye annak, hogy a kibertéren kívül is megjelennek, de a valós térbeli

kapcsolatok egy része (ld. akadályok, preferenciák) becsatornázható az online tér sajátos szegmensébe. A valós vagy kibertérben kialakuló, hub-fókuszú „ideológiai oktatással" foglalkozó csillag alakzatokban megjelenő aktor kapcsolatrendszere beszűkül, a vonatkoztatási csoport specializálódik, értékközpontú világnézeti átalakuláson megy keresztül. A nagy többség éveken keresztül áll ezen a szinten, hallgatja a tanítást, kommentel, kérdez, az ismereteket továbbítja a közösségi oldalakon keresztül, de nem válik aktív toborzóvá, nem vesz részt és nem tervezi, hogy részt vesz akcióban.

Számunkra azonban a kisebbség érdekes, azaz azok, akik miután ideológiailag átképzésen esnek át, tevőleges cselekvésre alkalmassá válnak, akár azért, mert értékes szaktudásuk van (informatika, vegyészet, oktatás stb.), így érdemes őket bevonni, illetve azért, mert maguk kívánnak tenni valamit (pl. küzdeni a hitetlenek ellen, a szenvedő muszlimok mellett, vagy mert támadás érte hub-jukat, stb.). A kapcsolati modulok és mintázataik ekkor válnak jellegzetesen, karakteresen eltérővé: a kibertérbeli társas aktivitás lecsökken, közvetlen „felettes" irányába intenzívebbé, majd szinte jelentéktelenné válik a kapcsolat, új funkcionális szereplők lépnek be. Ha a diád/triád más tagja is szintén aktivizálódik, akkor ez a kapcsolat fennmarad, s része lehet a csapatmunkának, de sokszor felszámolódik, ahogy az ellenérdekelt kapcsolatok maradványai is. Az operatív cselekvést megelőzően a kibertérbeli szerep minden tekintetben visszahúzódik, a valós térben is izolálódik, s csak az utolsó pillanatban keres társaságot és önkifejezésbe torkollik a kibertérbeli kommunikáció. Azonban a kapcsolatai ekkorra jórészt felszámolódnak, így úgymond nincs egy, a szereplő kiberaktivitására rálátó jelzőrendszer vagy szereplő – ha és amennyiben eltekintünk az adatbányász módszerek sikereitől.

Összességében a kapcsolati modulok a stabilitást, a vonatkoztatási pontot jelölik ki az abban résztvevők számára, s segítik a véletlenszerű támadások utáni regenerációt, körükben jelennek meg a passzív támogatók és a későbbi radikalizálódásra attribútumaiknál fogva nyitott aktorok is.

2.6 Interakciók, szerepek valós térben, kibertérben

Ahogy jelen tanulmányban több helyen is utalok rá, a valós és kibertér közötti átjárás az iszlám szélsőségesség hálózataiban is fontos szerepet játszik. Részben a kortárs kommunikációs csatornák miatt, részben társasági igények kielégítése végett a legtöbb aktor jelen van a kibertérben is. Miközben óvatos jelenlétük tudatos, IT-biztonságtudatossága a

hálózat legtöbb szereplőjének nincs. Több, gyakran összekapcsolt profillal, több néven jelennek meg, aktív véleménynyilvánítók, s csak kevesen veszik figyelembe a digitális lenyomat szempontjait. A hálózatok legtöbbje számára az az informatikai tudás, amely a terrorizmus központi sejtjeinek védelmét, kódolt üzeneteit és a kibertámadásokat jelentik, nem hozzáférhető. Így, amikor audiovizuális elemeket postolnak/tweetelnek, megjelenést biztosítanak, véleményt formálnak, akkor olyan digitális nyomokat hagynak, amelyből adatbányász módszerek segítségével, személyhez köthető profil rajzolható ki. Természetesen a digitális biztonság a szélsőséges hálózatok részéről sem teljesen elmaradott, de sokan vannak a hálózataikban, akik digitális analfabéták, miközben online jelen vannak, s óhatatlanul is részt vesznek üzenetek továbbításában, a hibásan használt felületeken szélesebb körben osztanak meg információkat, stb.

A hálózatok teljes vertikuma nem, de egyre több folyamat jelenik meg a dark web csatornáin, ezzel is kiszélesítve azon palettát, ahol értékes információforrásokat találhatunk.

A közösségi oldalakon, fájlmegosztó, videómegosztó portálokon való aktivitás a hubok köré koncentrálódó kapcsolatokat és a hálózatban található fokszámeloszlást idézik: kevés szereplő (imám, véleményvezetők, véleménybrókerek) relatíve nagy elérést „teljesítenek", miközben néhányan még produkálnak egy közepesen jó elérést, a toborzók relatíve kis létszámmal dolgoznak (de stabilabban). A radikalizációt segíti, hogy sok ismeretlen körében a korábbi normatív kontroll nem működik, ellenben új normák alakulnak ki, amelyek lehetővé teszik a dzsihád lájkolását, radikális imámok előadásából részletek megosztását és kommentelését, az illegalitás határán túl is.

A kockázatot éppen ez a kiegyensúlyozatlanság és új norma jelenti a kibertérben: a radikalizálódóknak érdekük fűződik ahhoz, hogy a kibertérben is működő csoportdinamikák fokozódjanak és így alkalmas kapcsolatokat tudnak kiépíteni, miközben azok, akiket fentebb az extremizmus fogadótereiként aposztrofáltam, gyenge, kisszámú kapcsolataik miatt a közösségi normáktól könnyen eltérnek az alternatív kontroll mellett, ráadásul támogató, elfogadó környezetet kapnak, így a befolyásolás terei bővülnek. A kiszolgáltatottságot növeli a fiatal életkor, az izoláltság, a közösségi és családi normatív kontroll hiánya, a vallási vezető és más szereplők iránti tisztelet és elkötelezettség, az egzisztenciális válság (Liang, 2015; Nagy, 2011).

Egyszerre több entitás is számot tarthat az érdeklődésünkre: a közvetítő médium sajátságai (Stieglitz és Dang-Xuan, 2012; Ahn és mtsai, 2010; Darmon és mtsai, 2015) és az üzeneteket megfogalmazó és transzferáló egyének, jellemzően hubok (Cilluffo és mtsai, 2007;

Grandjean, 20,15) és az üzenet megjelenésének okai (Cilluffo és mtsai, 2007. 5). Hálózati szempontból azonban elsősorban a kibertér attraktivitására és a radikalizációra fogékony fogyasztók hálózati szerepe és a beavatkozási lehetőségek fontosak.

2.7 Az iszlám terrorizmus, az iszlamizmus hálózatai és a hálózatok sebezhetősége

A láncok kapcsán jeleztem, hogy a lánc aktorai nagy távolságokat hidalnak át. A távolságok lehetőséget adnak az iszlám terrorizmus szakaszainak elkülönülésére: a tervezés, felkészülés és kivitelezés térben is egymástól távol zajlik, a távolságok bejárását a hálózatok – és a láncok – támogatják. Ugyanakkor a hálózatban való mozgás segítségével a szereplők képesek arra, hogy információt áramoltassanak, a hálózatok pedig arra, hogy az aktorok mobilitását és átmeneti letelepedését, helyi kapcsolatait támogassák (Nagy, 2011).

Jelen tanulmányban az iszlám szélsőségesek hálózataira fókuszálunk, amelyek egyes esetekben a terrorizmushoz vezetnek el – azonban látnunk kell ennek a lehetőségnek a hálózati hátterét, feltételrendszerét. Tosini (2007) úgy véli, hogy a terrorizmus akkor állhat fenn, ha van stratégiája, mögötte politikai, gazdasági, kulturális konszenzus áll és az egyéni aktorok motivációit feltételezi. Ez utóbbira példaként a bosszú, a krízis, a család anyagi támogatása, a mártíromság közösségi elismertsége motivációkat tételezi. A szélsőséges eszmék érkezési pontjaiként megjelenő aktorok motivációi kapcsán e felsorolás kiegészül hálózati szempontból a vonatkoztatási csoportok által közvetített értékekkel, illetve a hálózat főbb szereplőinek traumatikus elvesztését övező disszonáns érzésekből fakadó motivációkkal. Azaz, ha a vonatkoztatási csoport vagy hub a dzsihádban való részvételt alapvető értéknek tekinti, kommunikációjában azt közvetíti, hogy az iszlám fenyegetve van, az ummának szüksége van egyéni áldozatokra, akkor képes radikalizálni a korábban izolált, de már bevont szereplőket. Ha e véleményvezető elfogása – vagy más módszerekkel a hálózatból kiiktatása – radikálisan történik, az egyébként instabil szereplők és instabil hálózatok mobilizálódnak, az addig felhalmozott ismeretekre alapozva reagálnak.

Sok más mellett, például a terrorizmus eszmei holdudvarába való bekerülés és az ott terjedő narratívák mellett, most az iszlám terrorizmus hálózati megközelítése kapcsán azt kívánjuk megérteni, hogy az iszlám terrorizmus hálózata mennyire áll ellen a támadásoknak. A hálózatok modularitását és topológiáját áttekintve megállapíthatjuk, hogy a valós és a kibertérben párhuzamosan létező hálózatok egymást támogatják, amennyiben a földrajzi mozgást alternatív kibertérben készítik elő, vagy a láncok révén áramló információt a kibertérbeli rizómák felszíni aktorainak bizalmi összekapcsolása támogatja. Összességében ez

azt jelenti, hogy a hálózatokat együttesen kell tekintenünk, s a fentebb leírt sajátságok mentén értelmezni a hálózat támadástűrését.

A természetes hálózatok, melyek néhány nagy hub attraktivitása mellett számos mérsékeltebb fokszámú, klikkesedésre hajlamos aktort foglalnak magukba, a véletlenszerű támadásokkal szemben ellenállók, mert a véletlen támadások (beavatkozások, elfogások, stb.) a komplex hálózatok esetében kis valószínűséggel érik el a nagy fokszámú aktorokat. Azaz a hálózat sokáig ellenáll, majd hirtelen – amikor a kritikus küszöbérték 1-hez divergál – szétesik (vö. Barabási, 2006 és 2016). A komplex hálózatok azonban nem tudják megőrizni a stabilitásukat, azaz nem tudnak ellenállni a támadásoknak, ha a nagy fokszámú aktorokra (hubokra) fókuszálnak a beavatkozások. A célzott beavatkozás modelljét (Gao és mtsai, 2014) adaptálva olyan beavatkozási pontokat kell meghatároznunk, amely sok irányba indít kapcsolatokat, így a hálózat topológiai sajátosságainak megfelelően nagyszámú aktort ér el közvetlenül és rajtuk keresztül közvetve is. Több aktorra kell beavatkozást előirányoznunk, ha a hálózat erősen klaszterezett. Azonban a hubok kiemelésével, eltávolításával a hálózat kisebb egységekre esik szét, a diádok, triádok és láncok, valamint az izolációra hajlamos klikkek hajlamosak radikalizálódni vagy új, hasonló potenciállal rendelkező hubhoz kapcsolódni, óriáskomponensbe tömörülni (Barabási, 2016. 316. és Strogatz, 2001), így a felszámolás kudarcba fulladhat. A hubok alkalmasak arra, hogy értékeket, információkat vagy forrásokat közvetítsenek, azonban érdekeltségeik a hálózati pozícióikhoz és erőforrásaikhoz kötik, így pacifikálásuk esélye mérsékelt, kiemelésük pedig további problémákat vethet fel. A szélsőséges iszlamizmus hálózati specifikuma azonban a hubok körül kialakuló csillagalakzatból elvándorló, láncszemmé váló aktorok elhelyezkedése és szerepe. A sebezhetőséget ez esetben a láncszemeken keresztül valósít(hat)juk meg, a hub körül közvetetten elérhető aktorok záródó gyűrűjében, így a hub elveszíti konvertálható kapcsolatrendszerét, attraktivitása csökken, de a korábban izolált vagy alacsony fokszámú szereplők közvetett kapcsolódásai a hubhoz nem egyszerűen felszámolandók, hanem a hálózat harmadik szintjén lévő aktorokra gyakorolt beavatkozás által elterelhetők, új – más irányultságú – attraktív szereplővel pacifikálhatók.

A beavatkozást követő reakciók jellemzően reziliens reakciók, mert a hálózatok összekapcsoltsága a beavatkozásoknak sokáig ellenáll, a fennálló útvonalak mellett átvághatnak, így újjáépíthetik a hálózatot, különösen, hogy a hálózat küldetése funkcionalitásokhoz ragaszkodik és nem személyekhez. Ennek tudatában kell az ellentevékenységeket tervezni és a láncok sajátságainak megismerését előtérbe helyezni.

3 A hálózatelmélet gyakorlati alkalmazhatósága

3.1 A beavatkozási pontok kijelölése és a kockázatok

A hálózatelméleti megközelítés a maga reflektáltságával és kontextusba helyezkedő viszonyulásával, a hálózat statisztikai, topológiai értelmezésével hozzájárul ahhoz, hogy megértsük a szélsőséges iszlám terrorizmus térnyerésének kapcsolati vonatkozásait. E megértés eredményeképp jelölhetjük ki a beavatkozási pontokat, s érthetjük meg a hálózati látenciát, a rizóma-jellegét, valamint azt, hogy hogyan jelennek meg a szélsőséges eszmék fogadóterei, milyen utakon közlekednek az információk és más erőforrások.

Ezen ismeretek komplex valósága biztosítja a praktikus megközelítést, amely a hálózatok sebezhetőségére építve jelöli ki a beavatkozási pontokat, annak érdekében, hogy a szélsőséges iszlám terrorizmus hálózataira irányuló ellenérdekelt kezdeményezések hatékonyak legyenek.

Tehát a hálózatok sajátságaiból következően és a sebezhetőség elvét figyelembe véve a következő beavatkozási pontokat lehet kijelölni annak érdekében, hogy a szélsőséges eszmék terjedését és az arra épülő operatív akciók kockázatát csökkentsük:

1) A szélsőséges eszmék fogadótereiben kialakuló diádok és triádok számára új vonatkoztatási pontok tudatos felépítése a diádok/triádok bizalmi szintjének megbontása nélkül. Ez a beavatkozás szofisztikált, nagy humánerőforrást igénylő és tartós folyamat, amely ugyan hatékony, de költséges eljárás lenne, így még ha a hálózati sajátságokból következtethetünk is arra, hogy az elterelés hatékonysága nagy, nem kivitelezhető.
2) Hub szerepű aktorok „eltávolítása” a hálózatból. A hálózat sebezhetősége a huboknál történő beavatkozásnál magas, a hálózat ez esetben diádokra, triádokra, klikkekre és láncokra (a klikkesedés esélyével) szétesik. Biztonsági szempontból ez a legkevésbé járható út, hiszen a bizalmi hálózatok és az elkötelezettségek megmaradnak, ellenben a hálózatból megmaradó apró részek könnyen eltűnnek. Ráadásul arra is esély van, hogy a támadás miatt radikalizálódnak.

3) Híd szerepű aktorok esetében a közvetlen beavatkozás hatékonysága abban mérhető, hogy a hálózat nem szenved olyan nagy roncsolódást, amely miatt a radikalizálódó egységek el tudnának tűnni és ez ellehetetlenítené az érdemi munkát.
4) A láncba való bekapcsolódás szenzitivitást igénylő, de nagy hatékonysággal működő elterelési akció lehet. Előnyös, hogy a lánc új tagjai közbeékelődéssel is megjelenhetnek, s nincsenek olyan kontrollok, amelyek közvetlenül tudnák ellenőrizni. Hátránya, hogy a láncok a rizóma-jelleg felbukkanását jelzik egy háttér-hálózatból, amely magasabb bizalmi szinten dolgozik. A láncszemek vagy a láncon terjedő információk elterelése megakadályozza a szélsőséges iszlám terrorizmus hálózatának hatékony működését, nem okoz drasztikus változást addig, míg a láncszemekből álló gyűrű a hubokat körbe nem zárja, s ez alatt a láncok és rákapcsolódó modulok elterelésében fejt ki törekvést.
5) A magas tudástranszferáló pontok, amelyek a hálózat geodézikus távolságait átlag alatti szinten tudják elérni, alkalmasak arra, hogy új vonatkoztatási pont kijelölése mellett pacifikálódjanak.

Összességében a beavatkozási pontok kijelölése maximálisan kihasználja a hálózattudomány ismereteit, s miközben kevésbé vagy inkább drasztikus beavatkozásokat végez el, a hozzárendelt kockázatok ismeretében megalapozza a helyes döntéseket.

4 Összegzés

Tanulmányomban a hálózattudományi megközelítést alkalmaztam a nemzetközi, szélsőséges iszlám terrorizmus kapcsolatainak vizsgálatában, elsősorban a biztonság, az iszlám szélsőségesség és terrorizmus dimenzióiban. A tanulmányom során arra kerestem a választ, hogy a hálózat különböző szereplői a valós- és a kibertérben milyen szerepeket, feladatokat töltenek be és mi vezet a radikalizálódáshoz. A tanulmányom során diaszpórák és iszlám fundamentalista csoport köreiben végzett terepmunka eredményeimet a hálózattudomány módszerével interpretáltam, annak érdekében, hogy az iszlám extremizmus és terrorizmus elleni küzdelem gyakorlati eszköztára fejlődjön. Arról is szót ejtettem, hogy a nemzetközi iszlám terrorizmus hálózataiban megjelenő szereplők hogyan mozdulnak el a hálózatban, hogyan használják ki a hálózati erőforrásokat és e sajátos, többdimenziós hálózat hatékonyan mely aktorokon keresztül sebezhető.

Mint minden háló, a szélsőséges iszlám extremitás is különböző potenciával rendelkező aktorokból áll össze, dinamikusan fejlődik és a terület sajátságai miatt egy-egy szervezett háttérhálózatból felbukkanó elemei láncolatát figyelhetjük meg, valamint azt is, hogy a szélsőséges eszmék terjedésének a hálózatokban (és a térben is) vannak kihasználható lehetőségei, de ugyanabban a hálózatban bukkannak fel a terjedést akadályozó tényezők is.

Tanulmányom során bemutattam a sok kapcsolattal rendelkező központi szereplők és az izolált aktorok szerepeit a radikalizálódásban, a tudástranszferáló láncokban. A vizsgált hálózatok szereplői eltérő attitűdökkel, tudással és képességekkel érkeznek, elterelésük az integrációtól nem is olyan nehéz, mert ugyan közel élnek a befogadó társadalomhoz, de tapasztalataik, a diszkrimináció, a kapcsolati kudarcok elősegítik az attól való elfordulást, a felmerülő egzisztenciális kérdésekre pedig az izoláltságuk miatt sem kapnak választ. Az izolálódó mikroközösségek a diaszpórák hálózataiban, a globális diaszpóra-hálóban, de az extremizmus hálózataiban sem érvényesülnek jól, ha nincs egy kezdeményező hub. A kibertér azonban olyan teret jelent, ahol a normatív kontroll szerepe és tartalma megváltozik, ahol a potenciális jelöltek közé kerülhetnek az izoláltak, s végül akár előnyös is lehet: olyan közösséget, amelybe bekapcsolódva bizalmi kapcsolatok és hálózati erőforrások jelennek meg, s amely ideológiai-eszmei közösséget is jelenthet. A hálózat nagy csomópontjai, amelyek megőrzik a kevésbé sikeres kapcsolatépítőket is, fontos szerepet töltenek be a tudástranszferben, elmozdulásuk vagy kiszakításuk éppen ezért súlyos csapás a hálózatra, amely ilyen esetekben szétesik. Szétesik, de nem számolódik fel, ezért a kevésbé célszerű beavatkozási pontként is értékelhetjük a hubokat.

A tanulmány során a hálózati megközelítés gyakorlati alkalmazhatóságának irányából, a hálózatok tulajdonságain alapuló sebezhetőség-koncepciók alapján jelöltem meg a lehetséges beavatkozási pontokat és azok kockázatait. A gyakorlati értékű megközelítés lehetőséget biztosít a kapcsolatok megértésére és a hálózatok strukturális hiányainak felismerésére, a hálózattudományi megközelítés pedig hozzájárul a valós- és kibertérben fejlődő szélsőséges iszlamista hálózatok térnyerése elleni küzdelemhez.

5 Felhasznált irodalom

AHN, Yong-Yeol – BAGROW, James P. – LEHMANN, Sune (2010) Link communities reveal multiscale complexity in networks. Nature 466. 761–764.

BARABÁSI Albert-László (2006) A hálózatok tudománya: a társadalomtól a webig. Magyar Tudomány, 2006/11. 1298 pp.

BARABÁSI Albert-László (2016) A hálózatok tudománya. Budapest: Libri Kiadó

BRISSETTE, Ian - COHEN, Sheldon – SEEMAN, Teresa E. (2000) Measuring Social Integration and Social Networks. In: Cohen, Sheldon - Underwood, Lynn Gottlieb, Benjamin (eds): Social Support Measurement and Intervention: A Guide for Health and Social Scientists. New York: Oxford University Press, 53–85.

CHATURAPRUEK, Sorathan –BRESLAU, Jonah –YAZDI, Daniel és tsai (2013) Crime modeling with Lévy flights, SIAM Journal on Applied Mathematics, 73(4), 1703–1720. DOI: 10.1137/120895408

CILLUFFO, Frank – LANE, Jane – WHITEHEAD, Andrew – SAATHOFF, Gregory – CARDASH, Sharon – MAGARIK, Josh (2007) NETworked Radicalization: A Counter-Strategy. A special report by The George Washington University Homeland Security Policy Institute – The University of Virginia Critical Incident Analysis Group. http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HSPI_Report_11.pdf

DARMON, D., OMODEI, E., GARLAND, J. (2015). Followers are not enough: A multifaceted approach to community detection in online social networks. PloS ONE. 10, e0134860. doi: 10.1371/journal.pone.0134860

EDGAR, I. R. (2011) The Dream in Islam: From Qur'anic Tradition to Jihadist Inspiration. Berghahn Books

ELDEN, S. (2007) Terror and Territory. Antipode, 39. 821–845

GAO, Jianxi – LIU, Yang-Yu – D'SOUZA, Raissa M. – BARABÁSI, Albert-László (2014) Target control of complex networks. Nature communications, 5. 5415. doi:10.1038/ncomms6415

GRANDJEAN, Martin (2015) A social network analysis of Twitter: Mapping the digital humanities community. Cogent Arts & Humanities (2016), 3: 1171458

KITSAK, M., GALLOS, L.K., HAVLIN, S., LILJEROS, F., MUCHNIK, L. és mtsai (2010) Identification of influential spreaders in complex networks. Nature Phys 6: 888–893. doi: 10.1038/nphys1746.

KOVÁCS I., PALOTAI R., SZALAY M., CSERMELy P. (2010) Community Landscapes: An Integrative Approach to Determine Overlapping Network Module Hierarchy, Identify Key Nodes and Predict Network Dynamics. PLoS ONE 5(9): e12528. doi:10.1371/journal.pone.0012528

KREBS, Valdis E. (2002) Mapping Networks of Terrorist Cells. Connections 24. 3. 43–52.

LIANG, Ch. Schori (2015) Cyber Jihad: Understanding and Countering Islamic State Propaganda. GCSP Policy Paper 2015/2

NAGY, T. (2009) Kötődések és kudarcok. A kapcsolatok és kapcsolati kudarcok szerepe az integrációban. Egy menekültek körében végzett terepmunka eredményei. Budapesti Corvinus Egyetem, doktori értekezés

NAGY, T. (2011) Utazó kultúrák és a diaszpórák letelepedése. Tér és Társadalom, 4. 20–37.

SAFRAN, William (1991) Diasporas in Modern Societies. Myths of Homeland and Return. Diaspora 1. 83–99.

STROGATZ, Steven H. (2001) Exploring complex networks. Nature, vol. 410. 268–

STIEGLITZ, S., DANG-XUAN, L. (2012). Political communication and influence through microblogging, an empirical analysis of sentiment in Twitter messages and retweet behavior. System Science (HICSS), 3500–3509.

TOSINI, D. (2007) Sociology of Terrorism and Counterterrorism: A Social Science Understanding of Terrorist Threat. Sociology Compass, 2. 664–681

6 Ábrajegyzék

Krajcsik Zsolt

A biztonságos jövő és a felsőoktatás

Absztrakt

A XXI. század egyik legfontosabb fogalmává vált a biztonság. A fenntarthatóság olyan jelenbeli előírásokat ad, melyek a jövő generáció számára biztosítják a biztonságos élethez szükséges feltételeket. A cikk célja, hogy a biztonságos jövőt és a felsőoktatást összekapcsolja a fenntarthatóság révén, emellett megvizsgálja, hogy milyen változások szükségesek környezeti, gazdasági és társadalmi dimenzió mentén. A cikk bemutatja, hogy a felsőoktatási intézmények a fenntarthatóság jegyében milyen átalakuláson mennek majd keresztül.

Kulcsszavak:

fenntarthatóság, felsőoktatás, jövő, társadalom, gazdaság, környezet

Safe future and higher education

Abstract

Safety has become one of the most important concepts in the 21st century. The present regulations are given by the sustainability can ensure the conditions of the safe life for the future generations. The aim of the article to link the safe future and the higher education by the sustainability and to eximane what kind of environmental, economic and social changes are necessary. The article represents through what kind of transformation will the universities go by the sustainability.

Keywords:

sustainability, higher education, society, economy, environment

Tartalomjegyzék

1. Bevezetés

A biztonság a XXI. század egyik legfontosabb fogalmává vált – akár az elmúlt évek történései, akár a tágan értelmezett biztonság tekintetében. Tálas Péter szerint a biztonságnak a katonai biztonságon túl létezik gazdasági, környezeti és társadalmi vonatkozása, illetve az ezekre ható kiberkiztonsági vonzata is ismert. A fejezet célja, hogy a biztonság különféle dimenzióit összekapcsolja a felsőoktatással, valamint felvázolja az elkövetkező évtizedekben bekövetkező változásokat a felsőoktatás területén.

2. A biztonság dimenzióinak értelmezése a felsőoktatásban

A társadalmi, gazdasági, környezeti elemek jövő generációi számára történő előállítását a fenntarthatóság biztosítja, utóbbi annál jóval tágabb fogalmat takar. A fenntartható fejlődés több, minthogy az emberek boldog és értelmes életvitel folytatására törekednek, ami a közjó kiteljesedését tűzi ki célul úgy, hogy a saját jólétét az adott generáció nem feléli, az erőforrásokat hatékonyan használja fel, mivel megfelelő mennyiségben és minőségben a

következő generáció számára is biztosítani kell azokat, emiatt törekszik világunk erőforrás-kínálatának megőrzésére, bővítésére. (NFFT)

A fenntartható fejlődés három dimenziója – környezeti, gazdasági és társadalmi – szorosan kapcsolódik a felsőoktatáshoz, a cikk célja, hogy rövid betekintést nyújtson az olvasónak a felsőoktatás területén különböző dimenziók mentén bekövetkező változásokra. Környezeti szempontok alatt elsősorban a környezetterhelés csökkentését, az energiafelhasználás racionalizálását értjük, a gazdasági fenntarthatóság olyan rendszer felépítését tűzi ki célul, amely hosszú távon pénzügyileg fenntartható, jövedelmező, míg a társadalmi szempont szerint a különféle, jellemzően társadalmi csoportok szerepét, integrálását tűzi ki célul, tágabb értelmezésben a diplomák szociális megítélésével foglalkozik.

2. 1. Környezeti dimenzió a felsőoktatásban

A biztonság környezeti megközelítése alatt olyan akció- és tevékenységsorozatot értünk, amely a biológiai környezet fenntarthatóságát, a fajok diverzitását, a környezeti értékek megőrzését tűzi ki célul.

Az egyetemek szignifikánsan eltérő mikrovilága a környezeti biztonság adaptálását megnehezíti. Szinte lehetetlen olyan akciótervet készíteni, mely a világ bármely pontján működő felsőoktatási intézményt lépésről lépésre környezeti szempontból fenntartható felsőoktatási intézménnyé változtatna egy rögzített periódus alatt. A markánsan eltérő intézményi jegyek miatt a kiinduló lépések hasonlók (ANYANGWE, 2011):

- A dolgozókkal, illetve hallgatókkal szükséges megértetni, miért releváns intézményünk számára a fenntarthatóság. A szervezet fenntarthatóvá válásához a rendelkezésre álló humán erőforrás elkötelezettsége elengedhetetlen, ameddig nem vázoljuk fel számukra az elérni kívánt célt, nem fogalmazzuk meg, milyen úton kívánjuk ezt elérni, csekély támogatottságban részesülünk.
- Ahhoz, hogy a fenntarthatóság a mindennapok szerves részévé válhasson, ahhoz a személyzet viselkedését kell formálnunk, segítenünk kell a környezettudatos magatartás kialakulását, fenntartását.
- Szintén elengedhetetlen, hogy a fenntarthatóság nem átmeneti állapot – mint például a Föld napján kerékpárral menjünk munkahelyünkre mozgalom –, hanem egy, a mindennapi tevékenységsorozatba szervesen beilleszkedő, annak részévé váló

tevékenység. Fontos, hogy éreztessük dolgozóinkkal, hallgatóinkkal, hogy az év valamennyi napján így cselekedjenek, alakítsuk úgy attitűdjüket, hogy egy bizonyos idő után ne pusztán a szabályok betartása végett cselekedjenek, hanem automatikus válaszreakció legyen a környezeti ingerekre (például a szemetet szelektív hulladékgyűjtőbe helyezzük).

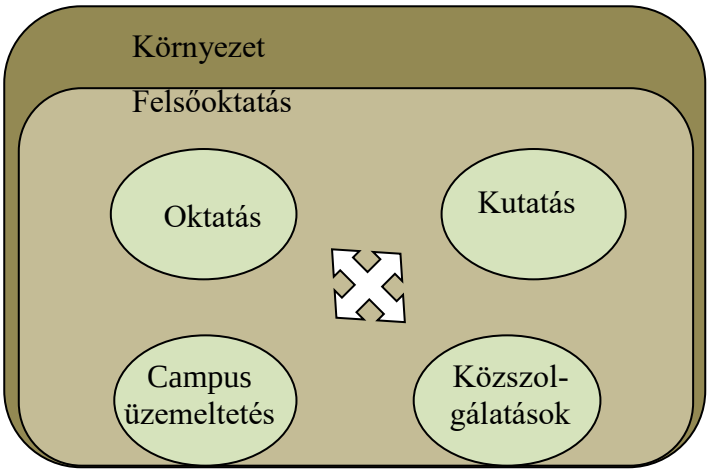
- A fiatalok eléréséhez a klasszikus médiumok, mint a nyomtatott sajtó, televíziós hirdetések kevésnek bizonyulnak. Az új generációt a közösségi média nyújtotta lehetőségekkel lehet a leghatékonyabban elérni, ezen keresztül napi kapcsolatban lehetünk velük, emellett jóval olcsóbb, valamint a kétoldalú kommunikáció révén a visszacsatolások segítségével a hatékonyság egyértelműen javul. Fontos szempont, hogy üzenetünket úgy fogalmazzuk meg a fiatalság számára, hogy a milliónyi inger közül, amely őket éri a közösségi média használata során, kitűnjön az adott projekt, figyeljen fel rá az egyén, ezért az ilyen feladatot is célszerű szakemberre bízni.
- Természetesen a változásokat nagyban befolyásolja a szervezet befogadókészsége, a szervezeti hierarchia. Lehetőséget kell biztosítanunk ahhoz, hogy a tehetséges, kiemelkedő egyének tevékenységének eredménye adaptálható legyen, átvehessék a különböző szervezeti egységek az innovatív megoldásokat, amihez elengedhetetlen a bürokratikus akadályok leomlasztása.

A környezeti szempontból fenntartható és racionális felsőoktatási intézmény nem pazarolja erőforrásait, nagy arányban hasznosítja a természet által kínált erőforrások úgy, hogy törekszik a környezet minél kisebb mértékű szennyezésére. Napjainkban ez abban nyilvánul meg számos intézmény esetében, hogy szelektíven gyűjtik a hulladékot, geotermikus energiával fűtenek, napkollektorok segítségével állítják elő a szükséges elektromos áram jelentős részét, megfelelő szigetelést biztosítanak az épületek számára, támogatják a tömegközlekedést, közösségi közlekedést, kerékpár-közlekedést a dolgozók és hallgatók között.

2. 2. Gazdasági dimenzió a felsőoktatásban

A biztonság gazdasági megközelítése alatt a pénzügyi biztonságot, az energiabiztonságot, illetve a szociális biztonságot értjük alapvetően, ezek a területek szorosan kapcsolódnak a már említett környezeti, vagy a későbbiekben kifejtésre kerülő szociális biztonság kérdéseihez.

A gazdaságpolitikai döntéshozók célja a társadalom jólétének maximalizálása, az eltérő politikai irányok mögött más-más járható utak állnak, ugyanakkor a végső cél mindegyikben azonos az elmélet szerint. (BOD, 2014) Fontos, hogy a különböző politikai struktúrák eltérő mértékben avatkoznak közbe a jellemzően nem hatékonyan működő felsőoktatás piacába. A szakirodalomban sem található konszenzus az állami szerepvállalás mértékének helyességéről, azonban a két végpont, a kvázi tervutasításos jelleggel működő, totális ellenőrzésen áteső felsőoktatási intézmények, valamint a piac kezére bízott intézmények léte igen ritka.



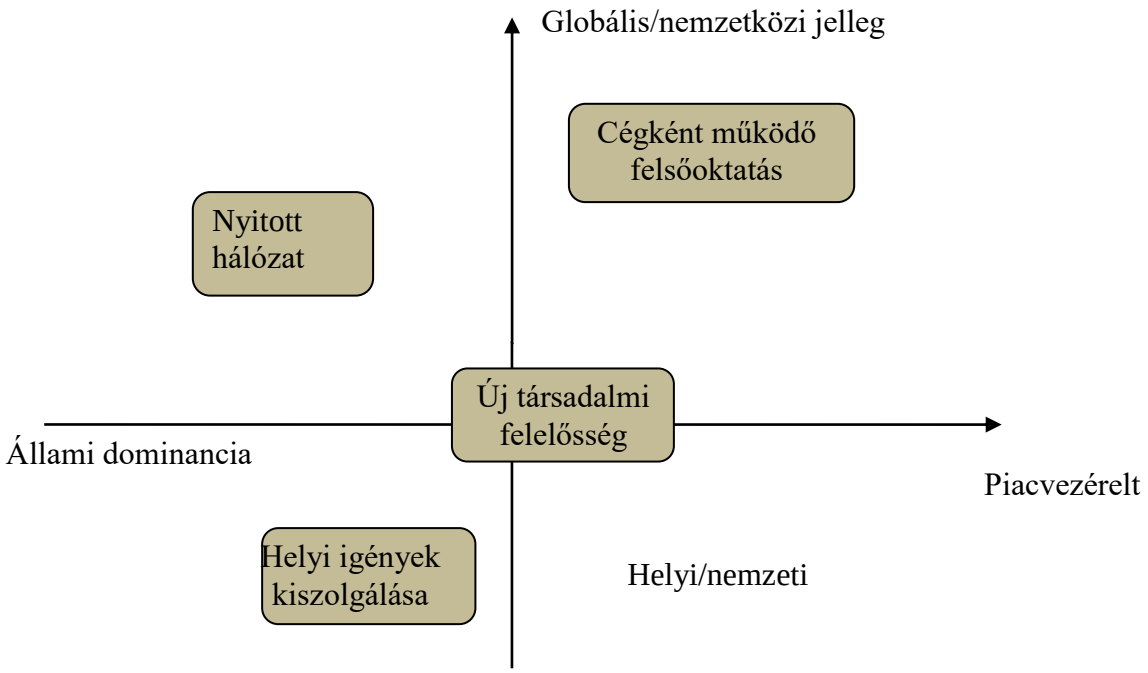
1. ábra: A felsőoktatási intézmények feladatai

Forrás: WAAS (2012) alapján saját szerkesztés

Az 1. ábrán látható, hogy a felsőoktatási intézmények világszerte jelenleg jellemzően négy lényeges feladatot látnak el: a jövő generációjának oktatását, az új ismeretek kutatását végzik a campus üzemeltetése és bizonyos közszolgáltatások (közhivatali tevékenység) végzése mellett. A különböző feladatok intenzitása egyrészt országonként eltér, másrészt a különböző regionális adottságok más-más lehetőséget biztosítanak az intézményeknek, így nem ritka a szinte csak oktatással foglalkozó, vagy a kutatásra nagyobb hangsúlyt fektető intézmények jelenléte.

A gazdaságilag stabil és fenntartható felsőoktatáshoz olyan intézményrendszer létrehozása szükséges, amely egyrészt a piac által vezérelt, tehát a munkaerő-piaci igények, a kereslet, megteremti a felsőoktatási intézmények kínálatát. Az állam túlzott szerepvállalása, melyben ellehetetlenít bizonyos tudományterületeket, míg másakat indokolatlan előnyben részesít, makrogazdaságilag helytelen döntésnek látszik.

Dirk Van Damme, a CERI/OECD vezetője 2008-as prezentációjában négy lehetséges utat (szcenáriót) vázol fel a felsőoktatási intézmények előtt. Egyrészt működhetnek helyi igények kiszolgálására, így például a duális képzés keretében amennyiben az állam bizonyos területeket nem támogat, a hallgatók és a vállalatok együttműködéséből profitálva kvázi a hallgatók a helyi igényekhez igazodva szerzik meg az oklevélhez szükséges ismereteket. Másrészt működhet az intézmény nyitott hálózatként, mikor az állam erős szerepvállalása mellett a gloablizált világ igényeihez igazodik, míg a másik „véglet" a szinte cégként működő felsőoktatási intézmény, ahol a piac diktál, az állami intervenciók nem jelentősek és a globális, határokat átlépő jelleg a fontos. Az új társadalmi felelősség majdhogynem az origóban helyezkedik el, amely – véleményem szerint – a jelenlegi rendszer újragondolt változatát jelenti, egyrészt a helyi igényeknek megfelelve, ugyanakkor a globális trendekkel egy vonalban, az állam és a piac szerepvállalásával alakítják ki kínálatukat az intézmények. (VAN DAMME, 2008)



2. ábra: Lehetséges szcenáriók a felsőoktatás előtt állam-piac, globális-lokális tengely mentén
Forrás: VAN DAMME (2008) alapján saját szerkesztés

Egyrészt maga a felsőoktatás, mint rendszer gazdasági fenntarthatóságáról is beszélhetünk, továbbiakban pedig annak a makrogazdasági teljesítményre gyakorolt hatását is vizsgálhatjuk. A szakirodalom is jelentősen megosztott a felsőoktatás és a makrogazdasági teljesítmény közötti kapcsolat viszonylatában. Bizonyos publikációk egyértelműnek tekintik

az oktatási kiadások növekedése és a gazdasági fejlődés kapcsolatát (pl. REISZ és STOCK, 2012; CHICAGO FED LETTER, 2006; KONSTANTYUK, 2014), míg más vélekedés szerint az államnak nem fontos ilyen szinten beavatkozni az emberi tőke fejlesztésébe, ugyanis annak hatása jellemzően mikroszinten, a jövőben realizálható magasabb jövedelemben realizálódik, a makrogazdasági többletteljesítmény egyértelműen nem kifejezhető, nehezen mérhető, így megkérdőjelezik a felsőoktatás és a gazdasági növekedés közötti kapcsolatot. (pl. WOLF, 2003)

A gazdaság biztonságának megingását a felsőoktatási intézmények rövid időn belül megérzik, csökkenhet a képzés iránt a kereslet, növekedhetnek a képzések díjai, melynek tovagyűrűző hatása miatt úgy vélem, szükséges a fenntartható mértékű, emberi szabályozás.

2. 3. Társadalmi dimenzió a felsőoktatásban

A felsőoktatás tekintetében a társadalmi dimenzió megerősödése hazánkban a rendszerváltással kezdődött meg, majd erőteljes növekedését a bolognai folyamat átvétele eredményezte.

1. táblázat: A bolognai folyamat szociális dimneziója

Időpont, helyszín	Prioritás
2001, Prága	Szociális dimenzió megjelenése
2003, Berlin	Egyenlő hozzáférés kiszélesítése
2005, Bergen	Szociális dimenzió megerősítése
2007, London	Hatékony monitorozás
2009, Leuven	2020-ig szóló nemzeti célkitűzések mérése
2010, Budapest-Bécs	Egyenlő hozzáférés kiszélesítése
2012, Bukarest	Egyenlő hozzáférés kiszélesítése és a végzettségi arányok emelése
2015, Yerevan	Nyitott, befogadó és egyenlő esélyeket biztosító felsőoktatás

Forrás: HERA OKTATÁS- ÉS NEVELÉSKUTATÓK EGYESÜLETE, 2016.

Szociális szempontok alapján bizonyos társadalmi csoportok felsőoktatásban való részvételét kiemelt figyelemmel kell kísérni, milyen arányban lépnek be, hogyan haladnak

előre, a végzettségükkel milyen munkaerő-piaci kimenetre számíthatnak. Ilyen szempontok alapján vizsgálhatjuk a szociálisan hátrányos helyzetű hallgatókat, roma hallgatókat, fogyatékossággal élő hallgatókat, kisgyermekkel rendelkező hallgatókat, továbbá a határon túli hallgatókat. (HERA, 2016)

A szociális dimenziót tágabban értelmezve az egész társadalom tekintetében vizsgálhatjuk a diploma értékét, a diplomások helyzetét. Ma Magyarországon a diplomával rendelkezők életkeresete jóval magasabb, mint az alacsonyabb iskolai végzettségűeké, amennyiben nem így lenne, nem lenne célszerű a humán tőkébe beruházni. Másodsorban a költségtérítéses képzés révén jellemzően a társadalom tehetősebb része vehet részt a felsőoktatásban, a szerényebb anyagi hátterű családoknak legfeljebb vidéki felsőoktatási intézmények maradnak, ahol nem ritka, hogy a fővárosihoz képest fele összegű a tandíj, azonban mindez a diplomák általános megítélésén érződik. A felsőoktatásból a kormányzat vélekedése szerint kevesen maradnak ki a Diákhitel nyújtotta lehetőség miatt, azonban általánosságban véve ez sem feltétlen jelent megoldást a fiatalok számára, hiszen egy tehetős családból érkező pályakezdő számára sokkal egyszerűbb a munkába állás és otthonteremtés, mint egy hátrányos helyzetű hallgató számára. A felsőoktatásnak éppen ezt az ellentétet kellene feloldania, biztosítania kellene széles bázis számára a hozzáférhetőséget és ingyenességet bizonyos keretek között annak érdekében, hogy a biztonság társadalmi dimenziója megvalósulhasson. Azzal, hogy tehetséges, ám szegény hallgatók kimaradnak a felsőoktatásból, a jövőjüket nem tudják megalapozni és nem biztosított számukra a kitörési lehetőség. (CSEKEI, 2008)

A hallgatók finanszírozásának oldala egyrészt lehet méltányos, másrészt pedig hatékony, törekedni kell a felsőoktatási intézménynek az adott társadalom igényeihez illeszkedő rendszer kiépítése. A méltányos felsőoktatási rendszer előnyben részesíti a hátrányos helyzetű hallgatókat, anyagi, vagy nem pénzbeli támogatásban részesíti őket, előmozdítja társadalmi kitörésüket, azonban ennek üzemeltetése jelentés bürokratikus terhet ró az államra, vagy az intézményfenntartóra, ugyanakkor a hatékonyság elvét szem előtt tartva az adott intézmény kvázi egyenlőnek tekint mindenkit, azt is, aki nehéz körülmények mellett vesz részt a felsőoktatásban, és azt is, akinek családja jelentős támogatást biztosít. Úgy gondolom, olyan szociális ellátórendszer kiépítésére, fejlesztésére van szükség, amely a ténylegesen hátrányos helyzetű, ugyanakkor tehetséges hallgatók esetében biztosítja a havi kiadásokhoz történő anyagi hozzájárulást, elősegíti a másoddiploma, szakirányú képzettség megszerzését, amely mellett fontos, hogy a támogatások ne hallgatók tömegei között aprózódjanak el, hanem a ténylegesen rászorulók anyagi támogatását segítsék. Emellett

kiemelten fontos véleményformáló erőként jelentkezik a felsőoktatás a fenntartható fejlődés szempontjából, a diplomát szerezni kívánók itt kaphatnak útmutatást arra, hogy az élet számos területéhez hogyan viszonyulhatnak fenntarthatóan.

3. Felsőoktatás területén szükséges változások

A számítógépek és az internet segítségével az előző évszázadokhoz képest jelentősen felgyorsult világunk, a változások a korábbiakhoz képest sokkal intenzívebbek és gyorsabbak, azonban a felsőoktatás bürokratikus rendszerét kevésbé érintették, hatásuk jobban érezhető például termelővállalatok mindennapi életében.

2. táblázat: Jelen és jövő, az átalakuló felsőoktatás

Jelen		Jövő
Inkoherens, széttöredezett jelleg		Szisztematikus rendszer, pozitív szinergikus hatások kiaknázása
Túlburjánzott, óriási nagyság, kapcsolatok hiánya		Emberi léptékű, szoros kapcsolatokra építő
Zárt közösség		Nyitott, átjárható szervezeti struktúra
Oktató szervezet		Tanulószervezet
Nem fenntartható viselkedésmód		Fenntartható viselkedésmód

Forrás: WAAS et al. (2012) alapján saját szerkesztés

A jövő felsőoktatási intézményei jelentősen átalakulnak, ugyanis a korábbiakkal ellentétben előtérbe kerül a felfedezésen alapuló oktatás, a hallgatóközpontú megközelítésmód, az együttműködésen alapuló tudásátadás, az elméleti és gyakorlati ismeretek koherenciája, a kognitív, affektív és gyakorlatorientált megközelítésmód, valamint a legtöbb tudományterületen az érintettek (stakeholder) segítségével történő oktatás.

3. táblázat: Változások ellen és mellett ható tényezők

	Belső	Külső
Gátló tényezők	intézmény szabadsága, szervezeti struktúra, konzervatív vezetés	társadalmi nyomás hiánya
Támogató erők	támogató vezetés, intézményi jó gyakorlatok adaptálása, intézményi összeköttetések, méret, koordináló egység	társintézmények nyomása, pénzügyi erőforrások biztosítása

Forrás: FERRER-BALAS et al. (2008) alapján saját szerkesztés

Ahhoz, hogy egy felsőoktatási intézmény fenntarthatóvá váljon, az alábbi akciósorozat végrehajtása szükséges (WAAS et al., 2012):

- Normativitás fontossága, előírások, szabályok betartása, amelyek olyan társadalmi szerkezet kialakítását segítik, melyek a különböző iránymutatásokat betartják, társadalmi, gazdasági, környezeti szempontból fenntartható mértékű fejlődés során.
- Méltányos rendszer kiépítése a jövő generációi számára az épített környezet, a földrajzi környezet, vagy a természeti környezet tekintetében.
- Integráció alkalmazása, mivel olyan összetett társadalmi-gazdasági jelenséggel állunk szemben, amelynek megközelítése interdiszciplinaritást igényel.
- A társadalom és környezet állandó változása miatt a dinamikus megközelítés elengedhetetlen.

Ugyanakkor az új generációk szükségletei, igényei, elvárásai is jelentősen eltérnek a korábban megszokottól, az infokommunikációs eszközöket jól használó fiatal generáció egyrészt kihívást jelent a munkaerőpiac számára, hogy miként tudják hasznosítani sajátos képességeiket és beállítódottságukat, másrészt kihívást támaszt a felsőoktatással szemben is. Ezek a következők (WAAS et al., 2012):

- megváltozott hallgatói érdeklődés,
- átalakuló kutatási támogatás,
- minőségközpontúság,
- közösségi, társadalmi eredmények,

- alkalmazhatóság,
- elszámolhatóság,
- morális kötelezettség.

Ennek érdekében a jövő felsőoktatási intézményének olyannak kell lennie, amely elősegíti a társadalmi, gazdasági és környezeti biztonságot, szem előtt tartja a kiberbiztonságot, ennek fényében a környezetkárosodást csökkenti, az erkölcsi felelősségvállalást növeli, fenntartható tudományos környezetet épít ki, a stakeholderekkel és társintézményekkel hatékonyan együttműködik, jelentései nyilvánosak, átfogó, interdiszciplináris tudományos megközelítésen alapul, megfelelő intézményi keretek kialakítása mellett az oktatók képzésére is nagy hangsúlyt helyez. (WAAS et al., 2012)

A hallgatók esetében több lépcsős változásra van szükség, egyrészt magát a fenntarthatóságot, mint ismeretanyagot kell elsajátítaniuk, másodsorban olyan képességekre is szükségük van, amivel fenntarthatóvá válhatnak, harmadsorban pedig személyes és érzelmi hatásokra van szükség, amik az attitűdjüket megváltoztatva a berögzült magatartásformákat átírják. (WAAS et al., 2012)

4. Összefoglalás

A felsőoktatási intézmények életében a korábbiakhoz képest a kutatás előkelőbb helyet foglal majd el, ugyanis számos területen az állami szerepvállalás csökkenése miatt az intézmények szolgáltatásaik egy részét piacosítják. Így például vállalati problémák megoldásában segédkeznek üzleti tanácsadás révén, vagy piackutatás végeznek. Az oktatás területén is jelentős változások várhatók, a friss diplomások által gyakran említett, elméleti ismeretek és gyakorlati elvárások közötti szakadék az új megközelítéseken alapulva csökken, a gyakorlati ismeretek integrálódnak az elméleti tudásanyaghoz.

Az intézmények a korábbi időszakokhoz képest sokkal inkább globalizáltak, egyre nagyobb arányban tanulnak külföldi hallgatók akár teljes képzés alatt, vagy néhány féléven át tartó részképzéssel.

A felsőoktatás fenntarthatóvá és biztonságossá tételéhez egyrészt szükséges országos szinten megfelelő jogszabályi környezetet biztosítani, illetve racionalizálni a mai bürokratikus, hierarchikus felépítést. Ezt követően a felsőoktatási intézményeknek megfelelő időt biztosítva adaptálniuk kell ezeket az előírásokat, szabályokat a mindennapi életbe,

valamint az alulról jövő javaslatokat, véleményeket egyeztető fórumon keresztül folyamatosan implementálni kell annak érdekében, hogy az érintettek bevonásával hosszú távon fenntartható, élhető világot alakítsunk ki.

Irodalomjegyzék

Alison WOLF: *Education and growth: Questioning a false consensus*. New Economy, Institute of Education, University of London, (2003) 10-15.

BOD Péter Ákos: *Bevezetés a gazdaságpolitikába*, Akadémiai Kiadó, Bp., 2014.

CSEKEI László: *A bolognai folyamat szociális dimenziója*, Felsőoktatási Műhely, (2008)/1, 27-43.

Dirk VAN DAMME: *Future scenario's for higher eudcation, OECD, CERI, Higher Education to 2030*, What Futures for Quality Access int he Era of Globalisation? Conference, 2008.

Eliza ANYANGWE: How can higher education institiutions become more sustabinable?, 2011. Forrás: https://www.theguardian.com/higher-education-network/blog/2011/oct/13/sustainability-in-higher-education (2016. 07. 23.)

FERRER-BALAS D. et al.: *Az international comparative analysis of sustainability transformation acroos seven universities*, International Journal of Sustainability in Higher Education, (2008) Vol. 9 Iss: 3. 294-316.

Nataliya KONSTANTYUK: *Higher Education as a Determinant of Sustainable Economic Development of Ukraine: Financial aspects*, Barometr Regionalny, Tom 14 Nr 1. (2014), 69-77.

NFFT (NEMZETI FENNTARTHATÓ FEJLŐDÉSI TANÁCS): *A fenntartható fejlődés fogalma,* Forrás: http://nfft.hu/a-fenntarthato-fejlodesrol/a-fenntarthato-fejlodes-fogalma/ (2016. 07. 26.)

Richard H. MATTOON (2006*): Chicago Fed Letter: Can higher education foster economic growth*, The Federal Reserve Bank of Chicago, (2006) August, Number 229.

Robert D. REISZ, Manfred STOCK: *Private Higher Education and Economic Development*, European Journal of Education, (2012) Vol. 47, No. 2, 198-211.

WAAS Tom et al.: *Sustainable Higher Education – Understanding and Moving Forward*, Universiteit Antwerpen, IMDO: Instituut Voor Milieu & Duurzame Ontwikkeling (2012)

Tárgymutató

E számunk szerzői

DÉRI ATTILA

BREHEL JÓZSEF

HORVÁTH DÁVID

DR. SZABÓ CSABA – HORVÁTH ALEXANDRA – NAGY BENCE

DR. NAGY TERÉZIA

KRAJCSIK ZSOLT

---

[i] Daniel MIESSLER: The Internet, the Deep Web, and the Dark Web, 2016. Forrás: https://danielmiessler.com/study/internet-deep-dark-web/ (2016.08.25.)

[ii] Over 5000 .onion link 2016, Forrás: http://pastebin.com/hWyD5ZKP (2016.08.25.)

[iii] Ingmar ZAHORSKY: Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum, 2011. Forrás: http://www.monitor.upeace.org/innerpg.cfm?id_article=816 (2016.08.25.)

[iv] Daniel MOORE, Thomas RID: Cryptopolitik and the Darknet, Survival, 58:1, 7-38.

[v] Google Terms of Service, Forrás: https://www.google.com/intl/en/policies/terms/ (2016.08.25.)

[vi] Jeremy KIRK: Researcher: RSA 1024-bit Encryption not Enough, 2007. Forrás: http://www.pcworld.com/article/132184/article.html (2016.08.25.)

[vii] Arvind NARAYANAN, Vitaly SHMATIKOV: Robust De-anonymization of Large Sparse Datasets, Oakland 2008. Forrás: http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (2016.08.29.)

[viii] Testing for Command Injection (OTG-INPVAL-013), Forrás: https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013) (2016.08.29.)