Karkus Viktor

Közösségi hálózatok és a privacy viszonyának elemzése

15. téma

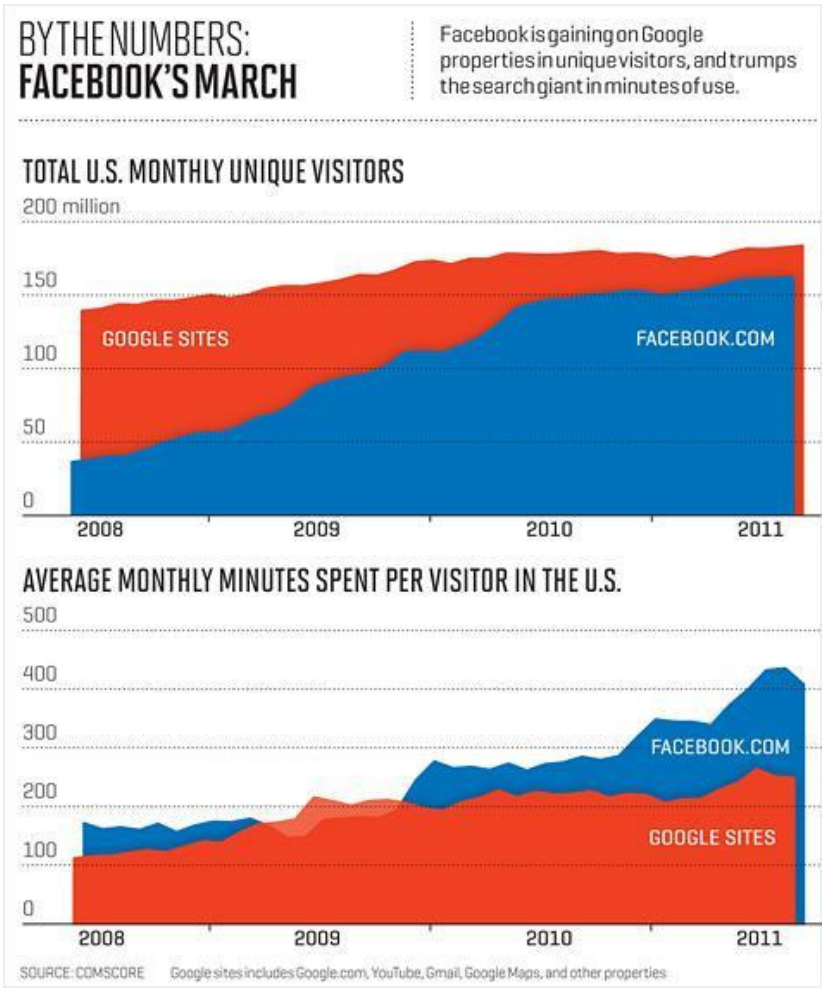
Tartalomjegyzék

1 Bevezető

Manapság a leglátogatottabb oldalak egyike a Facebook, ha nem a leglátogatottabb. Így jogosan merül fel az emberben, ha egy ilyen oldalt néznek a legtöbben, ami az emberek személyes adatainak eladásából él ezt milyen feltételekkel teszi. De kinek van arra ideje, hogy minden használt szolgáltatás felhasználási feltételeit átolvassa? Egy tanulmány szerint [1] évente 154 órát venne igénybe már az is, ha csak átfutnánk ezeket az irányelveket.

A probléma ott kezdődik, hogy az emberek azáltal, hogy otthon a kényelmes székben osztják meg a fél életüket, fel sem merül bennük, hogy mennyien látják azokat az információkat, melyeket publikál az internetre. Egy német cég felmérése szerint [2] a felhasználók nagy része aggódik a személyes adatinak biztonságáért, de valamiért annyira nem érdekli az embereket, hogy kikényszerítsenek az oldalak üzemeltetőitől valamiféle megnyugtató megoldást.

Tanulmányom első részében kitérek arra, hogy mi is az az adatvédelem, majd a világszerte legnépszerűbb közösségi oldal a Facebook, és a Magyarországon piacvezető Iwiw adatvédelmi szabályzatát veszem górcső alá. Ezek után több privátszférát sértő atrocitást mutatok, utána pedig lehetséges megoldásokat veszek számba.



1. ábra: a google és a facebook látogatottsága, és az ott eltöltött idő [3]

2 Az adatvédelem

A wikipédián lévő szócikk a következőképp definiálja [4]: „Az **adatvédelem** a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozásával, az érintett személyek védelmével foglalkozik. Nevével ellentétben tehát nem elsősorban az adatokat védjük, hanem azokat a személyeket, akikkel az adatok összeköthetők. Ennek eszközei lehetnek jogi szabályok, eljárások, de akár technológiai eszközök is.”

2.1 Miért fontos az adatvédelem?

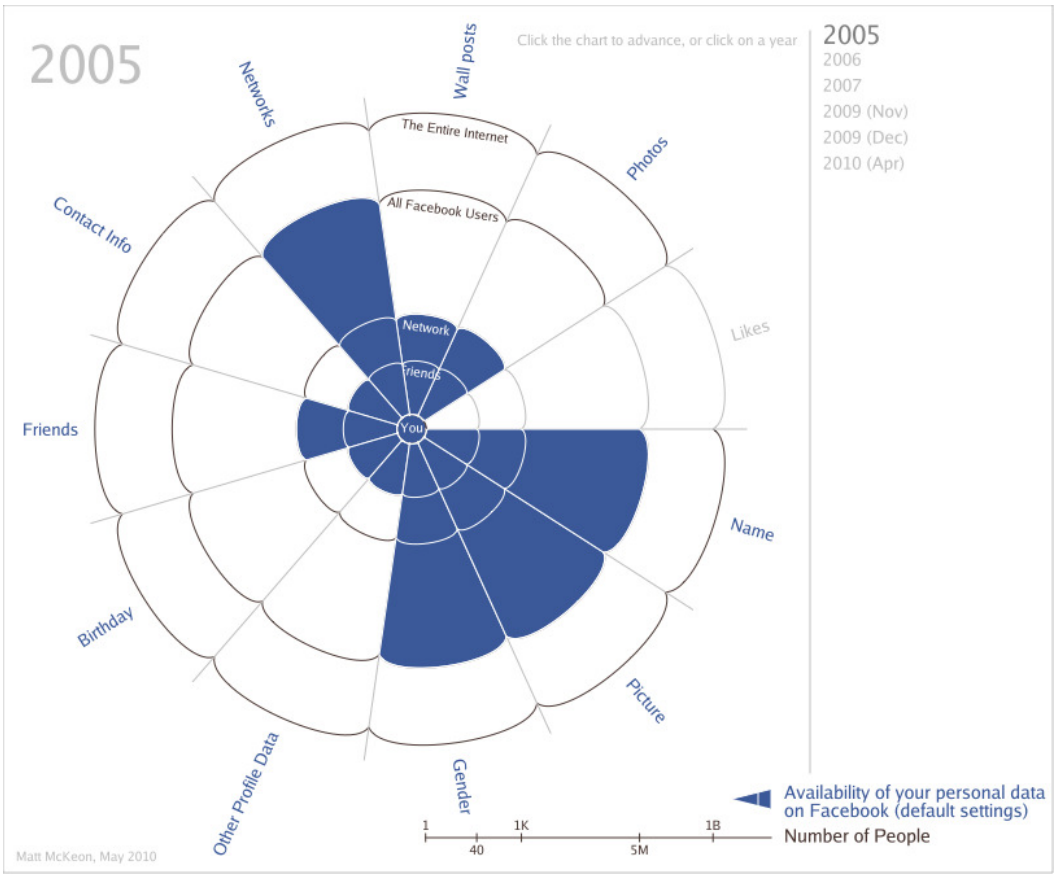
Gondolom mindenkivel volt már olyan, hogy valamiről azt hitte, jó, ha közzéteszi, aztán később kiderült, mégse kellett volna. Természetesen nem akarja senki a főnöke orrára kötni, ha henyél munkaidőben stb. Több részre lehet osztani a személyes adataink védelmének kérdését.

Először ott vannak azok az adatok, amit fel se kéne tenni az internetre. Ilyenek például egy-egy rosszul sikerült buli fotói. Ezeket a felhasználó magatartás megváltoztatásával lehet leginkább megvédeni, mert amikor jelentkezünk egy állásra, vagy karrierünk során valaki kellemetlen perceket akar okozni, az ilyen dolgok mindig előkerülnek. Ide tartozik az is, amikor az ember folyton megosztja, merre van épp, ezzel egy meghívót küldve a betörőknek, hogy most jöjjenek, mert elutazott pár hónapra. Ha valamiért mégis a megosztás mellett döntünk, legalább azoknak a körét, akik látják az adott bejegyzést, állítsuk be pontosan, és ne lássa boldog-boldogtalan.

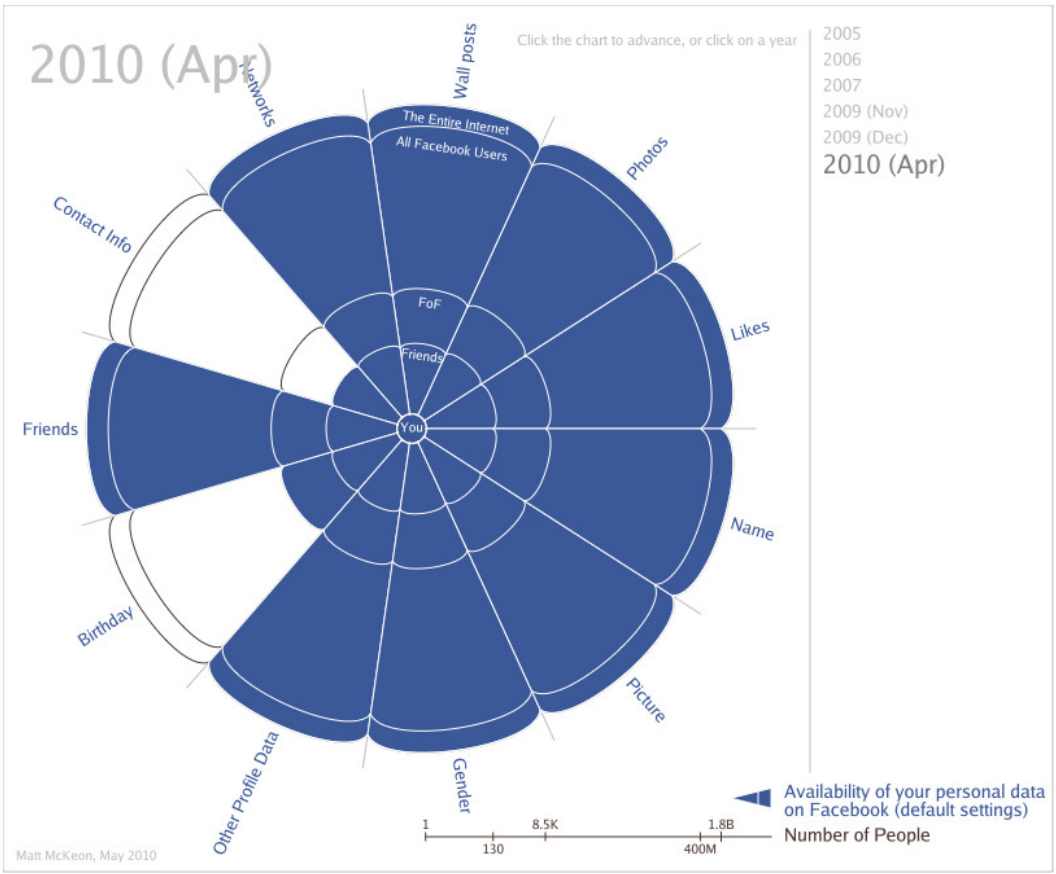
A másik csoport az melyek vagy kellenek az adott szolgáltatáshoz, vagy nem, mindenesetre a szolgáltató elkéri ahhoz, hogy használhassuk a szolgáltatását. Például a legtöbb Facebookos alkalmazás hozzáfér a teljes adatlapunkhoz, pedig kétséges, hogy egy játéknak mire kellhet a barátaim hálója, vagy az e-mail címem. Persze abban sem lehetünk biztosak, hogy a szolgáltató megfelelően tárolja a mi adatainkat, még mindig gyakran hangos a sajtó újabb, és újabb adatbázis betörésektől. Szóval dönthetünk, hogy vagy megadjuk ezeket az adatokat, vagy vétünk a végfelhasználói szerződés ellen, és hamis adatokkal töltjük fel a mezőket.

A harmadik rész pedig az, amit az ismerőseink osztanak meg rólunk. Hálózatkutatók egyik kedvelt témája, hogy miket lehet megállapítani olyan emberekről, akik nem is tagok egy közösségi oldalon, az ismerőseik által megosztott információk alapján [5].

A következő ábrák szemléltetik, hogy hogyan változott az alapértelmezett beállítása bizonyos adataink nyilvánosságának Facebookon 2005 és 2010 közt [6]. Az látszik, hogy egyre több adatunk nyilvános az egész internet számára alaphelyzetben, ezért fontos, hogy ezeket a beállításokat mindenképp módosítsuk:



2. ábra: 2005-ös alapbeállítása a személyes adatok nyilvánosságának Facebookon



3. ábra: 2010-es alapbeállítása a személyes adatok nyilvánosságának Facebookon

3 Az adatvédelmi irányelvek

A legnépszerűbb magyar oldallal kezdem az Iwiwvel [7]. Itt a legtöbb felvitt adatot két féle képpen tehetjük közzé. Vagy csak a barátaink látják, vagy az oldal összes felhasználója, de az összes felhasználó számára elérhetővé tett adatokat az Iwiw publikussá is teheti. Ezeken kívül természetesen naplózzák az IP címünket, hogy mikor léptünk be illetve ki, de ezekhez csak az adatkezelő fér hozzá (az utolsó látogatás időpontja a felhasználók számára publikus). Úgy fogalmaznak, hogy bizonyos esetben az operációs rendszer és a böngésző típusát is. Az általunk végzett tevékenységek, és megadott alapján személyre szabott reklámokhoz is felhasználják a megadott adatainkat. A klubok és az apróhirdetések is nyilvánosak az interneten. Az alkalmazások pedig a Facebookhoz hasonlóan azt csinálnak, amit akarnak, nem felel értük senki. Törölni lehet magunkat, elvileg 5 napon belül véglegesen törölnek a rendszerből.

Tehát röviden, elég gyengén szabályozhatóak a bevitt adatok, gyakorlatilag az az érzése az embernek, hogy teljesen hidegen hagyja az üzemeltetőket a felhasználók privát szférája, ilyen lehetőségek mellett képtelenség értelmesen beállítani. Mondjuk nem ez az egyetlen oka, hogy manapság már fiatalok elenyésző része használja aktívan, tényleg csak kapcsolattartásra, és kémkedésre jó az oldal.

A Facebook adatvédelmi irányelvei már érdekesebbek [8]. Eleve strukturáltabban vannak összeszedve az egyes részekre vonatkozó rendelkezések, de erre szükség is van mivel sokkal hosszabb olvasmány. Kezdjük azokkal a dolgokkal, amik mindenképp publikusak. Ezek a felhasználónév és user ID, a név, a profilkép, és azok a hálózatok, amikhez csatlakoztunk, ilyen lehet például az iskola ahova jártunk. A bejegyzéseink és az adataink viszonylag könnyen beállíthatóak, hogy kiknek látszódjanak. Bár publikus, a barátaink, és csak a felhasználó a három alap kategória, viszont az egyéni menüpont alatt, listákkal vagy személyenként beállítható, hogy ki lássa az adott bejegyzést. Ez mind szép és jó, de attól még az üzemeltető ugyanúgy hozzáfér az adatainkhoz.

Mivel segíti a még célzottabb reklámokat? Például nyilvántartja a bejelentkezésünk kori IP címet, ha lehet, akkor a GPS koordinátákat. A játékok és a weboldalak adatait ahol be van építve a Facebook Platform. Ez a gyakorlatban azt jelenti, hogy a weboldalak nagy részén nyomon tudnak követni, hogy mi érdekel, ugyanis alig látni manapság olyan oldalt ahol nincs egy like vagy egy megosztás gomb, esetleg még kommentezési lehetőség is. Aztán még a reklám partnerektől is kapnak adatokat, hogy miket azt nem részletezi a szabályzat. Persze itt is törölhetjük a létrehozott fiókot, de itt már csak egy hónapon belül törlődik a fiók, és még 90 napig a törlés után is maradhat itt-ott biztonsági mentés.

Ahhoz, hogy egy alkalmazást használatba tudjunk venni, az alkalmazás által kért adatokhoz hozzáférést kell adnunk, amiken nem is tudunk csak utólag változtatni, hogy bizonyos dolgokhoz mégse adunk. Tehát ha el akarja lopni valamilyen adatunk, addigra már úgy is megtette.

4 Visszaélési példák, védekezés

Az adatainkat két féle támadó ellen kell védenünk. Vannak az úgynevezett belső támadók, ezek a hirdetők, az alkalmazások, illetve maga az oldal fenntartója. Az, hogy ők hogyan használják az adatainkat az a közösségi háló tulajdonosának jóindulatán, illetve a hatályos jogi szabályozáson múlik, ez utóbbi jelenleg még nem elég kiforrott. Másik fajta támadó, akikre már vonatkoznak a mi adatvédelmi beállításaink. Őket három csoportba lehet osztani, ismerősünk az oldalon, ismerősünk ismerőse, vagy ismeretlen. Az, hogy tagja-e az adott hálózatnak lényegtelen, mivel a legtöbb esetben ezekre az oldalakra szabad a regisztráció, így ez nem jelent akadályt. A következőkben néhány megtörtént, Facebookkal kapcsolatos visszaélést ismertettek, illetve azt, hogy hogyan lehet ellenük védekezni.

4.1 Belső támadások

4.1.1 Nyomon követés

Mint az ismert [9] a Facebook, az oldalon kívül is nyomon követi a felhasználói aktivitást. Sőt, az is kiderült, hogy ezen az se segít, ha kijelentkezünk a fiókunkból [10]. Azzal, hogy regisztrálunk az oldalra, és ha nem védekezünk sehogy, egész jó profilt tudnak építeni rólunk, és ehhez nem szükséges megnyomni az oldalakon elhelyezett „tetszik” gombokat.

Ez ellen több féle képp védekezhetünk.[11] Az első ilyen, ha a Firefox és Chrome alatt elérhető Adblock Plus nevű kiegészítőbe egy „Facebook Privacy List”[12] nevű listát importálunk. Ez a Facebookon kívül minden más oldalon blokkolja a Facebookhoz tartozó szkripteket, így semmilyen gomb, vagy szolgáltatás (például a kommentelés lehetősége) nem jelenik meg. Hasonlóképp működik a Disconnect nevű kiterjesztés, ami ugyancsak Chromra és Firefoxra érhető el, de ezek a Facebook mellett több szolgáltatás követését blokkolják (pl. Twitter, Google stb.), illetve itt könnyebb az egyes oldalakhoz kapcsolódó szolgáltatások visszakapcsolása kis időre. Kis különbség, hogy Chromera ez egy kiterjesztés formájában is elérhető, a Firefoxos verzió valamiért törölve lett és csak külön Facebook Disconnect, Twitter Disconnect, Google Disconnect néven érhető el. Van még egy jobb kezdeményezés ez a Priv3 nevű Firefox extension[13]. Ez nem blokkolja a kommunikációt a harmadik féllel (itt pl. a Facebook számít annak), hanem, amikor lekérdezi a sütiben tárolt információt, akkor nem adja vissza. Így működőképesek maradnak a beágyazott elemek, ugyanis ez a kiegészítő figyeli a kattintásokat, és ha ilyen elemre kattintunk, újratölti az oldalt, most már elküldve a süti információt, ezáltal használhatóvá válik az adott elem.

4.1.2 Alkalmazások

Nem is olyan régen volt az az eset, amikor a „Mi az indián neved?” nevű alkalmazás elkezdett terjedni[14]. Ez egy jól álcázott adathalász eszköz volt, arra ment rá, hogy az egyébként népszerű véletlen generált mondatokat adó alkalmazások mintájára viselkedett. Ezek az alkalmazások annyit tudnak, hogy az ember használja, az pedig az adatbázisából véletlenszerűen ad egy bejegyzést, amit a felhasználó megoszthat. Például a „Hányast kapok ma?” nevű alkalmazás visszaadja, hogy „Kapát”, én meg jól kiteszem a falamra és együtt nevetünk a barátaimmal ezen a marhaságon. Szóval így álcázta magát az alkalmazás, pedig valójában arra adtak engedélyt a felhasználók, hogy az

alkalmazás lementse a nyilvános adataikat, a barátaikat, esetleg az ő adataikat is, valamint a rajongói lettek egy ékszerüzlet oldalának.

Az ilyen támadások ellen úgy védekezhetünk hatékonyan, ha elolvassuk, hogy mikhez kér hozzáférést az adott program, ha gyanús, inkább ne használjuk. Valamint érdemes az eddig engedélyezett alkalmazások jogosultságait eltávolítani. Sajnos nem lehet finom hangolni az applikáció engedélyezése előtt a jogokat, csak utána, így az alatt, amíg az engedélyezés után átverekedjük magunkat a Facebook menüjén, az alkalmazások jogaihoz addig bármihez hozzáférhet, de ott már letilthatunk bizonyos dolgokat például, hogy e-mailt tudjon küldeni stb. Amennyiben egy olyan adatot tiltunk le, amit fontosnak érez, újra kérni fogja az engedélyt.

4.1.3 Álvideók

Ezekhez az alkalmazásokhoz hasonló az, amikor többnyire egy álvideóra kattintva lefut egy szkript, ami mondjuk egy bizonyos alkalmazásnak megosztási jogot ad, vagy üzenetet küld az összes ismerősünkbe, vagy csak simán közzétesz valamit a falunkon. Az ilyenek ellen leginkább a NoScript nevű, és a hasonló kiegészítőkkel lehet védekezni, bár kicsit körülményessé válik miatta a böngészés, mivel az weboldalak igen nagy része használ javascriptet, amit forrásonként (mármint az alapján, hogy melyik weboldalról származik) kell engedélyezni a kiterjesztésben, de sok kellemetlenségtől kímélhet meg. Ha valami gyanúsan szenzáció hajhász, akkor valószínűleg ilyen álvideóról van szó, terjedésüket lassítja, ha tiltjuk, hogy ismerőseink közzétehessenek a falunkon.

4. ábra: Egy tipikus álvideó [15]

4.1.4 Bugok

Persze ide tartozik még, ha valamilyen hibát ejtenek a programozók, és nem a hozzáférési beállításaink szerint férnek hozzá mások a közzétett adatainkhoz. Például mára már befoltozták, de volt olyan hiba, hogy rejtett albumokhoz lehetett hozzáférni, ha akár egyetlen képet közzétettek valahol ahol eléri a támadó [16][17].

4.2 Külső támadások

4.2.1 Minden nyilvános

Először azt vesézzük ki, hogy miért gond az, ha nem megfelelően állítjuk be, hogy ki férhet hozzá bizonyos tartalmakhoz. Néhány lehetséges példa, arra hogy miért nem jó megoldás az, ha minden publikus. A megosztott információkból a jelszó emlékeztető kitalálható, így a nevünkben bármit elkövethetnek a közösségi oldalon. Felvételin nem biztos, hogy előny, ha ismerik szexuális, vagy politikai beállítottságunk. A már említett

betörés is valós veszély, a pleaserobme.com egy olyan oldal ami Twitter felhasználó név alapján kikeresi az adott felhasználó tweetelt bejelentkezéseit. Volt olyanra is példa, hogy valakit „jóakarói" jelentettek az adóhivatalnál, egy utazás képei alapján, hogy ugyan egy vagyonosodási vizsgálat keretében nézzék már meg, miből telik nekik erre, de ehhez nem is mindig kell jóakaró, az adóhatóság emberei egyébként is böngészik a közösségi oldalakat ilyen céllal [18]. és ez csak néhány példa a rengeteg visszaélési lehetőség közül.

Védekezni leginkább úgy lehet, az ilyen jellegű atrocitások ellen, ha az adott közösségi oldalon megfelelően beállítjuk, hogy az egyes képeket, albumokat, bejegyzéseket kik láthatják. Facebookon már azt is be lehet állítani, hogy a megjelölések publikálása előtt a jóváhagyásunkat kérje a rendszer. Bár, így nem linkelve ugyanúgy érhető el rólunk tartalom, de ezt jóval nehezebb megtalálni. Érdemes a kínos képekről levenni a bejelölést, és ha annyira vállalhatatlan töröltetni a képet. Ugyan ezt lehet alkalmazni a bejegyzésekre vagy bármire. Igaz persze, hogy ami egyszer fölkerült a netre, azt nem lehet eltűntetni, de legalább dolgozzon meg rendesen, ha valaki ilyesmit keres rólunk.

Ide tartozik az is, hogy meg lehet tiltani, hogy külső keresők hozzáférjenek a profilhoz, így legalább az nem dobja ki rögtön. Valóban működik, amióta létezik jómagam is eltűntem a Googleből, pedig előtte az első oldalon ott volt, a megfelelő keresőszavakra. Régebben volt olyan funkció is a Facebookon, hogy név alapján ne legyen kereshető az ember, még a rendszeren belül se, de ezt megszűntették, arra hivatkozva, hogy másképp is felfedhető a nevünk, (például barátaink, vagy barátaink barátain keresztül, ahol valamilyen bejegyzésben vagy képen linkelve van a profilunk). Ehelyett most a barátnak jelölést és az üzeneteket lehet tiltani.

4.2.2 Ismerőseink listákba szervezése

Vannak olyan esetek, hogy az embernek muszáj bizonyos embereket fölvenni az ismerősei közé. Példának okáért Magyarországon is vannak olyan iskolák, ahol a diákoknak kötelező bizonyos csoportokba belépni, vagy visszaigazolni tanárukat [19]. Ezáltal rögtön ki is esett az a lehetőség, hogy mindent csak a barátaim láthatnak és minden rendben, mert voltak olyan esetek is ezért csaptak ki diákot vagy bűntettek meg.

Viszont ha csoportokba szervezzük az ismerőseinket, és megfelelően beállítjuk, hogy ki mihez férhet hozzá ez elkerülhető. Azért is hasznos, ha csoportokba rendezve vannak a barátaink, mert az ember könnyen megfeledkezhet egyes ismerőseiről, de ha jók a beállítások, akkor nincs olyan baki, hogy szidom a munkahelyet, a főnök pedig ezt látja. Ennél egyel fejlettebb, ha az oldal támogatja a részidentitásokat, de ezt a Facebookon sajnos még nem vezették be.

4.2.3 Csoportok, és hamis profilok

A csoportok nem jelentenek különösebb adatvédelmi kockázatot, olyan szempontból viszont okozhat kellemetlen perceket, ha hirtelen a „Cica kedvelők társasága" nevet vált és „Plázacica kedvelők társasága" lesz az új név.

A hamis profilok már egy kicsit nagyobb gondot jelentenek, ugyanis ezek nagy része elve csalási céllal jön létre, például azért, hogy személyes adatokat lopjon. A legjobb ha csak olyan embereket igazolunk vissza akiket tényleg ismerünk.

Egy kis segítség a következő táblázat egy tanulmány néhány eredményét foglalja össze, ami arról szól, hogy hogyan tudjuk megkülönböztetni az igazi és az álfelhasználókat:

	Valós profil	**Hamis profil**
Nőnek vallja magát	40%	97%
Nők, akiket nők és férfiak is érdeklik	6%	58%
Barátok átlagos száma	130	726
Felsőoktatásban részt vett	40%	68%
Átlagos bejelölések fotónként	1/4	34
Soha nem frissítette a státuszát	15%	43%

1. táblázat: valós, hamis profilok összehasonlítása [20]

4.2.4 Az sincs biztonságban, amit nem láthat senki

Vannak olyan esetek, amikor nem ér semmit az, hogy hogyan állítjuk be a bejegyzések láthatóságát, mert mondjuk egy állásinterjún az ember felé fordítanak egy laptopot, és megkérik, hogy lépjen be a Facebook accountjával [21]. Ilyenkor, ha kell az állás nem sok választása van a jelentkezőnek.

Ez ellen azt tehetjük, hogy tényleg minden kellemetlen bejegyzést eltávolítunk, illetve hogy korlátozzuk saját magunkat, azaz kétszer is meg kell gondolni, hogy vajon egy-egy bejegyzés ilyen esetben is vállalható-e. Persze az se megoldás, ha teljesen üresen tartjuk a profilunkat, mivel az gyanút kelt. A másik megoldás az, hogy az ilyen cselekedeteket törvénytelenné nyilvánítja a törvényhozó. Egy ilyen törvény már készül az Egyesült Államokban [22].

4.3 Általános védelem

Az eddigi támadások ellen hatásos az is, ha titkosítva kommunikálunk az ismerőseinkkel, vagy szteganográfiát is alkalmazhatunk, de a jelenlegi megoldások használata túl körülményes, és többnyire nem azért vagyunk fenn egy ilyen oldalon, hogy egy néhány fős klikkel kommunikáljunk. Bár titkosítás esetén, még mindig megkérhetnek, hogy oldjuk fel azt, a szteganográfia ilyen szempontból biztonságosabb.

Ezekhez hasonló megoldás még, ha ál-adatokkal töltjük fel a fiókunk, ezzel gyakorlatilag azt tesszük lehetetlenné, hogy a potenciális ismerőseink megtaláljanak, de egy komolyabb kereséssel valószínűleg megtalálna az, akiknek ez a munkája.

Ezen eszközök bővebb bemutatása túlmutat ezen esszén, így inkább csak néhány nevet sorolok fel, amikre érdemes keresni: FaceCloak, FlyByNight, Scramble, StegoWeb

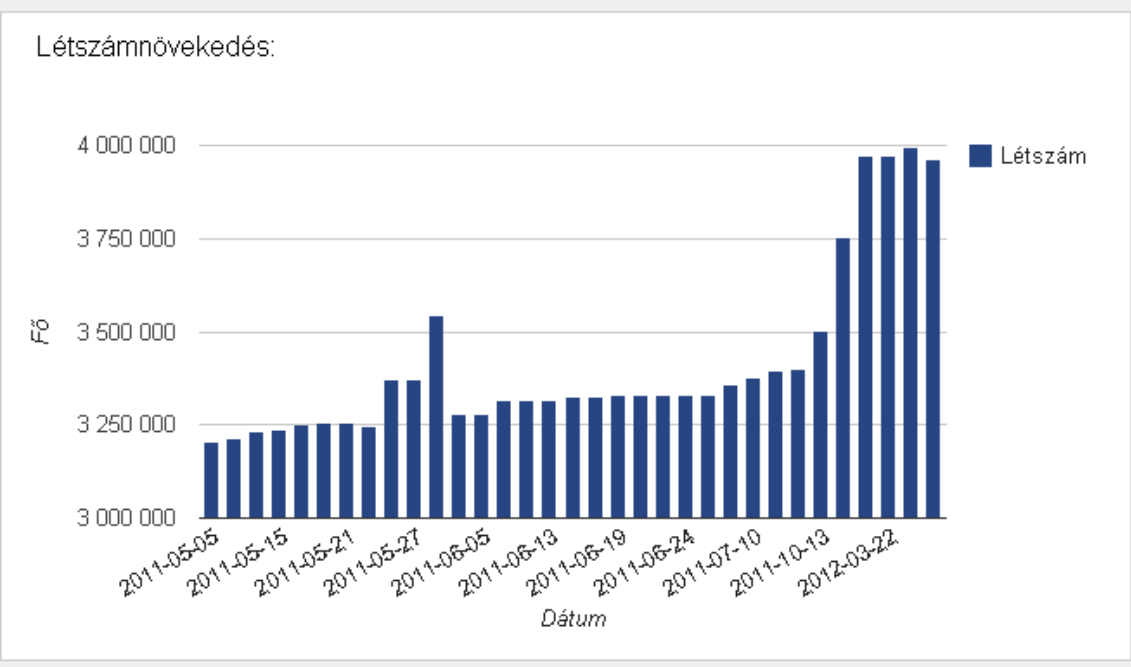
5 Összefoglalás

Elmondható, hogy az elmúlt évekhez képest a Facebookon kicsit javult a helyzet a beállítási lehetőségek terén a tárolt adatokat tekintve már kevésbé. Iwiwen nem vettem észre semmilyen változást. Mivel azonban napról napra változnak ezek a feltételek, így leginkább a trendeket érdemes figyelni.

A rengeteg felkapott botrány miatt egyre inkább nő az igény a felhasználó barátiabb feltételek iránt, de ez szöges ellentétben áll a cégek bevétel növelési szándékával. Így egyre több útmutató jelenik meg az alapvető beállításokkal, mivel eredetileg nem ezt részesíti előnyben a felület. A Facebook is arra megy rá, hogy még részletesebb adatokat tudjon a hirdetői számára biztosítani [23]. Sokat mutat az is, hogy már van olyan cég melyen keresztül halálunk után is posztolhatunk a közösségi oldalakra, illetve az, hogy Amerikában készül egy törvény mely a közösségi oldal accountokat is hagyatékként kezeli, mint egyfajta digitális vagyont [24].

Összességében azt gondolom, az ember túl sokat veszítene azzal, ha nem használná ezeket az oldalakat, olyan szempontból, hogy kimarad abból a kommunikációból, ami itt folyik. Így nem érdemes emiatt teljesen lemondani a közösségi oldalak nyújtotta előnyökről, csak ésszel kell használni, amíg valaki ki nem talál valami jobbat. Esetleg lehet remélni, hogy a törvényileg szűkebb keretek közé szorítják ezeket, és nem leszünk kiszolgáltatva a szolgáltatók jóindulatának.

Végül egy kis statisztika, hogy miből maradnánk ki. A socialtimes.hu szerint a magyar lakosság 39,65%-a fenn van a Facebookon, az internet eléréssel rendelkezők 86,2%-a. Ez mutatja az adatvédelem fontosságát illetve, hogy nem csoda, ha már sok mindent itt szerveznek meg, beszélnek le, hiszen „mindenki fenn van” [25]:



5. ábra: Az aktív magyar Facebook felhasználók száma

Irodalomjegyzék

[1] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf, 2008

[2] http://computerworld.hu/a-negyotod-nem-erzi-magat-biztonsagban-a-kozossegi-oldalakon--20120503.html, 2012. május 16.

[3] http://money.cnn.com/2011/11/03/technology/facebook_google_fight.fortune/index.htm , 2012. május 18. , csak a kép: http://i.cdn.turner.com/money/2011/images/11/02/by_the_numbers_facebook_google.jpg

[4] http://hu.wikipedia.org/wiki/Adatv%C3%A9delem

[5] http://www.sg.hu/cikkek/89483/a_facebookbol_kimaradok_sincsenek_inkognitoban, 2012. május 16.

[6] http://mattmckeon.com/facebook-privacy/, 2012. május 17.

[7] http://iwiw.hu/i/adatkezelesi-szabalyzat, 2012. május 16.

[8] https://www.facebook.com/about/privacy, 2012. május 16.

[9] http://www.ofczianka.hu/facebook/facebook-like-gomb-nyomkoveto, 2012. május 17.

[10] www.sg.hu/cikkek/84769/kijelentkezes_utan_is_figyel_a_facebook, 2012. május 18.

[11] http://lifehacker.com/5843969/facebook-is-tracking-your-every-move-on-the-web-heres-how-to-stop-it, 2012. május 18.

[12] http://www.squirrelconspiracy.net/abp/facebook-privacy-list.html, 2012. május 18.

[13] http://priv3.icsi.berkeley.edu, 2012. május 18.

[14] http://magyarinfo.blog.hu/2011/12/10/adathalasz_atveres_a_mi_az_indian_neved_alkalmazas_a_facebookon, 2012. május 18.

[15] http://www.technet.hu/hir/20110724/heti_facebookos_atveresek_norveg_robbantas_bor_alatti_pok_hamis_nevetes/, 2012. május 18. ,csak a kép: http://www.technet.hu/data/cikk/39/71/83/cikk_397183/1.jpg

[16] http://buhera.blog.hu/2010/06/05/rejtett_kepek_elerese_facebookon, 2012. május 18.

[17] http://buhera.blog.hu/2010/10/20/szeretunk_facebook, 2012. május 18.

[18] http://www.origo.hu/gazdasag/20120301-a-nagyhalaknak-volt-idejuk-felkeszulni-arra-hogyan-csusszanjanak-ki-a.html, 2012. május 18.

[18] http://www.origo.hu/techbazis/internet/20120320-meg-a-facebook-jelszot-is-elkerhetik-az-allasinterjun.html, 2012. május 18.

[19] http://www.origo.hu/techbazis/20120502-altalanos-es-kozepiskolakban-egyre-nagyobb-kerdes-hogyan-hasznaljak-a-facebookot.html, 2012. május 18.

[20] http://www.sociableblog.com/2012/02/09/facebook-fake-profiles-vs-real-users/, 2012. május 18.

[21] http://eduline.hu/felsooktatas/2012/3/8/Ujabb_botrany_Facebookjelszavakat_csaltak_k_VULC4E, 2012. május 18.

[22] http://techline.hu/it/2012/5/11/Torvenyt_hoznak_hogy_senki_ne_kerhesse_a_Fa_XVYBNH, 2012. május 18.

[23] http://socialtimes.hu/articlepage/?article=2426-reszletesebb-adatokkal-javitja-az-analitikajat-a-facebook, 2012. május 16.

[24] http://index.hu/tech/2012/04/28/a_halottak_is_posztolhatnak_a_facebookon/, 2012. május 16.

[25] http://socialtimes.hu/facebook-statisztika/, 2012. május 18.

[26] http://antivirus.blog.hu/2010/08/04/minden_amit_a, 2012. május 18.

[27]Madocsai Judit, Privacy problémák közösségi hálózatokban, http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2010/HF-reports/MadocsaiJudit.pdf, 2010