Bányász Péter[1]

A KÖZÖSSÉGI MÉDIAHASZNÁLAT BIZTONSÁGI KÉRDÉSEI A VÉDELMI IPARBAN

Rezümé:
A hadiipari vállalatok a védelmi potenciál biztosításában betöltött szerepüknél fogva kiemelt célpontjai a támadóknak, akik egyre kifinomultabb technikákat alkalmaznak a biztonsági rendszerek leggyengébb láncszeme, a felhasználók ellen. Ennek a hírszerzésnek vált a közösségi média rendkívül jól használható elemévé. Jelen tanulmány elemzi a közösségi média védelmi iparra vonatkozó kockázatait, illetve megvizsgálja egy olyan biztonsági minimumkövetelmény lehetőségeit, amelyek ajánlásként szolgálhatnak egy keretrendszer kidolgozásához.
Kulcsszavak:
közösségi média, védelmi ipar, informatikai biztonság, hírszerzés

Bányász, Péter

THE SAFETY ISSUES OF THE SOCIAL MEDIA IN THE DEFENSE INDUSTRY

Abstract:
Companies in the defence industry are frequent targets of computer hackers who are using more and more sophisticated technics against the weakest chain-link of the security systems, the users. Social media became an important platform of intelligence-gathering and counter-intelligence activity. This study analyzes the risks of using social media regarding the defence industry and examines the possibilities of a security minimum requirements.
Keywords:
social media, defence industry,IT-security, intelligence

A közösségi média alig egy évtizedes múltja alapjaiban formálta át a társadalmakat. A kezdetekben szórakoztatatásra létrehozott oldalak hamar túlléptek alapfunkciójukon, és – többek között – a politikai döntéshozatal-befolyásolás, a hírszerzés fontos elemeivé váltak. Ha figyelembe vesszük a felhasználók nagy számát, az egyes oldalakon eltöltött időt, nem véletlen, hogy kiemelt érdeklődés övezi a különböző érdekek által vezérelt támadók részéről. Ebből adódóan – munkájuk speciális természetéből fakadóan – a védelmi szférában dolgozók hangsúlyosabban jelennek meg a célpontok között.

A tanulmány kiemelten foglalkozik a védelmi ipar szereplőivel, melynek indokául a szerző kutatási területe szolgál. A védelmi ipar sajátosságából

[1] Szerző a Nemzeti Közszolgálati Egyetem Hadtudományi- és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola doktorandusza, a Magyar Hadtudományi Társaság Védelemgazdasági és Logisztikai Szakosztályának titkára, a Kritikus Infrastruktúra Védelmi Kutatások TÁMOP-4.2.1.B-11/2/KMR-0001 számú projekt, „Közlekedési Kritikus Infrastruktúra Védelme” kiemelt kutatási terület kutatója.

következően fontos szerepet tölt be egy állam védelmi potenciáljának megteremtésében, amely megköveteli az ehhez szükséges innovációk kiemelt védelmét.

Hazánk szövetségi politikájából fakadóan a védelmi ipar szereplői bizonyos szakmai, pénzügyi, gazdasági, biztonsági feltételek teljesítése esetén „NATO Beszállításra Alkalmas" minősítést szerezhetnek, ami még szigorúbb biztonsági elvárásokat követelhet meg. Ahogy a közelmúlt tapasztalatai bizonyítják, a külföldi kormányok előszeretettel használják politikai, gazdasági és ipari kémkedésre a kiberteret, ahol a védelmi ipar szereplőit, illetve azok beszállítóit támadják az elégtelen, sokszor nem létező biztonsági előírások okán.

2013 novemberében a német Spiegel magazinban jelent meg egy hír,[2] miszerint a brit Government Communications Headquarters (GCHQ), amely a kormány és a fegyveres erők információbiztonságáért, valamint SIGINT-tevékenységért felel, hamis Linkedin-t és Slashdot-ot hoztak létre, hogy közbeékelődéses támadással élve vírussal fertőzzék meg a kiszemelt oldalak rendszereit. A dokumentumok szerint a kvantumillesztés fedőnevű művelet eltérítette a hamis weboldalakra a látogatókat, amelyek végül vírussal fertőzték meg.

A különböző titkosszolgálatok rendszeresen használják a közösségi oldalakat hírszerzésre, még pedig roppant kreatív módon.

A hatályos magyar jogszabályokban jelenleg nem létezik egy keretrendszer, amely ajánlással élne a közösségi média használatát illetően.

A tanulmány célja annak vizsgálata, hogy megalkotható-e egy olyan szabályozó, amely a fent nevesített biztonsági rést képes betömni, és amennyiben igen, milyen tartalmai elemeket szükséges belefoglalni. Ennek érdekében – a közösségi média fejlődésének bemutatását követően – ismertetjük az eszközeit, valamint meghatározzuk az egyes alkalmazásokhoz kapcsolódó kockázatokat. Ezt követően elemezzük a kockázatokat és fenyegetettségeket a védelmi szféra különböző területein, amelyek a közösségi média használatából származhatnak, kiemelten a védelmi ipar szereplőire.

A közösségi média használatnak számos negatív hatása van a pozitívumok mellett. Jelen tanulmány keretei nem biztosítanak lehetőséget, hogy minden területre terjedően vizsgáljuk a kockázatokat. Így a kutatás elsősorban a felhasználók adatbiztonságára, a felhasználókon keresztül történő információszerzésre fókuszál.

A közösségi médiahasználat trendjei

Egy tudományos probléma megválaszolásában talán az egyik legnagyobb nehézséget a fogalmak értelmezése jelenti. Amennyiben egy közel évtizedes múlttal bíró fogalomról beszélünk, amely beszivárgott életünk minden területére, még bonyolultabbá válik a definíció, hiszen mást értenek alatta a különböző szakmák képviselői.

[2] SOTTECK, T. C.: British intelligence reportedly intercepted LinkedIn and Slashdot traffic to plant malware. In The Verge, 2013. november 10. http://www.theverge.com/2013/11/10/5088048/british-intelligence-gchq-linkedin-slashdot-quantum-insert (2013. november 11.)

A közösségi média fogalmát számos (elsősorban marketinggel foglalkozó) szerző próbálta meghatározni, ebből következően alapvetően marketinghez kapcsolódó fogalmakkal tarkítva. Heidi Cohen marketing szakértő 30 ilyen közösségi médiadefiníciót gyűjtött össze.[3] Az Oxford Dictionaries a közösségi médiát weboldalak és alkalmazások összességeként írja le.[4] Ezek böngészése során a felhasználók tartalmakat készíthetnek és oszthatnak meg a közösségi hálózatokon. Ehhez a definícióhoz köthetők az Andreas Kaplan és Michael Haenlein által megfogalmazottak, miszerint a közösségi média „*… internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom*”.[5]

Jelen tanulmány szerzője – elfogadva, de mégis kiegészítve a fenti meghatározást – a közösségi média alatt olyan internetes oldalak és alkalmazások összességét érti, amelyeknél a szolgáltató csupán a keretet biztosítja, a tartalmat a felhasználók állítják elő. Ebből következik, hogy a közösségi média elsősorban a felhasználók interakciójából alakul ki, amely a többi felhasználó megosztásaiból, kiegészítéseiből akár részben, akár teljesen új tartalom előállítását jelentheti. Elméletileg ez a tartalom folyamatosan változhat, kiegészülhet, új információk hatására bővülhet.

Látszólag nincs minőségi változás a két megfogalmazás között. Ha azonban elfogadjuk az általunk javasoltakat, kibővül a közösségi eszközök köre. Ez alapján a szerző a közösségi médiához sorolja a különböző okostelefonokra írt alkalmazásokat is, hiszen egyrészt ezek is a felhasználók közti interakcióra épülnek, másrészt integratív szerepet töltenek be a különböző közösségi eszközök között. Ez alapján a közösségi média eszközeinek tekintjük a blogokat és mikroblogokat, a közösségi hálózatokat, videó- és fényképmegosztó oldalakat, hírmegosztó oldalakat, közösségi szerkesztésű tudásbázisokat, közösségi játékokat. Ez csupán egy rövid felsorolása az egyes eszközöknek, mert egyre több oldal jön létre a közösségi média alapján (közösségi vásárlás, közösségi akció, információ-aggregációs oldalak, szolgáltatás és termékvéleményező oldalak stb.), itt csupán a legjelentősebbeket igyekeztünk felvázolni.

Az integráció okát gazdasági szempontok magyarázzák, ugyanis rendkívül nagy és folyamatosan bővülő reklámpiacról beszélhetünk. Ebből következően óriási verseny van a nagy szolgáltatók közt, állandó innovációra kényszerítve a szereplőket. Annak a vállalatnak, amelyik nem képes folyamatosan megújulni, romlanak piaci pozíciói. A magyar fejlesztésű IWIW története remekül példázza ezt az állítást, hiszen megmerevedett struktúrájából következően képtelen volt felvenni a versenyt globális szinten. Nem véletlen tehát, hogy a nagy cégek az internet szerepét akarják átvenni.

Szükségesnek mutatkozik egy kis kitérés, ugyanis érthetőbbé teszi, miért bírnak kiemelt érdeklődést a nagy online szolgáltatók. Említettük a reklámbevételekért folytatott harcot. Ahhoz, hogy minél pontosabban célozzák

[3] COHEN, Heidi: 30 Social Media Definitions. In HeidiCohen.com, 2011. május 9. http://heidicohen.com/social-media-definition/ (2013. november 24.)

[4] Definition of social media in English. In Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/social-media (2013. november 24.).

[5] KAPLAN, Andreas – HAENLEIN, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010

meg a felhasználókat, a cégek rengeteg információt gyűjtenek a felhasználói szokásokról. A Facebook közel 10 000 szempontot vesz figyelembe az adatgyűjtés során, de a Google sem marad le ezen a téren.

Ha figyelembe vesszük, hogy egy átlagos felhasználó hány Google-szolgáltatást használ napi szinten (e-mail, térkép, videó- és képmegosztó, Androidos okostelefon, naptár, felhőszolgáltatás, közösségi hálózat stb.), az ezeken való aktivitás mind naplózásra kerül a rólunk vezetett adatbázisban. Nem túlzás kijelenteni, a teljes online jelenlétünk ismert lehet a cégeknek, amelyekhez való hozzáférés nem csak a cégeknek jelent kincset, de a különböző hírszerző szolgálatoknak is.

Az egyes közösségi oldalak ismertetésére, részletes bemutatásukra – terjedelmi korlátok miatt – a jelen tanulmányban nincs lehetőség.[6]

Ha kockázatokról és fenyegetettségekről beszélünk, elengedhetetlen, hogy ne határozzuk meg azokat a mutatókat, ami alapján állításainkat megfogalmazzuk. Amennyiben a közösségi média használatából eredő veszélyeket elemezzük (függetlenül magától a fenyegetés típusától), elengedhetetlen a statisztikai adatok ismertetése, amelyek a közösségi oldalak látogatottságára vonatkoznak.

Magyarországi viszonylatban részletes „up to date", azaz friss statisztikával sajnos nem rendelkezünk a különböző közösségi oldalak elterjedtségéről.[7] A „legfrissebb" nyilvános kutatások közelítenek az egyéveshez, ami egy ilyen dinamikusan fejlődő terület esetében – megítélésünk szerint – nem használható. Így a nemzetközi trendekből szükséges levonni a konzekvenciákat.

Az Ipsos 2013 novemberében publikálta az internet használatát vizsgáló nemzetközi közvélemény-kutatásának eredményeit.[8] Ebből kiderül, hogy bár számtalan oldal közül választhatnak a felhasználók, alapvetően három kategóriát használnak rendszeresen: a Google szolgáltatásait, a közösségi oldalakat és a különböző webes levelezőket. Ez alapján világszerte az internetezők 74%-a használja hetente legalább egyszer a Google-t (Magyarországon ez 67%), a közösségi oldalak látogatottsága 64%-nak felel meg (hazánkban ez magasabb, 78%), míg levelezés aránya a globális elterjedtség tekintetében 55% (Magyarországon 68%-ra tehető).

Ha a fentieket kiegészítjük a Világbank adataival, ami alapján a magyarországi internethasználatot 100 emberből 72 főre méri,[9] legitimnek véljük a módszertant, ami alapján a magyarországi közösségi média használatot a nemzetközi adatokból származtatva megegyezőnek becsüljük.

---

[6] Ezt a szerző korábban elvégezte több tanulmányában. (l. *A közösségi média szerepe a katasztrófaelhárításban a Sandy - hurrikán példáján keresztül.* [In. Fejezetek a kritikus infrastruktúra védelemből. Magyar Hadtudományi Társaság, Budapest, 2013., pp. 281–292. old.], *A közösségi média szerepe a 21. század hadseregeiben.* Hadtudomány, 2012/1–2. 152–161. old.).

[7] Például szociológiai tényezők alapján lebontva.

[8] A különböző internetes oldalak három típusát látogatja heti rendszerességgel a netezők többsége. IPSOS, 2013. november 5. http://www.ipsos.hu/site/a-k-l-nb-z-internetes-oldalak-h-rom-t-pus-t-l-togatja-heti-rendszeress-ggel-a-netez-k-t-bbs-ge/ (2013. december 3.)

[9] Internet users (per 100 people). World Bank, 2012 http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=default (2013. december 3.).

Egy 2013-as, az internetezési szokásokat vizsgáló, kettőezer magyar felnőtt interjújából készült felmérés alapján 2012. első negyedévében a 18 éves, vagy ennél idősebb népesség 38 százaléka volt tagja valamelyik közösségi oldalnak, ami egy év alatt 250 ezer fővel növekedve 41%-ot ért el az idei év azonos időszakában, megközelítette a 3 és félmillió főt.[10]

A közösségi eszközök használata továbbra is sokkal jellemzőbb a fiatalabb (40 év alatti) korcsoportokra, amelyeken belül a népesség többségének van valamilyen közösségi oldalhoz köthető tagsága. De aktívnak mondható ebből a szempontból a 40–49 évesek jóval több, mint egyharmada is (43%), illetve az 50–59 évesek több mint negyede (28%), valamint a 60 év felettiek egytizede is.

2012-ben az átlag magyar felhasználó naponta 207 percet internezett,[11] ami – kiegészítve egy 2013-as, a közösségi média használatára vonatkozó felméréssel – jól mutatja ezen oldalak népszerűségét (l. 1. táblázat).[12] Nemzetközi viszonylatban az átlag felhasználó naponta 3,6 órát töltött el valamilyen közösségi oldalon, addig Magyarországon ez 2,8-t jelent, ami megegyezik a nemzetközi viszonylatban az 50 év felettiek átlagos közösségi médiahasználatával. A 35 év alatti korosztály esetében mind Magyarországon, mind globálisan naponta 4,2 órát töltünk valamilyen közösségi oldalon, ami az átlagos internethasználat releváns része.

Korcsoport	Nemzetközi viszonylat (óra)	Hazai viszonylat (óra)
Átlag	3,6	2,8
35 év alatt	4,2	4,2
35-49 év	3,1	3,1 körül
50 év fölött	2,8	2,3

1. táblázat
Közösségi média használattal töltött idő
(saját szerkesztés, forrás: Ipsos)

A tanulmánynak nem célja a különböző közösségi alkalmazások látogatottságának mélyebb elemzése, de fontos látni, hogy a különböző oldalak látogatottsága kultúrafüggő. Míg a nyugati országokban a legnépszerűbb oldalak a Facebook, Twitter (2. táblázat),[13] addig globálisan többüket megelőzik

[10] Félmillióval nőtt a Facebook tábora egy év alatt. Mediameter, 2013. június 14. http://mediameter.hu/kutatasok-elemzesek/mediameter-felmillioval-nott-a-facebook-tabora-egy-ev-alatt/ (2013. december 7.)

[11] Egyre nő az internethasználat Magyarországon. GfK, 2012. június 10. http://www.gfk.hu/pressreleases/press_releases/articles/010194/index.hu.html (2013. december 8.)

[12] A közösségi média úgy vonzza az embereket, mint fény a pillangókat. IPSOS, 2013. január 10., http://www.ipsos.hu/site/a-k-z-ss-gi-m-dia-gy-vonzza-az-embereket-mint-f-ny-a-pillang-kat/ (2013. december 8.)

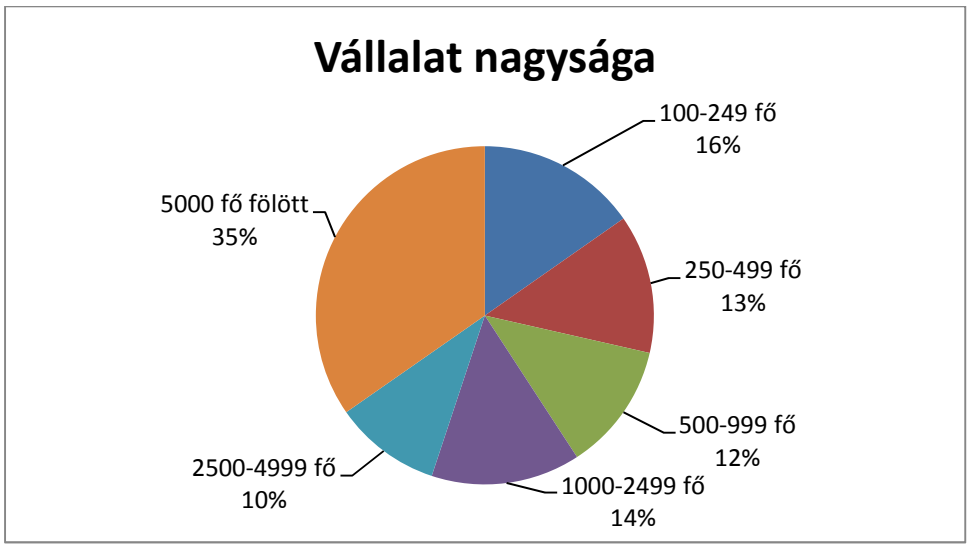
[13] AJMERA, Harsh: Social Media facts, figures and statistics 2013. Digital Insights, 2013. szeptember 4. http://blog.digitalinsights.in/social-media-facts-and-statistics-2013/0560387.html (2013. december 8.)

az olyan nyugaton kevésbé ismert oldalak, mint a kínai Sina Weibo, a Qzone és a Tencent.[14]

Közösségi oldal	Felhasználók száma
Facebook	1,15 milliárd fölött
Twitter	500 millió fölött
Google +	500 millió fölött
LinkedIn	238 millió fölött
Instagram	130 millió fölött
Pinterest	70 millió fölött

1. táblázat
Közösségi oldalak a felhasználók száma alapján 2013-ban
(saját szerkesztés, forrás: Digital Insights)

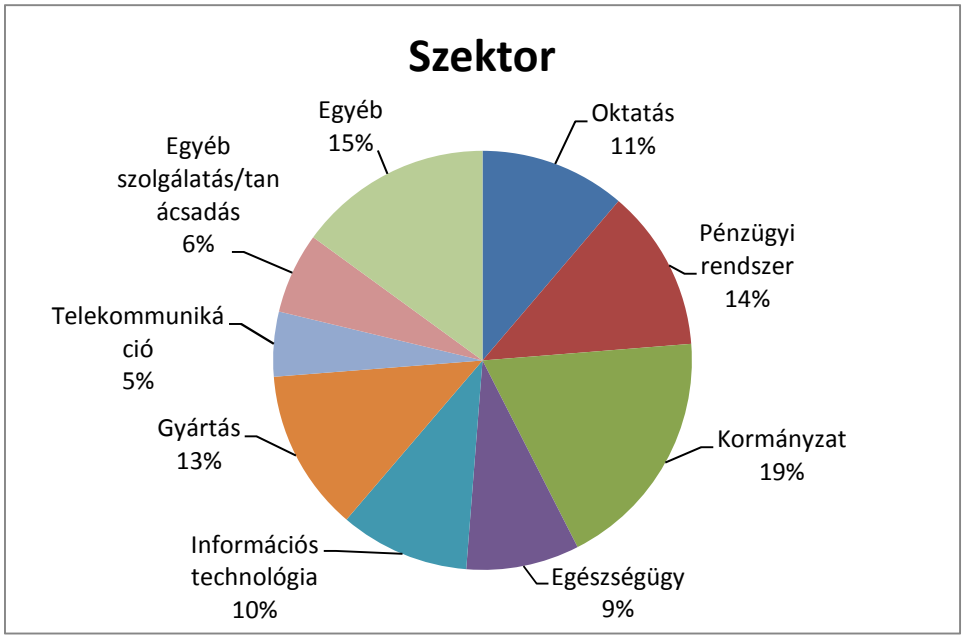
Ami esetünkben a statisztikai adatok tekintetében igazán relevanciával bír, az a munkahelyeken történő közösségi médiahasználat. Egy 2013-as, 32 országra kiterjedő vizsgálatból számos tanulságot vonhatunk le erre nézve.[15] A közel 10 ezer válaszadó 15%-a dolgozott olyan vállalatoknál, amely 100 és 249, 13%-uk 250 és 499, 12%-uk 500-999, 14%-uk 1000-2499, 10%-uk 2500-4999 és 34%-uk 5000 főnél több személyt foglalkoztat (1. ábra).



1. ábra
Felhasználók megoszlása a vállalat nagysága alapján
(saját szerkesztés)

A megkérdezettek szektor szerint eloszlását a 2. ábráról olvashatjuk le:

[14] BULLAS, Jeff: 5 Insights into the Latest Social Media Facts, Figures and Statistics. Jeffbullas.com, 2013. június 4. http://www.jeffbullas.com/2013/07/04/5-insights-into-the-latest-social-media-facts-figures-and-statistic/ (2013. december 8.)
[15] Social Tools in the Workplace. Microsoft, 2013. május 6. http://www.microsoft.com/enterprise/it-trends/social-enterprise/articles/Social-Tools-in-the-Workplace-Infographic.aspx#fbid=y6bL-YMGQle (2013. december 8.).



2. ábra
Felhasználók megoszlása a szektor alapján
(saját szerkesztés)

A válaszadók 46%-ának önbevallása szerint nőtt a produktivitása a közösségi média használata következtében. 34%-uk szerint a vezetők alábecsülik a közösségi oldalak munkahelyen való használatának előnyeit, míg 37%-uk úgy gondolja, ha a vezetőség támogatná a közösségi média használatot, hatékonyabb munkavégzésre lenne képes. A korcsoportos bontásban hasonlóságokat fedezhetünk fel e téren: míg a 18–24 év közöttiek 46%-a, a 25–34 közöttiek 45%-a, a 35–44 közöttiek 39%-a, a 45 év felettiek 28%-a vélekedik hasonlóan.

A vállalatok általában a produktivitás csökkenésével, illetve biztonsági megfontolásokkal indokolják a közösségi oldalak használatának tiltását. A megkérdezettek nemek szerinti bontásából kiolvasható, hogy a férfiak nagyobb hányadának (71%) akadnak biztonsági aggályai, mint a nőknek (65%), míg a termelékenység csökkenésétől a nők nagyobb számban (61%) tartanak, mint a férfiak (56%).

A válaszadók 28%-a ismer olyan munkatársat, akik figyelmen kívül hagyják a vállalat IT-biztonságra vonatkozó előírásait a céges számítógépein és telefonjain, míg 17%-uk vallotta be, hogy nem tartják be ezen előírásokat. Ez korcsoport szerint megoszlásban közel kétszer annyira valószínű a 18–24 év közöttiekre (30%), mint a 35–44 év közöttiekre (16%), valamivel több, mint háromszorosa a 45 év fölöttiek esetében (9%), illetve 7%-al magasabb, mint a 25 és 34 év közöttiek esetében. Az ismertetett statisztikai adatok megítélésünk szerint érzékeltetik a közösségi média elterjedtségét és helyét a felhasználók életében.

Nem telik el nap, hogy ne értesülnénk valamilyen állami vagy piaci szereplőt ért kibertámadásról. A támadók célja a lehető legtöbb információ megszerzése, legyen szó a rendszer sebezhetőségéről vagy katonai, gazdasági, politikai titok megismeréséről, amelyet valamilyen érdekérvényesítés során használnak fel. A védelmi ipar szereplői az általuk kezelt információk okán kiemelt célpontjait jelentik a támadóknak. Az ily módon

megszerzett érzékeny információkat felhasználhatják saját iparuk fejlesztésére, valamint az ellenség védelmi rendszereinek kijátszására. Ennél fogva nagyobb szerepet kell szánni a védelmi ipar információbiztonsági követelményeinek megalkotására, amely nem nélkülözheti a közösségi média használatra vonatkozó iránymutatásokat.

A Symantec évről évre (idén már a 18-adik alkalommal) adja közre az internetbiztonságot vizsgáló jelentését. A 2012-es trendeket elemezve egy érdekes változást olvashatunk ki:[16] a 250 főnél kevesebb munkavállalót foglalkoztató KKV-k váltak a támadások leggyakoribb célpontjaivá, letaszítva a kormányzati szereplőket az első helyről. A jelentés szerint nem a cégvezetők szerepelnek elsősorban a támadók célpontjaik közt, hanem a szellemi termékeket előállító alkalmazottak, így a mérnökök, szakértők, esetleg a vállalat kereskedelmi osztályának dolgozói.

Mindezekből megfogalmazhatjuk: az elsődleges célpont a felhasználó. Mivel a felhasználó ember, legyen szó bármilyen biztonságos rendszerről, bármilyen alapos, szigorú biztonsági előírásról, mindig lesz legalább egy gondatlan felhasználó, aki miatt sebezhetővé válik a legalaposabban felkészített biztonsági rendszer.

A következő fejezetben látni fogjuk, nem csupán az adathalászat, a social engineering jelenti a veszélyeket a közösségi média használatára, hanem a kormányzati hírszerzés növekvő képessége is.

A közösségi média használatából eredő kockázatok és fenyegetettségek a védelmi iparban

A kockázatok, kihívások, fenyegetések olyan veszélyt jelentő állapot jelentenek, amelyek negatívan befolyásolják az adott ország biztonságát, annak összetevőit. Azonban más-más veszélyek jellemzik a közigazgatást, a rend- és honvédelmet, valamint a nemzetbiztonsági szerveket vagy a védelmi ipar szereplőit. A kibertérből érkező támadások száma, kifinomultsága erősödő tendenciát mutat, így ismernünk kell a közösségi média használat védelmi szférára specializált kockázatait, különös tekintettel a védelmi iparra.

A már idézett, 2012-re vonatkozó internet biztonsági jelentés kapcsán fogalmazta meg Teasdale Harold, a Symantec magyarországi és szlovéniai országmenedzsere: „*A támadások egyre kifinomultabbak, az IT-szektor fejlődése pedig egyre összetettebb újdonságokat szül – ez a kettős tendencia proaktív viselkedésre kényszeríti a vállalkozásokat. Az információrobbanás, a virtualizáció, a mobilitás, a felhőalapú technológiák és általában az IT egyre szélesebb körű felhasználása miatt a cégeknek teljes mélységében kell átgondolniuk a biztonsági óvintézkedéseket annak érdekében, hogy a jövőben is a támadók előtt tudjanak járni.*”

Ezt erősíti egy, szintén a Symantec által közzétett jelentés, amit minden hónap tapasztalatainak feldolgozásából állít össze a cég:[17] 2013 szeptemberére

[16] Internet Security Threat Report 2013 Vol. 18. Symantec, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (2013. december 8.)

[17] SYMANTEC CORPORATION: Symantec Intelligence Report. 2013. September, In. Symantec,

bár csökkent kibertámadások száma, a módszerek sokkal kifinomultabbá, hatékonyabbá váltak. A célpontok – elsősorban az újonnan megjelent kártevők és újonnan alkalmazott technikák tekintetében – továbbra is a KKV-k maradtak.

Miközben a KKV-k sok esetben úgy gondolják, nem kell tartaniuk kibertámadástól, megfelelő infrastruktúra és biztonsági protokoll hiányában könnyű és jövedelmező célpontjai a támadóknak. A Symantec 2013. szeptemberi jelentése is kiemeli, a 2012-ben nagy arányban támadott hadi- és gépipari vállalatok voltak a hackerek kiemelt célpontjai. A nagyvállalatok, levonva a megfelelő konzekvenciákat, fokozatosan növelték védekezési képességeiket a kibertámadások elhárítására. A támadók a változó feltételekhez igazodva a beszállítói láncok sérülékenyebb, kevésbé védett pontjaira, a kisebb szolgáltató vállalatokra összpontosították akcióikat, hogy onnan terjeszkedjenek tovább a beszállítói lánc "értékesebb" tagjai felé.

A Symantec jelentéséből kiderül, hogy a sikeres célzott támadások előtt a rosszindulatú programok készítői megfigyelik az áldozatukat. Ennek érdekében roppant alapos nyílt forrású felderítést végeznek: megpróbálják kideríteni az e-mail címét, barátainak nevét, érdeklődési körét – bármilyen információt, ami alapján a felhasználói szokásokat kihasználó, social engineering támadást indíthatnak, amelyhez a közösségi média rendkívül nagy segítséget nyújthat a felkészült támadóknak.

De nem csak a social engineering jelent kockázatot a vállalatoknak. Sok esetben a kormányok állnak a támadások mögött. A már említett PRISM-botrány nem hagy kétséget a felől, hogy a nagy online szolgáltatók által megszerzett adatokat gazdasági hírszerzésre is felhasználják, ahogy a kereken 25 esztendővel korábban kirobbant Echelon-botrány esetében bizonyossá vált.[18] Emlékezetes, R. James Woolsey, a CIA akkori igazgatója az ily módon megszerzett információkat úgy védte, hogy ezzel az USA csupán esélyegyenlőséget teremt a gazdasági versenyben, ugyanis a francia kormány és a francia hadiipari vállalatok megvesztegetéssel szereznek új ügyfeleket. Egy az Európai Parlament által 2001-ben közzétett jelentés[19] szerint 1993 és 2000 között 25–30 ezermilliárd dollárnyi olyan üzlet jött létre az USA és más országok között, ahol az eredeti partnert az Echelonnal szerzett információk segítségével került helyzeti előnybe az Egyesült Államok.[20]

A különböző platformok elterjedtsége okán nem hagyhatjuk figyelmen kívül a mobileszközök sérülékenységét. A Symantec 2012-es jelentése megállapítja, hogy tavaly 58 százalékkal nőtt a mobiltelefonokra tervezett kártevők száma. A személyes információk (például e-mail címek és telefonszámok) eltulajdonítására irányuló mobilfenyegetések 32 százalékát teszik ki a támadásoknak. Ennek okait nem a mobilos sérülékenység 30 százalékos növekedésében kell keresni. Míg az Apple iOS esetében tudunk a legtöbb dokumentált sérülékenységről, addig ezen a platformon mindössze egyetlen fenyegetést regisztráltak a tavalyi év folyamán. Ezzel szemben az

---

http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_09-2013.en-us.pdf (2013. december 8.)

[18] CAMPBELL, Duncan – HONIGSBAUM, Mark: Britain and US spy on world. The Guardian, 1999. május 23.
http://www.duncancampbell.org/menu/journalism/guardian/britain.pdf (2013. december 03.)

[19] Temporary Committee On The Echelon Interception System Directorate-General For Committees And Delegationsbrussels Meeting. 2001. január 22–23.

[20] Többek között műholdrendszerek, repülőtenderek, telekommunikációs- és vegyipari fejlesztések, energiatermelés, szemétfeldolgozás stb.

Androidon, mely kevesebb sérülékeny ponttal rendelkezik ugyan, több támadás volt, mint bármely más mobil operációs rendszerben. Az Android piaci részesedése, a nyitott platform és a szerteágazó terjesztési modell miatt ez a felület jelenti a legvonzóbb célpontot a támadók számára. További okként lehet megfogalmazni a nagyobb volumenű támadást az Androidos programok esetében, hogy míg az App Store-ba való alkalmazás feltöltését szigorú biztonsági követelményeknek kell megfeleltetnie a program fejlesztőének, addig a Google Play esetében bárki feltölthet bármilyen alkalmazást, ellenőrzés nélkül.

Mindezek alapján, úgy vélem, kijelenthetjük, hogy a védelmi iparra specializált cégek kiemelt célpontoknak számítanak a kiberbűnözők számára. De milyen mértékű a magyar védelmi ipar kockázata? A Magyar Védelmiipari Szövetség katalógusa alapján 33 védelmi ipari céget vizsgáltunk meg az alkalmazottak száma alapján (l. 3. táblázat).

Létszám	**Vállalatok száma**
1–10	5
11–50	14
51–250	10
251–2000	1
2000 fölött	1[21]
Nincs adat	2
Összesen	**33**

2. táblázat

Magyar védelmi ipari vállalatok az alkalmazottak száma alapján
(Saját szerkesztés. Forrás: Magyar Védelmiipari Szövetség 2012-es katalógusa)

A 3. táblázatban csupán a foglalkoztatottak létszáma alapján végeztük el a csoportosítást. Az árbevétel – véleményünk szerint – irrelevánsnak tekinthető abban a tekintetben, hogy a cég milyen biztonsági stratégiát követ, de feltételezzük, a nagyvállalatok nagyobb arányban alkalmaznak valamilyen IT-biztonsági protokollt.[22] Az adatokból kiolvasható, hogy a 33 vállalatból 29 minősül KKV-nak, ezen belül 5 mikrovállalkozásként, 14 kisvállalkozásként értékelhető. A 33 vállalatból 19 rendelkezik NATO beszállítói minősítéssel.[23] Figyelembe véve a Symantec 2012-es jelentését, ami a KKV-kat jelölte meg elsődleges áldozatként, magukat a magyar védelmi iparban pozícionált vállalatok 87%-a tartozik bele a primer célpontok közé.

A Symantec jelentései elsősorban a „watering hole”-t és a „spear pfishing”-et, nevesítik, mint a támadók által leggyakrabban használt módszert. Ezen kívül léteznek egyéb „phishing”, azaz adathalász technikák, mint „whaling”, a „sniffing”, "sniffer”, „keylogging”, trójai falovak alkalmazásával.

[21] HM EI Zrt. 4000 alkalmazottal

[22] KIRÁLY László – PATAKI István: Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz. Hadtudomány 2013/1. elektronikus szám, http://mhtt.eu/hadtudomany/2013_e_Kiraly_Laszlo_Pataki_Janos.pdf (2013. december 11.)

[23] Aktuális NATO Beszállítói céglista. NATO Beszállítói Információs Honlap, http://www.natotender.gov.hu/aktualis_nato_beszallitoi_ceglista/ (2013. december 9.)

Javaslat a közösségi média használatra vonatkozó biztonsági minimumkövetelmények kialakítására

Elemezve a közösségi média használatból eredő kockázatokat, meg kell határozni azokat a követelményeket, amelyek egyfajta biztonsági minimumként jelentkezhetnek. Max Weber fogalmi meghatározását kölcsönözve külön kell kezelni a „sollen", azaz „mi legyen", illetve a „sein", azaz „mi a lét" kérdéseit a védekezés tekintetében. Amennyiben ezt elmulasztjuk, akkor papíron megalkothatjuk ugyan a legszigorúbb biztonsági előírást, de ha az nincs köszönőviszonyban a valós élettel, akkor ugyanúgy sebezhetőek maradunk. Megítélésünk szerint a teljes tiltás kivitelezhetetlen, éppen ezért a követelményrendszer felállítása mellett legalább olyan fontos a felhasználók oktatása, információ- és adatbiztonságra vonatkozó érzékenységük megteremtése.

Elöljáróban le kell szögezni, nem létezik, nem is létezhet 100%-osan biztonságos rendszer. Hatványozottan igaz a kijelentés a közösségi média esetében, amikor nem csak egy eszközön vannak jelen, hanem számos platform kínál hozzáférést (számítógép, okostelefon, tablet stb.). Ez a fajta átjárhatóság nem csak azért nehezíti meg a szabályozást, mert azt különböző eszközökre kell kiterjeszteni, amelyekre adott esetben nem léteznek jól működő védelmi rendszerek (pl. vírusirtó, tűzfal). A hordozhatóság megteremti a lehetőségét annak, hogy bár munkahelyi számítógépen nem férünk hozzá a közösségi oldalakhoz, egy saját telefon vagy tablet esetében, amelyet munka közben használhatunk az esetleges tiltások ellenére, ugyanúgy információkat szolgáltathatunk ki magunkról.

További nehézséget okoznak a munkavégzés sajátosságából fakadó jellemzők, amelyek elsősorban a szellemi munkát végzők esetében jelentkeznek. Az nevezetesen, hogy összemosódik a szabadidő a munkaidővel. Ez nem csupán azt jelenti, hogy munkaidőben élünk magánéletet (többek között a közösségi oldalak látogatásával), hanem azt is, a munkaidő lejárta után is munkahelyi kötelezettségeivel foglalkozunk. Egy reprezentatív felmérés[24] szerint a 18 és 69 év közti, hetente többször internetező munkavállalók esetében 58%-ra tehető azok aránya, akik munkaidőn túl, akár szabadság alatt, még a családi programot is háttérbe szorítva dolgozik.

Mindezeket figyelembe véve, felmerül a kérdés, hogyan szabályozhatunk, hogyan fogalmazhatunk meg biztonsági követelményeket, amelyet az érintettek elfogadnak és be is tartanak? A jogalkotás alapja, hogy a törvényhozó hatalom által elfogadott norma betartását a végrehajtó hatalom a legitim erőszak monopóliumával kikényszerítheti. Első olvasatra amilyen egyszerűnek tűnik ez az állítás, a valóságban olyan bonyolult. Ha egy megalkotott törvény a társadalom többségénél nem képes legitimációt szerezni, legyen az államnak bármilyen szigorú válasza (rendszeres rendőri ellenőrzés, szigorú bírói ítéletek), az állampolgárok többsége nem fogja betartani a törvényt. Napjainkban az internet szabályozására tett kísérletek mutatnak azonosságokat.

[24] A netező magyaroknak nincs külön munka és pihenés. Híradó, 29. http://www.hirado.hu/Hirek/2013/10/28/15/A_netezo_magyaroknak_nincs_kulon_munka_es_pihenes.aspx (2013. december 10.)

Az internet szabályozásával kapcsolatban is hasonló harc folyik a különböző érdekcsoportok közt, amit a SOPA, PIPA, ACTA törvénytervezetek világítanak meg leginkább. A szerzői jog megsértése és hamisítás visszaszorítása érdekében a nagy jogvédő cégek olyan törvények elfogadása érdekében lobbiznak, amelyet a biztonság oldaláról tematizálnak, és a terrorizmussal, a pedofíliával és egyéb hívószavakkal indokolnak. Az említett törvénytervezetek eddig folyamatosan elbuktak a felhasználók tiltakozásai hatására. Ebben nem kis szerepet vállaltak a Google-höz, Facebook-hoz hasonló ellenérdekű nagyvállalatok.[25]

Egyetértés mutatkozik arra nézve, hogy a társadalmunk az információ szabad áramlásán alapul, amelyet a szólásszabadsághoz való alapjoggal egyenértékűnek tekintenek a demokratikus berendezkedésű államokban. Megítélésünk szerint amennyiben egy állam megpróbálná törvényileg tiltani az olyan jellegű oldalak látogatását, amelyek, az emberek mindennapjában folyamatosan jelen vannak az első fejezetben ismertetett látogatottsággal, bizonyos, hogy a tiltás kontraproduktív lenne. A Pentagon 2007-ben megtiltotta az amerikai katonáknak a közösségi oldalak használatát, de végül 2010-ben, 7 hónapos vizsgálat eredményeként feloldották a korlátozást, belátva annak eredménytelenségét.[26] Reményeink szerint mindezek igazolják, hogy egy, a közösségi médiára vonatkozó szabályozás nem képezheti elemét a használatát tiltó rendelkezések.

A veszély ennek ellenére valós, a védekezés elengedhetetlen. A következőkben megvizsgáljuk, milyen pontokat célszerű beépíteni egy ilyen jellegű keretrendszerbe. Az első védelem minden esetben az infrastruktúrára kell, hogy vonatkozzon. A támadók tevékenységének egyik fő iránya az adathalászat, amelyhez kémprogramokat igyekeznek az informatikai eszközünkre telepíteni. Elengedhetetlen a megfelelő fizikai védelem, vírusirtó, antivírus program, tűzfal használata, de célszerű a különböző internetes böngészőkre fejlesztett kiegészítőket is alkalmazni,[27] amelyek védelmet nyújthatnak a fertőzött oldalak betöltése vagy az adathalászat ellen. Nem szabad elhanyagolni a programokhoz kiadott frissítések telepítését sem, hiszen számos esetben használják ki a programoknál feltárt sérülékenységet.[28] Ahogy a korábbiakban bemutattuk, a munkaidő végeztével otthon folytatjuk az elkezdett munkákat vagy készülünk elő a következő feladatokra. Ebből következően ezt a fajtat védelmet nem csupán a munkahelyen kell alkalmazni, hanem az otthoni eszközökön is érvényesíteni szükséges.

A második lépcső a felhasználói tudatosság növelését jelenti, hiszen a támadások legtöbb esetben a naiv felhasználóra és az emberi gyengeségre építenek. Információt nem csak a számítógépre telepített kémprogrammal lehet szerezni, hanem social engineering útján is. A támadók ezt többféleképpen érhetik el. Minél több időt töltünk el az interneten (legyen szó munkáról, szabadidőről), aktivitásunkat naplózza az internetszolgáltató, de a tartalomszolgáltató is. Ha valaki képes összegyűjteni a különböző

[25] Természetesen ezeknek a vállalatoknak is komoly gazdasági érdekeik fűződtek a törvénytervezet bukásához, de érvrendszereiket az internet szabadságának védelmére építették.

[26] Újra használhatják a közösségi portálokat az amerikai katonák. Sg.hu, 2010. március 2. http://m.sg.hu/cikk.php?cid=72827&cim=ujra_hasznalhatjak_a_kozossegi_portalokat_az_amerikai_katonak (2013. december 11.)

[27] Például Web of Trust, Better Privacy.

[28] Lásd a különböző Flash, Java „0-day” sérülékenységeket.

tevékenységeinket az egyes meglátogatott oldalaknál (milyen videókat, képeket néztünk, milyen kulcsszavakra kerestünk rá, kikkel váltunk szöveges üzeneteket), hozzájuthat rengeteg információhoz, amivel esetleg zsarolni lehet a célszemélyt.

Ezt egészítik ki az okostelefonokra készített alkalmazások, ugyanis a felhasználási feltételekhez hozzátartozik, hogy bizonyos fokú hozzáférést engedélyez a telefonon levő adatokhoz. Ha a legnépszerűbb és előre telepített alkalmazásokat vesszük alapul, akkor az alábbi adatokhoz biztosítunk hozzáférést: személyes adatok (névjegyadatok), tartózkodási hely (hálózatalapú és GPS alapú helymeghatározás), hálózati kommunikáció (teljes internet hozzáférés), fiókok adatai (üzenetek olvasása), tárhely (lehetőség az USB-tároló tartalmának módosítására vagy törlésére), telefonhívások, hardvervezérlők (fénykép- és videókészítés, hangrögzítés), rendszereszközök (szinkronizálás). A felsoroltak mindegyike a Facebook használatához szükséges.

A célszemély megfigyelését segíti elő a cookie-khoz való hozzáférés. Ennek segítségével lehetőség nyílik kiszűrni egyes személyek online kommunikációját, adott esetben feltörni számítógépét.[29]

Ne feledjük, ezekhez az adatokhoz nem csak a Facebook fér hozzá, hanem akár az egyes titkosszolgálatok is. Hogy mit lehet kezdeni velük, ha nem csak reklámcélokra kívánjuk felhasználni? Gondoljunk egy csalfa férjre, aki üzenetben rendszeresen szervezi a szeretőjével a randevúk időpontját, helyszínét, míg a feleségének az állandó túlórák miatt panaszkodik, és ezekkel indokolja az éjszakába nyúló kimaradásokat. Tegyük fel, hogy ez a férj rendszergazda egy olyan hadiipari vállalatnál, amelyiknek az informatikai rendszerében rendkívül értékes adatok vannak, amit ennek megfelelően nagyon erős informatikai védelemmel láttak el. Az Echelon bebizonyította, az általa megszerzett adatokat nem egy esetben használták gazdasági érdekek érvényesítésére. Mindenki eldöntheti magában, vajon felhasználná-e az NSA ebben a hipotetikus történetben a rendszergazda által küldött üzeneteket, GPS-alapú helymeghatározásából kinyert adatokat, hogy a megzsarolásával behatolhasson a kívánt rendszerbe.

A social engineering az emberi hiszékenységre, az emberi természet gyengeségeire épít. A hírszerzés története dúskál a szexuális interakciókból megszerzett információkból. Nem véletlen tehát, hogy a szex visszatérő eleme a közösségi oldalakon való információszerzésnek.

2013 októberében két biztonsági szakértő, Aamir Lakhani és Joseph Muniz igazolta a fenti tételt egy konferencia-előadásában.[30] A kísérletet három hónapig folytatták, de egy hét alatt siker koronázta tevékenységüket. A kutatók felhasználták a különböző párkapcsolatokra vonatkozó statisztikákat: 5 párból 1 online ismeretségből jön létre, 5 házasságból 1 a Facebook miatt következik be, illetve egy amerikai egyetemistákkal végzett kutatás kimutatta, a válaszadók 65%-a választaná az internetet a szex helyett. Egy ismerősük fényképét felhasználva, melyhez a hölgy előzetesen hozzájárult, megalkották a 28 éves

[29] Az NSA a szolgáltatók cookie-jait használja. Sg.hu, 2013. december 12. http://sg.hu/cikkek/101938/az_nsa_a_szolgaltatok_cookie_jait_hasznalja (2013. december 13.)

[30] LAKHANI, Aamir – MUNIZ, Joseph: Social Media Deception. In. RSA Konferencia Európa 2013. 2013. október 29–31, http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (2013. december 11.)

csinos Emily Williams[31] hamis Facebook és Linkedin profilját, majd kapcsolatépítésbe kezdtek egy meg nem nevezett amerikai kormányügynökség alkalmazottaival, akik kiberbiztonság területén dolgoztak és – védelmi technikák kialakítása mellett – többek között kibertámadások kivitelezésére szakosodtak. Az eredmény megdöbbentő: nem csak ajánlatokat és vacsorameghívásokat kapott, de laptopot is ajándékoztak neki. A „kapcsolat" előrehaladtával Emily elektronikus képeslapokat küldött a célszemélyeknek, amelynek egy fertőzött támadó oldalra mutató link is részét képezte. Ezt követően az áldozatok számítógépére települt malware különféle jogosultságokhoz, jelszavakhoz jutatta hozzá a támadókat: alkalmazásokat telepítettek a rendszerbe, bizalmas információkat tartalmazó dokumentumokat loptak el. Az áldozatok egyike a hivatal informatika biztonságáért felelős vezető személy volt. A kísérlet tanulságait levonva megállapíthatjuk, hogy az emberi természet alapvetően hiszékeny, pláne, ha egy csinos, intelligens[32] nőről van szó, ami egy olyan szektorban, ahol a nemek szerinti bontásban a férfiak dominálnak, kiemelt fenyegetettséget jelent. A legfontosabb tanulság azonban nem más, minthogy hiába vannak szigorú biztonsági előírások, komoly fizikai védelem, az emberi tényezőből fakadó kockázatok ellen nagyon nehéz védekezni.

Az idézett Symantec jelentésekből egyöntetűen kiderül, a támadók rengeteget finomítottak a social engineeringen alapuló technikákon. Alaposan felderítik a célszemélyt. Ez azonban csak az első lépés. A legújabb trendek az irányba mutatnak, hogy a korábban feltérképezett célszemélyt telefonon is megkeresik, hogy ezzel fejlesszék a bizalmat, megerősítsék a biztonságérzetet.

Egy szabályzó megalkotásakor az eddig bemutatottakat nem szabad figyelmen kívül hagyni. Megítélésünk szerint egy ilyen irányú keretrendszernek két releváns pontra kell fókuszálni: a fizikai és emberi fenyegetettségekre. Ebből következően a szabályoknak ki kell terjednie arra, hogy milyen programokat kell telepíteni a munkahelyi, illetve otthoni informatikai eszközökre, valamint a telepített programok rendszeres frissítésének kötelezettségére.

Komplexebb feladatot jelent a felhasználói tudatosság növelése. Ennek nem csupán az egyes közösségi média eszközök használatából fakadó veszélyekre kell vonatkoznia, hanem a különböző oldalak működésének ismertetésére, kiemelten a bekövetkező változásokra. Ahogy korábban megfogalmaztuk, gazdasági megfontolásból rendkívül kiélezett verseny uralkodik a szolgáltatók közt, állandó innovációba kényszerítve őket. Ezek a változtatások azonban sok esetben alapjaiban rúgják fel adott esetben a korábbi adatvédelmi beállításokat.

A tanulmány elkészítése alatt szüntetett meg például a Facebook egy korábbi adatvédelmi beállítást, mely lehetővé tette, hogy a felhasználó letiltsa, hogy a nevére bárki rákeressen.[33] De a Google is rendszeresen konfrontálódik mind a felhasználókkal, mind a jogvédőkkel a felhasználási feltételek változtatása kapcsán, ahogy legutóbb valós névhez kötötte a kommentelési

[31] Érdemes megjegyezni, próbálkoztak egy hamis férfi profil megalkotásával is, de azzal eredménytelennek bizonyultak.

[32] A legenda szerint Emilly a Massachusetts Institute of Technology-n szerzett diplomát.

[33] Ön sem rejtőzhet el mostantól a Facebookon. HVG.HU, 2013. október 11. http://hvg.hu/tudomany/20131011_facebook_rejtozes_off (2013. november 14.)

lehetőséget a YouTubeon[34] vagy belefoglalta, hogy reklámcélra a felhasználók profilképét és preferenciáit felhasználhatja.[35] Az átlag felhasználó ezekről a változásokról nem értesül, így megítélésünk szerint rendkívül fontos a tudatosság megteremtése érdekében az ilyen jellegű tájékozottság. Amennyiben a felhasználó nem tudja, mi mindent használhatnak ellene az online aktivitásából, rendkívüli kockázatoknak teszi ki magát, ezen keresztül a vállalatot, amelynek alkalmazásában áll.

Tisztában vagyunk az oktatás korlátaival, mely szerint egy kötelezően előírt tanfolyam nem feltétlenül érné el a kívánt hatást az esetleges érdektelenségből kifolyólag, mégis hasznosnak gondoljuk a bevezetését, amelyen nem csak adat- és információbiztonságról, de a közösségi média veszélyeiről, alkalmazhatóságáról is ismereteket szereznének a hallgatók, valamint az oktatást követően rendszeresen értesülhetnek a bekövetkezett változásokról.

A fentiek alapján úgy véljük, a biztonsági minimumkövetelményeknek az alábbiakra kell kiterjedniük:

- megfelelő fizikai védelem a munkahelyi és otthoni informatikai eszközökre;
- az alkalmazottak adat- és információbiztonságra vonatkozó érzékenységének növelése;
- a közösségi média használatából fakadó kockázatok ismerete;
- a saját sebezhetőség feltérképezése (mind fizikai, mind humán kockázatok esetében);
- a biztonsági beruházások növelése;
- az adatokhoz való hozzáférés korlátozása;
- a hálózat szegmentálása.

Természetesen az itt felsoroltak mindegyike nem tartozik közvetlenül a közösségi média használathoz, de szükségesnek mondhatóak. Hiszen ha egy alkalmazottat zsarolással sikerül a támadóknak információszerzésre felhasználni, védelmet jelenthet, ha például nem fér hozzá minden adathoz. Ahogy a PRISM-botrány is bebizonyította, az Edward Snowden által kiszivárogtatott dokumentumok nagy része a munkatársai átveréséből került a birtokába, átadva nekik a felhasználói azonosítójukat, illetve jelszavukat.[36] Ez, ha nem is lenne 100%-ban elkerülhető, megfelelő adat- és információérzékenység esetében minimalizálható lehet.

---

[34] Százezrek követelik a YouTube kommentrendszerének visszaállítását. PCFórum, 2013. november 18.
http://pcforum.hu/hirek/15589/Szazezrek+kovetelik+a+YouTube+kommentrendszerenek+visszaallitasat.html (2013. december 14.)

[35] Lázadnak a webezők a Google új adatvédelmi módosításai ellen.
PCFórum, 2013. október 14.
http://pcforum.hu/hirek/15470/Lazadnak+a+webezok+a+Google+uj+adatvedelmi+modositasai+ellen.html (2013. december 14.)

[36] Kollégái jelszavával szerzett NSA-adatokat Snowden. MNO, 2013. november 8. http://mno.hu/kulfold/snowden-kollegai-jelszavaval-szerzett-nsa-adatokat-1194265 (2013. december 14.)

Összefoglaló gondolatok

Az emberi természet talán egyik legjellemzőbb tulajdonsága az összetettség. Legyen szó bármilyen egyéb tulajdonságról, ez az összetettség garantálja, hogy nem értelmezhetjük azt csupán feketének vagy fehérnek. A legpozitívabb jellemzői az emberiségnek a kíváncsiság, a kreativitás, a felfedezés vágya, ugyanakkor ezek a tulajdonságok azok, amik a legsötétebbek is egyben. A történelem során a megalkotott szerkezeteket, amelyek alaprendeltetésük szerint az emberiség javát igyekeztek szolgálni, roppant gyorsan sikerült átalakítani pusztításra. A közösségi média, mint eszköz, ugyanúgy beleillik ebbe a mintába. Az eredetileg interperszonális interakciók online művelésére, szórakozásra létrehozott oldalak számos olyan kockázatot és fenyegetést hoztak magukkal, amik a biztonságot alapvetően alakították át. A tanulmánynak nem volt célja, hogy komplexen foglalkozzon a kockázatokkal, egy speciális terület a védelmi ipar fenyegetettségét vizsgálta.

Egy állam biztonságának megteremtésében a megfelelő védelmi potenciál biztosítása elengedhetetlen. Az informatikai eszközök elterjedtsége és fejlettsége azonban egy új hadszínteret hozott létre, amely nem csak a hírszerzésben, de akár a fizikai pusztításban is kiemelt szerepet kaphat. Ebből következően az egyes államok mindent megtesznek, hogy a lehető legtöbb információval rendelkezzenek az ellenséges/szövetséges államok képességeiről. Ennek a virtuális hidegháborúnak vált egy kiterjesztett terepévé a közösségi média. Mindez nem mondható meglepőnek, hiszen a közösségi eszközök használata a mindennapjaink részét képezik, ott vannak a munkahelyeken, az iskolákban, a magánéletünkben.

Elemezve a kibertámadások trendjeit, a védelmi ipari cégek, elsősorban a KKV-k kerültek a támadók célpontjai közé. Ezek ugyanis a vélhetően kevesebb költségvetés miatt nem alakítottak ki megfelelő informatikai biztonságra vonatkozó protokollt. Rajtuk keresztül el lehet jutni a nagyobb cégekhez, amelyek a sorozatos támadások hatására kénytelen voltak erre vonatkozó stratégiát kidolgozni.

Legyen szó bármilyen biztonságos rendszerről, elég egy felelőtlen felhasználó, akit kihasználva a támadók rendkívül értékes adatokat szerezhetnek meg. Ennél fogva kísérletet tettünk egy olyan biztonsági minimumkövetelmények megfogalmazására, amelyek a védelmi iparban jelenlevő vállalatoknak nyújthatnak iránymutatást a közösségi média használatra. Ennek érdekében elemeztük a közösségi média trendjeit, megvizsgáltuk a védelmi ipar fenyegetettségét. Megítélésünk szerint az egyik legnagyobb biztonsági kockázatot a felhasználó jelenti, legyen szó állami vagy szervezett bűnözői érdekkörről. A támadók a naiv, adat- és információérzékenység tekintetében gyenge felhasználón keresztül próbálnak hozzáférni a kívánt adatokhoz. Nem hisszük, hogy a tiltással eredményesen védekezhetünk, így a felhasználók oktatására kell összpontosítani, hogy ez által minimalizálhassuk a kockázatot.

A terjedelmi korlátok nem tették lehetővé, hogy kimerítően foglalkozzunk minden egyes területtel, a szerző az egyes fejezetek írása közben döbbent rá, hogy mennyi mindennel kellene foglalkozni az adott témát illetően, de a nagyobb összefüggések megvilágítása érdekében önkorlátozásra kényszerült. Az egyes fejezetek, de akár a bennük foglaltak külön-külön tanulmányt érdemelnének (például a felhasználói tudatosság növelésének érdekében

hasznosnak ítélt oktatás kialakítása). Ebből következően célunk a tudományos diskurzus megindítása volt annak reményében, hogy az ráirányítja a figyelmet a közösségi média használatából eredő kockázatokra. Nem csak a védelmi ipar tekintetében, de a védelmi szféra minden területén.

FORRÁSOK

SOTTECK, T.C.: British intelligence reportedly intercepted LinkedIn and Slashdot traffic to plant malware. The Verge, 2013. november 10. http://www.theverge.com/2013/11/10/5088048/british-intelligence-gchq-linkedin-slashdot-quantum-insert (2013. november 11.).

COHEN, Heidi: 30 Social Media Definitions. HeidiCohen.com, 2011. május 9. http://heidicohen.com/social-media-definition/ (2013. november 24.).

Definition of social media in English. Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/social-media (2013. november 24.).

KAPLAN, Andreas – HAENLEIN, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010

BÁNYÁSZ Péter: A közösségi média szerepe a katasztrófaelhárításban a Sandy - hurrikán példáján keresztül. Fejezetek a kritikus infrastruktúra védelemből. Magyar Hadtudományi Társaság, Budapest, 2013.

BÁNYÁSZ Péter: A közösségi média szerepe a 21. század hadseregeiben. Hadtudomány, 2012/1–2.

A különböző internetes oldalak három típusát látogatja heti rendszerességgel a netezők többsége. IPSOS, 2013. november 5. http://www.ipsos.hu/site/a-k-l-nb-z-internetes-oldalak-h-rom-t-pus-t-l-togatja-heti-rendszeress-ggel-a-netez-k-t-bbs-ge/ (2013. december 3.).

Internet users (per 100 people). World Bank, 2012 http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=default (2013. december 3.).

Félmillióval nőtt a Facebook tábora egy év alatt. Mediameter, 2013. június 14. http://mediameter.hu/kutatasok-elemzesek/mediameter-felmillioval-nott-a-facebook-tabora-egy-ev-alatt/ (2013. december 7.).

Egyre nő az internethasználat Magyarországon. GfK, 2012. június 10. http://www.gfk.hu/pressreleases/press_releases/articles/010194/index.hu.html (2013. december 8.)

A közösségi média úgy vonzza az embereket, mint fény a pillangókat. IPSOS, 2013. január 10., http://www.ipsos.hu/site/a-k-z-ss-gi-m-dia-gy-vonzza-az-embereket-mint-f-ny-a-pillang-kat/ (2013. december 8.).

AJMERA, Harsh: Social Media facts, figures and statistics 2013. Digital Insights, 2013. szeptember 4. http://blog.digitalinsights.in/social-media-facts-and-statistics-2013/0560387.html (2013. december 8.).

BULLAS, Jeff: 5 Insights into the Latest Social Media Facts, Figures and Statistics. Jeffbullas.com, 2013. június 4.
http://www.jeffbullas.com/2013/07/04/5-insights-into-the-latest-social-media-facts-figures-and-statistic/ (2013. december 8.).

Social Tools in the Workplace. Microsoft, 2013. május 6. http://www.microsoft.com/enterprise/it-trends/social-enterprise/articles/Social-Tools-in-the-Workplace-Infographic.aspx#fbid=y6bL-YMGQle (2013. december 8.).

Internet Security Threat Report 2013 Vol. 18. Symantec, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (2013. december 8.)
SYMANTEC CORPORATION: Symantec Intelligence Report. 2013. September, In. Symantec, http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_09-2013.en-us.pdf (2013. december 8.).
CAMPBELL, Duncan – HONIGSBAUM, Mark: Britain and US spy on world. The Guardian, 1999. május 23. http://www.duncancampbell.org/menu/journalism/guardian/britain.pdf (2013. december 03.)
Temporary Committee On The Echelon Interception System Directorate-General For Committees And Delegationsbrussels Meeting. 2001. január 22–23. http://www.duncancampbell.org/menu/surveillance/echelon/Contract_analysis.pdf (2013. december 3.).
Magyar Védelmiipari Szövetség 2012. évi katalógusa.
KIRÁLY László – PATAKI István: Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz. Hadtudomány 2013/1. elektronikus szám, http://mhtt.eu/hadtudomany/2013_e_Kiraly_Laszlo_Pataki_Janos.pdf (2013. december 11.).
Aktuális NATO Beszállítói céglista. NATO Beszállítói Információs Honlap, http://www.natotender.gov.hu/aktualis_nato_beszallitoi_ceglista/ (2013. december 9.).
A netező magyaroknak nincs külön munka és pihenés. Híradó, 29. http://www.hirado.hu/Hirek/2013/10/28/15/A_netezo_magyaroknak_nincs_kulon_munka_es_pihenes.aspx (2013. december 10.).
Újra használhatják a közösségi portálokat az amerikai katonák. Sg.hu, 2010. március 2. http://m.sg.hu/cikk.php?cid=72827&cim=ujra_hasznalhatjak_a_kozossegi_portalokat_az_amerikai_katonak (2013. december 11.).
Az NSA a szolgáltatók cookie-jait használja. Sg.hu, 2013. december 12. http://sg.hu/cikkek/101938/az_nsa_a_szolgaltatok_cookie_jait_hasznalja (2013. december 13.).
LAKHANI, Aamir – MUNIZ, Joseph: Social Media Deception. In. RSA Konferencia Európa 2013. 2013. október 29–31, http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (2013. december 11.).
Ön sem rejtőzhet el mostantól a Facebookon. HVG.HU, 2013. október 11. http://hvg.hu/tudomany/20131011_facebook_rejtozes_off (2013. november 14.).
STING: Százezrek követelik a YouTube kommentrendszerének visszaállítását. PCFórum, 2013. november 18. http://pcforum.hu/hirek/15589/Szazezrek+kovetelik+a+YouTube+kommentrendszerenek+visszaallitasat.html (2013. december 14.).
Lázadnak a webezők a Google új adatvédelmi módosításai ellen. PCFórum, 2013. október 14. http://pcforum.hu/hirek/15470/Lazadnak+a+webezok+a+Google+uj+adatvedelmi+modositasai+ellen.html (2013. december 14.).

Kollégái jelszavával szerzett NSA-adatokat Snowden. MNO, 2013. november 8., http://mno.hu/kulfold/snowden-kollegai-jelszavaval-szerzett-nsa-adatokat-1194265 (2013. december 14.)