Műszaki Katonai Közlöny

XXIV. évfolyam, 2014. 4. szám

Vanderer Gábor[1]

SECURITY AWARENESS ÉS TÁRSADALMI FELELŐSSÉG[2]

Információs társadalomban élünk, akár tudomást veszünk róla, akár nem. A újabb generációk már ebbe nőnek bele. Felnőtt egy új generáció, amelyik a korábbinál sokkal természetesebben használja a technológiát, de az idegenkedéssel együtt elveszett az egészséges félelemérzet is: ma az információbiztonság-tudatosságunk (information security awareness) nagyon alacsony. Publikációmban ennek a társadalmi vonatkozásait elemzem, rámutatok a veszélyforrásokra, valamint megemlítek néhány, már létező kezdeményezést.

Kulcsszó: Információbiztonsági-tudatosság, negyedik generációs hadviselés, információs társadalom

SECURITY AWARENESS AND SOCIAL RESPONSIBILITY

We are living in the Information Society – whether we acknowledge it or not. A new generation has grown up. Using Internet technology is more natural for them, but with the loss of aversion also the healthy sense of fear is lost. Our security awareness is really low. In my publication, I give an analysis of the social aspects; I pinpoint threats and mention some already existing initiatives.

Keywords: Information security awareness, Fourth generation warfare, information society

INFORMÁCIÓS TÁRSADALOM

Információs társadalomban élünk, életünket egyre mélyebben szövik át a különböző elektronikus rendszerek. Egyre több ügyet intézhetünk elektronikusan a közigazgatásban, a felsőoktatás már régóta a NEPTUN rendszerben rögzíti az eredményeket, és lassan a középfokú oktatás is átáll az e-naplóra; sőt, legújabb Nemzeti Konzultációnkat is Internet-alapon készül megoldani kormányunk megbízottja. Ez a trend természetesen nem csak Magyarországon érvényesül, a nyugati világ is ebbe az irányba halad.

A társadalom egyre szélesebb rétegei használnak Internet alapú információs csatornákat, de sajnálatos tény, hogy ezeknek a felhasználóknak a túlnyomó többsége nincs tisztában ennek a kommunikációs módnak a veszélyeivel.

Fontosnak tartom megjegyezni, hogy az Információbiztonság (Information Security) sokkal több, mint, mint az Informatikai biztonság (IT Security). Jelen munkában azonban nem egy szervezettel, hanem a társadalom egészével foglalkozom, így ebben a kontextusban a két fogalom erősen összemosódik: az információ szinte kizárólag Internet-alapon kerül továbbításra, ami – vegyük észre – még az IT biztonságnak is csak egy szűk szegmense.

Az információ-biztonság évezredes múltra tekint vissza. Mindig is voltak szervezetek (államok, egyházak, de természetesen magánszemélyek is), melyeknek érdekük fűződött adataik védelméhez, ez pedig értelemszerűen kinevelte az ezzel foglalkozó szakembereket is.

[1] Óbudai Egyetem, Biztonságtudományi Doktori Iskola, E-mail: gvanderer@gmail.com
[2] Bírálta: Prof. dr. Lukács László CSc., a Zrínyi Miklós Nemzetvédelmi Egyetem, majd a Nemzeti Közszolgálat Egyetem nyugalmazott egyetemi tanára.

Az informatikai biztonság sokkal rövidebb múltra tekint vissza, de ennek ellenére is komoly változáson ment keresztül.

20–25 ével ezelőtt ez még csak a szakemberek problémája volt. Adatokat már akkoriban is tároltak elektronikusan (de legalább elektronikusan is), ezekre általában a papír-alapú dokumentumok már létező szabályozását igyekeztek ráhúzni, és az adathordozó kezelését szabályozni.[3] Kevés szakember foglalkozott akkoriban kifejezetten informatikai biztonsággal, a társadalom egészét pedig egyáltalán nem érintette a probléma.

Később, ahogy az számítástechnika beszivárgott a munkahelyekre, egyre több helyen kezdtek számítógépeket használni. Az informatika térhódításával az információ-biztonság egyre inkább a munkaadók problémája lett. Tipikus korabeli kérdések:

- Hogyan tudom megakadályozni, hogy a cég adatai kiszivárogjanak?
- Hogyan vegyem rá az alkalmazottakat, hogy ne vigyék haza a céges dokumentumokat?
- Hogyan oldjam meg biztonságosan a távmunkát?[4]

Véleményem szerint ma már az informatika, valamint az Internet-alapú informatikai rendszerek olyan szinten terjedtek el és ivódtak be a társadalomba, hogy ez ma már mindenki problémája, akár hajlandó valaki tudomást venni róla, akár nem. Ez pedig szorosan összefügg a Security Awareness problémájával, amit magyarul talán biztonságtudatnak lehet fordítani, de egyelőre még nincs kialakult magyar terminológiája.

Nagyságrendi különbség, hogy egészen eddig megbízott szakemberek foglalkoztak a kérdéssel. Egy IT rendszerintegrátor feladata már 2005-ben sem az volt, hogy meggyőzze a leendő vásárlóját: biztonságra szükség van. Megoldást kellett adnia a problémára. A társadalomban az informatikai rendszereket használó egyének azonban nem így működnek: elsődlegesen nem megoldást kell nekik adni, hanem felkelteni az igényt arra, hogy ezzel nemcsak hasznos, de szükséges is foglalkozni.

SECURITY AWARENESS

A munkaadók egyik (régi) tipikus problémája az volt, hogy a felhasználók a laptopjaikon esetleg kiviszik a céges adatokat a munkahelyükről. Ma már a felhasználók jelentős része okostelefont használ, és teljesen magától értetődő, hogy a telefonon olvassam a céges emailjeim (kritikus adatok!), mindezt párhuzamosan a privát Google fiókkal.

10 éve még az volt magától értetődő, hogy érzékeny adatokat NEM tárolunk ilyen kevéssé biztonságos környezetben.

Az okostelefon a legkevésbé sem védett: egyrészt informatikai eszközökkel is támadható[5], másrészt könnyű elveszíteni és a lopásnak (ami lehet akár célzott támadás is!) is fokozottan ki van téve.

---

[3] Érdekességképp: A jelenleg is hatályos 1998. évi XIX. törvény (A büntetésbégrehajtásról) 244/D. § -ában a tárgyalás során keletkező kép- és hangfelvételt az iratokhoz csatoltatja. Természetesen ezek ma már az „iratok" is elektronikusan, dokumentumkezelő rendszerben laknak.

[4] A legújabb informatikai óvintézkedések és technikák, 2005, http://www.ma.hu/tart/rcikk/e/0/113131/1, 2014.11.14.

[5] Forrás: Nyikes Zoltán: Mobil eszközök biztonsági kérdései. 2014. Kommunikáció 2014 konferencia tézisfüzet, ISBN 978-615-5491-94-8, 165–174. oldal.

A világ tehát változik, és nekünk együtt kell változni vele. Vallom, hogy az informatikai biztonság bármikor növelhető a használhatóság rovására, és informatikai szakemberként egy használható állapotot kell megcélozni, mindazokkal a tervezett kockázatokkal egyetemben, amelyek ezzel együtt járnak.

El kell fogadnunk, hogy a felhasználók szeretik az okostelefonokat, és nem fognak lemondani róluk még egy céges környezetben sem, csak azért, mert ez az IT-nek ez nem tetszik; össztársadalmi szinten pedig egyértelmű, hogy a szakembereknek kell lekövetni a változást.

Vegyük észre, hogy napjaink átlag okostelefonja rengeteg jelszót, belépési azonosítót tárol (és akkor még nem volt szó az esetleg offline elérhető céges levelekről). Ez egy szakemberben fel is veti a következő kérdést: vajon az okostelefon-használók hány százaléka képes összeírni, hogy milyen hozzáférései kompromittálódtak egy elveszett telefonnal?

Hasonlóképp: elveszett/ellopták a laptopom pótolhatatlan adatokkal, visszavásárolnám… Bizonyára sokan láttunk már ilyen hirdetést. Hol van ilyenkor a biztonsági mentés? Egy szakembernek teljesen egyértelmű, hogy a kritikus adatokat menteni kell. Napjaink felhasználója ugyan tisztában van vele, hogy (számára) kritikus adatokat tárol, mégsem kezeli őket ennek megfelelően.

A BANKOK, A PIN KÓD ÉS AZ INTERNET-BANK

Egy remek példa a security awareness hiányára a bankok magatartása, akik bő egy évtizeden keresztül próbálták nevelni a felhasználóikat (és mivel bankkártyája szinte mindenkinek van, ezen keresztül szinte az egész társadalmat):

- Ne írjuk rá a PIN kódot a bankkártyára.
- Ne tartsuk a felírt PIN kódot a tárcánkban a bankkártya mellett.
- Ne írjuk fel a PIN kódot.

Azt hiszem felesleges konkrét példákat hoznom, mindenki emlékszik ezekre az időkre.

Az Internet-banki hozzáféréseket annak idején egy egyszerű felhasználónév/jelszó páros védte, amire szintén illett vigyázni, de ez sosem kapott akkora súlyt a banki kommunikációban. Az Internet se volt annyira elterjedve, kevesen is használták.

Ahogy egyre több felhasználó kezdett Internet-alapú bankolást használni, a bankok már nem is kezdtek biztonságtudatosság-növelésbe: bevezették a telefonra SMS-ben elküldött egyszer használatos jelszavakat (pl. OTP), vagy a jelszó-generáló tokeneket (pl. CIB).

A bankok a felhasználóik helyett is védik az adatokat, hiszen egy célzott támadás esetén ők is sokat veszítenek anyagilag és presztízsben egyaránt. Vegyük észre, hogy ez egyfajta kivonulás: a technológia használatával megkerülő megoldást adok egy problémára („A felhasználóim nem vigyáznak a hozzáférésükre”), de ettől még a probléma megmarad. A bankok helyzete viszonylag speciális, hiszen kényszeríthetik a felhasználóikat ezeknek a technológiáknak az alkalmazására pont ugyanúgy, ahogy a cégek is képesek rákényszeríteni az eljárásrendeket az alkalmazottakra. De a magánjellegű, privát felhasználás síkján társadalmi méretekben ez nem működik.

A Z GENERÁCIÓ PROBLÉMÁJA

Érdekes felvetés, hogy a biztonsági kockázatok emberi tényezői között a generációs különbségek is szerepet játszanak. A szociológusok és a marketing szakemberek szerint a mai munkavállalók születésük alapján három jellegzetes csoportba sorolhatók (Lancastar-Stillmann, 2010)[6]:

- ún. „baby boom"-osok (1946 és 1965 között születettek);
- X generáció (1965-1980 között jöttek a világra);
- Y generáció (1980 után születtek);
- A Z generáció (1995 után születettek).

Az első csoport tagjai tipikusan lojálisak munkaadójukhoz, de kevésbé tudnak alkalmazkodni az információtechnológia robbanásszerű fejlődéséhez: tudásbeli hiányosságaik lehetnek.

Az X generáció tagjai függetlenek, a biztonsági előírásokat gyakran nem veszik figyelembe („ők jobban tudják"). Rosszindulatból is okozhatnak kárt.

Az Y generáció kifejezetten fogékony az információtechnológia iránt, de türelmetlen is. Ők azok, akik inkább megkeresik a megoldást a Google keresővel, minthogy napokat várjanak egy bangladesi call-centerre. Leginkább rájuk jellemző, hogy saját mobil eszközre töltenek le bizalmas vállalati anyagokat.

A Z generáció tagjai már az Internet világába születtek bele, igénylik és elvárják a folyamatos online jelenlétet. Egy hagyományosan nagy biztonságú munkahely kiszakítja őket ebből a számukra természetes közegből. Érdekes kérdés a jövőre nézve, hogy milyen változásokat fog előidézni ennek a generációnak a megjelenése a munkaerőpiacon.

A generációs különbségeket, a korcsoportok sajátosságait tehát célszerűen figyelembe kell venni az információvédelem szabályozásakor (Kelemen, 2008)[7].

Ugyan a fenti kutatások a munkaadók szempontjából vizsgálták a problémát, de természetesen ezek a generációk magánemberként is léteznek, magánemberként is használják az Internetet (és a vonatkozó technológiákat) ügyeik intézésére. A mi szempontuntunkból az az érdekes, hogy a technológia mindennapokba épülésével elvész egyfajta egészséges félelemérzet is. Az X generáció tagjai ugyan „jobban tudják", de ezzel együtt tisztában vannak a veszélyekkel, legfeljebb a megoldás módjával nem értenek egyet. Az Y generáció már nem is feltétlenül látja, hogy ez problémát jelent („működik, mi kell még"), a Z generáció pedig már a veszélyekkel sincs tisztában.

Felnőtt egy új generáció, amelyik sokkal természetesebben használja a technológiát, de az idegenkedéssel együtt elveszett az egészséges félelemérzet is.

[6] Forrás: Lynne C. Lancaster (Author), David Stillman (Author): The M-Factor: How the Millennial Generation Is Rocking the Workplace, HarperCollins, 2010.
[7] Forrás: Kelemen László: Nem sztereotípiák, IT-business, 2008. szeptember 28, VI évf. 37. sz. 32. oldal.

Forráskritika

Szintén az Y és Z generáció problémája a forráskritika hiánya. (Ez valamilyen szinten már az Y generációban is megjelenik, de itt teljesedik ki igazán.) Ennek a generációnak a tagjai elutasítják a mainstream médiát, elsődleges hírforrásuk az Internet, illetve a barátoktól kapott (linkelt) információk.[8]

Az Interneten azonban nemhogy tipikusan minden megtalálható, hanem bárminek az ellenkezője is.

Amíg a tudás elsődleges forrásai a különböző szakkönyvek és lexikonok voltak (X generáció és előtte), volt egyfajta kontroll, ami mára teljesen megszűnt. Természetesen léteznek ma is hiteles források, de az információforrások elenyésző hányada ilyen. Épp ez a WEB 2.0 lényege, hogy bárki lehet tartalomszolgáltató: elmosódik a határ az információforrások és a fogyasztók között. (Márpedig a WEB 2.0 se friss dolog.) A mai, Internet uralta világban nem evidens egy forrás hitelességéről meggyőződni, de az Y és Z generációnak erre (nagy általánosságban) igazából igénye sincs. A Z generáció mindent megkérdőjelez (ami nem feltétlenül probléma), de a hozzá érzelmileg közelebb álló forrást tekinti hitelesnek (ami viszont probléma).

„Az Y-generáció tagjai már egy olyan világban nőttek fel, ahol a médiában csak a terrorizmust, veszélyt, gazdasági válságokat, tönkre ment embereket mutatják, valamint számukra ismert a szüleik világa, ami nekik egy állandó, unalmas körforgásnak tűnik, ezek után nehéz megteremteni egy biztos érzelmi hátteret, amire minden tagnak szüksége lenne. Ezek után kénytelenek megteremteni saját maguknak egy olyan képzeletbeli világot, ahol érzik a csoporthoz való tartozást és közösségi élményekben lesz részük. Mindezt sajnos az Interneten találják meg blogok vagy közösségi portálok formájában.”[9]

Információs társadalomban élünk, amikor nem az információ megszerzése, hanem a feldolgozása jelenti a nehézséget. Az ehhez nélkülözhetetlen forráskritikát pedig tanulni és szokni kell, ez pedig erőteljesen hiányzik a mai közoktatásból. Ez pedig egyre fontosabb kérdés lesz, ahogy a felnövő generációk szorítják ki az idősebbeket.

Mondhatjuk persze, hogy előbb-utóbb majd tanul mindenki a maga kárán (vagy megpróbálja a második laptop adatait is visszavásárolni), de véleményem szerint itt társadalmi felelősségünk van.

[8] Forrás: Szonda Ipsos felmérés, 2013, http://www.ipsos.hu/site/legink-bb-a-t-v-b-l-t-j-koz-dnak-a-fiatalok/, 2014.11.15.
[9] Forrás: Tari Annamária: Y-Generáció-klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban. Jaffa Kiadó, Budapest, 2010, 27–29. oldal.

FENYEGETETTSÉGEK

A hitelválság kapcsán többször elhangzott, hogy Magyarország lakosságának pénzügyi műveltsége mennyire alacsony. [10] (Természetesen – visszakanyarodva kicsit az előző fejezethez – ennek az ellenkezője is megtalálható az Interneten.[11]) Véleményem szerint valóban alacsony, de azt is vallom, hogy az információbiztonság, biztonság-tudatosság is legalább ennyire el van hanyagolva. Nem feltétlenül érdemes megvárni, amíg ebből is kipattan egy válság, márpedig a lehetőség megvan rá.

A pénzügyi kultúránk azért is jó példa, illetve párhuzam, mert itt is megpróbáltak technikai eszközökkel megkerülni egy problémát: az emberek nem is értették a különböző banki megoldások költségstruktúráját, bevezették hát törvényileg a THM mutatót12, ami összehasonlíthatóvá tette a hiteleket. Ez természetesen a pénzügyi kultúra hiányát nem igazán tudta pótolni.

Az informatikai hadviselés egyrészt egyértelműen eleme a 4. generációs hadviselésnek (Somkuti, 2012)[13,] másrészt igen hatékony terrorista-fegyver. Somkuti másik, számunkra fontos megállapítása a média szerepének felértékelődése: „Globális média: nem lehet elégszer hangsúlyozni, hogy az új generációs hadviselés messze túllép a hagyományos politika-háború fogalmakon, ráadásul az új eszközöknek köszönhetően az Al Dzsazíra katari non-stop hírcsatorna már akár tíz perccel egy cél tévesztett bomba után telekürtölheti a világot a „barbár amerikaiak rémtetteivel”.”

Ennek az információs/dezinformációs hadviselésnek a hatékonyságát pedig határozottan erősíti a felnövekvő új generációk Internet-alapú információszerzési módja.

Mindez szépen látszott az 2007-es orosz-észt konfliktus („kiberháború”) során. Az erősen Internet-alapú észt államigazgatást és bankrendszert sikeresen bénították meg DDoS[14] támadással. A megbénítás mellett fontos szerep jutott a tudatos dezinformációnak is.

Azt sem szabad figyelmen kívül hagyni, hogy ez egy eléggé gyengén szabályozott terület. A Tallini Jegyzőkönyv ugyan definiálja, hogy egy informatikai eszközökkel végrehajtott csapásmérés mikor minősül fegyveres támadásnak, de egyrészt ezek a szabályok továbbra sem teljesen objektívek, másrészt az Internet jellegéből adódóan sosem egyértelmű, hogy ki a támadó.

A hagyományos hadviselésben, ha A ország megtámadja B országot C ország területéről (például: Az Egyesült Államok Szaúd-Arábia területén lévő támaszpontokról bombázza Irakot), akkor ez tipikusa C ország tudtával és beleegyezésével történik. Egy informatikai

[10] Forrás: Dr. Csiszárik-Kocsir Ágnes PH.D. A huszonéves fiatalok pénzügyi alapfogalom-ismerete egy kérdőíves kutatás eredményinek tükrében, 2013, http://kgk.sze.hu/images/dokumentumok/VEABtanulmanyok/csiszarik_kocsir_agnes.pdf, 2014.11.15.
[11] Forrás: Egy ING IM felmérés. Url: http://www.portfolio.hu/befektetesi_alapok/ongondoskodas/penzugyi_muveltseg_teren_az_elbolyban_van_magyarorszag.176938.html, 2014.11.11.
[12] 41/1997. (III. 5.)-es kormányrendelet.
[13] Forrás: Sommkuti Bálint: A negyedik generációs hadviselés – az érdekérvényesítés új lehetőségei. PhD értekezés, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Hadtudományi Doktori Iskola, 2012. 79–82. oldal.
[14] Distributed Denial of Service.

csapásmérés esetén még azt se evidens eldönteni, hogy terrorista cselekményről, vagy hagyományos állam-állam közötti konfliktusról van szó. Az ominózus C ország pedig alkalmasint nem is tud semmiről.

Hasonlóképpen hiába találnak a támadó kódban orosz nyelvű kommenteket: ez csak azt bizonyítja, hogy az elkészítésében részt vettek orosz nyelven beszélő emberek is. A támadó kódokat adják-veszik; sőt, a csapásmérésre alkalmas zombigép-hálózatok is bérelhetők. Egy orosz kóddal végrehajtott csapásmérés semmivel se erősebben utal az orosz forrásra, mint a hagyományos fegyverzet esetében.

Hasonló eset játszódott le Grúziában is 2008-ban, bár ott a kibertámadás hatásai eltörpültek a tényleges katonai beavatkozás mellett. Fontos azonban, hogy az orosz hivatalos szervek mind a két esetben kategorikusan tagadták, hogy közük lenne a támadásokhoz.

Egy esetleges, hagyományos fegyverzettel végrehajtott válaszcsapásnak pedig mindig konkrét célpontja van.

A mai tipikus DDoS csapásméréseket általában előre elkészített (gyakorlatilag „bérelhető") zombigép-hálózatokból hajtják végre.[15] Ezek pedig nyilvánvalóan ott fognak létrejönni, ahol a legkisebb ellenállással találkoznak: ahol a legkisebb a lakosság információ-biztonsági tudatossága. Egy Magyarországról kiinduló támadás esetén pedig eléggé kétesélyes, hogy a (Tallini Jegyzőkönyv értelmében akár konvencionális fegyverekkel végrehajtott) válaszcsapás előtt mit tudunk kezdeni a konfliktussal.

Pénzügy és informatika

Ugyan a Tallini Jelentés csak az informatikai eszközökkel végrehajtott támadásokról szól, de vegyük észre, hogy pénzügyi eszközökkel ezzel teljesen összemérhető károkat lehet okozni. (ha annak következtében emberek halnak meg, vagy kiemelt anyagi kárral kell számolni.)

A 4. generációs hadviselésben pedig a résztvevő államok nem feltétlenül hagyományos katonai eszközökkel próbálják elérni a politikai céljaikat, hanem okosan kiírt népszavazással, terroristáknak juttatott fegyverekkel és pénzzel, és igen, gazdasági szankciókkal. Egy-egy hedge fund pedig már ma is képes akkora tőkét megmozgatni, ami összemérhető egyes államok lehetőségeivel, és természetesen pénzügyi szervezetek is támogathatóak, a terroristákhoz hasonló módon.

FEJLESZTÉSI IRÁNYOK

Véleményem szerint a legfontosabb a lakosság (máris elkésett) felkészítése az információs társadalomra. Amiben már benne élünk, de sajnos az iskolarendszerű képzésben minimális súlyt kap. A bankok feladhatják, de a társadalomnak ezt nem szabad megtennie.

Az információ-biztonsági tudatosság növelése egyrészt garantálhatja, hogy ne mi legyünk az ominózus C ország, másrészt egy informatikai csapásmérés esetén minimalizálhatja a károkat.

[15] Forrás: Sági Norbert – Dr. magyar Sándor: A kiberbűnözés legújabb trendjei. Kommunikáció 2014 konferenciakiadvány, 2014, ISBN 978-615-5491-94-8, 84.oldal.

Egyre több eszköz csatlakozik az Internetre: A legújabb trendet az okosTV-k jelentik, de fűtési rendszerek, kábel TV set-top boxok, vagy akár villanykapcsolók is vezérelhetők Interneten keresztül. Egyre több eszköz kerül be a háztartásokba, amelyek potenciális veszélyforrások lehetnek (megfelelő szoftverekkel támadhatóak, DDoS támadás kezdeményezésére képes zombigép-hálózattá alakíthatóak), viszont megvédésük igénye még annyira sem tudatosul az átlagos felhasználóban, mint az okostelefoné.

Véleményem szerint szintén nagyon fontos annak a tudatos kezelése is, hogy az Internetről tájékozódó generáció hogyan fog viszonyulni egy tudatos dezinformációs támadás esetén. Az Y és Z generáció nem fog rádiót hallgatni csak azért, mert a népszerű Internetes portálok elnémulnak, és nem feltétlenül fogják felismerni a dezinformációt.

Előremutató, hogy a felnőttképzésben az EDCL része lett az IT biztonság modul, és középiskolában is tantárgy az Informatika – még ha nem is érettségi tárgy. Véleményem szerint az informatika és ehhez kapcsolódóan az informatikai biztonság a mai világban – mivel életünk szerves része - sokkal nagyobb súlyt kellene, hogy kapjon.

Szintén jó kezdeményezés az Óbudai Egyetem biztonságtechnikai mérnök képzése, illetve Biztonságtudományi Doktori Iskolája, vagy a BME-n működő CrySyS labor: ezeknek az eredményei a társadalom elenyésző hányadához jutnak el, de egy adott ország jó szakemberekkel való ellátottsága önmagában is valószínűsíti, hogy nem mi leszünk leggyengébb láncszemként a kiválasztott C ország.

FELHASZNÁLT IRODALOM, FORRÁS

1. Nyikes Zoltán: Mobil eszközök biztonsági kérdései, 2014, Kommunikáció 2014 konferencia tézisfüzet, ISBN 978-615-5491-94-8
2. A legújabb informatikai óvintézkedések és technikák, 2005, http://www.ma.hu/tart/rcikk/e/0/113131/
3. Lynne C. Lancaster (Author), David Stillman (Author): The M-Factor: How the Millennial Generation Is Rocking the Workplace, HarperCollins, 2010
4. Kelemen László: Nem sztereotípiák, IT-business, 2008. szeptember 28, VI évf. 37. sz.
5. Szonda Ipsos felmérés, 2013, http://www.ipsos.hu/site/legink-bb-a-t-v-b-l-t-j-koz-dnak-a-fiatalok/
6. Tari Annamária: Y-Generáció-klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban. Jaffa Kiadó, Budapest, 2010
7. Dr. Csiszárik-Kocsir Ágnes PH.D.: A huszonéves fiatalok pénzügyi alapfogalom-ismerete egy kérdőíves kutatás eredményinek tükrében, 2013, http://kgk.sze.hu/images/dokumentumok/VEABtanulmanyok/csiszarik_kocsir_agnes.pdf
8. 41/1997. (III. 5.)-es kormányrendelet
9. Sommkuti Bálint: A negyedik generációs hadviselés – az érdekérvényesítés új lehetőségei. PhD értekezés, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Hadtudományi Doktori Iskola, 2012
10. Sági Norbert – Dr. Magyar Sándor: A kiberbűnözés legújabb trendjei, Kommunikáció 2014 konferenciakiadvány, 2014, ISBN 978-615-5491-94-8