DOI: 10.18427/iri-2016-0023

Társadalom és információbiztonság. A humán információbiztonság a digitális korban

Kollár Csaba
Nemzeti Közszolgálati Egyetem, Budapest
kollar.csaba@uni-nke.hu

Bevezetés

Az információs társadalom, illetve azzal párhuzamosan futó, majd azt idővel leváltó digitális kor, vagy más néven az adatok kora a korábbi korokkal ellentétben már elsősorban nem a materializálódott, hanem a szimbolikus gazdasági javakra, vagyis az adatokra, az információkra, s az ezekből képzett tudásra fókuszál. Az adatok, az információk és a tudás felértékelődése számos folyamatot indít el, a tanulmány ezek közül elsősorban kettővel foglalkozik. Egyfelől ezen javak birtokosai idővel megtanulják értékelni ezeket a javakat, s erőforrásokat organizálnak a tárolásra, a védelemre, a műszaki/informatikai megoldások szükségszerű javítására. Másfelől az értékek közvetlen (pl.: adatlopás), vagy közvetett (pl.: adathordozó) megszerzése a társadalom egészét érintő újfajta bűnözői csoportok megjelenését és számának dinamikus növekedését jelzi.

A társadalom tagjainak jelenleg még szokatlan az újfajta értékfókusz. Az idősebbek egy része idegenkedik az új eszközöktől és alkalmazásoktól, a fiatalabbak pedig – különösen az Z generáció tagjai – ugyan magától értetődő természetességgel használják ki a digitális kor által nyújtott digitális lehetőségeket, de megfeledkeznek az ezeken a platformokon megjelenő veszélyektől. A kíberbűnözés tág fogalmi kerettel bír, s beletartozik többek között a személyes, illetve titkosnak minősített vállalati/szervezeti információk megszerzése, a jelszóval védett személyes fiókokba (pl.: Facebook), vállalati intranetes hálózatokba történő illetéktelen belépés, a személyiséglopás, a személyről, illetve a vállalatról rendelkezésre álló információk ártó szándékú megváltoztatása, illetve hamis információk terjesztése. A tanulmány a társadalom tagjait és csoportjait (beleértve a vállalatokat is) érő, social engineering típusú támadásokat és ezek lehetséges elkerülésének módjait mutatja be a humán információbiztonságra fókuszálva.

Egyén, közösség, társadalom

Az ember társas lény (Aronson, 2008), aki rendszerint már születésétől fogva egészen haláláig megannyi csoport tagja lesz. Az egyén – amennyiben nem jellemző rá a szélsőségesen deviáns és aszociális viselkedés – törekszik arra, hogy megfeleljen a csoportnormáknak.

Számos olyan csoport létezik, amelyik hatást gyakorol(hat) a társadalom tagjára, az egyénre. Egy lehetséges felosztás szerint létezik elsődleges és másodlagos csoport (Kotler, 1999 referenciacsoportjai; Giddens, 1997), továbbá aspirációs és aszociális csoport (Kotler, 1999), formális és informális csoport (Szabó, 1998), illetve nyílt és zárt – szélsőséges esetben karcerszervezet (Goffman, 1961) csoportjai.

Az elsődleges csoport (informális csoport) az, amelyiknél az egyének közötti kölcsönhatások, interakciók folyamatosak. Ide sorolhatóak a család, a bárátok, a szomszédok (nagyvárosi kultúrában rendszerint nem) és a közvetlen munkatársak. Az interakciók folyamatossága – ha annak célja a párbeszéd és a kapcsolatok ápolása – azt eredményezheti, hogy leginkább ezek azok a csoportok, illetve ennek tagjai azok, amelyek a csoportok közül a legnagyobb hatást tudják gyakorolni az egyénre, alakítják értékrendjét, formálják kultúráját. A másodlagos csoportok formálisabbak, a kommunikáció formalizált módon (séma) történhet, kevesebb egyénieskedést enged meg. Ide tartozhatnak a vallási, munkahelyi, iskolai, szakszervezeti csoportok, illetve a szakmai szövetségek. A másodlagos csoportoknál is megfigyelhetőek olyan személyek (véleményvezérek), akikre az egyén jobban hallgat, illetve kialakulhatnak baráti kapcsolatok, de akkor azok már nem a formalizált kommunikáció szabályait fogják követni. Ezek a csoportok – állítja Kotler (1999) – mint referenciacsoportok az egyént újfajta magatartás és életmód felvételére késztetik, hatnak egyéni viselkedésére és énképére. Vannak olyan csoportok, amelyeken az egyén kívül helyezkedik el. Ezekhez vagy tartozni szeretne (aspirációs csoport), mert a csoporthoz tartozás a számára előnyöket, elismerést, presztízst, stb. jelent, vagy nem (aszociális csoport), mert az ilyen csoportok értékrendje, normarendszere nem elfogadható a számára. A fentebb leírtak a digitális korra is igazak. A nyílt csoportok leginkább az olyan közösségekhez hasonlítanak (pl.: nyílt Facebook csoport), akik mindenkit (örömmel) befogadnak. Ez azt is jelenti, hogy a csoporthoz való tartozás nem jár különösebb erőfeszítéssel az egyén részéről, de – rendszerint – ha csak nem kap sok megerősítő impulzust és megannyi kellemes élményt, akkor nem kötődik különösebben a csoporthoz (ezért fontos, hogy milyen tartalmakat osztanak meg egymással a csoporttagok, vannak-e trollok stb.).

A zárt csoportokba vagy eleve nem lehet önként bekerülni, vagy a bekerülés csak bizonyos feltételek megléte esetén valósulhat meg (pl.: egy Linkedin csoport csak akkor fogadja el a jelentkezést, ha az egyénnek a csoport számára értékes és igazolható szakmai múltja van). A csoportok kialakítják a maguk szabályait, amihez rendszerint ragaszkodnak. Aki nem fogadja el azokat, azt a csoport, vagy kiveti magából, vagy az admin kizárja.

Riesman (1996) elképzelése szerint a magányos tömeg „főszereplője a kívülről irányított ember: a XX. század (és vélhetőleg a XXI. század – szerző) gyermeke” (Kerékgyártó, 2006). A kívülről irányított ember három altípusra osztható: (1) autonóm, (2) beilleszkedő, (3) anómiás.

Az autonóm ember Kerékgyártó (2006) szerint „érzékenysége, fogékonysága és nyitottsága folytán képes alkalmazkodni a beilleszkedés szabványához, de megválaszthatja, hogy akarja-e ezt megtenni vagy ellenszegül.” Az autonóm ember önképet alkot, s ennek része az is, hogy meghatározza, hogy milyen információkat akar, s milyeneket nem akar megosztani nyilvánosan. Az ilyen ember elemzi szükségleteit (pl.: milyen adatokra van szüksége a boldogulásához), s elvárja a társadalom működését szabályozó rendszerektől (pl.: törvénykezés), hogy ebben őt támogassák, segítsék. Fontosnak tartja saját folyamatos fejlődését, minél tudatosabban akarja sorsát irányítani, s ennek része az is, hogy tudatosan alakítja és fejleszti biztonságtudatosságát. Felméri a digitális kor lehetőségeit és veszélyeit, s legjobb tudása szerint mindent megtesz azért, hogy a lehetőségeit kihasználja, a veszélyeit pedig minimalizálja. Az autonóm ember, mint életstratégia Riesman (1996) szerint is sikerstratégia, amiben nem csak az egyén, hanem a környezete boldogulása is megjelenik.

A beilleszkedő altípus – akit tömegembernek is hívhatunk – a lehetőségekhez képest a kényelmi- és komfortzónáján belül maradva általában megteszi azt, amit elvárnak tőle. Rendszerint ő az, aki szenvtelenül elmegy az utcán fekvő magatehetetlen ember mellett, s ő az, aki bár tudomást szerez arról, hogy fiatalkorú ismerősét az interneten pedofilok zaklatják, vagy, hogy a munkahelyén a részeg kolléganőről a vállalati bulin készített meztelen fotókat az egyik kolléga nyilvánosan megosztotta egy weblapon, de nem tesz érdemben semmit. Nem akar részese lenne az ilyen történéseknek, nem szól, tudatosan nem veszi észre, nem akar tanúskodni, nem akarja a kollégával meglevő kapcsolatot tönkretenni. Figyel arra is, hogy haverjai és barátai előtt jól viselkedjen, nekik ne okozzon csalódást.

Az anómiás egyén ugyan mindent megtesz azért, hogy a társadalom tagja legyen, de próbálkozása hosszabb távon sikertelen, illetve a csoporttagság elvesztését képtelen megfelelő módon feldolgozni. Nem vonható egyértelmű párhuzam az anómiás személyek és a (kíber)bűnözés között, de Agnew (1997) általános feszültségelmélete alapján feltételezhető, hogy az átlagnál nagyobb valószínűséggel válnak/válhatnak bűnözővé. Az anyagi célok elérése mellett az alábbi események keltenek feszültséget:

- az egyén nem képes elérni az általa, vagy környezete által pozitívan értékelt célokat. Ez a (belső) feszültség arra vezeti őt, hogy törvénytelen eszközöket vegyen igénybe. Pl.: a számítástechnikához profi módon értő fiatal rövid időn belül szeretne nagyon gazdag lenni, s emiatt – engedve a kísértésnek – olyan hacker lesz, aki a vállalati adatok, adatbázisok megszerzése és értékesítése révén viszonylag hamar komolyabb bevételhez tud jutni.
- az egyén elveszti környezetétől a pozitív ösztönzést (pl.: szakítás, válás, munkanélkülivé válás, hozzátartozók halála, emberi kapcsolatok elvesztése). A feldolgozatlan élmény bosszúvá fordulhat át, az egyén bosszút akar állni mindenkin, akit felelősnek tart. Pl.: a munkahelyéről elbocsájtott munkavállaló törli a vállalat adatait a felhőben, vagy a kikosarazott udvarló feltöri szíve választottja Facebook és e-mail fiókját.
- az egyént negatív ösztönzések, vagy más szóval stresszhelyzetek érik. Ilyen stresszhelyzet lehet pl. az őt ért fenyegetés és bántalmazás, a munkahelyi problémák. Az egyén ahelyett, hogy logikusan és értelmesen megoldaná a problémákat, menekülni akar előlük, vagy bosszút akar állni az őt ért sérelmekért, vagy véget akar vetni a problémának. Pl.: az egyik vezetőtől kapott kritika miatt a munkavállaló létrehozza a vezető hamis Facebook profilját (klónozza azt), megszerzi a kapcsolati hálóját, majd a nevében hamis üzeneteket küld, vagy akár a családját is tönkreteszi információk (pl.: megcsalás) megosztásával.

A társadalom tagjai és a social engineering

A social engineering kifejezést – amennyiben lefordítjuk – pszichológiai manipulációnak hívhatjuk, s olyan eljárások és módszerek összességét értjük alatta, amikor az emberek nagy részére jellemző pszichológiai ismérveket használják ki a támadók arra, hogy az egyéntől jelszavakat szerezzenek meg, védett rendszerekbe jussanak be, az egyén digitális klónozásával hamis kapcsolatokat építsenek ki, bizalmas adatokhoz és információkhoz jussanak hozzá. Az emberek többségére igaz, hogy:

- kerüli a konfliktust
- ha segítséget kérnek tőle, akkor segíteni akar
- könnyen belemegy a női-férfi szerepjátékokba (szerepcsapda)
- kíváncsi
- szereti, ha szeretik
- örül a kedves szónak, szimpatizál a kedves emberrel
- társas lény, aki igyekszik fenntartani az emberi kapcsolatait
- ha felszínesen is, de elfogadja a tekintélyt (pl.: főnök-beosztott viszony, öltönyös ember)
- fél az ismeretlen dolgoktól (pl.: főleg idősebbek félelme a technikai eszközöktől)

A social engineering rendszerint az információbiztonság humán oldala, mely a gyakorlatban kiegészül (különösen csoportosan elkövetett támadások során) hackerismeretekkel is.

Információbiztonság és -veszély a társadalomban

Az alábbiakban az információbiztonság és –veszély gyakoribb előfordulásai és a veszélyek csökkentésére vonatkozó fontosabb megoldási javaslatok olvashatóak. A megoldási javaslatok Oroszi (2008), Schneier (2010), Mitnick és Simon (2006), Warren és Streeter (2005) munkái, a Youtube releváns dokumentum- és előadás-videóinak elemzése, valamint Kollár és Poór (2016) kutatási jelentése alapján készültek, terjedelmi korlátok miatt több pontban csak felsorolás jelleggel.

1. *Eszközök (általában)*: ellopás, elvesztés, eladás, kölcsönadás, szervizeltetés. Megoldás lehet (a) hogy az eszközökre csak jelszóval lehet belépni, (b) az értékes adatokat tartalmazó, ellopott/elveszett eszközök (pl.: okostelefon, laptop) visszavásárlása, jutalom a „becsületes” megtalálónak, (c) ha a tettes ismert, mihamarabb meg kell tenni a büntetőfeljelentést, (d) Az eladásra szánt eszközöknél eladás előtt el kell végezni az adatmentesítést (végleges törlés), (e) csak ismert szervizbe javasolt bevinni az elromlott eszközt, (f) Lehetőleg ne adjuk senkinek sem kölcsön az eszközöket/írható adathordozókat.
2. *Eszközök (okostelefon, számítógép, laptop) és alkalmazások feltörése*, de még inkább az ezekbe történő nem programozói tudást feltételező bejutás. Megoldási lehetőségek: (a) tudatosítjuk magunkban, hogy nem kell mindent eseményt azonnal megosztani, (b) bonyolultabb jelszót/jelszókat használunk, (c) időnként cseréljük a jelszókat.
3. *Eszközök vírusfertőzése.* Megoldási lehetőségek: (a) még az ismerősöktől érkező csatolt dokumentumokat is kellő óvatossággal kezeljük (pl.: ha csak csatolt fájlt küld minden kísérőszöveg nélkül), (b) a telepített szoftverek által megjelenített automatikus figyelmeztetések figyelembe vétele, (c) vírusellenőrző szoftver használata, (d) idegen forrásból származó (pl.: megtalált) adathordozót nem csatlakoztatjuk a számítógéphez.
4. *Eszközökről és távoli helyekről (felhő) történő adatlopás.* Megoldási lehetőségeket (a) lásd fent, illetve (b) megfelelő belépési jelszó és/vagy biometrikus azonosítás használata, (c) olyan alkalmazás használata, amelyiknél lehetőség van az azonosításnál időkorlát beállítása.
5. *Az eszközökön és távoli helyeken (felhő) történő adatmódosítás.* Megoldási lehetőségeket lásd fent.

6. *Az eszközökön és távoli helyeken (felhő) történő adattörlés.* Megoldási lehetőségeket (a) lásd fent, valamint (b) a fontos adatokról célszerű másolatot készíteni.
7. *Weboldalak feltörése és/vagy elérhetetlenné tétele és/vagy az itt található információk módosítása.* Ennek elsődleges célja az itt található információk törlése, módosítása. A megoldás rendszerint nem az egyén feladata, de az egyénnek célszerű tudatosítania, hogy fenntartásokkal kell kezelnie a webes tartalmak valódiságát.
8. *Az egyén adatait tartalmazó adatbázisok feltörése és onnan adatok ellopása.* A megoldás rendszerint nem az egyén feladata, de az egyénnek (a) célszerű tudatosítania, hogy nem szükséges minden lehetséges helyre regisztrálni, (b) ha az egyén mégis kíváncsi, akkor az ilyen helyekre egy újonnan, erre a célra létrehozott e-mail-lel érdemes regisztrálni. Célszerű továbbá azt is tudatosítani, hogy (c) a regisztrációs oldalakon egyedi név/e-mail cím és jelszó párost érdemes használni.

Három klasszikus social engineering technika

Számtalan social engineering technika létezik, ezek közül tanulmányom hármat nevez meg:

1. *Illetéktelen behatolás valamely vállalat székhelyére/telephelyére*. A támadók ilyenkor elsősorban hamisított belépőkártyával, megnyerő modorral, a vállalat (felső)vezetőjére történő hivatkozással, a férfi-női szerepek hangsúlyos játszásával, a megtámadott fél anyaszerepének és az emberi hiszékenység kihasználásával, s csak másodsorban programozói és hálózati ismereteik birtokában képesek bejutni az épületbe.
2. *Adathalászat.* Vagy a behatolás után gyűjtött információk (pl.: asztalra ragasztott belépési jelszó, nem megsemmisített dokumentumok), vagy a behatolástól függetlenül szerzett információk „halászata”. Az egyének megannyi információt adnak meg magukról publikus formában a közösségi oldalakon (pl.: név, életkor, családi állapot, iskolai végzettség, lakhely, születésnap kirándulások, fényképek, kapcsolati háló), melyekből könnyen összerakható az egyén közel teljes profilképe.
3. *Személyiséglopás, megszemélyesítés.* Az adatok alapján megalkotható egy olyan személyiségprofil, amelyik el tudja játszani, hogy ő az igazi személy (pl.: azt hazudja az ismerősöknek, hogy feltörték a Facebook fiókját, s ezért újat regisztrált). A visszaélés lehet egy bizalmas, intim fénykép nyilvános megosztása, vagy egy profilkép és néhány egyéb adat ismeretében egy hamis felhasználói profil létrehozása. Egy ilyen hamis profil alkalmas lehet arra, hogy a gyanútlan egyénről hosszabb távra is hamis képet építsen, a nevében mindenféle nemkívánatos oldalakra regisztráljon, ott véleményt fejezzen ki. Mivel a digitális lábnyom a szervereken és a logfájlokban akkor is megmarad, ha az adatok már nyilvánosan nem elérhetőek, így gyakorlatilag egy életre megmarad ez a hendikep.

Összefoglalás

Földi (2002) szerint mind „az emberi szabadság oltalma, mind pedig a társadalom biztonsága hallatlan mértékben felértékelődik. Ennek a kihívásnak is csak magasabb elméleti felkészültséggel tudunk megfelelni.” A társadalom, s annak tagjai még csak most tanulják, hogy mit is jelent a biztonság a digitális korban. Miközben a fizikailag megfogható (materializálódott) dolgok védelme (pl.: riasztórendszer telepítése, objektumvédelem, kiemelt személyek védelme) egyre több ember és vállalat számára magától értetődik, addig az adatok és adathordozók, valamint a személyes és vállalati/szervezeti adatok és információk védelme viszonylag rövid múltra tekinthet vissza. Annak ellenére, hogy a technikai lehetőségek egy része adott a védelemhez, az igazi gyenge pont valamennyi rendszerben a humán tényező. Ennek számos oka van, ahogy arról fentebb is írtam.

Ami a jövőt illeti: számát tekintve a jelenleginél lényegesen több (rosszindulatú) social engineerrel, hackerrel és egyéb kíberbűnözővel kell majd a társadalomnak felvennie a harcot. A megállíthatatlan technikai fejlődés pedig számos esetben csak növeli a technikai színvonal és a törvényalkotás és -alkalmazás közötti időbeni távolságot. A kiterjesztett valóság, a drónok, az IoT eszközök megannyi új biztonsági kérdést vetnek fel, melyekre a társadalom tagjai közül elsősorban csak a képzett, tudatos, autonóm emberek tudnak majd hatékony válasz adni.

Irodalomjegyzék

Agnew, R. (1997). *The Future of Anomie Theory.* Boston: Northeastern University Press.

Aronson, E. (2008). *A társas lény.* Budapest: Akadémiai.

Földi P. (2002). *Filozófia és biztonság.* Budapest: Clavis.

Giddens, A. (1997). *Szociológia.* Budapest: Osiris.

Goffman, E. (1961). *Asylums: Essays on the Social Situtation of Mental Patients and Other Inmates.* Harmondsworth: Penguin.

Kerékgyártó Á. (2006). Az értékválságok ideológiája. *Világosság*, (3), 17-26.

Kollár Cs., & Poór J. (2016). *Szervezetek a digitális korban. Rövid kutatási jelentés.* Budapest: PREMA Consulting.

Kotler, P. (1999). *Marketing menedzsment.* Budapest: Műszaki.

Mitnick, Kevin D., & Simon, William L. (2006). *A legendás hacker. A behatolás művészete.* Budapest: Perfact-Pro Kft.

Oroszi E. (2008). *Social engineering.* Budapest: BCE.

Riesman, D. (1996). *A magányos tömeg.* Budapest: Polgár.

Schneier, B. (2010). *Schneier a biztonságról.* Budapest: HVG.

Szabó I. (1998). *Bevezetés a szociálpszichológiába.* Budapest: Nemzeti Tankönyvkiadó.

Warren, P., & Streeter, M. (2005). *Az internet sötét oldala.* Budapest: HVG.