XXII. Fiatal Műszakiak Tudományos Ülésszaka, 2017. Kolozsvár, 327–330. DOI: 10.33895/mtk-2017.07.74
http://hdl.handle.net/10598/29837

A BIZTONSÁGTUDATOSSÁG FEJLESZTÉSÉNEK EGYES LEHETŐSÉGEI

SOME SAFETY AWARENESS DEVELOPMENT OPPORTUNITIES

Nyikes Zoltán

Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 1034 Magyarország Budapest, Bécsi út. 96/b, nyikeszoli@gmail.com

Abstract

Digital world hides enormous possibilities for us, what we can't imagine totally nowadays. Even that the digitalization is global in all parts of the life means everybody like potential user needs to be ready to use expansively the information safety viewpoints. Without this capabilities the users will be unprotected and defenceless again the harmful attacks from anywhere of the world because this is a virtual "new world". Essential assumption of the safety initiation for "expert" professionals is the safety awareness development of users.

***Keywords**: safety awareness, cyber safety and security, information security*

Összefoglalás

A digitális világunk hatalmas lehetőséget rejteget számunkra, amit még nem is nagyon tudunk elképzelni. Viszont, miután a digitalizáció az élet minden területét átszövi, szinte mindenkinek fel kell készülni, mint potenciális felhasználónak, az információbiztonság szempontjainak a széleskörű alkalmazására. Ugyanis, ha ezt a felhasználók nem teszik meg, abban az esetben védtelenek lesznek és kiszolgáltatottak, egy olyan „új" világban, ami kézzel nem megfogható és lehet, hogy az ellenünk elkövetett ártalmas cselekmények a Világ másik szegletéből indultak. Ezért a felhasználók biztonságtudatosságának növelése elengedhetetlen feltétele kellene, hogy legyen a „hozzáértő" szakemberek számára.

***Kulcsszavak:** biztonságtudatosság, kiberbiztonság, információbiztonság*

1. A digitális világ kihívásai

Korunkban, amikor az internet és az informatika fejlődése megváltoztatta életünket és annak mindennapjait, annak hatására kitárult a világ. Az információ gyors és szabad áramlása az életünket is felgyorsította. Gyorsabban élünk, több információ, több impulzus ér minket. Ennek már akkora a befolyásoló hatása, hogy már-már függői lettünk az információáradatnak. Viszont a társadalom ebből a szempontból kettészakadt, a fiatalabb és az idősebb generációk között éles a kontraszt.

1.1. A generációs probléma

A 35 évnél idősebb generációk számára az informatikai eszközök és alkalmazások használata kihívást jelent. Az informatikai robbanást mindenki megérezte, a többség rendelkezik internet hozzáféréssel, annak használata már a funkcióját tekintve inkább csak a szórakoztatást és a kapcsolattartást szolgálja. Az internet és az informatikai

eszközök adta lehetőségek nem, vagy csak nagyon korlátozott számban kerülnek kihasználásra. Ez különösen nagy veszélyt rejteget, mert ezek a korosztályok ez által leszakadnak, és saját magukat rekesztik ki a digitális jólétből.

1.1.1. A fiatalabb generációk esélyei

Ezzel szemben a 35 évnél fiatalabb korosztályok már teljes természetességgel használják és alkalmazzák a digitális világ adta lehetőségeket. Használják az internetet, használják a különböző informatikai eszközöket. Itt is jellemző a szórakozás és a kapcsolattartási funkciók elsődleges használata, de sokkal szélesebb körben alkalmaznak egyéb, az internet és az informatikai eszközök által biztosított más lehetőséget. Nem okoz problémát elsajátítani egy-egy új funkcióval bíró alkalmazást. Ez azért alakulhatott így ki, mert ezek a korosztályok vagy már nagyon kicsi gyerekkoruk óta ebben a digitális világban élnek, vagy már eleve ebbe születtek bele és teljesen természetes a számukra digitális jelenlét [1].

1.2. A digitális világ veszélyei

Azonban minden esetben elmondható, úgy ebben az esetben is, hogy a digitális világ számtalan veszélyt rejteget a számunkra. Elsősorban azokra, akik használják azt, de másodsorban azokra is, akik nem túl aktívak a digitális világban, vagy egyáltalán nem is használják azt. Mivel életünk és a társadalmunk működésének döntő többsége már a digitális térbe tevődött át, és kikerülhetetlenül azon keresztül zajlik, ezért annak a biztonsága rendkívüli fontossággal kell, hogy bírjon mindenki számára.

1.2.1. A digitális élet „kezdetén"

A biztonságtudatosság és a védelmi reflexeink még nem alakultak ki úgy, mint ahogy az a fizikai valós térben, az evolúciós fejlődés során évezredek során már biztosította az ember túlélését. A digitális térben történő élet nem nyúlik vissza évezredekre, de még évszázadokra sem. Az elmúlt negyed évszázadban indult meg és vált egyre népszerűbbé a digitális világ. Azonban annak felfedezése nem szorítkozott elsősorban a biztonságos tevékenységre. Mint ahogy minden új dolognak és térnek a felfedését nem a biztonságosság jellemezte, úgy a digitális tér felfedezését sem.

1.2.2. Digitális világ vs. fizikai világ

A digitális, virtuális vagy kiber világot összevetve a fizikailag valós terek felfedezésével, úgy, mint itt a tengerek, a légtér, vagy akár a világűr felfedezése és az első használói számára sem a biztonság volt az elsődleges szempont. Miután széleskörben elterjedt azok használata, egyrészt kialakult egyfajta biztonsági reflex, másrészt a számos, a biztonságot érintő szabályozás történt az adott területeken. A digitális térre a biztonsági reflexek kialakulása és a biztonsági szabályozások még nem túl régóta kezdődtek meg [2].

1.2.3. A szabályozás

De mit sem ér a szabályozás, hogyha az csak követi az eseményeket, nehézkes és egyébként sem tartják be, mert adott személyre az internet világában már nem érvényes. Gondolok itt arra az anomáliára, hogy a törvények és jogszabályok csak a fizikális világban, a földrajzilag elkülönített közigazgatási egységekre vonatkoznak. Úgy, mint különböző szintű önkormányzatok, országok vagy szövetségi egységek. De például a magyar szabályok már nem vonatkoznak az ellenünk más országból elkövetett kiberbűntények idegen állampolgárjaira. Egy ázsiai hackert nem tart távol egy uniós, vagy magyar szabályozás attól, hogy feltörje a közösségi profilunkat és visszaéljen adatainkkal. Ennek ellenére hiszem és vallom, hogy

márpedig a társadalmi rend alapja maga a törvénykezés. E nélkül anarchia uralkodna.

2. A biztonságtudatosság kérdései

Viszont a törvénykezés kevésnek bizonyul, ha az emberek nem a törvény szellemében élnek és önmaguk nem tesznek a saját biztonságuk érdekében a fizikai valóságban és a kibertérben egyaránt. Teljesen alapvető dolog, hogy az emberek a lakásuk ajtaját bezárják, és kulccsal becsukják, ha riasztójuk van, azt is élesítik.

2.1. Biztonsági reflexek

Az autóba, ha beszállnak, bekapcsolják a biztonsági övet és betartják a közlekedési szabályokat, ha pedig az út- és látási viszonyok romlanak, akkor csökkentik a sebességet és fokozottabban figyelnek vezetés közben. Az is teljesen természetes, hogy nem mennek egyedül éjszaka olyan környékre, ahol tudvalevő a magas bűncselekmények száma és nem vásárolnak az utcán kétes kinézetű személyektől értékes dolgokat.

2.1.1. Prevenció a biztonság területén

Vizsgálataim ennek mintájára a kibervilágban zajló életünk biztonsági kihívásaira keresnek választ, mert mint az egészségügyben is a prevenció sokkal kevesebbe kerül, mint az elvesztett egészség visszaszerzése, a megelőzés itt is elsődleges. Mindig az embert kell meggyőzni arról, hogy tegyen magáért, az egészségéért még a betegséget megelőzően, így a kiberbiztonság tekintetében is magának az embernek a biztonságtudatosságát kell növelni az elkerülhető incidensek megelőzésének érdekében.

2.1.2. Információbiztonsági tudatosság

De a biztonságtudatosság növekedése akkor érhető el a felhasználók körében, ha tudják és értik, hogy mit is csinálnak az interneten az informatikai eszközeikkel különböző alkalmazások segítségével, egyszóval magas a digitális kompetenciájuk és a digitális kulturáltságuk. Természetesen, ahhoz, hogy legyen mivel védekezni a veszélyek ellen, a terület szakembereinek gondoskodniuk szükséges a megfelelő szabályzók kidolgozásáról, a technikai megvalósításról is, úgy, mint a megfelelő szabványok valamint a szükséges hardver és szoftver eszközök fejlesztéséről is [3].

3. A megelőzés, mint a védelem eszköze

A prevenció, mint ahogy említettem sokkal hatékonyabb és kifizetődőbb az információbiztonság területén is. Több okból kifolyólag [4].

3.1. A „leggyengébb láncszem”

Először is, mint tudjuk, az ember a leggyengébb láncszem minden rendszerben. Nem létezik olyan védelem, amit emberek ne lennének képesek kijátszani, feltörni. Amit ember tervezett, azt ember képes feltörni.

3.2. „Black Box”

Másod sorban, a felhasználó oktatása a biztonságtudatosságra sokkal kifizetődőbb sok esetben, mint méregdrága „black box”-ok megvásárlása és integrálása, ami a gyártó szerint „mindentől” megvéd. Még a leghatékonyabb védelmi technológia alkalmazása sem ér sokat, ha az emberek nem tudatosan cselekszenek és azt sem magas fokon teszik. Legyen az a munkahelyen vagy a magánéletben. Bár ez sokszor már nem különíthető el, mivel már a technológiák alkalmazása során keveredik sokszor a biznisz és a privát szféra, gondoljunk csak a céges telefonok használatára [5].

3.3. A „példakép”

Harmad sorban, a felhasználó oktatása nem csak önmagára lesz hatással, hanem a szűkebb és tágabb környezetére is. Ha egy

felhasználó megfelelő (magas) szintű, rendszeres és aktuális képzést kap, ami számára nem az unásig ismételgetett „dogmákat" tartalmazza, abban az esetben megfelelően motivált lesz arra, hogy a közvetlen munkahelyi környezetében is és a magánéletében, a családjában példa értékű viselkedésével a környezetét is a biztonságtudatosságra ösztönözze [6].

3.4. Ez „nem paranoia"

Természetesen önmagában csak a felhasználók biztonsági oktatása nem elegendő. A biztonsági éberség fenntartása mindenki érdeke. A biztonsági éberség nem csak az IKT (Infokommunikációs Technológia) eszközök alkalmazása esetén elegendő. Már a közvetlen fizikális környezetünk folyamatos felügyelete is ide sorolható, mert ha gyanús személyt, elhagyott tárgyat, szokatlan eseményeket észlelünk és azt az illetékes szakemberek számára jelezzük, előfordulhat, hogy egy komoly biztonsági eseményt előzünk meg ezzel. Ez természetesen az egészséges biztonsági érzet határát nem lépheti át és nem válhat paranoiás szokássá.

4. Következtetések

A biztonságtudatosság magas fokú megtartása nem csak az egyén érdeke, hanem a társadalom részéről is nagyon fontos. A gazdasági szereplők akkor tudnak hatékonyan termelni és szolgáltatni, hogyha a biztonsági feltételek megfelelőek és nem pl. a kibertámadások által okozott károkra kell fordítani a megtermelt javakat. A kormányzat számára is fontos az egyén biztonságtudatosságának magas szinten tartása, mert ha az állampolgár biztonságban tudja magát, abban az esetben hatékonyabban tudja élni az életét, fizetni az adóját és elégedettsége jeleként eleget tesz az állampolgári kötelezettségeinek.

Szakirodalmi hivatkozások

[1] Lazányi Kornélia: *Stressed Out by the Information and Communication Technologies of the 21st Century.* SCIENCE JOURNAL OF BUSINESS AND MANAGEMENT 4:(1-1) pp. 10-14. (2016). http://article.sciencepublishinggroup.com/pdf/10.11648.j.sjbm.s.2016040101.12.pdf letöltve: 2017. január 31.

[2] Lazányi Kornélia *A biztonsági kultúra szerepe a vezetői döntések támogatásában.* Taylor: Gazdálkodás- és Szervezéstudományi Folyóirat: A virtuális intézet közép-európa kutatására közleményei 8:(1) pp. 143-150. (2016). http://vikek.hu/?page_id=11 letöltve: 2017 február 10.

[3] Rajnai, Zoltán; Fregan, Beatrix: *Kritikus infrastruktúrák védelme (jogi szabályozás).* XXI. Fiatal Műszakiak Tudományos Ülésszaka, 2016. Kolozsvár, 349–352. http://hdl.handle.net/10598/29102. letöltve: 2017. január 29.

[4] Lazányi Kornélia: *Who do You Trust? – Safety Aspect of Interpersonal Trust among Young Adults with Work Experience.* Proceedings of the11th IEEE International Symposium on Applied Computational Intelligence and Informatics SACI 2016. 412 p. Timisoara, Románia, pp. 349-354..http://ieeexplore.ieee.org/document/7507400/?reload=true, letöltve: 2017. január 30.

[5] Lazányi, K.: *A biztonsági kultúra*. Taylor: Gazdálkodás- és Szervezéstudományi Folyóirat: A virtuális intézet közép-európa kutatására közleményei 7:(1-2) pp. 398-405. (2015). http://vikek.hu/wp-content/uploads/2015/10/TAYLOR_2015-nyomdai.pdf, letöltve: 2017. január 31.

[6] Rubóczki, E.; Rajnai, Z.: *Moving towards Cloud Security.* Interdisciplinary Description of Complex Systems. INDECS, 13(1). pp. 9-14 doi:10.7906/indecs.13.1.2. http://hrcak.srce.hr/133681. letöltve: 2017. január 29.