HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 3. szám 81–95.
DOI: 10.32567/hm.2022.3.6

Bak Gerda,[1] Kelemen-Erdős Anikó[2]

Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján

Information Security Awareness from Generation Y Perspective Based on a Qualitative Approach

A digitális technológia behálózza életünk, a pandémia pedig tovább növeli és erősíti az elektronikus eszközökkel való kapcsolatunkat. Ezzel együtt a kibertámadások száma is jelentősen megnövekedett, annak ellenére, hogy ezek jelentős része megelőzhető lenne.

Jelen tanulmány célja az Y generációs fiatalok információbiztonsággal kapcsolatos attitűdjét, tudatosságát befolyásoló tényezők feltárása, mélyebb megértése kvalitatív jellegű empirikus kutatás, mélyinterjúk alapján. Az interjúk elemzése trianguláció keretében két megközelítésben, tartalomelemzéssel és *grounded theory* módszertannal történt. Az interjúk rámutatnak, hogy az alanyok jelentős tényezőként tekintenek elméleti síkon az online és digitális biztonságukra, azonban a gyakorlatban a megfelelő védekezési módok hiányossága, az alanyok sebezhetősége derül ki a kutatásból. Az alapozó jellegű kutatás további kvantitatív kutatás alapját képezheti.

Kulcsszavak: **információbiztonság-tudatosság, kiberbiztonság, Y generáció, mélyinterjú, tartalomelemzés, grounded theory**

Digital technology is embedded in our lives, and the pandemic will further increase and strengthen our connection to electronic devices. At the same time, the number

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bak.gerda@uni-obuda.hu
[2] Óbudai Egyetem Keleti Károly Gazdasági Kar Gazdaság- és Társadalomtudományi Intézet, e-mail: kelemen.aniko@kgk.uni-obuda.hu

of cyberattacks has increased significantly, despite the fact that a significant part of them could be prevented.

This study aims to explore and deepen the understanding of the factors influencing the attitudes and awareness of Generation Y youth towards information security, based on qualitative empirical research in form of in-depth interviews. The interviews were analysed using a triangulation approach with two perspectives: content analysis and grounded theory methodology. The interviews demonstrate that the interviewees consider their online and digital security as a significant factor on a theoretical level, however, the practice reveals the lack of appropriate protection methods and the vulnerability of the respondents. This foundational research can form the basis for further quantitative approaches.

Keywords: **information security awareness, cybersecurity, Generation Y, in-depth interview, content analysis, grounded theory**

1. Bevezetés

Az információbiztonság még mindig jelentős problémát okoz nemcsak a szervezetek számára, hanem az egyének életében is, annak ellenére, hogy számos technológiai megoldást, védekezési módot fejlesztettek ki a probléma leküzdésére,[3] s bár a szakirodalomban az a meglátás terjedt el, hogy az egyén a leggyengébb láncszem az információbiztonsági láncban,[4] mégsem sikerült erre megoldást találni.[5] Ez pedig akár egészen addig komoly problémákat okozhat, ameddig az egyének tudatosságát nem sikerül növelni.

Az információbiztonság-tudatosság (*information security awareness,* ISA) témakörét számos megközelítésből vizsgálják,[6] és annál is több kutatás próbálja feltárni, melyek azok a tényezők, amelyek hatással lehetnek az egyének és a szervezetek információbiztonság-tudatosságára, illetve annak mérése, növelése,[7] valamint előrejelzése miként lehetséges.

[3] Kevin Grant et al.: 'Risky Business': Perceptions of E-Business Risk by UK Small and Medium Sized Enterprises (SMEs). *International Journal of Information Management,* 34. (2014), 2. 99–122.

[4] Verena Zimmermann – Karen Renaud: Moving from a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset. *International Journal of Human-Computer Studies,* 131. (2019). 169–187.

[5] Gershon Hutchinson – Jacques Ophoff: A Descriptive Review and Classification of Organizational Information Security Awareness Research. In H. Venter et al. (szerk.): *Information and Cyber Security.* Cham, Springer, 2020. 114–130.

[6] Abdul Rahman Ahlan – Muharman Lubis – Arif Ridho Lubis: Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science,* 72. (2015). 361–373.; Bak Gerda – Kiss Sándor: A biztonságtudatosság szisztematikus szakirodalmi áttekintése. *Hadmérnök,* 16. (2021), 4. 85–99.

[7] Zeng Zhongping et al.: Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management. In *2013 Fourth International Conference on Digital Manufacturing & Automation.* IEEE, 2013. 684–687.

A viselkedési modelleket alapul vevő kutatások megpróbálják megérteni és magyarázni az egyén és a biztonság, valamint a technológia viszonyát.[8] A viselkedéstudományi megközelítések közelebb visznek a releváns aspektusok megértéséhez, azonban az egyén vagy szervezet információbiztonság-tudatosságának hátterét nem képesek megvilágítani.[9] Jelen kutatás célja az információbiztonság-tudatosságot befolyásoló egyéni tényezők feltárása és azonosítása, valamint az interjúalanyok információbiztonság-tudatosságról alkotott képének, illetve a digitális technológiában rejlő veszélyek ismeretének vizsgálata, aminek következtében növelhető a tudatosság a digitális eszközöket használók körében, esetlegesen csökkenthetők és/vagy megelőzhetők a kibertámadások mind mennyiségben, mind az okozott károk értékében, hatásaiban.

Kutatásunkban az Y generációra fókuszálunk, az 1980 és 1994 között születetteket vizsgáljuk.[10] Számos, akár ettől eltérő kategorizálás létezik a generációs megkülönböztetésre, ugyanakkor azért választottuk a magyar szerző kormeghatározását, mert alapvetően történelmi, társadalmi fejlődésbeli eltérések határozzák meg az egyes generációk elkülönülését.

Ennek alapján a következő kutatási kérdéseket fogalmaztuk meg:

K1. Hogyan érzékelik a megkérdezett Y generációs fiatalok az információbiztonsági kockázatot?

K2. Mely tényezők határozzák meg az Y generációs interjúalanyok információbiztonság-tudatosságát?

K3. Mely tényezők járulhatnak hozzá az Y generációs interjúalanyok információbiztonság-tudatosságának fokozásához?

A cikk első felében szakirodalmi áttekintés keretében az információbiztonság-tudatosság témakörét vizsgáljuk, majd az Y generáció körében végzett kvalitatív mélyinterjúk elemzésére alkalmazott módszertant, a kvalitatív tartalomelemzést és a *grounded theory* módszertant mutatjuk be. Ezt követően a kutatás főbb eredményeit és további kutatási irányokat fogalmazunk meg.

2. Szakirodalmi áttekintés

A digitális technológia fejlődésével egyre több információt tárolunk digitális eszközeinken és a felhőben, a technológia nemcsak lehetőségeket, hanem biztonsági kockázatokat is magában rejt. A közösségimédia-felületek térnyerésével napjainkban egyre több információt tudnak megszerezni rólunk digitális lábnyomunk és digitális eszközeink nem megfelelő használatának eredményeképp. A felhasználók ennek következtében

[8] Burcu Bulgurcu – Hasan Cavusoglu – Izak Benbasat: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34. (2010), 3. 523–548.

[9] Kathryn Parsons et al.: Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security,* 42. (2014). 165–176.

[10] Tari Annamária: *Y generáció. Klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban*. Budapest, Jaffa Kiadó, 2010.

sokszor kellemetlen helyzetbe kerülhetnek, akár a saját, akár mások kárára, hiszen előfordulhat, hogy zsarolás áldozatai is lehetnek.[11] Mivel a döntéshozatal az egyének szintjén történik, az emberi tényező fontos szerepet játszik az információbiztonság szempontjaiban.

A szervezet információs rendszerének biztonságát gyengítő incidensek egyik leggyakoribb tényezője az alkalmazottak viselkedésére vezethető vissza.[12] A legmodernebb és legerősebb vírusirtórendszerek, szabályozások és egyéb védelmet célzó intézkedések ellenére, az alkalmazottak közül elég, ha csak egy valaki kaput nyit a támadók próbálkozásainak, mert ezáltal támadhatóvá válik a rendszer.[13] A technológiai biztonsági megoldásokra támaszkodva ezért soha nem tudjuk megfelelően megvédeni rendszereinket.[14] Fontos, hogy megértsük a megfelelő biztonsági viselkedéshez kapcsolódó emberi tényezőket, hogy ne csak a sebezhetőséget csökkentsük, hanem olyan képzési és oktatási programokat is tervezhessünk, amelyek ezeket a mögöttes tényezőket kezelik.

A *social engineering*[15] olyan támadásokra vonatkozik, amelyek során az embereket szándékosan manipulálják, hogy bizalmas információkat adjanak ki, vagy a támadó által kiszemelt személy vagy vállalat biztonságát veszélyeztető cselekményeket hajtsanak végre.[16] A támadás arra épít, hogy az egyének hiszékenyek és manipulálhatók.[17] A social engineering támadások fizikai, társadalmi és technikai szempontokat is tartalmaznak, amelyeket a támadás különböző fázisaiban használnak. Még ha egy ilyen támadás kezdetben sikertelen is, az egyéni és szervezeti biztonsági folyamatokba való betekintés felhasználható a jövőbeli támadásokhoz. A social engineerek olyan technikákat használnak, mint a célzott (szigonyozó) adathalászat *([spear] phishing),* a látszatüzenet, vagy egy kifejezőbb kifejezést használva operatív csapda *(pretexting),*[18] a célcsoport weboldalainak megfertőzése, a befurakodás *(water holing),* az adatkiszivárogtatás *(data breach),* a csalás *(scam),*[19] vagy a személyes adatokhoz, védett rendszerekhez való hozzáférés. Az adathalászat során a támadók főként e-mailek formájában szereznek az áldozataikról információkat, amelyet

[11] Samar Muslah Albladi – George R. S. Weir: User Characteristics that Influence Judgment of Social Engineering Attacks in Social Networks. *Human-centric Computing and Information Sciences,* 8. (2018), 1.

[12] Reza Alavi – Shareeful Islam – Haralambos Mouratidis: An Information Security Risk-Driven Investment Model for Analysing Human Factors. *Information & Computer Security,* 24. (2016), 2. 205–227.

[13] Sonja Stirnimann: *Der Mensch als Risikofaktor bei Wirtschaftskriminalität: Handlungsfähig bei Non-Compliance und Cyberkriminalität*. Wiesbaden, Springer, 2018.

[14] Steven Furnell – Kieran Millet – Maria Papadaki: Fifteen Years of Phishing: Can Technology Save Us? *Computer Fraud & Security,* (2019), 7. 11–16.

[15] A *social engineeringnek* nincs tudományos körökben széleskörűen elfogadott magyar megfelelője.

[16] Deanna Hauser: Social Engineering Awareness in Business and Academia. In *MWAIS 2016 Proceedings.* Wisconsin, 2016. 3–6.

[17] Oroszi Eszter Diána: Social engineering technikák. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 77–118.

[18] Magyar Sándor: *Adatbiztonság, adatvédelem az egészségügyben.* Előadás. Semmelweis Egyetem, 2019. március 4.

[19] Soudabeh Vahdati – Niloofar Yasini: Factors Affecting Internet Frauds in Private Sector: A Case Study in Cyberspace Surveillance and Scam Monitoring Agency of Iran. *Computers in Human Behavior,* 51. (2015), 180–187.

a későbbiekben akár egy további látszatüzenet keretében való támadás alkalmával felhasználnak. A célzott adathalászat esetében a célközönség szűkebb. A befurakodás során a célszemély által gyakran látogatott weboldalakat törik fel, és helyeznek el rajta vírust azzal a céllal, hogy így fertőzzék meg az áldozat számítógépét, vagy jussanak be a munkahelyi hálózatára.[20] Az adatkiszivárogtatás külső fél elektronikus vagy offline, sokszor titkos adatokhoz való szándékos vagy nem szándékos hozzáférése.[21] Az internetes csalás célja az áldozat(ok) becsapása,[22] amelynek során a csaló különböző módszereket alkalmaz az áldozatok személyes információinak ellopására és pénzügyi tranzakciók elvégzésére.[23] Ennek egyik legismertebb típusa az online vásárlásokhoz kapcsolódó csalás, amelynek során a csalók összegyűjtik az internetfelhasználók hitel- vagy bankkártyaadatait és PIN-kódját, amelyeket arra használnak, hogy pénzt hívjanak le az áldozat számlájáról.[24]

A social engineering biztonsági kockázataival kapcsolatos ismeretekkel nem rendelkező alkalmazottak a vállalat legnagyobb kockázatai közé tartoznak.[25] Jelen tanulmány az Y generációra fókuszálva kutatja az információbiztoság-tudatosság főbb tényezőit, hátterét.

3. Módszertan

Kvalitatív megközelítést, mélyinterjúkat alkalmaztunk a kutatási probléma mélyebb megértésére. A mélyinterjú lehetővé teszi, hogy a biztonságtudatosságot a fentiekben bemutatottaktól eltérő módon közelítse meg a tanulmány. Ez a módszertan hozzájárul a kutatási probléma és különösen annak érzékenyebb területe feltárásához.[26]

A vizsgálat eszközeként félig strukturált interjúkon keresztül tártuk fel az interjúalanyok információbiztonság-tudatosságának és az érzékelt kockázatnak a főbb tényezőit, illetve attitűdjüket.

Az interjúk átiratait tartalomelemzéssel és *grounded theory* (GT-) módszertannal, azaz megalapozott elmélettel elemeztük. A tartalomelemzés Krippendorff szerint egy komplex technika, amelynek segítségével a kutató nemcsak a szöveget, hanem a szöveg kontextusát is figyelembe véve értelmez és értékel.[27] A módszer lényege,

[20] Szappanos Gábor: Kártékony kódok használata a célzott támadások végrehajtásában. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 119–159.

[21] Freeha Khan et al.: Data Breach Management: An Integrated Risk Model. *Information & Management,* 58. (2021), 1. 103392.

[22] Tom Buchanan – Monica T. Whitty: The Online Dating Romance Scam: Causes and Consequences of Victimhood. *Psychology, Crime & Law,* 20. (2013), 3. 261–283.

[23] Vahdati–Yasini (2015): i. m. 31.

[24] Arokia Jesu Prabhu Lazar et al.: Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud. *Wireless Personal Communications,* (2021).

[25] Jéri Tamás: Az elektronikus levelezés és a kiberbiztonság összefüggései. *Hadmérnök,* 16. (2021), 2. 169–185.

[26] Hanna Kallio et al.: Systematic Methodological Review: Developing a Framework for a Qualitative Semi-Structured Interview Guide. *Journal of Advanced Nursing,* 72. (2016), 12. 2954–2965.

[27] Klaus Krippendorff: *Content Analysis. An Introduction to Its Methodology*. Thousand Oaks, SAGE, 2018.

hogy az interjúkban elhangzottakból induktív módon következtetünk az elhangzottak mögött megbújó, rejtett gondolatokra, tartalmakra, ezáltal felfedjük az elsőre nem észrevehető összefüggéseket.[28] Ugyanakkor az elméleti megközelítés integrációjával abduktív megközelítést alkalmazunk. Az alapvetően kvalitatív jellegű tartalomelemzés lehetővé teszi a narratívák alapján a kutatás szempontjából releváns tényezők feltárását, azonosítását.[29]

A GT-módszertan lényege, hogy a kvalitatív adatok értelmezéséből jutunk el az elmélethez közeli általánosabb szintű megfogalmazásokig. Mint a szövegelemzési módoknál, itt is lényeges hangsúly van a kódoláson és az elemzésen, akárcsak a kutatón, ami általában a kvalitatív kutatások egyik korlátozó tényezője.[30]

A félig strukturált interjúk során projektív technikák közül is alkalmaztunk két módszer, a szóasszociáción alapuló módszert, illetve a mondatkiegészítési technikát. A szóasszociáció lényege, hogy az elhangzott ingerszavakra a vizsgált alany a számára elsőként eszébe jutó gondolatot adja meg.[31] A mondatkiegészítés során alkalmazott nyitott mondatok, amelyeket az alanyoknak kell befejezni korlátlan és változatos válaszokat eredményeznek.[32] A projektív technikák révén kapott eredményeket beépítettük az elemzésbe.

3.1. A minta

Az interjúalanyok kiválasztása során szűrőkritériumot alkalmaztunk. Az Y generáció tagjait, vagyis az 1980–1994 között születetteket kértük fel. A megkérdezett interjúalanyok közül kettő a szakmai hátterét, illetve tapasztalatait tekintve kiemelkedik a többiek közül, hiszen a biztonságtudatosságot tekintve a többiekhez képest messzemenően mélyebb információkkal rendelkeznek a témában.

Az interjúk során 11 személlyel, 7 nővel és 4 férfival, foglalkozásukat tekintve 5 tanulóval és 6 munkavállalóval készítettünk interjút. Az elméleti telítődést ezzel a mintával jól sikerült közelíteni, miután az interjúalanyok válaszai már a hetedik válaszadót követően összecsengtek. Az életkor terjedelem 27–40 év. Az aktuális pandémiás helyzet miatt az interjúk átlagosan 1–1,5 óráig online formában zajlottak.

[28] Ehmann Bea – Balázs László: A Sarkvidéktől a világűrig: A pszichológiai tartalomelemzés alkalmazása izolált kiscsoportok vizsgálatára. *Magyar Pszichológiai Szemle,* 70. (2015), 4. 723–742.
[29] Kelemen-Erdős Anikó – Molnár Adél: Cooperation or Conflict? The Nature of the Collaboration of Marketing and Sales Organizational Units. *Economics and Culture,* 16. (2019), 1. 58–69.
[30] Szokolszky Ágnes: *A pszichológiai kutatás módszertana*. Budapest, Osiris Kiadó, 2020.
[31] Lewis R. Aiken – Gary Groth-Marnat: *Psychological Testing and Assessment*. Boston, Allyn and Bacon, 2006.
[32] Horváth Dóra – Mitev Ariel Z.: *Alternatív kvalitatív kutatási kézikönyv.* Budapest, Alinea Kiadó, 2015.

4. Eredmények

A kutatási eredmények elemzésének első fázisában kvalitatív tartalomelemzést alkalmaztunk. Ennek keretében narratívák segítették elő az eredmények vizsgálatát. Ezt követően az elemzést *grounded theory* módszertannal végeztük.

4.1. Eredmények kvalitatív tartalomelemzés alapján

Az interjúalanyok digitális eszközökkel való kapcsolata úgy jellemezhető, hogy az a mindennapjaik szerves része, mondhatni létszükséglet mind a munkát, mind a magánéletet tekintve, annak ellenére, hogy igyekeznek offline módon is kikapcsolódni azért, hogy legalább a magánéletükben egyensúlyt tudjanak teremteni az offline és online tér között. Az interjúalanyok számára az információbiztonság az adatvédelemmel és az információmegosztás feletti kontrollal, valamint az információs önrendelkezéssel hozható kapcsolatba. Az információbiztonság „… nagyon fontos, pozitív dolog, amiért érdemes tenni…" (I3). Két olyan vélemény is elhangzott azonban, amelyek szerint figyelni kell az adataink és az okoseszközeink védelmére, annak ellenére, hogy ez „néha túl komplikált" (I4). Ez a biztonság percepciójának komplexitására utal.

4.1.1. A digitális eszközök használatának potenciális kockázatai

A válaszadók által azonosított észlelt kockázat főként a személyes adataik illetéktelenek általi megszerzésére, illetve az azokkal való visszaélésre vonatkoztak, azonban többen is megemlítették mint potenciális veszélyt az emberi felelőtlenséget, felkészületlenséget. Az alanyok által érzékelt digitális kockázatokat és a kockázatforrásokat az 1. táblázat tartalmazza.

A kockázatokkal összefüggésben a potenciális áldozatok körére is kitértek az interjúk, ahol elmondható, hogy az alanyok két gondolatsíkon fogalmazták meg válaszaikat. Egyrészt azt hangsúlyozták, hogy bárkiből lehet áldozat, illetve azt hogy, melyek azok az egyéni jellemzők, amelyek hozzájárulnak egy-egy személy kitettségének növekedéséhez. „A veszélyek nagyrészt a védekezés hiányából, emberi naivságból és lustaságból adódnak." (I4); „Sokan azt hiszik, hogy nekik nem lehet bajuk. A legtöbb ember még vírusirtót sem használ." (I6); „Miután feltörték a cégem rendszerét, az adataim többsége elveszett, új megoldásokat kerestem, most már tudatosabb vagyok." (I8). Másrészt az alanyok az áldozatok és elkövetők közötti elmosódó határvonalat hangsúlyozták, valamint az ipari, vállalati sebezhetőségre asszociáltak. „Vannak egyértelmű helyzetek, amikor elkülöníthető az áldozat és az elkövető […] nagyon sok esetben azonban a határok nem ilyen élesek […]. A GDPR rengeteg adatkezelési dolgot szabályoz, de a vállalatok felé semmiféle hivatalos elvárást nem támasztanak a hatóságok kiberbiztonsági szempontból." (I6).

1. táblázat: Az interjúalanyok által érzékelt digitális kockázatok

A kockázat forrása	Digitális kockázat – interjúrészlet
Emberi tényező	„az ember a leggyengébb láncszem, nem is a különböző jelszavak, tűzfalak, biztonsági megoldások" (I1); „elhúzzák az orra előtt a mézesmadzagot és ráharap…" (I3); „a felelőtlen viselkedés" (I4); „tudatlanság, nemtörődömség," (I3); „a kíváncsiság, felelőtlen kattintgatás" (I3); „egy része emberi hülyeség, másik része emberi lustaság, vagy szimplán felkészületlenség, plusz a távmunkát is idesorolnám" (I6); „amikor nem saját gépen kell bejelentkezned valamelyik e-mail-fiókodba, és utána elfelejtesz kijelentkezni" (I10);
Nem megfelelő technológiai adottságok	„webes alkalmazások, mobileszközök, végpontok és szerverek sérülékenysége – védelmi hiányosságok és egyéb technikai jellemzők, hozzáférési problémák" (I6)
Social engineering	*„a különböző social engineering technikák"* (I5)
potenciális adatsértés *(data breach)*	„jelszó meg hozzáférési adatok kiszivárogtatásáról vagy megszerzéséről" (I5)*;* „a különböző cégek adatokat gyűjtenek rólunk" (I2); „tudnak rólunk mindent, […] mindenhová követnek, hogy ez legális-e, nem tudjuk azonosítani." (I8); „Gyakran kapok olyan spameket, amit a spamszűrő nem ismer fel. Több levél megpróbálja elérni, hogy válaszoljak rá azért, hogy ellopja a jelszavaimat." (I11) „adatlopás (anyagi haszonszerzés, know-how-k megismerése, ipari kémkedés, zsarolás stb.)" (I6)
internetes csalás *(scam)*	„egyrészt megpróbálnak pénzt kicsalni az emberből, információt megtudni módszerek" (I1); „ellopják a kártyaadataimat, jelszavaimat, a személyes adataimat"; „már ellopták a kártyaadataimat valószínűleg" (I7); „visszaélhetnek az adataimmal" (I2); „elvesznek az adataim, vagy ellopják őket" (I4)
adathalászat *(phising)*	„a különböző felhasználói fiókok feltörése" (I1); „az adathalászati módszerek" (I4, I5); „a közösségimédia-profilok feltörése meg a kamuprofilok" (I9); „adatlopás (anyagi haszonszerzés, know-how-k megismerése, ipari kémkedés, zsarolás stb.)" (I6)
internetes befurakodás *(water holing)*	„bizonyos oldalak megnyitásával vírus kerülhet a gépünkre." (I11)

Forrás: a szerzők szerkesztése

4.1.2. Információbiztonság-tudatosság

Az információbiztonság-tudatos személy az interjúalanyok számára ismeri a rá leselkedő veszélyeket, tudja, hogy egyes tevékenységei, tettei mivel jár(hat)nak, valamint érti is ezeket. „Tisztában van a veszélyekkel, azzal hogy melyik lépésnek milyen következményei lehetnek, pl. ha az egyes internetes oldalakon elfogadja a sütiket…, érti is,,hogy miről van szó, illetve szem előtt tartja azt is, hogy semmi sincs ingyen, a kérdés csak az, hogy ezt hol és mivel fizeted meg." (I1) A tudatosság kapcsán egyéni tulajdonságokat is megemlítettek a válaszadók, miszerint olvasatukban egy információbiztonság-tudatos egyén kritikus gondolkodású, óvatos, felelősségteljes, mértékletes, és többnyire naprakész tudással rendelkezik a témában.

A biztonság növelése, vagy épp a sebezhetőség mértékének csökkentése kardinális kérdés az adatok védelmét tekintve. Az az érdekes következtetés vonható le, hogy

az általunk megkérdezett személyek főként a legalapvetőbb és talán a legnépszerűbb védekezési módokat gyakorolják, mint a bonyolult jelszavak és a biztonsági mentések.

„Igyekszem tudatosan többféle jelszót használni és próbálom nem a hétköznapi életből vett adatokat alkalmazni (pl. születési dátum, nevek), amelyek tartalmaznak speciális karaktereket. A több e-mail-cím használata is kifizetődő tud lenni, mindegyik egy-egy célra (egy magáncélra, egy munkaügyben stb.)." (I4); „Minimum egy vírusirtó használata azért ajánlatos, az adataimról, a különböző fájlokról van biztonsági mentésem a felhőben is és egy külső merevlemezen is, bár ezeknek a frissítése nem mindig rendszeres" (I3).

A kiszolgáltatottság csökkentésére egy-egy interjú során még említették a zárt rendszerek használatát, a hozzáférés korlátozását akár az interneten, közösségi médiában megosztott információkat tekintve, akár a munkahelyi hálózaton az egyes mappákat, dokumentumokat tekintve, továbbá a rendszeres sérülékenységvizsgálatát. A válaszokat tekintve meglepő, hogy az alanyok csak egy-két esetben tértek ki akár egyéni, akár szervezeti szinten az oktatásra, képzésekre, amelyek a felhasználók digitális tudását hivatottak növelni, ezáltal is csökkentve a kockázatot.

4.1.3. Potenciális kibertámadás lehetséges következményeinek értékelése

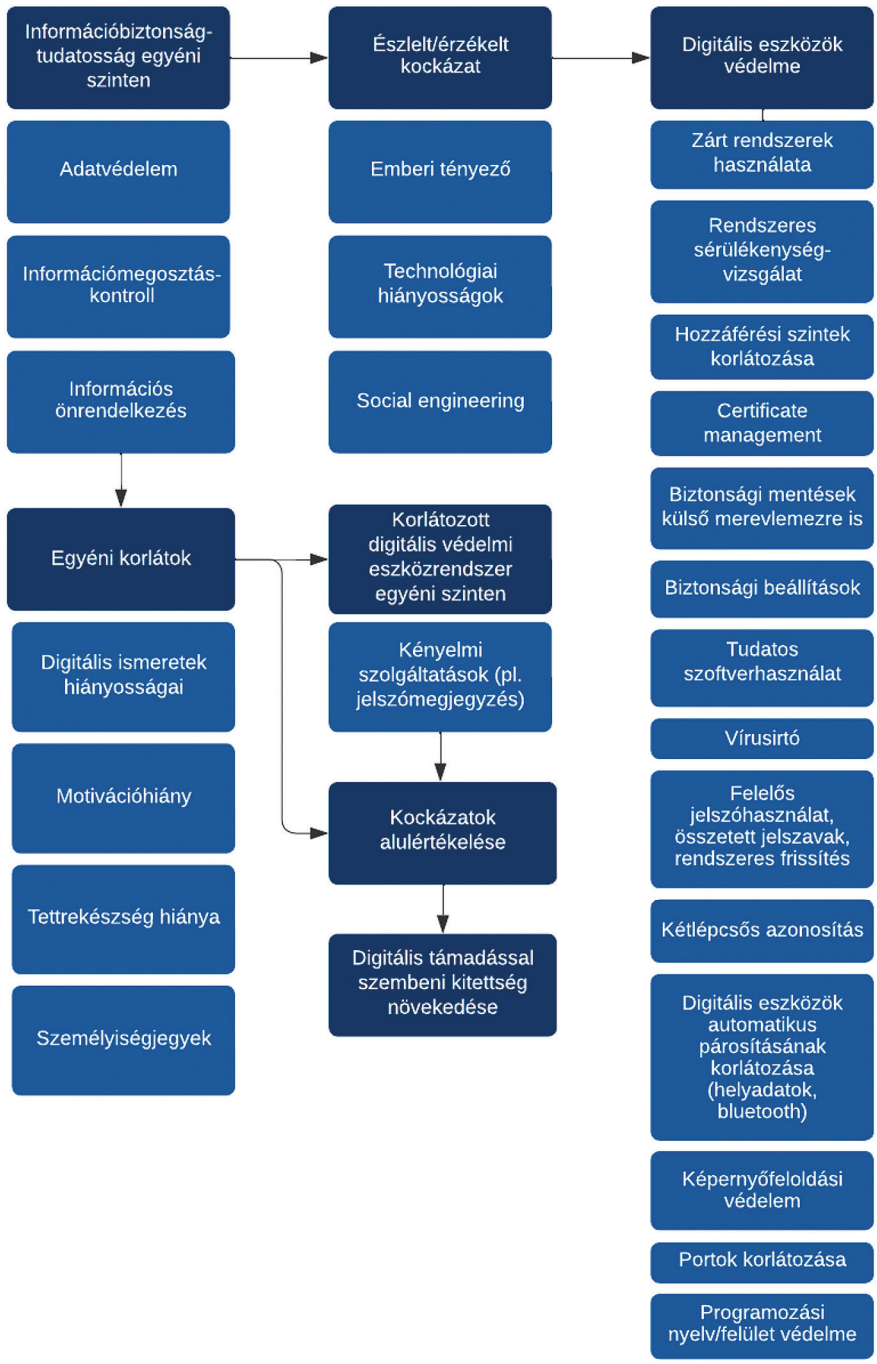
Egy esetleges kibertámadás potenciális következményeit is vizsgáltuk az adott alanyra nézve, illetve vállalati szinten. A felhasználók magukra nézve leginkább az anyagi kárt említették meg, míg a munkavállalók az anyagi kár mellett a jogi és presztízsbeli következményeket is említették.

„Mindig az anyagi kárról szól alapvetően, kivéve, ha valaki olyan személyről van szó […] és őt zsarolni, bár az is tulajdonképpen pénzre fordítható dolog, de szerintem alapvetően mindig a pénz körül forog." (I3); „Szinte elölről kéne kezdeni mindent, ez hatalmas anyagi ráfordítással járna, valószínűleg a vállalatoknál is, mivel esetükben akár hátrányba is kerülhetnek a versenytársakkal szemben, elveszthetik a vevőiket, meg persze a jogi következmények." (I2).

4.2. Eredmények grounded theory (GT-) módszertan alapján

Az interjúk vizsgálata abduktív módon történt, a *grounded theory* módszertan alapján. A GT szerinti elemzés során az interjúk egészére vonatkozó visszatérő motívumok keresése a fő mozzanat, ezt követően az egyes interjúkban beazonosított mintákat a többi interjúban is be kell azonosítani és összehasonlítani egymással, majd szükséges a kapcsolatokra rávilágítani, illetve szűrni az egyes tényezők között alkalmazva. A cél egy modell vagy keretrendszer felállítása, amely az adatok definiálása során integrálja az elméleti (szakirodalmi) tényezőrendszert is. A GT esetében egy négyszintű kódrendszer állítható fel, amelynek szintjei a következők: nyílt kódok, axiális, szelektív és teoretikus kódok.[33] Az 1. ábra a kódok hierarchikus rendszere, valamint a képzett fő kategóriák alapján definiálható modellt mutatja be.

[33] Szokolszky (2020): i. m. 42.



1. ábra: Információbiztonság-tudatosság grounded theory módszertan alapján
Forrás: a szerzők szerkesztése a mélyinterjúk alapján, N = 11

5. Összegzés

A kutatás célja az volt, hogy képet adjon az Y generációs felhasználók információbiztonság-tudatosságáról, kiberbiztonsággal és kibertámadásokkal kapcsolatos asszociációiról, attitűdjéről. Bár a jelen kutatás kvalitatív jellegéből adódóan nem minősül reprezentatívnak, nem tesz lehetővé általánosítást, illetve nem vonhatók le az eredményekből messzemenő következtetések, alapozó kutatásként hasznosítható eredményekkel szolgálhat. További vizsgálat, vállalatvezetők körében végzett szakértői mélyinterjú elősegítené a téma megközelítését más szemszögből.

A kutatás egyik legfontosabb eredménye, hogy az alanyok annak ellenére, hogy eltérő mértékben és mélységben rendelkeznek információkkal a különböző kibertámadásokról, azok módjáról, következményeiről, valamint azok kiváltó okairól, könnyelműen bánnak saját és személyes adataik védelmével. Egyes kutatások szerint az egyén biztonságtudatosságára a közvetlen környezetéhez való viszonya, gondolkodásmódja is hatással van,[34] mások szerint a személyiségjegyek is befolyásoló tényezőknek minősülnek.[35]

Az interjúalanyok biztonságtudatossága nem megfelelő szintű, esetenként az információbiztonsággal kapcsolatos ismereteikhez, tudásukhoz képest messze elmarad. Ezzel több nemzetközi kutatás is egybecseng, Hanus Bartlomiej és szerzőtársai[36] szerint a fenyegetések ismerete mit sem ér, ha a felhasználó nem képes felismerni és használni azokat az eszközöket, amelyek a védelmét szolgálják. Burcu Bulgurcu és munkatársai a szabályok mögötti okok megértését is kiemelik, azaz a tudatos viselkedést elősegíti, ha a felhasználó érti, mit miért tehet, vagy nem tehet.[37]

Az előzőkkel kapcsolatban álló újszerű eredmény, hogy az alanyok alulértékelik saját sebezhetőségüket. Az interjúalanyok annak ellenére, hogy saját elmondásuk alapján bárki lehet az emberi tényezőt kihasználó spam és *social engineering* áldozata, mégis úgy érzik, nem tartoznak különböző okok miatt (munkahely, jövedelem, online aktivitás stb.) ezek célpontjai közé, például „nem érdeklek senkit, hogy az én adataimra kíváncsiak legyenek" (I2). A nemzetközi kutatásokból egyértelműen kiderül, hogy a felhasználók kockázatérzékelése nagymértékben előrejelzi az online térben való viselkedést és a kiberbiztonság kérdéséhez való hozzáállást.[38]

További eredmény, hogy a kibertámadásokkal kapcsolatos személyes tapasztalatok nagyban befolyásolják a biztonságtudatosságot és a sebezhetőség megítélését. A 11 válaszadó közül három tapasztalt a saját eszközeihez, adataihoz kapcsolódóan

[34] Charlette Donalds – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020), 102056; Réka Saáry – Ágnes Csiszárik-Kocsir – János Varga: Examination of the Consumers' Expectations Regarding Company's Contribution to Ontological Security. *Sustainability,* 13. (2021), 17. 9987.

[35] Jaime Ortiz et al.: The Contradiction between Self-Protection and Self-Presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017). 406–416.

[36] Bartlomiej Hanus – Yu "Andy" Wu: Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management,* 33. (2015), 1. 2–16.

[37] Burgurcu et al. (2010): i. m. 29

[38] Mark J. Keith et al.: Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior. *International Journal of Human-Computer Studies,* 71. (2013), 12. 1163–1173.; Ardion D. Beldad: Sharing to be Sociable, Posting to be Popular: Factors Influencing Non-Static Personal Information Disclosure on Facebook among Young Dutch Users. *International Journal of Web Based Communities,* 11. (2015), 3–4. 357–374.

kibertámadást, amelynek következtében azóta fokozottan ügyel a kiberbiztonságra. A kibertámadásokkal kapcsolatos tapasztalat és a biztonságtudatosság szintje közötti összefüggést más tanulmányok is megerősítik.[39]

Az oktatás hozzájárulhat az egyének információbiztonság tudatosságának növeléséhez, amelyet már az általános iskolai képzésbe célszerű integrálni. Ennek során érdemes újabb interaktív módszerekkel, illetve játékosítással (gamifikációval) egyéni elkötelezettséget kiváltani, amely támogatja a későbbi tudatos magatartást az egyének és a vállalatok tevékenysége során.[40] A képzési programok, illetve ennek eredményeként az információbiztonság-tudatosság növekedésének társadalmi és gazdasági haszna egyaránt jelentős.

Köszönetnyilvánítás

A kutatás az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Felhasznált irodalom

Ahlan, Abdul Rahman – Muharman Lubis – Arif Ridho Lubis: Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science,* 72. (2015). 361–373. Online: https://doi.org/10.1016/j.procs.2015.12.151

Aiken, Lewis R. – Gary Groth-Marnat: *Psychological Testing and Assessment.* Boston, Allyn and Bacon, 2006.

Alavi, Reza – Shareeful Islam – Haralambos Mouratidis: An Information Security Risk-Driven Investment Model for Analysing Human Factors. *Information & Computer Security,* 24. (2016), 2. 205–227. Online: https://doi.org/10.1108/ICS-01-2016-0006

Albladi, Samar Muslah – George R. S. Weir: User Characteristics that Influence Judgment of Social Engineering Attacks in Social Networks. *Human-centric Computing and Information Sciences,* 8. (2018). 1. Online: https://doi.org/10.1186/s13673-018-0128-7

Bak Gerda – Kiss Sándor: A biztonságtudatosság szisztematikus szakirodalmi áttekintése. *Hadmérnök,* 16. (2021), 4. 85–99. Online: https://doi.org/10.32567/hm.2021.4.7

Beldad, Ardion D.: Sharing to be Sociable, Posting to be Popular: Factors Influencing Non-Static Personal Information Disclosure on Facebook among Young Dutch Users. *International Journal of Web Based Communities,* 11. (2015), 3–4. 357–374. Online: https://doi.org/10.1504/IJWBC.2015.072132

[39] Lennart Jaeger – Andreas Eckhardt: Eyes Wide Open: The Role of Situational Information Security Awareness for Security–Related Behaviour. *Information Systems Journal,* 31. (2021), 3. 429–472.

[40] Kovács László et al.: Structuration Theory and Strategic Alignment in Information Security Management: Introduction of a Comprehensive Research Approach and Program. *AARMS,* 16. (2017), 1. 5–16.

Buchanan, Tom – Monica T. Whitty: The Online Dating Romance Scam: Causes and Consequences of Victimhood. *Psychology, Crime & Law,* 20. (2013), 3. 261–283. Online: https://doi.org/10.1080/1068316X.2013.772180

Bulgurcu, Burcu – Hasan Cavusoglu – Izak Benbasat: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34. (2010), 3. 523–548. Online: https://doi.org/10.2307/25750690

Donalds, Charlette – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020). 102056. Online: https://doi.org/10.1016/j.ijinfomgt.2019.102056

Ehmann Bea – Balázs László: A Sarkvidéktől a világűrig: A pszichológiai tartalomelemzés alkalmazása izolált kiscsoportok vizsgálatára. *Magyar Pszichológiai Szemle,* 70. (2015), 4. 723–742. Online: https://doi.org/10.1556/0016.2015.70.4.2

Furnell, Steven – Kieran Millet – Maria Papadaki: Fifteen Years of Phishing: Can Technology Save Us? *Computer Fraud & Security,* (2019), 7. 11–16. Online: https://doi.org/10.1016/S1361-3723(19)30074-0

Grant, Kevin – David Edgar – Arun Sukumar – Martin Meyer: 'Risky Business': Perceptions of E-Business Risk by UK Small and Medium Sized Enterprises (SMEs). *International Journal of Information Management,* 34. (2014), 2. 99–122. Online: https://doi.org/10.1016/j.ijinfomgt.2013.11.001

Hanus, Bartlomiej – Yu "Andy"Wu: Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management,* 33. (2015), 1. 2–16. Online: https://doi.org/10.1080/10580530.2015.1117842

Hauser, Deanna: Social Engineering Awareness in Business and Academia. In *MWAIS 2016 Proceedings.* Wisconsin, 2016. 3–6.

Horváth Dóra – Ariel Mitev: *Alternatív kvalitatív kutatási kézikönyv.* Budapest, Alinea Kiadó, 2015.

Hutchinson, Gershon – Jacques Ophoff: A Descriptive Review and Classification of Organizational Information Security Awareness Research. In H. Venter – M. Loock – M. Coetzee – M. Eloff – J. Eloff (szerk.): *Information and Cyber Security.* Cham, Springer, 2020. 114–130. Online: https://doi.org/10.1007/978-3-030-43276-8_9

Jaeger, Lennart – Andreas Eckhardt: Eyes Wide Open: The Role of Situational Information Security Awareness for Security–Related Behaviour. *Information Systems Journal,* 31. (2021), 3. 429–472. Online: https://doi.org/10.1111/isj.12317

Jéri Tamás: Az elektronikus levelezés és a kiberbiztonság összefüggései. *Hadmérnök,* 16. (2021), 2. 169–185. Online: https://doi.org/10.32567/hm.2021.2.12

Kallio, Hanna – Anna-Maija Pietilä – Martin Johnson – Mari Kangasniemi: Systematic Methodological Review: Developing a Framework for a Qualitative Semi-Structured Interview Guide. *Journal of Advanced Nursing,* 72. (2016), 12. 2954–2965. Online: https://doi.org/10.1111/jan.13031

Keith, Mark J. – Samuel C. Thompson – Joanne Hale – Paul Benjamin Lowry – Chapman Greer: Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus

with Actual User Behavior. *International Journal of Human-Computer Studies,* 71. (2013), 12. 1163–1173. Online: https://doi.org/10.1016/j.ijhcs.2013.08.016

Kelemen-Erdős, Anikó – Adél Molnár: Cooperation or Conflict? The Nature of the Collaboration of Marketing and Sales Organizational Units. *Economics and Culture,* 16. (2019), 1. 58–69. Online: https://doi.org/10.2478/jec-2019-0007

Kelemenné Erdős Anikó: A közforgalmú közlekedési szolgáltatás és piac vizsgálata marketing és fenntarthatósági nézőpontból. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem, 2014.

Khan, Freeha – Jung Hwan Kim – Lars Mathiassen – Robin Moore: Data Breach Management: An Integrated Risk Model. *Information & Management,* 58. (2021), 1. 103392. Online: https://doi.org/10.1016/j.im.2020.103392

Krippendorff, Klaus: *Content Analysis – An Introduction to Its Methodology.* Thousand Oaks, SAGE, 2018. Online: https://doi.org/10.4135/9781071878781

Lazar, Arokia Jesu Prabhu – Sudhakar Sengan – Luigi Pio Leonardo Cavaliere – Thillaiarasu Nadesan – Deepesh Sharma – Mukesh Kumar Gupta – Thangam Palaniswamy – Mahendiran Vellingiri – Dilip Kumar Sharma – Thirukumaran Subramani: Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud. *Wireless Personal Communications,* (2021). Online: https://doi.org/10.1007/s11277-021-08585-y

Oroszi Eszter Diána: Social engineering technikák. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 77–118. Online: https://bit.ly/3D5AqlD

Ortiz, Jaime – Shu-Hao Chang – Wen-Hai Chih – Chia-Hao Wang: The Contradiction between Self-Protection and Self-Presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017). 406–416. Online: https://doi.org/10.1016/j.chb.2017.07.031

Parsons, Kathryn – Agata McCormac – Marcus Butavicius – Malcolm Pattinson – Cate Jerram: Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security,* 42. (2014). 165–176. Online: https://doi.org/10.1016/j.cose.2013.12.003

Saáry, Réka – Ágnes Csiszárik-Kocsir – János Varga: Examination of the Consumers' Expectations Regarding Company's Contribution to Ontological Security. *Sustainability,* 13. (2021), 17. 9987. Online: https://doi.org/10.3390/su13179987

Stirnimann, Sonja: *Der Mensch als Risikofaktor bei Wirtschaftskriminalität: Handlungsfähig bei Non-Compliance und Cyberkriminalität.* Wiesbaden, Springer, 2018. Online: https://doi.org/10.1007/978-3-658-20813-4

Szappanos Gábor: Kártékony kódok használata a célzott támadások végrehajtásában. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 119–159. Online: https://bit.ly/3z4dl1J

Szokolszky Ágnes: *A pszichológiai kutatás módszertana.* Budapest, Osiris Kiadó, 2020.

Tari Annamária: *Y generáció. Klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban.* Budapest, Jaffa Kiadó, 2010.

Vahdati, Soudabeh – Niloofar Yasini: Factors Affecting Internet Frauds in Private Sector: A Case Study in Cyberspace Surveillance and Scam Monitoring Agency of Iran. *Computers in Human Behavior,* 51. (2015). 180–187. Online: https://doi.org/10.1016/j.chb.2015.04.058

Zhongping, Zeng – Yang Kaifeng – Zhang Yi – Zhou Peipei: Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management. In *2013 Fourth International Conference on Digital Manufacturing & Automation.* IEEE, 2013. 684–687. Online: https://doi.org/10.1109/ICDMA.2013.162

Zimmermann, Verena – Karen Renaud: Moving from a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset. *International Journal of Human-Computer Studies,* 131. (2019). 169–187. Online: https://doi.org/10.1016/j.ijhcs.2019.05.005