Magyar Rendészet 2022/2. 245–261. DOI: 10.32577/mr.2022.2.16

A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról

GYARAKI Réka[1]

Az életünk egyre inkább az informatikai eszközöktől és rendszerektől függ. Egyre többen használják a 4. ipari forradalom hozta újításokat, de annak veszélyeivel már annál kevesebben vannak tisztában. Az internet és az információs rendszerek olyan technológiai robbanást hoztak, amellyel az átlagos felhasználók nem feltétlenül képesek lépést tartani. Márpedig, ha az átlagfelhasználó a saját eszközein és rendszerein nem képes a biztonságtudatosságra, akkor joggal lehet feltételezni, hogy ugyanaz a felhasználó a munkahelyén sem lesz biztonságtudatos.
Az állami és a magánszektorban a kibertámadások megelőzése és a szektorok sérülékenységének vizsgálata során az ember kerül a középpontba mint az információs rendszerek sérülékenységét okozó leggyengébb láncszem.
A tanulmányban arra keresem a választ, hogy a kiberbiztonság kialakítása során milyen gyakorlat van jelenleg Magyarországon, és mely képességek fejlesztésével erősíthetjük meg az embereket mint a lánc alkotóelemeit.

Kulcsszavak: *kiberbiztonság, tudatosság, felhasználók, jó gyakorlat, információs rendszerek*

1. Biztonságunk az interneten

Mit is értünk biztonság alatt? Mielőtt kiberbiztonságról beszélünk, a biztonságról kell hogy szót ejtsünk. A biztonság szubjektív fogalom, vagyis mindenkinek mást és mást jelent, helytől, személytől és képzettségtől függően. A biztonságtudatosságot három irányban vizsgálom. Az egyik a felhasználók viselkedésének vizsgálata az online térben kérdőívvel, a másik a kiberbiztonsággal foglalkozó hazai szervezetek feladatai az online térben megjelenő veszélyek és támadások elhárítása érdekében, és a harmadik terület az információtechnológiával foglalkozó cégek előrejelzései. Ezek a három terület által készített éves jelentések.

[1] Rendőr őrnagy, egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék; doktori hallgató, Rendészettudományi Doktori Iskola. E-mail: Gyaraki.Reka@uni-nke.hu

2. A kutatás módszertana

A kutatás első részében bemutatom azokat a kiberbiztonság területével összefüggő, hazai és nemzetközi vállalatok által készített felméréseket, amelyek mellett nem lehet elmenni, ha a kiberbiztonság kérdésének fontosságáról beszélünk. A tanulmány második részében egy témával foglalkozó kérdőívem válaszait mutatom be. A téma lezárásaként, a harmadik részben azzal foglalkozom, ami jelenleg még nincs teljesen meghatározva a kiberbiztonság és a kiber-bűnmegelőzés témában.

A tanulmányhoz felhasználtam továbbá a Belügyi Tudományos Tanács Gyakornoki Programjában való részvétel során szerzett tapasztalatokat, valamint eddigi saját tudományos kutatásaim eredményeinek egy részét. A kiberbiztonság kérdésével a kibertérben ma már egyre többen foglalkoznak. Egy rövidebb kérdőívben olyan felhasználókat kérdeztem meg, akik érzéseik szerint még nem váltak kiberbűncselekmény sértettjévé. A tanulmányban arra szeretnék rámutatni, hogy a felhasználók, akik saját (!) bevallásuk szerint nem estek áldozatul kiberbűncselekménynek, milyen magatartást tanúsítanak az online térben.

3. Veszélyek a kibertérben

A digitalizációval új veszélyek jelentek meg. Amíg a fizikai térből érkező veszélyekkel kapcsolatban már kialakultak a megelőzéssel és biztonságtudatossággal kapcsolatos védekező reflexek, a kibertérből származó veszélyekkel szemben a tudatosság kialakulása még folyamatban van. A kibertér veszélyei több irányból is érkeznek. Egyrészt a fizikai térből, így a laptop, mobiltelefon, adathordozók eltulajdonítása és a rajtuk lévő adatok törlése az eszköz újraformázásával, vagy az eszköz és ezzel összefüggésben az adatok fizikai megsemmisítésével. A másik veszély, amikor fizikailag tulajdonítják el az IT-eszközöket, amelyeknek védelmét kijátsszák (Btk. 423 §. információs rendszer vagy adat megsértése),[2] és a rajta lévő adatokhoz hozzáférnek, esetleg vissza is élnek azokkal. A harmadik eset, amikor az információs rendszert éri támadás az online téren keresztül, amely során a rendszerben tárolt adatokat megszerzik, hozzáférhetővé teszik, módosítják vagy törlik.

A fent felsorolt esetekben közös a humán faktor, vagyis az ember, pontosabban a felhasználók jelentette kockázatok, ami szoros összefüggésben van a biztonságtudatossággal, illetve annak hiányával. A tanulmányban azt vizsgálom, hogy a felhasználók milyen magatartása vezethet az információs rendszerek elleni támadásokhoz (humán kockázatok), és ez lehet-e hatással a kiberbűncselekmények fejlődésére és számára?

[2] 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.).

4. Biztonságtudatosság

Ha elgondolkodunk ezen a szón, rögtön az jut eszünkbe, hogy tudatosan vagyunk biztonságosak. A biztonság ugyanakkor sokkal több összetevőből áll, mintsem ezt gondolnánk. A biztonság szubjektív érzés és fogalom is. Biztonságban érezzük-e magunkat egy adott helyen vagy egy adott cselekmény végzése közben? Erre a kérdésre valószínűleg megmondanánk azokat a helyeket és cselekményeket, amelyek során és ahol igen lenne a válasz, és fel is tudnánk sorolni. Vagyis konkrét választ tudunk adni. Biztonságban vagyok a házamban, mert kulcsra zártam az ajtót, és ha nem engedek be az ingatlanomba számomra idegen embereket, vagy olyanokat, akikben nem bízom meg, mert a viselkedésük, a külső tulajdonságaik vagy ezek együttesen bizalmatlanság érzését keltik bennem. Félelmet válthat ki egy függőhíd, amennyiben azt látjuk, hogy korhadt fából van, vagy a kötél, amely tartja, szakadt, régi, ezért nem fogunk rajta átmenni. Még lehetne sorolni, hogy kit, milyen látvány vagy tapasztalás renget meg a bizalomban, és milyen biztonsággal kapcsolatos szabályok szerint élünk. Az internettel kapcsolatos biztonság ugyanakkor a fizikai életben megtapasztalt biztonságtól sokban eltér jelenleg.

A fent említett kérdőívet közel 200 kitöltő nyitotta meg és töltötte ki. Ezt a közösségi médiában osztottam meg többek között a www.kerdoivem.hu-n az ingyen elérhető kérdőívkitöltő alkalmazáson.[3] A kérdőív azóta is folyamatosan elérhető, és olyan személyeket kértem meg, hogy töltsék ki, akik saját álláspontjuk szerint még nem váltak bűncselekmény áldozatává az online térben. A tapasztalatokat és kérdéseket az alábbiakban részletezem.

5. Humán kockázatok a kibertérben

A humán kockázatok alatt egyértelműen a felhasználók jelentette kockázatos viselkedést értjük, amely során az adott felhasználó és más személy vagy vállalat, kormányzati szerv és egyéb szervezetnek az információs rendszerben tárolt adatait, a róla szóló információkat veszélyezteti, a hozzáférést jogosulatlanok számára lehetővé teszi, vagy az adott rendszerhez fűződő bizalmat kockáztatja. Az emberi kockázatok például egy adott rendszer sérülékenységénél jelenhetnek meg.

Kollár Csaba és Zakar Ákos egyik tanulmányában a támadások veszélyességével kapcsolatban megjegyzik a felhasználók viselkedését kihasználó támadásokkal kapcsolatban, hogy pszichológiai és kommunikációs szempontból ez igényli a legmagasabb fokú felkészültséget a támadó részéről, ugyanakkor a lebukás veszélye is itt a legnagyobb, hiszen – pár kivételtől eltekintve – közvetlen kontaktust létesít a célszeméllyel.[4] A közvetlen kontaktus alatt nemcsak fizikai kapcsolatot kell érteni,

[3] Ennek a mondatnak a jelentőségét majd a későbbiekben részletezem.

[4] Kollár Csaba – Zakar Ákos: A Social Engineering és a manipulációs technikák és módszerek. *Biztonságtudományi Szemle*, 2. (2020), 2. 24.

hanem bármelyik online vagy offline kommunikációs technológiát fel lehet használni arra, hogy információt szerezzenek a *social engineering* támadás során a célszemélytől, célszemélyről. Igen, akár e-mailen, telefonon vagy szórólapon, vagy ajándékba adott pendrive-val.

Kollár és Zakar továbbmennek, amikor megállapítják a humán kockázatok veszélyességével kapcsolatban, hogy:

> „Sok esetben kevesebb idő- és energiaráfordítást igényel végrehajtásuk, mint egy technológiai módszernek. További előnyük, hogy olyan jellegű információk birtokába juthatunk, melyekkel más jellegű támadások kivitelezését meg lehet könnyíteni, illetve a célszemélyt rá tudjuk venni arra is, hogy helyettünk hajtson végre valamilyen támadást (pl. adatbázishoz hozzáférés). Ebbe a kategóriába sorolhatók azon módszerek, melyek végrehajtásához nincs szükség az informatika, szűkebb értelemben véve a számítógép használatára."[5]

Milyen alapvető humán kockázatokat lehet azonosítani?

A humán kockázat egyrészt olyan tulajdonságokat takar, amelyek közvetlenül a felhasználó jelleméhez tartoznak. Ilyenek többek között a segítőkészség, a naivitás, a nyitottság és vizualitás.[6]

Oroszi Eszter ugyanakkor ennél még továbbment az osztályozásban, amikor négy csoportba sorolta azokat az emberi tényezőket, amelyeket a social engineering auditok alapján tapasztalt. Ezek a személyes, a munkahelyi, a pillanatnyi és az incidens kategóriák, amelyekhez további tulajdonságokat határozott meg.[7]

Kárász még további tulajdonságokat is felsorolt, amelyek összefüggésben állnak azzal, hogy a felhasználók jelentik az egyik legnagyobb kockázatot a kibertérben:

- hanyagság;
- kihasználható emberi tulajdonságok;
- vezetői viselkedés és interakciók;
- tudatosság hiánya.[8]

A felhasználók tulajdonságai, viselkedése a fizikai térben vajon minden esetben megmutatják, hogyan viselkedik online térben?

Gyerekkortól kezdve hallgattuk, hogy ne állj szóba idegennel. A fizikai térben ennek betartása nem nehéz, hiszen megismerjük az ismerőst, aki az utcán, a munkahelyen

---

5 Kollár–Zakar (2020): i. m. 24.

6 Gyaraki Réka: A közösségi média hatása a kiberbűncselekmények elkövetésére. *Magyar Rendészet,* 21. (2021), 2. 67–82.

7 Oroszi Eszter Diána: Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük. *Dunakavics,* 8. (2020), 5. 6.

8 Kárász Balázs: Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata. *Biztonságtudományi Szemle,* 2. (2020), 2. 58.

beszélgetni kezd velünk, vagy szívességet, segítséget kér. Ha egy munkavállaló találkozik a vezetőjével, akkor a beosztott megismeri őt, és a szemtől szembe érkező kérést, utasítást végrehajtja. A munkahelyen – függetlenül egy vállalkozás vagy szervezet nagyságától – ma már többször érkezik elektronikusan vagy telekommunikációs eszközön keresztül kérés, utasítás, információkérés.

Mennyit érhetnek a kötelezően előírt évente egy vagy két alkalommal lefolytatott biztonságtudatosító oktatások, továbbképzések a munkahelyeken?

5.1. IT-eszközök kockázatai – a mai ember által használt IT-eszközök veszélyei

Az IT-eszközök – azok eltulajdonítása mellett – kockázatait az azon tárolt adatok és információk, valamint annak a segítségével megszerzett adatok, információk jelentik. Az alapvető tudás hiánya jelenti véleményem szerint a legnagyobb kockázatot. A KSH adatai szerint míg 2010-ben a háztartások 58%-a rendelkezett internet-hozzáféréssel, addig 2020-ban ez a szám már 88%.[9]

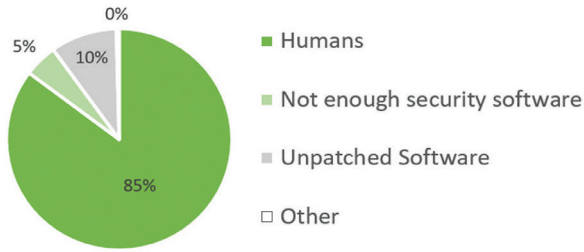
A Nemzeti Média és Hírközlési Hatóság felmérésében – amelyet a 16 év feletti lakosság körében végeztek, és a minta nagysága 4000 fő – azt lehet látni, hogy a megkérdezettek 12%-a nyilatkozta az internethasználati szokásaival kapcsolatban, hogy teljesen profinak érzi magát, 23% az átlagosnál lényegesen több tudással rendelkezik, 44% átlagos felhasználói tudásúnak érzi magát, míg a maradék 21% gondolja úgy, hogy átlag alatti a tudása.[10]

Ezek a számok vajon mit mutatnak? Soknak vagy kevésnek ítélhetjük meg a 12%-ot? Mennyire tekinthetjük profinak, ha azt nézzük, hogy a közösségimédia-felületek közül 92%-uk használja a Facebookot, míg a Messengert mint chatprogramot 87%-uk?

2017-ben Las Vegasban tartottak konferenciát a Black Hat Hackereknek (fekete kalapos hekkerek), amely során a résztvevőknek különböző kérdéseket tettek fel. Kérdés volt, hogy mi vagy ki a leginkább felelős a kiberbiztonság megsértéséért? Az ember, a szoftver vagy az elégtelen biztonsági technológia? A felmérésben részt vevők több mint 85%-a az embereket nevezte meg a leginkább felelősnek a biztonsági szabályok megsértéséért. A javítás nélküli szoftver (10%) és az elégtelen biztonsági technológia (5%) messze elmaradt. Vagyis a fekete kalapos hackerek egy információs rendszer elleni támadás során inkább összpontosítanak az emberi gyengeségre (biztonságtudatosság hiánya vagy nem megfelelő ismerete), mint az eszközre vagy a szoftverre (1. ábra).

[9] A lakosság internethasználata 2020-ban, lásd: www.ksh.hu/infografika/2021/internethasznalat_2021.pdf

[10] Nemzeti Média- és Hírközlési Hatóság: *Az elektronikus hírközlési piac fogyasztóinak vizsgálata. Internetes felmérés* (2020).



1. ábra: Black Hat Hackers Survey 2017

Forrás: https://thycotic.com/resources/black-hat%20%20-2017-survey/

A hackerek az emberi sérülékenység egyik okának az úgynevezett „(kiber) biztonsági fáradtságot" jelölték meg, amely miatt a kiberhigiénia szabályait nem tudják betartani a napi feladatok ellátása során.

Ennek némiképp ellentmond a Microsoft által készített felmérés, amely szerint aggályos, hogy a cégek 58%-ának nincs átfogó biztonsági stratégiája. Ezt a tényt fokozza, hogy a felméréssel érintett cégek 86%-a szerint a biztonsági stratégia hiányának ellenére, általában elégedettek a saját IT-rendszereik biztonságával. Ami véleményem szerint megrázóbb, hogy a cégek 38%-a készül csupán biztonságtudatossági kampány indítására.[11]

Ugyanakkor, amint a Microsoft publikálta a felmérését, sajnos szomorú és azonnali reagálást kívánó kép jelenik meg: „A vállalat megbízásából 1500 cseh, görög, lengyel, magyar, orosz és román vállalkozás vezetői körében elvégzett, felhőbiztonságot érintő felmérés szerint régiónk vállalkozásainak csak alig több mint fele tart egy lehetséges kibertámadástól."[12]

5.2. A „(kiber)biztonsági fáradtság" és kiberhigiénia

A Nemzetbiztonsági Szakszolgálathoz tartozó Nemzeti Kibervédelmi Intézet évente készít lakossági kérdőívet, felmérést a biztonságtudatossággal kapcsolatban. Emellett az állami és önkormányzati szervek információs biztonságáról szóló 2013. évi L. törvény az eseménykezelő központ feladatának jelöli meg, hogy „a biztonságtudatos felhasználói magatartás elősegítése céljából oktatási anyagokat dolgozhat ki és tréningeket tarthat, felvilágosító, szemléletformáló kampányokat szervezhet".[13]

---

[11] Microsoft: *Kiberbiztonsági trendek Közép- és Kelet-Európában. A 2020-as év digitális biztonsági kihívásai és hasznos javaslatok cége ellenálló képességének fokozására*.

[12] Térségi kiberbiztonsági kitekintés a Microsofttól. *Securinfo,* 2021. május 17.

[13] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 20. § (1) bekezdés *k)* pont.

Hogyan lehet belefáradni a kiberbiztonságba?

Ahogy a vállalatok és az állami szervek, a magánszemélyek is védik az információs rendszereikben tárolt adatokat. Már egy új IT-eszköz vásárlásánál vagy a régi eladásánál a gyártó által megadott biztonsági intézkedéseket szükséges elvégezni ahhoz, hogy a készülék előnyeit a felhasználók maradéktalanul élvezhessék.

A folyamatos biztonsági figyelmeztetésekkel és beállításokra kötelezéssel tartják napra készen az eszközök és az adatok védelmét a gyártók és a szoftverfejlesztők, ezt addig jelzik az eszköz vagy alkalmazás/szoftver tulajdonosának, amíg a szükséges változtatásokat el nem végzi. A különböző kényelmi szolgáltatásokat nyújtó szolgáltatók (netbankszolgáltatás, telefontársaság online ügyintézésére létrehozott alkalmazások, e-ügyintézés stb.) esetében viszont tapasztalható volt már nem egy esetben, hogy figyelmeztették a felhasználót, arra, ha az operációs rendszerét frissíti, szolgáltatásukat nem tudja ugyanolyan minőségben igénybe venni, mintha vár.

Az információs rendszerek biztonságára való állandó figyelmeztetések mellett, megjelennek még a közösségi oldalak fejlesztőinek is a biztonsági fejlesztései, a rádióból és televízióból érkező figyelmeztetések, a fényképekkel, videófelvételekkel kapcsolatos figyelmeztetések, visszaélések. Ezek mellett a felhasználók egymás kioktatását is szívesen végzik, amivel a többi felhasználót elbizonytalanítják.

Amikor a social engineering veszélyeiről van szó, egy vállalat fizikai és adminisztratív védelmét ismertetik. Ez a támadás ugyanúgy összefüggésben van a rendszerben dolgozók fáradtságával, a kötelezően betartandó szabályokra való odafigyeléssel. A szinte rutinná váló napi tevékenységek ugyanúgy fáradtságot és figyelemhiányt okoznak.

Az alábbi pontokban „röviden" felsorolom a jelszókezelési hiányosságokat, amelyek összefüggésben állhatnak a hanyagsággal[14] vagy a kiberfáradtsággal is:

- alapértelmezett, illetve túl egyszerű jelszavak használata;
- jelszavas védelem hiánya, hivatkozások előzetes ellenőrzés nélküli megnyitása;
- „túl bonyolult" jelszavak nem megfelelő kezelése (például felírása cetlire);
- azonos jelszó használata különféle felületeken – akár többszintű autentikáció miatt;
- ritka jelszócsere, jelszó megjegyeztetése böngészővel számítógépen, illetve mobileszközön;
- alapértelmezett ellenőrző kérdés és egyszerű válasz alkalmazása visszaállításhoz;
- jelszótároló alkalmazás nem megfelelő használata („saját" jelszavak tárolása);
- mobileszköz nem megfelelő védelme (például feloldása mintával vagy számkóddal);

[14] Kárász (2020): i. m. 61–62.

- fizikai biztonsági előírások (például tiszta asztal, *„clear desk"* politika[15]) figyelmen kívül hagyása;
- nem megfelelő hulladékkezelési és iratmegsemmisítési gyakorlat;
- felületesség az előírások elsajátításában és tudatossági képzésen való részvételben.

A jelszóhasználaton kívül még érdemes említeni az ismeretlenektől érkező leveleket, üzeneteket, amelyek linket vagy pdf-fájlt tartalmaznak, vagy figyelmeztetésnek tűnnek.

5.3. A tudatos magatartás a kérdőív és a számok tükrében

A felhasználók kiberbiztonsági tudatosságának növelése érdekében a mobil eszközök és a rajta tárolt adatok és az ahhoz való biztonságos hozzáférés területei kiemelt feladatnak tekintendők. Ahogy a tanulmány elején is írtam, a felhasználók biztonságát hasonlóan kell értelmezni, mint a fizikai térben érzett biztonságot. Az információs rendszerbe behatolók célja közvetetten a sértett felhasználó adatai, pénze, közvetlenül az ezek megszerzéséhez szükséges felhasználónév, jelszavak. Ez utóbbiak révén nemcsak a kiválasztott felhasználó adatait, hanem rajta keresztül további felhasználók adatait is meg tudja szerezni. Az Egységes nyomozó hatósági és ügyészségi bűnügyi statisztika rendszer (ENyÜBS) alapján lekérdezett, az információs rendszer vagy adat megsértésének tényállása, amelynek statisztikai adataiban a legjobban lehet szemléltetni a kiberbiztonság (tudatosság) főbb pontjait.

A bűncselekmények számának vizsgálatakor a felhasználók biztonságtudatosságát jól szemlélteti az 1. és 2. táblázat.

A sértettek számának 2018 és 2020 közötti alakulása ugyanakkor érdekes, hiszen a magánszemélyek száma 2018. évben 462 fő, 2019. évben 321 fő, míg 2020. évben 579 fő volt. Az információs rendszer vagy adat megsértése a cégeknél 2019-ben volt magasabb, akkor 112 vállalkozást érintett, míg 2018-ban és 2020-ban 96-96 cég tett feljelentést.

[15] A *clear desk* vagy tiszta asztal politika egy információbiztonsági, adatvédelmi intézkedés, amely arra figyelmezteti a felhasználót, hogy a munkaállomásán ne hagyjon iratokat, jegyzeteket, információkat hordozó dokumentumokat.

1. táblázat: Közösségi médiával összefüggő bűncselekmények száma

Btk. 423. § (ENYÜBS)	2018	2019	2020
Lezárt bűnügyek darabszáma	602	488	726
Közösségi médlafelületet érint	257	177	394
Érintett közösségi oldalak:			
Facebook	234	153	360
WhatsApp	0	0	2
Messenger	12	4	14
Instagram	4	6	9
Twitter	0	0	1
Pínterest	0	0	0
Snapchat	1	2	1
iWiW	0	0	0
myVIP	0	0	0
Myspace	0	0	0
Google+	2	2	4
LinkedIn	0	0	0
YouTube	2	2	3

Forrás: KR NNI Kiberbűnözés Elleni Főosztály

2. táblázat: Weboldalak ellen irányuló támadások

Btk. 423. § (ENYÜBS)	2018	2019	2020
Weboldalak ellen irányult			
Összesen	68	18	102
Deface (weboldal arculatának megváltoztatása)	3	5	3
DDoS (túlterheléses támadás)	11	16	24
Ransomware (zsarolóvírus)	71	109	85
Phishing (adathalászat)	59	78	67

Forrás: KR NNI Kiberbűnözés Elleni Főosztály

A törvény három külön fordulattal határozza meg a bűncselekmények elkövetési magatartásait. Ezeknek a fordulatoknak az elkövetési tárgya az információs rendszer, amelynek a betöltött funkciója a meghatározó.[16] A Büntető Törvénykönyvről szóló 2012. évi C. törvény 459. §-a alapján információs rendszernek tekintünk minden olyan berendezést – vagy egymással kapcsolatban lévő ilyen berendezések összeségét –, amely automatikusan végez adatfeldolgozást, azaz adatok bevitelét, kezelését, tárolását, továbbítását látja el. Az információs rendszerek körébe tartoznak a számítástechnikai adatfeldolgozásra épülő memóriával rendelkező olyan egységek

[16] Tóth Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In Gál István László – Nagy Zoltán András (szerk.): *Informatika és büntetőjog.* Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2006. 184.

is, amelyek megjelenésükben eltérnek a „hagyományos" számítógépektől (például közcélú távbeszélő-szolgáltatás, információs rendszerek felhasználásával működő hírközlési, telekommunikációs rendszerek stb.).[17]

Ahogy azt a tanulmány „Biztonságtudatosság" pontjában is említettem, kérdőívet tettem közé a közösségi médiában, több, leginkább szakdolgozat és műhelymunka során szükséges kérdőíveket megosztó csoportba, amelyeknek igen magas a csoportlétszáma. A saját kutatásom szempontjából már az is érdekes volt, hogy ennyi felhasználó töltötte ki, vagyis egy, a számukra ismeretlen személy által megosztott weboldalt megnyitották és letöltötték.

Amennyiben összevetem saját kutatási eredményeimet, amelyeket a kérdőívben tapasztaltam a rendőrségtől beszerzett statisztikai számokkal, valamint az elérhető felmérésekben megállapítottakkal (szekunder forrásokkal), akkor elmondható, hogy:

- a felhasználók nem tesznek feljelentést a jelszavaikkal kapcsolatos visszaélésekkel összefüggésben;
- a hatóság nem foglalkozik a jelszavak megszerzésével, a felhasználói fiókok feltörésével, ami viszont előbb-utóbb a felhasználók bizalomvesztéséhez fog vezetni (ez pedig az online bűnözők malmára hajtja a vizet).

5.4. Biztonságban az interneten (kérdőív és számok tükrében)

Az elkészített kérdőívben nagy hangsúlyt fektettek a felhasználók a jelszó kezelésére, mivel egy jól megválasztott, biztonságos jelszóval védett eszköz vagy rendszer esetében sem lehet kijelenteni, hogy feltörhetetlen, mégis nehezebb hozzáférést biztosít külső támadások esetén.

A kérdőívben a megkérdezett személyek 22,6%-a a jelszókezelésnél azt a lehetőséget jelölte meg, hogy a jelszókiválasztásnál kis- és nagybetű kombinációt használ (közel ugyanennyi kitöltő írta, hogy a jelszó-kombinációja: nagybetű, kisbetű és a szám a jelszó végén található), de csak 15,1% válaszolta azt, hogy valamennyi felhasználói fiókjához eltérő jelszót használ. Ezek a százalékos számok még mindig kevésnek mondhatók, hiszen ez azt jelenti, hogy a kitöltők 77,4%-a kisbetűt használ a jelszavainál. Ezek a számok azért kétségbeejtők, mert az információs rendszer vagy adat megsértése bűncselekményének megállapításához szükséges, hogy az információs rendszer technikai intézkedésekkel biztosított védelemmel legyen ellátva, és az a védelem aktív legyen, azaz rendelkezzen felhasználónévvel, jelszóval,

[17] Molnár Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In Kónya István (szerk.): *Magyar Büntetőjog. Kommentár a gyakorlat számára.* 3. kiadás. Budapest, HVG-ORAC Lap- és Könyvkiadó, 2016. 1764–1780.

tűzfallal vagy egyéb védelemmel.[18] Ezek hiányában viszont nem valósul meg a bűncselekmény.

A Készenléti Rendőrség Nemzeti Nyomozó Iroda által megnevezett jellemző elkövetési magatartások:

- e-mail-fiók „feltörése" (jogosulatlan, engedély nélküli belépés, üzenetek továbbítása, törlése, jelszó módosítása kapcsán a sértett számára a fiók hozzáférhetetlenné tétele);
- e-mail-fiók feltörése kapcsán Facebook-fiókba történő jogosulatlan, engedély nélküli belépés;
- Facebook-fiók „feltörése" (jogosulatlan, engedély nélküli belépés, üzenetek, fotók továbbítása, törlése; jelszó módosítása kapcsán a sértett számára a fiók hozzáférhetetlenné tétele, megszerzett adatokkal új „ál" fiók létrehozása);
- adathalászatra vonatkozó adatok évi adatai 59-78 darabszám körül mozog;
- digitális menetíró (tachográf) készülék mágneses „manipulálása";
- cég szerverét, illetve elenyésző számban magánszemély számítógépes hálózatát ért zsarolóvírus-támadás;
- eltulajdonított laptop, mobiltelefon újra formázása;
- túlterheléses támadások (ezek száma évről évre emelkedik).[19]

3. táblázat: Jelszókezelések a bűncselekményekben

Btk. 423. § (ENYÜBS)	**2018**	**2019**	**2020**
Lezárt bűnügyek darabszáma	602	488	726
Közösségi médlafelületet érint	257	177	394
Jelszóhoz kapcsolódó Információk			
Sértetten kívül másnak is tudomása volt a jelszóról (sértett nyilatkozata alapján)	74	30	49
Papíralapon rögzítésre került (sértett nyilatkozata alapján)	1	0	5
Jelszóvédelem felhasználó-azonosítással	385	306	426
Jelszóvédelem – kettős hitelesítéssel	76	122	252

Forrás: KR NNI Kiberbűnözés Elleni Főosztály

A 3. táblázatba az elkövetett bűncselekményekben a jelszóval kapcsolatos nyilatkozatok kerültek (sajnos ezek a számok nem fedik a valóságot, hiszen feljelentéskor

[18] Nagy Zoltán András: XLIII. fejezet. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In Tóth Mihály – Nagy Zoltán András (szerk.): *Magyar büntetőjog. Különös rész*. Budapest, Osiris Kiadó, 2014. 594–595.

[19] Vetter Dániel rendőr őrnagy, Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály előadása nyomán.

és a sértett vagy tanúk kihallgatása során nem minden esetben kérdeznek rá a kihallgató rendőrök a jelszókezelésre).

5.5. Biztonságtudatosító kampány vagy bűnmegelőzés?

A Nemzeti Közszolgálati Egyetem Rendészettudományi Karának oktatói között már felmerült annak a kérdése, hogy a biztonságtudatosítás és a bűnmegelőzés között van-e különbség, illetve érdemes-e a két fogalom között különbséget tenni?
Ennek a kérdésnek a megválaszolása annyira nem is egyszerű, hiszen általában véve a kibertér fenyegetéseit és a megelőzésüket összemossák az ezzel foglalkozó szakemberek. Jó példa erre a Magyar Rendőrség hivatalos honlapján található bűnmegelőzés során adott tanácsok áttekintése, amelyek között több is foglalkozik például a tavalyi évben megjelent FluBottal vagy több zsarolóvírussal, zsaroló e-maillel.

A két fogalom között a következő különbségeket lehet tenni:

Biztonságtudatosság/biztonságtudatosítás:

- feladata nem feltétlenül a bűncselekmények megelőzése, hanem a biztonságos magatartásra vagy viselkedésre történő felhívás;
- kevésbé vagy egyáltalán nem játszik szerepet a predikció (jóslás), sokkal inkább a jelenben történő veszélyek, helyes magatartások betartásának meghatározása a feladata.

Bűnmegelőzés:

- feladata a bűncselekmények megelőzése, a bekövetkezett bűncselekmények esetén szükséges lépések meghatározása;
- a jelenlegi IT-eszközök és -rendszerek, valamint a velük kapcsolatos jövőbeni veszélyekre való figyelmeztetés lehetősége (prediktív rendészet).

5.6. Mire lehet ebből következtetni?

A kiberreziliencia, vagy más néven kiber-helyreállítóképesség az informatikai hálózatok és rendszerek túlélőképességét elősegítő, alkalmazkodóképesség-növelő, redundanciabiztosító elemek és eljárások összességét fedi. Mindazok a technológiák és folyamatok tartoznak tehát ide, amelyek egy esetleges informatikai támadás esetén biztosítani képesek a működés folyamatosságát, illetve egy kibertámadást követően a működés teljes helyreállítását.

A tanulmány első részében bemutatott, a fekete kalapos hackerekkel készített felmérés eredményei felébresztették már a szervezeteket, hogy erősítsék meg kiberbiztonsággal kapcsolatos tevékenységüket. Hosszú időn keresztül a kiberbiztonságot sokkal inkább a rendszerek és az informatikai eszközök fejlesztésében látták.

Azok tökéletesítésében bízva egyre nagyobb összegeket ruháztak be, hogy minél gyakrabban cseréljék, fejlesszék azokat. Az információs rendszereket és eszközöket működtető szoftverek frissítése, cseréje szintén első helyen szerepelt annak érdekében, hogy a szervezet vagy vállalat minél nagyobb biztonságban tudja az adatait. A nem jól kiválasztott és képzetlen munkavállalókra úgy tekintettek, mint olcsó munkaerőre. A valamennyire vagy már jól képzett, biztonsággal foglalkozó szakemberekre kevésbé tartottak igényt, vagy épp csak olyan területeken alkalmazták őket, ahol a tudásukat csak meghatározott körben ismerték meg.

A 2013. évi L. törvény előírja a szervezetek vezetőinek, hogy kötelesek gondoskodni az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maguk és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról.[20]

Az alábbi tevékenységek megerősítését kiemelten fontosnak ítélték meg a vállalatok és szervezetek számára, azért, hogy az információs rendszereikhez kapcsolódó munkavállalók be tudják tartani a kiberbiztonsághoz fűződő feladataikat a már említett 2017-es Black hat hackers konferencián:

- A vállalat számára minden érdekelt fél oktatása a kiberbiztonság alapjairól.
- Emberközpontú megközelítés a kiberbiztonságban, amely a biztonsági beállítások könnyű kezelhetőségét helyezi előtérbe, miközben mások számára a vállalati rendszer bonyolultságát súgja.
- Multi-Factor Authentication megvalósítása e-mailekben és minden érzékeny, kiemelt fiókban.
- Titkosítás engedélyezése a felhasználói hitelesítő adatok és a magánélet védelme érdekében.
- A privilegizált fiókok kezelésének és biztonságának automatizálása.

Elsődleges kutatásom alapján a fentiekre tekintettel:

- alapvetően a kibertudatossággal összefüggő kifejezések és készségek megvannak (csak 4% mondta, hogy szokott ingyen wifire csatlakozni, ami hotelekben vagy bevásárlóközpontokban van);
- a jelszó megválasztásnál a biztonságos jelszó sémával tisztában volt (de legalábbis tudja, hogy milyennek kellene lennie);
- a kitöltők 68,2%-a 3-asra értékelte a biztonságérzetét az interneten (ez a szám leginkább azt mutatja, hogy ennyi figyel a weboldalak biztonságára).

Szekunder kutatásom ugyanakkor arra enged következtetni:

- a legtöbb felhasználója a Facebook közösségi oldalnak van, amivel összefüggésben tesznek a legtöbb feljelentést a jelszóval való visszaélés miatt;

[20] 2013. évi L. törvény az állami és önkormányzati rendszerek elektronikus biztonságáról 11. § (1) bekezdés *g)* pont.

- a hatóságok a kihallgatások során nem kérdeznek rá a sértettekt/feljelentők jelszóhasználati szokásaira, amivel nem erősítik bennük, hogy mire kell figyelni, mitől lesz biztonságos az internetes fiókjuk;
- még mindig több magánszemély tesz feljelentést, mint cég vagy vállalkozás, holott például az említett Microsoft-felmérés azt mutatja, hogy sokkal több céget kellene hogy érintsen egy-egy támadás.

6. Összegzés

Az elmúlt években a kibertérben elkövetett bűncselekmények és kibertámadások száma megnőtt, a támadók újabb és újabb támadási technikát és módszereket találnak ki. Az információs rendszerek és eszközök alkalmazása nemcsak egyre népszerűbb, hanem most már valamennyi generációra hatással van.

A kiberfenyegetések mennyisége és kifinomultsága folyamatosan növekszik. 2020-ban a Világgazdasági Fórum a 10 legnagyobb globális kockázat közé sorolta a kibertámadásokat, amelyek mintegy 530 milliárd eurós kárt okoztak világszerte, míg az EU-ban a kiberkémműveletek akár 60 milliárd eurós gazdasági kockázatot is jelentenek.

A 21. század előrehaladtával egyre több területen kerül sor a digitalizációra. Ez a társadalom szinte minden területére érvényes.[21] Az olyan új élethelyzetek, mint a pandémia is, magával hozza, hogy az élet még több területén jelenjenek meg az információs rendszerek. A digitális munkahelyek mellett az önvezető járművek, a mesterséges intelligencia és a robotok segítik a hatékonyabb munkavégzést, de ugyanúgy a távirányítással működő drónok, amelyek a mezőgazdaságban az öntözést, az áruszállítást, és az objektumvédelemben a terület megfigyelését, a határ védelmét és a közlekedés biztonságát felügyelik.

A technika fejlődik, de ez nem elég, hiszen ezen eszközök hozzáféréséhez még mindig köze van az azt üzemeltetőnek, vagy épp a fejlesztőnek.

Mára már felismerték, hogy a „leggyengébb láncszem az ember" kifejezésnek sokkal mélyebb jelentése van a kiberbiztonság és kibervédelem területén, mint a fizikai térben. Kiemelten sérülékeny csoportot jelentenek a fiatalkorúak is.[22]

A kiberrezilienciával két európai szervezet is foglalkozik. Az egyik az Európai Űrkutatási Ügynökség (*European Space Agency,* ESA), a másik az Európai Védelmi Ügynökség (*European Defence Agency,* EDA).[23]

---

[21] Czenczer Orsolya: Külföldi minták – honi tennivalók a fiatalkorúak büntetés-végrehajtásában. *Börtönügyi Szemle,* 28. (2009), 1. 1–10.

[22] Czenczer Orsolya: A gyermekbántalmazás és az erőszakos bűnelkövetés összefüggéseinek vizsgálata a hazai büntetés-végrehajtásban. In Homoki-Nagy Mária et al. (szerk.): *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis: Acta Juridica et Politica,* (81). Szeged, Szegedi Tudományegyetem Állam- és Jogtudományi Kar, 2018. 187–198.

[23] Nemzeti Kibervédelmi Intézet hírlevele: Európai ügynökségek akciószövetsége a kiber reziliencia erősítésére. *E-gov Hírlevél,* 2021. október 18.

Az együttműködésnek az alábbi feladatok végrehajtása a célja:

- folyamatos információmegosztás és a megfelelő képességek megosztása;
- továbbfejlesztett képzés és személyre szabott kiberreziliencia-tanfolyamok és -gyakorlatok;
- az egyes szervezetek hozzáférésének megkönnyítése a saját közösségeikhez, szakértelmükhöz és infrastruktúrájukhoz;
- az EDA és az ESA közötti együttműködés kiterjesztése más kulcsfontosságú kiberbiztonsági szereplőkre Európában, mint például az Európai Bizottság, a Külügyi Szolgálat, az EU Műholdközpontja, az ENISA, az Európai Biztonsági és Védelmi Főiskola és az Európai Kiberbiztonsági Kompetencia Központ és Hálózat, hogy csak egy párat említsek.

Egy vállalatnál vagy egy szervezetnél a biztonsági és védelmi feladat végrehajtása akkor működik, ha az elvárt biztonsági szint megfelelő, az azt végrehajtó személyek ismerik és figyelemmel követik a szükséges intézkedéseket, és reagálnak a fellépő problémákra. Nem elhanyagolható az oktatás kérdése. Ennek egyik legnagyobb hibája, amikor egy, már bekövetkezett probléma vagy támadás esetén nem tudnak reagálni, a bekövetkezett kárt elhárítani vagy csökkenteni. Épp emiatt sok helyen az évi egyszeri oktatás vagy e-learning-anyag, vizsga nem feltétlenül elegendő, hiszen ezzel nem tud kialakulni a tényleges tudatosság.

A tanulmányhoz készített kérdőív és az állami vagy magánszektorban elkészített felmérések azt mutatják, hogy a munkahelyi és az otthoni biztonságtudatosság nincs párhuzamban egymással. Amíg a munkahelyi tudatosságot különböző szinteken ellenőrzik, az otthonit nem. Ennek a legnagyobb hibája, hogy az otthoni munkavégzés során elkövetett egyéb hibák kihatással lehetnek egy szervezet biztonságára (social engineering támadások).

Mezei Kitti megállapításával egyetértve a biztonságtudatosság többlépcsős feladat. Fontos belátni, hogy a kiberbűnözés komplex problémakört foglal magában, amellyel szemben többlépcsős stratégiának az alkalmazása vált indokolttá. Ebben kiemelt jelentősége van elsődlegesen a prevenciónak, különösen a felhasználókhoz igazított oktatásnak, ismeretterjesztésnek, mert még mindig az ember a leggyengébb láncszem a kiberbiztonság szempontjából. Fontos a harmonizált, egységes nemzetközi szabályozás megteremtése büntető anyagi és eljárásjogi tekintetben. A fokozott együttműködés elősegítése is lényeges elem a magánszektor és a bűnüldöző hatóságok között, illetve az egyes bűnüldöző hatóságok között. Szükséges továbbá, hogy az új kihívásokra a jogalkotók adekvát módon és gyorsan reagáljanak, és a jogalkalmazókat is felkészítsék erre, mert a technológiai fejlődés új elkövetési módokat teremt meg, amelyeknek jogi minősítése vitatott lehet.[24]

[24] Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. *Magyar Jog*, 66. (2019), 5. 305–314.

A cégek, vállalkozások tekintetében erősíteni kellene azt, hogy a hatóságok felé intézett jelzés egy kibertámadásról nem maradhat abban az esetben sem magánügy, ha képesek annak elhárítására, vagy a kár csökkentésére, hiszen a bejelentési kötelezettséggel az ország kiberbiztonságát és -védelmét is erősítik.

A *Biztonságtechnikai szakportál* által publikált jelentésben kiemelték, hogy kelet-közép-európai régiós szinten a tagállamok között Magyarországon a második legsúlyosabb veszélyforrás a munkavállalók alacsony tájékozottsága. Ennek ellenére az alkalmazottak felkészítését célzó kiberbiztonsági képzéseket Magyarországon csak a cégek 30%-a tervezett elindítani 2021-ben.[25]

Ez azt is jelenti, hogy nemcsak szükséges, hanem muszáj foglalkozni a biztonságtudatosítással a kibertérben és az online eszközökön.

A tudatosításban és oktatásban kiemelt szerepe van a Nemzeti Közszolgálati Egyetemen folyó oktatásoknak, kutatásoknak és együttműködési megállapodásoknak, amivel remélhetőleg újabb és újabb biztonságtudatosító ismeretterjesztő anyagokkal járulnak hozzá a közszolgálatban és a magánszektorban lévő képzésekhez.

FELHASZNÁLT IRODALOM

Czenczer Orsolya: Külföldi minták – honi tennivalók a fiatalkorúak büntetés-végrehajtásában. *Börtönügyi Szemle,* 28. (2009), 1. 1–10.

Czenczer Orsolya: A gyermekbántalmazás és az erőszakos bűnelkövetés összefüggéseinek vizsgálata a hazai büntetés-végrehajtásban. In Homoki-Nagy Mária – Karsai Krisztina – Fantoly Zsanett – Juhász Zsuzsanna – Szomora Zsolt – Gál Andor (szerk.): *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis: Acta Juridica et Politica,* (81). Szeged, Szegedi Tudományegyetem Állam- és Jogtudományi Kar, 2018. 187–198.

Európai ügynökségek akciószövetsége a kiber reziliencia erősítésére. *E-gov Hírlevél,* 2021. október 18. Online: https://hirlevel.egov.hu/2021/10/18/europai-ugynoksegek-akcioszovetsege-a-kiber-reziliencia-erositesere/

Gyaraki Réka: A közösségi média hatása a kiberbűncselekmények elkövetésére. *Magyar Rendészet,* 21. (2021), 2. 67–82. Online: https://doi.org/10.32577/mr.2021.2.4

Kárász Balázs: Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata. *Biztonságtudományi Szemle,* 2. (2020), 2. 57–68. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/51/52

Kollár Csaba – Zakar Ákos: A Social Engineering és a manipulációs technikák és módszerek. *Biztonságtudományi Szemle,* 2. (2020), 2. 23–38. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/58/50

Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. *Magyar Jog,* 66. (2019), 5. 305–314.

Microsoft: *Kiberbiztonsági trendek Közép- és Kelet-Európában. A 2020-as év digitális biztonsági kihívásai és hasznos javaslatok cége ellenálló képességének fokozására.* Online: https://info.microsoft.com/CE-SCRTY-CNTNT-FY21-04Apr-27-JelentesKiberbiztonsagitrendekKozepesKeletEuropaban-SRGCM4609_01Registration-ForminBody.html

[25] Térségi kiberbiztonsági kitekintés… (2021): i. m.

Molnár Gábor: XLIII. fejezet. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In Kónya István (szerk.): *Magyar büntetőjog. Kommentár a gyakorlat számára*. 3. kiadás. Budapest, HVG-ORAC Lap- és Könyvkiadó, 2016. 1764–1780.
Nagy Zoltán András: XLIII. fejezet. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In Tóth Mihály – Nagy Zoltán András (szerk.): *Magyar büntetőjog. Különös rész*. Budapest, Osiris Kiadó, 2014. 589–604.
Nemzeti Média- és Hírközlési Hatóság: *Az elektronikus hírközlési piac fogyasztóinak vizsgálata. Internetes felmérés* (2020). Online: https://nmhh.hu/dokumentum/218531/internetes_felmeres_2020.pdf
Oroszi Eszter Diána: Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük. *Dunakavics*, 8. (2020), 5. 5–20. Online: http://dunakavics.uniduna.hu/Online_2005.pdf
Pusztai Ferenc – Csábi Szilvia: *Magyar értelmező kéziszótár.* Budapest, Akadémiai Kiadó, 2004.
Térségi kiberbiztonsági kitekintés a Microsofttól. *Securinfo,* 2021. május 17. Online: www.securinfo.hu/hirek/12278-tersegi-kiberbiztonsagi-kitekintes-microsofttol.html
Tóth Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In Gál István László – Nagy Zoltán András (szerk.): *Informatika és büntetőjog.* Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2006. 180–188.

Jogi források

2012. évi C. törvény a büntető törvénykönyvről
2013. évi L. törvény az állami- és önkormányzati szervek elektronikus információbiztonságáról

ABSTRACT

The Role of Security Awareness, Questions about Cybersecurity

Réka GYARAKI

Our lives are increasingly dependent on IT tools and systems. More and more people are using the innovations brought about by the 4th Industrial Revolution, but the dangers are less and less known. The web and information systems have brought a technological explosion that the average user may not be able to keep up with. However, if the average user is not aware of security on their own devices and systems, it can be reasonably assumed that the same user will not be aware of security at work.
In the public and private sectors, the prevention of cyber-attacks and the examination of the vulnerabilities of the sectors will focus on the weakest link in the chain that causes the vulnerability of information systems. In this study, I am looking for the answer to the current practice of developing cyber security in Hungary and the skills we can use to strengthen people as components of the chain.

Keywords: *cybersecurity, awareness, users, good practice, information systems*