Biztonságtudatosság és jelszavak

Keszthelyi András

Keszthelyi.Andras@kgk.uni-obuda.hu

Absztrakt: Közhelyszerű megállapítás, hogy világunkat információs társadalomnak nevezzük, de hívhatjuk akár virtuális világnak is. A tágan értelmezett informatika robbanásszerű fejlődése az elmúlt három évtizedben alapjaiban alakította át az életet. Ennek következtében jelentősen felértékelődött a biztonság szerepe a virtuális világban. Ennek egyik kulcsfontosságú eleme a jelszó (mint eszköz) és általában a biztonságtudatosság, ha úgy tetszik: óvatosság (mint emberi tényező). Sajnos naponta szembesülünk avval, hogy van még lehetőség a fejlődésre, mind a magunk szempontjából, mind pedig az új generációk oktatása-nevelése terén. A jelen tanulmány a jelszavak helyes (és eredményes) használatának néhány fontos szempontját hangsúlyozza, illetve eloszlat néhány tévképzetet.

Kulcsszavak: jelszó

Bevezetés

Megjelent egy tanulmány a Z-generáció biztonságtudatosságáank vizsgálata egyetemi hallgatók körében címmel. [1] Ezen tanulmányban a szerző azt vizsgálja, hogy a digitális korszakba beleszületett Z-generációs fiatalok vajon mennyire vannak tisztában a kiberbiztonsági módszerekkel, hogy vajon milyen mértékben képesek tudatos döntéseket hozni digitális adataik védelmében, és hogy milyen mértékű a biztonságtudatosságuk.

A szerző két hipotézist állít föl. A H1 hipotézis szernt a Z-generációs fiatalok nem elég óvatosan a kiberbiztonság területén, ill. a H2 szerint nem is kapnak megfelelő oktatást-nevelés a kiberbiztonság terén.

A szerző ezen belül kiemelten vizsgálja a jelszóhasználati szokásokat. A kérdőíves felmérésének eredményei szerint a válaszadók negyede még sosem változtatta meg a jelszavait, 45% hat hónapnál régebben változtatott jelszót. Minden fontos helyre egyedi jelszó szükséges, és a jelszó vegyes összetételénél fontosabb a jelszó hossza.

A jelen tanulmányban a jelszavakkal kapcsolatos hiedelmeket, ill. azok egy részét veszem nagyító alá.

Az információs társadalom vagy a kiberbűnözés kora

Szokás úgy beszélni korunkról, mint az információs társadalom koráról, ahol és amikor az infokommunikációs technológiák robbanásszerű fejlődése az elmúlt kb. három évtizedben igen jelentős mértékben alakította át a mindennapi életet. Ez az átalakulás olyan mértékű, hogy teljesen indokolt a külön, új elnevezés. Az információs társadalom kifejezés mellett nyugodtan használhatjuk a virtuális világ kifejezést is, mint olyant, ami találóan rátapint a lényegre.

A virtuális világban – sajnos – megjelent a virtuális bűnözés is. Amíg csak arról volt szó, hogy délután ötkor a számítógép eljátssza a Yankee Doodle dalt [1], jelezve a munkanap végét, azt még lehet akár jópofa, vicces dolognak is tekinteni. Ezen a szinten azonban hamar túlfutott a „fejlődés", és a virtuális világbeli virtuális bűnözés nagyon is valóságos károkat okoz.

Olyannyira valóságos károkat okoz, hogy nevezhetnénk korunkat akár a kiberbűnözés (és -háborúk) korának is. „A kiberbűnözés (…) egy 1 trillió dollár feletti iparág, amely az Egyesült Államok és Kína után a világ harmadik legnagyobb gazdasága lenne, ha arról lenne szó. Már rég lekörözte a kartelleket, a drogkereskedelmet és minden mást" [3].

De nézzünk néhány kézzelfogható példát, sajnos bőséges készletből lehet válogatni.

Az MVM Next külön honlapot üzemeltet a nevükkel visszaélő adathalász kísérletek miatt és ellen. [3] „Az MVM Next felhívja ügyfelei figyelmét az egyre gyakoribb adathalász üzenetekre, amelyek banki és személyes adatok megszerzésére irányulnak. A csalók gyakran fizetési felszólítással vagy visszatérítéssel próbálják becsapni a felhasználókat." [4]

2021-ben a Ferencváros a Rijeka labdarúgócsapatától szerződtette Stjepan Loncart. Az FTC átutalta a kialkudott összeget a Rejkának csakhogy a Rijeka levelezőrendszerét időközben meghekkelték, az átigazolási díjat egy álszámlára utaltatták. [5] Pedig a naiv ember úgy gondolná, hogy egy cégszerű utalás elég sok kézen megy keresztül ahhoz, hogy közülük valakinek feltűnjenek a gyanús jelek. De, úgy látszik, nem mindig.

A célba vett személyek száma esetenként igen jelentős is lehet. 2025 augusztusában egy fórumon közel tizenhat millió PayPal felhasználó belépési adatai jelentek meg, ide értve a nyílt szöveg formájú jelszavakat is. Vita tárgya volt, hogy ez az adatszivárgás mikor történt, vagy történhetett meg, a PayPal azt állította, hogy ezek az adatok még a 2022. évi adatlopásból valók (ami miatt az amerikai hatóságok kétmillió dollárra büntették a PayPal vállalatot. [6]

Egy hekkercsoport sikeresen feltörte a Google adatbázisát, és mintegy 2,5 milliárd felhasználó különböző adataihoz fért hozzá – a cég állítása szerint a támadók nem tudtak igazán érzékeny adatokat (mint pl. jelszavak) megszerezni. [7]

Nemcsak az áldozatok mozognak széles skálán a magánembertől a nemzetközi óriásvállalatokig, hanem az elkövetők is. A kommunista Észak-Korea állami szinten űzi a kiberbűnözést, 2024 januárjától az idei év szeptemberéig közel hárommilliárd amerikai dollárnak megfelelő kriptovalutát tulajdonítottak el közel-keleti és ázsiai kriptotőzsdékről. [8]

Van olyan – a lehetőségeknek csak a fantázia szab határt –, amikor a támadás közvetett. Netes csalók előszeretettel használják a booking.com szállásközvetítő oldalt álcázásra. A szállásadó rendszerébe törnek be, booking.com-os bejelentkezési adatokat keresnek, és ha találnak, a booking.com-on keresztül küldik az üzenetet a reménybeli áldozatnak, így a hitelesség erősebb látszatát keltve. [9]

Lehet vitát nyitni arról, hogy milyen mértékű kárt jelent (dollárban vagy forintban) egy olyan eset, amikor felhasználói adatokat lopnak el sikeresen egy nagyvállalattól, mint pl. a Google/Gmail vagy a PayPal. Ennél azonban sokkal komolyabb, igen jelentős összeget is veszíthet az áldozat.

Már évekkel ezelőtt azon a szinten volt a „mesterséges intelligencia" fejlődése, hogy kiváló minőségben tudta adott ember beszédét, hangját és hanghordozását utánozni. A csalók 35 millió dollárt utaltattak el egy átvert banki alkalmazottal az Egyesült Arab Emirátusban. A csalók „a fiókvezető hangját utánozva telefonon kapcsolatba léptek a banki alkalmazottal. (...) Hogy biztosra menjenek, az utalásra vonatkozó kérést hamis levelekkel is megtámogatták, így a beosztott végképp nem gyanakodott. Pedig kellett volna." [10]

Ezt lehet még tovább is finomítani. Tavaly például kilencmilliárd forintnyi összeget utaltattak el sikeresen egy átvert banki dolgozóval. „Az ügy egy olyan üzenettel indult, ami még a pénzügyi munkatárs számára is gyanús volt. Adathalászatra gyanakodott, mivel egy „titkos tranzakcióról" esett szó benne. Miután azonban videóhívást is folytatott a cég pénzügyi vezetőjével – valamint több, általa ismert személlyel –, már nem voltak kétségei." [11] A videokonferencia azonban hamisított volt, az átvert dolgozón kívül minden résztvevőt mesterséges intelligenciával generáltak. És eléggé élethűen ahhoz, hogy a végül sikeresen átvert munkatárs kezdeti gyanakvását eloszlassák. [12]

A Jaguar Land Rover szeptember elején bejelentette, hogy kibertámadás érte, ami olyan súlyos, hogy le kellett álllítani a gyártásirányító informatikai rendszert (is). A kényszerszünet legalább október 1-ig eltartott, a helyzet súlyosságát mutatja az a körülmény is, hogy a brit kormány – ez alkalommal először – másfél milliárd fontig terjedő hitelgaranciát vállalt annak érdekében, hogy a vállalat beszállítóinak pénzügyi nehézségeit enyhíteni tudják. [13]

Lehetne folytatni a példák szinte végtelen sorát, azonban ez is bőven több példa a kívánatosnál. Mindenképpen indokolt úgy tekinteni korunkra, mint olyan időszakra, amelyben meghatározó jelentősége van a kiberbűnözésnek, sőt a kiberháborús cselekményeknek is.

A jelszavak helyes használatáról

Mivel az infokommunikációs technológiák, magyarán a hálózatba kötött számítógépek – a ChatGPT és a Google szerverparkjaitól az asztali gépünkön át az okostelefonunkig – olyan szinten nélkülözhetetlenek a mindennapjainkban, hogy jószerivel megmozndulni sem tudnánk nélkülük. A tét nagysága és a helyzet súlyossága miatt nézzünk jobban utána a jelszóhasznáalt azon szűk területének, amelynek kapcsán a hivatkozott cikk [0] is vizsgálja a jelszóhasználati szokásokat.

A továbbiakban funkcionális elvű megközelítést alkalmazok, vagy másképpen mondva a vezető és a felhasználó szemszögéből vizsgálom az alapvető követelményeket, amelyeket a jelszavakkal, jelszóhasználattal kapcsolatosan támasztani lehet, illetve kell.

A legfontosabb két elvárás az, hogy a jelszó legyen a) megjegyezhető, b) megtippelhetetlen.

A megjegyezhetőség követelménye lgalább valamennyire szubjektív követelmény, de szélsőséges eseteket leszámítva nem okozhat problémákat. A megtippelhetetlenség követelményéhez viszont a tippelési módszereket kell ismerni, annak érdekében, hogy olyan jelszót válasszon a felhasználó, ami ezen módszereknek – értelemszerűen – ellenáll. Ezeket dióhéjban összefoglalom az alábbiakban.

Alapértelmezett és legrosszabb jelszavak esete. Amikor a felhaszáló nem változtatja meg a gyári alapértelmezett jelszót (pl. a wifi-routerben), vagy a világviszonylatban, ill. saját nyelvén a leggyakoribb és leggyöngébb jelszavak közül választ (pl. asdfgh). Ezen esetek a súlyos felelőtlenség csoportjába tartoznak.

A felhasználói név és a jelszó hasonlít egymásra (pl. admin – admin, admin – admin01), a jelszó megegyezik a felhasználónévvel vagy annak egyszerű toldalékolása. Ugyancsak a súlyos felelőtlenség csoportjába tartoznak.

A jelszó a felhasználó valamely személyes adata (pl. születési dátum, kedvenc csapata, első gyerekének a neve). Ugyancsak felhasználói felelőtlenség, ismertek olyan esetek, amikor meglepően eredményes illetéktelen hozzáféréseket tett lehetővé az ilyen jelszóválasztás.

Kézenfekvő jelentésbeli kapcsolat van a jelszó és a felhasználói név között (pl. Drakula – LugosiBela). Szintén felelőtlenség.

Szótár alapú támadás, amikor az illetéktelen személy egy célprogrammal végigpróbáltatja egy lista összes elemét, amely lista a(z adott helyzetben) legvalószínűbbnek ítélt jelszavakat tartalmazza, ide értve az adott nyelv ezer-kétezer leggyakoribb szavát is. Mindenképpen gondatlanság.

A továbbfejlesztett szótár alapú támadás a következő lehetőség, az előzőt kiegészítjük avval, hogy a listázott szavak egyszerű toldalékolásait (pl.

ablak00..ablak99) is kipróbáltatjuk az erre szlgáló célprogramok valamelyikével. Megjegyzendő, hogy ezeket alapvetően offline módban lehet alkalmazni, amennyiben sikerült valamilyen módon megszerezni a célrendszerből az ún. árnyékjelszavakat. Ha online lehetőség is lenne erre (pl. egy régi időkből ottfelejtett, naplózatlan POP3 szolgáltatás révén), az üzemeltetői gondatlanság.

A nyers erő alkalmazása a legutolsó eset. Ekkor a célprogram minden lehetséges karakterkombinációt kipróbál. Nyilvánvaló, hogy meg fogja találni az adott jelszót előbb-utóbb, a kérdés csak az, hogy vajon reális idő alatt-e. Ugyancsak offline alkalmazható, ez esetben a fő paraméterek a jelszavakra alkalmazott hash függvény számításigénye, a töréshez rendelkezésre álló számítási teljesítmény, ezek értelemszerűen az üzemeltető felelősségi körébe tartoznak. Valamit ugyancsak lényeges paraméter a jelszó hossza, ami viszont elsősorban felhasználói felelősség. Nem felejtettük el, hogy ha a jelszó hosszát növeljük, a lehetséges karekterkombinációk száma a hossz exponenciális függvénye. Hogy ezen a területen a kvantumszámítógépek közeljövőben várható elterjedése milyen változásokat fog jelenteni, az érdekes kérdés, illetve a posztkvantum algoritmusok jelentőségét hangsúlyozza. [15]

Az eddigiek alapján nyilvánvaló, hogy a jelszó jóságának a fő szempontjai azok, hogy elég hosszú legyen, és a nagy keresők ne adjanak egetlen találatot sem rá (vagy érdemi részeire), viszont ez utóbbit nem célszerű kipróbálni, de érdemes észben tartani.

Van olyan világhírű, élvonalbeli egyetem, ahol hivatalos honlapjukon hirdetik azt a módszert, miszerint választani kell négy könnyen vizualizálható szót (sas, narancs, kulcs, cipő), majd ezeket összefűzve aránylag könnyen megjegyezhető és elegendően hosszú jelszót kapunk. Ez igaz, de! Ha adott helyzetben a támadó felteheti, hogy a felhasználóknak legalább egy része megfogadja ezt a tanácsot, akkor a nyers erős törést nem a 18-25 betűnyi jelszavakra fogja alkalmazni a siker reális esélye nélkül, hanem az adott nyelv mondjuk kétezer leggyakoribb szavából képez négyes csoportokat, és (másod)percek alatt megvalósítja a sikeres törést.

Ejtsünk szót a jelszó időnkénti megváltoztatásának követelményéről is, ami a legtöbb helyen előírás, és gondolatébresztő tanulmányunk [0] felmérésének is egyik eleme.

Hasonló kérdés, hogy otthon a bejárati ajtónkon mikor cserélünk zárat. Akkor cserélünk zárat, ha a kulcsunkat elhagytuk (akkor is, ha később visszakapjuk a becsületes(?) megtalálótól), illetve ha fölmerül annak a gyanúja, hogy valaki hozzájuthatott.

Informatikai rendszerekre alkalmazva: ha a rendszer biztonságát érintő esemény történt, vagy ennek a megalapozott gyanúja fölmerül, ide értve az olyan lehettséges eseményeket is, mint pl. hogy a felhasználó háta mögül valaki leleshette a jelszavát annak begépelésekor. Egyébként nyilvánvalóan fölösleges.

A másik lehetőség, ha fennáll annak a reális esélye, hogy a megszerzett jelszót a támadó egy jövőbeli alkalomra tartalékolja, vagy titokban és a jogos felhasználóval párhuzamosan akarja használni. Mint ha pl. a leleményes diák szeptemberben ügyesen meglesi a tanár Neptun-jelszavát abból a célból, hogy majd januárban gondot viseljen az Információbiztonság jegyére, vagy ha valaki nagyon szeretné tudni, hogy mi mindenről levelezget a leendő exe.

A közismert, mindenhoz szajkózott további előírások, miszerint minden helyre különböző és erős jelszót kell választani, nem tűnnek reálisnak. Manapság egy nem informatikus embernek is lehet több tucat jelszóvédett hozzáférése. Nem reális elvárás, hogy ezek mindegyike teljesen különböző, elegendően erős jelszó legyen (és esetleg ezeket is rendszeresen változtatgassa). Ezen a ponton csoportosítani kell a jelszóvédett hozzáféréseket fontosság, érték szepontjából, és a legfontosabbak (legdrágábbak) esetében kell az egyedi erős jelszó, a többiekre pedig használhatunk valamilyen, nem első látásra nyilvánvaló szabály szerint egységes szerkezetű jelszavakat, vagy – ha megbízunk ilyesmikben – jelszómenedzser alkalmazást, vagy megjegyeztetjük a böngészővel stb.

Összefoglalás

Feltétlenül igaza van gondolatébresztő tanulmányunk [1] szerzőjének abban, hogy a fiatalok oktatása-nevelése terén bizony vannak hiányosságok, jelesül és esetünkben az információbiztonság területén is. Viszont nem árt, sőt kifejezetten hasznos, ha a régi időkből öröklődött szabályokat újragondoljuk.

Források

[1.] Csercsa, K. (2025). Security awareness of Generation Z among university students. In: In: Keszthelyi, András; Szikora, Péter (szerk.) 23rd International Conference on Management, Enterprise and Benchmarking. Proceedings II., Óbuda University, Budapest, 2025. ISBN 978-963-449-385-3, pp. 98-106.

[2.] Yankeedoodle (é.n.), The Virus Encyclopedia, http://virus.wikidot.com/yankeedoodle

[3.] Mucsi, V. (2025): Ez lenne a világ harmadik legnagyobb gazdasága, ha nem lopnák el az összes pénzt. Index, 2025.09.19. https://index.hu/techtud/2025/09/19/kiberbiztonsag-kiberbunozes-hacker-bodis-akos-szakerto-tortenelem-bitcoin/

[4.] Tudnivalók az adathalászatról (é.n.). https://www.mvmnext.hu/Adathalaszat

[5.] Mucsi, V. (2025). Riadót fújt az MVM, egyre több ember számláját nullázzák le a csalók. Index, 2025.10.18. https://index.hu/belfold/2025/10/18/adathalaszat-csalok-online-mvm-energetika-rezsi-szamla-hamisitvany/

[6.] R. Gy. B. (2025): Kiberbűnözők károsították meg a Ferencvárost és a Rijekát. Nemzeti Sport, 2025.09.23. https://www.nemzetisport.hu/labdarugo-nb-

i/2025/09/dontott-a-cas-a-fifa-altal-megallapitott-osszeg-felet-kell-csak-fizetnie-a-ferencvarosnak

[7.] Petkauskas, V. (2025). PayPal breach exposed nearly 16M login credentials, hackers claim. Cybernews, 2025.08.18. https://cybernews.com/security/paypal-credential-dump-hacker-claims/

[8.] Winter, D. (2025). Google Confirms It Has Been Hacked — What User Data Has Been Stolen?. Forbes, 2025.08.09. https://www.forbes.com/sites/daveywinder/2025/08/09/google-confirms-it-has-been-hacked---user-data-stolen/

[9.] Seung-yeon, K. (2025). N. Korea has stolen about US$2.84 bln in virtual assets: report, Yonhap News Agency, 2025.10.22. https://en.yna.co.kr/view/AEN20251022001000315

[10.] Bartók, D. (2025). Adathalászat és a Booking.com esete, Zsebinformatikus, 2025.06.27. https://zsebinformatikus.hu/blog/alapozo/2025-06-27-adathalaszat-es-a-booking-pont-com-esete

[11.] sz.n. (2021). Mesterséges intelligenciával raboltak bankot, 11 milliárd forint a kár. HVG, 2021.10.21. https://hvg.hu/tudomany/20211021_mesterseges_intelligencia_csalas_egyesult_arab_emirsegek

[12.] sz.n. (2024). Megérkezett a jövő: 9 milliárd forintot utalt el csalóknak egy cég pénzügyese, akit deepfake technológiával csaltak tőrbe. HVG, 2024.02.05. https://hvg.hu/tudomany/20240205_deepfake_penzugyi_vezeto_atveres_videohivas

[13.] Chen, H. - Magramo, K. (2024). Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’, CNN, 2024.02.04. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

[14.] szn.n. (2025). Gigantikus kár érte a híres autógyárat a kiberbűnözők miatt, a brit államnak kell kisegítenie, Privátbankár, 2025.09.28. https://privatbankar.hu/cikkek/vallalat/gigantikus-kar-erte-a-hires-autogyarat-a-kiberbunozok-miatt-a-brit-allamnak-kell-kisegitenie.html

[15.] Szikora, P., & Lazányi, K. (2022). The end of encryption?–The era of quantum computers. In Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach (pp. 61-72). Dordrecht: Springer Netherlands.