A GÉPÉSZ HALLGATÓK JELSZÓHASZNÁLATI SZOKÁSÁNAK VÁLTOZÁSA INFORMÁCIÓBIZTONSÁGI KURZUS UTÁN

DIE VERÄNDERUNG DER KENNWORT NUTZUNGSGEWOHNHEIT DER MASCHIENENBAUINGENIEUREN NACH EINEM INFORMATIONSSICHERHEITSKURS

Kiss Gábor, PhD., gabor.kiss@bgk.uni-obuda.hu

INHALT
In diesem Publikation wollten wir analysieren die Veränderung der Kennwort Nutzungsgewohnheit der Maschienenbauingenieuren. Vor dem Kurs und nach dem Kurs sollten die Studenten ein Fragebogen ausfüllen, die enthalt verschiedene Fragen über die benutzten Kennwörtern (wie lang, wie kompliziert, wie unterschiedlich, usw). In dem Kurs haben wir für die Studenten über Blackboard und Power Point basierte Vorlesungen mit Videounterstützung, wie schnell kann man ein kodierten Kennwort hacken, wenn es nicht denug lang und kompliziert ist. Die Analyse zeigt, wie diese Eigenschaften der benutzter Kennwörter verändern. Nach dem Analyse können wir schon sehen, die Maschienenbauingenieuren konnten nicht die Vorteil der neue Informationen über die sicherer Kennwörten benutzen um die eigenen sensitive Daten sicherer zu lagern. Wir müssen anderen didaktische Methode ausprobieren, wie die Softwareunterstüzte, wo kann man die kodierten Kennwörtern mit unterscheidlichen Programme hacken, so kann man leichter erkennen, wie lange dauert es bei einem kurzen und einfachen Kennwort.

1. BEVEZETÉS

A nemzetközi tapasztalat alapján hiába jelennek meg a médiában és az információbiztonsággal foglalkozó cégek oldalán cikkek azzal kapcsolatban, hogy éppen melyik szolgáltatónál lévő felhasználók adatait (esetenként több millió embert érintve) szerezték meg feketekalapos hackerek[1], esetenként még ki is téve közfelhasználásra az adatokat az internetre [2], a felhasználók továbbra is gyenge, könnyen kitalálható, illetve visszafejthető jelszavakat használnak [3][4]. Előfordul, hogy a jelszavak visszafejtésével sem kell törődni, hiszen a rendszerben eredeti formájában tárolják azokat [5]. Az emberek többsége napjainkban sincs tisztában a szenzitív adatainak megfelelő védelméről, és nem használ nehezen feltörhető jelszavakat. Az Óbudai Egyetem gépészmérnöki szakán végző hallgatók többnyire nemzetközi cégekhez kerülnek, ahol szenzitív adatok kerülnek a bírtokukba és fontos, hogy tudatában legyenek ezek védelmi lehetőségeinek, ezért információbiztonsági kurzuson vehettek részt.

Az információbiztonsági kurzuson áttekintettük az egyes titkosítási módszereket, majd átbeszéltük a titkosított jelszavak feltörési módjait, táblán, PowerPoint prezentációval, esetenként videófelvétellel bemutatva a gyenge jelszavak feltöréséhez szükséges időt a rendelkezésre álló erőforrás függvényében.

A hallgatók mind a kurzus előtt, mind a kurzus után kitöltöttek egy kérdőívet, melyben a jelszóhasználati szokásikra kérdeztünk rá. Az adatokat összehasonlítva akartunk fényt deríteni arra, hogy az oktatás során használt módszer milyen változásokat gyakorol a hallgatók által használt jelszavak egyes tulajdonságaira?

2. ELEMZÉS

A kurzus előtt 82 gépészhallgató töltötte ki a kérdőívet, a kurzus után 38 fő. Az ő általuk megadott adatokat dolgoztuk fel.

A jelszóhasználati szokásaikról megadott adatokat biztonságos/kockázatos voltuk alapján pontoztuk, sorrendi skálán mértük. A változás- és eltérésvizsgálatot leíró statisztikákkal, a szignifikanciatesztelést nemparaméteres próbákkal végeztük.

2.1. A jelszótulajdonságok pontozása

Első körben az egyes jelszótulajdonságokhoz rendelt adatokat kellett sorrendi skálán pontoznunk, hogy a statisztikai elemzést elvégezhessük.

Minél különbözőbb jelszavakat használt valaki az egyes internetes szolgáltatásokhoz, biztonsági szintjét tekintve annál több pontot kapott (1. táblázat).

1. táblázat. Jelszavak különbözőségének pontértéke

Jelszókülönbözőség	*pont*
azonosak	1
van egy közös, állandó részük	2
teljesen különbözőek	3

Ha valaki állandó jelszavakat használ, akkor biztonságosság szempontjából alacsony pontszámot rendeltünk hozzá, miközben a jelszavakat gyakran változtatókhoz magasat (2. táblázat).

2. táblázat. Jelszóváltoztatás pontértéke

Jelszóváltoztatás	*pont*
nem cserélem	1
ha fölmerül a gyanú, hogy valaki megtudhatta	2
évente vagy ritkábban	3
3-6 havonta	4
1-2 havonta	5

Amennyiben valaki 8 karakternél rövidebb jelszavakat használ, alacsony pontot kapott erre a tulajdonságra a magasabb kockázata miatt (3. táblázat).

3. táblázat. Jelszavak hosszához rendelt pontértékek

Jelszavak karakterhossza	*pont*
<8 karakter	6
8-10 karakter között	9
11-13 karakter között	12
14-16 karakter között	15
>16 karakter	18

4. táblázat. Jelszavak komplexitásához rendelt pontértékek

Jelszavak komplexitása	*pont*
Csak kisbetűt használ	1
Nagy- és kisbetűt vegyesen használ	2
Nagybetűt, kisbetűt és számokat vegyesen használ	3
Nagybetűt, kisbetűt számokat és egyéb karaktert (pl. írásjel, #, &, @, stb.) használ	4

Az egyes internetes szolgáltatások egyre szigorúbb előírást tartatnak be a felhasználókkal a jelszó komplexitását tekintve, ezzel is biztonságosabbá téve az általuk nyújtott szolgáltatást, mégis találkozunk még napjainkban is olyan rendszerekkel, amelyeknél nem kötelező a számok, illetve speciális karakterek használata a jelszóképzésnél, melyre a legmagasabb pontot adtuk az elemzésünknél (4. táblázat).

5. táblázat. Jelszókezeléshez rendelt pontértékek

Jelszókezelés	*pont*
Mindet felírom	1
Van, amelyiket felírom	2
megjegyeztetem egy részét a böngészővel	3
Mindet megjegyzem	4
Jelszómenedzser programot használok	5

Amennyiben valaki minden jelszavát felírja, a megítélésünk szerint a legkevésbé biztonságos jelszókezelési módon jár el, ugyanis, ha azt valaki megtalálja, minden rendszerbe beléphet az illető nevében. A jelszómenedzser programok esetében csak egy jelszót kell megjegyeznünk a többi jelszóhoz való hozzáféréshez, így azok tetszőlegesen összetettek és hosszúak lehetnek, ezért ítéltük ennek a választásnak a legmagasabb pontszámot (5. táblázat).

A hallgatók által megadott értékeket ordinális skálán lévő pontszámra váltva elvégeztük az egyes jelszóváltozók esetében az átlag és szórás számítását (6. táblázat). Az adatok lényeges javulást nem mutatnak a kurzus végére, sőt a jelszavak különbözőségi értékének átlaga alacsonyabb is lett, de ahhoz, hogy a szignifikáns különbséget igazolni, vagy elvetni tudjuk mélyebb statisztikai elemzésre van szükség az egyes jelszótulajdonságoknál.

6. táblázat. A kurzus előtt és után megadott jelszótulajdonságokhoz rendelt pontok átlaga, szórása

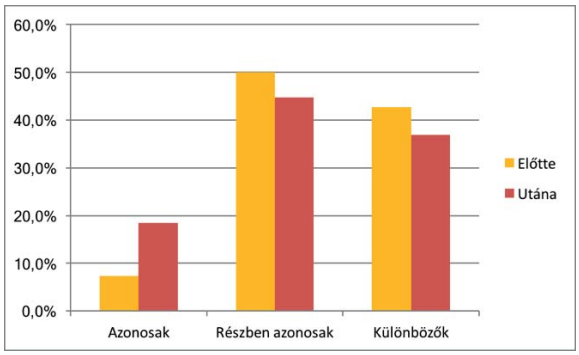
	Előtte		Utána	
	átlag	szórás	átlag	szórás
Jelszó-különbözőség	2,35	0,61	2,18	0,72
Jelszó-változtatás	2,44	1,04	2,58	1,08
Karakterszám	11,45	3,27	11,13	3,03
Karakterfajták	3,24	0,46	3,29	0,51
Jelszókezelés	3,15	1,01	3,71	1,01

2.2. Jelszótulajdonságok gyakoriságértékei a kurzus előtt-után

Az alábbiakban az egyes jelszótulajdonságok értékeinek gyakoriságát vizsgáljuk az információbiztonsági kurzus előtt és után.

A jelszavak megválasztása az egyik sarkalatos kérdése az adataink védelmének, ugyanis, ha azonos jelszavakat használunk a különböző rendszereknél, abban az esetben, ha az egyik rendszerből a támadó sikeresen megszerzi a titkosított jelszavunkat, a többi rendszerbe is beléphet vele a nevünkben.

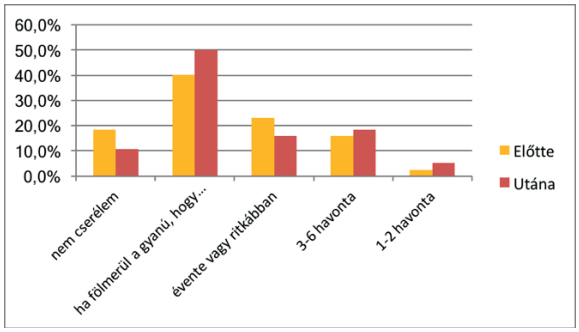
A hallgatók több, mint 42%-a teljesen különböző jelszavakat használt a kurzus előtt, 50%-uk pedig részben azonosat. Az információbiztonsági kurzus után meglepően a teljesen azonos jelszavakat használók tábora nőtt, a különböző jelszavakat használók tábora csökkent (1. ábra).



1. ábra. Jelszókülönbözőségek információbiztonsági kurzus előtt és után

Ezzel szemben a kurzus végére 18,3%-ról 10,5%-ra csökkent azok száma, akik egyáltalán nem cserélik a jelszavukat, ahogy a gyanú esetén váltóké is (40,2%-ről 50,0%-ra) (2. ábra).

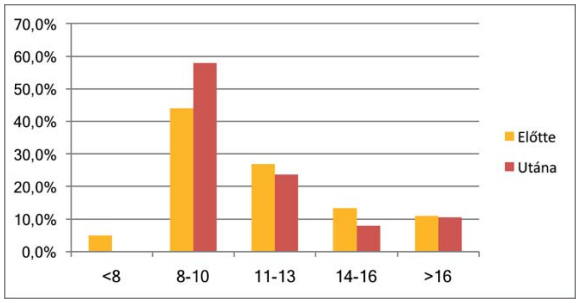
Nőtt azok száma, akik 3-6 havonta (15,9%-ról 18,4%-ra), illetve 1-2 havonta váltogatják őket (2,4%ról 5,3%-ra), mégis nem túl szembetűnő a pozitív irányú változás.



2. ábra. Jelszóváltoztatási szokások információbiztonsági kurzus előtt és után

Az információbiztonsági kurzus előtt még a hallgatók 4,9%-a használt 8 karakternél rövidebb jelszavakat, a kurzus végén már senki, ami előrelépést mutat.

A legnagyobb változás a 8-10 karakter hosszú jelszavakat használók létszámában történt, 43,9%-ról 57,9-ra emelkedett az arányuk. Az ennél hosszabb jelszavak esetében inkább kis mértékű arányvesztés figyelhető meg (3. ábra).

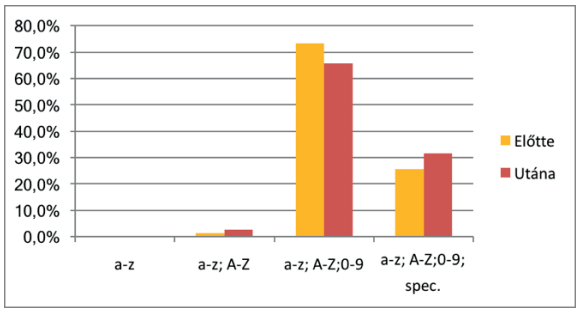


3. ábra. Jelszavak hossza információbiztonsági kurzus előtt és után

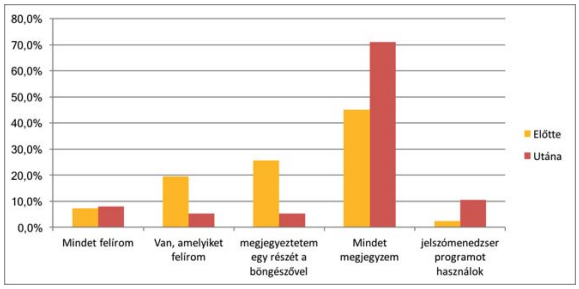
A jelszavak komplexiása a képzésük során felhasznált karakterek sokféleségében mutatkozik meg. A kurzus előtt és után sem használt senki csak kisbetűből álló jelszavakat, és elenyésző azok aránya is, akik csak kis- és nagybetűt használnak.

Korábban említettük, hogy a szolgáltatók egy jelentős része már összetett előírással rendelkezik a kötelezően használandó karakterfajtákra vonatkozóan, mégis találunk olyan rendszereket napjainkban is, melyeknél semmilyen előírás nincs a jelszavakra.

A betűket és számokat használók száma a kurzus végére alacsonyabb lett (73,2%-ről 65,8%-ra csökkent), a speciális karaktereket használók aránya pedig emelkedett (25,6%-ról 31,6%-ra), ami örvendetes változás (4. ábra).



4. ábra. Jelszavaknál használt karakterfajták információbiztonsági kurzus előtt és után



5. ábra. Jelszókezelés információbiztonsági kurzus előtt és után

A jelszókezelés tekintetében szintén pozitív irányú változást láthatunk (5. ábra).

Ugyan valamivel nőtt azok aránya az információbiztonsági kurzus végére, akik minden jelszavukat felírják (7,3%-ról 7,9%-ra), viszont csökkent azok száma, akik a jelszavaik egy részét felírják, vagy a böngészővel jegyeztetik meg, amelyből egy kártékony kód akár távolról is elérhetővé teszi a támadó számára azokat.

Lényegesen nőtt viszont azok aránya, akik minden jelszavukat megjegyzik (45,1%-ról 71,1%-ra), és többen használnak kifejezetten a jelszavak biztonságos tárolásához kifejlesztett jelszószéf programokat (2,4%-ról 10,5%-ra nőtt az arányuk).

2.3. Mann-Whitney-próba

A kurzus előtti és utáni jelszóhasználati szokások statisztikai eszközökkel történő összehasonlításához a Mann-Whitney-próbát alkalmaztuk a pontok sorrendi skálája miatt [6].

A Mann–Whitney-próba a két időszakra jellemző jelszótulajdonságok között nem mutatott szignifikáns eltérést. A jelszókezelésnél, a kurzus végén viszont szignifikáns javulás figyelhető meg (7. táblázat).

7. táblázat. Mann-Withney-próba eredménye az egyes jelszótulajdonságok esetében

Jelszótulajdonságok	*p*
Jelszó-különbözőség	0,252
Jelszócsere	0,585
Jelszóhossz	0,535
Karakter-fajták	0,590
Jelszó-kezelés	0,001

Ez azt jelenti, hogy a táblás, PowerPoint alapú előadás videofelvétellel támogatva, ami passzív befogadást jelent, nem volt elég erős hatással a hallgatók jelszóhasználati szokásaira. Ugyanazt az eredményt érjük el vele, mint a médiában az adott témában megjelenő cikkekkel.

3. ÖSSZEFOGLALÁS

Kutatásunkban arra kerestük a választ, milyen hatással van az információbiztonsági kurzuson használt tanítási módszer a hallgatók jelszókezelési szokásaira.

Egyre több helyen olvashatunk arról, hogy újabb és újabb internetes szolgáltató által kezelt személyes adatainkhoz jutottak hozzá a rendszer támadói megszerezve így az általunk használt jelszavak titkosított változatát. A visszafejtésének ideje nagyban függ attól, milyen hosszú és milyen összetett jelszót választottunk. A többi rendszerben tárolt adataink biztonsága pedig attól, mennyire eltérő jelszavakat használunk az egyes rendszereknél.

A kurzus elején és végén a hallgatók által megadott jelszótulajdonsági adatokat ordinális skála szerint pontoztuk annak érdekében, hogy statisztikai elemzést végezhessünk.

A Mann-Whitney-próba eredménye azt mutatta, hogy a hagyományos eszközöket felvonultató oktatás (tábla, PowerPoint prezentáció) megtámogatva esetenként videofelvételekkel, melyek szemléltetik a különböző jelszavak feltöréséhez szükséges időt, nem bizonyultak túl hatékonynak a hallgatók jelszóhasználati szokásainak biztonságosabbá tételéhez. Egyedül az jelszótárolásban lettek szignifikánsan tudatosabbak a hallgatók és használnak biztonságosabb megoldást, mely csak részben védi őket jobban egy célzott támadás esetén a többi tulajdonság nem megfelelő mértékű változása esetén.

A tábla, PowerPoint prezentáció és videofelvétel a hallgatók részéről passzív befogadást jelent. Érdemes kipróbálni a hallgatók részéről aktivitást igénylő módszerek használatát az információbiztonsági képzés során, vizsgálva annak hatását az információbiztonsági attitűdjükre.

4. IRODALOM

[1] Larson S..: Every single Yahoo account was hacked - 3 billion in all, 2017. október 4. http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

[2] Pleasant R. 200 million emails compromised: Is yours on the list? 2016. május 4. https://siliconangle.com/blog/2016/05/04/200-million-emails-compromised-is-yours-on-the-list/

[3] Pauli D.: Just give up: 123456 is *still* the world's most popular password, 2017. január 16. https://www.theregister.co.uk/2017/01/16/123456_is_still_the_worlds_most_popular_password

[4] Keszthelyi A.: About passwords, Acta Polytechnica Hungarica, Volume 10., 2008, pp: 99-118., 2013, ISSN: 1785-8860.

[5] Sixx: Bárki feltörheti a BKK elektromos jegyvásárló rendszerét, 2017. július 15. http://index.hu/tech/2017/07/15/barki_feltorheti_a_bkk_elektromos_jegyvasarlo_rendszeret/

[6] T.P. Hettmansperger, J.W. McKean, :Robust nonparametric statistical methods. Kendall's Library of Statistics. 5 (First ed., rather than Taylor and Francis (2010) second ed.). London; New York: Edward Arnold; John Wiley and Sons, Inc. pp. xiv+467. ISBN 0-340-54937-8., 1998