sciendo

Műszaki Tudományos Közlemények vol. 11. (2019) 149–152.
https://doi.org/10.33895/mtk-2019.11.33
https://eda.eme.ro/handle/10598/31230
Angol nyelven: https://doi.org/10.33894/mtk-2019.11.33

EME MTSZ MTK

A ZSAROLÓVÍRUS-TÁMADÁSSAL SZEMBENI VÉDEKEZÉS A BIZTONSÁGTUDATOSSÁG NÖVELÉSÉVEL

PREVENTION OF RANSOMWARE ATTACK BY INCREASING SECURITY AWARENESS

Nyikes Zoltán[1], Szűcs Endre[2]

Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Gépészeti és Biztonságtudományi Intézet, Budapest, Magyarország

[1] *nyikes.zoltan@phd.uni-obuda.hu*

[2] *szucs.endre@bgk.uni-obuda.hu*

Abstract

There is a strong relationship between the user's lack of anti-virus software use and the lack of data backup in case of the user groups meaning that users don't use these two applications on average in the same proportion. In the case of users who lack knowledge in informatics virus attacks numbers are high, a large number of them don't use anti-virus software and the data backup. For the digital systems, the lower level rated users are at risks based on the numbers of the occurred virus attacks. For all user groups is necessary the continuous and repeated safety awareness training Keywords to reach and retain a high-level safety..

Keywords*: ransomware, security awareness, cyber security, attack, prevention.*

Összefoglalás

A vírusvédelem és az adatmentés együttes hiánya a felhasználói csoportok esetében erős kapcsolatot mutat, ami azt jelenti, hogy a felhasználók a két alkalmazást közel azonos arányban nem használják. Azoknál a felhasználóknál, akik nem rendelkeznek informatikai ismeretekkel, mind a vírustámadások aránya, mind a vírusvédelem hiánya és az adatmentés hiánya magas. Az elszenvedett vírustámadások alapján az alacsonyabb értékelésű felhasználók kockázatot jelentenek a digitális rendszerekre. A felhasználók mindegyik csoportja számára szükséges a folyamatos és ismétlődő jellegű biztonságtudatossági képzés a magasfokú biztonság elérése, megtartása érdekében.

Kulcsszavak*: zsarolóvírus, biztonságtudatosság, kiberbiztonság, támadás, védekezés.*

1. Bevetetés

A biztonságtudatosság és a digitális kompe-tencia kapcsolatának kutatása céljából egy kérdőívet állítottunk össze. A kérdőívet össze-sen 1274-en töltötték ki, amiből az online kér-dőívet 1195-en, a papíralapút 79-en. A kérdőív hat kérdéscsaládból tevődött össze. *Általános kérdések; Felhasználói szokások és alkalmazott eszközök; A digitális kompetenciára és a biz-tonságtudatosságra vonatkozó kérdések; Inter-netes zaklatás (Cyberbullying); Rosszindulatú kódok elleni védelem; Adatvagyon védelme.*

A kérdőíves felmérés kiértékelése során bi-zonyítást nyert többek között az, hogy mely felhasználói csoport is van kitéve a legjobban a zsarolóvírus-támadásoknak. A felmérés alapján az is megállapítást nyert, hogy ezeket a támadásokat miként lehet a leghatékonyabb módon megelőzni. Ez pedig nem más, mint a felhasználók folyamatos és megfelelő biztonsági oktatása és digitális kompetencia fejlesztése.

2. A digitális kompetencia értékelési szempontrendszere

A kutatás során a különböző mérési eredménA kutatás során a különböző mérési ered-mények értékelésére korrelációs vizsgálatot alkalmaztunk, ahol a korrelációs együttható abszolút értéke a mértékadó, amely alapján vizsgálati szempontok szerinti korrelációkat találtam. A felhasz-

nálók iskolai végzettséget tekintettük mérvadónak, és a hozzá válaszul adott önértékelési szintet kritikával kezeltem. A definiált öt csoporthoz következő osztályzatokat adtuk a felhasználóknak: *magabiztos (5), védendő (2), szerény (4), veszélyes (3), belépő (1).* A kérdőívek kiértékelése során alkalmaztuk a *Pearson korrelációs együttható* értékének meghatározását (*r*), valamint ebből az értékből a determinációs együtthatót (*d = r2 •100* (%)) is meghatároztuk, mely a lineáris típusú korrelációs kapcsolat mérőszáma. A korrelációs együttható abszolút értéke, ha *|r|= 0 nincs kapcsolat, 0<|r|<0,3 gyenge kapcsolat, 0,3<|r|<0,7 közepes kapcsolat, 0,7<|r|<1 erős kapcsolat, |r|=1 determinisztikus kapcsolat*. Lineáris regresszió esetén, ami a változók közötti lineáris kapcsolat erősségére utal, a kapcsolat erősségét a determinációs együttható %-ban határozza meg [1].

2.1. A „Veszélyes” felhasználó

Ebbe a kategóriába azokat az amatőröket soroltuk, akik a potenciális veszélyforrást jelenthetik. Általában ebből a kategóriából kerülnek ki a cégek „shadow IT” azaz a „árnyék informatikus” szakemberei.

2.2. A „Védendő” felhasználó

Ebbe a kategóriába azokat a kezdő felhasználókat soroltuk, akik szintén veszélyforrást jelentenek, viszont mivel feltehetően tisztában vannak a saját képességeikkel (a végzettség és a saját kompetenciaszint megítélése közel azonos), ezért óvatosabban használják az internetet.

2.3. A „Szerény” felhasználó

Ebbe a kategóriába azokat a félprofi felhasználókat soroltuk, akik rendelkeznek valamilyen informatikai végzettséggel/tanfolyammal, viszont a képességeiket alacsony szintűnek ítélik meg (az iskolai végzettség és a saját önértékelés azonos szintet mutat).

2.4. A „Magabiztos” felhasználó

Ebbe a kategóriába azokat a profi felhasználókat soroltuk, akik rendelkeznek informatikai végzettséggel/tanfolyammal és digitálisan kompetensnek, valamint biztonságtudatosnak vallják magukat.

3. A felhasználók vírusvédelemi szokásainak vizsgálata

Az informatikai eszközeink egyik legfontosabb védelmi megoldása a vírusvédelem. [1, 2] Ennek alkalmazása minden informatikai eszközön kiemelten szükséges. Tévhit, hogy bizonyos operációs rendszerekhez nincs szükség vírusvédelemre, mondván, arra az operációs rendszerre nem készítenek rosszindulatú szoftvert. [3]

3.1. A felhasználók tevékenységének vizsgálata vírustámadás esetén

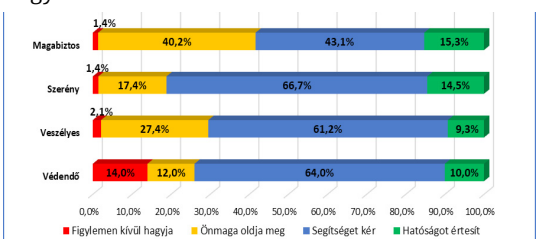
Az alábbiakban a felhasználói csoportok tevékenységét vizsgáltuk egy esetleges vírustámadás esetén (1. ábra). A felhasználói csoportoknak a felmérés „Esetleges vírustámadás, és/vagy egyéb rosszindulatú támadás esetén tisztában van azzal, hogy mi a teendő?” kérdésre adott válaszait elemeztük. A felmérés alapján megállapítható, hogy a felhasználók a biztonságtudatosságuknak és a digitális kom-petenciájuknak, valamint az informatikai ismereteiknek megfelelően tevékenykednének esetleges vírustámadás esetén. Míg az önmaga által végrehajtott kármentés a „Magabiztos” csoport esetében a tudásszintjük miatt érthetően magas, addig ugyanez aggasztó és ezáltal kockázatos a „Veszélyes” csoport esetében, akik nem rendelkeznek semmilyen informatikai végzettséggel.

Pozitívan értékelendő, hogy a felhasználók nagy számban valamilyen segítséget kérnének szakemberektől, azonban negatív viselkedésnek tekinthető, hogy a hatóságokat az esetleges víruseszkalálódás megelőzése érdekében csak kevés számban értesítenék. Negatívan értékelendő, hogy a „Védendő” csoport 14%-a nem tenne semmit vírustámadás esetén.

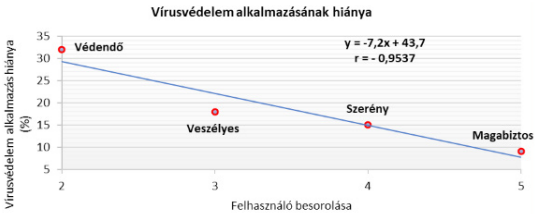
3.2. Kapcsolat a felhasználó besorolása és a vírusvédelem között

A korrelációs együttható abszolút értéke jó egyezést mutat a lineárishoz (*|r|=0,9537*), mivel a korreláció előjele negatív, ebből látszik, hogy a felhasználó egyre magasabb besorolási értéke szerint egyre alacsonyabb a vírusvédelem hiánya, az ebből kiszámított determinációs együttható pedig 90,95%, mely azt mutatja, hogy az értékek jól illeszkednek a lineáris függvényre, tehát közöttük erős kapcsolat van (2. ábra) .

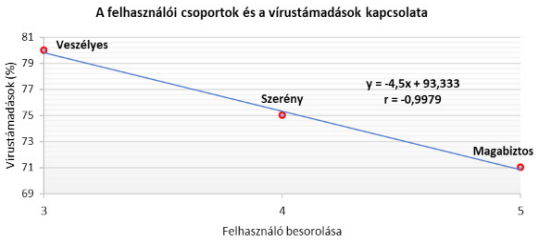
A kutatási eredmények alapján megállapítható, hogy a vírusvédelem alkalmazása és a felhasználó besorolási szintje közötti kapcsolat közel lineáris, tehát a magasabb képzettségű felhasználók nagyobb számban alkalmaznak vírusvédelmet.



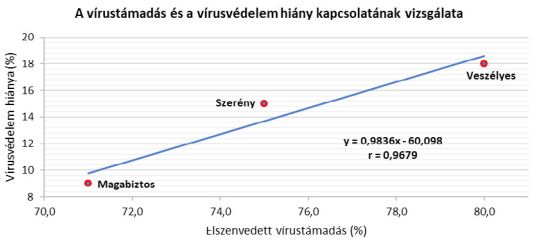
1. ábra. *A felhasználók tevékenységének vizsgálata vírustámadás esetén* [4]



2. ábra. *A felhasználó besorolása és a vírusvédelem alkalmazásának hiánya közötti korreláció* [4]



3. ábra. *Korreláció a felhasználó besorolása és a vírustámadások között* [4]



4. ábra. *A vírustámadás és a vírusvédelem hiány kapcsolatának korrelációs vizsgálata* [4]

3.3. Kapcsolat a felhasználó besorolása és a vírustámadások között

Az alábbi korreláció rávilágít arra, hogy a felhasználó a digitális rendszer szempontjából kockázatot jelent, mert az elszenvedett vírustámadások szerint a kockázati szint fordítottan arányos a felhasználó besorolási szintjével (**3. ábra**). Látható, hogy csak három csoport adatai lettek értékelve. A "Védendő" csoport eredménye ki lett zárva, mivel nem egyértelmű, hogy a felhasználók kompetenciájukból adódóan képesek voltak minden vírustámadást felismerni, ezért a válaszok eredményei ebben a korrelációban nem használhatók.

A pontok lineárisra illeszkedése igen jó közelítéssel valósul meg, a korrelációs együttható $|r| = 0{,}9979$, mely fordított arányt mutat az elszenvedett vírustámadások száma és a besorolási szint között, a determinációs együttható pedig $d = 99{,}58\%$, ami a kapcsolat erősségét mutatja. A felhasználó besorolása és a vírustámadások közötti kapcsolat **erős**, erősebb, mint a felhasználó besorolása és a vírusvédelem alkalmazás hiánya közötti.

3.4. Kapcsolat a vírustámadások és a vírusvédelmi alkalmazások hiánya között

Nem derül ki a „Védendő" felhasználói csoport kutatási eredményeiből, hogy hány felhasználót ért „lappangó" vírustámadás, melyről a felhasználó nem is tud, hiszen nem alkalmaz megfelelő vírusvédelmet, csak lassul a számítógépe, vagy csak később derül ki, hogy vírusfertőzés érte. Ezért ahogyan indokoltuk, ezt a csoportot ebben az esetben is kizártuk a korrelációs vizsgálatból. Látszik (**4. ábra**), hogy a vírusvédelem hiánya és a vírustámadások száma között erős korreláció van, $|r| = 0{,}9679$. **Megállapítható az eredmények alapján, hogy amennyiben a felhasználó nem használ vírusvédelmet, abban az esetben vírustámadás éri.** A vírusvédelem hiánya fordítottan arányos a felhasználónak a szempont-rendszer szerinti szintjével, valamint a vírusvédelem hiánya és a vírustámadások előfordulása között lineáris kapcsolat mutatható ki.

4. A felhasználó besorolása és az biztonsági adatmentés hiányának vizsgálata

Az eredményekből látható, hogy a „Védendő" csoportba tartozók közül vannak a legtöbben (28%), akik nem készítenek biztonsági adatmentést. Valószínűsíthető, hogy ez a csoport az, aki nem tudja, hogy egyrészt miért is fontos a biztonsági adatmentés, másrészt nem áll rendelkezésére olyan technikai megoldás, aminek segítségével elkészíthetné az adatai mentését. Kimondható, hogy a „Magabiztos" csoport azon tagjai, akik nem készítenek biztonsági adatmentést, felelőtlenül viselkednek. Míg a „Veszélyes" csoport azon tagjai, akik nem készítenek biztonsági adatmentést, az informatikai ismeretük hiányáról tesznek tanúbizonyságot. A „Szerény" csoportba tartozók 17,5%-a nem készít biztonsági adatmentést. Valószínűsíthető, ahogyan korábban már megállapítást nyert, hogy ennek a csoportnak vagy nincs vagy bevallottan alacsony a biztonságtudatossága, annak ellenére, hogy rendelkeznek valamilyen szintű képzésben szerzett informatikai ismerettel.

A felmérés alapján megállapítható, hogy a felhasználók körében szükséges a rendszeres biztonságtudatossági képzés/oktatás, mivel a biztonsági adatmentésre a végzettségnek erős hatása van, ezt a 81,54%-os értékű determinációs együttható is alátámasztja (**5. ábra**). A biztonsági adatmentés hiánya és a felhasználó besorolási szintje között fordított arányosság van, a magasabb szintű felhasználók esetében alacsony a biztonsági mentés hiánya. A besorolási szint és az adatmentés hiá-

nya lineárissal jól közelíthető, amit a korrelációs együttható abszolút értéke (|r|=0,9203) is mutat. A negatív előjel arra utal, hogy minél jobban képzett az adott felhasználó, annál gyakoribb a fontos adatainak biztonsági mentése.

5. A felhasználók vírusvédelmi és adatmentési szokásainak vizsgálata

Mivel az elmúlt évek legnagyobb biztonsági kihívása a zsarolóvírusok támadása elleni védekezés, ezért elsődleges a felhasználók ilyen irányú felvilágosítása [5, 6].

5.1. A felhasználók vírusvédelmi és adatmentési szokásainak aránya

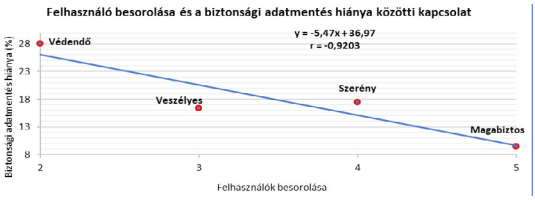
A vizsgálat alapján látható (6. ábra), hogy a vírusvédelem hiánya és a biztonsági adatmentés hiánya milyen szorosan összefüggően, szinte közel azonos arányban jelenik meg az adott felhasználók esetében. Továbbá az is szembetűnő, hogy a felhasználói csoportoknak az felállított rangsor szerint növekszik (egy kivételével) mindkét szokásnak az aránya. Látható, hogy a „Magabiztos” 9,16-9,39% aránypárral, a „Szerény” 15-17,5% aránypárral, a „Veszélyes” 17,78-16,44% aránypárral és a „Védendő”, kimagaslóan a többi közül, 32-28% aránypárral szerepel.

5.2. A felhasználók vírusvédelmi és adatmentési szokásainak relációja

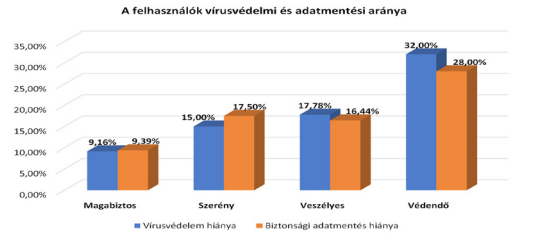
A vírusvédelem hiánya és az adatmentés hiánya a felhasználói csoportok esetében erős kapcsolatot mutat (|r|=0,9545), a determinációs együttható értéke 94,91%, ami azt jelenti, hogy a felhasználók a két biztonsági megoldást közel azonos arányban nem használják, közöttük erős kapcsolat van (7. ábra). A felhasználói csoportok ezen alkalmazásokat pedig besorolási szintjüknek megfelelően a diagramon bemutatott erős lineáris korreláció szerint nem alkalmazzák.

6. Összegzés

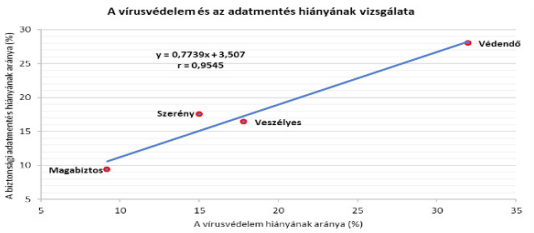
A fenti vizsgálat alapján látható, hogy azon felhasználók körében, akik rendelkeznek oktatás útján megszerzett informatikai ismeretekkel, magasabb a biztonsági adatmentés és a vírusvédelem alkalmazása. Akik nem tanultak informatikát, azok körében gyakrabban előfordul, hogy se vírusvédelmet, se biztonsági adatmentést nem alkalmaznak. Megállapítom, hogy egy esetleges zsarolóvírus-támadást azok szenvedhetnek el nagyobb arányban, akik nem rendelkeznek tanult informatikai ismeretekkel. Ennek a kockázati tényezőnek a korai felismerése, valamint ennek prevenciója jelentősen javíthatja akár az egyén, akár egy vállalat adatvagyonának a védelmét.



5. ábra. *Korreláció a felhasználó besorolása és a biztonsági adatmentés között* [4]



6. ábra. *A felhasználók vírusvédelmi és adatmentési aránya* [4]



7. ábra. *A vírusvédelem és az adatmentés hiányának vizsgálata* [4]

Szakirodalmi hivatkozások

[1] Rajnai Z., Mógor T.né: *Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása.* Bolyai Szemle 4/2. (2014) 43–59.

[2] Simon L., Magyar S.: *A terrorizmus és indirekt hatása a kiberterében.* Nemzetbiztonsági Szemle 3. (2017), 89–101.

[3] Michelberger P., Keszthelyi A.: *Információbiztonság alapjai – mesterfokon.* Informatika a felsőoktatásban, Debrecen, 2011, 579-583.

[4] Nyikes Z.: *Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel.* doktori értekezés, Óbudai Egyetem, Budapest, 2019. Torres-Gastelú C. A., Kiss G.: *Comparison of the ICT Literacy Level of the Mexican and Hungarian Students in the Higher Education*, Procedia - Social and Behavioral Sciences, 176. (2015) 824–833.

[5] Torres-Gastelú C. A., Kiss G.: *Comparison of the ICT Literacy Level of the Mexican and Hungarian Students in the Higher Education*. Procedia - Social and Behavioral Sciences, 176. (2015) 824–833. https://doi.org/10.1016/j.sbspro.2015.01.546

[6] Kerti A.: *Az információbiztonsági kockázatkezelés oktatásának buktatói.* Kommunikáció, Budapest, 2013. 53–60.