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

PREVENTION OF RANSOMWARE ATTACKS BY INCREASING SECURITY AWARENESS

Zoltán NYIKES,[1] Endre SZŰCS[2]

Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Institute of Mechanical Engineering and Security Science, Budapest, Hungary

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

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

Abstract

There is a strong relationship between groups of users who don't use anti-virus and those who don't backup their data, meaning that a similar proportion of users don't use either of these two means of protection. In case of users who lack knowledge in informatics there is an increase in the number of virus attacks; these users are more likely to not use anti-virus and neglect to back up their data. For digital systems, users who are – based on our classification – in a lower rank, represent increased risk based on the number of the occurred virus attacks. For every user group there is a need for continuous and repeated safety awareness training to reach and retain a high safety level/

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

1. Introduction

We compiled a questionnaire in order to explore the relationship between safety awareness and digital competence. This questionnaire was answered by a total of 1274 people, 1195 of whom completed the online version, the remaining 79 the paper-based version. It contained six groups of questions. General questions; User habits and applied tools; Questions regarding digital competence and safety awareness; Cyberbullying; Malware protection; Dataset protection.

During the analysis of the questionnaire we obtained clear evidence regarding the user group that is most exposed to ransomware attacks. Based on the answers we could establish the most effective ways to prevent these attacks. And the best way to achieve that is by continuously and adequately informing the users about safety and by developing their digital competence.

2. Criteria for evaluating digital competence

During the research, in order to evaluate the different results of measurements, we used a correlation analysis where the absolute value of the correlation coefficient was decisive. Based on this, and according to the research criteria, we found the correlation. We regarded the users' level of completed education to be the decisive factor and the self-evaluating answers regarding that were considered with critique. To the defined five groups, we assigned the following classification: confident (5) protect (2), modest (4), dangerous (3), entry level (1). During the evaluation of the questionnaires we used the definition of the Pearson coefficient value (r), from this we also determined the determination coefficient (d = r2*100(%)) which is a measure of the linear type correlation relationship. The absolute value of the correlation coefficient if $|r|=0$ no relationship $0<|r|<0.3$ week relationship $0,3<|r|<0.7$ moderate relationship $0.7<|r|<1$ strong relationship $|r|=1$ deterministic relationship. In case the of linear regression, that is, a measure of the strength of the linear relationship between the variables, the strength of the relationship is given by the determination coefficient in % [1 During the research, in order to evaluate the different results of measurements we used a correlation analysis where the absolute value of the correlation coefficient was decisive, based on this and according to the research criteria we found a correlation. We regarded the users' level of com-

pleted education to be the decisive factor and the self-evaluating answers regarding that were considered with critique. To the defined five groups we assigned the following classification: confident (5) to be protected (2), modest (4), dangerous (3), entry level (1). During the evaluation of the questionnaire's we used the definition of the Pearson coefficient value (r), from this we which we also determined the determination coefficient (d = r2*100(%)) which is a measure of the linear type correlation relationship. The absolute value of the correlation coefficient if $|r|=0$ no relationship $0<|r|<0.3$ week relationship $0,3<|r|<0.7$ moderate relationship $0.7<|r|<1$ strong relationship $|r|=1$ deterministic relationship. In the case of linear regression, that is a measure of the strength of the linear relationship between the variables, the strength of the relationship is determined by the determination coefficient in % [1].

2.1. The „Dangerous" user

To this category we assigned the amateurs who could be a potential source of danger. As a general rule this is the category that gives the so-called „shadow IT"-s of companies.

2.2. The „To be protected" user

The users who belong to this category are those amateurs that also represent danger, but because they are aware of their own level of competence (schooling and autoevaluation are almost identical) they are more careful when using the internet.

2.3. The „Modest" user

We assigned to this category the semiprofessional users who have some level of education in informatics through school or a specialty course but they judge their own skills as modest (schooling level and auto-evaluation are identical.

2.4. The „Confident" user

These are the professionals who have some degree or certificate in informatics and see themselves as digitally competent and aware of safety issues.

3. Analysis of the anti-virus protection habits of users

One of the most important protection tools in our IT devices is anti-virus protection. [1, 2] The use of such protection is a must on every IT device. It's a misbelief that certain operating systems don't need anti-virus protection because nobody creates malware for that particular system. [3]

3.1. Analysis of the users' actions in case of a virus attack

We analysed the activities of the user groups in cases of an actual virus attack (Figure 1.). We analysed their answers to the question „Are you aware of the steps that you need to take in the case of a virus attack?" The answers made it clear that the user's actions in such cases are determined by their safety awareness, their digital competence and their level of knowledge in informatics. While the damage control executed by the „Confident" group is effective according to their level of knowledge, the same attitude results in high risk and a reason for concern when performed by the informatically uneducated „Dangerous" group.

It is commendable that many of the users would seek professional help but it remains a concern that only a few of them would alert authorities in the case of an escalation of virus attacks. The fact that 14% of the „To be protected" group would do nothing in the case of a virus attack is a negative result.

3.2. Relationship between the users' group assignment and anti-virus protection

The absolute value of the correlation coefficient approaches linearity ($|r| = 0.9537$), since the value of the correlation is a negative number, we can see that the higher the user's level of group assignment, the lower the lack of anti-virus protection, the determination coefficient calculated from this is 90.95% which shows a very close fitting to a linear function so there is a strong relationship between them (Figure 2.) .

According to the research results the relationship between the use of anti-virus protection and the user's group assignment is almost linear, that is to say that users with higher education are more likely to use such protection.

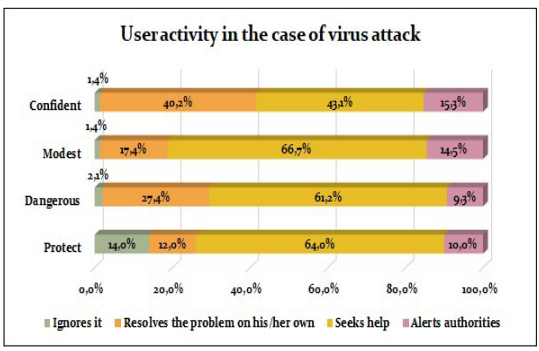

Figure 1. *Analysis of the users' activities in case of virus attack* [4]

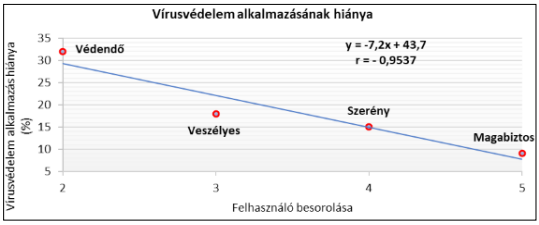

Figure 2. *The correlation between the user's group assign-ment and lack of anti-virus protection* [4]

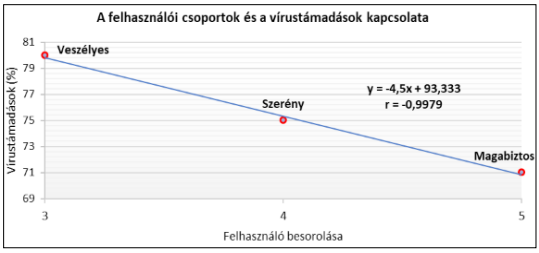

Figure 3. *Correlation between the user's group assignment and virus attacks* [4]

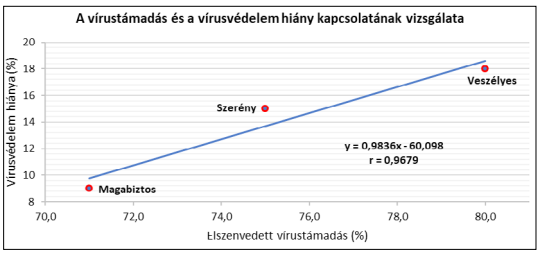

Figure 4. *Correlation analysis of the relationship between the lack of anti-virus protection and virus attacks* [4]

3.3. Relationship between the user's group assignment and virus attacks

The correlation showed below makes it clear that the user represents a risk for the digital system, because the level of risk according to the suffered virus attacks is inversely proportional to the user's assigned level (**Figure 3.**). As it can be seen, data from only 3 groups was considered, the group "To be protected" was excluded because it was not clear whether the users belonging to this group were able or not – due to their level of competence – to recognize every virus attack, therefore their answers regarding this correlation could not be used. The linear fitting of the dots shows a good approximation, the correlation coefficient is $|r| = 0.9979$, which shows an inverse proportion between the assigned group level and the number of virus attacks, the determination coefficient is d = 99.58% which shows a strong relationship. This relationship qualifies as strong, stronger than the one between the user's group assignment level and the lack of anti-virus protection.

3.4. Relationship between virus attacks and lack of anti-virus protection

From the part of the research that concerned the "To be protected" group, it is not clear how many of them were victims of latent attacks of which they weren't aware, since they don't use anti-virus software, the only thing that happens is that their computer slows down and only later it becomes clear that it has been infected by a virus. Therefore, as we have already indicated, in this case also this particular group was excluded from the correlation analysis. It is clear from **Figure 4.** that there is a strong relationship between lack of anti-virus software and virus attacks, $|r| = 0.9679$. It can be stated based on the results that if the user does not use anti-virus software, virus attacks will occur. Lack of anti-virus software is inversely proportional with the user's level according to our system of criteria, also, there is a linear relationship between lack of anti-virus software and the frequency of virus attacks.

4. Analysis of the user's assigned level and the lack of security data backup

It is clear from the results that the "To be protected" group has the greatest proportion of users who never perform a security data backup (28%). It is likely that members of this group don't understand why such backups are important on one hand, on the other hand it is also likely that they lack the technical means in order to perform security data backups. We must also stress the fact that members of the "Confident" group who don't perform backups show irresponsible behavior. At the same time, members of the "Dangerous" group show their lack of knowledge when they don't perform security backups. 17.5% of members of the "Modest" group don't perform security data backups. It can be inferred as previously stated, that members of this group either don't have a safety awareness, or it is admittedly low in spite of the fact that they do possess some level of training in informatics. According to the results of the survey it can be stated that it is necessary to provide users with a systematic training in safety awareness, since schooling level has a strong effect on security data backups, this is supported by the value of the determination coefficient, 81.54% (**Figure 5.**). There is an inverse proportion between lack of data backup and the user's

assigned level, users with a higher assigned level show low lack of data backup. Assigned level and lack of data backup can be approximated with linear which is also shown by the absolute value of the correlation coefficient (|r| = 0.9203). The negative number refers to the fact that the more educated a user is, the more often he or she will perform a security backup of any important data.

5. Analysis of the users' habit of virus protection and data backup

Since the greatest safety challenge of the previous years was the ransomware attacks, informing the users about this kind of attack is of primary importance [5, 6].

5.1. The proportion of users who lack anti-virus protection and those who don't perform data backup

Based on this research (Figure 6.), it is clear that there is a strong correlation between lack of anti-virus software and lack of security data backup, the proportion of these two is almost identical within the given user group. It is also obvious that in the user groups the proportion of both these habits increases according to their established rank (with one exception). Clearly the pair of proportions for the "Confident" is 9.16 – 9.39%, that of the "Modest" is 15 – 17.5%, the "Dangerous" 17,78 – 16.44% while that of the "To be protected" is exceptionally high, 32 – 28%.

5.2. Relationship between the users' virus protection and data backup habits

There is a strong relationship between lack of virus protection and that of data backup within the groups (|r| = 0.9545), the value of the determination coefficient is 94.91% which means that the users don't use the two security solutions in approximately the same proportion, there is a strong relationship between them (Figure 7.). Also, the users don't use these in a strong linear correlation according to their assigned level.

6. Conclusion

From this analysis it is clear that among those users who possess a higher level of knowledge in informatics obtained through education, there is a higher use of safety backup and of virus protection. Among those who didn't learn informatics the proportion of those who use neither safety backup nor anti-virus software is higher. We can affirm that the likelihood of a ransomware attack is higher among those who don't possess learned knowledge in informatics. The early recognition and prevention of this risk factor can significantly

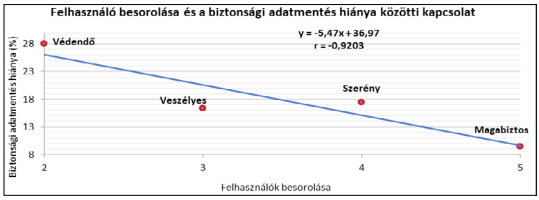

Figure 5. *Correlation between user assignment and safety data backup* [4]

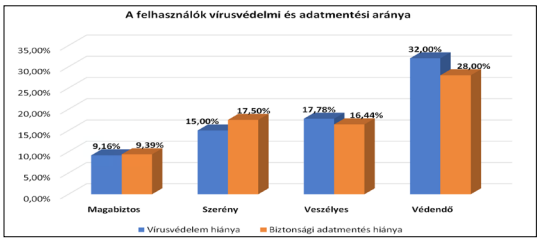

Figure 6. *The proportion of virus protection and data back-up of users* [4]

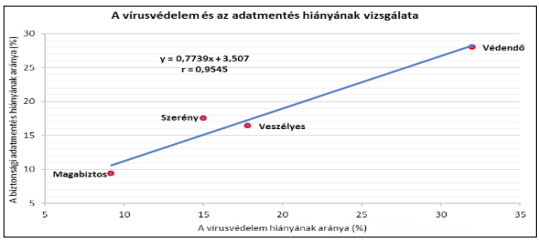

Figure 7. *Analysis of the lack of virus protection and lack of data backup* [4]

improve data protection for both individuals and companies.

References

[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.