МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2021
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2021
Proceedings of the Fiftieth Spring Conference
of the Union of Bulgarian Mathematicians
2021

INFORMATION SECURITY AWARENESS LEVEL EVALUATION AMONG BULGARIAN PUBLIC AND LOCAL ADMINISTRATION EMPLOYEES

Veselina Jecheva, Evgeniya Nikolova

A number of studies show that the human factor is among the weakest elements in today's interconnected network environment. The development of a methodology for raising awareness of vulnerabilities, threats and solutions in the field of information security through training and thus increasing the overall level of security of users and organizations is the main goal of the project "Immersive Learning in Information Security" (MISSILE). The tasks of the project include defining the user needs and requirements in the field of information security training and developing a concept for information security training, covering the main problems related to the most important modern challenges in the field. In order to assess the level of knowledge and skills of the target group on the technical aspects, legal provisions and economic aspects of information security, their needs and expectations from an electronic course on information security, a survey was conducted. This report presents the main results of this survey.

1. Introduction. Information security is among the most important challenges in the contemporary highly connected world. Both organizations and people in their ordinary lives are becoming more and more dependent on their information systems and online services – purchases, education and training, business, communication, collaborative work, all requiring personal or sensitive data. Many surveys ([1], [4]) reveal that a considerable number of end-users are unaware of their exposure to security risks and many of the organizations surveyed currently do not have an awareness program or have an *immature* program that is solely focused on compliance. The reason they give is that after the EU general update to data protection regulation (GDPR) [2] came into place in May 2018, organisations are more likely to report attacks. On the other hand, these results also demonstrate that the huge amounts of data collected by companies or states, are not immune to intruders. These threats, most of them rapidly evolving and coming from any location, are highly critical for local and state authorities, who work with private and sensitive data [3]. The Internet and other aspects of the information infrastructure are inherently transnational. The number and sophistication of transnational attacks on computers and the information infrastructure are increasing at alarming rates. Finding effective solutions to counteract implies collaboration with international teams.

So it is critical to raise security awareness among the wide audience and especially among the employees from local and state authorities of the present vulnerabilities and

threats, the potential security breaches so as to prevent many successful intrusions. The project MISSILE[1] is focused on a training which includes technical aspects, legal regulations and economic aspects of information security in fully compliance to the GDPR (Regulation (EU) 2016/679) initiative to strengthen and unify data protection within and outside the EU.

The main purpose of the project is to develop a methodology for raising awareness of the information security vulnerabilities, threats and security solutions through learning and training. This purpose can be achieved by the following objectives: to define user needs and requirements in the field of the information security training; to minimize the gap between user needs and security training solutions (the project team aims at understanding the fragmentation of demand by studying training needs of users and organizations in relation to state-ofthe-art platform offerings); to develop a concept for information security training, covering the major issues regarding the contemporary information security; to develop a platform, which implements the created methodology in a feasible and reliable way; to create learning materials, related to information security issues, social engineering, users' beliefs and understandings about sensitive data and information security, as well as selecting and applying properly defined security policies, mechanisms and countermeasures.

The next sections of the paper present the main results of a study conducted in 2020 as a part of an international initiative supported by the European Commission in the framework of the project MISSILE, aiming to assess the degree of awareness of respondents in the area of information security.

2. Scope of the survey. The study covers five European countries: Bulgaria, Turkey, Cyprus, Romania and Austria. The research methodology is based on a survey method. The report presents some results of the survey, conducted in Bulgaria. The online questionnaire, provided to the respondents from Bulgaria into Bulgarian language, had been designed to cover the following aspects of the sample: general personal data; establishing the common perceptions and attitudes of the respondents on issues about using the opportunities of ICT in the training process; determining preferences and needs in developing an e-training course through a virtual learning environment; assessment of the respondents' degree of awareness in the area of information security. The questionnaire contained 20 multiple choice questions. The study was conducted during the period March 2020–May 2020 with the responding rate being approximately 78.5%.

3. Respondents' Profiles Outline. The main characteristics of the target group are represented in the next figures. The analysis shows that the women respondents are 63,6 %, while male surveyed are 36,4% in total and they are almost equally distributed among the proposed age groups (Fig. 1).

Figure 2 indicates that the majority of the individuals have a master's degree (69,7%), 24,2% – a bachelor's degree and the remain 6,1% respondents have secondary education.

The highest percentage indicates that most of the participants are employed in municipal administration (42.4%). The next two large groups of people participating in this survey are working in state administration and financial institutions (Fig. 3). The other respondents were distributed as follows: 6.1% working in educational institutions

[1]This research is supported under project 2019-1-BG01-KA204-062331 – Immersive Learning in Information Security (MISSILE), Erasmus+ Programme.

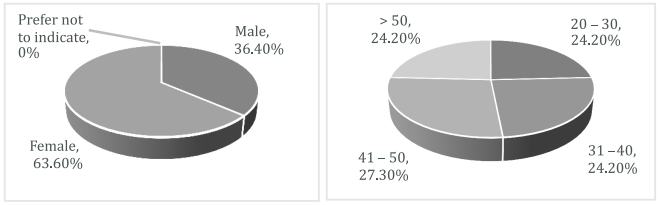

Fig. 1. *Gender* (a) and *age* (b) characteristics of the sample

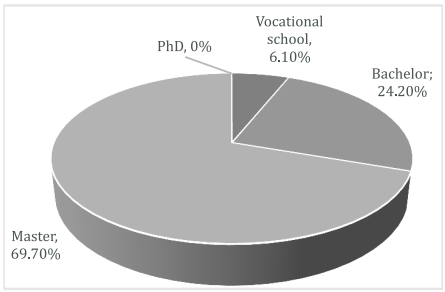

Fig. 2. Education level of respondents

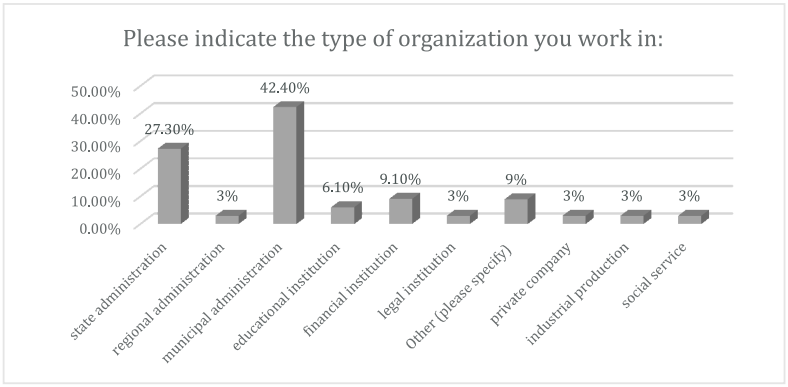

Fig. 3. Distribution of type of organization

and 3% working in each of the following organizations: regional administrations, legal institutions, private company, industrial production, social service.

Figure 4 shows that about half of the respondents, 45.5%, have more than 10 years of experience, 27.3% have 5 to 10 years of experience, 18.2% have 2 and 5 years of experience and the remaining 9.1% less than 2 years of experience in their current positions.

4. Assessment of the degree of awareness of respondents in the area of information security. The particular interest to the research team conducting the survey was the identification and evaluation of the target group' level of awareness in the area of information security.

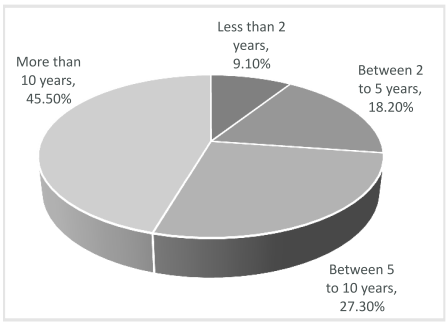

Fig. 4. Distribution of years of experience

4.1. Assessment of the degree of awareness of respondents in the technological aspects of information security. First multiple-choice question from this part (Fig. 5) indicates that respondents protect against malware software by prohibiting the use of unauthorized software and not opening emails from unknown source and attached files, while – 42.4% by using strong passwords. It should be noted that no respondent responded "I do not know".

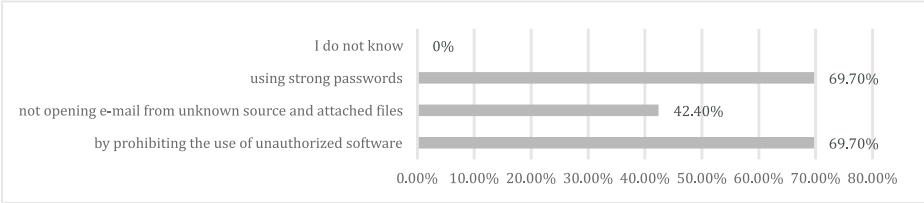

Fig. 5. Assess the degree of awareness of protection against malware software

According to most of the respondents Antivirus software (27 out of 33), and Firewall (16 out of 33) are the best ways to protect organization's information systems against unwanted or malicious software (Fig. 6). Other participants have also indicated Intrusion Detection System (36.4%), and Anti-spam filter (33.3%) as mechanisms of protection. It is noteworthy that there are significant percentage (9.1%) who responded "I do not know".

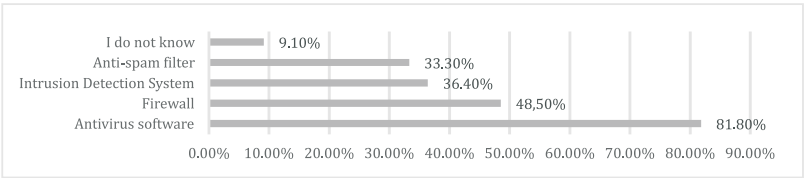

Fig. 6. Assess the degree of awareness of protection organization's information systems against unwanted or malicious software

4.2. Assess the degree of awareness of respondents in the legal aspects of information security. The results show that 75.8% of the participants believe that the purpose of the GDPR is to regulate the processing and storage of personal data of individuals by other persons, companies or organizations (Fig. 7).

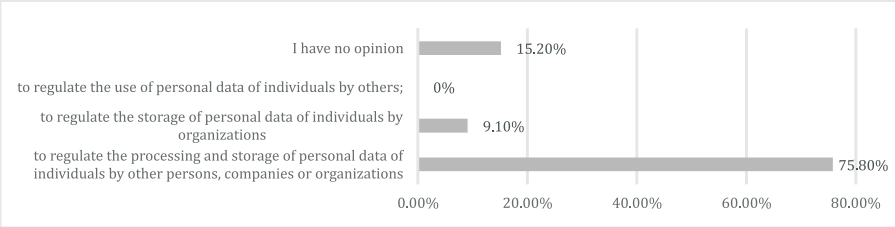

Fig. 7. Assess the degree of awareness of the purpose of the General Data Protection Regulation

The survey shows that participants with a percentage of 57,6% have stated almost uniformly that their organization requires the implementation of the General Data Protection Regulation (Fig. 8). There is a significant percentage (33,3%) who responded "I do not know".

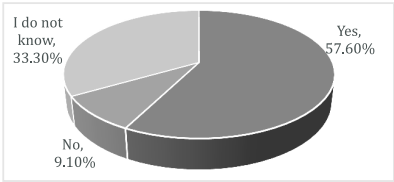

Fig. 8. Assess the degree of awareness of the implementation of the General Data Protection Regulation

5. Conclusion. The presented results reveal that the target group representatives have some previous knowledge and positive attitude of the information security domain. It should be emphasized that no respondent answered they were unaware how to protect their systems against malware. The vast majority of the participants claimed they were familiar with anti-virus programs and about the half – with firewalls. However, about 10 percents of the respondents were not sure what kind of security software should be used.

More than a half of them were aware of the GDPR regulations application in their organisations, probably due to the massive information campaign in European media during the preceding years. However, there's still significant number of respondents not aware of it, or in their opinion the organizations do not comply with the GDPR regulations.

The presented survey results acknowledge there is significant need of information security training for raising awareness of the information security vulnerabilities, threats and security solutions. Information security training should include people with different fields and professions, social status, education, age group, etc. Since the basic and the most lasting results are given by school-age education, this training is best to start within

the school courses and later upgraded during the university courses and continue with certificate courses that meet the goals and needs of an organization. This kind of training would comply with the lifelong learning idea.

The next project steps include effective valorisation of the created concept and its realization piloting with a selected target group of users (employees from local and state authorities). This piloting will be accomplished in order to perform proof-of-concept of the created solution. It will be performed with purposes to determine whether the solution meets the learners' needs, acquire information for a larger rollout and gain acceptance by users.

REFERENCES

[1] J. L. Grama. Legal Issues in Information Security, Jones & Bartlett Learning, 2020.

[2] GDPR (Regulation (EU) 2016/679) initiative, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[3] H. Sadaf, P. D. D. Dominic. Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, **60**, No 3 (2020), 201–211.

[4] https://www.forbes.com/sites/kateoflahertyuk/2018/12/19/breaking-down-five-2018-breaches-and-what-they-mean-for-security-in-2019/

Veselina Jecheva, e-mail: vessi@bfu.bg
Evgeniya Nikolova, e-mail: enikolova@bfu.bg
Burgas Free University
62, San Stefano Str.
8001 Burgas, Bulgaria

ОЦЕНКА НА НИВОТО НА ОСВЕДОМЕНОСТ ПО ОТНОШЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ СРЕД СЛУЖИТЕЛИ НА ДЪРЖАВНАТА И МЕСТНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ

Веселина Жечева, Евгения Николова

Редица проучвания сочат, че човешкият фактор е сред най-слабите елементи в съвременната взаимосвързана мрежова среда. Разработването на методология за повишаване осведомеността по отношение на уязвимостите, заплахите и решенията в областта на информационната сигурност чрез обучение и по този начин повишаване на общото ниво на сигурност на потребителите и организациите е основната цел на проекта "Immersive Learning in Information Security" (MISSILE). Задачите на проекта включват дефиниране на потребителските нужди и изисквания в областта на обучението по информационна сигурност и разработване на концепция за обучение по информационна сигурност, покриващо основните проблеми, свързани с най-важните съвременни предизвикателства в областта. С цел оценяване на нивото на знанията и уменията на целевата група за техническите аспекти, правните разпоредби и икономическите аспекти на информационната сигурност, потребностите и очакванията на членовете ѝ от електронен курс по информационна сигурност, беше проведена анкета. Настоящият доклад представя основните резултати от тази анкета.