IMPLEMENTATION OF PROBLEM-BASED LEARNING IN BUILDING AND DEVELOPING A CULTURE OF CYBERSECURITY IN A UNIVERSITY INFORMATION ENVIRONMENT

I. Peteva, S. Denchev, K. Bosakova

University of Library Studies and Information Technologies (BULGARIA)

Abstract

Cybersecurity is a matter of care and responsibility of all participants in cyberspace. The process of providing cybersecurity requires much more than simply imposing technical measures. The report examines the implementation of a human-oriented approach to building and developing culture of cybersecurity in a university environment through problem-based learning.

The culture of cybersecurity concerns the knowledge, beliefs, perceptions, attitudes, norms and values of people and how this manifest themselves in the behaviour of students in their interactions with information technologies.

The report aims to make security considerations an integral part of students' learning, habits and behaviour by incorporating them into their daily actions through a problem-based approach.

Adopting such an approach to cybersecurity allows a sustainable digital culture to evolve from the behaviour and attitude of users to information assets in cyberspace, and subsequently to take the function of a natural firewall.

A well-developed culture shapes security thinking in every student, improving their resilience to emerging cyber threats, while avoiding the imposition of subsequent strict security measures.

The implementation of problem-based learning is designed to improve the effectiveness of the development of culture in the context of cybersecurity and to help develop a wide range of skills in students. In this way, students have the opportunity to take control of their studies and make their own decisions.

Keywords: Cybersecurity, culture, problem-based learning.

1 INTRODUCTION

The development of the range of issues related to the culture of cybersecurity is directly dependent on the increasing consumption of modern information and communication technologies. The Internet has changed and continues to transform everyone's life, work and social behaviour. Internet users are growing by the second. Globally, approximately 4.66 billion people use the Internet, or 60 per cent of the global population. [1] According to the NSI (National Statistical Institute of the Republic of Bulgaria) in 2020 78.9% of households in Bulgaria had access to the Internet in their homes, which is 3.8% more than in the previous year. The highest percentage of people who regularly use the Internet (every day or at least once a week) are between the ages of 16 and 24 (91.5) [2]

The global pandemic caused by the spread of the coronavirus has also affected consumer behaviour worldwide. In October 2020, online traffic in 20 different industries increased by 1.5 percent compared to the reference period in January 2020. [3] Measures imposed to limit the spread of the disease have changed the way households use the Internet, as daily activities have become more virtual. The closure of universities and the transformation of traditional teaching into online learning are part of these measures. Thanks to the Internet, students have the opportunity to continue their education, but unfortunately they have also become potential victims of Internet attacks. [4] [5]

Awareness of cybersecurity is an important topic for everyone. The challenges that Covid-19 posed to all users of the World Wide Web necessitated a reassessment of the level of cybersecurity culture for all users of the World Wide Web and of the learning platforms.

This report is part of the Research Fund project №DN 15/2 "Conceptual model for generating trust and leadership based on image in the university information environment" of the University of Library Studies and Information Technologies and focuses on students at higher education institutions, who are one of the main groups of active users of all services and resources provided on the Internet.

Research shows that nowadays students spend a lot of time on the Internet not only in their free time, but also in searching and researching information related to their studies. [6]

Although technological advances make everyday life easier, they also add additional risks to students, due to the fact that often younger people do not pay the necessary attention to information security for reasons of different nature. The continuous improvement of personal knowledge and skills regarding the safety of cyberspace is of paramount importance, which leads to the application of different approaches to learning.

2 METHODOLOGY

E-learning has changed the way higher education works, becoming more proactive in building or finding new services, approaches and methods that can enable students to continue their education, despite the circumstances imposed by the global pandemic. [7] Naturally, the widespread use of e-learning has put on the agenda the issues of safe use of various platforms and information resources and last but not least the overall behaviour of learners in cyberspace.

Achieving an acceptable level of cybersecurity requires the development of solutions that encourage certain consumer behaviour in the reality of cyberspace. The increased level of cybersecurity culture, in turn, enhances consumer protection online without requiring the acquisition of in-depth technological knowledge. In order to change users' overall behaviour in terms of security, the methods for building cybersecurity culture should be focused on the social, cultural and ethical aspects of the user. When we talk about cybersecurity, we should not limit our focus to the integration of information security technologies only. We should think about people, about consumers. [8] The level of cybersecurity culture is important for everyone, but shaping and developing it in the younger generation can be particularly challenging. Students need to build and develop such a culture of cybersecurity that provides them with safety and protects them from the ever-increasing, in both form and quantity, number of online frauds or attacks. According to researchers in the field of security culture, it consists of three main factors - awareness, compliance, ownership, and research puts emphasis on the fact that cyberculture is much more than awareness. [9] [10]

Cybersecurity training is increasingly being implemented in syllabi in all specialties, not only for information and communication technologies professionals. This process seems to be still in a development stage, and it is not uncommon for lectures in cybersecurity disciplines for non-specialist students to focus more on "informing" about cyberspace threats. A method is needed to make students want to upgrade both their knowledge and their skills regarding their personal online safety; a method that is oriented both to students and the specific discipline. [11]

Achieving the goals of cybersecurity education for students from specialties outside the IT field implies methods that meet their needs and attract their attention, creating conditions for upgrading competencies and a desire for continuous improvement. Problem-based learning is such type of an appropriate method of teaching in disciplines related to Internet security. Problem-based learning is based on students' work in groups (teamwork) in order to solve a real problem. Applying a problem-oriented approach during university studies, strengthens teamwork among students, stimulates their critical thinking, especially the ability and skills needed in decision-making and problem solving. [12], [13] Another advantage of problem-based learning is the reduction of "information overload" since it is easier for students to select only important information without having to study a large amount of unnecessary information. [14]

The application of problem-based approach in cybersecurity education in a university information environment allows the focus to be placed on the human factor as a key component of the environment in the context of cybersecurity.

Although most crimes in cyberspace are targeted, they are often committed accidentally, too. Clicking on a supposedly harmless link in an email from a friend or just a bad habit like using a weak password can make it easier for cybercriminals. The application of a technical method as a stand-alone solution is ineffective in preventing security breaches. Investing in information security products cannot guarantee complete protection if it is not accompanied by the right IT security skills and a good understanding of cyber threats. Users have certain understanding that can affect the security process positively or negatively. [15] Problem-based learning provides an opportunity to examine and explore the behaviour, attitudes and the way to protect the user when using virtual space. In combination with the application of the game approach, students find it much easier to learn the basic principles and methods of protection against malicious IT attacks. [16] This creates prerequisites for a natural

construction of the main element of cybersecurity culture - lasting changes in consumer behaviour, leading to compliance with certain security measures and a way of using virtual environment.

The application of problem-based learning methods in a university learning environment provides ample opportunities to acquire basic skills and experience on key topics of cybersecurity, as well as to realize its importance and overcome the restricting perception that cybersecurity refers only to the application of technological solutions by IT specialists.

3 RESULTS

When implementing and using problem-based learning to raise the level of cybersecurity culture, it is necessary that students should be acquainted with the specific approach in advance; they should be given clear instructions and possess basic knowledge of the discipline. In order to make an appropriate choice of the level of difficulty of the specific problem, presented for solving to students, it is necessary to establish their initial level of awareness. For this purpose, a short questionnaire, covering key topics on cyber threats, can be used.

Such a questionnaire was used at the University of Library Studies and Information Technologies among second-year students majoring in National Security before proceeding to solve more complex problems. The questions concerned:

- Determining / identifying a phishing attack;
- Threats when using public Wi-Fi networks;
- Choosing a secure/strong password;
- Ways of storing/remembering the used passwords online;
- Naming known types of malware;
- Online presence and social networks.

The results of the completed questionnaire gave us an idea not only of the level of students‘ cybersecurity culture, but also directed us to the questions that triggered the greatest interest, comments and discussions. Students’ answers in this type of questionnaire help in choosing a problem that will be assigned to them to solve later. The questions can be selected for various reasons such as: the most common cyberattacks, the most commonly used technologies, some of the most important means of providing protection, etc.

The specific current issues highlighted in the process of problem-based learning, aimed at enhancing cyber security culture, can be synthesized in the so-called "social engineering".

3.1 Social engineering

As we have pointed out in the previous sections, technology alone is not enough to achieve a sufficient level of online protection. It is an indisputable fact that cyberspace users are often the weakest link in information security systems. They are often cheated / deceived in order to spread sensitive information. Jeremy Schoeneman: “Today, there are many ways an attacker will try and compromise a corporate network, but in the end, the individual is at the highest risk from an attack. Attackers will take whatever means necessary to break into a network and steal information, and the most popular, and most successful, is by way of social engineering. “[17]

The social engineering attack is based on the impact on people to disclose/share valuable information. Like the malicious hacker who seeks vulnerability in information systems, the social engineer takes advantage of traits such as human curiosity, devotion, naivety, etc. [18] Attackers can contact their targets by phone, email or direct contact to gain access to a valuable information resource. Examples are deception, phishing emails, fake websites, etc. This gives grounds for choosing specific tasks to be assigned to students in the process of cybersecurity training to focus on current situations that have led or may lead to a real threat.

3.1.1 Pretexting

Pretexting or creating a false identity or pretending to be someone else for malicious purposes is a very popular type of social engineering attack. An attacker can befriend people and ask for passwords and login information, telling them that these are needed for his role as a computer systems administrator, or simply someone in trouble and in need of help. [19], [20] The essence of pretexting is

that a social hacker invents a story to persuade his victims to reveal information they should not disclose. Direct face-to-face meetings require increased attention to detail, such as our body language.

3.1.2 Phishing attack scenario via email or website

Phishing remains a popular method of identity theft, fraud and the spread of malware. The practice of sending emails, using known sources as senders, in order to mislead the user and obtain sensitive information. These emails address topics that are relevant at the moment, such as holidays, events with great popularity among the public, even charity topics, fake emails from technical support, banks, etc. are used. These messages aim to extract valuable information mainly about credit / debit cards, as well as usernames for the purpose of misuse and profit. In indirect meetings, such as by phone or email, the social engineer is required to focus more on verbal manners.

And since the topic of the phishing email needs to be relevant in order to intrigue the recipient, what is more relevant than emails with information about medicines / vaccines using the confusion caused by the spread of coronavirus; [21]

Sample Phishing click bait Subject Lines:

- Click here for COVID-19 vaccinations;
- Message from the World Health Organization;
- Click here for Coronavirus-related information;
- COVID 19 Preparation Guidance;

COVID-19 related phishing emails with malicious file attached:

- Dear friend, go through the attached document for safety measures regarding the spreading of corona virus….
- Good day, please find attached report for COVID-19 preparation guidance…

The examples are also based on actual attacks in cyberspace. [22]

4 CONCLUSIONS

Threats in cyberspace will continue to be successful as long as there is someone who can be psychologically manipulated in some way. Control over online security depends on users who need to take care of their cybersecurity culture and, above all, its development. The application of problem-based learning with students is a good choice not only for developing the culture of cybersecurity, but also for exploring comprehensive and often ill-defined cybersecurity issues in the real world. Problem-based learning is oriented towards students and active pedagogy, which presents complex, open and real problems to promote the study of concepts and principles.

ACKNOWLEDGEMENTS

This report is part of the implementation results of the project "Conceptual model for generating trust and leadership positions based on image in the university information environment", according to Contract №DN 15/2 of 11.12.2017 with the Research Fund. Thanks to that project, the application of problem-based learning was analyzed in order to develop the culture of cybersecurity in the university information environment.

REFERENCES

[1] DataReportal, “DIGITAL AROUND THE WORLD,” 2020. [Online]. Available: https://datareportal.com/about.

[2] НСИ, “ИЗПОЛЗВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ В ДОМАКИНСТВАТА И ОТ ЛИЦАТА ПРЕЗ 2020 ГОДИНА,” 2020.

[3] J. Clement, “Coronavirus global online traffic impact as of October 2020.” [Online]. Available: https://www.statista.com/.

[4] F. A. Loan, “Internet use by the college students across disciplines: A study,” *Ann. Libr. Inf. Stud.*, vol. 58, no. 2, pp. 118–127, 2011.

[5] G. Blank and C. Lutz, “Benefits and harms from Internet use: A differentiated analysis of Great Britain,” *New Media Soc.*, vol. 20, no. 2, pp. 618–640, 2018, doi: 10.1177/1461444816667135.

[6] T. Hunt, “Cyber Security Awareness in Higher Education.”

[7] K. Maher and B. Indrachapa, “CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION.” Accessed: Jan. 14, 2021. [Online]. Available: https://www.academia.edu/36392436/CYBER_SECURITY_CONCERNS_IN_E_LEARNING_EDUCATION.

[8] G. Zhablyanova, M. Pavlova, B. Tetevenska, and K. Bosakova, “CYBER CULTURE - MYTH OR REALITY. BUILDING CYBER SPACE SURVIVAL COMPETENCIES,” in *EDULEARN19 Proceedings*, Jul. 2019, vol. 1, pp. 2480–2485, doi: 10.21125/edulearn.2019.0678.

[9] S. Al-Janabi and I. Al-Shourbaji, “A Study of Cyber Security Awareness in Educational Environment in the Middle East,” *J. Inf. Knowl. Manag.*, vol. 15, no. 1, 2016, doi: 10.1142/S0219649216500076.

[10] H. de Bruijn and M. Janssen, “Building Cybersecurity Awareness: The need for evidence-based framing strategies,” *Gov. Inf. Q.*, vol. 34, no. 1, 2017, doi: 10.1016/j.giq.2017.02.007.

[11] I. Pavlova, G. Zhablyanova, M. Pavlova, and S. Tsekova, “PROBLEMS AND PERSPECTIVES OF UNIVERSITY EDUCATION IN NATIONAL SECURITY IN THE ERA OF GLOBALIZATION,” in *EDULEARN17 Proceedings*, Mar. 2017, vol. 1, pp. 9224–9226, doi: 10.21125/edulearn.2017.0730.

[12] T. S. Chou, “Multi-learning techniques for enhancing student engagement in cybersecurity education,” *ASEE Annu. Conf. Expo. Conf. Proc.*, 2019, doi: 10.18260/1-2--33127.

[13] S. M. M. Loyens, P. Kirschner, and F. Paas, “Problem-based learning,” 2011.

[14] M. Shivapurkar, “Problem-based Learning for Cybersecurity Education,” vol. 7, no. 1, pp. 1–6, 2020.

[15] N. Gcaza, R. Von Solms, M. M. Grobler, and J. J. Van Vuuren, “A general morphological analysis: Delineating a cyber-security culture,” *Inf. Comput. Secur.*, vol. 25, no. 3, pp. 259–278, 2017, doi: 10.1108/ICS-12-2015-0046.

[16] N. Asanka and G. Arachchilage, “Security Awareness of Computer Users: A Game Based Learning Approach,” 2012.

[17] “Social Engineering Attacks: Common Techniques & How to Prevent an Attack | Digital Guardian.” https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack (accessed Jan. 14, 2021).

[18] F. Mouton, L. Leenen, and H. S. Venter, “Social engineering attack examples, templates and scenarios,” *Comput. Secur.*, vol. 59, pp. 186–209, 2016, doi: 10.1016/j.cose.2016.03.004.

[19] “Pretexting - an overview | ScienceDirect Topics.” https://www.sciencedirect.com/topics/computer-science/pretexting (accessed Jan. 14, 2021).

[20] “What is pretexting? Definition, examples and prevention | CSO Online.” https://www.csoonline.com/article/3546299/what-is-pretexting-definition-examples-and-prevention.html (accessed Jan. 14, 2021).

[21] “US DoJ to shut down 300 fraudulent websites exploiting coronavirus | The Daily Swig.” https://portswigger.net/daily-swig/us-doj-to-shut-down-300-fraudulent-websites-exploiting-coronavirus (accessed Jan. 14, 2021).

[22] D. Warburton and F5 Labs, “2020 Phishing and Fraud Report Phishing During A Pandemic,” p. 46, 2020.