INFORMATION SECURITY ADULT TRAINING IN COVID-19 CRISIS

Veselina Jecheva

Abstract: The purpose of this article is to familiarize readers with the approach used in the project "Immersive Learning in Information Security" (MISSILE) to develop a methodology for raising awareness of the information security vulnerabilities, threats and security solutions through learning and training. This purpose was achieved by solving the following objectives: By training solutions, MISSILE will aim at understanding the fragmentation of demand by studying training needs of users and organizations in relation to state-of-the-art platform offerings; By developing a concept for information security training, covering the major issues regarding the contemporary information security trends; By developing a security training platform able to incorporate different learning methodologies in an intelligent and highly cohesive way by exploiting individual characteristics and synergies between the learning approaches. By creating learning materials, related to information security issues, social engineering, users' beliefs and understandings about sensitive data and information security; to conduct effective valorisation of the created concept and its realization by piloting with a selected target group.

Keywords: MISSILE, project, information, security, training, covid-19, crisis

ИНФОРМАЦИОННА СИГУРНОСТ ОБУЧЕНИЕ ЗА ВЪЗРАСТНИ В КРИЗА COVID-19

Веселина Жечева

Абстракт: Целта на тази статия е да запознае читателите с подхода, използван в проекта „Имерсивно обучение в информационната сигурност" (MISSILE) за разработване на методология за повишаване на осведомеността относно уязвимостите на информационната сигурност, заплахите и решенията за сигурност чрез обучение и обучение. Тази цел беше постигната чрез решаване на следните цели: Чрез решения за обучение MISSILE ще се стреми да разбере фрагментацията на търсенето, като изучава потребностите от обучение на потребители и организации във връзка с най-съвременните платформени предложения; Чрез разработване на концепция за обучение по информационна сигурност, обхващаща основните въпроси, свързани със съвременните тенденции за информационна сигурност; Чрез разработване на платформа за обучение по сигурност, способна да включва различни методологии за обучение по интелигентен и силно сплотен начин чрез използване на индивидуални характеристики и синергии между учебните подходи. Чрез създаване на учебни материали, свързани с проблемите на информационната сигурност, социалното инженерство, вярванията и разбиранията на потребителите относно чувствителните данни и информационната сигурност; Да проведе ефективна валоризация на създадената концепция и нейната реализация чрез пилотиране с избрана целева група.

Ключови думи: MISSILE, проект, информация, сигурност, обучение, covid-19, криза

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. The major threats to the important information in digital age include social engineering, identity theft, malware propagation, various kinds of network attacks, social media and third party attacks, etc. Recent surveys, like SANS Security Awareness Report 2018 (https://www.sans.org/security-awarenesstraining/reports/2018-security-awareness-report) 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[1].

According to many surveys, like the one, described by Forbes in 2018 (https://www.forbes.com/sites/kateoflahertyuk/2018/12/19/breaking-down-five-2018-breaches-andwhat-they-mean-for-security-in-2019) this year has seen a surge in reported security breaches, although they are not new for the last two decades. The reason they explain is that after the EU general update to data protection regulation (GDPR) came into place in May 2018, organisations are more likely to report attacks. On the other side these results also demonstrate that the huge amounts of data collected by companies or states, is 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. 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 on international teams.

This leads to the idea that it is critical to raise security awareness of the wide audience and especially the employees from local and state authorities of the present vulnerabilities and threats, to the potential security breaches could prevent many successful intrusions. This idea fully complies to the GDPR (Regulation (EU) 2016/679) initiative to strengthen and unify data protection within and outside the EU. Apart from the technical aspects the training will include also legal regulations and economic aspects of information security[2].

Project purpose and objectives

The main purpose of the project "Immersive Learning in Information Security" (MISSILE) 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, MISSILE will aim at understanding the fragmentation of demand by studying training needs of users and organizations in relation to state-of-the-art platform offerings;
- to develop a concept for information security training, covering the major issues regarding the contemporary information security trends - in order to create an effective and feasible methodology for the information security training, the present learning approaches

(immersive, role-based, problem-based, adaptive learning, etc.) will be examined and the synergies between the most appropriate ones will be combined into a complete methodology;

- to develop platform, which implements the created methodology in a feasible and reliable way – this objective aims to develop a security training platform able to incorporate different learning methodologies in an intelligent and highly cohesive way by exploiting individual characteristics and synergies between the learning approaches.
- 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. These materials will be organised as training modules, covering various topics and levels and uploaded into the developed platform, which will provide 24x7 access of the learners. The materials will be accessible various kind of devices, including PCs, laptops, tablets, smartphones, etc.;
- to conduct effective valorisation of the created concept and its realization by 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 roll-out, gain acceptance by users, etc.

The project MISSILE is focused on extremely hot topic, developing key competencies, related to awareness about the information security vulnerabilities, threats and countermeasures. The main goal of the project is to develop a methodology for raising awareness of the information security vulnerabilities, threats and security solutions through learning and training and therefore increase overall security level of users and organizations. It can be achieved by the following objectives:

- to define user needs and requirements in the field of the information security training;
- to develop a concept for information security training, covering the major issues regarding the contemporary information security issues;
- to develop platform, which represents an actual implementation and actualizes 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;
- to conduct effective valorisation of the created concept and its realization by conducting of piloting with a selected target group of users.

By basing our solution into iterative working platform and user trials, we will push our system into piloting for testing and evaluating the created methodology. Apart from the innovative methodology for information security training and learning, we also foresee the formulation and exploitation of security and awareness training methods' synergies as a major outcome of the MISSILE project. This view is supported by our approach to allow dynamic definition of training and learning and by enabling novel methodology ahead of the state of the art.

The MISSILE information security and awareness training / learning strategy is properly designed to

have a multi-purposed impact, by (directly or indirectly) affecting the:

- creating new ideas and practical results in science;
- development of a methodology for training / learning in the field of information security;
- reaching a wide public of specialists and non-specialists and new audiences at both European and local levels;

- ensuring visibility across Europe, covering different countries and languages;
- ensuring further dissemination and strong follow-up.

The project target group consists of employees of local or state administration in all 5 countries of project partners. They include representatives from municipalities, district administration, educational authorities, legal authorities, etc. This training is important, since they access and process critical and sensitive information and therefore need to be trained about information security risks, threats, policies and mechanisms, including legal regulations and economic analysis. All project partners have close contacts with local and state authorities it their countries. According to these relations, the participants for envisaged project activities were selected according to the principle of closeness to critical data and their interests to the topic. Each partner will contact the authorities in their country and involve participants, who are the most vulnerable to the most common attacks (social engineering, identity theft, privilege escalation, etc.)[3].

The selected participants were included in the research phase with purpose to receive and analyze their feedback in order to develop the training methodology. As a first step, the level of their skills and familiarity with the topic, were evaluated by a survey. The obtained results were analyzed and taken into account during the next stages.

After outputs development the participants were introduced to the platform and they have been granted access to the learning resources in order to be involved into the next stage: piloting. During this stage they were participating in training and learning in order to conduct effective valorization of the created concept and its realization. Overall 100 public administration employees have been directly concerned by the pilot tests: each participating organization will be required to lead pilot test sessions involving at least 20 people. Pilot tests have been run by the participating organizations technical staff. After pilot tests completion, a survey was conducted with purpose to evaluate the participants' experience with the platform and their satisfaction from the training. According to the obtained results the learning resources will be adjusted to meet user expectations and requirements.

The platform and the learning resources were designed to be deployed even upon completion of the project. Participating organizations as well as organizations from within their professional networks will be able to borrow the platform and apply it for the purposes of their activities targeting specialists from public administration.

The participants' satisfaction of the piloting activity were evaluated and analyzed using surveys about the user experience with the platform, user scenarios passed and the overall impression, advantages and disadvantages of the training. The participants from the target group will also be involved in dissemination events - newsletters, social networks, media, websites, etc.

Methodology

The project activities started with examining the state-of the art training and learning methods and techniques. They included detailed research on the state-of-the-art training and learning methods and techniques will be conducted with purpose to develop an effective training. The contemporary learning and training methodologies will be surveyed and their advantages and drawbacks will be analysed. The detailed report, containing conclusions and recommendations about applied training methodology was produced. In order to develop an effective e-training course aiming at improvement the competences and knowledge of the target group in the area of information security in technological, legal and economic aspects, polls will be held for determining the attitudes and needs of trainees. For this purpose, questionnaires have been developed to collect information and assessments of the level of competence of administration officials in the subjects of the courses; thematic areas where training should be prioritized; the

common competences that need to be developed. The results of the surveys helped the project staff to adapt the training to the specific roles of different groups of civil servants. Studies among potential participants in the training outlined the need for training in the training modules[4].

In parallel, a detailed review and analysis of the contemporary virtual learning environments were produced with purpose to select the most appropriate training platform, meeting the trainees' needs.

In addition, a technical report, containing conclusions and recommendations was produced. And last, but not least, the training curricula was developed, covering the modules for technological, legal and economic aspects of the information security. Its content was based on the analysis of tools and methodologies for the non-formal teaching of adults, performed as part of preparation for the project. Particular attention has been paid to the following points:

- redundancies and overlaps between the proposal concerning three modules curricula
- the strengths and competences of the participating organizations involved in this project
- the potential for the work that is envisaged to meet the project's objectives
- the feasibility of the work given temporal and financial constraints
- the extent to which the work envisaged is original, innovative and complementary to existing
- resources

In parallel, defining what user requirements and scenarios was continued with platform design and development. This platform is available at https://project-missile.eu/moodle/ and contains 3 basic categories for the three intellectual outputs. They correspond to the 3 training modules: respectively, technological, legal and economic aspects of security. All the modules are:

- comprehensive: it will contain an exhaustive and up to date set of activities on the topic of coding
- self-contained: people in charge of delivering the module won't need to rely on any external resource to deploy it
- participative: it will allow users to act as a group in order to tackle some of the challenges, it will also involve interaction between facilitators and users
- adjustable: facilitators will be able to adjust it based on the needs of their target public, their background knowledge, competences, and skills
- immersive - non-linear, game-based, interactive, engaging

The training module for the technological aspects of information security includes the technological content in the field of the information security, which will be delivered to the learner. The purpose of the module is to raise trainees' awareness about security issues and to obtain knowledge and skills for analysis and assessment of information security in computer networks and systems. The learning outcomes are the following:

- understanding basic problems regarding contemporary systems security;
- analysis and assessment of security threats and risks;
- development and application of security policy and mechanisms.

The materials cover the defined topics, aiming at introducing the following major issues and related security solutions:

- theoretical basics, like confidentiality, integrity, availability, security policy and mechanisms,
- risk assessment and management, etc.

- malware, vulnerabilities and threats, like viruses, worms, trojans, spam, spyware, adware, sniffing, spoofing, etc.
- network attacks - DoS, man-in-the middle, buffer overflow, code injection, etc.
- security countermeasures, like antivirus software, firewalls, applied cryptography, intrusion
- detection and prevention systems, audit software, etc.
- security standards and frameworks (ISO/IEC 2700x, NIST, IEC 62443, etc.)
- social engineering attacks – like phishing, tailgating, infected USB devices

The learning materials contain text, multimedia elements, like images, video, audio, interactive materials, practically oriented cases and projects, etc.

The module will also include some theoretical fundamentals like the concepts of confidentiality, availability and integrity, and the relations between them including physical, software, devices, policies and people; the basis of authentication, non-repudiation, access control and privacy. The resources will also cover how the appropriate policies will be adequately defined and the security techniques and mechanisms could be selected in order to tackle and solve problems and to achieve the maximum security with the present resources.

Information technologies have entered into all aspects of public life and have prompted global integration of the information space. This led to the development of legislation regulating the field of information security and protection of information - classified, public and private (personal data). Taking into account the global trends, the legislators in EU and member countries adopted numerous new laws regulating the information security. At the same time, there are few opportunities to acquire follow-up training for employees involved in this field. This imposes the obvious need for a welldesigned and structured curriculum to build up new knowledge and skills.

The aim of the training is to create the necessary prerequisites for improving the qualification of the learners and for fulfillment of their duties at every level in the ministries, agencies and all non-profit public organizations. The training is useful to all professionals working in the field of information security and managers and specialists from the state and municipal administrations[5].

The main task was to develop the knowledge, skills and abilities of professionals and to increase their professional qualifications in the field of information security and information protection in computer systems and networks. At the end of the course, learners will acquire the knowledge for:

- the basic concepts and policies for protection of classified, public and personal information and the legal framework in force in this field;
- to search, find and use new developments in the field of information security and information protection;
- to respond successfully to new situations in the area of information security and decision-making in the sphere of information protection.

Therefore, logically the education addressed key issues related to the legal protection of certain types of information. The subject of the training includes protection of classified information, public information and personal data and legal aspects of information security and the general concept, strategy and policies for ensuring information security at European and national level.

The module is divided in two parts:

- The first aspect revealed the regulation within the European Union. Attention has been paid to each of the three levels of regulatory protection - policy documents, directives and standards, but the focus was on the most significant of them - the General Data Protection Regulation - Regulation (EC) 2016/679). The EU's requirements for the storage of personal data and information storage measures, including the requirement for certain types of organizations to appoint a Data Privacy Officer (DPO), was examined.

- Next stage was to inspect the regulation on a national level in each of the member states. The legal framework in partner countries is formed by:

- The Classified Information Protection Framework which introduced effective mechanisms to ensure information security for all entities that create, process, store and transmit classified information. In this regard, the concept of state secret and its delimitation from similar concepts such as official secret, trade, military, etc. are considered. Learners were introduced to the levels of information classification, unauthorized access to classified information and criminal law protection.
- The Law on Access to Public Information – The learners were introduced to the scope and content of the public information, the obligation to provide such information to the subjects and way to access and the restrictions on access to public information.
- Personal Data Act – The learners were introduced to the concept and categories of personal data and the general principles for the protection of personal data. An overview of the national legislation and the data protection legislation have been made, paying special attention to the new moments in the GDPR.
- Special attention has been paid to the criminal law protection of the information in national legislation and the most frequently committed crimes - protection of personal data, commercial and public information, computer crimes - illegal access to computer systems, theft of information, computer fraud.

As a conclusion we can say that the development and implementation of such a curriculum has created traditions and advanced experience for the needs of future ventures and initiatives in this field.

Economics of information security is one of the most complementary and neglected field of information security studies and trainings. By integrating a module on economic aspects of information security not only increase the target groups' awareness towards economic outputs but also will affect their perceptions and applications in market mechanism. Because the economics of information security has become a growing field of economics. More generally, many of the most basic information security issues are in the current economic debate. The economics of information security is mainly related to market failure. According to a recent survey by Global Threat Intelligence Report, NTT Group, 2017 the economic impact of information security in EU breaches vary between 1 and 26.19 million euro (£14 million) annual cost per company.

Many researchers have started to work on the economics of information security as a market failure and its aspects. This module training aim to teach managing the economics of information security

against market failures. The learning outcomes are the following:

- understanding the security and privacy economics, including utility, incentives, public goods, externalities and internalities, and trade-offs;
- comprehension of economic resources and risk assessment with respect to security policy;

- using and comparing models to understand security policy, technology, and decision-making.

One of the major aspects in economics of information security is about economic vulnerability. Economic vulnerability refers to risks caused by exogenous shocks to system of production, distribution and consumption that arising out of economic openness. However, markets for vulnerability can be managed to reduce the cost of securing the soft wares and mobile applications. Vulnerabilities are mostly thought by the banking systems and financial economic, however a larger perspective will be the focus of this module after a comprehensive need analysis.

Externalities are another aspect in economics of information security. Information economics are characterized by many positive and negative externalities where economic decision making units' actions have effects on third parties. The module covered the following major topics:

- Information security vulnerabilities
- Privacy problems as an externality and free rider problem
- Security as an externality
- Price discrimination
- Asymmetric information: adverse selection and moral hazard
- Policy options for dealing with market failures

Although a rare number of this module on the economics of information security contributed to the Project during the Project lifetime to its stakeholders but its teaching materials remained after the Project with high potential of contributing to the growing body of literature with the evidence from EU. Since a literature review exists, a deep review and conceptualization were made through a deep literature from an interdisciplinary perspectives, such as from IS, MIS, Economics, Law and Business studies.

At the end of each training, surveys will be conducted to determine the degree of satisfaction with the training, with the assessment of the following criteria:

- Actuality - conformity of the curriculum content of the current regulatory framework and the contemporary knowledge;
- Relevance - correspondence between the learning objectives and the curriculum; correspondence between the curriculum and the needs / activity of the administration;
- Practical relevance - linking the content with the practical needs of the participants in the training.

The piloting phase included also examination of different user-profile studies from the test case environments, as well as from testing activities in controlled environments to pilot the created learning environment with real target audience, ascertain the level and limitations of their pre-existing knowledge to comprehend how much the target users know about information security and to what extent the training is useful.

In addition, a number of broad practice used for assuring the quality of products or services have been applied. This activity has been held during almost the whole project duration, verifying the quality of all project activities. For that purpose it has been monitoring all project activities, evaluate their quality and generate reports.

Acknowledgement

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

References

[1.] https://project-missile.eu/

[2.] Erasmus+ project number 2019-1-BG01-KA204-062331; Start/End Dates 01-10-2019 – 28-02-2021.

[3.] Caciuloiu, A. (2020). UNODC tackling cybercrime in support of a safe and secure AO-IS. UN Office of Drugs and Crime.

[3.] Custers, B.H.M., Pool, R.LD. & Cornelisse, R. (2018). Banking malware and the laundering of its profits. European Journal of Criminology. 1(8): 1-18.

[4.] CyberEdge Group (2020). Cyberthreat defense report. Retrieved 25 August 2020

[5.] ENISA (2018). Enisa Landscape Threat Report Retrieved 25 August 2020 from