SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Simulation framework for practical cybersecurity training in the public service sector

Veronika Deák

deak.veronika@uni-nke.hu

https://orcid.org/0000-0001-9220-2002

Doctoral School of Military Engineering, National University of Public Service,
2 Ludovika tér, H-1083, Budapest, Hungary

Abstract

The public service sector is a key target of cyberattacks. In order to prevent and effectively tackle such attacks, organisations should continuously develop their defence capabilities. As part of developing such capabilities, public service cybersecurity training is required to teach students about cyberattacks. The present study uses quantitative research techniques including (i) how to identify key requirements for the practical aspects of public service cybersecurity training and (ii) sampling to utilise international best practices from cybersecurity education and conceptual architectures from existing public service organisations. A schematic structure with a two-level practical training course is proposed. On the first level, the students learn about the defence mechanisms of their own info-communication devices and try to prevent attacks in a simulated environment. On the second level, the students apply protection strategies against cyberattacks in organisational infrastructure. Finally, a technical framework is defined to simulate cyberattacks against (a) personal devices and (b) a fictional organisational infrastructure. The specification of a public service cybersecurity training programme should not only focus on theoretical education but also provide practical knowledge to students. By simulating specific attacks, theoretical and practical knowledge can be combined. As a result, students will be able to recognise threats and potential risks from cyberspace.

Keywords:

simulation framework, cyber security, cyber security education, public service, practical training

Article info
Received: 9 September 2020
Revised: 29 December 2020
Accepted: 29 December 2020
Available online: 19 March 2021
DOI: http://doi.org/10.35467/sdq/132026

Introduction

Cybersecurity is a rapidly changing, constantly evolving and expanding field that holds new challenges and threats for us. Creating the right level and quality of cybersecurity is considered to be critical in both the public and private sectors. The continuous increase in the number of cyberattacks that are emerging means that alternative defence mechanisms need to be developed. This is especially true for the critical infrastructures of public service and is an indispensable condition for the day-to-day operation of society, hence it is essential to ensure the continuous and reliable operation of the information systems on which it is based.

Cyberspace and, consequently, threats from cyberspace have become a natural part of everyday life. The use of cyberspace is essential for the efficient and effective operation of the public service sector, but in addition to its many advantages, we must also take into account its disadvantages and potential risks. Attackers are increasingly exploiting vulnerabilities in various information systems and the human factor. In many cases, the purpose of attacks is to restrict and hinder the operation of the information society and the attackers often target certain areas of the public service sector, as well as critical infrastructures.

Therefore, the continuous development and strengthening of cyber defence capabilities and cybersecurity are fundamental in the public service sector where the development of cybersecurity training, education and exercises are essential elements.

A considerable number of attacks target the unpreparedness and lack of security awareness of users. This is why the primary goal is to create and continuously improve the awareness and cyber defence capabilities of public service employees, which requires a form of training to achieve these goals. According to a survey by The International Information System Security Certification Consortium Inc. (ISC), cybersecurity workforce shortages will reach 1.8 million by 2022 (Morgan, 2017). An article by Csaba Krasznay highlights the need for the training of cybersecurity professionals and points to a number of events in cyberspace that undoubtedly have an impact on the physical world (Krasznay, 2017).

Cybersecurity training for public service is required to provide its participants with practical knowledge and problem-solving skills, which enable them to recognise and map the attack surfaces of cyberattacks and take preventive measures at cyberattack points in their environment. In addition, participants should be able to identify a specific attack or intervene if necessary. By completing such training, people working in the public service sector should receive knowledge about both the theoretical and practical aspects of cyber defence.

The aim of the two-stage structure of the training is to enable the students to apply the acquired theoretical knowledge in practice and to transfer it to real situations. Therefore, special attention should be paid to the practical part, and the definition of its content and components, in order to transfer practical knowledge and simulate attack techniques in the most authentic way.

In this paper, I present the schematic structure of two-stage practical training in general, which will be part of the cybersecurity training for the public service sector in Hungary; however, the approach can be adapted by any other nation. During the training, the students first get familiar with the protection mechanisms of their own infocommunication devices, and then they perform various cyberattack techniques and methods in a simulated environment. At the second level, the general architecture and components of a fictive organisational infrastructure and their protection mechanisms are identified, and then protection strategies are applied during simulated cyberattacks.

In order to achieve this, I identify a framework that describes the simulation environment that forms the basis of practical training, which serves to prepare people working in the public service sector for the detection and prevention of complex organisation-level cyberattacks. Finally, an automated assessment infrastructure is introduced based on the extension of the proposed simulation environment to enable practical exams for the training, even in a remote manner.

Goals and challenges

According to the presented concept of the two-staged training programme and its required required elements, I formalised the goals of the present paper as follows:

G1 Practical training: Defining the structure and elements of the two-stage practical training, the cyber defence mechanisms and knowledge areas to be transferred.

G2 Simulation Framework: Defining a framework that describes a simulation environment that can be used to prepare people working in the public service to defend against cyberattacks.

G3 Automated assessment: Developing an automated assessment system for the accountability of the knowledge transferred during the practical training.

Table 1. Goals and challenges.

	GOALS		
	G1 Practical training	**G2 Simulation Framework**	**G3 Automated assessment**
CHALLENGES	C1.1. Specify the required topics	C2.1. Use devices of students	C3.1. Quantifying the success of defence
	C1.2. Order of the topics	C2.2. Identification of public service specific IT systems	C3.2. Storing and replaying
		C2.3. Generic framework	
		C2.4. Extensible framework	
		C2.5. Support for distance learning	

In order to achieve these goals (G1-3), I faced additional challenges, which are illustrated in Table 1. Challenges are indicated by the letter C, where the first digit identifies the goal to which it relates.

C1.1. Specify the required topics: To define the knowledge to be acquired, special attention must be paid to be able to adapt people to the jobs, organisational system and experience of the public service sector. Defining public service-specific knowledge is essential for the development of effective theoretical and practical education.

C1.2. Order of topics: The order of theoretical and practical education should be taken into account when the structure of practical training is determined to avoid references to topics that will be acquired later in the semester by the students.

C2.1. Use of devices by students: It is important for students to be able to connect their own devices to the simulation framework that forms the basis of the practical part of the training. Examining the devices of the students is warranted because students use these on a day-to-day basis, in many cases even for employment purposes. For example, they download, edit, and transmit documents using their own devices and the applications on them.

C2.2. Identification of public service specific IT systems: It is necessary to identify the IT systems and infrastructure characteristics of the public service sector, as an environment must be created that does not contain irrelevant components for public service employees.

C2.3. Generic framework: The simulation framework should be general enough to not only support cyberattack patterns related to a pre-defined job, but to be able to cover many areas of public service.

C2.4. Extensible framework: The framework must be extensible so that more components and attack patterns can be added later. The framework can therefore be prepared for future and so far unknown attacking techniques.

C2.5. Support for distance learning: The framework should be designed to be suitable for distance learning. The current pandemic situation also proves that in addition to traditional education, some forms of distance learning need to be prepared when creating the educational environment, as often unforeseen external conditions can significantly affect the effective implementation of practical education.

C3.1. Quantifying the success of defence: The quality and success of the defence measures against attacks performed in a simulation environment should be quantified. When evaluating students in an exam, it is important to identify a grade based on the performance, which can be achieved by defining clear and consistent metrics.

C3.2. Storing and replaying: The sequence of actions performed during the exams must be storable and manually re-executable. The purpose of these properties are to make the number of points and marks obtained for a given task identifiable for both the instructor and the student after solving the exam task.

The structure of the present paper is organised as follows: the relevant related literature is overviewed in Section 2 while Section 3 defines the two-stage practical training. In Section 4, a high-level definition of the simulation framework is presented and, finally, in Section 5, the extension of the framework to be able to support automated evaluation is presented. Sections 3, 4, and 5 of this publication reflect the goals and challenges presented in this chapter.

Literature review

In order to achieve a comprehensive definition of the two-stage practical training aimed at in the present study and the framework describing the necessary simulation environment, a deeper evaluation of the relevant domestic and international literature is essential.

Studies on the environment of cybersecurity practice education

Topham *et al.* (2016) provide an insight into the methods and approaches used in practical cybersecurity education and also set out requirements and good practices for future training methods. As part of this, the authors present and compare the types of each practical laboratory, analyse some examples and then identify suggestions and requirements for future platforms. The authors identify three types of laboratories: physical, simulation, and virtual laboratories. The study sets out the requirements for the teaching process that all cybersecurity laboratories must meet. In order for teachers to be able to create scenarios and exercises for real-life situations and attacks, the labora-

tory must provide the conditions for carrying out the most creative exercises possible, in accordance with the principle of flexibility. Instructors should be able to display practical assignments quickly and easily to multiple students at once. Laboratory info-communication equipment and software should be separated from external networks. It should be possible for students to be granted administrative rights to the machine assigned to them, which is essential for certain experiments. Continuous storage and backup should be guaranteed to ensure continuity of student work and recovery in the event of a failure.

Williems *et al.* (2012) investigated the possibilities of practical cybersecurity education, the so-called Tele-Lab platform where its operation and use are presented in detail. Tele-Lab provides a hands-on cybersecurity training system in a remote virtual laboratory environment that is accessible to everyone. The authors outline the basics of practical cybersecurity education based on classical laboratory training and its disadvantages. Such disadvantages include the fact that devices in classical computer laboratories are difficult to move, expensive to purchase and maintain, do not allow access to the internet, and it is essential to separate these devices from other networks. In addition, the study mentions several disadvantages related to other software and simulation systems. To overcome these, the authors recommend the Tele-Lab project, which can also be interpreted as an internet-based distance learning system that is also compatible with traditional offline cybersecurity practice laboratories. Tele-lab is basically a web-based education system that consists of a training environment built with virtual machines and that provides the acquisition of the necessary cybersecurity knowledge with learning units consisting of practical tasks. Virtual machines can be used to simulate many forms of cyberattack, so that both the attacker's and the victim's side can be illustrated. This includes, for example, simulating user behaviour and the actions of an attacker, which makes a significant contribution to presenting the real attack situation. The content of the learning units is characterised by both theoretical and practical knowledge, where the aim is to apply the acquired theoretical knowledge in specific practical situations. Each learning unit also gives a tip on how to prevent and eliminate the currently described attack method.

Beuran *et al.* (2018) point out that only through hands-on education can students achieve the knowledge, skills, and abilities needed to respond to cyberattacks that will help them respond immediately to real events. In their study, the authors present the integrated cybersecurity training framework they have developed, called CyTrONE, its design, implementation, and effectiveness. There are three main categories of training activities: attack-oriented training, analysis-oriented training, and defence-oriented training. The training framework uses both traditional printed and digital learning materials and provides students with a range of e-learning opportunities and practical tasks that can be performed in a specially designed training environment. According to the authors, the implementation of two requirements is necessary to create an effective cybersecurity training framework. One is the ability to modify and add new training content, the other is the ability to automatically create and manage the training environment. After that, the authors outline the design, process and steps of the framework, as well as the advantages and usability of this type of training. They then present some elements of the framework, such as the user interface, the training database, the management module, possible additional modules that can be added, and the infrastructure of the servers and network devices. The authors explain that the advantage of the present training is the reduction of barriers to entry, as the easy-to-use descriptions facilitate the understanding of complex technical specifications and standardise the management of the training content and environment, which significantly reduces operating and installation time, and integrate it to support the entire cybersecurity education process. In addition, the public disclosure of the framework allows for wide access and further effective development and expansion.

Other studies related to practical cybersecurity education

Dimkov *et al.* (2011) have developed a course that focuses not only on the technical aspects of cybersecurity and information security, but also on the physical and social aspects of security. As part of this, students will have the opportunity to acquire practical knowledge of physical security, social engineering and penetration testing. The aim of the course is to assess and continuously improve the level of security awareness of students. The duration of the course is eight weeks, during which students must write a scientific study and take part in a practical assignment suggested by either them or the instructors. The introductory part of the course introduces the basic concepts of computer security in terms of physical, digital and social security. Students may encounter tasks in which, for example, a general security environment, system, and security event must be planned and analysed in order to learn what techniques can be used to achieve different goals. In addition, this course provides first-hand students with first-hand experience of real-world experiences. Students learn about the attackers 'perspective as part of a hands-on task, in which they perform a physical intrusion exercise using social engineering techniques, followed by an offline and an online attack on the target's laptop. The aim of the internship is to learn more about each type of social engineering and to study its application in more depth, and to gain a kind of insight for students to attack information systems using offline and online methods.

Patriciu and Furtuna (2009) provide a number of steps and guidelines that are recommended to follow when designing or implementing a new cybersecurity practice. Seven steps have been identified, which include defining goals, selecting the right strategy, designing the network topology, creating a scenario, creating a set of rules, and selecting the right indicators and lessons. Based on the objectives, a decision is made as to what tools and software will be used in the execution of the task, and the general topology was determined on this basis. Based on these, the rule book and practice scenario will be developed. The definition of relevant indicators is essential for measuring and monitoring its practical effectiveness. In general, practice has two main sides, the offensive side and the defensive side. On both sides are various computers and other devices that are managed by the participants. The number of participants in the exercise is not maximised. The article provides a detailed insight into the content and importance of each step.

The two-stage practical training

This chapter examines the structure of public service cybersecurity training, the content and structure of the two-stage practical training, and the knowledge and cyber protection mechanisms to be transferred to the students are defined. The aim of this chapter is to find a solution to achieve the goal identified by G1.

Knowledge to be acquired during practical training

To determine the structure and content of hands-on training, it is essential to identify the general cybersecurity tasks that civil servants need to perform, either in their day-to-day work or in the event of a possible cyberattack as already described in challenge C1.1. After defining the tasks, the knowledge areas of the practical training can be specified. In my previous study, I identified the knowledge to be acquired by civil servants during such training, which is necessary for the performance of everyday cybersecurity related tasks, with the help of the knowledge set fixed for the cybersecurity positions of the NICE Framework[1] and the good practices discovered during the evaluation of international training (Newhouse *et al.*, 2017). These knowledge areas are shown in Table 2.

1. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

Knowledge (K)
K1. basic concepts related to computer networks
K2. risk management processes
K3. cybersecurity, data protection legislation, guidelines, principles
K4. threats from cyberspace
K5. wireless technologies
K6. the components of a cyber defence system
K7. cybersecurity and data protection positions within the organisation
K8. techniques and procedures applicable in the case of cyberattacks
K9. interfaces between human factors and cybersecurity

Table 2. Knowledge areas of the practical training.

Structure of public service cybersecurity training

During the training, people working in the public service can get acquainted with both the theoretical and practical aspects of cyber defence, as the training consists of a theoretical and a practical part. The analysis of the previously identified areas of knowledge and the good practices revealed during the examination of the domestic and international trainings helped to determine the structure of the training.

The schematic structure of the training is illustrated in the figure below to ensure the appropriate order of the selected topics to address the challenge C1.2.

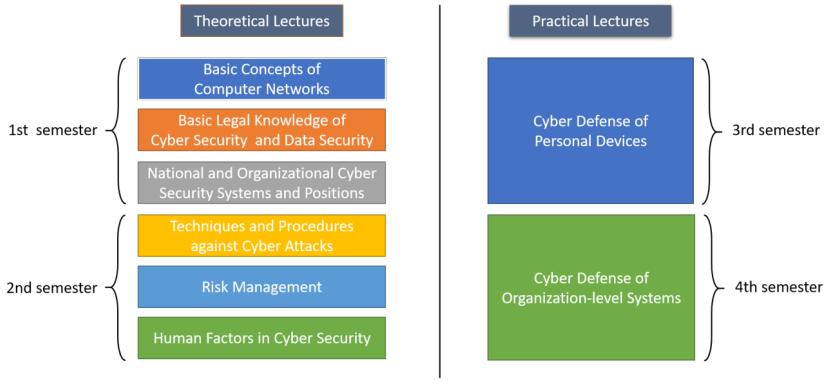


Figure 1. The schematic structure of the training.

The content of the theoretical part

In the theoretical part of the training programme, students can acquire the following main topics: general IT basics, cybersecurity and data protection legislation, basic concepts, the structure of the state cyber protection system, and cybersecurity and data protection positions within the organisation. After that, in the second semester, they will be introduced to additional necessary knowledge, such as the types of various cyberattacks, attack techniques, and methods for preventing and combatting them. In addition, they master the methodology of risk management and explore the role of the human factor in cybersecurity and their interfaces. A detailed discussion on these topics is part of the scope of the current study.

In order for participants to put the acquired theoretical knowledge into a sharp situation, the practical part of the training makes them face specific attacks. The purpose of this is

to ensure that civil servants are expectedly hit by a real attack and to make the necessary, and in many cases, strategic decisions.

The content of the practical part

The condition of the practical part of the training is the acquisition of the theoretical knowledge of the first two semesters, since in order for students to apply various cyber defence mechanisms in practice, it is essential to examine the theoretical background of cybersecurity. The practical part can be divided into two further phases, which will be held in the third and fourth semesters. During this two-step hands-on training, students first become familiar with the defence mechanisms of their own infocommunication tools and then perform attack prevention in a simulated, organisational-level environment.

During the practical part of the training, theoretical and practical knowledge can be combined by simulating specific attacks based on existing knowledge. As a result, students will be able to recognise threats and potential risks from cyberspace.

In the third semester of the cybersecurity training, the first stage of the practical training takes place, which basically covers the security settings of the students' own infocommunication devices, the threats affecting them and the practical tasks related to their prevention and response. In addition, the students must cope with the daily operational tasks and the adequacy of the information system and the related processes and procedures. The aim is to enable students to put into practice the various tasks involved in operation, prevention and control. The range of the students' own infocommunication tools covers the devices used by public service employees on a day-to-day basis, such as smartphones, tablets, laptops, and smartwatches. Of course, due to advances in technology and the emergence of newer tools, this list needs to be constantly expanded. Examination of one's own assets is justified because, in many cases, employees may use them for employment purposes. For example, they download, edit, and transmit documents using their own devices and the applications on them. Your workplace may allow your employees to work with their own device within the framework of the BYOD (bring your own device) policy. There are many advantages to this principle, but we must not forget its disadvantages and dangers either. In addition, even though most organisations are not allowed to use their own devices for work purposes or vice versa, in many cases, employees may still use them despite the fact that they might receive a punishment. A number of additional safety issues are raised by the fact that any work done at home can only involve the use of work equipment or even your own infrastructure. Furthermore, it is important to mention that the protection of one's own infocommunication devices is not only essential to avoid various cybersecurity incidents but is also important for the protection of personal data and privacy.

In the first stage, students will learn about the operation of the tools and applications they use, their security and privacy settings, the threats to their devices, and cyberattack techniques. They examine browser security settings such as logins and passwords, cookies, permission requests (location, camera, microphone etc.), data collection, content blocking, or even the role and importance of customising certificates and the associated threats. Students will learn the specific rules, vulnerabilities and settings of social media, including the forms of password management and authentication, the types, importance and possibilities of personal data protection settings. The participants will get acquainted with the various e-mail systems, as well as cloud technologies, their dangers, as well as the importance and details of the various security and data protection settings. In addition, during the semester, special attention will be paid to the vulnerabilities of various operating systems (e.g. Windows, iOS, Android, and Linux), the rules for using them, and the possibilities of implementing various protection measures. Students

will become familiar with the basic rules and dangers of the most commonly used text, spreadsheet, and slide editing programs. In addition, they perform a number of additional basic operational tasks related to infocommunication devices, as well as perform vulnerability detection and basic steps to prevent and defend against various threats. Importantly, this semester, students will not only implement various security settings and detect vulnerabilities as part of prevention, but will also encounter device- and application-specific cyberattacks, as well as implement and practice each step and method for responding to them.

Figure 2. Infocommunication devices and applications.

The second half of the practical part will take place in the fourth semester of the public service cybersecurity training. In this context, students implement cyberattacks in a simulated organisational environment, either individually or in a team. The essence of this is to simulate an organisational level environment during the semester, as it is only through such practical activities that students can acquire the necessary skills and abilities that will enable them to respond to a real security incident or event in the shortest possible time.

As part of this, students will become familiar with the structure of workplace tools and the information system, their vulnerabilities, related operational tasks, and possible alternatives to prevention and control. The types of basic systems (operating system) that ensure the operation of the devices, the conditions for operating them, vulnerabilities and various protection and security settings are explored. The installation of many applications and software on workplace devices is warranted, so exploring their installation, operation, and hazards, as well as examining the origins of licences, is especially important if the employee is installing them on their workplace device. Practical examples illustrate the dangers of connecting foreign devices to work devices and connecting them to an open internet network. In addition, the basic rules and vulnerabilities of the use of e-mail systems and the practical experience of receiving various phishing emails and malware as attachments are mentioned.

Students will experience in a simulated organisational environment what cyberattacks pose a threat to the information infrastructure and what preventive and protective measures can be used to prevent these attacks. These include, but are not limited to, DoS, DDoS, XSS, SQL injection attacks, various types of malware, phishing, and social engineering techniques in real-life situations. This semester, social engineering methods will be presented and simulated on a separate course. Social engineering makes it possible to obtain inside and confidential information by deceiving, exploiting and manipulating a person, or even infecting an infocommunication device with malware. These techniques work well in cyber warfare, as they exploit technological vulnerabilities and user vulnerabilities together and, in many cases, with a high level of protection for information systems, the attacks target the user. Furthermore, students face additional cybersecurity challenges, such as misuse of user IDs and unauthorised access to a system or data, for any

service, system, infocommunication device used by the user (e.g., e-mail, professional system, etc.). In addition, data leakage, which may take the form of intentional or accidental transmission of non-public data that forms part of the data assets of the organisation concerned, to unauthorised organisations, people or systems which are unreliable from the point of view of data confidentiality. It is important that not only threats from cyberspace are emphasised during the training, but also various physical changes in the condition of the devices, such as the loss or damage of the student-owned infocommunication devices, or even the handling of signs of disruption.

The purpose of the practical training is for students to practice the steps and techniques to be used during emergencies in a realistic environment and to check the applicability of strategic plans.

A framework describing a simulation environment

During hands-on education, it is important to create an environment through which students can face with known cyberattack techniques and try out the defence mechanisms learned during the training in a simulated environment. For this reason, it is necessary to define a framework that can provide support during training for learning about the protection of individual infocommunication tools and the use of protection mechanisms at the organisational level. The aim of this chapter to address the G2 goal by proposing a solution for defining the simulation framework.

Main components of the framework

When defining the framework, it is necessary to distinguish between the application layer and the infrastructure layer because, based on practical experience, cyberattacks can also be grouped into cases that exploit hardware and software.

The three main components of the framework are identified as follows:

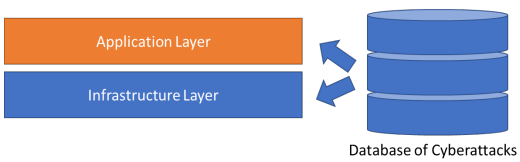


Figure 3. Main components of the framework.

Application layer: a set of applications and operating systems required to simulate software cyberattacks.

Infrastructure layer: the architecture required to simulate hardware cyberattacks.

Database of Cyberattacks: A definition of each cyberattack that can be used to execute an attack in a simulated environment.

Infrastructure level

The main considerations in determining the level of infrastructure in the framework were:

- Not accessing the Internet during the simulation due to data protection, legal and other regulations and avoiding possible threats from cyberspace.

- Individual infocommunication devices being easy to connect.

• Characteristic elements of the public service infrastructure being available.

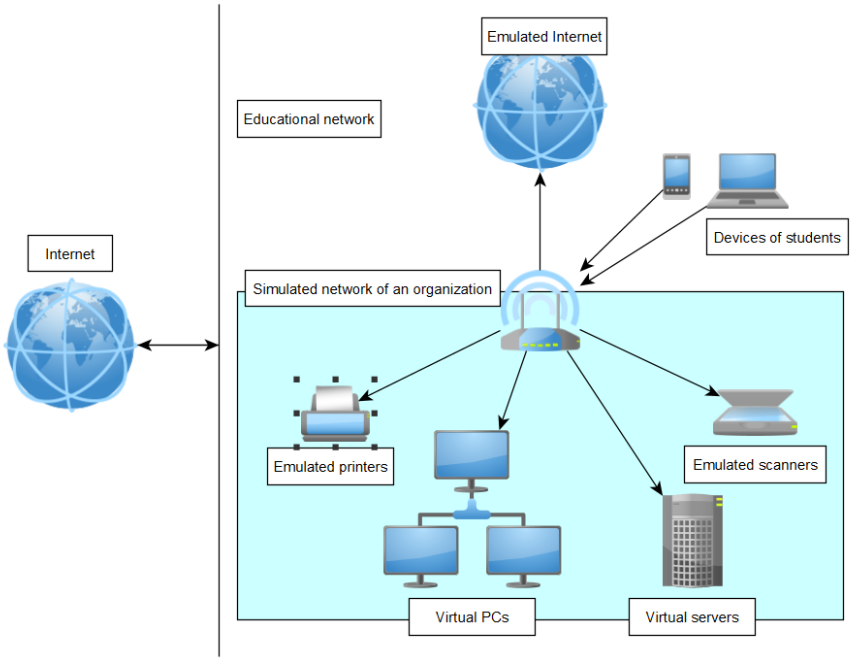
• Cyberattacks related to different jobs being simulated.

The first aspect is necessary so that education cannot be considered illegal in terms of legal and university regulations. The other points address the challenges of C2.1, C2.2, and C2.3.

Hardware architecture

The architecture plan I have defined is illustrated in Figure 4. All the elements in the framework are in a network for teachers/instructors which has no connection with the outside world, i.e. the internet. Central to the architecture is a wireless router that connects all elements of the system. Students can connect their own infocommunication devices, and relevant IT elements are also part of the organisational infrastructure: printers, scanners, servers and personal computers. The devices associated with the organisation are emulated, so there is no need for them to exist, it is enough just to use their software counterpart, which makes it look as if they are present. For the design of servers and personal computers, a private cloud-based virtualisation should be created, which can be used to integrate any number of machines into the framework. Finally, an important added value is the role of the emulated internet with the architecture, in which copies of several known websites (e.g. google.com, facebook.com, etc.) can be hosted by the system and made available to the students involved in the simulation.

Figure 4. Hardware architecture.



Simulation of cyberattack at the hardware level

To implement an infrastructure-level attack, an external component must be connected to the instructor network or the simulated organisational network. A device connected to the instructor network may carry out attacks against the organisational network, such as port scanning, DDoS, and so on. A component connected to an organisational network may steal a MAC address (e.g., pretend to be a printer, thus stealing materials sent for printing), modify memory, delete server data, and so on.

Extensibility

Due to the characteristics of the network, it is easy to connect additional components to the system. Because of the private cloud-based solution, additional virtual elements can be added to the system. Virtual machines also make it possible to connect components, such as a USB stick, programmable mouse and keyboard, and interfaces.

Application level

The application level builds on the elements defined at the infrastructure level, that is it endows the existing personal computers and servers in the framework with software elements.

Default Applications

The main consideration in determining the level of application of the framework was the emergence of applications specific to public service tasks, and that cyberattacks typical of several different jobs should be feasible.

● Server components:

• Mail server;

• Working time register database;

• Document storage database;

• Web server for hosting organisational pages etc.

● Personal computer components:

• Windows Operating System;

• Browser applications (Chrome, Firefox, Internet Explorer);

• Mail client;

• Time and attendance application;

• Document editor, etc.

Cyberattack simulation at the application level

To implement an application-level attack, an external component should be connected to the instructor network or to the simulated organisational network. The device connected may then send phishing emails that link to a malicious page on the emulated internet or contain attached files that run malicious code on computers when they are opened. The component connected to the organisational network may be capable of SQL injection-type attacks to gain access to confidential documents, possibly personal data, and so on.

Expandability

Due to the fact that both personal computers and servers are in a virtualised environment, they can be easily expanded with extra features and applications. To build virtual

machines, so-called virtual images are required, which describe the operating system, hardware needs, and software application on a virtual machine. The virtual images can then be replicated and launched in a private cloud at the beginning of the simulation.

Cyber Attack Database

As mentioned earlier, the database of cyberattacks defines the execution of each type of attack in the simulated environment. To define a new attack type, the following parameters need to be specified as shown in Figure 5.

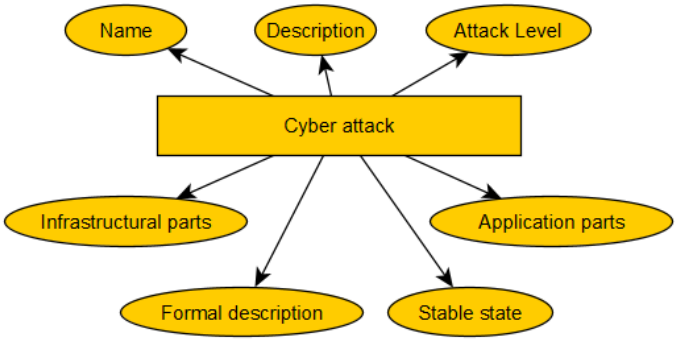


Figure 5. Properties of cyberattacks for the Simulation.

When designing a simulated environment, efforts should be made to make as many cyberattacks as possible, but of course this is not always the case. Due to the extensibility of the framework, it can be easily reconfigured for a specific case.

Simulation process

The process of the simulation is visualised in Figure 6 using an Activity Diagram defined by the UML standard. An activity diagram consists of activity nodes (represented by square boxes with inner labels), decision nodes (represented with diamonds with outer labels) and the control flow (represented by directed edges) between the activities and diamonds. Activities are executable actions, whereas the control flow defines the order between the execution of the activities (the activity at the beginning of the arrow must be executed before the activity at the end). The decision node is responsible for directing the control flow based on the current state of the system (in our case, the simulation framework) according to the question on its outer label. The activity diagram also identifies the first activity to be executed by the initial node (represented by the circle with solid border) and the final node (marked by the circle with bold border) which means the process is finished.

The infrastructure and application levels are first set. Due to the available applications and infrastructure elements, the selectable cyberattacks have to be filtered accordingly to make sure all the selected attacks can actually be executed. The selection process can be by manual instructor or random. It is also possible to parameterise how many such attacks will be executed. It is clear from the diagram that the simulation executes only one attack at a time and waits until the students have brought the system to a stable state that has been marked as the target state in the cyberattack database. If this is achieved, another attack will be executed. If there are no more attacks to execute, the process ends.

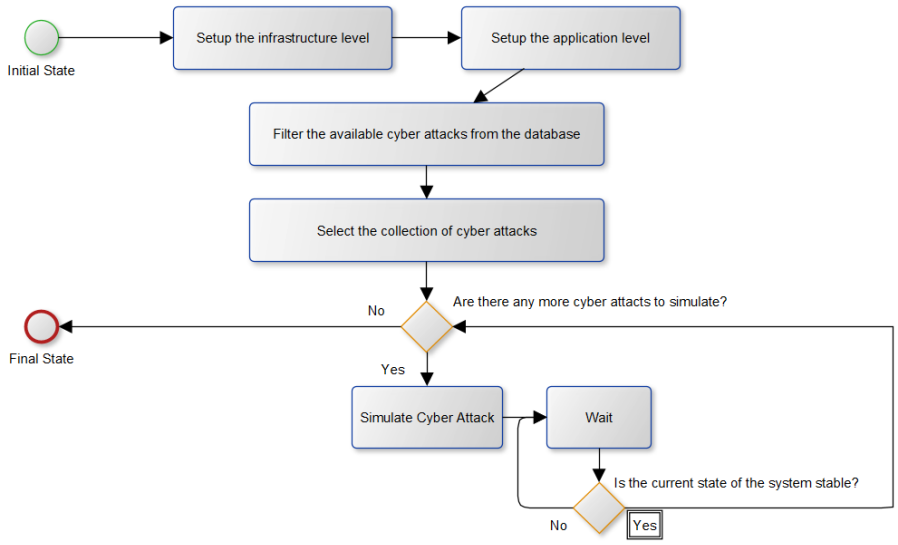


Figure 6. Simulation process.

Supporting distance learning during training

The current pandemic situation also proves that the implementation of distance learning is essential for the effective performance of practical education, which is significantly influenced by external, often unforeseen circumstances, as I have already identified in the case of challenge C2.5. That is why it is important for the educational environment to be prepared for the difficulties caused by such events. There are many solutions for transferring theoretical knowledge, from platforms that create virtual classrooms to video and file sharing to a variety of streaming applications, but it is important that hands-on sessions that were previously required to be held in person can be held online. The solution is to connect students via a virtual private network (VPN), which can be used to remotely access the simulation framework outlined earlier. The tasks in the simulation environment can be solved. In addition, students should be provided with tutorials and video files on the steps required to counter attacks on the dedicated e-learning portal. Furthermore, the instructor can help you understand and apply these materials by holding online lessons. With the help of these, students will be able to master the measures to prevent cyberattacks.

Automated assessment system

The automated assessment system and its characteristics are presented in this chapter to address the goal G3. The concept of the automated assessment system can monitor and evaluate student work even without instructor oversight. To make this happen, the C3.1 and C3.2 challenges need to be addressed by expanding the simulation framework.

Qualification and quantification of cyber defence measures

When assessing students, it is important to identify the grade based on the work performed, which requires the definition of clear and consistent metrics. Two such metrics can be distinguished to support the quantification requested by challenge C3.1:

1. Number of cyberattacks prevented: during the simulation, the student must prevent more cyberattacks. The more attacks the student managed to prevent, the more points the student scored during the audition.

2. Number of sub-states reached during a cyberattack: during the simulation, the student must prevent a complex cyberattack, but the student can also receive a point for a partial solution.

Metric 1) can already be implemented with the current simulation framework; however, the application of the 2) metric requires the extension of cyberattack descriptors with additional state definitions that determine whether the system has reached a state that corresponds to a sub-solution. In addition, there is a limited amount of time available to students during examinations, so the cyberattack descriptor should be extended with this information, as shown in Figure 7.

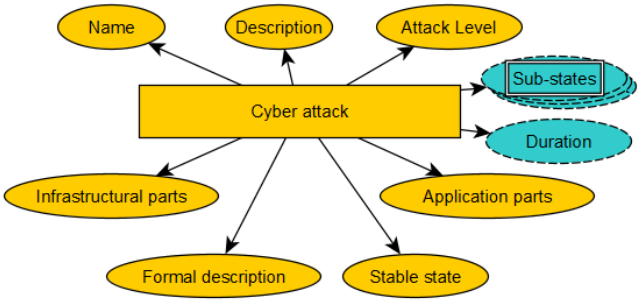


Figure 7. Extended properties of cyberattacks for the Simulation.

The simulation process must be extended with new decision and implementation elements to reflect the proposed behaviour, as shown in Figure 8 (the figure shows only the lower, expanded part of the previous full process diagram):

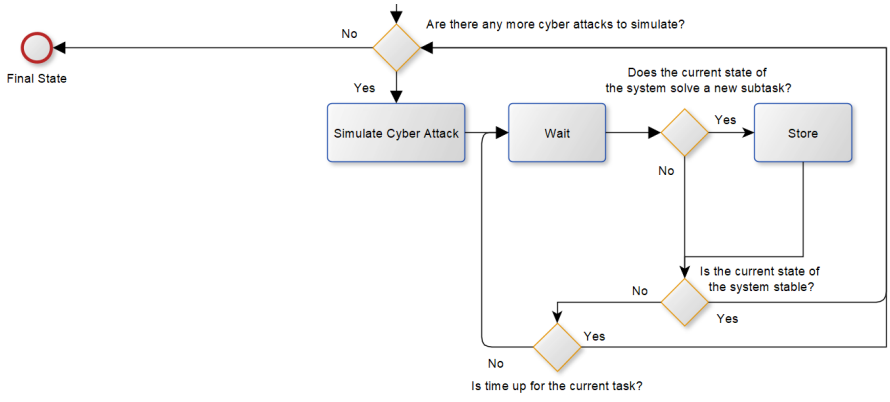


Figure 8. Extended simulation process.

After performing the "waiting" action, we need to check if the system has reached a new partial state (and then the student can get a new point). If it is in a new state, this is saved so that the next time we can check if the student has found another state. After that, we check to see if the system is in a stable state, because if it is, it means that the particular attack was successfully dealt with. If not, we check if the time allocated for that task has expired. When the system is in a stable state or the time has elapsed, we jump to the next task (if there is still another task to execute).

Storage and replay of protection measures

The purpose of storing and replaying the protection measures executed by the student is to make the number of points obtained for the given task identifiable to both the instructor and the student after solving the exam task. In addition, it allows the instructor to perform the actions after solving the exam task as the student did before. The instructor

is therefore allowed to identify individual deficiencies, errors, and any points in question. If the student does not agree with the scores obtained, the specific measures taken to prevent the cyberattack will be tracked due to the storability and re-enforceability.

During storage, the framework makes sure that all commands and actions are logged. A simple solution is for students to create documentation by placing screenshots, or a more sophisticated, higher-level solution for logging all operating system-specific instructions issued from the student machine. The latter solution, while providing a much more accurate replay option, requires a much greater investment of time and effort on the part of the instructor.

Conclusion

In the present study, I sought solutions to the following three main objectives and they were prepared and presented in detail in the previous chapters.

The first goal was to define the structure and elements of the two-stage practical training, as well as the cyber defence mechanisms and knowledge to be transferred. At first, I presented the knowledge to be acquired during public service cybersecurity training, which I identified in a previous study with the help of the set of knowledge fixed for positions related to cybersecurity in the NICE Framework and the good practices discovered during the mapping of international training programmes. Next, I outlined the structure of the training, based on which students can acquire the previously presented set of knowledge during a theoretical and a practical part. In the theoretical half of the course, students can acquire basic IT skills, cybersecurity and data protection legislation, basic concepts, the structure of the state cyber protection system, and positions of cybersecurity and data protection within the organisation. They will also learn about the different types of cyberattacks, attack techniques and methods for preventing and combatting them, learn the methodology of risk management, and explore the role of the human factor in cybersecurity and their interfaces. During the practical part of the training, theoretical and practical knowledge can be combined by simulating specific attacks based on existing knowledge. As a result, students will be able to recognise threats and potential risks from cyberspace.

During this two-stage practical training, students first become familiar with the defence mechanisms of their own infocommunication devices and then perform attack prevention in a simulated, organisational-level environment. Students will learn about the structure of workplace devices and the information system, their vulnerabilities, related operational tasks and, in a simulated organisational environment, experience cyberattacks that threaten the information infrastructure, and become familiar with what preventive and protective measures can be used to prevent these attacks.

The second goal was to define a framework that describes the simulation environment. To address this goal, I divided the framework into application and infrastructure layers, and identified the database of cyberattacks that form the basis of the framework. I outlined the hardware architecture of the framework and presented its components and the simulation of cyberattacks to the hardware and application level. I defined the specific process of the latter and then examined how distance learning can be implemented in such a simulation environment.

The third main goal of the study was to define a possible assessment system for practical education in a simulation environment. The goal was to create an automated assessment system that could monitor and evaluate students' work even without instructor supervision. I defined the grade based on the work performance by defining clear and consistent

metrics. One such metric is the number of cyberattacks eliminated, while the other is the number of sub-states reached. To apply the latter, it was necessary to extend the cyberattack descriptors with additional state definitions that determine whether the system has reached a state that corresponds to a sub-solution.

In the future, work will be necessary to define the formal language for describing the execution of the cyberattacks. In addition, an overall budget estimate of the framework should be carried out to identify the material conditions for setting up such a framework. In order to examine the operation of the framework, it is essential to perform a student usability test, during which it is possible to determine how the framework works in a real situation and whether it can be used during specific training. Finally, it is important to identify potential threats when connecting the infocommunication devices of the students and to identify measures to address these threats.

Funding

This research received no external funding.

Data Availability Statement

Not applicable.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Beuran, R., Tang, D., Pham, C., Chinen, K. I., Tan, Y., and Shinoda, Y. (2018) 'Integrated framework for hands-on cybersecurity training: CyTrONE', *Computers & Security*, 78, pp. 43–59. doi: 10.1016/j.cose.2018.06.001.

Dimkov, T., Pieters, W., and Hartel, P. (2011) 'Training students to steal: a practical assignment in computer security education', in *Proceedings of the 42nd ACM technical symposium on computer science education*, pp. 21–26. doi: 10.1145/1953163.1953175.

Krasznay, Cs. (2017) 'A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban', *Nemzet és Biztonság: Biztonságpolitikai szemle*, 10(3), pp. 38–53.

Morgan, S. (2017) 'Cybersecurity Jobs Report: A Special Report From the Editors at Cybersecurity Ventures', *Cybersecurity Ventures*, 31 May 2017. Available at: https://bit.ly/3vnbwcR (Accessed: 20 September 2020).

Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2017) 'National initiative for cybersecurity education (NICE) cybersecurity workforce framework', *NIST Special Publication*, 800(2017), p. 181. doi: 10.6028/NIST.SP.800-181.

Patriciu, V. V. and Furtuna, A. C. (2009) 'Guide for designing cybersecurity exercises', in *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy.* World Scientific and Engineering Academy and Society (WSEAS), pp. 172–177.

Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., and Askwith, B. (2016) 'Cybersecurity teaching and learning laboratories: A survey'. *Information & Security*, 35(1), 51. doi: 10.11610/isij.3503**.**

Willems, C. and Meinel, C. (2012) 'Online assessment for hands-on cybersecurity training in a virtual lab', in *Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON),* pp. 1–10. doi: 10.1109/EDUCON.2012.6201149.