Cybersecurity Fundamentals

GUIDE

Co-funded by the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The handbook is one of the results of the Erasmus+ project 'Cybersecurity Fundamentals'.

Project coordinator:

Lipinski University in Kielce, Poland

Partners:

Ambis vysoká škola, Prague, Czech Republic

Instituto Politécnico de Beja, Portugal

Co-funded by the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

What is this publication?

This is a handbook for the course/semester instructor to use the collection of online materials found on the Cybersecurity Fundamentals platform. The handbook will also be useful for students, especially those studying on their own.

The materials were developed as part of the project 'Cybersecurity fundamentals', funded by EU funds under the Erasmus+ programme, from 2019 to 2022. The project was coordinated by the Prof. Edward Lipinski Academy of Applied Sciences in Kielce, and the partners were universities from the Czech Republic and Portugal.

The online materials (video lectures, subject-specific textbooks, instructional videos) are designed to enhance understanding of the broad context of cyber security and develop skills to deal with different types of threats. The whole can be adapted to different educational contexts, depending on the needs.

The publication provides detailed materials and guidance for conducting blended learning or online workshops.

The choice and order in which the topics are presented should be tailored to the needs of the specific group of participants and is therefore up to the individual class or course leader. There is no requirement to conduct all modules or to conduct them in exactly the order suggested in this resource.

Who is this publication for?

This publication is intended for academics and trainers in computer systems security. A flexible approach is suggested: the course can be integrated into existing curricula or offered as a stand-alone training course. Although the material is intended for the higher education sector, it will also be useful for those training working people. Geographically, the immediate context of the resource is audiences in the partner countries, but due to the transnational approach and the nature of the issues presented, the material is easily adaptable to the needs of educators in other countries.

What are the objectives of this publication?

The key beneficiaries of the 'Fundamentals of Cyber Security' project are students of various faculties, as it is difficult today to find a field of life in which the threat of attacks on IT systems is not an issue. The course is recommended especially for students of majors such as homeland security, as cyber-attacks on various institutions today are incomparably more frequent (and more profitable) than physical attacks. The aim of this publication is to help the course/class leader to select from the numerous online materials proposed those that are useful for his/her group of students and to conduct *blended learning activities* (classroom activities and independent online work by the student) or completely *online*. In the case of *blended learning, it* is advisable to use the *flipped classroom* method where students come to class having read the pre-set online material.

Pedagogical approach

"Knowledge is created by students".

The course adopts Kolb's (1984) approach to experiential learning. According to Kolb's Cycle, a cycle of four steps is repeated in the learning process: experience, reflection, generalisation and application.

The training of cybersecurity professionals relies exceptionally heavily on experiential learning - by experiencing increasingly difficult tasks while developing knowledge and skills.

In all the activities proposed for use in the classroom, we try to show the relationship of the topic under discussion to the daily working practice of the course participants in order, in accordance with the principles of Human Centered Design, to provide them with an engaging training experience.

Notes for the trainer

Instructor notes are based on the content of the online modules and follow the order of the modules on the platform. Each session is expected to last approximately two lesson hours. A description of the hourly load is included in the syllabus of each module. Sessions may also be extended or shortened with appropriate changes to materials and topics.

Equipment and materials

The equipment and materials needed for each workshop are generally available in the higher education sector. These include a computer room suitable for interactive group work, projector, screen, internet access, speakers, flipchart, pens, etc.

Use of the course

Go to: https://moodle.cybersecurity-fundamentals.eu/.

Select the course language and module.

Select a status (possible to log in as a 'Guest', but this will restrict access to some material and functionality). It is possible to create an account yourself and to log in with a Google or Microsoft account.

This teacher's manual concerns the Polish version.

The course materials can be used sequentially or selectively as required.

Information for universities

Any university can easily host the course on their server and use it to educate their students. The LMS of the course is Moodle, a popular free open-source e-learning platform. The course is also free of charge.

Interested universities are invited to contact us at: erasmus@wsepinm.edu.pl . Those wishing to do so will receive a packaged course that they can run on their own server within minutes. This applies not only to the Polish, but also to the English, Czech and Portuguese language versions. We would particularly like to draw your attention to the possibility of using the English version of the course to teach in this language, which is difficult to navigate in cyberspace, if only because of the prevalence of English terminology.

Course content

The teaching content of the course is organised in the following modules:

Module 1

Basics of networking

1. Introduction

1.1 Summary of the module

The module focuses on the basic concepts of computer networks (e.g. protocols, addresses, topologies, etc.) and is intended for those who have not had any previous exposure to the subject of computer networks. Computer science students will probably be able to skip this module.

1.2 Course objectives

The module aims to introduce the basic concepts of network fundamentals. It is intended for people who have not yet been exposed to the topics of network configuration, protocols, network topology, etc.

On completion of the course in the blended learning method, the student should have acquired the ability to set up a simple local area network, connect it to the Internet, test network performance, troubleshoot faults.

The knowledge gained in this way is necessary to understand what the internet is and the dangers of just being connected to the network.

1.3 Course content

The individual lectures introduce students to the physical layer and the logical layer of the network. Students are introduced to the concepts of protocols, data packets, physical and logical addresses and basic network services.

1.4 Learning objectives

- Gain basic knowledge of computer networks, network infrastructure.
- Familiarisation with LAN, MAN, WAN network architecture.
- Familiarisation with the 7-layer ISO/OSI model
- Familiarisation with the TCP/IP network value model. Knowledge of the basics of TCP and UDP protocols.
- Knowledge of the basics of VoIP communication.
- Understanding the issue of network performance. Familiarisation with methods of reducing network traffic.
- Use of computers, digital tools and computer networks, including knowledge of the principles of digital devices and computer networks and performing basic computer network tests.

1.5 Syllabus

Learning effect	Students who have passed the subject knows/knows/can:
	NEWS
W1	Characterises network/server services
W2	Has a broad, structured knowledge of the services and applications used in computer networks. Is familiar with network operating systems
W3	Has knowledge of network equipment configuration
W4	Has knowledge of the risks in computer networks. Understands the importance and role of selected network protocols with attribution to specific reference model layers
W5	Has knowledge of computer network design and its components
W6	Describes and analyses IP address classes
W7	Can name the ISO/OSI layers
W8	Recognises local area network topologies
W9	Knows the TCP/UDP port addresses
W10	Knows the concepts related to: administration and management of computer networks
W11	Knows the principles of network equipment
	SKILLS
U1	Describes and analyses IP address classes
U2	Connects the local computer network to the Internet
U3	Be able to analyse traffic in computer networks. Can configure network addressing and selected security elements.
U4	Able to configure basic network devices. Knows and can use a simulation tool in the analysis and design of computer networks.
U5	Able to configure web service servers
U6	Be able to configure a workstation to work in a network
U7	Can check network performance
U8	Be able to design a local area network
U9	Be able to build a simple local area network using actual network equipment. Can independently prepare structured cabling.
U10	Able to remotely manage workstations on the network
U11	Designs the IP address structure in the network
U12	Recognises and applies standards for structured cabling
U13	Recognises local area network protocols and wide area network access protocols
U14	Recognises network devices (description, symbol, appearance)
U15	Performs measurements and tests of the logical network
	SOCIAL COMPETENCES
K1	Describes the configuration of network interfaces
K2	Be able to identify priorities for action
K3	Able to work and interact in a group as far as the configuration of addressing and selected network services is concerned.
K4	Able to work in a team, solve tasks together
K5	Explains the principles of computer network protocols

Content of the module (programme of lectures and other activities)		Reference to learning outcomes
LECTURES 1. Physical network structure, types of network equipment, cables 2. Data units in networks 3. Logical network structure, topologies 4. ISO/OSI, TCP/IP models 5. Discussion of the use of layers WORKSHOPS 1. Creation of a physical network 2. Network configuration 3. Network survey 4. Network connection to the internet		W 1-11 U1-15 K1-5
ECTS credit balance		
Form of student workload		Number of hours
Number of hours with direct participation of academic teacher		
1.1	Participation in lectures	6
1.2	Participation in seminars	
1.3	Participation in workshops	30
1.4	Participation in laboratory activities	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times per semester)	
1.7	Participation in the project consultation	
1.8	Participation in examinations/tests	2
1.9	Other ...	
1.10	**Number of hours spent with direct assistance of academic staff (sum 1.1 - 1.9)**	38
1.11	**Number of ECTS credits obtained by the student in classes requiring direct participation of an academic teacher)**	1,5
Individual student work		
2.1	Individual studies (including e-learning lectures)	10
2.2	Individual preparation for workshops	10
2.3	Individual test preparation	
2.4	Individual preparation for laboratory classes	
2.5	Preparation of reports	
2.6	Implementation of self-performed tasks (projects, documentation)	
2.7	Preparation for the final examination/tests of the workshop	10
2.8	Preparation for final examination/testing of lectures	
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 - 2.9)**	30
2.11	**Number of ECTS credits obtained by the student in individual teaching assignments**	1
Total workload (h)		**68**
ECTS credits for the module		**2,5**

Methods of verifying learning outcomes									
Learning outcome	Forms of assessment								
	Oral examination	Written examination	Partial written assignment	Final written assignment (essay	Test	Design/presentation	Report	Classroom activities	Other ...
NEWS									
W1-11					x			x	
SKILLS									
U1-15					x			x	
COMPETENCES									
K1-5								x	

Criteria for assessing student competence
The minimum requirements for the three groups of learning outcomes that a student must achieve in order to pass the subject are summarised below. In order for a student to pass a module, all learning outcomes described in the syllabus must be positively verified by the person(s) teaching the module.

W - KNOWLEDGE
Assessment:
Satisfactory - The student remembers and reproduces the knowledge to be mastered within the module.
Good - Student additionally interprets phenomena / problems and is able to solve a typical problem
Very good -Student is able to solve even complex problems in a given field, is able to synthesise, carry out a comprehensive evaluation, create a work that is original and inspiring to others.

U - SKILLS
Assessment:
Satisfactory - The student knows the nature of the activities and is able, under the guidance of the academic teacher, to carry out activities / solve problems related to the content of the module
Good - Student is able to independently carry out activities / tasks / solve typical problems related to the content of the module
Very good - The student has fully mastered the ability / skill to perform the activities / tasks / problems provided for in the module content, also in more complex cases.

K - SOCIAL COMPETENCE
Assessment:
Satisfactory - Student passively assimilates module content, demonstrating ability to concentrate and listen
Good - Student actively participates in classes, makes value judgements according to the criteria accepted in the given field, can actively cooperate in a group
Very good - The student integrates the attitude according to the proposed model, develops his/her own system of professional and social values, is able to take responsibility for the actions of the group, including leadership.

2. Basic materials for the teacher

Definitions (glossary)

Computer network - A collection of devices, such as computers, printers, telephones and televisions, that are interconnected to exchange data. A transmission medium is used to connect the devices and a communication protocol is used to transmit data.

IPv4 address - This is a 32-bit number, entered in decimal form for ease of use (e.g. 192.168.31.190), to identify devices and address data
on the network.

HOST - This is a device with an IP address that is the source or recipient of data transmitted over the network, i.e. it receives data from other devices or sends such data. The term host is sometimes used interchangeably with the term terminal device, as it usually refers to a computer, tablet or smartphone, i.e. a device with which the network user has direct contact.

Client - The device, or more precisely its software, uses the services provided by the server. The most common client today is the web browser, which allows the content of web pages hosted by a web server to be viewed. Examples of a client would also include FileZilla, which allows files to be exchanged over the Internet, and all sorts of email software to facilitate the use of mail. Game consoles or smartphones will also be clients, as long as they are connected to the Internet, of course.

Server - This is a computer with dedicated specialised software installed to serve other computers. The service that a server can provide is, for example, a website, email or file resource. A server can be any computer on which such software is installed and configured, such as APACHE, which is used to maintain and share websites, or MySQL, which is a database management system. A server is usually a dedicated computer with high computing power that is capable of handling many connections and queries simultaneously.

Transmission medium - In other words, the medium that is the network element through which devices communicate with each other and exchange data. This medium can be copper cable, fibre optic cable and radio waves (WiFi).

Communication protocol - This is the method or language of communication and data exchange between devices that defines the rules and principles of that communication.

Internet - It is a set of interconnected wide area networks that form a global computer network. The origins of the Internet can be traced back to the creation of the ARPANET network in the late 1960s, and the first Internet connection in Poland was launched in September 1990. The Internet is seen by many as a collection of sites to browse, but this is not the case as the Internet is a collection of many wide networks spread across the globe and websites are specific network services.

Intranet - This is a private internal network that uses exactly the same communication standards (protocols) as the Internet, but only has access to authorised users, such as employees of a particular company. In most cases, access to an intranet, or this internal company network, is via a website, so communication is said to use the same standards as the Internet.

Extranet - is an extensive variety of intranets that allow access to its resources not only to the employees of a given company, but also to other users.

DNS (Domain Name System) - A network service whose task is to change a human-readable name, the so-called mnemonic name, to the IP address of a device on the network. It is a

basic service of the Internet, changing the addresses of websites to the corresponding IP addresses of the servers where these websites are stored, e.g. changing the internet address onet.pl to IP address 214.180.141.140.

DHCP (Dynamic Host Configuration Protocol) is an automatic configuration protocol that assigns an IP address, subnet mask or default gateway address to a host. It is the most common method of assigning IP addresses to computers on a network, as it does not require manual IP address configuration on each computer.

3. During classes

Some ideas for activities:

WORKSHOPS

With the students, set up a local network in the studio and connect it to the internet.

Together with the students, install an RJ45 connector on the UTP cable and check the cable's performance.

REVIEW QUESTIONS

- Which protocols are used for email and which for websites?

- Name the 7 layers of the ISO/OSI model?

- What is a MAC address and what is an IP address?

- What do the terms encapsulation and decapsulation mean?

- How does IPv4 differ from IPv6?

- What are the main advantages and disadvantages of fibre optics compared to twisted pair cables?

WORKING IN PAIRS/GROUPS

'Deaf phone' scenario in different network configurations:

1. Divide into groups: Divide participants into groups, each group should consist of at least three people.

2. Linear configuration: In the first configuration, the network should be set up in a linear way. The first person in the group comes up with a short sentence and then passes it to the next person via a 'dumb phone'. The last person in the group passes the sentence aloud. Compare the sentence received with the original one and discuss with the participants how the message has changed.

3. star configuration: In the second configuration, the network should be set up in a star way. Choose one person to be the start of the sentence handover. This person passes the sentence to one person, who passes it to the next person and so on until all the people in the group have heard the sentence. Compare the sentence received with the original sentence and discuss with the participants how the message has

changed.

4 Grid configuration: In the third configuration, the grid should be set up in a grid fashion. Each person in the group should have two neighbours and pass the sentence to one of them. See how the sentence changes as it passes through different people and discuss this with the participants.

After each grid configuration, discuss with the participants what lessons can be learned from this exercise in the context of computer network topology. Examples of questions to ask are:

- How do different network configurations affect the quality of information transmission?
- What problems can occur with different network configurations?
- What are the benefits and disadvantages of different network topologies in the context of information transfer?

TOPICS FOR DISCUSSION

- Who owns the internet, who controls it?
- What are the risks of open access to the web?
- Should there be more control over content appearing on the internet? Who should do so?
- What other networks besides computer networks can be recognised? How does the approach to privacy change depending on the size of the network and other factors?
- Can a restaurant be an example of a chain? What are the roles of customers, waiters, cooks? What do the protocols and data packets look like?

4. **Internet resources**

https://learn.microsoft.com/pl-pl/training/modules/network-fundamentals/
https://www.icann.org/
https://isportal.pl/
https://www.speedtest.net/
https://www.intgovforum.org/
https://www.whatismyisp.com/
https://uke.gov.pl/

5. Additional questions/tests

What does VoIP stand for?
A. Voice on Internet Protocol
B. Vice over Internet Protocol
C. Voice over Internet Position
D. Voice over Internet Protocol

The first 'technical' cybercriminal was Leonard Kleinrock, who in 1973 sent a message via ARPANET regarding:
A. his missing electric razor.
B. his girlfriends
C. the desired textbook
D. songs

What is the name of the programme that acts as a telephone exchange?
A. IP-PBX
B. CVoIP
C. Skype
D. MS Teams

Which of the following programmes does not use VoIP technology?
A. MS Teams
B. Zoom
C. Google Meet
D. Photoshop

What is the Asterix programme?
A. SIP server
B. file server
C. photo server
D. file compressor

Which of the following does not affect the performance of the computer network?
A. Passive parts of a computer network
B. active devices
C. electromagnetic interference
D. atmospheric pressure

What material is the twisted-pair cable made of?
A. copper
B. aluminium
C. steel
D. fibreglass

Category 5 twisted-pair network cable provides transmission up to a maximum of:
A. 1 Gbps
B. 100 Mbps
C. 1 Mbps
D. 10 Gbps

Which medium carries data over a greater distance?
A. optical fibre
B. copper cable (twisted pair)
C. steel cable
D. aluminium cable

What is a HOST in a computer network?
A. any device connected to the network
B. host
C. a central device in a computer network
D. external drive

What is a network card?
A. a device that allows a host to connect to a computer network
B. part of the main processor
C. power supply device
D. SSD

Which program can be used to measure download speeds on a computer network?
A. wget
B. ping
C. MS Teams
D.

The web address through which you can check your network performance is:
A. speedtest.net
B. google.com
C. yahoo.com
D. google.net

A home network router can be used to:
A. restrict network traffic
B. search for information
C. video surveillance
D. mp3 playback

By typing "CMD" in MS Windows 10/11 in the search window, we will run:
A. command line
B. network card configuration
C. calculator
D. file compression program

What is the ping programme used for?
A. indicates the response time to the packet sent
B. changes the time of the system
C. displays the help manual
D. closes all programmes

Which program returns a list of consecutive routers along the route to the destination computer on the network?

A. Tracert

B. wget

C. ping

D. span

Module 2

Law and other regulations

3. Introduction

1.5 Course summary

The course focuses on basic legal concepts related to the Internet and introduces the student to the topic of liability in cyberspace. A knowledge of the legal foundations of an Internet Service Provider (ISP) is also necessary to understand the entire subject. A significant part of the course covers cyber security and the corresponding legal provisions. In addition, the protection of personal data in cyberspace cannot be overlooked. Privacy and security in ICT and data protection in cyberspace are also key topics that form an essential part of the course.

1.2 Course objectives

Students will learn about the relationship between law and cyberspace. They will be familiar with the legal basis of Internet Service Providers (ISPs). For their studies, they will additionally focus on cyber security and its regulation. In addition, students will study the information security management system. Finally, they will discover the importance of data protection in cyberspace.

The aim of the module is to familiarise students with the application of the law in the field of information and communication technologies. An additional objective is to identify the legal boundaries of cyber security.

At the end of the course, the student should have acquired the ability to orient himself/herself in the legal norms of the European Union and the participating countries that are directly related to the issue of cyber security.
In addition, the student will gain a basic overview of civil and public law issues that are used in cyberspace, with a particular focus on the practical application of the acquired knowledge in practice. The student will not only be introduced to the theory of the application of the law in cyberspace and the de lege lata regulation, but also to the practical application of the law in practice (de lege aplicata).

The knowledge gained will be further applied in modules on cyber-attacks and how to defend against them, as well as a module on building and operating security teams.

1.3 Course content

The individual lectures introduce students to the legal system in question, the legal norm, the law and the Internet. In addition, students are introduced to liability in cyberspace and the legal basis of Internet Service Providers (ISPs). One of the key topics is cyber security and its legal regulation. Privacy and related security in ICT, data protection in cyberspace are also extremely important, which is why the last part of the lectures is devoted to them.

1.4 Learning objectives

1) Introduction to the subject of the legal system, the legal norm, the law and the Internet
2) Responsibility in cyberspace
3) Understand the legal basis of the ISP (Internet Service Provider) business
4) Protection of personal data in cyberspace
5) Privacy and security in ICT, data protection in cyberspace

3.5 Equipment and materials required

Laws and regulations on cyber security - available online

EU primary law

- Charter of Fundamental Rights of the European Union

Directives of the European Parliament and of the Council

- 91/250/EEC on the legal protection of computer programs
- 98/34/EC on a procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/EC
- 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity
- 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
- 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)
- 2002/20/EC on the authorisation of electronic communications networks and services (Authorisation Directive), as amended by Directive 2009/140/EC
- 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC
- 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)
- 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
- 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
- 2008/114/EC on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection
- 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA
- 2013/11/EU on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on alternative dispute resolution for consumer disputes)
- 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
- 2015/1535 on the procedure for the provision of information in the field of technical regulations and rules on information society services
- 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC ("the revised Payment Services Directive")
- 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, on the free movement of such data and repealing Council Framework Decision 2008/977/JHA

- 2016/1148 on measures for a high common level of security for network and information systems in the European Union (NIS)

Regulations of the European Parliament and of the Council

- 460/2004/EC establishing the European Network and Information Security Agency as amended by Regulation No 1007/2008
- 1077/2011/EC establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
- 526/2013 on the European Union Network and Information Security Agency (**ENISA**) and repealing Regulation (EC) No 460/2004 Text with EEA relevance
- 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (**eIDAS)**[1]
- 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - **GDPR**)

Council of Europe decisions

- 92/242/EEC in the field of information systems security
- **2005/222/JHA on attacks against information systems**
- 2011/292/EU on the security rules for protecting EU classified information

Other documents

- Council of Europe Convention 185 on Cybercrime
- Council of Europe Additional Protocol 189 to the Convention on Cybercrime
- Council of Europe Convention 196 on the Prevention of Terrorism
- Commission Implementing Regulation (EU) 2018/151 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further clarification of the elements that digital service providers should take into account when managing risks to the security of networks and information systems, and the parameters for determining whether an incident has a significant impact

International standards

- ISMS ISO/IEC 27000 Series

Other

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the digital single market in services (Digital Services Act) and amending Directive 2000/31/EC
- Private and public liability for user or company actions in the online environment
- Characteristics and definition of the different ISPs and their cyber security rights and obligations
- ISMS and the relationship to cyber security law

[1] Hereinafter referred to as '**eIDAS'.**

1.6 Syllabus

Learning outcome	The student who successfully completes the module will know/be competent in the following.
NEWS	
W1	The student will acquire professional knowledge and broaden his/her legal awareness of information and communication technologies.
W2	The student will acquire professional knowledge related to the legal definition of cyber security according to international law (in particular EU law) and the national law of the participating countries.
SKILLS	
U1	He is able to identify the different ISPs, their rights and obligations and, based on this identification, is able to argue areas of law related to cyber security.
U2	Be able to analyse the basic framework of assets in cyberspace (e.g. technologies, processes, data, etc.) and identify legal recommendations for their protection.
COMPETENCES	
K1	The student partially masters the legal provisions, is able to apply the individual legal institutes to the case-studies.

Content of the module (programme of lectures and other activities)	**Reference to learning outcomes**
LECTURES 1. International legal standards governing cybercrime 2. National legal standards governing cybercrime WORKSHOPS 1. Analysis of individual cyber-attacks and their subsumption under the provisions of the Cybercrime Convention (ECJ No. 185) and national law (Czech Republic, Poland, Portugal)	W1, W2 U1, U2, K1

ECTS credit balance		
Form of student workload		Number of hours
Number of hours with direct participation of academic teacher		
1.1	Participation in lectures	6
1.2	Participation in seminars	
1.3	Participation in workshops	14
1.4	Participation in laboratory activities	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times per semester)	
1.7	Participation in the project consultation	
1.8	Participation in examinations/tests	2
1.9	Other ...	
1.10	**Number of hours spent with direct assistance of academic staff (sum 1.1 - 1.9)**	22
1.11	**Number of ECTS credits obtained by the student in classes requiring direct participation of an academic teacher)**	1
Individual student work		
2.1	Individual studies (including e-learning lectures)	25
2.2	Individual preparation for workshops	10

2.3	Individual test preparation	
2.4	Individual preparation for laboratory classes	
2.5	Preparation of reports	
2.6	Implementation of self-performed tasks (projects, documentation)	
2.7	Preparation for the final examination/tests of the workshop	5
2.8	Preparation for final examination/testing of lectures	5
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 - 2.9)**	45
2.11	**Number of ECTS credits obtained by the student in individual learning activities**	1,5
Total workload (h)		**67**
ECTS credits for the module		**2,5**

Methods of verifying learning outcomes

Learning outcome	Forms of credit classes								
	Oral examination	Written examination	Partial written assignment	Final written assignment (essay	Test	Design/presentation	Report	Classroom activities	Other ...
NEWS									
W1		x	x		x			x	
W2		x	x		x			x	
SKILLS									
U1						x			
U2						x			
COMPETENCES									
K1								x	

Criteria for assessing student competence
The minimum requirements for the three groups of learning outcomes that the Student must achieve in order to pass the subject are presented below in synthetic form. In order for the Student to pass the module, all learning outcomes described in the syllabus must be positively verified by the person(s) teaching the module.

W - KNOWLEDGE
Assessment:
Satisfactory - The student remembers and reproduces the knowledge to be mastered within the module.
Good - The student additionally interprets phenomena / problems and is able to solve a typical problem
Very good -Student is able to solve even complex problems in a given field, is able to synthesise, carry out a comprehensive evaluation, create a work that is original and inspiring to others.

U - SKILLS
Assessment:
Satisfactory - The student knows the nature of the activities and is able, under the guidance of the academic teacher, to carry out activities / solve problems related to the content of the module
Good - Student is able to independently carry out activities / tasks / solve typical problems related to the content of the module
Very good - The student has fully mastered the ability / skill to perform the activities / tasks / problems provided for in the module content, also in more complex cases.

K - SOCIAL COMPETENCE
Assessment:
Satisfactory - Student passively assimilates module content, demonstrating ability to concentrate and listen
Good - Student actively participates in classes, makes value judgements according to the criteria accepted in the given field, can actively cooperate in a group
Very good - The student integrates the attitude according to the proposed model, develops his/her own system of professional and social values, is able to take responsibility for the actions of the group, including leadership.

Form of student workload		Number of hours
Number of hours with direct participation of academic teacher		
1.1	Participation in lectures	6
1.2	Participation in seminars	
1.3	Participation in workshops	14
1.4	Participation in laboratory activities	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times per semester)	
1.7	Participation in the project consultation	
1.8	Participation in examinations/tests	2
1.9	Other ...	
1.10	**Number of hours spent with direct assistance of academic staff (sum 1.1 - 1.9)**	22
1.11	**Number of ECTS credits obtained by the student in classes requiring direct participation of an academic teacher)**	1

Individual student work		
2.1	Individual studies (including e-learning lectures)	25
2.2	Individual preparation for workshops	10
2.3	Individual test preparation	
2.4	Individual preparation for laboratory classes	
2.5	Preparation of reports	
2.6	Implementation of self-performed tasks (projects, documentation)	
2.7	Preparation for the final examination/tests of the workshop	5
2.8	Preparation for final examination/testing of lectures	5
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 - 2.9)**	45
2.11	**Number of ECTS credits obtained by the student in individual teaching assignments**	1,5
Total workload (h)		**67**
ECTS credits for the module		**2,5**

2. Basic material for the teacher

Definitions (glossary)

Natural law *(ius naturale)* - exists independently of the state. It arises and develops in society. It generally encompasses a set of rules corresponding to the achieved level of development of society.
Positive law *(ius positivum)* - is legislated by the state or system of government. Positive law is therefore predetermined. It consists of predictable rules that are enforced, i.e. whose violation is punished.
Law - (or objective law) - a set of legal norms as generally applicable rules of conduct established or recognised and enforced by the state.
Right - the possibility for legal entities to behave as guaranteed by a legal norm. A right usually corresponds to a legal obligation of another legal entity.
Structure of the legal norm - consists of three parts, which are the **hypothesis, the disposition** and **the sanction**.
Dispositive legal norm - does not set out a basic rule of conduct at all, or sets it out only as a possibility. It leaves the determination of the rules to the addressees. If the addressees do not do so, the rules in the norm serve as a guide for the judge to know how to decide.
Cognitive legal norm - sets out the applicable rule of conduct. It leaves no room for the will of the addressee.
Entitlement **norms** - legal norms explicitly formulate only entitlements.
Binding norms - legal norms expressly formulate an obligation, in the form of an injunction or prohibition.
Public norms - legal norms apply where public power is exercised. Public power is exercised by the state through the offices of the legislature, the executive and the judiciary. We see public law as a field of law where relations are based on inequality of parties, where one party represents the public authority acting against private individuals by means of orders, prohibitions and enforcement.
Private norms - legal norms apply in the field of private law, i.e. where the subjects are in an equal position and neither of them can authoritatively decide on the rights and obligations of the other. Subjects regulate their mutual rights and obligations through contracts and agreements.
International norms - legal norms regulate relations between states or their peoples, possibly at European Union level.
National norms - legal norms regulate relations between actors within the jurisdiction of a state or usually within its territory.
Substantive law - legal norms define legal relations in general and set out the rights and obligations of subjects.
Procedural law - legal norms regulate the conduct of public authorities in the application of substantive law norms, which may result in the issuance of a public act.

The general legal norms apply to the entire territory of the State or the European Union. Furthermore, they apply to all entities without any limitation on their temporal scope.
Specific norms - legal norms operate only in a certain territory. Otherwise - apply only to a certain category of subjects or for a certain period of time.
Effectiveness of a legal norm - means that the addressees concerned are entitled to the rights and obligations arising from it.
Cyberspace - can be defined as the space of cybernetic activities or as the space created by information and communication technologies in which a virtual world (or space) parallel to the real space is created.
Cyberspace - a digital environment that enables the creation, processing and exchange of information, consisting of information systems and electronic communications services and networks.
Cyberspace - can be defined by the accessibility and traceability of data for the average user.
Cyberspace - is a space consisting of three layers: physical, logical and social
Physical layer - includes the term **geographical component** and the term **physical network elements**.
Logical layer - contains the logical **elements of the network**, i.e. the logical connections between network nodes. These are implemented using network communication protocols. Nodes can be computers, telephones and other network devices
Social layer - consists of components called '**cyberness**' and **personality**.
Defining standards - are created and implemented by those with the authority to define the information network environment. They are, in practice, *sui generis* standards that define information networks as such. They come in layers that are interdependent.
Defining authorities - are the creators of defining norms. This is the entity that, through its actions, creates the rules of the logical system in which the body operates
The internet only exists because of the defining authorities. It consists of. No operation will take place without the participation (execution or mediation of the execution of the operation) of the defining authority.
Service provider - any public or private entity **which provides its service users with the ability to communicate via a computer system**
Service provider - any other entity that processes or stores computer data on behalf of a communication service or users of such a service
Information society service means any service provided electronically at the individual request of a user notified by electronic means, normally provided against remuneration. A service is provided electronically if it is transmitted over an electronic communications network and retrieved by the user from electronic data storage devices.

Electronic communications service means a service that is normally provided for remuneration and is based on the (wholly or mainly) transmission of signals over an electronic communications network.
Publicly available electronic communications service - is an electronic communications service that no one is excluded from using at the outset.
An operator - providing or authorised to provide a public communications network or associated facilities is referred to by the Act as **an operator.**
Subscriber - is anyone who has concluded a contract for the provision of such a service with an undertaking providing publicly available electronic communications services.
User - is anyone who uses or requests publicly available electronic communication services.
Proportionality test - is a standard legal instrument of both international and constitutional (domestic) courts when assessing the collision of rules of law that serve to protect a constitutionally guaranteed right or public interest with another fundamental right or freedom.
The principle of fitness - (fitness for purpose), according to which a **measure must be capable of achieving its intended purpose,** which is to protect another fundamental right or public good.
Principle of necessity - provides for the **use of only the most environmentally friendly means to achieve the intended purpose** (interference with fundamental rights and freedoms) **among several possible means.**
Principle of proportionality - (in a narrower sense) aims **to** prevent **harm to a fundamental right disproportionate to the aim pursued,** i.e. measures restricting fundamental human rights and freedoms must not, in the case of a conflict between a fundamental right or freedom and the public interest, outweigh, through their negative consequences, the public interest positives of those measures.
GDPR/RODO - General Data Protection Regulation
Information Security Management System (**ISMS**)[2] - **is a set of policies** designed to maintain the confidentiality, integrity and availability of information by applying a risk management process and assuring stakeholders that risks are being appropriately managed.[3]
ISMS - is part of and integrated into the organisation's processes and overall management system.
PDCA cycle - stands for Plan-Do-Check-Act.
OPDCA variant - extends the original model to include **an Observation** phase preceding the Plan phase.
Risk assessment - refers to the **overall process of identifying, analysing and evaluating risks.**
Security policy - is a set of principles and rules that define how to ensure the protection of assets**.**
RACI matrix (**RACI matrix) - an acronym for responsible, accountable, consulted, informed.**

[2] Hereinafter referred to as **ISMS**
[3] Cf. introduction of ČSN ISO/IEC 27001

A support agent is a technical agent, employees and suppliers involved in the operation, development, administration or security of an ICT system.
The underlying asset is the information or service processed or provided by the ICT system.
BCM - stands for business continuity management.
Premises - is a building or other enclosed space.
Permission means the right to access any asset (usually a computer or communication system, application, etc.) In practice, it is a tool for 'managing users and groups' and a tool for setting permissions on files and directories. These tools are a proprietary component of all standard operating systems.
AAA central server - an acronym for Authentication, Authorisation, Accounting.
SIEM - short for Security Incident and Event Management.
Cryptography (encryption) - is the scientific discipline dealing with the transformation of intelligible information into a form that is unintelligible to the recipient if the recipient does not have the keys with which to decrypt the information.
GDPR Regulation - is a **general legal framework for the protection of personal data that** is valid and effective throughout the EU and, in some cases, beyond.
Personal data - is **any information relating to an identified or identifiable natural person**. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal data is **any information** (e.g. pictorial, written, verbal, digital, genetic, medical, etc.) that **is linked** (through content - e.g. name, address, position, email, etc.) **to a** data subject**.**[4]
"Objective criterion" - means that data such as **IP addresses could be considered as personal data** processed by non-connection service providers (e.g. by a website operator), **even if only a third party would be able to identify a specific user** (typically a connection ISP).
"**Relative**" **criterion -** means that **IP addresses could be considered personal data for an ISP connection**, as they allow the ISP to establish the identity of the user, **but no longer for ISP sites, which actually only have IP address information and do not know the visitor's name**.
Processing of personal data - means **an operation or set of operations** which is performed upon personal **data** or sets of personal data**, whether or not by automated means,** such as collection, recording, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[4]According to Article 4 (1) GDPR, a **data subject** is an identified or identifiable **natural person**.A **data subject may be identified:**

- **directly,**
- **indirectly (e.g. highlighting, etc.)**

DPIA - means personal data protection impact assessment
DPIA - is a tool to be used when a specific type of **processing, in particular using new technologies, is likely, given the** nature, scope, context and purposes of the processing, to give rise to **a high risk to the rights and freedoms of natural persons.**
RIR - abbreviation for **Regional Internet** Registry.
LIR - short for **Local Internet** Registry.

Key quotes from online material:

- Law is one of the most important instruments for stabilising social relations and regulating society
- The law is one of its possible regulation in the form of imperfect normative constructions, where, more than elsewhere, there is a rule of thumb that there is no overlap between the real-world conduct, i.e. what is actually implemented in the online environment, and the normative conduct, i.e. what should be (by the regulator's will and ours). The reality of the Internet and its normative regulation are therefore two relatively separate categories. This assumption will not be challenged in this publication either. On the contrary, it will be one of its pillars
- The actual concept of law is relatively difficult to define, as it is a multidisciplinary phenomenon and cannot be defined by a single definition:
- **Natural law** *(ius naturale* exists independently of the state. It arises and develops in society. It generally comprises a set of rules corresponding to the level of development reached by society.
- **Positive law** *(ius positivum)*. This law is enacted by the state or system of government. Positive law is therefore predetermined. It consists of predictable rules that are enforced, i.e. where infringement is punished.
- **Law** (or objective law) is understood as a set of legal norms as generally applicable rules of conduct established or recognised and enforced by the state.
- **Entitlement (right) -** is the possibility for legal entities to behave as guaranteed by a legal norm. An entitlement usually corresponds to a legal obligation of another legal subject. A subject's statement that 'this is my right' is legal in this sense.
- **A legal norm** is a generally applicable rule of conduct that regulates the rights and obligations of subjects. This rule of conduct is expressed in a specific legal form recognised by the State (or the European Union) and its observance is ensured by State enforcement.
- Legal norms can be divided according to various criteria. These include, in particular:

  1. *The nature of the rules established by a legal norm.* Due to the nature of the rules, legal norms are divided into:
  - Dispositive. A dispositive legal norm does not set out a basic rule of conduct at all or only sets it out as a possibility. It leaves the determination of the rules to the addressees. If the addressees do not do so, the rules contained in the norm serve as a guide for the judge to know how to decide. Dispositive norms are most often used in civil law or in civil law relations, which allow for greater variability in the resolution of different situations (self-regulation).
  - Cogent (categorical).A cogent legal norm sets out a binding rule of conduct. It leaves no room for the will of the addressee.

- **Cyberspace** is:
    - cybernetic action space, i.e. the space created by information and communication technologies in which a virtual world (or space) parallel to the real one is created.
    - the digital environment that enables the creation, processing and exchange of information, consisting of information systems and electronic communication services and networks.

- a space made up of three layers: physical, logical and social.

- **The characteristics of cyberspace** are its **decentralisation, globalisation, openness, wealth of information, interactivity** and the possibility for the user to influence opinions. An important attribute of cyberspace is that technology and related services play a fundamental role in it. Recently, it has become increasingly clear that the manifestations of the virtual world can and do have consequences in the real world.
- One of the more effective definitions of *cyberspace* is found in *Cyberspace Operations: Concept Capability Plan 2016-2028*, which defines **cyberspace as a space consisting of three layers:** [5]
  - physical,
  - logical,
  - Social.
- **Cyberspace can also be defined according to the accessibility and traceability of data for the average user.** According to this division, cyberspace can be divided into services and data accessible via the Internet, services and data accessible only within specific networks and devices, and services and data deliberately hidden and accessible with special tools.

The following names are usually used for these categories:
- Surface Web
- Deep Web
- Dark Web

- **Defining standards** are created and implemented by the entities authorised to define the information network environment. They are, in practice, *sui generis* standards that define information networks as such. They come in layers that are interdependent
- **Defining authorities** are the creators of defining norms. It is the entity that, through its action, creates the rules of the logical system in which the body operates.
- The biggest **defining body**, even if it is not the entity that creates the rules of the logical system, **is the user as such**.
- The concept of provision **by electronic means is defined** in Directive (EU) 2015/1535 of the European Parliament and of the Council in Article 1(b)(ii), where it is defined as a service that is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data.
- **An individual user request** means that it must be an active user action
- In order to determine the individual rights and obligations of connection providers, it is necessary to divide these providers into two groups - **public and non-public**. Both groups of connection providers are covered by the Law on Certain Information Society Services, but public connection providers are also covered by the Law on Electronic Communications, which defines further rights and obligations of these providers
- According to § 6 of ACISS, **the connection provider is not obliged** to supervise the content of the transmitted information or to actively ascertain the illegality of the transmitted information.

[5] TRADOC. Cyberspace Operations: Concept Capability Plan 2016-2028 [online]. [cited 18/02/2018], pp. 8-9 Available from: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

- **Electronic communications service** [ECA section 2 (n)[6]]. According to section 2 (n) of the ECA, the term means a service that is normally provided for remuneration and is based on the (wholly or mainly) transmission of signals over an electronic communications network.
- **Publicly available electronic communications service** [section 2 (o) ECA]. This service is an electronic communications service from which no one is previously excluded from using.
- **An undertaking** providing or authorised to provide a public communications network or associated facilities is referred to by this Act as **an operator** [section 2 (e) ECA].
- **A subscriber** [paragraph 2(a) ECA] is anyone who has concluded a contract for the provision of such a service with an undertaking providing publicly available electronic communications services.
- **A user** is anyone who uses or requests a publicly available electronic communications service.
- **The proportionality test** is a standard legal instrument of both international and constitutional (domestic) courts when assessing the collision of rules of law aimed at protecting a constitutionally guaranteed right or public interest with another fundamental right or freedom.
- **The Information Security Management System** (**ISMS**)[7] **is a set of principles designed to** maintain the confidentiality, integrity and availability of information by applying a risk management process and assuring stakeholders that risks are appropriately managed.[8]
- The ISMS solution requires a systemic and comprehensive approach, respecting the principles and elements of the entire cyber security lifecycle. The ISMS management system is based on the Deming cycle, or **PDCA** (**Plan-Do-Check-Act**) **cycle**.
- An asset can be, from a civil law perspective, a **tangible** thing (building, computer system, networks, energy, goods, etc.) or **an intangible** thing (information, knowledge, data, programmes, etc.).
- An asset can also be **quality** (e.g. availability and functionality of the system and data, etc.) or **good name,** reputation, etc.
- **People** (users, administrators, etc.), with their knowledge and experience, are also an asset from a cyber security perspective.
- **A support agent** is a technical agent, employees and suppliers involved in the operation, development, administration or security of an ICT system.
- **The underlying asset** is the information or service processed or provided by the ICT system.
- Business Continuity Management (**BCM**) is a process based on identifying key elements (systems and processes) in an organisation and then establishing processes and procedures to ensure the continuity or renewal of these elements, at a predetermined level at which it will still be possible to perform the organisation's core tasks.
- The term physical **security perimeter** designates a designated space or the boundaries of that space. Such a space can be, for example, a set of premises, the premises itself or part of the premises.
- **The premises** are a building or other enclosed space.
- **Premises boundary** means a building partition, physical barrier (fence) or other visibly defined land boundary.
- **A secured area** means a space in a building that is structurally or otherwise visibly separated.
- The term **permission** means the right to access any asset (usually an IT or communication system, application, etc.) In practice, it is a tool for 'managing users and groups' and a tool for setting permissions on files and directories.
- As part of physical security, some administrators are required to carry out **penetration testing of** the ICT system, focusing on important assets, namely:
    - before they are put into service and

[6] Hereinafter referred to as ECA
[7] Hereinafter referred to as **ISMS**
[8] Cf. introduction of ISO/IEC 27001

    - due to a substantial change.
- As part of application security, the undertaking also ensures that applications, information and transactions are protected at all times against:
    - unauthorised action,
    - refusal to perform.
- The value of risk is most often expressed as a function of impact, threat and vulnerability. For example, the following function can be used to self-assess risk:

  Risk = impact * threat * vulnerability

- The General Data Protection Regulation (EU) 2016/679 or GDPR/ RODO[9] is one of the most important international legal documents that directly relates to the issue of cyber security, although it is not primarily aimed at the ICT field.

  GDPR ≠ IT + software.

- **Personal data is mostly published on social media**, which by its very nature presupposes such disclosure and enshrines in the Terms and Conditions the rules under which such data is treated
- According to Article 4 (1) GDPR/RODO, personal data is "**any information relating to an identified or identifiable natural person**.
- According to Article 4(2) RODO, processing of personal data means **any operation or** set of **operations** which is performed upon personal **data** or sets of personal data, whether or **not by automated means,** such as collection, recording, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- One of the areas that the GDPR explicitly addresses is the **security of the processing of personal data**.
- A Data Protection Impact Assessment (**DPIA**) is a tool to be used when a specific type of **processing, in particular using new technologies,** taking into account the nature, scope, context and purposes of the processing, is **likely to present a high risk to the rights and freedoms of individuals**. It is a tool that can help controllers identify potential risks associated with the processing of personal data and implement appropriate measures.
- The data protection impact assessment should include:
    - description of the planned processing operations,
    - assessment of the necessity and appropriateness of the measures in view of the objective (**proportionality test**),
    - assessing the risks to the rights and freedoms of subjects,
    - the planned measures to address these risks, including guarantees, security measures, etc.
- Digital traces, based on whether they can be influenced by the user, can be broadly **divided into traces that can be influenced (active) and those that cannot be influenced (passive).**
- By default, an IP address is not anonymous, and a computer system uses it as one of its identifiers when communicating with other computer systems. IP addresses are assigned hierarchically, with the dominant role being played by **ICANN,** which divides the real world into regions managed by **Regional** Internet **Registries** (**RIRs**).
- The regional registries further divide the allocated IP ranges between **Local** Internet Registries (**LIRs**). The local registry is usually an ISP - a connection provider, either public or non-public. This registry may then share its IP address range with, for example, parts of its organisation or other entities.

[9] [online]. Available from: http://eur-lex.europa.eu/legal-content/

3. During classes

Some ideas for activities:

WORKSHOPS

1. Defining the scope of the law in cyberspace (boundaries, possibilities, etc.).
2. Private and public liability for the actions of a user or company in the online environment.
3. Characteristics and definition of the different ISPs and their rights and obligations in relation to cyber security.
4. ISMS and the relationship to cyber security law.
5. Basic rights and obligations for individual entities from Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security for network and information systems in the Union, also from national legislation.
6. Applying GDPR/RODO rights and obligations in cyberspace.
7. Practical analysis of the terms and conditions of sample ISP privacy agreements.

REVIEW QUESTIONS

1.

- What is the law?
- What is a legal norm and how is it divided?
- What is cyberspace?
- What layers does cyberspace consist of?
- Does the law apply in cyberspace, and if so, what legal standards apply?
- How can the law be applied in cyberspace, including possible sanctions or other measures?
- Give some examples of the application of the law in cyberspace.
- Define ISMS.

2.

- Define PSI.
- How are ISPs divided? According to what criteria?
- What are the responsibilities of ISPs?
- What is a defining standard?
- Who is the defining authority and what is its role?
- What is data retention?

3.

- What is the PDCA cycle and what is its application?
- What elements can be included in physical security?
- What is: Business Continuity Management?
- Define the threat.

- Define risk.
- Define impact.
- Define vulnerability.
- Define assets.
- What is an asset, what are the assets?

4.

- What is the territorial scope of the GDPR?
- What is personal data?
- Is an IP address personal data?
- What are the responsibilities of the personal data controller?
- What is meant by processing personal data?
- What does a data protection impact assessment mean?

5.

- Define the term " digital footprint ".
- What is the difference between digital footprints?
- What components does the passive digital footprint consist of?
- What is an LIR?
- What information about the user does the IP address carry?
- What is an EULA?

Working in pairs/groups

- **Pairs - mini-project**
  In pairs, students choose one of the topics discussed. They write down their conclusions and present them to the others. After the presentation, the other students prepare additional questions for the presenting group.

- **Map of thoughts**
  Students in pairs choose one of the topics covered and create a mind map, which they then describe to the other students in a short presentation.

- **Keywords**
  Students in pairs individually select key words from the glossary.

They write the definitions of these words on strips of paper. They turn the strips over with the blank side up. A student chooses a strip, reads the definition and the other student looks for a matching keyword.
or
Students write some key words from the glossary on a piece of paper. They turn the cards over with the blank

side up. One student takes the first card and says what the word means. The second student guesses the key word.

- 10 keywords
  Students choose 10 keywords related to their chosen topic. These 10 keywords are given to other pairs. The pairs write a text which must contain all the keywords. One sentence can only contain one keyword. So the text consists of at least 10 sentences.

- Panel discussion

  Students choose 3 speakers. Each speaker chooses one topic to discuss. The other students ask questions about the topics. Each speaker can use an answer type -TRUE X FALSE. The student gets a point for each true answer, e.g. Does GDPR stand for General Data Protection Regulation? - TRUE X FALSE.

4. Internet resources

See bibliography.

5. Additional questions/tests

SELECT THE CORRECT ANSWER:
(The correct answer has been underlined)

1. _____ is established by the state or system of government and is therefore predetermined. It consists of predictable rules that are enforced, i.e. their violation is punished.

   a) Positive law
   b) Natural law
   c) Subjective right
   d) Objective law

2. _____represents a generally applicable rule of conduct that governs the rights and obligations of actors.

   a) Legal standard
   b) Legal law
   c) Legal standard
   (d) Legal line

3. _____ - a rule of conduct regulates social relations with binding effect

   (a) a final decision
   (b) legally leading
   (c) legally justified
   (d) legally binding

4. The standard structure of a legal norm consists of three parts, which are _____.

(a) hypothesis, disposition and sanction
(b) anticipation, disposition and sanction
(c) hypothesis, infringement and sanctions
(d) hypothesis, disposition and penalty

5. _____ is the expression of the consequences of a breach of a legal obligation arising from the disposition of a legal norm.

a) Repatriation
(b) Judgement
(c) Sanction
(d) Revision

6. The _____ standard does not specify a basic rule of conduct at all or only defines it as a possibility. It is left to the addressees to determine the rules. If the addressees do not do so, the provisions in the norm serve as a guide for the judge when deciding.

(a) logical
(b) dispositive
(c) categorical
(d) significant

7. _____ legal norms regulate relations between actors within the jurisdiction of a state or usually within its territory

a) Public
(b) International
c) Private
d) National

8. _____ legal norms apply to the entire territory of a state or the European Union. Moreover, they apply to all entities without limitation of their temporal scope.

(a) International
b) National
c) Substantive
d) Civil

9. Cyberspace can also be defined as the space of cybernetic activities or as the space created by information and communication technologies in which a _____ world (or space) parallel to the real space is created.

(a) digital
(b) actual
(c) virtual
(d) current

10. Cyberspace can also be defined according to the availability and _____ of data to the average user.

(a) effectiveness
(b) effectiveness
(c) performance
(d) traceability

11. The _____ principle implies the use of only the most environmentally friendly means to achieve the intended purpose (interference with fundamental rights and freedoms) out of several possible ones.

(a) necessity
(b) adequacy
(c) proficiency
(d) suitability

12. What does the abbreviation ISMS stand for?

(a) Secure Information Management System
(b) Information Security Management System
(c) Systematic Management of Secure Information
(d) System Information Security Team

13. A security policy is a set of principles and rules that _____policies to ensure/-e/-u protection of assets.

(a) determine
(b) affect
(c) prevent
(d) influence

14. The term _____ means the right to access any asset (usually an information or communication system, application, etc.).

    (a) application
    (b) the licence
    (c) permission)
    (d) pass

15. What does the abbreviation DPIA stand for?

    a) Assessment of the Impact of Permitted Data
    b) Data Protection Impact Assessment
    (c) Data Impact Assessment
    (d) Evaluation of the Impact of Promising Data

Bibliography

ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cited 10/06/2016].

BARLOW, Perry John. *Declaration of cyberspace independence.* [online]. [cited.23.09.2014]. Available from: https://www.eff.org/cyberspace-independence.

CAETANO, Lianne. *Are Your Apps Oversharing? 2014 Mobile Security Report Tells All.* [online]. [cited 10/04/2015]. Available from: https://blogs.mcafee.com/consumer/mobile-security-report-2014/.

CNN on paedophile sex in Second Life. [online]. [cited 18.06.2009]. Available from: http://www.youtube.com/watch?v=AQM-SiiaipE
Current world population. [online]. [cited 10.08.2015]. Available from: http://www.worldometers.info/world-population/.

Interesting statistics on mobile strategies for digital transformation. [online]. [cited 15/07/2016]. Available from: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

Data retention unconstitutional in its current form. [online]. [cited 16/07/2016]. Available from: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

Digital, Social & Mobile in the World 2015. [online]. [cited 09/08/2015]. Available from:http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

ENGLEHARDT, Steven and Ardvin NARAYANAN. *Online tracking: Measuring and analysing 1 million sites.* [online]. [cited.05.08.2016]. Available from: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

Facebook will soon be able to identify you in every photo. [online]. [cited 09.08.2015]. Available from: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

FBI exploits Flash vulnerability to crack Tor network security. [online]. [cited.23/07/2016]. Available from: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/.

First Amendment. [online]. [cited 10/07/2016]. Available from: https://www.law.cornell.edu/constitution/first_amendment.

German Bundestag passes new data retention law. [online]. [cited 16/07/2016]. Available from: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

HAINES, Lester. *Online gamer stabbed by 'stolen' cybersword.* [online]. [cited 03/10/2006]. Available from: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Prague: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, pp. 101-102.

Censorship on the Internet. [online]. [cited 10.08.2016]. Available from: http://www.deliveringdata.com/2010_10_01_archive.html.

Internet history of the 1980s [online]. [cited 07.06.2016]. Available from: http://www.computerhistory.org/internethistory/1980s/.

JOHNSON, David R. and David POST. *The Rise of Law in Cyberspace.* [online]. [cited 10/07/2016].

KOLOUCH, Jan and Andrea KROPÁČOVÁ. Responsibility for one's own device and the data and applications stored in it. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14). [*B.m.], c2014, pp. 321-324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

KOLOUCH, Jan. *Cybercrime.* Prague: CZ.NIC, 2016, p. 78 et seq. and pp. 109 et seq.

Leading social networks in the world, as of April 2016, ranking by number of active users (in millions) [online]. [cited 10.08.2015]. Available from: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

LESSIG, Lawrence. *Code v. 2. p.* 6 Available in full (eng) [online]. [cit.13/03/2008]. Available: http://pdf.codev2.cc/Lessig-Codev2.pdf

MAISNER, Martin andBarbora VLACHOVÁ. *Zákon o kybernetickébezpečnosti. Komentář.* Prague: Wolters Kluwer, 2015. p. 85

MATEJKA, Ján. *Internet jakoobjektpráva: hledánírovnováhyautonomie a soukromí.* Prague: CZ.NIC, 2013. ISBN 978-80-904248-7-6 pp. 25

National legal challenges to the Data Retention Directive. [online]. [cited 16/07/2016]. Available: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html.

The PDCA cycle. [online]. [cited 06/07/2018]. Available from: https://www.creativesafetysupply.com/glossary/pdca-cycle/.

PETERKA, Jiří. *Uchovávatprovozní a lokalizačníúdajenámuž EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cited 10/11/2015]. Available from: http://www.earchiv.cz/b14/b0428001.php3

REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, p. 218.
Regional online registries. [online]. [cited 04.08.2015]. Available from: https://*www.nro.net/about-the-nro/regional-internet-registries.*

ROSER, Christoph. *The Many Flavors of the PDCA.* [online]. [cited 06/07/2018]. Available from: https://www.allaboutlean.com/pdca-variants/.

SMITH, Craig. *By the Numbers: 100 amazing statistics and facts from Google search.* [online]. [cited 04/08/2016]. Available from: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/.

Court of Justice of the European Union. Press release No 54/14, 8 April 2014. Judgment in Joined Cases C-293/12 and C-594/12 [online]. [cited 15/07/2016]. Available from: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf.

Opinion of Advocate General Pedro Cruz Villalón. Case C-293/12 and C-594/12 [online]. [cited.15/07/2016]. Available in: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

Opinion of Advocate General SAUGMANDSGAARD ØE, dated 19/07/2016. In Joined Cases C-203/15 and C-698/15 [online]. [cited 10/8/2016]. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

Surface Web, Deep Web, Dark Web - what's the difference. [online]. [cited 20/07/2016]. Available from: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference.

Module 3

Cyber-attacks detection and prevention

1. Introduction

1.1 Course summary

The course initially focuses on an overview of the basic legal standards of cybercrime. It is also necessary to understand the concept of cybercrime in order to understand the whole issue. A significant part of the course deals with the classification of cybercrimes. The course reviews the various cybercrimes, which are described in great detail. The main part of the course is devoted to cyber-attacks and their sanctions.

1.2 Course objectives

Students are introduced to the legal norms governing cybercrime. The aim of the course is to familiarise students with the issue of cyber-attacks, which may have the characteristics of unlawful behaviour, as well as the possible legal qualification of such behaviour. The main part of the course is to identify the forms and methods of committing cybercrimes. The course also focuses on spam, fraud, hoaxes and botnets. In addition, students will study cyber-attacks, specifically those related to finance (pharming, spearphishing, mobile phishing), but also attacks related to society (cyberbullying, stalking, sexting, cyber grooming, etc.). Prevention of these negative phenomena is an important content of this module.

1.3 Course content

Individual lectures introduce students to the legal norms governing cybercrime. In addition, students are introduced to social engineering, spam, fraud, hoax and botnet. During the lectures, students are introduced to different types of cyber-attacks, such as hacking, cracking, malware, ransomware. Not only cyber-attacks such as attacks targeting finances (phishing, pharming, spearphishing, mobile phishing), but also social cyber-attacks (cyberbullying, stalking, sexting, cybergrooming, etc.) are also mentioned.

1.4 Learning objectives

1) Introduction to cybercrime terminology
2) Learning about national cybercrime regulations
3) Learning about international cybercrime regulations
4) Understanding the importance of social engineering in the context of cyber-attacks
5) Awareness of manifestations of cybercrime
6) Understanding cyber-attacks

1.5. Equipment and materials required

Detection and prevention of cyber-attacks - available online

1.6 Syllabus

Learning outcome	The student who successfully completes the module will know/be competent in the following.
NEWS	
W1	The student will obtain a general overview of national and international legal norms defining illegal activities in cyberspace.
W2	The student will learn the basic technical terminology that is related to cyber-attacks, cyber incidents, cyber crime, etc. He/she will be able to distinguish which legal norm or special provisions apply to a given attack and why.
SKILLS	
U1	Upon completion of the course, the student will be able to identify basic cyber-attacks, their modus operandi, the consequences caused, etc.
U2	Based on the above identification, the student will be able to apply specific legal instances to the violation in question. The student will be able to take basic preventive measures to possibly eliminate negative behaviour in the future.
COMPETENCES	
K1	The student is able to distinguish between different cyber-attacks, partially controls the legal provisions related to protection against these attacks and is able to apply basic preventive measures.

Content of the module (programme of lectures and other activities)	**Reference to learning outcomes**
LECTURES 1. Social engineering 2. Spam, scam, fraud 3. Botnet 4. Cyber-attacks - Hacking, cracking, malware, ransomware 5. Cyber-attacks - attacks of a financial nature (phishingpharming, spearphishing, mobile phishing) 6. Cyber-attacks - social attacks (cyberbullying, stalking, sexting, cybergrooming, etc.). WORKSHOPS 1. Analysis of individual attacks - modus operandi 2. Testing security against selected attacks. 3. Definition of options for preventing particular types of attack 4. Designing a customised solution to protect against individual cyber-attacks. 5. Security testing of certain systems, applications and data. Students will attempt to design their own solutions to enhance the security of these systems, applications or data. 6. Familiarise yourself with tools and resources for secure data storage and setting up secure online communication (e.g. VPN administration and settings, PGP, password manager, etc.).	W1, W2 U1, U2, K1
ECTS credit balance	

Form of student workload		Number of hours
Number of hours with direct participation of academic teacher		
1.1	Participation in lectures	6
1.2	Participation in seminars	
1.3	Participation in workshops	14
1.4	Participation in laboratory activities	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times per semester)	
1.7	Participation in the project consultation	
1.8	Participation in examinations/tests	2
1.9	Other ...	
1.10	**Number of hours spent with direct assistance of academic staff (sum 1.1 - 1.9)**	22
1.11	**Number of ECTS credits obtained by the student in classes requiring direct participation of an academic teacher)**	1
Individual student work		
2.1	Individual studies (including e-learning lectures)	25
2.2	Individual preparation for workshops	10
2.3	Individual test preparation	
2.4	Individual preparation for laboratory classes	
2.5	Preparation of reports	
2.6	Implementation of self-performed tasks (projects, documentation)	
2.7	Preparation for the final examination/tests of the workshop	5
2.8	Preparation for final examination/testing of lectures	5
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 - 2.9)**	45
2.11	**Number of ECTS credits obtained by the student in individual learning activities**	1,5
Total workload (h)		**67**
ECTS credits for the module		**2,5**

Methods of verifying learning outcomes

Learning outcome	**Forms of credit classes**								
	Oral examination	Written examination	Partial written assignment	Final written assignment (essay	Test	Project/presentation	Report	Classroom activities	Other ...
NEWS									
W1, W 2		x	x		x			x	
SKILLS									
U1						x		x	
U2						x		x	
COMPETENCES									
K1						x		x	

Criteria for assessing student competence
The minimum requirements for the three groups of learning outcomes that the Student must achieve in

order to pass the subject are presented below in synthetic form. In order for a Student to pass a module, all learning outcomes described in the syllabus must be positively verified by the person(s) teaching the module.

W - KNOWLEDGE
Assessment:
Satisfactory - The student remembers and reproduces the knowledge to be mastered within the module.
Good - The student additionally interprets phenomena / problems and is able to solve a typical problem
Very good -Student is able to solve even complex problems in a given field, is able to synthesise, carry out a comprehensive evaluation, create a work that is original and inspiring to others.

U - SKILLS
Assessment:
Satisfactory - The student knows the nature of the activities and is able, under the guidance of the academic teacher, to carry out activities / solve problems related to the content of the module
Good - Student is able to independently carry out activities / tasks / solve typical problems related to the content of the module
Very good - The student has fully mastered the ability / skill to perform the activities / tasks / problems provided for in the module content, also in more complex cases.

K - SOCIAL COMPETENCE
Assessment:
Satisfactory - Student passively assimilates module content, demonstrating ability to concentrate and listen
Good - Student actively participates in classes, makes value judgements according to the criteria accepted in the given field, can actively cooperate in a group
Very good - The student integrates the attitude according to the proposed model, develops his/her own system of professional and social values, is able to take responsibility for the actions of the group, including leadership.

2. Basic material for the teacher

Definitions (glossary)

Cybercrime - is most commonly used to refer to crimes committed using information technology, and the use of the term has also moved from the normative field into the professional vocabulary. **Cybercrime** - is a crime in which means of information and communication technology are **used as a tool to commit a crime and as a target for an attack by the perpetrator**, **and the said attack is a crime, provided that these devices are used or abused in an information, system, software or communication environment (i.e. cyberspace).** **Cybercrime** can be defined as behaviour directed against a computer or, in some cases, a computer network, or as behaviour in which a computer is used as a tool to commit a crime. An indispensable criterion for applying the definition of cybercrime is that the environment in which the activity takes place is then a computer network, i.e. cyberspace. **Cyber crime - any crime in which the perpetrator has used information and communication technologies**
FP TERMINAL - Payment Fraud. Group dedicated to providing support in online fraud.
FP Cyborg - High-Tech Crimes. A group dealing with and providing support for various cyber-attacks affecting critical infrastructure and information systems. In particular, these include attacks such as malware, ransomware, hacking, phishing, identity theft, etc.
FP Twins - Child Sexual Exploitation. A group that deals with and provides support in the investigation of child sexual abuse
Computer security incident (which can be understood as a computer attack or computer crime) - an illegal,

unauthorised, unacceptable action that affects a computer system or network.
Cyber-attack[10] - can therefore be defined as **any unlawful behaviour by an attacker in cyberspace that is directed against the interests of another person**.
A cyber security incident - is an event that may cause a breach of the security of information in information systems or a breach of the security of services or the security and integrity of electronic communication networks.
Cyber security incident - is a breach of information security in information systems or a breach of security of service provision or a breach of the security and integrity of electronic communication networks as a result of a cyber incident.
Computer data - means any expression of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of causing a computer system to perform a function.
Information - is data that has been processed into a form that is useful to the recipient. So any information is information, but any stored data does not necessarily become information.
Social engineering - involves influencing, persuading or manipulating people in order to get them to take a certain action or to obtain information from them that they would not otherwise give.
A botnet can be most simply defined as a network of software-connected bots[11] , which perform some action based on a command from the 'owner' (or administrator) of that network. A network constructed in this way can be used for legitimate activities (e.g. distributed computing) or for illegal activities
Decentralised architecture - is typically built on a peer-to-peer (P2P) architecture. This architecture allows for the sharing of resources and commands within a P2P network.
Malware- serves as a means to access, control and further spread malware or other tasks as directed by the attacker, and not just in the case of botnets. However, if malware is currently infecting a user's computer system, there is a high probability that it has become part of a botnet
Malware- (derived from *malicious software*) can be any program used to disrupt the standard operation of a computer system, gain information (data) or used to gain access to a computer system. Malware can take many forms, with many types of malware being named after the activity it performs.
Adware stands for '*advertising supported software'. It* is the least dangerous but profitable form of malware.[12]
Spyware is a combination of the English words '*spy*' and '*software'*. Spyware is used to obtain statistical data[13] about the operation of a computer system and send it to the attacker's data box without the user's knowledge or consent. This data may also include information of a personal nature or information about the user's person, as well as information about websites visited, applications run, etc.
Viruses - are a programme or malicious code that attaches itself to another existing executable file (e.g. software, etc.) or document. The virus is replicated when that software is run or the infected document is opened. Most commonly, viruses spread by sharing software between computer systems; no user cooperation is needed to spread them.
Computer worms are also **referred to** as viruses. The reason for the closer association with viruses is that

[10] It is necessary to distinguish the concept of a cyber-attack from that of a **security incident,** which is a breach of IS/IT security and the rules laid down to protect it (security policy).

[11]**Bot** (short for robot). This is a program that can execute the attacker's commands entered from another computer system. The most common way to do this is to infect the computer with a virus such as a worm, Trojan horse, etc. A computer system that is remotely controlled in this way is then referred to as a **zombie**. However, some sources even refer to an infected computer system as a bot.

The bot can collect data, process requests, send messages, communicate with the control element, etc.

[12] There are companies that specialise in "pay per install" (*PPI*). *"PPI" then results in a plethora of actions leading to the installation of add-ons or other unwanted software that (in the least harmful case) lists adverts on websites without the user's knowledge or inserts them where there are no adverts on the website.... **PPI relies on the fact that those offering these services do not care if the user wants to install anything. They receive up to US$1.50 per installation**, so it is more than certain that fraudulent and automated installations are an essential part of their 'business model'."*

[13] E.g. an overview of websites visited, their IP addresses, an overview of installed and used programmes, records of file downloads from the Internet, data on the structure and content of directories stored on the hard drive, etc.

worms do not need any host, i.e. they do not have an executable file (like viruses). Unlike viruses, which are included as part of another programme, these programmes usually spread separately.
Trojan horses are generally those computer programmes that contain hidden functions that the user does not agree with or is unaware of, and which are potentially dangerous to the continued operation of the system.
Backdoor-some Trojans, when launched without the user's knowledge, open the computer's communication ports, making it much easier for other malware to further infect the attacked system or facilitate direct control of the infected computer remotely.
Scanning[14] **programmes** ('*port scanners*') - i.e. programmes mainly used to determine which ports of a computer's communication network are open, what services are running on them and whether it is possible to launch an attack on such a system.
Rootkits- refers not only to computer programmes, but also to all the technology used to mask the presence of malware (e.g. computer viruses or Trojan horses, worms, etc.) on an infected system. They most often take the form of not very large computer programmes. Rootkits are not harmful in themselves, but are exploited by the creators of malicious programmes such as viruses, spyware, etc.[15]
Keylogger- is software that records specific keystrokes on an infected computer system. Most commonly, a keylogger is used to record login details (username and password) for accounts that are accessed from the computer system. The information obtained is then usually sent to the attacker.
Ransomware - is malware that prevents or restricts users from properly using a computer system until the attacker receives a 'ransom'. Ransomware most often gets onto a computer via malware (Trojan horse or worm) that is found on a website or is an email attachment. Once the malware has safely 'established itself' on the computer system, its own ransomware will be downloaded.
Crypto-ransomware - the purpose of this malware is to encrypt the hard drive or selected file types on the computer system. Primarily, it aims to encrypt the user's private files, such as images, text documents or spreadsheets, videos, etc.
Police ransomware - then blocks access to the user's Windows account[16] notifying the user that material that violates the laws of the country (e.g. copyright infringement, child pornography, etc.) has been found on their computer. At the same time, the user has been invited by the 'police' to pay the required amount of money, after which the computer will be unlocked and the whole matter will be 'resolved'.
Spam - can basically be understood on two levels. In **a narrow sense, it is the** mass dissemination of unsolicited messages, usually of an advertising nature via the Internet, and most often via electronic communication. In a **broad sense,** spam is all unsolicited messages received, and therefore also messages containing viruses, Trojan horses, etc. . [17]
Spam - is a **message sent electronically, en masse and especially without a request.**
Scam - Spam containing criminal or other fraudulent content is referred to as **scam**. Scams now make up a significant proportion of spam and their purpose is, usually using social engineering, to gain the user's trust and force them to perform certain required actions
Scam 419 - this is the designation for emails, better known as **Nigerian Letters**. These scams are an example of the transfer of ordinary crime (fraud) from the real world to the virtual world.
Hoax(fiction, joke, press canard) - is another form of spam or hoax. The label "hoax" is used for chain messages (such as: "*pass it on*", "*if you don't send this to 20 other people.... will become...*" etc.) that contain distorted, false, misleading or other false information. Hoax often includes attack warnings, threat

[14] These programmes are sometimes referred to as scanning programmes or scanners.

[15]For more details cf. BALIGA, Arati, Liviu IFTODE and Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 323-334.

[16] The application has been set to "StayOnTop". The user cannot see other applications hidden under this 'ransomware dialogue' and is unable to invoke the task manager. The Ransomware itself was registered in the Run and RunOnce registers and performed a check every 500 ms and hid the task manager within the same time range. The only other application running was communicating with the C&C server (masked in the browser process).

[17] To classify spam, cf. forexample GONZÁLES-TALAVÁN, Guillermo. A simple configurable SMTP spam filter: Greylists. *Computers& Security*, 2006, vol. 25, No. 3, pp. 229-236.

descriptions, pleas for help, appeals, petitions, celebrity statements, chain letters of good luck, funny messages, pictures and videos in presentations, playing cats and other animals, etc.
Fraudulent offers - this is a very effective form of fraud. Fraudulent offers can be sent in bulk or in a targeted manner. Nowadays, such offers are sent not only via email, but also via all kinds of instant messaging, social networks, auction sites, etc.
Phishing- is most commonly defined as fraudulent or deceptive conduct aimed at obtaining user information such as username, password, credit card number, PIN, etc.
Phishing - in a **narrow sense, phishing** is an action that requires the user to visit a fraudulent site (displaying e.g. an online banking site, online shop, etc.) and then fill in 'login information' or the information is requested directly (e.g. when filling out a form, etc.). **Phishing - in a broad sense,** phishing can be defined as any fraudulent behaviour that is designed to instil confidence in a user, reduce their alertness or otherwise force them to accept a scenario prepared in advance by the attacker.
Pharming[18] - is a more sophisticated and dangerous form of phishing. It is an attack on the DNS (Domain Name System) server, which translates a domain name into an IP address. The attack occurs when a user types the address of a web server they want to access into a web browser.
Spearphishing- is one form of phishing attack, but the difference is that spearphishing is a precisely targeted attack, as opposed to phishing, which is a rather common (random) attack. The target of the attack - is usually a specific group, organisation or individual, and specifically the information and data contained within that organisation (e.g. intellectual property, personal and financial data, business strategies, classified information, etc.).
Vishing[19] - refers to telephone phishing, in which the attacker uses a social engineering technique and attempts to extract sensitive information from the user (e.g. account numbers, login details - name and password, payment card numbers, etc.). The attacker deliberately tries to falsify the user's identity. Attackers often pose as representatives of real banks or other institutions in order to arouse as little suspicion as possible in the user. Vishing is used in VoIP (Voice over Internet Protocol) telephony.
Smishing[20] - works on a similar principle to vishing or phishing, but uses SMS messages to distribute messages. Smishing is essentially an attempt to get the user to pay an amount of money (e.g. call a toll-free line, send an SMS to a donor, etc.) or click on suspicious URL links. If the user visits such a URL, he or she is redirected to a page that exploits certain vulnerabilities in the computer system, or the user is asked to provide sensitive information or malware.[21]
Business Email Compromise[22] - is a type of scam attack in which an attacker impersonates an executive (usually the CEO) and tries to get an employee, customer or vendor to hand over money or sensitive information to the attacker.
CEO FRAUD (a form of BEC fraud) - Attackers pose as the CEO of a company or other company executive and send a spoofed email to employees with the ability to send wire transfers and instruct them to send funds to the attackers.
INVOICE (a form of BEC fraud) - a company, which often has a long-standing relationship with a supplier, is asked to transfer funds to pay an invoice to another, fake account. The attacker usually contacts the victim via email or telephone. An attack via email usually has a crafted source code (header) and subject line of the request, making it appear very similar to a legitimate request.
ACCOUNT COMPRISE (a form of BEC fraud) - This attack is similar to Fake Invoice. The attacker uses an employee's email account (hacked or spoofed) and then sends an email to customers to inform them that there has been a problem with their payment and they need to resend it to another account.

[18] It is a combination of the words farmingi **phreaking**.
[19] It is a combination of the words 'voice' and 'phishing'.
[20] It is a combination of the words 'SMS' and 'phishing'.
[21] E.g. Xshqi- *Android Worm on Chinese Valentine's Day.* [online]. [cited 14.8.2016]. Available from: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
Selfmite- *The Android SMS worm Selfmite is back, more aggressive than ever.* [online]. [cited 14.8.2016]. Available from: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html
[22] BEC fraud is also known as 'CEO fraud' or 'Man-in-the-Email'.

Business Executive and Attorney Impersonation (a form of BEC scam) - victims are contacted by attackers who pose as lawyers or representatives of law firms. The attacker asks for a large transfer of funds to help resolve a legal dispute or pay an outstanding bill. The attacker tries to convince victims that the transfer is confidential and time-sensitive, so the employee is less likely to try to confirm whether they should transfer funds.
DATA THEFT (a form of BEC scam) - A type of BEC that does not aim to directly transfer money. Typical victims of this attack are financial or HR departments / employees. The attacker asks them to send very sensitive data to their account. Social engineering is used and the data theft attack can be the starting point for the aforementioned financial transfer-oriented BEC attacks.
Fraudulent websites (companies) - On the Internet you can find many activities or websites[23] presenting amazing prizes or offering various goods at very affordable prices. Attackers use social engineering and rely primarily on people's distrust and carelessness. The attacker's own activities can then usually take two forms.
Hacking - is now seen pejoratively by the public as any action by a person to gain illegal access to someone else's system or personal computer.[24]
White hats - White hats: these are hackers who infiltrate a system by exploiting vulnerabilities in the system's security precisely in order to detect these vulnerabilities and create such mechanisms and barriers that should prevent such attacks. Often, they are employees or external collaborators of reputable companies operating in the field of information technology. Their intrusion into a system does not cause damage or other harm to users; on the contrary, in many cases they alert the administrator of such an infected system to security vulnerabilities. Their activities are essentially non-destructive in nature.
Black hats - Black hats: basically the opposite of white hat hackers. Their motivation is to attempt to cause harm or other harm to the user of an infected system, or to obtain property or other advantage. In addition to actually achieving a breach of the hacked system, another criminal element is evident in their actions.
Grey hats - **Grey hats:** this is the grey area of hackers, i.e. people who have not profiled themselves in the direction of these two groups. Occasionally they may violate some rights of others or moral principles, but their actions are not primarily dictated by a desire to cause harm, as is the case with black hats.
The term **cracking** - is associated with the term hacking, sometimes even these terms are confused by the public or in the media. In terms of content, the term cracking means breaking or bypassing the protective elements of a computer system, programmes or applications, with the intention of their subsequent unauthorised use.
Password cracking - is one form of cracking used to establish a password to access a computer system, licensed system or program. As far as copyright cracking is concerned, the cracker usually creates a keygen or crack[25] , which enables the subsequent use of the programme. Such modified programmes are usually made available on warez forums or P2P networks.
Internet piracy - is a general term covering crimes that violate intellectual property rights (very often limited to copyright). It is only with the expansion of computer systems and especially the advent of the Internet that we can speak of mass piracy as one of the most widespread forms of cybercrime.
Intellectual property right - is an intangible good, a so-called material good, which is **the result of a person's creative activity**. This right is **independent of the material substrate** (it can therefore be used anytime and anywhere in the world) provided that it is **unique, non-reproducible and sufficiently original**.
Copyright - protects e.g. original literary and artistic works, musical compositions, television broadcasts, computer programmes, databases, advertising creations, multimedia, etc.
Industrial rights - protect e.g. patents on inventions, designs, industrial models, trademarks, geographical

[23] Most often these are websites, advertising portals, but they can also be social media accounts, etc.

[24] For more details cf. e.g. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal,* 2000, vol. 73, no. 1, pp. 18-24.
YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, vol. 44, no. 4, pp. 387-399.

[25]**Keygen- Key** generator. A program that generates serial numbers or other data. **Crack** - A program used to remove or reduce the functionality of protective elements of another program.

origin, etc.
Software piracy - copyright infringement in relation to computer programmes.
Audiovisual piracy - infringement of copyright in audiovisual works - music and film.
Dissemination of a work by email (a case of copyright infringement in cyberspace) - is the easiest way to disseminate small files (especially copyrighted literary or graphic works).
Interference with computer programs (a case of copyright infringement in cyberspace) - to defeat the copyright owner's technical means of making copies of such protected programs impossible (so-called crack)
Dissemination of a work using data (a case of copyright infringement in cyberspace) - media directly between users (lending and subsequent copying of data from DVD, HDD, etc., sale of media and others).
Recording directly during a screening and subsequent distribution of the recording (e.g. recording a film work directly from the screen) a case of copyright infringement in cyberspace) -camcording.
Unauthorised demonstrations of audiovisual works (a case of copyright infringement in cyberspace) - the actual acquisition of a computer work. A computer program is particularly protected and it is not possible to make copies of such a work, even for personal use, without the consent of the copyright owners under copyright law.
Use of a computer program in breach of a licence.
Posting a work (whether audiovisual or software) in cyberspace (**uploading**) constitutes distribution of the work within the meaning of copyright law and (unless authorised by the author or other authorised person) may be punishable. **It is also an unauthorised use of a work to publish a link to a place in cyberspace from which the work can be obtained.**
Warez - is, in simple terms, **a form of software piracy** in which information technology is merely a means of accelerating the distribution of illegal copies of copyrighted works via the Internet. Warez forums are currently used mainly for downloading cracks and keygen, as well as complete modified programmes, films and music.
Sniffing - is a method of illegally intercepting data passing through a computer network during communication between the service provided and a computer system using a **sniffer.**[26]
DoS - stands for ***denial of service***. It is one form of attack on a (internet) service that aims to disable or degrade the performance of infected technical equipment.[27] This attack is implemented by flooding the compromised computer system (or network element) with repeated requests for the computer system to take action. This attack can also be implemented by flooding information channels between the server and the user's computer or by flooding free system resources.
Distributed Denial of Service (DDoS) - the target computer system is overloaded by **sending packets from multiple computer systems in different locations, making it difficult to defend against and identify the attacker**. This type of attack has been used, for example, against Yahoo! Inc, e-commerce, etc.[28]
DRDoS (Distributed Reflected Denial of Service), is a spoofed distributed DoS attack that uses what is known as a reflection mechanism. The attack involves sending spoofed connection requests to a large number of computer systems, which then respond to these requests, but not to the initiator of the connection, but to the victim. This is because the *spoofed connection requests* have as their source address the address of the victim, which is then flooded with responses to these requests.

[26]Sniffing **is** the English word for snooping or spying. A sniffer is therefore someone who snoops or spies.

[27] For more details, e.g. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO and Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 335-354. CARL, Glenn, Richard BROOKS and Rai SURESH. Wavelet-Based Denial-of-Service Detection. *Computers & Security*, 2006, vol. 25, no. 8, pp. 600-615

RAK, Roman and Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín*, 2007, vol. 14, no. 1, p. 3.

[28] For example, DoS attacks on the websites of the Presidency, Parliament, ministries, media and two Estonian banks - Estonia (2007). *Estonia recovers from massive DDoS attack.* [online]. [cit. 4. 3.2010] Available at: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

Ping-Flood - thanks to the Internet Control Message Protocol and the Ping tool (Packet Internet Groper), it is possible to use the "ping" command to determine the "life" of a computer system with a given IP address and to detect the response time of such a system. In a Ping-Flood attack, the victim is flooded with a large number of so-called ICMP echo request packets, to which the victim begins to reply - sending so-called ICMP Echo Reply packets
Flooding of free system resources (*SYN-Flood*) - is a type of attack in which the attacker attempts to overwhelm his victim with a large number of connection requests. The attacker sends a sequence of SYN command packets (SYN packets) to the target computer system (victim), with the target system responding to each SYN packet by sending a SYN-ACK packet, but the attacker no longer responds. The target computer system waits for a final acknowledgement, a so-called ACK packet, from the initiator of the connection (the attacker) and has allocated resources for this connection, but has a limited number.
Source address *spoofing* (*IP spoofing*) - is the action of forging the source address of sent packets, when an attacker initiating a connection from machine A with IP address **a.b.c.d** inserts e.g. IP address d.**c.b.a** as the source address and sends it to target B. Target B then responds to this source address, i.e. the response is not directed to IP address a.b.c.d, but to IP address **d.c.b.a.**
Smurf attack- is performed by misconfiguring the system to send packets to all computers connected to the computer network via a broadcast address
Dissemination of prohibited types of pornography - these are primarily the dissemination of pornographic material depicting contact with animals and the dissemination (or possession) of 'child pornography' (material depicting or otherwise exploiting a child - a person under the age of 18 or a person who appears to be a child).
Dissemination of hateful and extremist content - the offence includes, in particular, supporting and promoting a movement that clearly aims to suppress human rights and freedoms, expressing sympathy for such a movement, preaching racial, ethnic and national, religious or class resentment or resentment of another group.
Bullying- in the real world it involves an attempt by an attacker to harm, humiliate, ridicule or insult another person, either physically or mentally
Cyberbullying - then moves 'classic bullying' into the virtual world and allows the attacker to use tools and resources that can have a much greater impact on the victim than would be the case in the real world.
Cybergrooming - is an act of psychological manipulation of a person (usually using social engineering), carried out via the Internet or information and communication technologies (e.g. mobile phones, etc.). The aim of cybergrooming is to create false confidence in the victim and thus induce them to meet in person. The result of such an encounter can be any physical, sexual or other attack on the victim. Both children and adults can be victims of cybergrooming. According to statistics, girls aged 13-17 are the most common victims.
Sexting - is one form of dangerous behaviour, especially in the social networking environment, is known as sexting. The term sexting was coined from a combination of the words sex and texting, which makes its meaning clear. It is the electronic dissemination of text messages, photos or videos with sexual content. Such sexually explicit material may be posted on social networks or other data repositories directly by the authors themselves or by another user who has gained access to such material. This is most often done by voluntarily uploading files with sexual content, which are downloaded by the senders themselves.
Cyberstalking is a compound of the words cyber and stalking. Originally, the word stalking was used by hunters hunting game and meant following the game until it was killed.
Cyberstalking is the action of repeatedly contacting the victim, e.g. through text messages, emails, phone calls, VoIP, instant messaging, etc. The attacker's actions usually escalate and usually raise concerns about the victim's privacy, health or life.
Cyberstalkers are characterised by their persistence and systematic nature, and it is not uncommon for a cyberstalker to create multiple false identities, which they use to contact the victim. A cyberstalker may also demonstrate his or her power and strength, for example by publishing information about the victim's life, which he or she can obtain from various online sources.

Identity theft - is an attack in which a virtual identity is stolen[29] , or it is the taking of control (permanent or temporary) of that identity. The motive of the attacker may be financial gain, but also other benefits related to the fact that the attacker is acting on behalf of another person, e.g. access to information about other people, access to company data, etc.
APT - stands for advanced and persistent threat.
APT - is a sustained, systematic cyber-attack focused on a target computer system or the ICT of a target organisation. Different techniques and relatively large resources are used for such an attack, and usually secondary targets (e.g. computer systems, such as repeated DoS or other attacks) may be attacked to distract attention from the primary target (infiltration of the company by malware), which is then attacked.
Cyber-terrorism - is essentially the misuse of ICT (including the internet) as a means and environment to carry out an attack. Like a classic conventional terrorist attack, it is a planned activity, usually politically or religiously motivated and carried out by small rather than militarily organised structures. The aim of these groups is primarily to influence public opinion. Due to the rapid proliferation of information and communication technologies worldwide, cyber-terrorism poses a significant threat and is increasingly used by terrorist groups.[30]
Media terrorism - the planned misuse of mass media and other psychological weapons to influence the opinions of the population as a whole or of targeted populations.

Key quotes from online material:

- In order to understand cyberattacks and cybercrime, it is necessary to know the basic terminology that is directly related to the chosen field. This chapter presents selected technical as well as legal terms.
- It is impossible to find an area of human activity in which computer technology, or rather information, information or communication technology, is not directly or indirectly used.
- It can be argued that, **in principle, it is impossible to find an area of human activity in which computer technology, or an information system or information or communication technology, is not directly or indirectly used**.
- The EU Council Framework Decision 2002/584/JHA on the European Arrest Warrant defines '**computer-related crime'** as conduct directed against a computer or conduct in which a computer is the means to commit a crime. The definition of cybercrime is also based on the wording of the European Arrest Warrant.
- In international conventions, the term '**cybercrime**' is most commonly used to refer to crimes committed by means of information technology, and the use of the term has also been transferred from the normative field to the professional vocabulary. The concept of cybercrime is similar in nature to the terms *'violent crime', 'juvenile crime', 'economic crime', etc. Such terms refer to groups of crimes that have some common factor, such as the method of execution, the person of the perpetrator (at least in terms of type), etc. in essence, it can be a very diverse mix of crimes, linked by a common factor (computer, programme, data).*[31]
- When defining the content of the concept of **cybercrime**, it is important to realise that as the possibility of using ICT devices increases, so does the possibility of using (misusing) them to commit

[29] A virtual identity refers to any identity or avatar used by a person to interact in cyberspace (e.g. email, social network account,games, various online marketplaces, computer system, etc.). It does not matter whether the virtual identity is real or fake, i.e. whether it represents a real person or whether it is a completely artificially created identity with no real basis.

[30] JIROVSKÝ, Václav. *Kybernetickákriminalitanejen o hacking, cracking, virech a trojskýchkoních bez tajemnic.* Prague: Grada, 2007, p. 129

[31]Smejkal, Vladimír. *Kybernetickákriminalita.* Plzeň: AlešČeněk, 2015, p. 19.

a crime. Therefore, in principle, there is no universal, universally accepted definition that fully affects the scope and depth of the concept.

- "Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its elements may appear, or sometimes a larger number of computers either stand-alone or connected in a computer network, and either as the object of interest of that criminal activity (except for such criminal activity whose objects are the described devices treated as immovable property), or as an environment (object), or as an instrument of criminal activity (See Computer Crime)."
- ***Computer crime / Cyber crime*** **-** "A crime committed using or directly related to a data processing system or computer network."
- In the most general terms, cybercrime can be defined as **behaviour directed against a computer, or a computer network, or as behaviour in which a computer is used as a tool to commit a crime**. An indispensable criterion for applying the definition of cybercrime is that the computer network, or cyberspace, is then the environment in which the activity takes place.
- In defining the concept of cybercrime, it is first necessary to **define the concept of crime in general**. With regard to the use of information systems, computer technology or communication devices, there are a number of activities that are certainly undesirable but not punishable under criminal law, although they can be very dangerous (harmful) to society.
- In defining the concept of criminality (and this definition can be given from several points of view - sociological, forensic, etc.), we rely on the definition of criminality as a **compilation of all acts that qualify under the objective element regulated by criminal law**. **Based on this definition, criminality therefore does not include such acts that do not meet any objective element of crime, i.e. not even a misdemeanour or other administrative offence**. This definition of the concept of criminality is relatively precise and can be applied in the field of information and communication technologies.
- Cybercrime, therefore, is a crime involving the means of information and communication technology:
  a) ***used as a tool to commit a crime,***
  b) ***are targeted by the perpetrator*** **and the said *attack* is a** criminal offence,
- **Under the term cybercrime, crimes fall into three different categories:**
  - offences in which the individual object characterising the purpose is directly the protection of the computer system, its devices and components against certain types of attacks or the legitimate interests of persons in the unimpeded use of these technical devices,
  - crimes that are committed by means of information and communication technologies,
  - other qualifying offences which do not fall into either the first or second category, but which, in the case in question, can also be committed using information technology and which meet the above definition, because similar detection procedures can be used to detect them and shed light on them as those used to investigate offences in the first and second categories (e.g. similarly targeted expert opinions).

- **<u>Classification according to the Cybercrime Convention and according to the Additional Protocol.</u>**

The Cybercrime Convention divides cybercrime into four categories:

1. **Offences against the confidentiality, integrity and availability of data and computer systems**;
2. **Computer crime**;
3. **Content-related offences**;
4. **Offences related to the infringement of copyright and related rights**.

- An additional protocol then defines other cybercrimes:
  1. **Dissemination of racist and xenophobic material through computer systems***;*
  2. **A racially and xenophobically motivated threat***;*
  3. **Racist and xenophobically motivated insult***;*
4. **Denying, grossly minimising, condoning or justifying genocide or crimes against humanity.**

- **Classification of the Expert Committee on Cybercrime**

According to the 2000 Statute of the Council of Europe's Committee of Experts on Cybercrime, cybercrime can be divided into:

1. **According to the position of the computer at the time of the offence:**
   - *target of attack;*
   - *means* (tool) *of attack.*
2. **Depending on the type of act:**
   - *traditional infringements* (such as counterfeiting, etc.)
   - *new breaches* (such as phishing, DDoS, etc.)

- **Classification according to eEurope+**

  The document divided computer crime into:

1. **Offences against privacy**
   - Illegal collection, storage, modification, disclosure and dissemination of personal data.
2. **Computer content crime**
   - Child pornography, racism, incitement to violence, etc.
3. **Economic crimes**
   - Unauthorised access, sabotage, hacking, virus transmission, computer espionage, computer forgery and fraud.
4. **Intellectual property offences**[32]

- **Classification of computer crime according to criminology**

  Porada a Konrád[33] divide cybercrime into five basic groups.

1. **Unauthorised interference with data input**
   - changing the input document for computer processing,
   - creation of a document containing false data for subsequent processing by a computer,
2. **Unauthorised changes to stored data**
   - data manipulation, unauthorised data manipulation and subsequent return to normality,
3. **Unauthorised instructions for computer operations**
   - direct instruction to perform the operation or install software that performs the operation automatically,
4. **Unauthorised intrusion into computers, the computer system and its databases**

[32]More details: JIROVSKÝ, Václav. *Kybernetickákriminalitanejen o hacking, cracking, virech a trojskýchkoních bez tajemnic.* Prague: Grada, 2007, p. 92
[33]More details: STRAUS, Jiří et al. *Kriminalistickámetodika.*Plzeň: AlešČeněk, 2006, pp. 272-274

- informational access to a database, without using information,
- unauthorised use of information for personal use,
- alteration, destruction or substitution of information by others,
- illegal 'interception' and recording of electronic communication traffic.

5. **Attack on someone else's computer, software and files and data in databases**
   - development of attack programmes,
   - the introduction of a virus into computer software,
   - infections with viruses or other programmes.

- **<u>Europol's focus on certain types of cybercrime by degree of harm</u>**

Europol adheres to the Cybercrime Convention and complies with the division of offences contained therein. To support the fight against cybercrime and to assist Member States, the European Cybercrime Centre (EC3) was established within Europol[34] . This team has clearly defined its scope of action in the fight against cybercrime and has identified the following three areas (focalpoints - FPs) that it deals with:

FP TERMINAL - Payment Fraud. Group dedicated to providing support in online fraud.

FP Cyborg - High-Tech Crimes. A group dealing with and providing support for various cyber-attacks affecting critical infrastructure[35] and information systems. In particular, these include attacks such as malware, ransomware, hacking, phishing, identity theft, etc.

[34] *Combating cybercrime in the digital age.* [online]. [cited 7.5.2018]. Available from: https://www.europol.europa.eu/ec3.

[35] Regarding the definition of the concept of critical infrastructure, in the Czech Republic (in the case of cyberspace) one should start with the Act on Cyber Security and Amendments to Related Acts (Cybersecurity Act). Hereinafter referred to as the **Cybersecurity Act** or **AoCS.** In Article 2(b), this Act defines the concept of critical information infrastructure and a critical infrastructure element or system.
The definition of the term 'critical information infrastructure' is based on the legislation governing the area of crisis management. Critical information infrastructure is a part of critical infrastructure, which is defined by Act No. 240/2000 Coll. on Crisis Management and Amendments to Certain Acts (the Crisis Management Act), as amended (hereinafter referred to as the Crisis Management Act). In order to be counted as a critical information infrastructure, a specific information system or service and an electronic communications network must meet the definition criteria for critical infrastructure, as well as the critical infrastructure element as defined in the Crisis Management Act, and the cross-cutting and sectoral criteria as defined in Government Regulation No. 432/2010 Coll. on the criteria for defining the critical infrastructure element.
Section VI introduces industry criteria for defining a critical infrastructure element since the effectiveness of the Act and cyber security. "*Communications and information systems", G: cyber security.* Branch-specific criteria for defining a particular information system, service or electronic communications network as a critical information infrastructure element have been established here.
However, this definition only applies to the area of cyber security. In general, **critical infrastructure can be defined as follows**:

1. Critical infrastructure means an element of critical infrastructure or a system of elements of critical infrastructure, the operation of which would result in a significant impact on the security of the State, the satisfaction of the basic needs of life of the population, human health or the economy of the State.
2. Critical infrastructure element means a building, facility, tool or public infrastructure designated according to the cross-cutting and sectoral criteria, which are defined by Government Regulation No. 432/2010 Coll. on the criteria for the designation of critical infrastructure element.
3. The cross-cutting criterion for the designation of a critical infrastructure element is the aspect of
   (a) casualties with a threshold of more than 250 deaths or more than 2,500 people with subsequent hospitalization for more than 24 hours,
   (b) an economic impact with a threshold of economic loss in the country of more than 0.5% of gross domestic product, or
   (c) impact on society with a threshold of significant reduction in the provision of essential services or other serious disruption to the daily lives of more than 125,000 people.

FP Twins - Child Sexual Exploitation. A group dealing with and providing support in the investigation of child sexual abuse.

- **Classification of cybercrime according to its "relationship" with the digital environment**

  With the development of cybercrime as such, an opinion has emerged in recent years that postulates the possibility of viewing cybercrime as an act that can be described as 'pure' or 'true' cybercrime.

  According to the above division, it would then be possible to understand cybercrime as:

  - Narrow concept ('pure' cybercrime);
  - Broad concept ('ordinary' criminal behaviour in a new environment).

- **Cyber-attack**[36] can be defined as **any illegal behaviour by an attacker in cyberspace that is directed against the interests of another person**. These acts do not always take the form of a crime.
- The success of a cyber-attack is usually based on the breach of one of the elements that make up cyber security (**people, processes and technology**). **These elements must be applied or modified throughout the lifecycle**. **In particular, they relate to preventing, detecting and responding to an attack.**
- **A cyber-security event** is "an event *that may cause a breach of information security in information systems or a breach of the security of services or the security and integrity of electronic communications networks*." In reality, it is an event with no real negative consequences for the communication or information system in question. In essence, it is just a threat, but it must be real.
- **A cyber security incident** is "a *breach of information security in information systems or a breach of the security of service provision or a breach of the security and integrity of electronic communication networks as a result of a cyber event*".
- Computer data means *"any expression of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of causing a computer system to perform a function".*
- Information *"is data that has been processed into a form that is useful to the recipient. So any information is information, but any stored data does not necessarily become information."*

Convention on Cybercrime

- **The Convention on Cybercrime and the related Additional Protocol** should be mentioned first, **as these are two of the most important legal documents** that contribute to the protection of society from cybercrime, setting out the basic framework for cybercrime while providing the means to detect and investigate it. EU and EC legal documents related to cybercrime will also be presented
- The Convention on Cybercrime was approved by the Committee of Ministers of the Council of Europe at its 109th meeting on 8th November 2001. The Convention on Cybercrime was opened for signature on 23rd November 2001 in Budapest.[37] The Convention entered into force on 1st July 2004.
- The Cybercrime Convention[38] consists of a **preamble** and **48 articles,** which are divided into 4 chapters:

  Terms used

  Measures to be taken at national level

[36] It is necessary to distinguish the concept of a cyber-attack from that of a **security incident,** which is a breach of IS/IT security and the rules laid down to protect it (security policy).

[37] A list of countries that have signed and ratified the Convention on Cybercrime can be found at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D.

[38] The full text of the Convention can be found at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Part 1 - Substantive criminal law (Articles 2 to 13)

Part 2 - Procedural law (Articles 14-21)

Part 3 - Jurisdiction (Article 22)

International cooperation

Part 1 - General principles (Articles 23-28)

Part 2 - Specific provisions (Articles 29 to 35)

Final provisions

- An important step towards the unification of the law is the identification of four basic groups of offences (see Chapter II; Articles 2-13) and the anchoring of other general substantive criminal law provisions in them.

  Offences against the confidentiality, integrity and availability of data and computer systems. (Articles 2-6),

  Computer offences. (Articles 7-8),

  Content-related offences. (Article 9),

  Offences relating to infringement of copyright and related rights. (Article 10).

- **Council of Europe Additional Protocol 189 to the Convention on Cybercrime**[39] , adopted 28th January 2003.[40] , defines the scope of offences that are not covered by the Cybercrime Convention. The Cybercrime Convention does not cover offences relating to the dissemination of certain "*harmful material*".[41]

- The Additional Protocol consists of a **preamble** and **16 articles,** which are divided into 4 chapters:

1. **Common provisions**
2. **Measures to be taken at national level**
   - Article3 - Dissemination of racist and xenophobic material via computer systems
   - Article 4 - Threats motivated by racism and xenophobia
   - Article 5 - Racially and xenophobically motivated insults
   - Article6-Denying, grossly minimising, condoning or justifying genocide or crimes against humanity
3. **Relationship between the Convention on Cybercrime and the Additional Protocol**
4. **Final provisions**

- If we wanted to define the concept of social engineering, we could say that it involves influencing, persuading or manipulating people in order to force them to take a certain action or to obtain information from them that they would not otherwise give.

- In the case of social engineering, one of the key factors is to gain as much information as possible about the target of the attack (whether it is a computer system, a legal entity or an individual). Often

[39] *ECJ No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.* [online]. [cited.20.8.2016]. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f

[40] A list of countries that have signed and ratified the Additional Protocol can be found at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D

[41] With the exception of child pornography, which is directly included in Article 9 of the Cybercrime Convention.

there is a prolonged interaction with a key person and the building of 'trust' between the attacker and the victim prior to the attack, while the attacker usually exploits people's carelessness, trust, desire to help others, laziness, weakness, fear (e.g. of getting into trouble), irresponsibility, stupidity etc.

- Social engineering attacks are usually carried out in three ways, and these methods are combined:
    1. **Collection of freely** (publicly) **available data** about the target of the attack
    2. **Physical attack** (e.g. the attacker pretends to be an employee of a service agency - e.g. a printer service technician, maintenance man, etc.), in which the attacker tries to obtain as much information as possible "from inside" the company, or sensitive information about individual employees (e.g. through bin searches - dumpster diving)
    3. **Psychological attack**

  The most common methods of social engineering attacks include:

    1. **Fraudulent email** or **fake website**
    2. **Telephone call**
    3. **Face-to-face attack**
    4. **Dumpster diving** as well as "data straining"
    5. **Searching websites, social networks, etc.** (This is an easily accessible, open source of data for social engineering attackers to help identify or verify information about a potential target). **Public information available online** (e.g. online published CVs, theses, papers, proposals, etc.) **Annual reports and other publicly available company information**
    6. **Supply of advertising or other material on CD, DVD or other storage media**
    7. **Leaving a data carrier** (USB, etc.) **in a place of interest** (e.g., at the company, at an employee's home, etc., such a carrier then usually contains malware)
    8. **Offer to try an online service** (e.g., offer of cloud storage, or an interesting service for free, etc.).
    9. **Supply or finding of equipment** (computer system)
    10. **Fake service technician**
    11. **Other**
- A botnet can be most simply defined as a network of software-connected bots[42] , which perform some action based on a command from the 'owner' (or administrator) of that network. A network constructed in this way can be used for legitimate activities (e.g., distributed computing) or for illegal activities.
- Typical of **a botnet** is that if a **target computer system is infected, that system,** known as a 'zombie' or 'bot', **connects to a central control server** [called a command and control (C&C) server]. **The entire system** (containing the zombie and C&C) **is controlled by an attacker** (referred to as a botmaster or botherder) **who controls the bots through the C&C server**.[43]

[42] **Bot** (short for robot). This is a program that can execute the attacker's commands entered from another computer system. The most common way to do this is to infect the computer with a virus such as a worm, Trojan horse, etc. A computer system that is remotely controlled in this way is then referred to as a **zombie**. However, some sources even refer to an infected computer system as a bot.
The bot can collect data, process requests, send messages, communicate with the control element, etc.

[43] For more details see PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011 [online]. [cited.17.5.2015], p. 14. Available from: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence
Further botnet definitions and information can be found, for example, at:

- The following elements are characteristic (essential) of a botnet:
  1. **Command and control (C&C) infrastructure**

     It is an infrastructure that consists of a control element (or elements) and bots (controlled by computer systems).

  2. **Installation and control of the bot**

     This is usually malware that spreads via a botnet or other means. The primary purpose of such malware is to include other computer systems in the botnet. The malware exploits various vulnerabilities in computer systems.

  3. **Controlling bots through C&C infrastructure**

     A bot is software that operates in stealth and uses popular communication channels (IRC, IM, RFC 1459, etc.) to communicate with a C&C server. New bots try to get as much information as possible from the environment and promote themselves to other computer systems.

- Based on the architecture, botnets can be distinguished from:

1. **Centralised architecture**

   This architecture is typically built on the principle of client-server communication. The end computer systems (zombies/bots) communicate directly with the C&C server (the central control element) and execute instructions and use resources from this server.

2. **Decentralised architecture**

   It is usually built on a peer-to-peer (P2P) architecture. This architecture allows resources and commands to be shared within a P2P network. In its 'classic' form, there is no central control element, which makes this system more resistant to attempts to take control through this control element

- It is possible to categorise a botnet as a **crime-as-a-service** structure (where **a** service is offered: **botnet-as-a-service**), or as a malware economy[44] , where it provides the basic technical platform needed to carry out a range of cyber-attacks.

- **Possible criminal sanctions in Poland**

  Illegal access to a system (hacking) Art. 267 § 1 and 2 of the Penal Code. This offence is prosecuted at the request of the victim. It is punishable by a fine, restriction of liberty or imprisonment of up to 2 years.

- **Possible criminal sanctions in the Czech Republic**

  As regards the attacker's own activity of installing malicious software with the aim of subsequently taking control of a computer system, it is possible to assess this behaviour under **section 230 of the** Criminal Code (Unauthorised access to a computer system and storage medium). If the attacker had placed the malware on the computer system with the intention of causing damage or other harm to another person or obtaining an unauthorised benefit for himself or another person, his actions could be qualified under section 230 (2) (d) of the Penal Code.

What je to botnet a jak sešíří?[online]. [cited 15.7.2016]. Available from: https://www.youtube.com/watch?v=ywXqDon5Xtg
Botnets: nováinternetováhrozba. [online]. [cited 15.7.2016]. Available from: http://www.lupa.cz/clanky/botnety-internetova-hrozba/.
Válkysíťovýchrobotů - jak fungujísítěbotnets. [online]. [cited 15.7.2016]. Available from: http://tmp.testnet-8.net/docs/h9_botnet.pdf.
Botnets. [online]. [cited 15.7.2016]. Available from: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6.

[44] Malware management. More details can be found in: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011 [online]. [cited.17.5.2015], p. 21. Available from: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

- **Possible criminal sanctions in Portugal**
  According to Article 6(2) of the *Cybercrime Act, it* is criminalised as illegal access to one or more computer devices to illegally introduce any computer program, executable instruction, code or data intended to be executed illegally into a computer system. The same applies to the offences of damaging computer programs or other computer data [Data Interference] (Article 4(3)), computer sabotage [Illegal Interference] (Article 5(2)), and illegal interception (Article 7(3)).

- **Malware** (a malicious software compound) can be any software used to interfere with the standard operation of a computer system, acquire information (data) or used to gain access to a computer system. Malware can take many forms, and many types of malware are named after the activities they perform

    1. **Adware**
    2. **Spyware**
    3. **Viruses**
    4. **Worms**
    5. **Trojan horses**
    6. **Backdoor**
    7. **Rootkits**
    8. **Keylogger**
    9. **Ransomware**

- The term adware is an abbreviation for 'advertising *supported software*'. It is the least dangerous but profitable form of malware.[45] Adware displays advertisements on the user's computer system (e.g., pop-ups in the operating system[46] or on websites, advertisements displayed together with software, etc.).
- Spyware is a combination of the English words '*spy*' and '*software'*. Spyware is used to obtain statistical data[47] about the operation of a computer system and send it to the attacker's data box without the user's knowledge or consent. This data may also include information of a personal nature or information about the user's person, as well as information about websites visited, applications run, etc.
- Spyware can be installed as stand-alone malware, as well as often as part of other free and otherwise perfectly safe software. In this case, the installation and other activities of spyware are usually dealt with under the terms of the EULA, and the user usually unknowingly voluntarily agrees to monitor their own activity.
- Spyware poses a threat both because it sends various information from the user's computer system to the 'attacker' (which is further processed and correlated with data and information obtained from other sources

[45] There are companies that specialise in "pay per install" (*PPI*). *"PPI" then results in a plethora of actions leading to the installation of add-ons or other unwanted software that (in the least harmful case) lists adverts on websites without the user's knowledge or inserts them where there are no adverts on the website.... **PPI relies on the fact that those offering these services do not care if the user wants to install anything**. **They receive up to US$1.50 per installation**, so it is more than certain that fraudulent and automated installations are an essential part of their 'business model'."*

[46] A drawing of these pop-ups. For more details, see *Adware.* [Online]. [cited 10.8.2016]. Available from: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

[47] E.g. an overview of websites visited, their IP addresses, an overview of installed and used programmes, records of file downloads from the Internet, data on the structure and content of directories stored on the hard drive, etc.

- There are a large number of viruses whose purpose is destructive, while others are designed to 'establish themselves' on as many computer systems as possible and then use them to launch a targeted attack. Typical of these programmes is the ability to spread between systems without user intervention in the computer system.
- Depending on what files the viruses infect, they can be divided into:
    - boot viruses (only infect system partitions)
    - file viruses (only infect files)
    - multicomponent viruses (infect both files and areas of the system)
    - Macro viruses (attack applications that use macros)
- So-called **computer** worms are also **referred to** as viruses. The reason for the closer association with viruses is that worms do not need any host, i.e., they do not have an executable file (like viruses). Unlike viruses, which are included as part of another programme, these programmes usually spread separately. The damaged system is then used by the worm to continue sending copies of itself to other users via network communication.
- **Trojan horses** are generally those computer programmes that contain hidden functions that the user does not consent to or is not aware of, and that are potentially dangerous to the continued operation of the system. As with viruses, these programmes may be bundled with another secure programme or application, or they may look like a harmless computer programme. Trojan horses, unlike classic viruses, are unable to replicate or spread without 'help' from the user. If activated, a Trojan horse can be used, for example, to delete, lock, modify, copy data or disrupt a computer system or computer networks.
- Some Trojans, when launched without the user's knowledge, open the computer's communication ports, which makes it much easier for other malicious programmes to further infect the attacked system or facilitate direct control of the infected computer so-called remotely. Such Trojans are referred to as **backdoors**.[48]
- **Rootkits -** this term refers not only to computer programmes, but also to all technology used to mask the presence of malware (e.g., computer viruses or Trojan horses, worms, etc.) on an infected system. They most often take the form of not very large computer programmes. Rootkits are not harmful in themselves, but are exploited by the creators of malicious programmes such as viruses, spyware, etc.[49]
- A rootkit alters the behaviour of an entire operating system, its parts or additional applications so that users are unaware of the existence of malicious programmes on their computer system. In general, rootkits can be divided into **system** rootkits (which modify the kernel) and **application rootkits** (which modify the application configuration).[50]
- A keylogger is software that records specific keystrokes on an infected computer system. Most commonly, a keylogger is used to record login details (username and password) for accounts that are accessed from the computer system. The information obtained is then usually sent to the attacker.
- Ransomware will be described in more detail in a separate chapter.

Distribution of malware

[48] An overview of the most common Trojans, including a list of their functions and communication ports, can be obtained from various pages available on the Internet. For more details, cf. e.g., http://www.test.bezpecnosti.cz/full.php.

[49] For more details cf. BALIGA, Arati, Liviu IFTODE and Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 323-334.

[50] Cf. RAK, Roman and Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín*, 2007, vol. 14, no. 1, p. 5.

There are many ways in which malware can be delivered to a target computer system.

Several methods of spreading malware.

Malware can be spread through:

Portable storage media

For example, using CDs, DVDs, USBs, an external drive, etc. This is the oldest but still effective way of distributing malware, in which users pass infected files to each other or **computer networks** containing **infected files** (sharing such files within computer networks, usually P2P networks).

Drive-by-download

One of the most common ways to be infected with malware is to download it from the Internet and then run the file, usually with an .exe extension (executable file), from an unknown source. These can be fake or counterfeit programmes (e.g. Flapp Bird imitations, fake multimedia codecs, etc.), programmes used to circumvent copyright protection (crackers, keygenes, etc.**), real infected programmes, etc.**

- **Malware can be installed on almost any computer system.** An example of specific installations is when **micromalware is installed.** This is malicious code that spreads on a relatively small number of computer systems.
- Most Android devices do not allow the operating system to be updated to the latest version, which is usually modified to withstand known security vulnerabilities and already has bugs fixed from previous versions of this operating system. In fact, it is estimated that 77% of threats attacking the Android operating system could be eliminated by using the latest version of this operating system.
- For mobile devices, attackers mainly use:
    - **outdated version of the mobile device's operating system** (known vulnerabilities of individual systems);
    - **minimum protection of the mobile device** with anti-virus measures;
    - **user ignorance** (many users recklessly install applications "from an unknown source" or applications that require excessive access and permissions within the device);
    - **social engineering and 'waves of interest' in applications of a particular type.**

- **Possible criminal sanctions in Poland**
  Violation of data integrity (viruses, trojans) - 268 of the Criminal Code, Art. 268a of the Criminal Code. This offence concerns, among other things, the theft of personal data, making it available to third parties without the owner's consent, and using it in an unauthorised manner. There are financial penalties (up to PLN 100,000) for committing these acts.
- **Possible criminal sanctions in the Czech Republic**
  In the Czech Republic, an attack using malware can be punished under § **230** (Unauthorised access to computer system and information carrier) of the Criminal Code. Possession of malware, with the intention of committing an offence under §182 (Breach of secrecy of transported messages) or an offence under § 230 of the Criminal Code, is an offence under § 231 (Obtaining and possessing passwords to access devices and computer systems and other such data) of the Criminal Code. If the purpose of the virus was, for example, to obtain classified information or to support a terrorist group, the attacker could, for example, commit offences under **Section 311 (Terrorist attack), Section 316 (Intelligence) or Section 317 (Threat to classified information) of the Penal Code in the preparation phase**.
- **Possible criminal sanctions in Portugal**

According to Article 6(2) of the *Cybercrime Act, it* is criminalised as illegal access to create, distribute or disseminate any computer program, executable instruction, code or data intended to perform illegal access to a computer system. The same applies to the offences of damage to computer programs or other computer data [Data Interference] (Article 4(3)), computer sabotage [Illegal Interference] (Article 5(2)) and illegal interception (Article 7(3)), as the Portuguese legislator did not opt for a single provision on the misuse of devices, as the Budapest Convention did (Article 6).

Ransomware

- The malware group also includes so-called extortion malware, for which the term **ransomware was coined**[51] (sometimes also referred to as rogueware or scareware). Ransomware is malware that prevents or restricts users from properly using a computer system until the attacker receives a 'ransom'. Ransomware most often gets onto a user's computer via malware (Trojan horse or worm) that is found on a website or is an email attachment. Once the malware has safely 'established itself' on the computer system, its own ransomware will be downloaded.
- **The first type is ransomware, which restricts the functionality of the entire computer system** and does not allow the user to use the system at all (e.g. by preventing the operating system from starting or locking the system screen. A typical example of this type is '*Police ransomware*' - see below).
- **The second type is ransomware, which leaves the computer system functional but locks the user's data and makes it inaccessible.**
- A second type of ransomware, known as **crypto-ransomware,** is currently in use. The purpose of this malware is to encrypt the hard drive or selected types of files on the computer system. Primarily, it aims to encrypt the user's private files, such as images, text documents or spreadsheets, videos, etc.
- The massive emergence of ransomware can be dated back to around 2011, when a ransomware attack began to spread around the world, blocking access to a Windows user's account and announcing that the computer had been blocked by the state police.
- Various versions (page appearance) of the police ransomware gradually appeared in Europe. The first version was recorded at the end of 2011, it showed the IP address of the connection, the ISP connection and the location [where the IP address of the specific connection provider (ISP) was given], if the user had a webcam on, a picture was created and displayed.
- **Since 2013, there has been a significant shift in ransomware. Attackers have reduced attacks that involved reducing the functionality of an entire computer system and have primarily focused on locking down user data.**
- Crime-as-a-service has offered **ransomware-as-a-service** since 2016**. The** user (i.e. the attacker) has the possibility to define his own ransomware according to his ideas. At the same time, he or she receives technical facilities in the form of C&C servers, bitcoin wallets, 24/7 online support, etc. An example of ransomware-as-a-service is the **Ransom32** software**.**

- **Possible criminal sanctions in Poland**
  The laws that apply in Poland are:
  Article 267 Unlawful obtaining of information

[51]For exampleReventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, JigSawetc. More details can be found, for example, in:
Ransomware. [online]. [cited 14.8.2016]. Available from: https://www.trendmicro.com/vinfo/us/security/definition/ransomware.

Article 269a. Interference with an ICT system or network

- **Possible criminal sanctions in the Czech Republic**
  In the Czech Republic, an attack with malware like ransomware can be punished under § 230 (Unauthorised access to computer system and information carrier) of the Criminal Code. Possession of malware, with the intent to commit an offence under § 182 (Breach of secrecy of transported messages) or an offence under § 230 of the Criminal Code, is an offence under § 231 (Obtaining and possessing passwords to access devices and computer systems and other such data) of the Criminal Code.
  In the case of ransomware, it is also possible to apply the provisions of Section 230 (3) of the Criminal Code when the attacker commits such an offence with the intention of obtaining an unjustified benefit for himself or another person. It is also possible to consider the application of section 175 (Blackmail) of the Criminal Code when a person is coerced into paying an amount by threatening to cause him or her other serious harm (e.g. by filing a criminal complaint[52]]).
- **Possible criminal sanctions in Portugal**
  As in almost all jurisdictions, ransomware attacks are not particularly punishable, although such actions may be prosecuted as extortion. An alternative, from a strictly cybercrime point of view, would be computer fraud (Article 221 of the Criminal Code), as its material scope is quite broad, following the wording of the analogous offence in the text of the *Budapest Convention* (Article 8).

Spam

- From an information and communication technology perspective, the content of the concept of spam can basically be understood on two levels. In **a narrow sense,** it is the mass dissemination of unsolicited messages, usually of an advertising nature via the Internet, and most often via electronic communication. In a **broad sense, spam is** all unsolicited messages received, and thus also messages containing viruses, Trojan horses, etc. [53]
- A characteristic of spam is that it is a **message sent electronically, in bulk and, above all, without request.**
- Scam 419 is the designation for emails, better known as **Nigerian Letters**. These scams are an example of the transfer of ordinary crime (fraud) from the real world to the virtual world.
- A hoax (fiction, joke, press canard) is another form of spam or hoax. The label 'hoax' is used for chain messages (such as: "*pass it on*", "*if you don't send this to 20 other people.... will become...*" etc.) that contain distorted, false, misleading or other false information. The hook often includes attack warnings, threat descriptions, pleas for help, appeals, petitions, celebrity statements, chain letters of good luck, funny messages, pictures and videos in presentations, playing cats and other animals, etc.

[52] For the concept of other serious harm, see ŠÁMAL, Pavel et al. *Trestnízákoník II. § 140 až 421. (Criminal Code II. § 140 to 421). Komentář. (Commentary.)* 2nd Edition. Prague: C. H. Beck, 2012, pp. 1752-1753
Specifically, "the *threat of causing another serious harm may consist of a threat of property damage, serious damage to one's honour or reputation, etc". Another type of serious harm may be the initiation of criminal proceedings as a result of a report of a crime in which the perpetrator threatens the victim by forcing him or her to do, refrain from doing or tolerate something. At the same time, it is irrelevant whether or not the victim has committed the crime of which the report threatens him or her (cf. R 27/1982). "*
[53] To classify spam, cf. forexample GONZÁLES-TALAVÁN, Guillermo. A simple configurable SMTP spam filter: Greylists. *Computers& Security*, 2006, vol. 25, No. 3, pp. 229-236.

- A very effective form of fraud is the various fraudulent offers that can be sent in bulk or in a targeted manner. Nowadays, such offers are sent not only via email, but also via all kinds of instant messaging, social networks, auction sites, etc.
- With regard to **the mass distribution of** fraudulent offers, one can imagine a number of 'pyramid' or 'aeroplane' activities, offers of favourable work at home jobs[54] , 'guaranteed' value methods (with the highest interest rates), offers for a loan (with the lowest interest rates), 'great' job offers, etc.
- **Targeted sending of fraudulent** offers should also include behaviour that is not just spam, but is, for example, a combination of bidding for a certain type of goods on auction portals and subsequent communication with users who have accepted the bid. These are known as 'auction fraud'.

- **Possible criminal sanctions in Poland**
  In Poland, sending unsolicited commercial information by means of electronic communication is considered an offence and is punishable by a fine. This is regulated by the Act of 18 July 2002 on the provision of services by electronic means (Dz. U. of 2002, No. 144, item 1204):
- **Possible criminal sanctions in the Czech Republic**
  As far as criminal sanctions for spam and spammers are concerned, they are currently not fully (re)solved in the Czech Republic. There is no national or international legal protection against this undesirable behaviour. Even the Convention on Cybercrime does not include a definition of spam as a crime.
- **Possible criminal sanctions in Portugal**
- Also in Portugal, generally speaking, spam itself is not considered a criminal offence. However, according to Article 14(1)(f)(g)(h)(i)(j) of Law 41/2004, on data protection and privacy in electronic communications, spammers for commercial purposes have to pay administrative fines, from a minimum of €1,500 to a maximum of €50,000.

Phishing

- The term phishing is most commonly defined as a fraudulent or deceptive conduct aimed at obtaining user information such as username, password, credit card number, PIN, etc.
- In **a narrow sense,** phishing is an activity that requires the user to visit a fraudulent website (displaying e.g. an online banking page, an online shop, etc.) and then fill in 'login information' or the information is requested directly (e.g. when filling in a form, etc.).
- In a **broad sense,** phishing can be defined as any fraudulent behaviour that aims to instil confidence in a user, reduce their vigilance or otherwise force them to accept a scenario prepared in advance by the attacker.
- The principle of a '*classic*' phishing attack usually consists of sending a so-called phishing e-mail to the victim, which at first glance does not arouse any suspicion that it may be a fraudulent message. Such an e-mail usually contains a link that the user is persuaded to click on.
- **Planning a phishing attack**

[54] On the one hand, these offers may consist of a request such as: "*send us $10 to our account and we will send you instructions on how to earn $8,847 per month*". The second possibility is that these job offers do not require any upfront payment, they only require user registration. By registering, the attacker obtains personal information about the user. An email from this company may then be sent to the user's email address, containing, for example, malware etc.

In this phase of the phishing attack, the target (user group) is selected and the method to be used for the attack is chosen. It is assessed what kind of technical security the target uses, the risk of the attacker revealing his identity, etc.

- **Creating the conditions for a phishing attack**

  At this stage, the technical solution to the phishing attack takes place. The attacker acquires lists of e-mail addresses of users to whom the phishing e-mail is to be sent, a data box is created to which the system sends the acquired user data, a trusted message is created which is then distributed to the users.

- **Phishing attack**

  The phishing e-mail is delivered to the individual user and, depending on the quality of the processing of this e-mail and other factors (user experience, user awareness of phishing issues, target's anti-phishing software, etc.), the phishing e-mail is delivered to the user. In this phase of the phishing attack, the user encounters the phishing e-mail for the first time.

- **Data collection**

  Attacker obtains data that has been entered by individual users of the compromised system in a fake website environment.

- **Withdrawal of funds or other gains from a phishing attack**

  Using the data obtained, the attacker accesses the actual bank accounts of individual users and withdraws funds. By transferring to other, especially foreign accounts, diluting these funds and using other techniques, the withdrawn funds become virtually untraceable.

- **Possible criminal sanctions in Poland**

  Breach of secrecy of communication (sniffing) Art. 267 § 3 Penal Code. This type of offence involves obtaining proprietary information, e.g., through sniffers, i.e., programmes that intercept data (passwords and user IDs).

- **Possible criminal sanctions in the Czech Republic**
  In the case of combined forms of phishing attacks, where malware is used to infect a computer, such behaviour by the perpetrator must also be punished under **Section 230** (Unauthorised access to computer system and information carrier) of the Criminal Code. If the aim of the phishing attack is to obtain an unjustified advantage for oneself or another person, the provisions of Section **230 (3) of the Penal** Code may also be applicable.
- **Possible criminal sanctions in Portugal**
  Since the dissemination of malicious software is punishable (Article 6(2) of the Cybercrime Act), as mentioned, the mere creation of inauthentic data would be considered a computer forgery offence (Article 3 of the Cybercrime Act). Besides, if the purpose of such creation is a fraudulent or dishonest intention to obtain, unlawfully, a pecuniary benefit for oneself or for another person, at the expense of the victim, this would also be considered as computer fraud (Article 221 § 1 of the Criminal Code).

Pharming

- **Pharming**[55] is a more sophisticated and dangerous form of phishing. It is an attack on the DNS (DomainName System) server, which translates a domain name into an IP address. The attack occurs

[55] It is a combination of the words farmingi **phreaking**.

when a user types the address of the web server they want to access into their browser. However, he or she will not connect to the correct IP address of the original web server, but to a different, forged IP address.

- **Spearphishing** is one form of phishing attack, but the difference is that spearphishing is a precisely targeted attack, unlike phishing, which is a rather common (random) attack. The target of the attack is usually a specific group, organisation or individual, and specifically information and data within that organisation (e.g. intellectual property, personal and financial data, business strategies, classified information, etc.).

- **Possible criminal sanctions in Poland**
  The same laws apply as for phishing.
- **Possible criminal sanctions in the Czech Republic**
  The punishment for a spearphisher is similar to that for phishing. A terrorist organisation, for example, may be behind a spearphishing attack. In such a case, liability for an offence under **section 311** (terrorist attack) of the Criminal Code is not excluded.
- **Possible criminal sanctions in Portugal**
  The conclusion is the same as for phishing in general, including that related to terrorism.

Vishing

- The term vishing[56] refers to telephone phishing, in which the attacker uses a social engineering technique and attempts to extract sensitive information from the user (e.g. account numbers, login details - name and password, payment card numbers, etc.). The attacker deliberately tries to falsify his or her identity. Attackers often pose as representatives of real banks or other institutions in order to arouse as little suspicion as possible in the user. Vishing is used in Voice over Internet Protocol (VoIP) telephony.

Smishing

- Smishing[57] works on a similar principle to vishing or phishing but uses SMS messages to distribute messages. Smishing is essentially an attempt to get the user to pay an amount of money (e.g., call a toll-free line, send an SMS to a donor, etc.) or click on suspicious URL links. If the user visits such a URL, he or she is redirected to a page that exploits some vulnerability in the computer system, or the user is asked to provide sensitive information or malware.[58]

- **Possible criminal sanctions in Poland**
  The same laws apply as for phishing.
- **Possible criminal sanctions in the Czech Republic**
  The criminal penalties for vishing and smishing are similar to those for phishing.

[56] It is a combination of the words 'voice' and 'phishing'.
[57] It is a combination of the words 'SMS' and 'phishing'.
[58] E.g. Xshqi- *Android Worm on Chinese Valentine's Day.* [online]. [cited 14.8.2016]. Available from: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
Selfmite- *The Android SMS worm Selfmite is back, more aggressive than ever.* [online]. [cited 14.8.2016]. Available from: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

- **Possible criminal sanctions in Portugal**

  Again, the conclusion on criminalisation is the same as for phishing in general, including terrorism-related phishing.

Business Email Compromise

- Business Email Compromise[59] is a type of scam attack in which an attacker impersonates an executive (usually the CEO) and attempts to get an employee, customer or vendor to hand over money or confidential information to the attacker.
- Both small businesses and large corporations are victims of the BEC scam. BEC fraud is linked to other forms of fraud, including but not limited to: romance, lottery, employment and hiring scams.
- BEC attackers rely heavily on social engineering tactics to fool unsuspecting employees and managers. Some of the sample emails have subject lines containing words such as ***request, payment, transfer*** and ***urgent, among others.***

  BEC fraud typically takes one of the following forms:

  1. **"CEO" scam**

     The attackers pretend to be the CEO of the company or another member of the company's management team and send a spoofed email to employees with the option to send wire transfers and instruct them to send funds to the attackers.

  2. **False invoices**[60]

     The company, which often has a long-standing relationship with the supplier, is asked to transfer the funds to pay the invoice to another fake account. The attacker usually contacts the victim via email or telephone. The email attack usually has a crafted source code (header) and subject line of the request, so that it looks very similar to a legitimate request.

[59] BEC fraud is also known as 'CEO fraud' or 'Man-in-the-Email'.

[60] The attack is also referred to as: "The Bogus Invoice Scheme", "The Supplier Swindle" and "Invoice Modification Scheme".

3. **Damage to the account**

   This attack is similar to Fake Invoice. The attacker uses an employee's email account (hacked or spoofed) and then sends an email to customers to inform them that there has been a problem with their payment, and they need to resend it to another account.

4. **Impersonating businessmen and lawyers**

   Victims are contacted by attackers who identify themselves as lawyers or representatives of law firms. The attacker asks for a large transfer of funds to help settle a legal dispute or pay an outstanding bill. The attacker tries to convince victims that the transfer is confidential and time-sensitive, so the employee is less likely to try to confirm whether they should transfer funds.

5. **Data theft**

   A type of BEC that does not aim to directly transfer money. Typical victims of this attack are financial or HR departments/employees. The attacker asks them to send very sensitive data to their account. Social engineering is used, and the data theft attack can be the starting point for the aforementioned financial transfer-oriented BEC attacks.

- **Possible criminal sanctions in Poland**

  In Poland, this is regulated by Article 286 (fraud), which states that:

  § 1. whoever, in order to gain a material profit, leads another person to a disadvantageous disposition of his own or another person's property by means of deception or exploitation of a mistake or incapacity to grasp the intended action, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years.

- **Possible criminal sanctions in the Czech Republic**
  In the Czech Republic, it is possible to punish the conduct described above under **Section 209** (Fraud) of the Criminal Code. Complementing fraud is enrichment. The creation of a replica website and the acquisition of logins and passwords could then be classified as preparation or attempted offence under § 209 of the Criminal Code. If the attacker attempted (§ 21 Penal Code) to gain unauthorised access to another user's account using the access data obtained, such behaviour could also be classified under **§ 230** (Unauthorised access to a computer system and information medium) of the Penal Code.
- **Possible criminal sanctions in Portugal**
  Again, as explained in relation to phishing in general, such acts would be punishable as computer forgery (Article 3 of the Cybercrime Act), as well as computer fraud (Article 221 of the Criminal Code).

Hacking

- The term hacking is currently perceived pejoratively by the public as any action by a person to gain illegal access to someone else's system or personal computer.[61] In the media in particular, the term is generally used to describe any attacker whose actions are directed against information technology or whose activities are based on the use of such technology.

[61] For more details cf. e.g. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal,* 2000, vol. 73, no. 1, pp. 18-24.
YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, vol. 44, no. 4, pp. 387-399.

- Today, hackers themselves use the term hacker for people who have excellent knowledge of ICT systems, computer systems, their operating systems and other software, the principles and mechanisms of networks, and are also excellent programmers able to create their own software in a very short time.

- **Breakdown of hackers**

  It is the motivation for gaining unusual (not necessarily illegal) access, the method of committing such an intrusion, their motivation and their eventual handling of the data obtained, that are the key factors to categorise these individuals into the following three main groups:

  White Hats *(White Hats)*-these are hackers who infiltrate a system by exploiting vulnerabilities in the system's security precisely in order to detect these vulnerabilities and create such mechanisms and barriers that should prevent such attacks. Often, these are employees or external collaborators of reputable companies operating in the field of information technology. Their intrusion into a system does not cause damage or other harm to users; on the contrary, in many cases they alert the administrator of such an infected system to security vulnerabilities. Their activities are essentially non-destructive in nature.

  Black Hast *(Black Hats)*- basically the opposite of white hat hackers. Their motivation is to attempt to cause harm or other harm to the user of an infected system, or to gain property or other advantage. In addition to actually achieving a breach of the hacked system, another criminal element is evident in their actions.

  Grey Hats *(Grey Hats)*-this is the grey area of hackers, i.e. people who have not profiled themselves in the direction of these two groups. Occasionally they may violate some rights of others or moral principles, but their actions are not primarily dictated by a desire to cause harm, as is the case with black hats.

- **Forms of hacking**

  The actual activities of hackers consist of a number of actions. Typical activities used by hackers include:

  1. Social engineering
  2. Breaking passwords[62]
  3. Port scanning[63]
  4. Use of malware to infiltrate a computer system
  5. Phishing
  6. Cross Site Scripting[64]

[62] This is the process of obtaining a password for a computer system. The following are commonly used to crack passwords:
- Bruteforce password guessing (password testing. a sufficiently strong password is prevention);
- Guessing a password based on some knowledge of the user (obtained e.g. from social networks, etc.);
- Use of a dictionary of commonly used passwords (dictionary attack);
- Requesting a password from the system administrator by impersonating an authorised user (The attacker impersonates a forgotten password and tries to recover it).
- Intercepting passwords from unencrypted or insufficiently encrypted network communications between the computer system and the user
- Searching for passwords in data files stored by the system.

[63] This is a method that detects open network ports on a computer system that is connected to a computer network. Based on this discovery, it is possible to determine what services are running on the computer system (e.g. web server, ftp server, etc.). The actual attack is then focused on the detected running services based on their vulnerabilities.

[64] This is an attack that involves hacking into a website. This type of attack uses active elements (scripts) on a website into which malicious code is inserted and then offered to the victim.

7. Eavesdropping on communications

- Probably the most well-known hacker group today is Anonymous.

- **Possible criminal sanctions in Poland**
  The offence of hacking is regulated in Article 267§1 of the Penal Code.
- **Possible criminal sanctions in the Czech Republic**
  As mentioned above, there are a number of activities or attacks that can be categorised as hacking (ranging from password cracking to sophisticated phishing attacks that are combined with social engineering and the use of malware).
  A hacker's actions, which consist solely of using his or her skills to overcome security measures and gain access to a computer system or part of it, can be punished under Section 230(1)(Unauthorised access to a computer system and information medium) of the Criminal Code.

Cracking

- The term **cracking** is associated with the term hacking, sometimes even these terms are mistakenly confused by the public or in the media. In terms of content, the term cracking means breaking or bypassing the protective elements of a computer system, programmes or applications, with the intention of their subsequent unauthorised use.
- **Possible criminal sanctions in Poland**
  The same laws apply as in the case of hacking

Possible criminal sanctions in the Czech Republic

- The perpetrator's actions whereby the protection of a computer system or programme is breached, with the intention of obtaining information and its subsequent unauthorised use, fulfil the objective elements of an offence under Section 230 (1) or (2)(Unauthorised access to a computer system and information carrier) of the Criminal Code. If the purpose of the cracking attack is to obtain an unjustified advantage for oneself or another person, the provisions of Section 230 (3)of the Penal Code may also be applicable.
- **Possible criminal sanctions in Portugal**
  Illegal access to a computer system is itself punishable (Article 6(1) of the Cybercrime Act). In addition, defeating security measures and/or obtaining an undue advantage are not required as objective elements, being considered aggravating offences (Article 6(3) and (4)).
  As mentioned, the illegal creation, distribution or dissemination of any computer program, executable instruction, code or data intended to perform illegal access to a computer system is criminalised as Illegal Access (Article 6(2) of the Cybercrime Act), as an aggravated offence if the perpetrator had access to trade secrets or confidential data, the same in the case of obtaining a relevant undue advantage (Article 6(4) of the Cybercrime Act).

One of the less common, but all the more dangerous, activities is the exploitation of a vulnerability in a web application to run malware in the victim's browser. The victim is then unable to detect this behaviour. The malicious code works in the same way as the rest of the website, and the attacker has the ability to take over browser privileges on the system. More details can be found, for example, in *OWASP, XSS* [online] [cited 15.7.2016]. Available from: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Internet piracy

- The term Internet piracy is a general term covering crimes that violate intellectual property rights (very often limited to copyright). It is only with the expansion of computer systems and especially the advent of the Internet that we can speak of mass piracy as one of the most widespread forms of cybercrime.
- An intellectual property right is an intangible asset, a so-called tangible good, which is **the result of a person's creative activity**. This right is **independent of a material substrate** (it can therefore be used at any time and anywhere in the world) provided that it is **unique, non-reproducible and sufficiently original.**
- Intellectual property rights can be divided into two areas:

  1) **Copyright** (protects e.g. original literary and artistic works, musical compositions, television broadcasts, computer programmes, databases, advertising creations, multimedia, etc.).

  2) **Industrial rights** (protect e.g. patents on inventions, designs, industrial models, trademarks, geographical origin, etc.).
- The most commonly used terms are software **piracy** (with reference to copyright infringement in relation to computer programmes) and **audiovisual piracy** (with reference to infringement of copyright in audiovisual works - music and film). **However, the basis for software and audiovisual piracy is always the infringement of one of the copyright or rights related to copyright**
- Crimes against intellectual property have expanded considerably with the massive emergence of the Internet. The most common cases of copyright infringement in cyberspace include:
  - *distributing a work by e-mail*, which is the easiest way to distribute small files (especially literary or graphic works of authorship),
  - *publishing a work on a website* without the author's consent. This is another very simple way to infringe copyright. Smaller files (in terms of data size) are published and this illegal behaviour is usually detected very early.
  - *distribution of a work by uploading it to a specialised server* from which works can be freely downloaded (e.g. Megaupload, Rapidshare),
  - *dissemination of a work via Peer-to-Peer (P2P) networks*.[65] These networks are capable of transferring/sharing huge amounts of data (in the order of a few GB to tens of TB). These are the most flagrant cases of copyright infringement.
  - *tampering with computer programs in order to defeat the copyright holder's technical means of preventing the creation of copies of such protected programs* (so-called crack),
  - *dissemination of the work by means of data carriers directly between users* (lending and subsequent copying of data from DVDs, HDDs, etc., sale of data carriers, etc.),
  - *recording directly during projection and subsequent dissemination of the recording* (e.g. recording a film work directly from the screen) - camcording,
  - *unauthorised demonstrations of audiovisual works,*
  - *the actual acquisition of a computer work*. A computer program is particularly protected and it is not possible to make copies of such a work, even for personal use, without the consent of the copyright owners under copyright law,
  - *use of a computer program in breach of a licence,*

[65] By connecting to a P2P, the user, by default, starts to automatically share their content with other users (usually unknown to them). Usually, when downloading, the upload of the downloaded material is automatically set.

- **Posting a work** (whether audio-visual or software) in cyberspace (**uploading**) constitutes distribution of the work within the meaning of copyright law and (unless authorised by the author or other authorised person) may be punishable. **It is also an unauthorised use of a work to publish a link to a place in cyberspace from which the work can be obtained.**

Warez

- The term 'Warez' often comes up in connection with internet piracy. Warez **is**, in simple terms, **a form of software piracy** in which information technology is merely a means of accelerating the distribution of illegal copies of copyrighted works over the Internet. Warez forums are currently used mainly for downloading crack and keygen, as well as complete modified programmes, films and music. The final product of the warez scene is called a **release**.

- **Possible criminal sanctions in Poland**
  Intellectual property issues in Poland are regulated by two basic legal acts: the Copyright and Neighbouring Rights Act and the Industrial Property Law Act.
- **Possible criminal sanctions in the Czech Republic**
  File sharing, whether on warez or P2P networks, can be punished under section **270** (Infringement of copyright, copyright-related rights and database rights) or under **section 231** (Means and storage of computer system access devices and passwords and other such data) of the Penal Code.
- **Possible criminal sanctions in Portugal**
  In general, such acts are punishable as unauthorised copying, distribution and sale of works and/or as counterfeiting of copyrighted works (Articles 195 and 196 of the Copyright and Related Rights Code).

Sniffing

- Sniffing is a method of illegally intercepting data passing through a computer network during communication between the service provided and a computer system using **a sniffer.**[66]

- **Possible criminal sanctions in Poland**
  In Poland, sniffing (sniffing) is an offence punishable according to:
  Breach of secrecy of communication (sniffing) Art. 267 § 3 CC.
- **Possible criminal sanctions in the Czech Republic**
  Such an action can practically be described as **illegal interception and recording of telecommunications traffic**. The behaviour described above will certainly interfere with fundamental human rights and freedoms, in particular **Article 13 of the Charter, and it is completely indifferent whether the illegal sniffing is carried out by an external attacker or by a network administrator.** According to criminal law norms, it would be possible to subsume such behaviour under **Section 182(1)** (Breach of the secrecy of communications) of the Penal Code, and in the case of misuse of the information thus obtained, it could be an offence under **Section 182(2) of the** Penal Code.

[66]Sniffing is the English word for snooping or spying. Sniffer is therefore someone who snoops, sniffs or spies.

- **Possible criminal sanctions in Portugal**
  Such an action falls within the scope of Illegal Interception (Article 7 of the Cybercrime Act), but also the sharing and making available of any content may be considered a Breach of Secrecy of Correspondence or Telecommunications (Article 194 of the Criminal Code).

DoS

- The term DoS is an abbreviation for '***denial of service***'. It is one form of attack on a (internet) service that aims to disable or reduce the performance of infected technical equipment.[67] This attack is carried out by flooding the compromised computer system (or network element) with repeated requests for it to take action.
- The difference between DoS, DDoS and DRDoS attacks lies mainly in how the attack is carried out. For clarity, the different types of attack are accompanied by drawings demonstrating how the attack is carried out.
- In the case of **DoS (Denial of Service), the** source of the attack is one. This type of attack is relatively easy to defend against, as it is possible to block traffic from the attack source.
- With **Distributed Denial of Service (DDoS),** the target computer system is overloaded by **sending packets from multiple computer systems in different locations, making it difficult to defend against and identify the attacker**. This type of attack has been used, for example, against Yahoo! Inc, e-commerce, etc.[68] Botnets or the actions of users supporting a specific internet campaign (see below - Anonymous and LOIC) are very often used for this type of attack.In the case of **DRDoS (Distributed Reflected Denial of Service),** it is spoofed DoS attack, which uses a so-called reflection mechanism. The attack consists of sending fake connection requests to a large number of computer systems, which then respond to these requests, but not to the initiator of the connection, but to the victim.
- DoS, DDoS, DRDoS attacks very often exploit flaws such as the operating system, running programmes or network protocols - UDP, TCP, IP, http etc.
- There are several basic methods of DoS or DDoS attack, the most well-known being:

  Flooding with the ping command (*Ping-Flood*)

  Thanks to the Internet Control Message Protocol and the Ping tool (Packet Internet Groper), it is possible to use the 'ping' command to determine the 'life' of a computer system with a given IP address and to detect the response time of such a system.
  Flooding of free system resources (*SYN-Flood*)
  SYN-Flood is a type of attack in which the attacker attempts to overwhelm its victim with a large number of connection requests. The attacker sends a sequence of SYN command packets (SYN packets) to the target computer system (victim), with the target system responding to each SYN packet by sending a SYN-ACK packet, but the attacker no longer responds.

---

[67] For more details, e.g. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO and Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 335-354.
CARL, Glenn, Richard BROOKS and Rai SURESH. Wavelet-Based Denial-of-Service Detection. *Computers & Security*, 2006, vol. 25, no. 8, pp. 600-615
RAK, Roman and Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín*, 2007, vol. 14, no. 1, p. 3.

[68] For example, DoS attacks on the websites of the Presidency, Parliament, ministries, media and two Estonian banks - Estonia (2007). *Estonia recovers from massive DDoS attack.* [online]. [cit. 4. 3.2010] Available at: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

Source address *spoofing* (*IP spoofing*)

IP Spoofing is the action of forging the source address of sent packets, when an attacker initiating a connection from machine A with IP address a**.b.c.**dw sets as the source address e.g. IP address **d.c.b.**ai sends it to target B. Target B responds to this source address, i.e. the response is not directed to IP address a.b.c.d, but to IP address **d.c.b.a.**

Smurf attack

This attack is performed by misconfiguring the system to send packets to all computers connected to the computer network via a broadcast address.

- The aim of DoS/DDoS attacks **is** usually **not to infect a computer** or computer system**,** nor to **defeat the security features of the password** protecting it**,** but to **overwhelm or temporarily disable it with a** series of repeated requests. This usually results in restricted or blocked access to services.

- **Possible criminal sanctions in Poland**

  In this case, Article 268 of the Criminal Code applies.

- **Possible criminal sanctions in the Czech Republic**

  It follows from the wording of the provisions of Article **230(2)** (Unauthorised access to computer system and information carrier) of the Criminal Code:

  Whoever gains access to a computer system or storage medium and

  (a) makes unauthorised use of data stored in a computer system or on a storage medium, (b) deletes or otherwise destroys, damages, modifies, suppresses or corrupts the quality of data stored in a computer system or on information media, or renders it unusable without authorisation....

  It follows from this provision that an attacker committing a DoS or DDoS attack must gain unauthorised access to a computer system and then suppress the data within it in order to be held criminally liable.[69]

- **Possible criminal sanctions in Portugal**

  Such acts undoubtedly fall within the scope of computer sabotage [Illegal Interference] (Article 5(1) of the Cybercrime Act), possibly as an aggravated offence in the case of serious damage to or disruption of critical infrastructure or other essential services (Article 5(5)).

Dissemination of unwanted content

- Currently, two basic types of dissemination of undesirable content can be described. The dissemination of prohibited types of pornography and the dissemination of hateful and extremist content.

- **Possible criminal sanctions in Poland**

  In Poland, the following article of the Criminal Code applies:
  Article 200b. Public promotion of paedophile content
  Article 202 Presentation and dissemination of pornography.

- **Possible criminal sanctions in the Czech Republic**

  In the case of the creation, possession or distribution of material covered by the term child pornography, it is possible to punish the user under **section 192** (Production and other handling of

[69]Suppression means the action listed in Article 4 of the Cybercrime Convention.

child pornography), section **193** (Use of a child in the production of pornography) of the Penal Code. It is also an offence to take part in a pornographic or other similar performance involving a child (**section 193a of the Penal Code**). It is also an offence to access child pornography by means of information or communication technology (section **192 (2) of the Penal Code**).

- **Possible criminal sanctions in Portugal**
  Such acts, depending on the case, are criminalised differently. On the one hand, they can be considered as child pornography offences (Arts. 176 CC). On the other hand, they constitute Aggravated breach of privacy (Arts. 191(1)(b) and 197(b) of the Penal Code) or as Revenge pornography related to domestic violence (Art. 152(2)(b) of the Penal Code (Art. 193() of the Penal Code).

Cyber-attacks on social media platforms

- Within social media, it is possible to commit most of the cyber-attacks described earlier (e.g. malware, phishing, spam, etc.). The reason why cyber-attacks on social media platforms have been described separately is that they occur primarily (but not exclusively) in the social media environment.
- Cyberbullying then moves 'classic bullying' into the virtual world and allows the attacker to use tools and resources that can have a much greater impact on the victim than would be the case in the real world. Cyberbullying, through the use of ICTs and the persistence of data in cyberspace, allows for repeated attacks on the victim, even if the victim has geographically moved away in the real world from where they were originally harassed.
- **The most common manifestations of cyberbullying:**
  Gossiping, bullying, insulting, ridiculing or otherwise embarrassing (social networks, e-mail, SMS, chat, ICQ, Skype, games, etc.).

  Acquiring sound recordings, videos or photographs, processing them graphically or otherwise, and then publishing them in order to harm (ridicule) a selected person.

  Making videos in which the victim is physically attacked or otherwise psychologically abused and ridiculed. These videos are then published on the Internet (this is known as Happy Slapping).

  Creating websites, social media accounts (modifying original ones or creating new profiles), discussion sites, etc. that insult, denigrate or humiliate a specific person.

  Abuse of someone else's account - identity theft (email, discussion, etc.).

  Provoking and attacking users in discussion forums (chat rooms, etc.).

  Discovering other people's secrets.

  Blackmail using a mobile phone or the internet.

  Harassment and pursuit by calling, writing messages.

- **Possible criminal sanctions in Poland**
  In Poland, this is regulated by:
  Art. 212 CC - Defamation and Art. 190 § 1
- **Possible criminal sanctions in the Czech Republic**
  Cyberbullying (like classic bullying) is not in itself a crime or an offence. It always depends on the actions of the harasser. If such action was a form of, for example, physical harm to the victim, blackmail or intimidation, then the application of, for example, section 146 (Bodily Harm) or section

145 (Grievous Bodily Harm), section 175 (Extortion) of the Criminal Code could be considered. In the case of harassment and prosecution of a person, Section 354 of the Penal Code (dangerous prosecution) could be applied.

- **Possible criminal sanctions in Portugal**
  As such, cyberbullying is not a criminal offence. However, it can be considered a form of stalking (Art. 154-A of the Penal Code), but also sexual harassment, insult, defamation, grave invasion of privacy, and even discrimination and incitement to hatred and violence (Arts. 170, 181, 180, 192 and 197 (b) and 240, all of the Penal Code).

Cybergrooming

- Cybergrooming is an act of psychological manipulation of a person (usually using social engineering), carried out via the Internet or information and communication technologies (e.g. mobile phones, etc.). The aim of cybergrooming is to induce false confidence in the victim and thereby induce a personal meeting. The result of such an encounter can be any physical, sexual or other attack on the victim. Both children and adults can be victims of cybergrooming. According to statistics, the most common victims are girls between the ages of 13 and 17.

- **Possible criminal sanctions in Poland**
  In June 2010, an amendment to the Penal Code came into force. A completely new type of offence appeared in the Penal Code, regulated in Article 200 a KK, the so-called grooming, i.e. seduction via the Internet. It concerns persons who, by means of an ICT system or a telecommunication network, establish contact with a minor under 15 years of age with the aim of misleading them, taking advantage of their error or inability to grasp the situation properly or unlawfully threatening a meeting. This offence is punishable by up to three years' imprisonment.

- **Possible criminal sanctions in the Czech Republic**
  A person committing cybergrooming may, by his or her actions, fulfil the objective elements of certain offences set out in the Criminal Code. As a general rule, depending on the nature of the attacker's behaviour, these will amount to offences under the provisions of § 168 (Human trafficking), § 171 (Unlawful deprivation of liberty), § 175 (Extortion), § 185 (Rape), § 187 (Sexual abuse), § 201 (Threat to child custody), § 209 (Fraud), § 353 (Dangerous threat), § 354 (Dangerous prosecution) of the Criminal Code.
- **Possible criminal sanctions in Portugal**
  Solicitation of children for sexual purposes by means of information and communication technology is a criminal offence (Article 176-A of the Criminal Code).

Sexting

- One form of dangerous behaviour, especially in the social networking environment, is so-called sexting. The term sexting was coined from a combination of the words sex and texting. It is the electronic dissemination of text messages, pictures or videos with sexual content.

- **Possible criminal sanctions in Poland**

  According to Polish law, the following are prohibited:

  - production for dissemination;
  - recording;
  - dissemination;
  - presentation;
  - possession and storage;
  - Imports

  pornographic material with the participation of a minor - a person under the age of 18 (Article 202 CC).
- **Possible criminal sanctions in the Czech Republic**
  If photographs of another person are published without their consent, it is possible for them to assert their rights in civil proceedings
- **Possible criminal sanctions in Portugal**
  Sending such content to another adult can be prosecuted as sexual harassment (Art. 170 CC). However, if someone sends such content to a third party, it will be considered defamation, oppressive invasion of privacy, oppressive domestic violence or even discrimination and incitement to hatred and violence (Articles 180, 152, 192 and 197 (b) and 240, all of the Criminal Code).

Cyberstalking

- Cyberstalking is the act of repeatedly contacting the victim, e.g. through text messages, emails, phone calls, VoIP, instant messaging, etc. The attacker's actions usually escalate and usually raise concerns about the victim's privacy, health or life.
- *Cyberstalkers are* characterised by their persistence and systematic *nature*, and it is not uncommon for a cyberstalker to create multiple false identities, which they use to contact the victim.
- The cyberstalker can also demonstrate its power and strength, for example by publishing information about the victim's life, which it can obtain from various online sources.

- **Possible criminal sanctions in Poland**
  According to the Polish Penal Code, stalking can be committed in two ways. Through persistent harassment of a punished person (Article 190a § 1 of the Penal Code) or through impersonation (Article 190a § 2 of the Penal Code). The qualification of a specific behaviour as stalking depends on the perpetrator fulfilling several conditions.
- **Possible criminal sanctions in the Czech Republic**
  Stalking or cyberstalking can fall under **section 354** (Dangerous pursuit) of the Criminal Code under certain conditions. The basic conditions include that the stalker must contact the victim "*persistently by electronic, written or other means*" over a long period of time and such action is capable of causing reasonable fear for the life or health of the victim or the life and health of the victim's relatives. An aggravating circumstance under **Article 354 § 2 (a) of the** Criminal Code is if the said act was committed to the detriment of a child
- **Possible criminal sanctions in Portugal**
  Recently, stalking, including, cyberstalking has become a criminal offence as stalking (Article 154-A of the Criminal Code).

Identity theft

- Identity theft is an attack in which a virtual identity is stolen[70] , or it is the taking of control (permanent or temporary) of that identity. The motive of the attacker may be financial gain, but also other benefits related to the fact that the attacker is acting on behalf of another person, e.g. access to information about other people, access to company data, etc.

- **Possible criminal sanctions in Poland**
  Pursuant to Article.190 a § 2 of the Penal Code, whoever, by impersonating another person, uses that person's image or other personal data in order to cause material or personal damage to that person, shall be liable to imprisonment for up to three years.
- **Possible criminal sanctions in the Czech Republic**
  If the security is defeated and unauthorised access is gained to the victim's identity, the offence under **section 230 (1)** (Unauthorised access to computer systems and information media) of the Penal Code will be fulfilled. By using malware for the same purpose, the attacker commits an act under section 230 (2) of the Penal Code. If the purpose of identity theft is to obtain an unjustified advantage for oneself or another person, the provisions of Section **230 (3) of the** Penal Code may also be applicable. If the attacker steals an identity with the aim of deceiving another person, i.e. misleading someone in order to enrich himself or herself, such conduct may also be assessed under **Section 209** (Fraud) of the Penal Code
- **Possible criminal sanctions in Portugal**
  Pretending to be someone else is no longer punishable. However, creating inauthentic data for legally relevant purposes would be considered computer forgery (Article 3 of the Cybercrime Act). Furthermore, if the purpose of such impersonation is to fraudulently or dishonestly intend to unlawfully obtain a pecuniary benefit for oneself or another person at the victim's expense, this would also be considered computer fraud (Article 221(1) of the Criminal Code).

APT

- APT stands for advanced and persistent threat. It is a sustained systematic cyber-attack focused on the target computer system or ICT of the targeted organisation. Different techniques and relatively large resources are used for such an attack, and usually secondary targets (e.g. computer systems, such as repeated DoS or other attacks) can be attacked to distract attention from the primary target (infiltration of the company by malware), which is then attacked.
- During an APT attack, attackers may use other different types of attacks on the chosen target, depending on the data and information acquired.

[70] Virtual identity means any identity or avatar used by a person to interact in cyberspace (e.g. email, social network account, game, various online marketplaces, computer system, etc.). It does not matter whether the virtual identity is real or fake, i.e. whether it represents a real person or whether it is a completely artificially created identity with no real basis.

- **Possible criminal sanctions in Poland**
  When analysing the APT attack from the point of view of violations of the law in force in Poland, it should be recognised that if the attack had been carried out at all its stages, at least several criminal offences would have been committed. According to the applicable law, an APT attack can be considered as:
  - hacking under Article 267 § 1 of the Criminal Code.
  - the offence of making or providing computer devices or programmes, passwords and codes under Article 269b of the Penal Code
  - computer fraud under Article 287 of the Penal Code
- **Possible criminal sanctions in the Czech Republic**
  The possible criminal sanction of the attacker(s) carrying out the APT attack then depends entirely on their actions, which may take the form of, for example, malware distribution, one of the phishing attacks, Identity Theft, etc.
- **Possible criminal sanctions in Portugal**
  An APT attack is not specifically criminalised, even as an aggravated offence.

Terrorism

- Terrorism can be divided by form into *lethal* and *non-lethal forms,* where the first group is characterised by the use of commonly available means of violence (*conventional* - attacks committed with commonly available weapons such as firearms, and non-conventional - the misuse of weapons of mass destruction). In contrast, non-lethal **forms of terrorism**[71] or attacks using more modern tools in combination with lethal means are more common online.
- The conventional form of non-lethal terrorism includes the following subgroups:

  - *Unarmed terrorism*.

  - *Cyber terrorism* - one of the greatest threats of the 21st century. The principle is primarily the misuse of ICT (including the internet) as a means and environment to carry out an attack. Like a classic conventional terrorist attack, it is a planned activity, usually politically or religiously motivated and carried out by small rather than militarily organised structures.

Media terrorism, in which there is a planned misuse of media and other psychological weapons to influence the opinions of the general population or target groups

- **Possible criminal sanctions in Poland**
  In Poland, Articles 265 to 269 and Article 287 of the Criminal Code apply to the implementation of a cyber-terrorist attack, and depending on the effect of the cyber-terrorist attack, some other articles of the Criminal Code may also apply, such as:
  Article 163 Causing a catastrophe
  Article 164 Causing a danger of disaster
  Article 165 Causing public danger
  Article 173 Causing a road traffic accident
  Article 174 Causing an imminent danger of a traffic disaster

[71] However, a combination of these attacks can be imagined. More details can be found, for example, in: *Exclusive: Computer virus hits US drone fleet.* [online]. [cited 10.7.2016]. Available from: https://www.wired.com/2011/10/virus-hits-drone-fleet/.

- **Possible criminal sanctions in the Czech Republic**
  From the point of view of criminal law, the aforementioned acts may fulfil the objective elements of the offences under Section 311(2) (terrorist attack), Section 355 (defamation of a nation, race, ethnic group or other group of persons), Section 356 (incitement to hatred against a group of persons or suppression of their rights and freedoms), Section 364 (incitement to an offence), Section 403 (creating, supporting and promoting movements aimed at suppressing human rights and freedoms) and Section 404 (expressing sympathy for movements aimed at suppressing human rights and freedoms) of the Penal Code.
- **Possible criminal sanctions in Portugal**
  According to the Counter-Terrorism Law No. 52/2003, if the offences are related to terrorist purposes, the penalties for offences such as computer fraud or computer forgery will be increased by one third (Article 4(2)). In addition, penalties for offences relating to electronic communication (Article 4(3)(4)), recruitment (Article 4(5)(6)) or promotion of terrorist groups or activities are enhanced if committed via the Internet (Article 4(8)(9)).

3. During classes

Some ideas for activities:

WORKSHOPS

1. Analysis of individual cyber-attacks and their subsumption under the provisions of the Cybercrime Convention (ECJ No. 185) and national law (Czech Republic, Poland, Portugal).
2. Analysis of individual attacks - modus operandi
3. Testing security against selected attacks.
4. Definition of options for preventing particular types of attack
5. Designing a customised solution to protect against individual cyber-attacks.
6. Security testing of certain systems, applications and data. Students will attempt to design their own solutions to enhance the security of these systems, applications or data.
7. Familiarisation with tools and resources for secure data storage and setting up secure online communication (e.g. VPN administration and settings, PGP, password manager, etc.).

REVIEW QUESTIONS

1.

- What is cybercrime?
- What is not a cyber crime?
- What is a cyber-attack?
- What is the difference between cybercrime and cyberattack?
- What is the difference between data and information?
- What is the CIA triad?

2.

- What is characteristic of social engineering?
- What is a botnet and how does it work?

- What are typical botnet topologies?
- Can it be considered a criminal offence to own a botnet?
- What is malware?
- What are the most common examples of malware?
- What are the most common malware infection vectors?
- What is ransomware and what are its manifestations?
- What is phishing and how is this attack most commonly carried out?
- What is the difference between phishing and pharming?
- What is hacking?
- What is characteristic of cracking?
- What is the difference between hacking and cracking?
- What is a DoS attack and how does it work?
- What is the difference between DoS and DDoS?
- What can be included in the distribution of defective content?
- What is APT?

Working in pairs/groups

- **Pairs - mini-project**
  In pairs, students choose one of the topics discussed. They write down their conclusions and present them to the others. After the presentation, the other students prepare additional questions for the presenting group.

- **Map of thoughts**
  Students in pairs choose one of the topics covered and create a mind map, which they then describe to the other students in a short presentation.

- **Keywords**
  Students in pairs individually select key words from the glossary.

  They write the definitions of these words on strips of paper. They turn the strips over with the blank side up. A student chooses a strip, reads the definition and the other student looks for a matching keyword.
  or
  Students write some key words from the glossary on a piece of paper. They turn the cards over with the blank side up. One student takes the first card and says what the word means. The second student guesses the key word.

- 10 keywords
  Students choose 10 keywords related to their chosen topic. These 10 keywords are given to other pairs. The pairs write a text that must contain all the keywords. One sentence can only contain one keyword. So the text consists of at least 10 sentences.

- **Panel discussion**

  Students choose 3 speakers. Each speaker chooses one topic to discuss. The other students ask questions about the topics. Each speaker can use a -TRUE X FALSE answer type. The student gets a point for each true answer, e.g. Does GDPR stand for GENERAL DATA PROTECTION REGULATION? - TRUE X FALSE.

4. Internet resources

See bibliography below

5. Additional questions/tests

SELECT THE CORRECT ANSWER:
(The correct answer has been highlighted)

1. _____ can be defined as behaviour directed against a computer or, in some cases, a computer network, or as behaviour in which a computer is used as a tool to commit a crime.

   a) Cyber hacking
   b) Cybernetic effect
   (c) Cyber-attack
   d) Cybercrime

2. _____ can be defined as any illegal behaviour by an attacker in cyberspace that is directed against the interests of another person.

   a) Cyber incident
   (b) Cyber-attack
   d) Cyber accident
   (c) Cyber-assault

3. Computer _____ means "any expression of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of causing a computer system to perform a function."

   (a) concepts
   (b) guidance
   (c) time limits
   (d) data

4. _____ is "a breach of information security in information systems, or a breach of the security of service provision, or a breach of the security and integrity of electronic communication networks as a result of a cyber event."

(a) Cyber security crime
b) Achieving cyber security
c) Weakening of cyber security
(d) Cybersecurity incident

5. _____ cannot be considered directly applicable across the board to a cyber-attack, but it is a condition for the success of many cyber-attacks.

(a) civil engineering
(b) social engineering
(c) cybernetic engineering
(d) criminal engineering

6. _____ can most simply be defined as a network of software-connected bots that perform some action based on a command from the 'owner' (or administrator) of that network.

(a) Bennet
(b) Mask
(c) Botnet
(d) Bootnet

7. _____ are generally those computer programmes that contain hidden functions that the user does not consent to or is not aware of, and which are potentially dangerous to the continued operation of the system.

a) Data theft
(b) Pharming
c) Rootkits
(d) Trojan horses

8. The term _____ is most commonly used to describe fraudulent or deceptive behaviour aimed at obtaining user information such as usernames, passwords, credit card numbers, PINs, etc.

(a) phishing
(b) spyware
(c) backdoor
(d) worms

9. What does BEC stand for?

a) Business Economy Certificate
(b) Business Email Compromise
c) Contribution to the business effort
d) Business Efforts in Cyberspace

10. The term _____ is now seen pejoratively by the public as any action by a person to gain illegal access to someone else's system or personal computer.

(a) malware
(b) adware
(c) hacking
(d) fraud

11. The term _____ is an umbrella term covering crimes that infringe intellectual property rights (very often limited to copyright).

(a) Internet pirate
(b) Internet perceptions
(c) Internet piranha
(d) Internet piracy

12. What does DDoS stand for?

(a) Disturbed Denial of Service
(b) Distributed Denial of Service
c) Divided Day of Service
(d) Disastrous Deadlock of Service

13. What does APT stand for?

a) Advanced persistent threat
b) Advanced criminal threat
c) Advanced perceived threat
(d) Advanced trivial threat

Bibliography

1. *The 10 most notorious hacking groups.* [online]. [cited 15.7.2016]. Available from: https://www.hackread.com/10-most-notorious-hacking-groups/.
2. *7 types of hacker motivation.* [online]. [cited 16.8.2015]. Available from: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/.
3. *7 types of hackers you should know.* [online]. [cited 16.8.2015]. Available from: https://www.cybrary.it/0p3n/types-of-hackers/.
4. *Advanced Persistent Threat - life cycle*[online]. [cited 20. 8. 2016]. Available from: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg.
5. *Advanced Persistent Threat (APT).* [online]. [cited 20. 8. 2016]. Available from: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.
6. *Advanced Persistent Threat.* [online]. [cited.20.8.2016]. Available from: https://www.isouvislosti.cz/advanced-persistent-threat.
7. *Advanced persistent threats: How TheyWork.* [online]. [cited 10.7.2016]. Available from: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1
8. *Adware.* [online]. [cited 10.8.2016]. Available from: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking.
9. *Android Ransomware now targets your Smart TV, Too!* [online]. [cited 14.8.2016]. Available from: https://thehackernews.com/2016/06/smart-tv-ransomware.html
10. *Market share distribution of Android versions among smartphone owners as of May 2016.* [online]. [cited 14.8.2016]. Available from: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/
11. BALIGA, Arati, Liviu IFTODE and Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers& Security*, 2008, vol. 27, no. 7-8, pp. 323-334.
12. *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cited 14.8.2016]. Available from: https://www.hackread.com/fake-android-prisma-app-phishing-malware/
13. *Botnet - a historical list of botnets.* [online]. [cited 15.8.2016]. Availablefrom: http://www.liquisearch.com/botnet/historical_list_of_botnets
14. *Botnet.* [cited 8.7.2016]. Available from: http://research.omicsgroup.org/index.php/Botnet.
15. *Botnet.* [online]. [cited 15.7.2016]. Available from: https://en.wikipedia.org/wiki/Botnet.
16. *Botnets.* [online]. [cited 15.7.2016]. Available from: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6.
17. *Bots and botnets - a growing threat.* [online]. [cited 11.8.2016]. Available from: https://us.norton.com/botnet/
18. *Buffalo Spammerjde na 7 let za mřížekvůlirozesílánínevyžádanépošty.*[online]. [cited 14.8.2016]. Available from: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality.
19. CARL, Glenn, Richard BROOKS and Rai SURESH. Wavelet-Based Denial-of-Service Detection. *Computers& Security*, 2006, vol. 25, no. 8, pp. 600-615
20. CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, [cited 19.3.2014]. ISBN 978-1-921532-33-7. Available from: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

21. *Combating cybercrime in the digital age.* [online]. [cited 7.5.2016]. Available from: https://www.europol.europa.eu/ec3.
22. *Computer-generated 'Sweetie' catches online predators.* [online]. [cited 19.8.2016]. Available from: http://www.bbc.com/news/uk-24818769
23. Convicted spammer challenges Va. law[online]. [cited 14.8.2016]. Available from: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm
24. *Cyber-terrorism: how dangerous is the threat from the ISIS cyber-caliphate?* [online]. [cited 20.8.2016]. Available from: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html
25. *Cybercrime*. [online]. [cited 1.2.2015]. Available from: http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; et al.
26. *Digital Doom's Digi World*, 2008. ISSN 1802-047X. [online]. [cited 14.8.2016]. Available from: http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html.
27. *Disturbing ISIS video shows militants beheading four inmates and a gunman cornering shoppers at a market.* [online]. [cited 20.8.2016]. Available from: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017
28. Additional Protocol. ECJ No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189
29. DODGE, Ronald. C., Curtis CARVE ANDAARON J. FERGUSON. Phishing for user security awareness. *Computers& Security*, 2007, vol. 26, no. 1, pp. 73-80.
30. *Estonia recovers from powerful DDoS attack.* [online]. [cited 4. 3.2010] Available from: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack.
31. *Exclusive: Computer virus hits US drone fleet.* [online]. [cited 10.7.2016]. Available from: https://www.wired.com/2011/10/virus-hits-drone-fleet/.
32. *Combating cybercrime: cyber patrols and cyber investigation teams as a reinforcement of EU strategy.* [online]. [cited.10.7.2016]. Availablefrom: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827
33. *Flappy Bird Clones Help Mobile Malware Rates Soar*[online]. [cited 14.8.2016]. Availablefrom: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx
34. *FLocker Mobile Ransomware crosses to Smart TV.*[online]. [cited 14.8.2016]. Available from: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/
35. *France drops controversial 'Hadopi law' after spending millions*[online]. [cited 15.7.2016]. Available from:https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy etc.
36. *Fridge caught sending spam in botnet attack.* [online]. [cited 17.5.2016]. Available from: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/.
37. GONZÁLES-TALAVÁN, Guillermo. A simple configurable SMTP spam filter: Greylists. *Computers&Security*, 2006, vol. 25, No. 3, pp. 229-236.
38. GOODMAN, Marc. A *vision of crime in the future.*[online]. [cited.13.11.2014]. Availablefrom: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071
39. *Google says the best phishing scams have a 45 per cent success rate.* [online]. [cited 14.8.2016]. Available from: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/

40. GREENBERG, Andy. *Hackers remotely kill Jeep on highway - with me inside.* [online]. [cited 4.5.2016]. Available from: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
41. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal,* 2000, vol. 73, No. 1, pp. 18-24.
42. GŘIVNA, Tomáš and Radim POLČÁK. *Kyberkriminalita a právo*. Prague: Auditorium, 2008.
43. HILL, Kashmir. *These two Diablo III players stole virtual armour and gold - and were prosecuted IRL*. [online]. [cited 10.8.2015]. Available from: http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/
44. *A historical list of botnets.* [online]. [cited 15.8.2016]. Available from: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html.
45. *Historical maps of computer networks*. [Online]. [cited 10.7.2016]. Available from: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html.
46. *How do APTs work? The Lifecycle of Advanced Persistent Threats (Infographic).*[online]. [cited 10. 7. 2016]. Available from: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/
47. *How to use Wireshark to capture, filter and inspect packets.* [online]. [cited 15.7.2016]. Available from: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/
48. *Islamic State hacking division.* [online]. [cited.20.8.2016]. Available from: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355.
49. *Jessica Logan - 'The Rest of the Story'.*[cited 8.8.2016]. Available from: http://nobullying.com/jessica-logan/.
50. *Judge, 69, who downloaded child porn threatens 'catastrophic humiliation'.* [online]. [cited 1.9.2009]. Availablefrom: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo
51. *Kevin Mitnick Case: 1999* [online]. [cited 2.11.2011]. Availablefrom: http://www.encyclopedia.com/doc/1G2-3498200381.html
52. KOLOUCH, Jan, Pavel BAŠTA et al. *Cyber security*. Prague: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
53. KOLOUCH, Jan. Evolution ofPhishing Campaigns and Business Email Compromise in the Czech Republic. In: *Academic and Applied Research in Military and Public Management Science*. Budapest: National University of Public Service, 2018, pp. 83-100. ISSN 2498-5392.
54. KOLOUCH, Jan. *Cybercrime.* Prague: CZ.NIC, 2016. ISBN 978-80-88168-15-7.
55. KOLOUCH, Jan iAndrera KROPÁČOVÁ. Ransomware. In: ZHUANG, Xiaodong. *Recent Advances in Computer Science: Proceedings of the 19th International Conference on Computers*. B.m.: B.n., 2015, pp. 304-307. Recent Advances in Computer Engineering Series, [No. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109.
56. LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly Media, pp. 32-41. ISBN 978-1449388393.
57. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modeling and analysis of active worm spreading based on P2P systems. *Computers& Security*, 2007, vol. 26, no. 3, pp. 213-218.
58. *Malware, mayhem, and the McColo takedown*[online]. [cited 14.8.2016]. Available from: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/
59. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO and Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers& Security*, 2008, vol. 27, no. 7-8, pp. 335-354.

60. MELOY, Reid J. *STALKING (OBSESSIONAL FOLLOWING): A REVIEW OF SOME PRELIMINARY STUDIES.* [online]. [cited 3.10.2015]. Available from: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf.
61. MITNICK, Kevin D. and William L., SIMON. *Ghost in the Wires: my adventures as the world's most wanted hacker*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.
62. MITNICK, Kevin D. *The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley, 2006. ISBN 0-471-78266-1.
63. MUELLER, Robert. [Online]. [cited 3.4.2013]. Available from: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.
64. *New Ransomware encrypts game files.* [online]. [cited 14.8.2016]. Available from: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/
65. NIGAM, Ruchna. *Timeline of mobile botnets.* [online]. [cited 12.7.2016]. Available from: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf.
66. *OWASP, XSS* [online]. [cited 15.7.2016]. Available from: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
67. *Password Sniffer Spy.* [online]. [cited 18.8.2016]. Available from: http://securityxploded.com/password-sniffer-spy.php.
68. *Phishing activity report. Tresnds.* [online]. [cited 14.8.2016]. Available from: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf
69. *Phishing by the Numbers: Must-Know Phishing Statistics 2016.*[online]. [cited 14.8.2016]. Available from: https://blog.barkly.com/phishing-statistics-2016
70. PLETZER, Valentin. Unmasking spyware. *CHIP*, 2007, no. 10, pp. 116-120.
71. PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection &Defence.* ENISA, 2011 [online]. [cited.17.5.2015], p. 14. Available from: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence
72. PROSISE, Chris and Kevin MANDIVA. *Incident Response & Computer Forensic, 2nd ed.* Emeryville: McGraw-Hill, 2003.
73. RAK, Roman and Radek KUMMER. Informačníhrozby v letech 2007-2017. *security magazín*, 2007, vol. 14, no. 1, p. 4.
74. *Ransomware.* [online]. [cited 14.8.2016]. Available from: https://www.trendmicro.com/vinfo/us/security/definition/ransomware.
75. SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing.*[online]. [cited 6.11.2007]. Available from: https://www.schneier.com/crypto-gram/archives/2002/1215.html.
76. SCHNEIER, Bruce. *The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters.*[online]. [cited 10.8.2016]. Available from: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster
77. SCHNEIER, Bruce. *Seven types of hackers.* [online]. [cited 16.8.2015]. Available from: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html.
78. SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis. *Computers& Security*, 2007, vol. 26, No. 5, pp. 361-372.
79. Selfmite - *Android SMS worm Selfmite is back, more aggressive than ever.* [online]. [cited 14.8.2016]. Available from: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

80. *Spam statistics and facts.* [online]. [cited 14.8.2016]. Available from: http://www.spamlaws.com/spam-stats.html
81. *Spam statistics*. [online]. [cited 14.8.2016]. Available from: https://www.spamcop.net/spamstats.shtml.
82. *Stuxnet.* [online]. [cited.23.7.2016]. Available from: https://cs.wikipedia.org/wiki/Stuxnet.
83. *Journal of targeted cyber-attacks.* [online]. [cited 10.7. 2016]. Available from: https://apt.securelist.com/#secondPage
84. TAYLOR, Harriet. *How the 'internet of things' can be disastrous.* [online]. [cited 17.6.2016]. Available from: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html.
85. *TCP handshake step by step.* [online]. [cited 18.8.2016]. Available from: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000.
86. *Organised crime online threat assessment (iOCTA) 2014.* [online]. [cited 10.8.2015]. Available from: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
87. *The Malware Museum @ Internet Archive*. [online]. [cited 17.5.2016]. Available from: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/.
88. *Testimony of a former hacker.* [online]. [cited 26.9.2008]. Available from: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html
89. *The first mobile malware: how Kaspersky Lab discovered Cabir*. [online]. [cited 29.6.2015]. Available from: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
90. Tinba: *W32. Tinba (Tinybanker).* [Online]. [cited 15.8.2016]. Available from: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf.
91. *July 2016 Tip of the Month - Avoid getting hooked by Phishing*. [online]. [cited 14.8.2016]. Available from: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/
92. *Top Spammer Sentenced to Nearly Four Years*[online]. [cited 14.8.2016]. Available from: http://www.pcworld.com/article/148780/spam.html
93. Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
94. *United Nations manual on the prevention and control of computer crime.* [online]. [cited 20.8.2016]. Available from: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf
95. *Warning! Over 900 Million Android Phones Vulnerable to New 'QuadRooter' Attack.* [online]. [cited 10.8.2016]. Available from: https://thehackernews.com/2016/08/hack-android-phone.html
96. *WATCH: ISIS Downs Prisoners Alive & Blows Hostages Up With RPG & Kills Others With Explosives - Graphic video.* [online]. [cited 20.8.2016]. Available from: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382
97. WILSON Tracy,V.*How Phishing Works*[online]. [cited.14.8.2016]. Available from: http://computer.howstuffworks.com/phishing.htm.
98. Xshqi - *An Android worm for Chinese Valentine's Day.* [online]. [cited 14.8.2016]. Available from: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
99. YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, vol. 44, no. 4, pp. 387-399.
100. ZETTER, Kim. *Can passengers hack commercial airliners?* [online]. [cited 5.5.2016]. Available from: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

Module 4

CSIRT and CERT

1. Introduction

1.1 Course summary

The course focuses on cyber security and introduces the student to the principles of establishing cyber security. In order to understand the whole issue, it is also necessary to know the rights and responsibilities of security teams and their tasks, roles and processes. A significant part of the course covers CERTs and CSIRTs (structure, hierarchy) and the legal anchoring of CERTs and CSIRTs (rights and responsibilities). In addition, the topic of incident handling (IH) should not be overlooked. Open-source analysis within IH, data and information transfer capabilities are also key topics that form an essential part of this part of the course.

1.2 Course objectives

Security incidents, cyber-attacks and ICT-related crimes in the real and virtual worlds are becoming more serious and their consequences and effects are getting worse. There is a growing need to improve the defence against these attacks and, in particular, to improve the environment and means of tracking down the perpetrator, to standardise and formalise procedures and to educate users on how to identify, deal with and, ideally, prevent threats and risk situations. To this end, an infrastructure of security teams such as CERTs and CSIRTs is being built. The aim of the course is to familiarise students with these security teams, their functioning, hierarchy, accreditation process, data and information sharing capabilities, etc. In addition, students will explore the Information Security Management System. Finally, they will discover the importance of data protection in cyberspace.

1.3 Course content

Individual lectures introduce students to the topic of cyber security. Furthermore, students are introduced to the principles of setting up a cyber security and security team (tasks, roles, processes, etc.) One of the key topics is CERTs and CSIRTs (structure, hierarchy) and the legal anchoring of CERTs and CSIRTs (rights and responsibilities). In addition, students study the rights and responsibilities of security teams. Incident handling (IH), open source analysis within IH and data and information transfer capabilities are also extremely important, so the last part of the lectures is dedicated to them.

1.4 Learning objectives

1) Introduction to the principles of creating cyber security
2) Defining risks, assets, vulnerabilities
3) Understanding cyber threats and other key terms
4) Getting to know CERTs and CSIRTs
5) Definition of the legal framework for CERTs/CSIRTs

1.5 Equipment and materials required

CSIRTs and CERTs - available online

Directive (EU) 2016/1148 (NIS Directive)

1.6 Syllabus

Learning outcome	The student who successfully completes the module will know/be competent in the following.
NEWS	
W1	The student will gain information about the historical development of security teams operating in the Internet environment. The student will know the roles of the different security teams and the legal basis for their operation.
SKILLS	
U1	Understands the workings of security teams such as CERTs and CSIRTs, learn about their structure and the links between the teams.
U2	Understanding the issue of incident handling.
COMPETENCES	
K1	He will be able to act as a member of the safety team.

Content of the module (programme of lectures and other activities)	**Reference to learning outcomes**
LECTURES 1. Cyber security 2. Principles for establishing cyber security 3. Security team (tasks, roles, processes, etc.) 4. CERTs and CSIRTs (structure, hierarchy) 5. Legal powers of CERTs and CSIRTs (rights and obligations) 6. Rights and responsibilities of safety teams 7. Incident handling (IH) 8. IH open source analysis 9. Data and information transfer capabilities WORKSHOPS 1. Building a safety team	W1, U1, U2, K1

Methods of verifying learning outcomes

Learning outcome	**Forms of credit classes**								
	Oral examination	Written examination	Partial written assignment	Final written assignment (essay etc.)	Test	Project/presentation	Report	Classroom activities	Other ...
NEWS									
W1		x			x			x	
SKILLS									
U1						x		x	
U2						x		x	
COMPETENCES									
K1						x		x	

ECTS credit balance		
Form of student workload		Number of hours
Number of hours with direct participation of academic teacher		
1.1	Participation in lectures	10
1.2	Participation in seminars	
1.3	Participation in workshops	8
1.4	Participation in laboratory activities	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times per semester)	
1.7	Participation in the project consultation	
1.8	Participation in examinations/tests	2
1.9	Other ...	
1.10	**Number of hours spent with direct assistance of academic staff (sum 1.1 - 1.9)**	20
1.11	**Number of ECTS credits obtained by the student in classes requiring direct participation of an academic teacher)**	1
Individual student work		
2.1	Individual studies (including e-learning lectures)	25
2.2	Individual preparation for workshops	10
2.3	Individual test preparation	
2.4	Individual preparation for laboratory classes	
2.5	Preparation of reports	
2.6	Implementation of self-performed tasks (projects, documentation)	
2.7	Preparation for the final examination/tests of the workshop	5
2.8	Preparation for final examination/testing of lectures	5
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 - 2.9)**	45
2.11	**Number of ECTS credits obtained by the student in individual teaching assignments**	1,5
Total workload (h)		**65**
ECTS credits for the module		**2,5**

Criteria for assessing student competence
The minimum requirements for the three groups of learning outcomes that the Student must achieve in order to pass the subject are presented below in synthetic form. In order for a Student to pass a module, all learning outcomes described in the syllabus must be positively verified by the person(s) teaching the module.

W - KNOWLEDGE
Assessment:
Satisfactory - The student remembers and reproduces the knowledge to be mastered within the module.
Good - The student additionally interprets phenomena / problems and is able to solve a typical problem
Very good -Student is able to solve even complex problems in a given field, is able to synthesise, carry out a comprehensive evaluation, create a work that is original and inspiring to others.

U - SKILLS
Assessment:
Satisfactory - The student knows the nature of the activities and is able, under the guidance of the academic teacher, to carry out activities / solve problems related to the content of the module
Good - Student is able to independently carry out activities / tasks / solve typical problems related to the content of the module
Very good - The student has fully mastered the ability / skill to perform the activities / tasks / problems

provided for in the module content, also in more complex cases.

K - SOCIAL COMPETENCE
Assessment:
Satisfactory - Student passively assimilates module content, demonstrating ability to concentrate and listen
Good - Student actively participates in classes, makes value judgements according to the criteria accepted in the given field, can actively cooperate in a group
Very good - The student integrates the attitude according to the proposed model, develops his/her own system of professional and social values, is able to take responsibility for the actions of the group, including leadership.

2. Basic material for the teacher

Definitions (glossary)

Security - a state in which threats to a facility (most often a nation-state or even an international organisation) and its interests are reduced to the lowest possible degree, and the facility is effectively equipped and willing to cooperate to eliminate existing and potential threats."[72]
Security - a characteristic of an object or entity that determines the degree to which it is protected from potential harm and threats."[73]
Security - The property of an item (e.g. an information system) that is protected at some level against loss, or the state of being protected (at some level) against loss. IT security includes the protection of confidentiality, integrity and availability in the processing, storage, distribution and presentation of information. [74]
Cyber security - is the set of measures that are taken to protect a computer system from unauthorised access or attack. [75]
Cyber security is the **state in which we are protected from criminal or unauthorised use of electronic data**. Cyber security then encompasses the measures that need to be taken to achieve this state.[76]
Cyber security - is "**a set of** legal, organisational, technical and educational **measures designed to ensure the protection of cyberspace.** "[77]
Cyber security - represents **a set of** organisational, political, legal, technical and educational **measures and tools aimed at ensuring a safe, protected and resilient cyberspace in the Czech Republic,** both for public and private sector entities and for the Czech public in general." [78]
Cyber security - refers to the security of cyberspace, with cyberspace itself referring to the set of links and relationships between objects that are accessible via the general telecommunications network, and the

[72] ZEMAN, Petr et al. *Czech security terminology: interpretation of basic concepts* [online]. [cited 2018-07-10]. Available from: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 , s. 13
[73] *POŽÁR, Josef. Information security*. Pilsen: AleščČeněk, 2005, p. 37.
[74] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 23 [online]. [cited 2018-07-10]. Available from: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[75] *Cybersecurity.* [online]. [cited 2018-07-06]. Available from: https://www.merriam-webster.com/dictionary/cybersecurity Author's translation.
[76] *Cybersecurity.* [online]. [cited 2018-07-06]. Available from: https://en.oxforddictionaries.com/definition/cybersecurity Author's translation.
[77] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 69 [online]. [cited 2018-07-10]. Available from: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[78] *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [cited 2018-07-01]. Available from: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf p. 5

actual set of objects whose interfaces enable them to be remotely controlled, remotely access data or engage in control activities in cyberspace
The definition of cyber security according to Polish law is - the resistance of information systems to actions that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems
Cybersecurity - can be defined as: the totality of legal, organisational, technical and educational measures to ensure the protection of computer systems and other ICT elements, applications, data and users,
Cybersecurity-can be defined as: the ability of computer systems and services used to respond to cyber threats or attacks and their effects, and to plan for the recovery of the functionality of computer systems and related services.
CIA - stands for C - **Confidentiality**; **I** - **Integrity**; **A - Accessibility**
Computer data - means "**any expression of facts, information or concepts in a form suitable for processing by a computer system,** including a program capable of causing a computer system to perform **a** function."
Information "is data that has been processed into a form that is useful to the recipient. So all information is data, but any data stored does not necessarily become information."[79]
Information - is seen as something more 'qualified' than data. Data are facts that become information when they are perceived or expressed in context and carry meaning that people can understand.[80]
Top secret - unauthorised handling of information could cause extremely serious damage to state interests.
Secret - unauthorised handling of the information could cause serious damage to state interests.
Confidential - unauthorised use of the information could cause ordinary damage to the interests of the state.
Restricted - unauthorised use of the information could be detrimental to the interests of the state.
Protected - Unauthorised handling of the information could cause serious damage or destruction to the organisation (e.g. leakage of strategic information, source code, security schemes, passwords, etc.).
Internal - unauthorised handling of information could cause damage to the organisation (e.g. leakage of personal data, contracts, etc.).
Sensitive - unauthorised handling of information could have negative consequences for the company (e.g. unpublished information on projects, planned events, etc.).
Public - unauthorised use of information should not harm anyone and should not affect the public (e.g. publicly available contacts, project presentations, etc.).[81]
TLP stands for **Traffic Light Protocol**
Accessibility - is defined as "the property of being available and usable at the request of an authorised entity."
IDS - abbreviation for IntrusionDetectionSystém (intrusion detection system)
IPS - abbreviation for IntrusionPreventionSystém (intrusion prevention system)
Risk - is "(1) Danger, the possibility of harm, loss, failure. (2) The impact of uncertainty on the achievement of objectives. (3) The possibility that a threat will exploit the vulnerability of an asset or group of assets and cause harm to the organisation."[82]
Risk - can also be defined as the potential for a threat to materialise and exploit the vulnerability of an asset.
Risk- is defined as '**any reasonably identifiable circumstance or event that could adversely affect the security of networks and information systems.** '

[79] POŽÁR, Josef. *Information security.* Pilsen: AlešČeněk, 2005, p. 25
[80] ŠÁMAL, Pavel et al. *Kodekskarny II. §§ 140-421. commentary.* 2nd ed. Prague: C. H. Beck, 2012, p. 2308
[81] Cf. further: ŠULC, Vladimír. *Cybersecurity.* Plzeň: AlešČeněk, 2018. p. 20 ff.
[82] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015. p. 99. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

Asset - anything of value to a person, organisation or country**.**
Asset - from a civil law perspective, **an asset** can be **a tangible thing** (building, computer system, network, energy, commodity, etc.) **or an intangible thing** (information, knowledge, data, programmes, etc.).
Asset - can also be **property** (e.g. availability and functionality of the system and data, etc.) or **reputation,** etc. **People** (users, administrators, etc.) and their knowledge and experience are also an asset from a cyber security perspective.
Support assets - are the technical resources, employees and contractors involved in the operation, development, management or security of an ICT system
The primary asset is the information or service processed or provided by the ICT system.
Vulnerability - refers to a weakness in an asset, software or security that is exploited by one or more threats.
Threat - can most simply be defined as something capable of disrupting the normal or orderly state of affairs and interfering with the rights of others. It is a negative action that may or may not be carried out
A threat is considered to be "any phenomenon that has the potential to cause harm to the interests and values protected by the State. The degree of threat is determined by the magnitude of the potential harm and the temporal distance (usually expressed in terms of probability or risk) of the possible application of that threat."[83]
Hazard - is defined as "the potential cause of an unintended event that could cause damage to a system or organisation." [84]
Information Security Threat[85] - is defined as "the potential cause of an adverse event that could result in damage to the system and its assets, such as destruction, unwanted access (compromise), modification of data or unavailability of services." [86]
Cyber threat - is the possibility of a malicious attempt to damage or disrupt a network or computer system.[87]
A cyber **threat can** also be defined as an action aimed at altering[88] information, applications or the system itself.
Information leakage is when protected information is disclosed to an unauthorised party.
An integrity breach is the corruption, alteration or deletion of data.
Service suppression means deliberately preventing access to information, an application or a system.[89]
Illegal use is the use of information by an unauthorised party or in an unauthorised manner.[90]
"Computer security incident" (which can be understood as a computer attack or computer crime) -an illegal, unauthorised, unacceptable action involving a computer system or network.
A security incident - is "**an event that may cause or lead to a breach of** information systems and technologies and the rules defined to protect them (security policy)."[91]
Security event - is an **identifiable** system, service or network **condition indicating a possible breach of**

[83] *Jeopardy.* [online]. [cited 2018-07-28]. Available from: http://www.mvcr.cz/clanek/hrozba.aspx.
[84] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 52. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.
[85]In this case, we may notice a problem with the translation of some terms from English and vice versa. If we would like to consistently translate the term Information securitythreat, the correct Czech equivalent is e.g. threat to informationsecurity; threat to information security, etc.
[86] Ibid p. 25
[87] *Cyberthreat.* [online]. [cited 2018-07-06]. Available from: https://en.oxforddictionaries.com/definition/cyberthreat.
[88] Alteration also means stealing information, destroying it or thwarting its use.
[89]These include attacks such as **DoS - Denial of Service**, **DDoS - Distributed Denial of Service**, etc. More details can be found in the book KOLOUCH, Jan. *Cybercrime.* Prague: CZ.NIC, 2016, p. 295 ff.
[90] For example, a fee-based system is compromised and its services are used without payment for services.
[91] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015. p. 28. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

security policy or failure of security measures
A cyber security incident - is **an event that may cause a breach of the security of information in information systems or a breach of the security of services or the security and integrity of electronic communications networks.**
Information security incident - one or more unintended or unexpected security events that have a high probability of compromising an organisation's operations and compromising information security
Computer security incident - is a breach or imminent threat of a breach of security policies, acceptable use (system, service) policies or standard security practices."[92]
Cyber security incident - is a **breach of information security in information systems or a breach of service security or the security and integrity of electronic communications networks as a result of a cyber incident.**
Cyber-attack - "an attack on IT infrastructure to cause damage and obtain sensitive or strategically important information. It is most often used in the context of politically or militarily motivated attacks."[93]
Cyber-attack[94] - can be defined as **any deliberate action by an attacker in cyberspace that is directed against the interests of another person.**
Cybercrime - can be defined **as an action directed against a computer system, computer network, data or users, or as an action in which a computer system is used as a tool to commit a crime.**
CERT - stands for Computer Emergency Response Team
CSIRT - abbreviation for Computer Security Incident Response Team
CERT/CSIRT - can be **understood as the same type of team - a team that is responsible for handling security incidents and (cyber) threats in its clearly defined area of operation, from the perspective of users or other teams, a place to turn to with a detected security incident, requesting cooperation, information exchange, assistance, etc.**
Scope of the team - defines what the team is responsible for and what its role is. This of course depends on what kind of team it is.
In-house team - operates and is responsible for a specific network (e.g. a specific range of IP addresses, domains), and is usually appointed by the network operator.
Coordination team - a team whose main task is to coordinate the resolution of security incidents, not to solve them.
Vendor team- the team dealing with security incidents that involve a specific product (SW).
National/governmental team - special cases based on the principles of the first two teams mentioned (internal and coordination team), their scope and role depends on the founder and often on the legislation of the specific country.
Back-office - a tool for effective management of security incident reports that will trace the entire lifecycle of the report, i.e. when the report was sent, by whom, who dealt with the incident at what stages, why, how it was handled, who asked whom to cooperate, how serious the incident was and what escalation procedures were applied to it, etc.
The organisational basis is the aforementioned 'readiness' to solve the problem, i.e. defining the basic rules of the team, so that each team member knows his or her role, duties and responsibilities, security incident handling policy, rules for communication, information sharing and exchange, cooperation, etc. The basis in this area is generally well-managed so-called **incident management.**
FIRST stands for Forum for Incident Response and Security Teams
TF-CSIRT (Task Force for CSIRT) - is a working group that enables teams to collaborate through regular two-

[92] *Computer security incident handling guide* **[online]. [cited 2018-02-17]**, p. 6**. Available from:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[93] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015. p. 71. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[94] It is necessary to distinguish the concept of a security incident from that of a cyber-attack, which is a breach of IS/IT security and the rules defined to protect it (security policy).

day meetings held 3 times a year (the host of this meeting is usually the CERT/CSIRT team).
CSIRT training - is used to train new CSIRT/CERT team members or those who are just about to set up a CERT/CSIRT team. It is usually held twice a year and trainers are experienced members of reputable CERT/CSIRT teams and other top security experts.
Trusted Introducer[95] - an office whose main role is to build trust between CERT/CSIRT teams and help establish new ones.
The team with the status **listed** provided basic information about itself, declared its willingness to act as a CSIRT team and was accepted by the community.
A team with **accredited** status declares the level of practice desired by the community and commits to the common principles of TI.
The certified team then demonstrated their 'maturity level' through a certification process.
ENISA - means the European Network and Information Security Agency.
RIR - abbreviation for Regional Internet Registries
Incident handling - the process of reporting and resolving security incidents.
Botnet Feed- this tool is used to process data from downloaded C&C servers about end stations connected to botnets. In order to identify a potentially infected computer system, the IP address and information about the botnet to which it is connected are passed to the IP range manager.
IHAP - short for Incident Handling Automation Project
MDM - short for Malicious Domain Manager
Indicators of compromise - abbreviation IoC
Shadow server- the project focuses on the continuous search for relevant information about cyber vulnerabilities and the occurrence of these vulnerabilities on specific IP addresses.

Key quotes from online material:

- The word **cyber** signifies interdependence with elements of information and communication technology and cyberspace as such.
- Mareš defines security as "*a state in which threats to an object (usually a nation-state or even an international organisation) and its interests are reduced to the lowest possible degree, and the object is effectively equipped and willing to cooperate to eliminate existing and potential threats."*[96]
- *The property of an item (e.g. an information system) that is protected at some level against loss, or the state of being protected (at some level) against loss. IT security includes the protection of confidentiality, integrity and availability in the processing, storage, distribution and presentation of information.* [97]
- This widening of the circle of security necessitates addressing the following issues, among others:
  Whose security is at stake (international organisation, state, organisation, individual, etc.).
  What values are protected (organisations, people, data, etc.)**?**
  What are (should be) these values protected against (physical, cyber, combined attacks, etc.)**?**
  What resources are needed to protect these values? [98]

[95] Longer also **TI**.
[96] ZEMAN, Petr et al. *Czech security terminology: interpretation of basic concepts* [online]. [cited 2018-07-10]. Available from: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13
[97] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 23 [online]. [cited 2018-07-10]. Available from: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[98] More details can be found, for example, in MAREŠ, Miroslav. *Security.* [Online]. [cited 2018-07-10]. Available from: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511.

- In defining cyber security itself, it is useful to rely on established definitions. I will list some such established definitions:
    - **Cyber security** is a **set of measures that are taken to protect a computer system from unauthorised access or attack**. [99]
    - The Oxford Dictionary states that **cybersecurity** is **a state of protection against criminal or unauthorised use of electronic data**. Cybersecurity then encompasses the measures to be taken to achieve this state.[100]
    - According to Jirásek et al. **cyber security** is *"**a set of** legal, organisational, technical and educational **measures designed to ensure the protection of cyberspace.** "*[101]
    - The Czech Republic's National Cyber Security Strategy 2015-2020 defines cyber security in a relatively similar way, stating that *"Cyber security is a **set of** organisational, political, legal, technical and educational **measures and tools aimed at ensuring a safe, protected and resilient cyberspace in the Czech Republic**, both for public and private sector entities and for the Czech public **in** general."* [102]
- **The following principles, also known as the cyber triad, are implemented in the application of cyber security.**[103]
  For the purposes of this monograph, the following three triads will be defined:

  CIA [**C** - **Confidentiality**; **I** - **Integrity**; **A - Accessibility**].

  Elements of cyber security (People, Technology, Processes).

  Cybersecurity Lifecycle (Prevention, Detection, Response).
- The most well-known and widely used cybersecurity triad is the **CIA triad**, but the application of this basic triad of cybersecurity principles alone, without the implementation of other principles, is currently insufficient to maintain an adequate level of cybersecurity.
- For example, the literature points to the use of **Parker's hexads**[104] , the de facto CIA triad supplemented by three other elements: **P/C - Possession/Control**, **A - Authenticity** and **U - Utility**.
- Very often, the CIA triad is primarily associated with information.
  This narrowed concept is primarily due to the very definition of **information** security, which focuses on the protection of information. In the context of this protection, it is irrelevant on which medium

---

WAISOVÁ, Šárka. *Security: development and conceptual changes.* Pilsen: AlešČeněk, s.r.o., 2005. ISBN 80-86898-21-0
FRANK, Libor. *Security studies.* [Online]. [cited 2018-07-10]. Available from: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf.
[99] *Cybersecurity.* [online]. [cited 2018-07-06]. Available from: https://www.merriam-webster.com/dictionary/cybersecurity Author's translation.
[100] *Cybersecurity.* [online]. [cited 2018-07-06]. Available from: https://en.oxforddictionaries.com/definition/cybersecurity Author's translation.
[101] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 69 [online]. [cited 2018-07-10]. Available from: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[102] *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [cited 2018-07-01]. Available from: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf p. 5
[103] See, for example, HSU, D. Frank and D. MARINUCCI (eds.). *Advances in cyber security: technology, operations, and experiences*. New York: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. p 41.
KADLECOVÁ, Lucie. *Conceptual and theoretical aspects of cyber security.* [online]. [cited 2018-07-21]. Available from: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf.
[104] More details can be found, for example, in *ParkerianHexad*. [Online]. [cited 2016 Aug. 20]. Available from: https://vputhuseeri.wordpress.com/2009/08/16/149/.

(paper, electronic medium, etc.) or in which system the information is processed. Information security then refers to information throughout its life cycle.

- Information security is also defined by a number of ISO 27000 standards. The basic information security standards include:
  ISO/IEC 27001:2014 Information technology - Security techniques - Information security management systems - Requirements
  ISO/IEC 27002:2014 Information technology - Security techniques - Set of practices for information security measures
- According to the Cybercrime Convention[105] **, computer data** means *"**any expression of facts, information or concepts in a form suitable for processing by a computer system,** including a program capable of causing a computer system to perform **a** function."*
- **Information** *"is data that has been processed into a form that is useful to the recipient. So any information is data, but any stored data does not necessarily become information."*[106]
- **Information is therefore seen as something more 'qualified' than data.** Data are facts that become information when they are perceived or expressed in context and carry meaning that people can understand.[107]
- The concept of confidentiality defines the fact that only those authorised to have access to information, data or information and communication technology may have access to it
- ISO/IEC 27000 security standards specify that:
  "Information should be classified taking into account its value, legal requirements, sensitivity and criticality."
  "Procedures should be developed and implemented to label and handle information that is consistent with the classification scheme adopted by the organisation."
  "In order to prevent unauthorised access or misuse of information, rules must be established for its handling and storage."
- Examples of some classification schemes:
  1. **Classification of information according to Czech Act 412/2005 Coll., on protection of classified information and on security clearance**[108] :

- **Top secret** - unauthorised handling of information could cause extremely serious damage to state interests.
- **Secret** - unauthorised handling of the information could cause serious damage to state interests.
- **Confidential** - unauthorised handling of the information could cause ordinary damage to the interests of the state.
- **Restricted -** unauthorised use of the information could be detrimental to the interests of the state.

  2. **Classification of information used in the commercial sphere**:

- **Protected -** Unauthorised handling of the information could cause serious damage or destruction to the organisation (e.g. leakage of strategic information, source code, security schemes, passwords, etc.).

[105] Article 1(b) of the Cybercrime Convention. *Convention on Cybercrime.* [online]. [cited 2016 Aug 20]. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0.
[106] POŽÁR, Josef. *Information security.* Pilsen: AleščČeněk, 2005, p. 25
[107] ŠÁMAL, Pavel et al. *Criminal Code II. §§ 140-421. commentary.* 2nd ed. Prague: C. H. Beck, 2012, p. 2308
[108] For more details, seehttps://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/.

- **Internal -** unauthorised handling of information could cause damage to the organisation (e.g. leakage of personal data, contracts, etc.).
- **Sensitive -** unauthorised handling of information could have negative consequences for the company (e.g. unpublished information on projects, planned events, etc.).
- **Public -** unauthorised use of information should not harm anyone and should not affect the public (e.g. publicly available contacts, project presentations, etc.).[109]

3. **Traffic light protocol**

- Within the cybersecurity community, there has historically been a need to share information and data (usually relating to cyber-attacks) that is sensitive in nature. For this reason, the National Infrastructure Security Coordination Centre[110] created the **Traffic Light Protocol** (**TLP**)[111] in the early 2000s.

4. **Confidentiality assessment in accordance with Czech Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, cyber security notification requirements and data disposition** (Cyber Security Decree)[112]

- According to the Interpretive Cyber Security Dictionary[113] , **integrity is** defined as "*the property of accuracy and completeness".* **Data integrity** is further defined in the same dictionary as *'the confidence that data has not been altered'. Figuratively, it also refers to the validity, consistency and accuracy of data, such as databases or file systems. It is provided by checksums, hash functions, self-correcting codes, redundancy, logging, etc. In cryptography and information security in general, integrity refers to the validity of data."* **System integrity**, then, is *"the property that a system performs its intended function in an uninterrupted manner, without intentional or accidental, non-automated manipulation of the system."*
- **Integrity therefore means that information, data, computer systems, their settings,** etc. **cannot be tampered with by anyone other than those authorised to do so.**
- According to the Interpretive Cyber Security Dictionary[114] , **availability** is defined as "*the property of being available and usable at the request of an authorised entity."*
- Availability can therefore be defined as the guarantee of being able to access information, data or a computer system when needed. A stand-alone system that ensures integrity and allows access to the system, data or information itself is useless if it does not provide reliable access when needed.[115]
- *"The destruction of certain information is referred to in information security as the disruption of its availability."*
- The following three elements or their interaction allow cyber security to be created or established to some extent. These elements are:
    - People,

[109] Cf. further: ŠULC, Vladimír. *Cybersecurity.* Plzeň: AlešČeněk, 2018. p. 20 ff.
[110] Currently the Centre for the Protection of National Infrastructure - CPNI
[111]For more details, see e.g. Traffic Light Protocol (TLP) Definitions and Usage. [Online]. [cited 2018 Jan 13]. Available from: https://www.us-cert.gov/tlp.
[112] Hereinafter referred to as the Cybersecurity Regulation or **VoKB.**
[113] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015, p. 58 [online]. [cited 2018-07-10]. Available from: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.
[114] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015, p. 43 [online]. [cited 2018-07-10]. Available from: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.
[115]See, for example, EVANS, DONALD, PHILIP, BOND and ARDEN BEMET. *Standards for Security Categorization of Federal Information and Information Systems.* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cited 2017 Dec 10]. Available from: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.

- Technologies
- Processes.

- People interacting with cyber security can be seen as:
  the developer(s) of **that security** (i.e. typically the person(s) attempting to enforce and implement the various elements of cyber security, either for themselves or for the organisation),

  Beneficiaries of cyber security legislation (i.e. those who have chosen or are required to implement existing cyber security legislation), entities that need to be protected from cyber-attacks,

  Entities to be informed and trained on cyber security regulations and principles,
- **Risk or threat in the context of creating and maintaining cyber security**.
- In our view, it is important for people who use ICT and choose to interact in cyberspace:
  know at least **the basic principles and rules applicable to cyber security**,

  understand at least **the basic functions of the computer systems** (e.g. computer, laptop, mobile phone, smart TV, etc.) they **use** for this interaction,

  analyse the applications they use for this interaction, and if they do not feel confident in using these applications or in understanding their terms, they should stop using them,

  were educated on cyber security.
- Technology is usually a means for users to connect to the internet, social networks and other applications. It is a tool that uses various office packages to create documents, send emails, watch videos, etc. As a rule, the ordinary user perceives and interacts with the end technologies (PC, tablet, mobile phone, etc.) that he or she personally uses, while he or she is usually not interested in the other technological layers that are essential for his or her activity in cyberspace.
- In terms of technology, an integral part of an organisation's ICT should be the following, depending on the specifics of that organisation:
  - detection systems - Intrusion Detection System (**IDS**)/Intrusion Prevention System (**IPS**),
  - central management of users and roles,
  - centralised management of information classification,
  - protection against malicious code (application firewall, anti-virus, anti-spam and other solutions),
  - technology for recording the activities of individual ICT components, administrators and users (**log system)**,
  - active and offline backup systems; backups of important servers, applications and databases (**data recovery system)**,
  - network security management (VLAN, DMZ, firewall, etc.).
- Processes are the steps that need to be taken so that technology and related services can be used by people.
- In terms of the passage of time, the following processes can be tracked:
  - asset and risk management,
  - defining and categorising assets,
  - risk analysis and categorisation,
  - implementation of information and communication technologies and applications,
  - user and role management,
  - authorisation and authentication,

- maintenance (upgrades) of systems and services,
- security testing of individual computer systems and services,
- analysis of corrective action,
- implementation of corrective measures,
- cyber security audit,
- detection of anomalies or cyber-attacks,
- responding to cyber-attacks or other incidents,
- processes to ensure continuity,
- training and exercises, etc.

- In retrospect, the implementation of cyber security requires the application or modification of both the CIA triad and the cyber security sub-elements throughout their lifecycle. In particular, prevention, detection and response to attack. [116]
- The Data Breach Investigations Report[117] , which analyses security breaches leading to data compromise, for 2017 shows the following:
- the attacker was
  - **non-organisational person - 73 %.**
  - person in the organisation - 28 %.
  - **organised crime group - 50%**
- the attacker was used for the attacks:
  - **hacking - 48 per cent.**
  - **malware - 30%**
    - **49% of malware** was distributed and then installed by the attacker **via email**
  - **social engineering - 43 %**
  - physical assault - 8%[118]
- victims are organisations operating in:
  - healthcare - 24 %.
  - public sector (typically state and local government, etc.) - 14%
- the motive for the attack:
  - **enrichment - 76%**
  - acquisition of data and information (espionage) - 13%
- **68% of attacks were detected after several months or more**
- **According to a report by the National Cyber and Information Security Authority**, *"**further growth in cyber threats can be expected in 2018, especially** more next-generation phishing attacks, attacks on marketplaces, wallets and cryptocurrency exchanges, fileless variants of ransomware, use of artificial intelligence for cyber-attacks, attacks on data in Cloud solutions, attacks on IoT, industrial systems, etc. **The number of state-owned or state-sponsored entities in cyber-attacks is expected***

[116] For more details, see SVOBODA, Ivan. *Cyber security solutions.* Lecture at the CRIF Academy. (23. 9. 2014)
[117] *2018 Data Breach Investigation Report. 11th Edition. [*Online]. [cited 2018-07-28]. Available from: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.
[118] Single attacks usually involve a combination of techniques and tools.

to increase and massive leaks of personal data, passwords and access data are expected to continue. *Therefore, it is essential to build cyber security for ICT systems critical to the functioning of the state and its critical infrastructure."*[119]

- "Cybersecurity also helps to identify, assess and counter cyber threats, mitigate cyber risks and eliminate the effects of cyber-attacks, information crimes, cyber terrorism and cyber espionage in strengthening the confidentiality, integrity and availability of data, systems and other elements of the ICT infrastructure."
- **The main objective of cyber security is to protect the environment for the realisation of human rights to information.**" [120]
- The Cybersecurity Interpretive Dictionary defines risk as: *"(1) Danger, the possibility of harm, loss, failure. (2) The impact of uncertainty on the achievement of objectives. (3) The possibility that a threat will exploit a vulnerability in a resource or group of assets and cause harm to an organisation."*[121]
- **Risk can** also be defined as the **potential for a threat to materialise and exploit a vulnerability in an asset**. According to Article 4(9) of the NIS, **risk is defined** as *'**any reasonably identifiable circumstance or event that could adversely affect the security of networks and information systems.*** ' In cyberspace, risks are exposed to users, the computer systems and applications that use them, and other ICT elements.
- The term **risk expresses the probability of an undesired event**. The degree of probability with which this event will occur is expressed by means of a risk analysis. Minimum standard values for methods of identification, analysis, assessment and investigation of risk are specified in EN 31010.
- Valášek et al.[122] report that risk assessment is usually based on three basic questions:
  What bad (undesirable) things can happen? What can go wrong?

  What is the possibility/likelihood of this happening?

  How serious (intensity, magnitude, etc.) can the effects (impacts, consequences) be?
- A risk materiality level is calculated for each risk, which can be expressed as follows:
  Risk **significance** = **Impact of risk** * **Probability of risk** occurrence

- **An asset is anything of value to a person, organisation or country.**
- An asset can be a **tangible thing** (building, computer system, network, energy, goods, etc.) **or an intangible thing** (information, knowledge, data, programmes, etc.) from a civil law perspective.
- However, an asset can also be a **property** (e.g. availability and functionality of the system and data, etc.) or **reputation,** etc. **People** (users, administrators, etc.) and their knowledge and experience are also an asset from a cyber security perspective.
- In accordance with Section 2(f) and (g) of the VoKB, **assets are** divided into **ancillary** and **core assets.**

---

[119] *2017 State of Cybersecurity Report* [online]. [cited 2018 Jun 29]. Available from: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

[120] *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [cited 2018-07-01]. Available from: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[121] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015. p. 99. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[122] VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Crisis management in non-military emergency situations*. Prague: Ministry of Interior Affairs - General Directorate of the Fire and Rescue Corps Republic of the Czech Republic, 2008 [online]. [cited 1 July 2018]. Available from: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx.
ISBN 978-80-86640-93-8 pp. 73

- **Support assets** are technical resources, employees and contractors involved in the operation, development, management or security of an ICT system.
- **The primary asset** is the information or service processed or provided by the ICT system.
- Vulnerability means a weakness in an asset, software or security that is exploited by one or more threats
- Vulnerability, like hazard, can be caused by a variety of factors, consisting of human action, technical failure or possibly force majeure.
- In the field of cyber security, vulnerabilities are divided into:
- **known** (published) **security holes**
    - **patched** (**fixed**) - a typical case is software vulnerabilities for which the manufacturer has already issued an update
    - **unpatched** - the affected entity (manufacturer, administrator, etc.) knows about the vulnerability, but has not taken care to patch it
- **unknown vulnerabilities**
    - hidden
    - undiscovered
- The Cybersecurity Decree in Annex 3 lists some vulnerabilities by way of example.
  According to this **decree, the vulnerabilities are:**
    - inadequate maintenance of the information and communication system,
    - the obsolescence of the ICT system,
    - insufficient external circuit protection,
    - lack of security awareness among users and administrators,
    - incorrect access rights settings,
    - inadequate procedures for identifying and detecting adverse security events, cyber security incidents and cyber security incidents,
    - inadequate monitoring of users and administrators and failure to detect inappropriate or problematic behaviour,
    - insufficient definition of security rules, inaccurate or ambiguous definition of the rights and responsibilities of users, administrators and security roles,
    - insufficient protection of assets,
    - inadequate security architecture,
    - insufficient independent scrutiny,
    - failure to detect employee misconduct in a timely manner.
- A threat can most simply be defined as something capable of disrupting the normal or orderly state of affairs and interfering with the rights of others. It is a negative action that may or may not be realised. For a proper definition, it is sufficient that the possibility of a negative state of affairs is imminent and real.
- According to the diction of the Ministry of the Interior of the Czech Republic, a threat is considered to be "*any phenomenon that has the potential ability to harm the interests and values protected by the state. The degree of threat is determined by the magnitude of the potential harm and the*

temporal distance (usually expressed in terms of probability or risk) of the possible application of this threat."[123]

- The actual term threat **is** defined as "the *potential cause of an unintended event that could cause damage to a system or organisation."* [124]
- Directly related to this basic concept is the term **information** security risk[125] , which is defined as "*the potential cause of an adverse event that could result in damage to a system and its assets, such as destruction, unwanted access (compromise), modification of data or unavailability of services*." [126]
- In addition to the above two terms, the authors define the terms **active threat, passive threat and advanced and persistent threat** in the glossary**.** [127]
- The Oxford Dictionary states that a **cyber threat is the possibility of a malicious attempt to damage or disrupt a computer network or system.**[128] A system in this context is a computer system.
- A cyber **threat can** also be defined as an action aimed at altering[129] information, applications or the system itself.
- Jirovský defines four groups of basic threats and characterises their relationships:[130]
    - **Information leakage** is when protected information is disclosed to an unauthorised party.
    - **An integrity breach** is the corruption, alteration or deletion of data.
    - **Service suppression** means deliberately preventing access to information, an application or a system.[131]
    - **Illegal use** is the use of information by an unauthorised party or in an unauthorised manner.[132]
- There are many classifications of cyber threats, the most common being:

1. Sources of danger

a) **Man-made hazards.** If the hazard is man-made, the focus should also be on the form of culpability that led to the initiation of the hazard. From this perspective, hazards can be distinguished :

- **caused deliberately**

Deliberately caused cyber threats include, for example:

- deliberate deletion of data, system configurations, etc,
- physical damage to a computer system or other ICT component,
- theft of data and information,

[123] *Jeopardy.* [online]. [cited 2018-07-28]. Available from: http://www.mvcr.cz/clanek/hrozba.aspx.
[124] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 52. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.
[125]In this case, we may notice a problem with the translation of some terms from English and vice versa. If we would like to consistently translate the term Information security threat, the correct Czech equivalent is e.g. threat to information security; threat to information security, etc.
[126] Ibid p. 25
[127] Ibid, pp. 16, 81 and 87
[128] *Cyberthreat.* [online]. [cited 2018-07-06]. Available from: https://en.oxforddictionaries.com/definition/cyberthreat.
[129] Alteration also means stealing information, destroying it or thwarting its use.
[130] Cf. JIROVSKÝ, Václav. *Cybercrime not only about hacking, cracking, viruses and Trojans without secrets.* Prague: Grada Publishing, a. s., 2007. p. 21 ff.
[131] These include attacks such as **DoS - Denial of Service**, DDoS- **Distributed Denial of Service**, etc. More details can be found in the book KOLOUCH, Jan. *Cybercrime.* Prague: CZ.NIC, 2016, p. 295 ff.
[132] For example, a fee-based system is compromised and its services are used without payment for services.

- cyber-attacks (malware, DoS, DDoS, phishing, unauthorised eavesdropping, etc.).[133]

- **caused by negligence.**

Cyber risks caused by negligence / carelessness include:

- accidentally deleted data,
- physical damage to a computer system or other data communication item
- damage to data, systems or other elements due to lack of knowledge of internal (legal or technical) acts,
- other user errors.

b) **Technical errors** (e.g. software or hardware error).

c) **Vis maior (higher power)**.

Cyber threats caused by force majeure include, for example:

- unexpected power failure (unless it is a hazard caused by human negligence),
- natural events (lightning, storms, etc.) or disasters (floods, earthquakes, etc.),
- fire (unless it is a man-made hazard).

2. Sources of action

a) **Internal threats** (the source of the threat is inside the organisation)

b) **external threats** (the source of the threat is outside the organisation)[134]

3. Threat objectives

a) CIA triad attack.

- **Confidentiality** - e.g. theft of data, access data and keys, computer equipment, etc.
- **Integrity** - errors in databases, permission settings, etc.
- **Availability** - e.g. DoS and DDoS attacks; physical attacks on servers and structured cabling; power outages, etc.

b) Attack on the cyber security element.

- **People -** social engineering attacks (in the real world, but also in cyberspace), phishing, malware, theft, etc.
- **Technology -** all the hazards listed in Section 1 of this classification**.** Typically, hazards can act on:
  - hardware (endpoint computer systems, servers, network controllers, IoT, etc.).
  - databases,
  - networks and network infrastructure,
  - software (operating system or other applications),
  - information and data stored in computer systems.

[133] On individual cyber-attacks see, for example, KOLOUCH, Jan. *Cybercrime.* Prague: CZ.NIC, 2016, pp. 181 ff.
[134] More details can be found, for example, in POŽÁR, Josef. *Selected threats to information security in organisations.* [online]. [cited 6 July 2018]. Available from: https://www.cybersecurity.cz/data/pozar2.pdf.

- **Processes -** unauthorised testing of security or functionality of processes set up in the organisation, etc.

4. **Motivation**

If the threat is caused by a person's intentional action, the motivation of the threat must be addressed. By analysing the motivation for such actions, corrective actions can be developed as part of the threat response process to prevent this motivation from being stimulated in the future.
Depending on the motivation, one can observe:

- threats to financial benefits,
- threats in order to gain a competitive advantage,
- threats in order to prove their capabilities,
- threats in retaliation,
- dangers of non-compliance.[135]

5. **Type of hazard**

- social engineering,
- botnet,
- malware,
- ransomware,
- spam/fraud,
- fraudulent offers,
- phishing, pharming, spear phishing, vishing, smishing,
- hacking,
- sniffing,
- DoS, DDoS, DRDoS attacks,
- dissemination of harmful content,
- identity theft,
- APT (Advanced PersistentThreat),
- cyber-terrorism,
- cybernetic extortion.

The Cybersecurity Decree in Annex 3 lists some of the threats by way of example. **According to** this **decree, a threat is:**

- breach of security policy, unauthorised activities, abuse of privileges by users and administrators,
- failure or breakdown of technical equipment and/or software,
- misuse of identity,
- use of the software in breach of the licence conditions,
- malicious code (e.g. viruses, spyware, Trojan horses),
- physical security breaches,
- interruption of electronic communications services or electricity supply,
- misuse or unauthorised modification of data,

[135] What to protect against? - Security threats, events, incidents. [Online]. [cited 2018-07-06]. Available from: https://www.kybez.cz/bezpecnost/pred-cim-chranit

- loss, theft or damage to an asset,
- the supplier's failure to fulfil a contractual obligation,
- misconduct by employees,
- misuse of internal resources, sabotage,
- prolonged interruption of electronic communication services, electricity supply or other essential services,
- lack of staff with the necessary knowledge,
- targeted cyber-attack using social engineering, use of espionage techniques,
- misuse of interchangeable technical storage media,
- intrusion into electronic communications (interception, modification).

- Prosise and Mandiva characterise a **'computer security incident'** (which can be understood as a computer attack or computer crime) as an illegal, unauthorised, unacceptable action concerning a computer system or network. This action may be aimed at, for example, the theft of personal data, spamming or other harassment, embezzlement, distribution or possession of child pornography, etc.[136]
- Jirásek et al. define a security ***incident*** as *"**an event that can cause or lead to a breach of** information systems and technologies and the rules defined to protect them (security policy).*"[137]
- A definition of a security event can also be found in ISO/IEC 27001 clause 3.5, which states that such an event is: *"an **identifiable state of a** system, service or network **indicating a possible breach of security policy or failure of security measures**. It may also be any other situation that has not previously occurred that may be relevant to information security."*
- A similar definition can be found in the NIST document, 800-61 Computer Security Incident Handling Guide, which states that a security incident is "an *event with negative consequences, such as system failure, packet flooding, unauthorised use of system privileges, unauthorised access to sensitive data, or execution of malicious code that destroys data.*" [138]
- **A cyber security event** is also defined in Article 7(1) of the Cyber Security Act as *"**an event that may cause a breach of the security of information in information systems or a breach of the security of services or the security and integrity of electronic communications networks.**"*
- De facto **it is an event with no real negative consequences** for the communication or IT system, in fact it is just a threat, but it must be real.

- An appropriate definition of **an information security incident is provided in the** ISO/IEC 27001 standard. In Article 3.6 of this standard, an information security incident is defined as *"one or more unintended or unexpected security events that have a high probability of compromising an organisation's operations and jeopardising information security."*

[136] PROSISE, Chris and Kevin MANDIVA. *Incident response & computer forensics, 2nd ed.* Emeryville: McGraw-Hill, 2003, p. 13
Cf. further CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, p. 9 inast.
[137] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015. p. 28. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.
[138] *Computer security incident handling guide* **[online]. [cited 2018 Aug 13], p. 6. Available from:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

- A very similar definition of a **computer security incident** can also be found in the NIST document, 800-61 Computer Security Incident Handling Guide, which states that it is *"a violation or imminent threat of a violation of a security policy, acceptable use policy (system, service) or standard security practices."*[139]
- **A cyber security incident** is also defined in section 7(2) of the Cyber Security Act as *"a **breach of the security of information in information systems or a breach of the security of services or the security and integrity of electronic communications networks as a result of a cyber incident.*** "
- It is clear from the diction of the law that an incident can be caused by both intentional and negligent human action, but also by force majeure. What matters is that there is a **breach of the security of information or services and the ICT systems associated with them**
- Jirásek et al. define a cyber-attack as "An attack *on IT infrastructure to cause damage and obtain sensitive or strategically important information. It is most often used in the context of politically or militarily motivated attacks."*[140]
- **Cyber-attack**[141] can be defined as **any deliberate action by an attacker in cyberspace that is directed against the interests of another person.**
- When defining the content of the term **cybercrime, it is important to note** that as the possibility of using ICT means increases, so does the possibility of using (abusing) them to commit crimes. Therefore, in principle, there is no universal, universally accepted definition that fully captures the scope and depth of this concept.
- In the most general terms, cybercrime can be defined **as an activity directed against a computer system, computer network, data or users, or as an activity in which a computer system is used as a tool to commit a crime. The fact that** a computer network or cyberspace is the environment in which this activity takes place is essential for the definition of cybercrime to apply

- **CERT** (Computer Emergency Response Team) **and CSIRT** (Computer Security Incident Response Team). Although each of these abbreviations has a slightly different meaning and, more importantly, a slightly different historical genesis, in fact today both abbreviations can be understood as the same type of team - **a team that is responsible for dealing with security incidents and (cyber) threats in its clearly defined area of operation, from the perspective of users or other teams, a place to which they can turn with a detected security incident, requesting cooperation, information sharing, assistance, etc.**
- CERT/CSIRT teams are set up at the level of individual organisations, both organisations that mediate the operation of the Internet (ISPs) and organisations that use the Internet for their core business (e.g. IT companies, content providers, banks).
- **The primary responsibility of any CSIRT team is to respond to a threat ('response') and to cooperate in incident response.** A CSIRT team usually deals with a problem that occurs in its area of responsibility (e.g. its own network infrastructure), i.e. where it has a real opportunity to intervene.

- This is nothing revolutionary and is virtually non-existent; every major organisation, ISP or service provider has a security team. **The main difference between a regular security team and a CERT/CSIRT is the commitment to a global security infrastructure**, the **sharing of information within** that infrastructure **and the adherence to established formal procedures**.

---

[139] *Computer security incident handling guide* **[online]. [cited 2018-02-17]**, p. 6**. Available from:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[140] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated ed. Prague: AFCEA, 2015. p. 71. Available from: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[141] It is necessary to distinguish the concept of a security incident from that of a cyber-attack, which is a breach of IS/IT security and the rules defined to protect it (security policy).

- In each country, overarching **national** and **governmental summit teams have** an important and **specific role to play**, to which a separate subsection will be devoted.
- **A basic requirement of** the community **is for the CERT/CSIRT to publicly announce its contact details and operating rules:**
    - who is its operator,
    - who are its members,
    - How and when the team can be contacted,
    - what **services** it offers.

  The scope (AS number[142] , network, domains, services) in which the team is authorised to act and how, i.e. the definition of its authority and responsibility. Based on the scope, the team is then contacted (e.g. by those attacked) and resolves the relevant issues (incidents).
- The term **security incident resolution** can vary in specificity depending on the configuration of the team and its internal policies - it can be simple elimination of the attack (disabling the source of the problem, e.g. by disconnecting the compromised computer system from the network), tracking down the attacker, quickly restoring operation of the attacked service/network, etc.
- In order for a team to officially call itself a CERT/CSIRT, it must first and foremost offer the service of resolving or coordinating the resolution of security incidents within its defined scope, thus realising the idea of 'response' as used in the CERT/CSIRT acronyms, i.e. it must be able to *respond to a* security incident.
- From an 'external' perspective, a team becomes a CERT/CSIRT when it is accepted as such by other existing CERT/CSIRT teams in the world. The path to becoming a CERT/CSIRT team is not complicated, at the start of the journey it is sufficient to declare in clear terms the following:

1. **Basic contact information** - name of the team, name of the organisation running the team, -email address(es) of the team where security incidents can be reported or the team can be contacted, telephone number(s) of the team, address of the office, names of team members, hours when the team can be contacted, etc.
2. **Scope of the team** - defines what the team is responsible for and what its role is. This of course depends on what kind of team it is. It is possible to set up teams of roughly the following types:
    - ***Internal*** - operates and is responsible for a specific network (e.g. a specific range of IP addresses, domains), and is usually configured by the network operator,
    - ***Coordination-*** a team whose main task is to coordinate the resolution of security incidents, not to solve them,
    - ***vendor-*** the team dealing with security incidents that involve a specific product (SW),
    - ***national, governmental*** - special cases based on the principles of the first two teams mentioned (internal and coordination), their scope and role depend on the founder and often on the legislation of the specific country.
3. **Services offered - At a minimum, the** CERT/CSIRT must run a security incident response service.

- **The organisational basis** is the aforementioned 'readiness' to solve the problem, i.e. defining the basic rules of the team, so that each team member knows his or her role, duties and responsibilities, security incident handling policy, rules for communication, information sharing and exchange, cooperation, etc. The basis in this area is generally well-managed so-called ***incident management.***

[142] **AS** - Autonomous System. An autonomous system is a collection of IP networks and routers under a common technical management that represents a common routing policy towards the Internet.

- CERTs/CSIRTs are set up on a voluntary basis and have an interest in communicating effectively with each other, sharing relevant information and knowledge, and cooperating. This is why the teams come together in international organisations. Currently, the best known and most active organisations dealing with this issue and creating a suitable environment to achieve the above-mentioned objectives are the international organisation **GÉANT**[143] and **FIRST** (Forum for Incident Response and Security Teams)[144] .

- GÉANT, a European organisation, has several activities in which global CERTs/CSIRTs can participate if they are interested:

  TF-CSIRT (Task Force for CSIRT) is a working group that enables teams to collaborate through regular two-day meetings held 3 times a year (the host of this meeting is usually the CERT/CSIRT team). More information can be found at: https://tf-csirt.org/.

  CSIRT training - is used to train new members of CSIRT/CERT teams or those who are just about to set up a CERT/CSIRT team. It is usually held twice a year and the trainers are experienced members of reputable CERT/CSIRT teams and other top security experts. More information can be found at: https://tf-csirt.org/transits/.

  Trusted Introducer[145] - an office whose main role is to build trust between CERT/CSIRT teams and help establish new ones. More information can be found at: https://www.trusted-introducer.org/.

- Among the existing teams, there must also be at least two teams (called sponsors) that will support the new team, and none of the existing teams can object to the new team's admission. If all goes well, the new team's information is kept on a list maintained by the TI office (and some of it is made public), the team gains ***listed*** team status, and the community welcomes the new member.

- In the case of FIRST, the entry procedure is very similar, but ends with ***membership,*** not status.

- With Trusted Introducer, it is possible to achieve other, more important statuses, namely ***accredited*** and ***certified***. The differences are as follows:

  A team with a listed status ***provided*** basic information about itself, declared its willingness to behave as a CSIRT team and was accepted by the community.

  A team with ***accredited*** status declares the level of practice desired by the community and commits to the common principles of TI.

  The certified team then demonstrated their "maturity level" through a certification process.

- Being an ***accredited*** or ***certified team*** requires an ongoing effort to maintain team status. Part of this effort is the obligation to keep the team's information updated on the TI roster. Failure to do so over an extended period of time can result in loss of team status and, in the worst-case scenario, expulsion from the community.

- Another organisation active in the area of security is **ENISA** (European Network and Information Security Agency, http://www.enisa.europa.eu/). It works closely with EU Member States and the private sector and encompasses a range of activities, including pan-European cybersecurity exercises, the development of national cybersecurity strategies, cooperation and capacity building between CERTs/CSIRTs, dealing with personal data protection issues and working on the development and implementation of legislation on network information security (NIS) issues.

[143] The association was formed from the merger of TERENA (Trans-EuropeanResearch and Education Networking Association) and DANTE.

[144] More information about FIRST can be found at: https://www.first.org

[145] Longer also **TI**.

- CERT/CSIRT teams have no official hierarchy that makes one team superior to another. **All teams are equal in** terms of functioning, communication, cooperation and information sharing and are not limited in these areas.
- In the world of CERT/CSIRT teams, the **willingness to share important information about** incidents and threats is key. To do this, it is essential that teams trust each other, and users trust their teams.
- **A national CERT/CSIRT** acts as a **last *resort* - a last instance to which assistance and intervention can be** requested. Its purpose (within the country or region in which it operates) is to act as an intermediary between the attacked party and the initiator of the problem and to facilitate a successful resolution.
- Country teams do not (usually) control the physical infrastructure, so they do not have (unlike internal/institutional teams) the possibility to intervene directly. Their role is to mediate contacts or coordinate (hence the **coordination** team type) the activities of different actors when the problem is larger and requires the cooperation of several actors.
- A national CERT/CSIRT usually has **education and cooperation as** part of its responsibilities**.** This includes both educating the public and working within the Internet infrastructure. The aim is to support the establishment of other CERTs/CSIRTs in the country, to launch them internationally and to support the implementation of standard practices and procedures. All of this greatly enhances the transparency of the environment and gives those attacked a chance for effective redress.
- **Government CERTs/CSIRTs** typically focus on state and local authorities and on dealing with incidents that threaten the security of the state and its services. A government CERT/CSIRT may take the form of an internal team with the ability to intervene directly in the event of a problem. Its existence is usually supported by legislation.
- **The process of reporting and resolving security incidents** (or really 'who do I contact to report or resolve a security incident') **can be considered from two perspectives.** From the viewpoint of the **technicians** (network and service administrators, members of the security team) and from the viewpoint of the **users**
- For **technicians** (network and service administrators, members of security teams), the answer to the question "who should I actually contact to take action" is quite obvious, but this comes from experience and, above all, a very good knowledge of the internet environment and its basic principles, as well as knowing where to find contact information for the various existing networks, services, domains, etc.
- Regional Internet Registries (**RIRs**) store and make available information about who has been allocated a block of IP addresses. The world is divided into regions and each RIR (currently RIPE, ARIN, APNIC, LACNIC, AFRINIC) allocates IP addresses for its region. The Europe, Middle East and parts of Asia region is managed by the RIPE NCC (https://www.ripe.net/).
- The process of reporting and resolving security incidents (technically incident ***handling***) is not a strict process, on the contrary, and much depends on the experience and sometimes even the creativity of the person who performs the process. The exchange of information between teams is usually fast and efficient, although even this often does not guarantee a quick resolution, as the overall infrastructure is still quite 'sparse' for this, and unfortunately it has to be said that the level of teams varies.
- **The optimal state of the infrastructure would be if every IP address was within the reach of an official CSIRT.** In this situation, however, the infrastructure of CERT/CSIRT teams is a long way off.

- **From the perspective of an ordinary user,** the situation is very unclear and essentially confusing. So, what should a user do in the event of a security incident and who should they contact? It is difficult to require the user to know about CERTs/CSIRTs, find the right one, study its security incident reporting policy and take action.
- In the first instance, users should **contact their network or service administrator** (if they have one) or they should liaise with their connection provider, i.e. the ISP's **helpdesk or its user support**. There should be a clearly described point of contact on the ISP's side to which users can and should turn if they are targeted, discover a security incident or feel that something is wrong.
- **There is a very close cooperation** and exchange of information and relevant data **between the country team and the government team,** thus passing on a reported problem to be solved by one team to the other or working directly on a solution.
- **In general, however, it would be desirable for network and service administrators and security team members to master and apply the principles of the incident handling process and maximise communication directly** (not through higher level teams). This makes the incident handling process fast and efficient; additional intermediate steps can introduce delays and, unfortunately, disruption. But as mentioned, this depends on the severity of the situation and the problem being resolved.

- **CERTs/CSIRTs and their infrastructure are generally not comprehensive and do not represent security 'in a nutshell'**.
- On 6 July 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security for network and information systems in the Union (NIS Directive) was adopted by the European Parliament.
- On the basis of the Cyber **Security** Act in **the Czech Republic, two** CERT/CSIRT **teams are compulsorily established: a national one and a governmental one**. Each of these teams has strictly defined legal rights and responsibilities (§ 17 et seq. of the CERT Act).
- The NIS Directive provides legal measures to increase the overall level of cyber security in the EU by ensuring:
    - Member States' preparedness by requiring them to be adequately equipped. For example, in a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
    - cooperation between all Member States through the creation of a cooperation group to promote and facilitate strategic cooperation and the exchange of information between Member States.
    - safety culture in sectors that are key to our economy and society and rely heavily on ICT, such as energy, transport, water, banking, financial markets infrastructure, healthcare, and digital infrastructure.
- Member States have taken different approaches to implementing the NIS.

3. During classes

<u>Some ideas for activities:</u>

WORKSHOPS

1. Analyse the need for a safety team within the organisation.
2. Definition of individual assets and SWOT analysis in relation to them.
3. Creating and integrating the safety team into the organisation - adopting rules and policies.
4. Simulation of a cyber incident or event directed against an organisation.
5. Incident management.
6. Analysis of the measures taken.
7. Sharing information with others.

REVIEW QUESTIONS

1.

- What is the CIA triad?
- How can cyber security be defined?
- What are the elements of cyber security?
- What is meant by assets?
- How can a vulnerability be defined?

2.

- What is a CSIRT/CERT team?
- How is a CSIRT/CERT team formed and established?
- What is the focus of the national CSIRT team?
- What is the focus of the government's CSIRT team?
- What are the basic community requirements for a CSIRT/CERT team?

3.

- Is there a hierarchy between CSIRT/CERT teams?
- How is the scope of the CSIRT/CERT team defined?
- Who is the government's CSIRT/CERT team?
- Who is the national CSIRT/CERT team?
- What are the roles and responsibilities of other CSIRT/CERT teams?
- How are the CSIRT/CERT teams constituted in your country?

Working in pairs/groups

- **Pairs - mini-project**
  In pairs, students choose one of the topics discussed. They write down their conclusions and present them to the others. After the presentation, the other students prepare additional questions for the presenting group.

- **Map of thoughts**
  Students in pairs choose one of the topics covered and create a mind map, which they then describe to the other students in a short presentation.

- **Keywords**
  Students in pairs individually select key words from the glossary.

They write the definitions of these words on strips of paper. They turn the strips over with the blank side up. A student chooses a strip, reads the definition and the other student looks for a matching keyword.
or
Students write some key words from the glossary on a piece of paper. They turn the cards over with the blank side up. One student takes the first card and says what the word means. The second student guesses the key word.

- 10 keywords

  Students choose 10 keywords related to their chosen topic. These 10 keywords are given to other pairs. The pairs write a text that must contain all the keywords. One sentence can only contain one keyword. So the text consists of at least 10 sentences.

- Panel discussion

  Students choose 3 speakers. Each speaker chooses one topic to discuss. The other students ask questions about the topics. Each speaker can use an answer type -TRUE X FALSE. The student gets a point for each true answer, e.g. Does GDPR stand for General Data Protection Regulation? - TRUE X FALSE.

4. Internet resources

See bibliography below.

5. Additional questions/tests

SELECT THE CORRECT ANSWER:
(The correct answer has been highlighted)

1. _____ is a set of measures taken to protect a computer system from unauthorised access or attack.

   a) Cybersafe
   (b) Security in cyberspace
   c) Cybersecurity
   d) Cybersecure

2. Elements of cyber security include: _____

   (a) people, technology, processes

   (b) reality, software, hardware

   (c) suppliers, virtuality, procedures

   (d) users, technology, issues

3. _____ refers to a situation where only those who are authorised to do so have access to information, data or ICT.

   (a) Credibility
   b) Reality
   (c) Authenticity
   (d) Confidentiality

4. A degree of risk materiality is calculated for each risk, which can be expressed as follows:
   a) Risk significance = Impact of risk * Probability of risk occurrence
   (b) Significance of risk = Range of risk * Probability of risk.
   c) Significance of risk = Impact of risk * Possibility of risk occurrence
   d) Significance of risk = Risk issues * Probability of risk occurrence

5. _____ are technical resources, employees and suppliers involved in the operation, development, administration or security of the ICT system.

   (a) Underlying assets
   (b) Ordinary assets
   (c) receipts
   (d) Ancillary assets

6. _____ refers to a weakness in a resource, software, security that is exploited by one or more threats.

a) Fragility
(b) Vulnerability
c) Weakness
(d) Doubtfulness

7. _____ is the possibility of a malicious attempt to damage or disrupt a network or computer system.

a) Cyber threat
(b) Cyberculture
c) Cyber power
d) Cybercrime

8. **What does CSIRT** stand for?

(a) Computer Emergency Response Team
(b) Team Response to Computer Security Incidents
(c) Computer Emergency Response Team
(d) Computer Security Incident Response Team

9. CERT/CSIRT teams have no official hierarchy that makes one team superior to another. All teams are _____ in terms of operation, communication, collaboration, and information sharing and are not limited in these areas.

(a) different
(b) stable
(c) equal
(d) unspecified

10. Member States have adopted _____ approaches to NIS implementation.

(a) the same
(b) identical
(c) joint
(d) miscellaneous

11. What does CIS stand for?

a) Care, influence, accessibility
(b) Confidentiality, integrity, availability
c) Cooperation, Integrity, Accessibility
d) Impact, credibility, accessibility

12. The difference between a normal security team and a CERT/CSIRT is mainly the involvement in the infrastructure _____ , the exchange of information within this infrastructure and the adherence to established formal procedures.

(a) national security

(b) global unrest

(c) the global threat

(d) global security

13. What does ENISA stand for?

(a) the European Network and Information Security Agency
(b) the European Netsurfers and Information Security Agency
(c) the European Agency for Negotiations and Information Security
(d) the European Agency for National Security and Information

14. _____ - a team dedicated to resolving security incidents that affect a specific product.

a) Internal
b) Government
(c) Vendor
(d) Coordination

Bibliography

1. *2018 Data Breach Investigation Report. 11th Edition. [*Online]. [cited 2018-07-28]. Available from: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.
2. *Risk analysis [*online]. [cited 2018-07-01]. Available from: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/.
3. ANDRESS, Jason. *Fundamentals of information security*. 2nd Edition. Syngress. 9780128007440
4. CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, pp. 9 ff.
5. *CIA methodologies.* [online]. [cited 2018-07-10]. Available from: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png.
6. *Computer security incident handling guide* **[online]. [cited 2018 Aug 13]**, p. 6**. Available from:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf**.**
7. *Cybersecurity.* [online]. [cited 2018-07-06]. Available from: https://en.oxforddictionaries.com/definition/cybersecurity Author's translation.
8. *Cybersecurity.* [online]. [cited 2018-07-06]. Available from: https://www.merriam-webster.com/dictionary/cybersecurity Author's translation.
9. *Cyberthreat.* [online]. [cited 2018-07-06]. Available from: https://en.oxforddictionaries.com/definition/cyberthreat.
10. *Defining cyber security - gaps and overlaps in standardisation*. [online]. [cited 2017 Dec 10]. Available from: https://www.enisa.europa.eu/publications/definition-of-cybersecurity p. 30
11. *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cited 2021-03-16]. ISBN 978-92-9204-292-9. Available from: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, p. 6.
12. EVANS, DONALD, PHILIP, BOND and ARDEN BEMET. *Standards for categorising the security of federal information and information systems.* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cited 2017 Dec 10]. Available from: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.
13. FRANK, Libor. *Security studies.* [Online]. [cited 2018-07-10]. Available from: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf.
14. FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. [cited 2018-07-01]. Available from: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
15. HENDERSON, Anthony. *The CIA Triad: Confidentiality, Integrity, Availability.* [Online]. [cited 2018]. Available from: http://panmore.com/the-cia-triad-confidentiality-integrity-availability.
16. *Jeopardy.* [online]. [cited 2018-07-28]. Available from: http://www.mvcr.cz/clanek/hrozba.aspx.
17. HSU, D. Frank and D. MARINUCCI (eds.). *Advances in cyber security: technology, operations, and experiences*. New York: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. p 41.
18. JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Interpretive dictionary of cyber security.* [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 23 [online]. [cited 2018-07-10]. Available from: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
19. JIROVSKÝ, Václav. *Cybercrime not only about hacking, cracking, viruses and trojans without secrets.* Prague: Grada Publishing, a. s., 2007. p. 21 ff.

20. KADLECOVÁ, Lucie. *Conceptual and theoretical aspects of cyber security.* [online]. [cited 2018-07-21]. Available from: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf.
21. KOLOUCH, Jan. *Cybercrime.* Prague: CZ.NIC, 2016.
22. *Cyber security: what to do about it?* [online]. [cited 2018 Jun 29]. Available from: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html
23. *Macron's election staff was attacked by hackers, says Japanese anti-virus firm.* [online]. [cited 2017 Jun 29]. Available:http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san
24. MAREŠ, Miroslav. *Safety.* [Online]. [cited 2018-07-10]. Available from: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511.
25. MATUROVÁ, Jana and Miroslav VALTA. *Risk prevention - inspections of the condition of technical equipment.* [Online]. [cited 1 July 2018]. Available from: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni.
26. *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [cited 2018-07-01]. Available from: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf p. 5
27. *Parkerian Hexad*. [Online]. [cited 2016 Aug. 20]. Available from: https://vputhuseeri.wordpress.com/2009/08/16/149/.
28. *POŽÁR, Josef. Information security*. Pilsen: Aleš Čeněk, 2005, p. 37.
29. POŽÁR, Jozef. *Selected threats to the information security of organisations.* [Online]. [cited 2018 July 6]. Available from: https://www.cybersecurity.cz/data/pozar2.pdf.
30. PROSISE, Chris and Kevin MANDIVA. *Incident response & computer forensics, 2nd ed.* Emeryville: McGraw-Hill, 2003, p. 13
31. What to protect against? - Security threats, events, incidents. *[Online]. [cited 2018-07-06]. Available from: https://www.kybez.cz/bezpecnost/pred-cim-chranit*
32. *The coming of the hackers: the story of Stuxnet.* [Online]. [cited 2018-07-01]. Available from: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/.
33. RAK, Roman. Homo sapiens and security. ICT Forum/PERSONALIS 2006 [presented 27 September 2006]. Prague (conference presentation).
34. SCHNEIER, Bruce. [Online]. [cited 2018-07-18]. Available from: https://www.azquotes.com/quote/570039.
35. SCHNEIER, Bruce. [Online]. [cited 2018-07-18]. Available from: https://www.azquotes.com/quote/570035.
36. SCHNEIER, Bruce. [Online]. [cited 2018-07-18]. Available from: https://www.azquotes.com/quote/570047.
37. SCHNEIER, Bruce. [Online]. [cited 2018-07-18]. Available from: https://www.azquotes.com/quote/570040.
38. *NIS guidelines.* [online]. [cited 1 July 2018]. Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN.
39. SVOBODA, Ivan. *Cyber security solutions.* Lecture at the CRIF Academy. (23. 9. 2014)
40. ŠÁMAL, Pavel et al. *Criminal Code II. §§ 140-421. commentary.* 2nd ed. Prague: C. H. Beck, 2012, p. 2308
41. ŠULC, Vladimír. *Cyber security.* Pilsen: Aleš Čeněk, 2018. p. 20 ff.

42. *Intelligence: the campaign to influence the US presidential election was ordered by Putin.* [online]. [cited 2017 Jun 29]. Available from: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin
43. *The full range of CGI Cyber Security services.* [online]. [cited 2018-07-10]. Available from: https://mss.cgi.com/service-portfolio
44. *Traffic Light Protocol (TLP) Definitions and Applications.* [online]. [cited 2018 Jan 13]. Available from: https://www.us-cert.gov/tlp.
45. VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Crisis management in non-military emergency situations*. Prague: Ministry of the Interior - General Directorate of the Fire and Rescue Corps of the Czech Republic, 2008 [online]. [cited 1 July 2018]. Available from: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx.
46. WAISOVÁ, Šárka. *Security: development and conceptual changes.* Pilsen: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0
47. *WannaCry should never have spread in the first place. All you had to do was use the Windows Update service.* [online]. [cited 2017 Jun 27]. Available from: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx
48. WIENER, Norbert. *Cybernetics: or control and communication in living organisms and machines.* Prague: State Publishing House of Technical Literature, 1960. 148 p.
49. *Basic concepts.* [online]. [cited 2018-07-10]. Available from: https://www.kybez.cz/bezpecnost/pojmoslovi.
50. ZEMAN, Petr et al. *Czech security terminology: interpretation of basic concepts* [online]. [cited 2018-07-10]. Available from: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

Module 5

Digital forensics fundamentals

1. Introduction

Module five is a largely workshop-based, 'physical' module that should be done in the classroom. Students will be presented with a variety of situations where an intrusion or other cyber threat has occurred and will need to get to the bottom of it.

1.1 Course summary

The Digital Forensics Fundamentals module provides the theoretical and practical application of this knowledge in the collection, analysis, and preservation of evidence, resulting in its constitution as evidence in court. The content present in the programme of this module, allows you to consolidate this objective.

1.2 Course objectives

The objectives of this module are to provide a theoretical understanding of the concepts of computer forensics and to apply this knowledge to the collection, analysis, and preservation of evidence, resulting in its constitution as evidence in court. The content present in the programme of this module, allows you to consolidate this objective of this module.

1.3 Course content

Due to its practical nature, the course will mainly take place in physical classes under the guidance of an instructor. In the workshop, students will be challenged to secure a crime scene and obtain as many clear clues as possible as to the course of the incident, the losses sustained and possible leads.

1.4 Learning objectives

- basic definitions
- securing physical evidence
- securing digital evidence
- use of evidence in court

1.5 Equipment and materials required

Computer room with Internet access
1 Pen Disk (memory stick) < 8GB
1 Pen Disk (memory stick) > 8GB

1.6 Syllabus

Learning outcome	The student who successfully completes the module will know/be competent in the following.
NEWS	
W1	Student knows models of digital forensic analysis
W2	The student knows the relationship between clues, evidence and crime
SKILLS	
U1	The student makes forensic reports
U2	The student at the scene identifies, collects, acquires and secures digital evidence using a variety of techniques, protecting the integrity of the evidence
U3	The student applies best practices and procedures in the acquisition and processing of digital evidence
U4	The student is familiar with various computer forensics techniques for the collection and analysis of different types of digital evidence using specific techniques and tools
COMPETENCES	
K1	Will be able to serve as a member or leader of the investigation team

Content of the module (programme of lectures and other activities)	**Reference to learning outcomes**
LECTURES 1. concepts, definitions and models WORKSHOPS 1. Securing and collecting digital evidence at crime scenes 2. Procedures for obtaining digital evidence a. Sterilisation procedures b. Acquisition techniques 3. Information gathering and analysis 4. Identification and analysis of information stored in operational systems 5. Use of OpenSource analytical tools 6. Case studies in digital forensics a. Case study: Hacking using Windows SO tool	W1, W2 U1-4 K1

Methods of verifying learning outcomes									
Learning outcome	Forms of credit classes								
	Oral examination	Written examination	Partial written assignment	Final written assignment (essay	Test	Project/presentation	Report	Classroom activities	Other ...
NEWS									
W1					x			x	
					x			x	
SKILLS									
U1						x		x	
U2						x		x	
U3						x		x	
U4						x		x	
COMPETENCES									
K1						x		x	

ECTS credit balance		
Form of student workload		Number of hours
Number of hours with direct participation of academic teacher		
1.1	Participation in lectures	4
1.2	Participation in seminars	
1.3	Participation in workshops	30
1.4	Participation in laboratory activities	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times per semester)	
1.7	Participation in the project consultation	
1.8	Participation in examinations/tests	2
1.9	Other ...	
1.10	**Number of hours spent with direct assistance of academic staff (sum 1.1 - 1.9)**	26
1.11	**Number of ECTS credits obtained by the student in classes requiring direct participation of an academic teacher)**	1
Individual student work		
2.1	Individual studies (including e-learning lectures)	20
2.2	Individual preparation for workshops	10
2.3	Individual test preparation	
2.4	Individual preparation for laboratory classes	
2.5	Preparation of reports	
2.6	Implementation of self-performed tasks (projects, documentation)	
2.7	Preparation for the final examination/tests of the workshop	5
2.8	Preparation for final examination/testing of lectures	5
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 - 2.9)**	40
2.11	**Number of ECTS credits obtained by the student in individual learning activities**	1,5
Total workload (h)		**66**

ECTS credits for the module	2,5

Criteria for assessing student competence

The minimum requirements for the three groups of learning outcomes that the student must achieve in order to pass the subject are presented below in synthetic form. In order for a student to pass a module, all learning outcomes described in the syllabus must be positively verified by the person(s) teaching the module.

W - KNOWLEDGE
Assessment:
Satisfactory - The student remembers and reproduces the knowledge to be mastered within the module.
Good - The student additionally interprets phenomena / problems and is able to solve a typical problem
Very good -Student is able to solve even complex problems in a given field, is able to synthesise, carry out a comprehensive evaluation, create a work that is original and inspiring to others.

U - SKILLS
Assessment:
Satisfactory - The student knows the nature of the activities and is able, under the guidance of the academic teacher, to carry out activities / solve problems related to the content of the module
Good - Student is able to independently carry out activities / tasks / solve typical problems related to the content of the module.
Very good - The student has fully mastered the ability / skill to perform the activities / tasks / problems provided for in the module content, also in more complex cases.

K - SOCIAL COMPETENCE
Assessment:
Satisfactory - Student passively assimilates module content, demonstrating ability to concentrate and listen.
Good - Student actively participates in classes, makes value judgements according to the criteria accepted in the given field, can actively cooperate in a group.
Very good - The student integrates the attitude according to the proposed model, develops his/her own system of professional and social values, is able to take responsibility for the actions of the group, including leadership.

2. Basic material for the teacher

- All Definitions and key notes are included in the presentations.

3. Activities

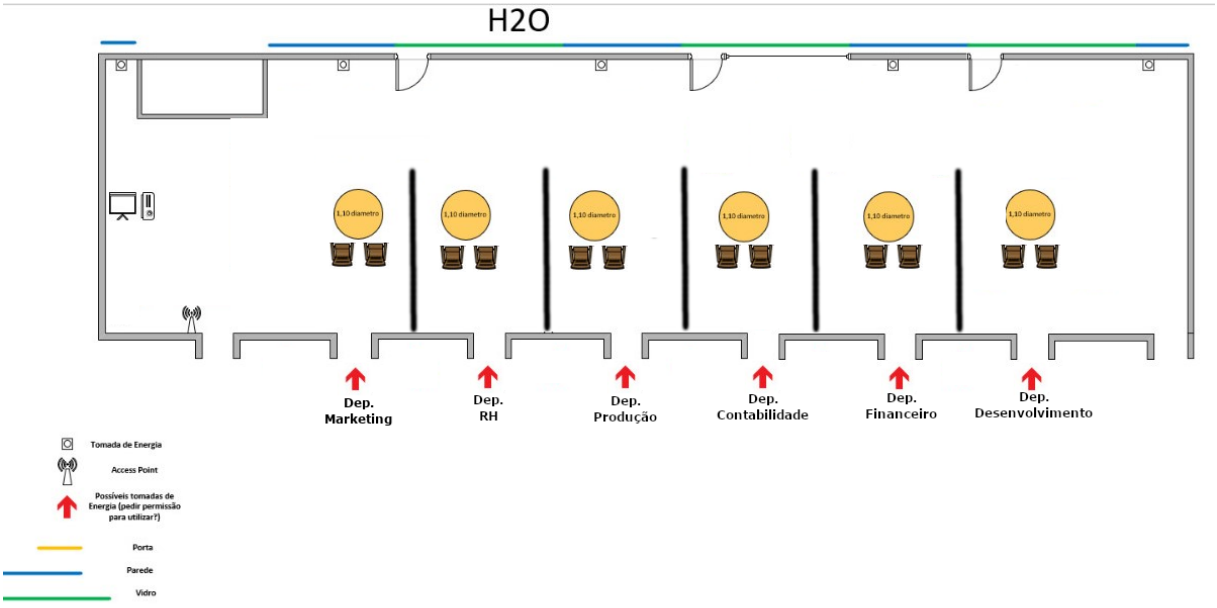
- **Discussion** (question delivery) - This type of questioning is used to get students thinking about the procedures and importance of digital forensics. Participants should arrive at an answer on their own or through group activities such as brainstorming.

  1- When we find an important document in a suspicious Desktop folder, how can we understand how that document was saved in that folder? What artefacts should be analysed?
  2- When all the clues point to the use of the cloud to store important evidence, knowing a user's credentials, do we need to go into that cloud and analyse the data contained there?
  3- Will using The Sleuth Kit autopsy be sufficient to analyse a Microsoft Windows hard drive? In what context should we use other tools?

- **Creating and analysing artefacts** - This could be an exercise to work in pairs/groups. The main aim is to have a team create just one type of digital artefact, sharing with the other team the activity that was associated with it. The other team, doing the analysis, will collect forensic evidence from this activity. When they get the expected forensic results, they reverse roles.

- **Creating pages for artefact analysis** - Operating systems are always creating new artefacts that needed to be subjected to forensic analysis. This analysis can be important information for forensic investigators in their procedures.

- Crime scene exercise - The purpose of this exercise is to develop the practical content related to operating at the crime/incident scene as well as operating in front of a powered computer (live-data forensics). It is necessary to prepare the following steps:
    1. **Setting up the scenario** - This starts with inviting / nominating students to be on site with the necessary tools to be part of the team to collect forensic evidence. It will be necessary to prepare the type of crime under investigation, the collection site, the equipment involved, etc.
    2. **Preparing the computers** - This is the most important stage, preparing the computers with the necessary artefacts that will be collected by the students. It will be necessary to create all the artefacts and once the first computer is prepared, we duplicate or clone the hard drive for the number of computers needed, according to the scenario.
    3. **Preparing the space** - With regard to the procedure space, it will be imperative to have the most realistic scenario as possible, like which section of the space with the Network Router and the Internet, with people as figureheads, and so on. It helps to draw the space as in the example below:



The premises can be just a room, but in this case the option was to have 6 teams working at the same time, spending less time but involving more people acting as figureheads and observing each team.

4. Evaluation - Each team will collect all necessary data and information before disconnecting the power cable, with confidence in the successful forensic analysis of the dead box. The

equipment will remain in the care of each team until the team has delivered all equipment and the forensic analysis report. The evaluation will focus on this report.

4. **Internet resources**

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition (ojp.gov) - https://www.ojp.gov/pdffiles1/nij/219941.pdf

NIST SP 800-86 Guide to integrating forensic techniques into incident **response** https://doi.org/10.6028/NIST.SP.800-86

Subcommittee on Digital Evidence | NIST - https://www.nist.gov/organization-scientific-area-committees-forensic-science/digital-evidence-subcommittee

Scientific Working Group on Digital, Digital and Multimedia Evidence (Digital Forensics) as a Forensic Science discipline

DFIRScience - YouTube - https://www.youtube.com/c/DFIRScience

Forensics - start.me - https://start.me/p/q6mw4Q/forensics

DFIR training - https://dfir.training/

FSIDIIN | Forensic Science International: Digital Investigation | Journal | ScienceDirect.com by Elsevier - https://www.sciencedirect.com/journal/forensic-science-international-digital-investigation

5. **Interesting cyclical events**

- **SANS Cyber Threat Intelligence Summit& Training [Online].**
- **IFIP Working Group 11.9 International Conference on Digital Forensics [Arlington, USA].**
- **General Police Equipment Exhibition& Conference (GPEC Digital) [Frankfurt, Germany].**
- **Techno Security & Digital Forensics [Pasadena, USA].**
- **Forensics Asia Expo [Jakarta, Indonesia].**
- **Forensics Europe Expo [London, UK].**
- **Magnet Virtual Summit [Online].**
- **Magnet User Summit [Nashville].**
- **National Conference on Cybercrime [Online].**
- **International Conference on Digital Forensics and Justice System [Online].**
- **International Association of Forensic Sciences (IAFS) [Sydney, Australia].**
- **Congreso Informatica y Ciberseguridad 2023 [Madrid, Spain].**
- **CHICYBERCON [Chicago, USA].**
- **DFRWS - Digital Forensic Research Workshop [Bonn, Germany].**

- **International Association of Computer Investigative Specialists (IACIS) [Orlando, Florida].**
- **ADFSL conference on digital forensics, security, and law**

6. Questions amd exercises

Q1.1. What is computer forensics?

a) It is the investigation process aimed at answering questions related to digital events.
b) It is investigation that uses science or technology to present evidence in court.
c) It is a science branch that studies processes of digital evidence acquisition, analysis, and preservation for legal purposes.
d) It is a science branch that studies processes of digital evidence acquisition, analysis, and preservation.

Q1.2. Which of these is not a basic principle of information security?

a) Capacity
b) Integrity
c) Authenticity
d) Confidentiality

Q1.3. What is the main objective of computer forensics?

a) Corrective
b) Internal organisation
c) Security assessment
d) Legal

Q1.4. Which of these statements is correct?

a) The forensics investigator must ensure confidentiality of all data under investigation.
b) The forensics investigation must ensure integrity of all data under investigation.
c) The forensics investigation must ensure authenticity of all data under investigation.
d) All statements are correct.

Q1.5. Identify the correct statement, bearing in mind that, in their conclusions, investigators must:

a) Determine the formal suspect's guilt or innocence.
b) Determine if the digital evidence recovered incriminates the formal suspect.
c) Statements a) and b) are incorrect.
d) Statements a) and b) are correct.

Q1.6. Which of these questions must be answered for each piece of digital evidence?

a) How? Why? How much? Where?
b) When? Who? What?
c) Statements a) and b) are incorrect.
d) Statements a) and b) are correct.

Q1.7. Which topics represent a technical challenge for computer forensics?

a) Encryption
b) Elimination
c) Volatility
e) All the previous topics.

Q1.8. Which of these topics does NOT represent a legal challenge in computer forensics?

a) Data privacy
b) Data protection

c) Data quantity
d) Changes to legislation

Q1.9. Who must start the equipment chain of custody?
a) The person responsible for analysing the equipment.
b) The person who seizes the equipment.
c) The person in charge of the investigation.
d) The judge who holds the case.

Q1.10. The chain of custory focuses on:
a) the equipment.
b) the formal suspect.
c) storage devices.
d) None of the previous answers is correct.

Q1.11. Which of these terms does NOT characterise a forensic analysis model?
a) DFRWS
b) EDRM
c) CFFTPM
d) IBIP

Q1.12. Indicate the correct order of the stages of investigation methodologies in digital forensics:
a) Identification, Preservation, Collection, Analysis, Presentation
b) Identification, Collection, Preservation, Analysis, Presentation
c) Identification, Preservation, Analysis, Collection, Presentation
d) Identification, Analysis, Preservation, Collection, Presentation

Q1.13. Should the chain of custody include content hash of the origin storage device?
a) Yes, at the beginning of the chain of custody.
b) Yes, when possible.
c) No, it's not necessary.
d) None of the previous answers is correct.

Q1.14. When a seized device is sent by carrier to another investigator, should the person responsible for transporting the device sign the chain of custody?
a) Yes.
b) No. He/She must not have access to the information under investigation.
c) No. That is not necessary as he/she does not participate in the investigation.
d) No. Transport must be carried out in maximum security.

Q1.15. Can the chain of custody form be modified according to the organisation that will apply it?
a) No, the form must be in a universally accepted format.
b) No.
c) Yes, the form can be modified at any time.
d) Yes, the form can be modified before it starts to be filled in.

2) Digital evidence preservation and recovery in the crime/incident scene.

Q2.1. According to ITIL, a cyber incident is:
a) a cyber attack.
b) a cybersecurity event.
c) an interruption or decrease in quality of an information technology service.
d) None of the previous answers is correct.

Q2.2. Which of the options does not represent one of the 5 stages in incident management and mitigation defined by ISSO/IEC 27035?

a) Preparation and planning
b) Assessment and decision
c) Risk definition
d) Detection and record

Q2.3. In the preparation for an incident, one must bear in mind

a) the briefing.
b) the risks.
c) the equipment.
d) the briefing, the risks, and the equipment

Q2.4. Which of these statements is more accurate?

a) Computer forensics is part of Incident Response.
b) Incident Response is part of Computer Forensics.
c) Computer Forensics and Incident Responde are not related.
d) Computer Forensics is part of Incident Response, but it can also be used in other contexts.

Q2.5. Which of these statements is false?

a) In the context of incident detection, the logs of involved pieces of equipment must be analysed.
b) According to the Law, in the context of incident detection, you should not respond to it.
c) In the context of incident detection, you should interrogate those involved.
d) According to the Law, in the context of incident detection, you should respond to it in a suitable way.

Q2.6. When a computer you are approaching in an incident response is turned on, should you shut it down immediately?

a) Yes, and carry out the analysis in a lab.
b) Yes, after the verification of destructive processes or the end of information collection.
c) Yes, always.
d) Yes, after the verification of destructive processes and the end of information recovery.

Q2.7. Should we turn on the device, even when it is found switched off?

a) Yes, if we belong to a Law Enforcement team.
b) No.
c) Yes, if the formal suspect is present.
d) Yes, on any occasion to obtain information.

Q2.8. When the computer is found turned on, should you photograph the screen?

a) Yes, if you belong to a Law Enforcement team.
b) No.
c) Yes, if the formal suspect is present.
d) Yes, on any occasion to obtain information.

Q2.9. According to ENISA's Good Practice Guide for Incident Management, how many incident severity levels are there?

a) 3
b) 4
c) 5
d) 6

Q2.10. According to ENISA's Good Practice Guide for Incident Management, a DDoS incident is classified as part of the … group.

a) blue

b) green
c) yellow
d) red

Q2.11. According to ENISA's Good Practice Guide for Incident Management, a phishing incident is classified as part of the … group.
a) blue
b) green
c) yellow
d) red

Q2.12. According to ENISA's Good Practice Guide for Incident Management, a spam incident is classified as an incident of … severity.
a) very high
b) high
c) regular
d) normal

Q2.13. When approaching a computer that is switched off in the context of incident response, should we verify the BIOS date/time?
a) Yes, at the beginning of the procedure.
b) Yes, when possible.
c) No.
d) Never.

Q2.14. When approaching a computer in the context of incident response, and the computer is turned on, should we disable communication functions?
a) Yes, at the beginning of the procedure.
b) Yes, when possible.
c) No.
d) Never.

Q2.15. When approaching a computer in the context of incident response, and a mobile device is found, should a Faraday bag be used?
a) Yes, after collecting information.
b) Yes, at the beginning of the procedure.
c) No.
d) Never.

3) Digital evidence acquisition procedures

Q3.1. Is a sterilization procedure absolutely necessary?
a) No.
b) Yes, it prevents the analysis of data that does not belong to the original device.
c) Yes, it guarantees authenticity.
d) No, it can be done afterwards.

Q3.2. The sterilisation procedure is aimed at writing all bits in 0 (zero) on:
a) the original disk.
b) the target disk.
c) operating system disk.
d) none of the previous items.

Q3.3. In the sterilization procedure, it is always necessary to validate the result. This can be done by using the following software:

a) dcfldd
b) dc3dd
c) dd
d) cat

Q3.4. It is possible to carry out a sterilization procedure on a device by using the following software:

a) lsblk
b) fdisk
c) dc3dd
d) cat

Q3.5. After the sterilization procedure, is it necessary to carry out any other procedure on the device?

a) No, the device is ready for the acquisition procedure.
b) Yes, the device needs to be formatted before the binary copy.
c) Yes, the binary copy can be made.
d) No, the device is ready for the binary copy.

Q3.6. Which software can be used for a sterilization procedure on MS Windows?

a) dc3dd
b) fdisk
c) Diskpart
d) All the previous answers are correct.

Q3.7. What is the importance of a lab photography report?

a) It allows the visualisation of the physical condition of the devices at the moment.
b) It helps to differentiate devices more easily.
c) It helps to know the exact dimensions of the devices
d) All the previous answers are correct.

Q3.8. In the photography report, must any damage on the devices be reported?

a) No, that is not part of the investigation team's responsibilities.
b) No.
c) Yes, it may be necessary in court.
d) Yes, but it must not be included in the report.

Q3.9. Should the photography report present all sides of the device?

a) Yes, at least 2 views must be presented.
b) Yes, at least 4 views must be presented.
c) Yes, at least 6 views must be presented, with a metric scale.
d) No.

Q3.10. Should the photography report include views of the inside of the device?

a) Yes, to present the storage device.
b) Yes, to present the condition of the internal components.
c) No.
d) Both a) and b) are correct.

Q3.11. Linux CAINE stands for:

a) Computer Aided Investigative Native Environment.
b) Computer Aided Investigative Environment.

c) Carving Access Investigation Natural Environment.
d) Computer Access Investigation Natural Environment.

Q3.12. Is Paladin Edge a Linux forensic distribution?
a) Yes, it is a Linux Live distribution.
b) Yes, it is a pentesting and forensic Linux distribution.
c) Yes, it is a Linux distribution that needs to be installed on the investigator's computer.
d) No.

Q3.13. The forensic acquisition can also be designated:
a) Binary copy (bit by bit).
b) Binary replication (bit by bit).
c) Both previous answers are correct.
d) None of the previous answers is correct.

Q3.14. Write protection is importance because it ensures:
a) data authenticity.
b) data integrity.
c) non-repudiation of data
d) None of the previous answers is correct.

Q3.15. The validation of the acquisition process can be done by:
a) Comparing the content hash of the original device and the copy on the target device.
b) Comparing the digital summary of the original device and the copy on the target device.
c) Comparing the SHA1 and SHA256 of the content on the original device and the copy on the target device.
d) All previous answers are correct.

4) Acquisition and analysis of volatile information

Q4.1. On a computer, volatile information is:
a) Information that is lost when a system is shut down.
b) Information in RAM memory.
c) Information that can be easily retrieved.
d) Information on the hard drive.

Q4.2. In a live-data forensic analysis, it is usual to collect information such as:
a) Active processes.
b) Cyphered volumes.
c) RAM memory.
d) All the previous answers are correct.

Q4.3. Which of these cannot be considered volatile information?
a) RAM memory
b) Services
c) Network connections
d) Thumbnails

Q4.4. Which of these types of information is most volatile?
a) Network connections
b) Registry keys
c) Processes in execution
d) RAM memory

Q4.5. In the collection of volatile information in a MS Windows system, you should use…

a) a command line or a Shell.
b) WMI.
c) PowerShell.
d) software with the lowest digital footprint.

Q4.6. Eric Zimmerman's tools are known for information collection on:

a) Linux.
b) MacOS.
c) MS Windows.
d) All previous answers are correct.

Q4.7. Nir Sofer's tools are known for information collection on:

a) Linux
b) MacOS
c) MS Windows
d) All previous answers are correct.

Q4.8. Which of these pieces of information should be collected from the screen of a computer under investigation?

a) Executed programs
b) Date/time and time zone
c) Open files
d) Desktop icons

Q4.9. Should the user information on the computer be verified?

a) Yes, all users' information
b) Yes, only the information referring to the logged-in user.
c) Yes, only the information of the user under investigation.
d) No.

Q4.10. The acquisition of memory can be done on Ms Windows by using:

DumpIT.
FTKImager.
Wimpmem.
All the previous answers are correct.

Q4.11. The pagefile.sys file is

a) a system file.
b) a file to virtually extend available system memory.
c) a non-volatile file.
d) All previous answers are correct.

Q4.12. Volatility is software that allows

a) RAM acquisition
b) RAM transfer
c) RAM analysis
d) RAM copy

Q4.13. When using the Volatility software, in order to determine the operating system of a RAM memory dump, the following plugin is used:

a) osinfo
b) operatingsystem
c) meminfo
d) imageinfo

Q4.14. The RegistryReport software allows the analysis of register files from the memory.

a) Yes, just like any other register file.
b) Yes, except for NTUSER.DAT.
c) Yes, except for SAM.
d) No.

Q4.15. In the content of a RAM memory dump, it is possible to identify:

a) image files.
b) documents.
c) internet browser URLs.
d) All previous items.

5) Identification and analysis of information points of interest in operating systems

Q5.1. Should user information be included in a report?

a) Yes, all users' information
b) Yes, only that of active users in the system
c) Yes, only that of the user under investigation.
d) No.

Q5.2. About the MS Windows registry:

a) It is a hierarchical information database.
b) It has a logical structure of 4 root keys.
c) HKCR stands for Hive Key Current Root
d) Most of its files are located at: C:\Windows\System\Config

Q5.3. The HKCU hive is a HKU subkey.

a) True
b) False, the HKCU hive is on the same hierarchical level as the HKU.
c) False, the HKCU hive is a HKLM subkey.
d) False, the HKCU hive is a HKCC subkey.

Q5.4. Most information on the hardware profile is stored in

a) HKey_Local_Machine
b) HKey_Current_Config
c) HKey_Current_User
d) HKey_Local_Config

Q5.5. The C:\Users\<username>\ntuser.dat file

a) stores information on the logged-in user.
b) stores information on all system users.
c) stores information on the user represented by <username>.
d) does not store information on the users.

Q5.6. Is it possible to copy all the register files with the computer turned on?

a) Yes, through Access Data FTKImager software.
b) Yes, through the RAWCopy software.
c) Sim, through Access Data Registry viewer software.
d) No, it's not possible.

Q5.7. The time zone setup information is located:

a) In the register key SYSTEM\ControlSet001\Control\TimeZoneInformation.
b) In the register key SOFTWARE\ControlSet001\Control\TimeZoneInformation.
c) In the register key SOFTWARE \ControlSet001\TimeZoneInformation.

d) None of the previous answers is correct.

Q5.8. The setup information of USB devices connected to the system is located:

a) In the register key HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
b) In the register key HKLM\SYSTEM\CurrentControlSet\Enum\USB
c) In the register key C:\Users\<username>\ntuser.dat
d) All previous answers are correct.

Q5.9. What does a user's SID stand for?

a) Security Identifier
b) State Identifier Domain
c) Security Identifier Domain
d) None of the previous answers is correct.

Q5.10. In Linux operating systems, application logs are usually located at:

a) /bin
b) /var/log
c) /root
d) /proc

Q5.11. In Linux operating systems, system settings are usually located at:

a) /proc
b) /bin
c) /etc
d) /root

Q5.12. In Linux operating systems, applications are usually located at:

a) /root
b) /proc
c) /etc
d) /bin

Q5.13. In Linux operating systems, information of USB devices connected to the system are located at:

a) /var/log/syslog
b) /var/log/USB
c) /var/log/devices
d) /var/log/usb

Q5.14. In Linux operating systems, operating system information is usually located at:

a) /var/log/syslog
b) /etc/os-release
c) /opt/os-release
d) /etc/log/syslog

Q5.15. In Linux operating systems, information on recenltly used files is usually located at:

a) /home/$USER
b) /home/user/<user>/recently-used.xbel
c) /home/user/.local/share/recently-used.xbel
d) /home/user/<user>/share/recently-used.xbel

6) Forensic analysis with free suites

Q6.1. Is EnCase software free?

a) Yes, but registration is required.
b) Yes, with no restrictions.
c) No, it is commercial software.
d) No, this is commercial software, with a temporary trial version.

Q6.2. Is IPED free?

a) Yes, it is open-source software.
b) Yes, it is free, but it is not open-source software.
c) No, it is a commercial licence.
d) None of the previous answers is correct.

Q6.3. What does IPED stand for?

a) Indexer and Digital Evidence Processor
b) Investigation and Processing of Digital Evidence
c) Integrated and processing Environment Decoded
d) None of the previous answers is correct.

Q6.4. Does IPED have multiprocessing capacity?

a) Yes, it uses multithreading.
b) Yes, but with a maximum of 2 cores
c) Yes, but with a maximum of 4 cores

Q6.5. Can you search file hashes with IPED?

a) Yes, in multiple formats, including SHA-256.
b) Yes, in MD5 and SHA1.
c) Yes, only MD5.
d) No.

Q6.6. On Autopsy, can you search file hashes in SHA-256?

a) yes, and MD5 also.
b) yes, and SHA-1 also.
c) Yes, and MD5 and SHA-1 also
d) No.

Q6.7. Is it possible to analyse Linux systems?

a) Both on IPED and Autopsy
b) On IPED
c) On Autopsy
d) On none.

Q6.8. The Sleuth Kit Library is used by the follow software:

a) IPED
b) Autopsy
c) Both by IPED and Autopsy
d) By none of the them.

Q6.9. A timeline can be used on:

a) IPED
b) Autopsy
c) Both on IPED and Autopsy
d) On none.

Q6.10. Is it possible to analyse MacOS systems?

a) On both IPED and Autopsy
b) On IPED
c) On Autopsy
d) On none.

Q6.11. Which software supports multi-users?

a) Both IPED and Autopsy
b) IPED
c) Autopsy
d) None

Q6.12. Is it possible to retrieve files through PhotoREC?

a) On both: IPED and Autopsy
b) On IPED
c) On Autopsy
d) No, on none.

Q6.13. Is it possible to identify text in image files?

a) Both on IPED and Autopsy
b) On IPED
c) On Autopsy
d) On none.

Q6.14. Is it possible to analyse Android systems?

a) Both on IPED and Autopsy
b) On IPED
c) On Autopsy
d) On none.

Q6.15. Known file databases can be supported by:

a) both IPED and Autopsy
b) IPED
c) Autopsy
d) None.

7. Additional questions/tests

https://quizlet.com/ca/750977127/computer-and-digital-forensics-flash-cards/

8. Bibliography

[1] BUNTING, Steve, The Official EnCE: EnCase Certified Examiner Study Guide, 2012.
[2] GRUNDY, Barry J., The Law Enforcement and Forensic Examiner'sI ntroduction to Linux (http://www.linuxleo.com/Docs/linuxintro-LEFE-4.31.pdf), 2017.
[3] CASEY, Eoghan, Digital Evidence and Computer Crime, Academic press, 2011.
[4] BROWN, Christopher L. T., Computer evidence: Collection and Preservation, 2nd Edition, 2009.
[5] CARVEY, Harlan, Investigating Windows Systems, 1st Edition, 2018.
[6] HALE LIGH, Michael, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory 1st Edition, 2014.
[7] ENISA, Identification and handling of electronic evidence Toolset, September 2013.
[8] ENISA, Identification and handling of electronic evidence Handbook, September 2013.

[9] NIST, Computer Security Incident Handling Guide, Special Publication 800-61r2.

Module 6

Comprehensive network security

1. Introduction

The Comprehensive Network Security module focuses on hardware and software methods of preventing and detecting intrusions and attacks. The methods presented should be widely used in all institutions and knowledge of them is essential for anyone who wants to be involved in cyber security.

1.1 Course objectives

The objectives of this module are to introduce students to the basic ways of protecting the local network in any institution. These methods are widely available, do not require very specialised knowledge and yet allow you to significantly increase the security of any network.

1.2 Course content

The lecture part of the course will mainly take place online, although the instructor may expand on the topics during classroom sessions.

1. Firewalls
1.1 Introduction to firewalls
1.2 The need for a firewall
1.3 Types and characteristics of firewalls
1.4 Firewall topologies and architectures
1.5 Examples of firewalls

2. intrusion detection systems
2.1 Introduction to intrusion detection systems
2.2 Types and characteristics of intrusion detection systems
2.3 Implementation architectures for intrusion detection systems
2.4 Intrusion detection systems common solutions and examples

3. intrusion prevention systems
3.1 Introduction to intrusion prevention systems
3.2 Types and characteristics of intrusion prevention systems

3.3 Implementation architectures for intrusion prevention systems
4 Antivirus
4.1 Introduction to malware
4.2 How a malware infection occurs
4.3 The most common types of malware
4.4 How to detect, remove and prevent malware infections
4.5 The special case of the antivirus programme
4.6 How the antivirus programme works
4.7 Choosing the right antivirus software

1.3 Learning objectives

1. Understand the role of the Firewall in cyber security technologies, its types and features, topologies and architectures, and common solutions;
2. Understand the role of intrusion detection systems in cyber security technologies, their types and characteristics, implementation architectures and commonly used solutions;
3. Understand the role of intrusion prevention systems in cyber security technologies, their types and characteristics, implementation architectures and commonly used solutions;
4. Understand the role of Anti-Malware in Cyber Security technologies, how malware spreads, the different types of malware, how to detect, remove and prevent against malware infections, how the specific case of Anti-Malware - antivirus - works and its common solutions.

1.4 Equipment and materials required

Computer room with Internet access
Anti-virus software

1.5 Syllabus

Learning outcome	The student who successfully completes the module will know/be competent in the following.
NEWS	
W1	The student knows the principle of operation of firewall systems, IPS, IDS and anti-virus programmes.
W2	The student understands the importance of using appropriate safeguards in his/her institution
SKILLS	
U1	Students will be able to apply commonly available methods to detect and prevent intrusions and attacks.
U2	Student is able to find weak links in the cyber security of an institution
COMPETENCES	
K1	The student is able to transfer knowledge and competences regarding basic security to the employees of his/her institution.

Content of the module (programme of lectures and other activities)	**Reference to learning outcomes**
LECTURES 1. Firewalls 2. intrusion detection systems 3. intrusion prevention systems 4 Anti-virus programmes WORKSHOPS 1. firewall configuration 2. configuration of IDS and IPS systems 3. familiarisation with and installation of anti-virus software 4. observing attack statistics and drawing conclusions	W1, W2 U1, U2 K1

Methods of verifying learning outcomes									
Learning outcome	Forms of credit classes								
	Oral examination	Written examination	Partial written assignment	Final written assignment (essay	Test	Project/presentation	Report	Classroom activities	Other ...
NEWS									
W1					x			x	
W2					x			x	
SKILLS									
U1						x		x	
U2						x		x	
COMPETENCES									
K1						x		x	

ECTS credit balance		
Form of student workload		Number of hours
Number of hours with direct participation of academic teacher		
1.1	Participation in lectures	4
1.2	Participation in seminars	
1.3	Participation in workshops	12
1.4	Participation in laboratory activities	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times per semester)	
1.7	Participation in the project consultation	
1.8	Participation in examinations/tests	2
1.9	Other ...	
1.10	**Number of hours spent with direct assistance of academic staff (sum 1.1 - 1.9)**	18
1.11	**Number of ECTS credits obtained by the student in classes requiring direct participation of an academic teacher)**	0,5
Individual student work		
2.1	Individual studies (including e-learning lectures)	30
2.2	Individual preparation for workshops	10
2.3	Individual test preparation	
2.4	Individual preparation for laboratory classes	
2.5	Preparation of reports	
2.6	Implementation of self-performed tasks (projects, documentation)	
2.7	Preparation for the final examination/tests of the workshop	10
2.8	Preparation for final examination/testing of lectures	5
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 - 2.9)**	55
2.11	**Number of ECTS credits obtained by the student in individual learning activities**	2
Total workload (h)		**73**
ECTS credits for the module		**2,5**

Criteria for assessing student competence
The minimum requirements for the three groups of learning outcomes that the student must achieve in order to pass the subject are presented below in synthetic form. In order for a student to pass a module, all learning outcomes described in the syllabus must be positively verified by the person(s) teaching the module.

W - KNOWLEDGE
Assessment:
Satisfactory - The student remembers and reproduces the knowledge to be mastered within the module.
Good - The student additionally interprets phenomena / problems and is able to solve a typical problem.
Very good -Student is able to solve even complex problems in a given field, is able to synthesise, carry out a comprehensive evaluation, create a work that is original and inspiring to others.

U - SKILLS
Assessment:
Satisfactory - The student knows the nature of the activities and is able, under the guidance of the academic teacher, to carry out activities / solve problems related to the content of the module.
Good - Student is able to independently carry out activities / tasks / solve typical problems related to the content of the module.
Very good - The student has fully mastered the ability / skill to perform the activities / tasks / problems provided for in the module content, also in more complex cases.

K - SOCIAL COMPETENCE
Assessment:
Satisfactory - Student passively assimilates module content, demonstrating ability to concentrate and listen.
Good - Student actively participates in classes, makes value judgements according to criteria accepted in the given field, is able to cooperate actively in a group.
Very good - The student integrates the attitude according to the proposed model, develops his/her own system of professional and social values, is able to take responsibility for the actions of the group, including leadership.

2. Basic materials for the teacher

- All definitions and key notes are included in the presentations.

3. Activities

- Workshop on "hacking" websites with demonstration of how security systems work

- Presentation of live attacks and statistics on how many of these attacks could have been blocked by commonly available security methods

4. Internet resources

- https://www.parallels.com/blogs/ras/types-of-firewalls/
- https://phoenixnap.com/blog/types-of-firewalls
- https://www.idc-online.com/technical_references/pdfs/data_communications/Firewall_Architectures.pdf
- https://phoenixnap.com/blog/intrusion-detection-system
- https://wisdomplexus.com/blogs/different-types-of-intrusion-detection-systems-ids/

- https://www.educba.com/types-of-intrusion-prevention-system/
- https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- https://www.snort.org/
- https://www.techtarget.com/searchsecurity/definition/malware
- https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

5. Interesting cyclical events

- European Cyber Security Conference (https://eucybersecurity.com/)
- The Official Cyber Security Summit (https://cybersecuritysummit.com/)
- Annual CPX Checkpoint Experience
- Cisco Live ALL IN (https://www.ciscolive.com/emea.html?zid=pp)
- International Conference on Communication and Network Security (http://www.iccns.org/)

6. Additional questions/tests

- https://quizlet.com/199055325/firewall-flash-cards/
- https://www.proprofs.com/quiz-school/topic/firewall
- https://quizlet.com/180954294/chapter-8-using-intrusion-detection-systems-flash-cards/
- https://quizlet.com/534059481/chapter-7-intrusion-detection-and-prevention-systems-flash-cards/
- https://quizlet.com/222087233/what-is-malware-flash-cards/
- https://quizlet.com/27987027/malware-flash-cards/
- https://www.gns3.com/
- https://www.brianlinkletter.com/open-source-network-simulators/

7. Questions and Exercises

Firewalls

Question 1

What's the meaning of the word "firewall" in computer's world?

"wall of fire" – its one of the main security mechanisms implemented worldwide
"wall of fire" – it's a special computer program to create design effects
"wall of fire" – it's a security tool dedicated to mobile devices
"wall of fire" – it's a security tool dedicated to desktop computers

Question 2

When were firewalls firstly developed?

By the end of 2000
By the end of 1890
By the end of 1980
By the end of 1990

Question 3

What's the name of the first computer virus?

"Morris Worm"
"Morris Vorm"
"Worm Morris"
"Vorm Morris"

Question 4
How firewalls used to work on their first generation?
- Filtering rules based on OSI's layer 6
- Filtering rules based on OSI's application layer
- Filtering rules based on IP addresses
- Filtering rules based on MAC addresses

Question 5
How firewalls used to work on their second generation?
- Filtering rules based on OSI's layer 6
- Filtering rules based on OSI's network layer
- Filtering rules based on OSI's session layer
- Filtering rules based on OSI's layer 4

Question 6
How firewalls used to work on their third generation?
- Filtering rules based up to OSI's transport layer
- Filtering rules based up to OSI's application layer
- Filtering rules based only on IP addresses
- Filtering rules based on the TCP port

Question 7
What type of security mechanism is able to control communications between internal and external networks?
- Router
- Firewall
- Network Hub
- Network Switch

Question 8
Please enumerate the most common attacks.
- Confidential Data Leak; Denial-of-Service
- Downstream Liability; Data Loss; Confidential Data Leak; Denial-of-Service
- Downstream Liability; Data Loss; Confidential Data Leak; SLQ Injection
- Downstream Liability; Data Loss; Confidential Data Leak; Dynamic Denial-of-Service

Question 9
Please identify one firewall limitation or disadvantage.
- Easy detection of a malicious insider, but just when directly connected to the device
- There are no constant updates, so it is necessary for administrators to manually update them
- New network services and protocols may not be properly identified and treated by the existing firewalls
- It is impossible for a firewall to detect a viruses

Question 10
Please identify one firewall advantages.
- Protection against vulnerable services
- Decentralized security
- Low privacy levels
- Cheap and easy to install

Question 11

In your opinion, what better describes a state-based firewall?

Bases the analysis on signatures and well-known vulnerabilities and attacks

Manipulate dynamic information and keep monitoring actions on packet analysis

Are present on personal computers and have just a reduced number of functionalities

Focus on the analysis and monitoring of applications and web applications only

Question 12

What better defines dynamic filtering?

Data are blocked or allowed simply based on rules and not on relations among the packets

Have limited performance and protection, allowing users to apply simple rules and configure access from apps and services to the Internet

Filtering URL only

Filtering according to the packet's context

Question 13

What does a Downstream Liability attack consist of?

Gain access to the network and delete files and other information

The network is used as an access to attack other networks

Stop the systems and network from communicating

None of the above

Question 14

What's the difference between a hardware and a software firewall?

A software firewall consists of the program used to secure the communications, while the hardware is just the server or appliance where it is installed

A hardware firewall is a type of firewall that is used only on industrial environments, while the software one may be used everywhere

There is no difference between them

None of the above

Question 15

In a screened host firewall architecture, what's the role of a bastion host?

Plays the role of an Internet router

Plays the role of an internal switch

Plays the role of an external router

Plays the role of an external switch

Intrusion Detection Systems (IDSs)

Question 1

What's the main role of an intrusion detection system?

a) Identify and prevent intrusions
b) Identify and monitor malware infections
c) Identify and alert about intrusions
d) Identify viruses and other malicious applications

Question 2

What's the main tasks that an efficient IDS should perform?

a) Collect and analyse all exchanged packets from internal and external communications
b) Analyse and prevent communications in specific ports
c) Prevent systems from being malware infected
d) None of the above

Question 3
Why can't a host-based IDS be implemented on a critical system?

a) Critical systems have closed networks
b) Critical systems have devices with low processing and battery power
c) Critical systems don't need this type of security
d) Critical systems don't have any communication to external networks

Question 4
How many main types of IDS can you identify?

a) 4
b) 2
c) 5
d) None of the above

Question 5
What better describes a network-based IDS.

a) Installed at every host in the network
b) Installed at the network and with host agents
c) Installed at the network level
d) Installed after the firewall and before the Internet router

Question 6
Focusing on a state-based IDS, what's their base of analysis?

a) This IDS uses well-known vulnerability signatures as base for intrusion identification
b) This IDS focuses on the system behaviour as base for intrusion identification
c) This IDS uses machine learning techniques as form of intrusion identification
d) None of the above

Question 7
In which cases should we implement a host-based IDS?

a) When there is a need to monitor single computers
b) When there is a need to monitor critical systems
c) When there is a need to prevent intrusions on a specific host
d) None of the above

Question 8
In which cases should we implement a network-based IDS?

a) When there is a need to monitor single computers
b) When there is a need to monitor critical systems
c) When there is a need to prevent intrusions on a specific host
d) None of the above

Question 9
What's an IDS most common implementation?

a) IDSs are usually placed in between the private and public networks
b) IDSs are used within the public network
c) IDSs are used separating each host
d) IDSs are used at the boarder of the public network and the Internet

Question 10
Which one of the following is an anomaly-based IDS advantage?

a) It takes advantage of a well-known signature database
b) It takes advantage of well-known attacks
c) It takes advantage of the server processing power to protect critical sensors
d) None of the above

Question 11
Which one of the following is an anomaly-based IDS disadvantage?

a) Higher false positive rates
b) Lower false positive rates
c) Higher processing power required
d) None of the above

Question 12
Why can't a SCADA system have HIDS installed on its components?

a) Its components have low processing and energy power
b) Its components are not connected to the networks
c) Its components already include a HIDS system on them
d) None of the above

Question 13
What type of IDS is SNORT?

a) Behavioural IDS
b) Machine Learning Technique
c) Signature-based IDS
d) Anomaly-based IDS

Question 14
What's the main distinguish feature between Suricata and SNORT?

a) Suricata has dynamic protocol protection with port agnostic, while SNORT doesn't
b) Suricata is an IPS and SNORT is an IDS
c) Suricata just works based on anomalies, while SNORT is also capable of signature analysis
d) None of the above

Intrusion Prevention Systems (IPSs)

Question 1
What's the main role of an intrusion prevention system?

a) Identify and alert intrusions and attacks
b) Monitor and prevent intrusions and attacks
c) Protect against malware
d) Perform access control through URL filtering

Question 2
What's the main difference between IDSs and IPSs?

a) IDSs are used to monitor the network, while IPSs are used to monitor hosts
b) IDSs are used to prevent intrusions, while IPSs just identify them and alert
c) IDSs are used to identify intrusions, while IPSs are used to prevent them
d) IDSs are used to prevent malware, while IPSs are used to prevent viruses

Question 3
What's the most common implementation form of an IPS?

a) IPSs are used within the public network

b) IPSs are used separating each host
c) IPSs are used at the boarder of the public network and the Internet
d) IPSs are usually placed in between the private and public networks

Question 4
Why isn't an IPS, on its own, able to fully protect the system or network?
a) Because it is not able to control on attacks
b) Because it is not able to alert intrusions
c) Because it is not able to be implemented on the network, just by host
d) None of the above

Question 5
In your opinion, why is an IPS customization an important factor?
a) Because it allows administrators to monitor the entire network
b) Because it allows to download vulnerability signatures
c) Because it allows a better adaptation to the organization's security policy
d) Because it allows users to personally control on the IPS rules

Question 6
Why are new IPS solutions being connected to cloud services?
a) Because it allows administrators to use them for cloud files
b) Because it provides a more sophisticated approach to protect the system
c) Because it allows the use on remote areas
d) None of the above

Question 7
How many IPS types and sub-types can you identify?
a) 9
b) 4
c) 6
d) 5

Question 8
What's an anomaly-based IPS based on?
a) It is based on vulnerability signatures
b) It is based on security policies employed by the enterprise
c) It is based on the host processing power
d) It is based on behaviour of the network and its systems

Question 9
What do you know about NBA, regarding an IPS?
a) Network-based anomaly analysis
b) Network behaviour assistance
c) Network behaviour analysis
d) None of the above

Question 10
What should be included on a good IPS planification?
a) System type
b) Comprehensive real-time protection
c) Protection against URL and port filtering
d) None of the above

Question 11
In your opinion, are IPSs a good security tool to be implemented on a critical infrastructure? Why?

a) Yes, because they will cut the communications, immediately protecting the system
b) Yes, because critical systems need the most advanced protection tools, such as IPSs
c) No, because it may break all communications, and this is a severe action to a critical system
d) No, because it demands a high processing power from all network devices

Question 12
What type of IPS is SNORT?

a) Behavioural IPS
b) Machine Learning Technique
c) Signature-based IPS
d) Anomaly-based IPS

Question 13
Complete the sentence: By nature, IPS is able to…

a) Alert and report intrusions only
b) Drop and block communications
c) Resets all connections
d) None of the above

Question 14
What's the best IPS type for DDoS (Distributed Denial of Service) prevention?

a) HIDS
b) WIPS
c) NBA
d) DoSIPS

Malware and Antivirus

Question 1
When was the term malware firstly used?

a) 1980
b) 1990
c) 2000
d) 2010

Question 2
What's the definition of malware?

a) Malicious piece of code or program
b) Malicious hardware components
c) Malicious virus
d) None of the above

Question 3
What are the main device behaviours of a malware infection?

a) Email not working, flood of annoying ads, system crashes, computer powers off, higher Internet activity
b) Computer slows down, flood of annoying ads, system crashes, loss of disk space, higher Internet activity
c) Flood of annoying ads, system crashes, computer powers off, constant virus alerts, computer slows down
d) None of the above

Question 4
What type of devices can suffer a malware infection?

a) Computers only, including desktops, laptops and servers
b) Mobile devices only, including smartphones and tablets
c) Servers only
d) All mentioned above

Question 5
Is there any chance for a device to be infected when there is not seen any malware infection behaviour?

a) No, all malware infections are perceptible
b) No, the only malware infection that doesn't present strange device behaviour is a virus
c) Yes, some malwares can hide their activity
d) None of the above

Question 6
How do we get a malware infection?

a) By phone calls and SMS texts
b) By Internet and Email
c) By phone SMS texts and Internet
d) None of the above

Question 7
In your opinion, what describes a virus?

a) It's a type of malware that displays unwanted ads to the user
b) It's a type of malware that records user's keystrokes
c) It's a type of malware that requires an action to start the infection
d) Virus is not a malware type

Question 8
What's the difference between a virus and a worm?

a) They are exactly the same, but called differently
b) Virus needs an action from the user, while a worm can act by itself
c) Virus are malicious code or programs, while worms are malicious emails
d) None of the above

Question 9
What is the most powerful weapon for attacker nowadays?

a) A trojan
b) A virus
c) A keylogger
d) A ransomware

Question 10
What's the best way to prevent a malware infection?

a) Navigate only through VPN connections
b) Browse the Internet with an anonymous browser
c) Install an antivirus
d) None of the above

Question 11
What's an antivirus?

a) It's a software capable of protecting against and removing viruses
b) It's a software capable of cleaning the websites from malicious files

c) It’s an appliance where the virus software is saved
d) It’s a piece of code able to infect a device

Question 12
Regarding virus protection, why are updates so important?
a) Updates increases the protection against new infections
b) Updates are not important
c) Updates brings information about well-known vulnerabilities and virus
d) None of the above

Question 13
What was the target of the first known malware?
a) Windows systems
b) ARPANET infrastructures
c) MacOS Systems
d) Linux Systems

Question 14
What’s an Exploit?
a) It’s a malware capable of recording all user’s keystrokes
b) It’s a malware that allows the user to use the computer to mine cryptocurrency
c) It’s a malware that takes advantages of bugs and other vulnerabilities
d) None of the above

Question 15
What type of malware are we talking about when the user’s keystrokes are recorded?
a) Adware
b) Virus
c) Worms
d) None of the above

8. Bibliography

1. Carter, E., & Hogue, J. (2006). *Intrusion prevention fundamentals*. Cisco Systems.
2. Chapman, D. B., & Zwicky, E. D. (1995). *Building internet firewalls*. Oreilly & Associates.
3. Grubb, S. (2021). *How cybersecurity really works: A hands-on guide for total beginners*. National Geographic Books.
4. Gupta, B., & Srinivasagopalan, S. (2020). *Handbook of research on intrusion detection systems*.
5. Guyer, J. P. (2017). *An introduction to intrusion detection systems*. CreateSpace Independent Publishing Platform.
6. Komar, B., Beekelaar, R., & Wettern, J. (2003). *Firewalls for dummies*. For Dummies.
7. Mendoza, H. (2018). *Remove malware, Spyware and viruses from your PC: Guide to increase your computer's security and speed by removing malicious viruses, malware, and Spyware*. CreateSpace Independent Publishing Platform.
8. Noonan, W., Noonan, W. J., & Dubrawsky, I. (2006). *Firewall fundamentals*. Cisco Press.
9. Pathan, A. K. (2016). *The state of the art in intrusion prevention and detection*. Auerbach Publications.
10. Verissimo, P. E. (2003). *Intrusion-Tolerant Architectures: Concepts and Design* [master's thesis]. https://www.di.fc.ul.pt/~nuno/PAPERS/TR-03-5.pdf