



CSIRTS AND CERTS



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



Publication financed by the European Commission under the Erasmus + programme.
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and neither the Commission nor the National Agency cannot be held responsible for any use which may be made of the information contained therein.



Table of contents

1. Cybersecurity
 - 1.1. Cybersecurity
 - 1.2. Principles of cybersecurity
 - 1.3. Risk, asset, vulnerability
 - 1.4. Cyber threats, events, incidents and attacks
2. CERT/CSIRT teams
 - 2.1. History
 - 2.2. CERT and CSIRT teams
 - 2.3. How a CERT/CSIRT team is formed
 - 2.4. CERT/CSIRT infrastructure cooperation
 - 2.5. Hierarchy of CERT/CSIRT teams?
 - 2.6. National and government CERT/CSIRT teams
 - 2.7. Situation in the Czech Republic and in the world
 - 2.8. National CSIRT of the Czech Republic
 - 2.9. Government CERT of the Czech Republic
 - 2.10. Which CERT/CSIRT team to contact?
 - 2.11. SUMMARY
3. Legislative framework of CSIRT/CERT
 - 3.1. Czech Republic
 - 3.2. Poland
 - 3.3. Portugal
 - 3.4. SUMMARY
4. Conclusion
5. References

1. Cybersecurity

Information and data represent considerable economic and political potential. Information, as both raw data and dataflow, can determine not only the existence or non-existence of an individual or company but also, by its nature, influence global development.[1]

We need to realise that the more we depend on information and communication technologies[2], and the more data these technologies collect and share about us, the more vulnerable we become.

Many of the consequences caused by cyberattacks, human recklessness or ignorance can be avoided if the basic principles of cybersecurity are followed.[3]

Cybersecurity is in essence an ever-evolving and changing process that is dependent on a number of variables. Of course, these variables can be data or the ICT elements themselves, which are the subject of protection, custom set processes and their revisions, etc. However, the most important element is the user (whether end user or administrator) who applies the elements of cybersecurity.

It is here where you will run into that theoretical stumbling block is, i.e. where you will be given the information, instructions and procedures that we have adopted and tested in good faith. What will be presented here is our view on the issue of cybersecurity and the processes associated with it. These instructions, procedures and recommendations work for us, but they may not work for you because, in the actual implementation of any security procedures, it is good to build on certain proven recommendations, but above all it is beneficial to tailor, modify or change these procedures depending on the specific conditions of either the individual user or the organisation.

The EU Network and Information Security Directive (NIS Directive) aims to create a CSIRT Network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". [1] The Directive states that each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in the Directive's point (1) of Annex I (requirements), covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. The Directive gives high-level requirements that designated CSIRTs must observe, and tasks that they must perform.[4]

[1] See information on influencing the presidential elections in the USA (2016) and France (2017). For more details, see e.g.:

Tajné služby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin. [online]. [cit. 29/06/2017]. Available from: <http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin>
Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma. [online]. [cit. 29/06/2017]. Available from: http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san

[2] Hereinafter referred to as the ICT

[3] *WannaCry se neměl vůbec rozšířit. Stačilo, abychom používali Windows Update.* [online]. [cit. 27/06/2017]. Available from: <https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx>

[4] *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cit. 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

1.1. Cybersecurity

"The prominence of cybersecurity has grown over the last decade and become one of the top priorities in many national policies. This is mainly due to the overlap with other security spheres and also due to incidents that have given this concept notoriety and forced the general public to think about the need for security in cyberspace. Connected to this is the need to protect cyberspace so that the comprehensive security of the Czech Republic is preserved as much as possible, as well as the right of individuals to informational self-determination."[1]

The definition of cybersecurity can be somewhat problematic. For many people, cybersecurity is an area that is essentially dealt with exclusively by information and communication technology departments.

This premise is wrong from the outset because cybersecurity concerns each of us who uses any element of ICT in our daily lives. If we do not realise that we are a key, and in many cases, crucial element of cybersecurity (whether in our private lives or at work), then we are actually increasing the likelihood of successful cyberattacks.

At present, cybersecurity cannot be underestimated or downplayed. It is an area that is crucial for many organisations, but also for individuals, and should therefore be addressed in a long-term and systematic way.

"Organisational management should understand and accept that cybersecurity management falls much more into other areas of security and crisis management. After all, even today's sophisticated attacks are often multidisciplinary and combine the areas of ICT, social engineering, personnel and object security."[2]

Returning to the concept of cybersecurity itself, it is appropriate to start from an analysis of this term. The word **cyber** represents a interconnection with elements of information and communication technologies and cyberspace as such.

Security

There are many definitions of **security**[3], but there is no single, generally accepted one. Most definitions of the term security are given in the literature rather than in the legislation itself.[4]

Mareš defines security as *"a state in which threats to a facility (usually a state, or even international organisations) and its interests are limited to the lowest possible level, and this facility is effectively equipped and willing to cooperate in eliminating existing and potential threats."*[5]

Požár defines *"security as a feature of a facility or entity that determines the degree, level of its protection against potential damage and threats."*[6]

This definition was further specified in the *Výkladový slovník kybernetické bezpečnosti* (Cybersecurity Glossary):

Security

A feature of an element (e.g. an information system) that is protected against losses at a certain level, or also the state of protection (at a certain level) against losses. IT security includes the protection of confidentiality, integrity and accessibility in the processing, storage, distribution and presentation of information.[7]

It should be noted that security is currently not just a concern of the state, which, however, still plays a primary role in ensuring security, but that it is a process implemented by other entities (legal entities and natural persons), which have recently been forced to deal more with the issue of security, or more precisely securing their activities against attacks.

Given this expansion of security's scope, it is necessary to address, inter alia, the following issues:

- **Whose security is it** (international organisation, state, organisation, individual, etc.)?
- **What values are protected** (organisation, people, data, etc.)?
- **What are (should be) these values protected against** (physical, cyber, combined attacks, etc.)?
- **What resources need to be spent to protect these values?** [8]

The ideal goal of security is to create a state of "absolute security". However, this state is a utopia, because it cannot be realistically achieved,[9] as there will always be a threat or risk that was not considered in the concept of security creation or was intentionally neglected.

However, the purpose of security is not to cover all real, less real or completely unpredictable and unlikely risks in all circumstances, as such an implementation would create a completely dysfunctional complex, which would in essence deny or even completely eliminate the application and implementation of security.

Example: *In everyday life, it can also happen to you, for example, that you lock yourself out of your apartment. If you have considered this possibility, you probably have spare keys with your family, friends, or elsewhere. However, if you do not have spare keys, you will probably call a locksmith or kick down the door.*

Cybersecurity

As with the concept of security, cybersecurity does not have a single generally accepted definition. Cybersecurity is a subset of security as such.

When defining cybersecurity, it is appropriate to start from already established definitions. Here are some of these definitions:

1. **Cybersecurity is a set of measures taken to protect a computer system against unauthorised access or attack.**[\[10\]](#)
2. The Oxford Dictionary states that **cybersecurity is the state of being protected against the criminal or unauthorised use of electronic data**. Cybersecurity must then include the measures that need to be taken to achieve this.[\[11\]](#)
3. According to Jirásek et al., **cybersecurity is "a set of legal, organisational, technical and educational tools designed to ensure the protection of cyberspace."**[\[12\]](#)
4. In a relatively similar way, cybersecurity is defined in "*Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.*" (The National Cybersecurity Strategy of the Czech Republic for 2015–2020). This strategy states that: "Cybersecurity is a **set of organisational, political, legal, technical and educational measures and tools aimed at ensuring a secure, protected and resilient cyberspace in the Czech Republic**, both for public and private sector entities and for the general Czech public."[\[13\]](#)

While these definitions seek to define the concept of cybersecurity, they are a little bit inaccurate.

The first definition focuses only on the computer and computer system and their protection against two types of cyberattacks, while the spectrum of both the targets of the attacks and especially the attacks themselves is much more diverse.[\[14\]](#)

The second definition then protects only electronic data and not computer systems as such.

The third definition focuses on the adoption of means to protect the elements of ICT in cyberspace. This definition is relatively precise, but its restriction to cyberspace can only be misleading as cybersecurity can also be applied to ICT elements that are not involved in cyberspace or create its own "off-line cyberspace".[\[15\]](#)

The last of the definitions is then explicitly limited to cyberspace in the Czech Republic, while completely ignoring the possibility of protecting the interests of citizens of the Czech Republic or other entities who are not established in the Czech Republic. We believe that the narrowing of cybersecurity to cyberspace in the Czech Republic is understandable from the point of view of the implementation of the Cybersecurity Act, but inappropriate from the point of view of the implementation of cybersecurity.

Another definition of cybersecurity can be found, for example, in the **Definition of Cybersecurity – Gaps and overlaps in standardization**[\[16\]](#) by ENISA, the European Agency for Cybersecurity[\[17\]](#): "*Cybersecurity refers to the security of cyberspace, where cyberspace refers to a set of links and relationships between objects that are accessible through a general telecommunications network and to a set of objects whose interfaces allow their remote control, remote access to data, or their connection to management actions within cyberspace. Cybersecurity will include the "CIA" paradigm of the triad for relationships and objects within cyberspace, and will be extended to ensure the protection of the privacy of entities (natural persons and legal entities) and the resilience [recovery from an attack].*"

Given the effort to define the concept of cybersecurity, it is appropriate to proceed from the procedural rules that cover cybersecurity.

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 of network and information systems across the Union states[\[18\]](#) in Article 4 (2) that "*security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible through, those network and information systems.*"

Definition of Cybersecurity by Polish law is – resistance of information systems to activities violating the confidentiality, integrity, availability and authenticity of the data processed or related services offered by these systems (Act of 5 July 2018 on the national cybersecurity system Journal of Laws of 2018, item 1560).

P – Definition of Cybersecurity – FIX ME

The above definitions seek in various ways to define the range of relationships, interests and entities against which cybersecurity is applied. At the same time, they also define cyberspace as the environment in which cybersecurity is applied.

Due to a certain inconsistency in opinions on what is and what is not cybersecurity, it is appropriate to present our own definition of cybersecurity, which arose both on the basis of an analysis of previous definitions and on the basis of our own experience.

Cybersecurity can be defined as:

- **a set of legal, organisational, technical and educational instruments aimed at ensuring the protection of computer systems and other elements of ICT, applications, data and users,**
- **the ability of computer systems and services used to respond to cyberthreats or attacks and their consequences, as well as planning to restore the functionality of computer systems and related services.**

Cybersecurity is implemented both within and outside cyberspace. It is not appropriate to limit the application of the above means and principles, geolocatively in any way (whether in the territory of a given state, the Union or cyberspace itself).

[1] Zpráva o stavu kybernetické bezpečnosti za rok 2017. [online]. [cit. 29/06/2018]. Available from: <https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf>

[2] Kybernetická bezpečnost: Co s tím? [online]. [cit. 29/06/2018]. Available from: <http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html>

[4] See, for example, Constitutional Act No. 110/1998 Sb., on the Security of the Czech Republic; Act No. 240/2000 Sb., on Crisis Management and on Amendments to Certain Acts (Crisis Act); Cybersecurity Act, etc.

[15] For more details, see e.g. *Příchod hackerů: příběh Stuxnetu*. [online]. [cit. 01/07/2018]. Available from: <https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/> or FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. [cit. 01/07/2018]. Available from: <https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html>

[3] With regards to the interpretation of the term itself, it is necessary to mention the relative inaccuracy of Czech language compared to English, which typically uses two terms for the Czech term "bezpečnost": **security** and **safety**. The term **security** is used in the sense of active protection or active securing, ensuring or protection and the term **safety** is usually used to express passive safety, prevention of harm, characteristics of the state or properties of a particular object.

[5] ZEMAN, Petr et al. *Česká bezpečnostní terminologie: Výklad základních pojmů*. [online]. [cit. 10/07/2018]. Available from: <http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048>, p. 13

[6] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, p. 37.

[7] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition Prague: AFCEA, 2015, p. 23. [online]. [cit. 10/07/2018]. Available from: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovník-kyberneticke-bezpecnosti---druhe-vydani/>

[8] For more details, see e.g. MAREŠ, Miroslav. *Bezpečnost*. [online]. [cit. 10/07/2018]. Available from: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0

FRANK, Libor. *Bezpečnostní studia*. [online]. [cit. 10/07/2018]. Available from: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf

[9] See WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Aleš Čeněk, 2005. 159 p. ISBN 80-86898-2-10

[10] *Cybersecurity*. [online]. [cit. 06/07/2018]. Available from: <https://www.merriam-webster.com/dictionary/cybersecurity>

[11] *Cybersecurity*. [online]. [cit. 06/07/2018]. Available from: <https://en.oxforddictionaries.com/definition/cybersecurity>

[12] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 69. [online]. [cit. 10/07/2018]. Available from: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovník-kyberneticke-bezpecnosti---druhe-vydani/>

[13] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. [online]. [cit. 01/07/2018]. Available from: <https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf> p. 5

[14] Applications, user accounts, etc. can also be attacked. Regarding attacks, then some individual attacks are described, for example, in: KOLOUCH, Jan. *CyberCrime*. Prague: CZ.NIC, 2016, p. 181 et seq.

[16] *Definition of Cybersecurity - Gaps and overlaps in standardisation*. [online]. [cit. 10/12/2017]. Available from: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity> p. 30

[17] The European Union Agency for Network and Information Security

[18] Hereinafter referred to as the **NIS Directive** or **NIS**. [online]. [cit. 01/07/2018]. Available from: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN>

1.2. Principles of cybersecurity

When applying cybersecurity, the following principles are instituted, which are also called the triads of cybersecurity.[\[1\]](#)

For the purposes of this monograph, the following three triads will be defined:

1. **CIA (C – Confidentiality; I – Integrity; A – Availability).**
2. **Elements of cybersecurity (People, Technology, Processes).**
3. **Cybersecurity life cycle (Prevention, Detection, Response).**

1.2.1 The CIA Triad

The best known and most widely used triad of cybersecurity is the **CIA** triad, but the simple use of this basic triad of cybersecurity principles without putting in place other principles is currently insufficient to maintain an adequate level of cybersecurity.

In the literature, for example, reference is made to the application of the **Parkerian hexad**[\[2\]](#), which is essentially the CIA triad, but supplemented by three other elements: **P/C – Possession/Control, A – Authenticity** and **U – Utility**.

The purpose of cybersecurity is to ensure both the security of ICT as such and, in particular, the data and information that are transmitted, processed and stored by these elements.

Very often, the CIA triad is primarily related to information.

This narrower concept results mainly from the very definition of **information security**, which focuses on information protection. Under this protection, the type of carrier (paper, electronic media, etc.) or information processing system is not an issue. Information security is then applied 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 – Code of practice for information security controls

The question is whether the definition of information security is currently adequate and sufficient, or whether it applies to all key elements of security in cyberspace.

Despite the fact that the term information security is more commonly used in professional literature and procedural rules, we are convinced that in relation to activities related to the use of ICT or to activities related to cyberspace, the term cybersecurity is a more appropriate term.

As mentioned above: *"information security refers to information as such"*. However, this omits key elements related to security in cyberspace.

We consider these important elements to be **data** and then the **computer systems** themselves (or individual elements of ICT), which enable the actual transmission of data and information.

There are a number of definitions of the terms data and information in the professional literature and in the legislation. For the purposes of this publication, definitions are selected that relate to the protection of information, data or cybersecurity.

According to the Convention on Cybercrime[\[3\]](#), **computer data** means *"any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function."*

Thus, data is any element with an information value that is processed by a computer system, and is processed to subsequently create information.

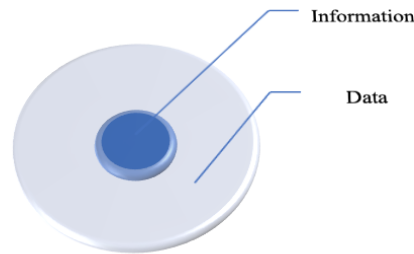
Information *"is data that has been processed into a form useful to a recipient. So every piece of information is a piece of data, but any stored data doesn't necessarily become information."*[\[4\]](#)

Wiener states that *"information is the name for the content of what is exchanged with the outside world as we adjust to it and make our adjustment felt upon it."* He also says that information is neither matter nor energy, but a separate physical category.[\[5\]](#)

Information is therefore perceived as something "more qualified" than data. Data are facts that become information when they are perceived or expressed in context and have a meaning that is understandable to people.[\[6\]](#)

It is the connection of "insignificant" data and the creation of a certain context, which only composes "significant" information from the data, which can be key from the point of view of cybersecurity. If we respect the above-mentioned thesis of information security, within which only information as such is protected, then there could be a significant security breach.

The following graph demonstrates the relationship between data and information. [7]



Data and information are transmitted within cyberspace using computer systems [8], which are an integral part of cyber- or information security.

Based on the above, we are convinced that the CIA [9] triad should be applied not only to the information itself, but also to other elements of cybersecurity (data, computer systems, etc.)

Confidentiality

Confidentiality means a situation where only such entities that are authorised to do so have access to information, data or ICT.

Given the large amount of processed information, it is appropriate to introduce or apply one of the classifications of information. These classifications can then be applied to other elements of cybersecurity and access to them.

ISO/IEC 27000 security standards define that:

- "Information should be classified according to its value, legal requirements, sensitivity and criticality."
- "Procedures in accordance with the classification scheme adopted by an organisation should be established and implemented for the marking and handling of information."
- "In order to prevent unauthorised access to or misuse of information, rules should be laid down for the handling and storage of information."

Examples of some classification schemes:

1. Classification of information according to Act 412/2005 Sb., on the Protection of Classified Information and on Security Clearance [10]:

- **Top secret** – unauthorised handling of information could cause extremely serious harm to the interests of the Czech Republic.
- **Secret** – unauthorised handling of information could cause substantial harm to the interests of the Czech Republic.
- **Confidential** – unauthorised handling of information could cause simple harm to the interests of the Czech Republic.
- **Restricted** – unauthorised handling of information could be disadvantageous to the interests of the Czech Republic.

2. Classification of information used in the commercial sphere:

- **Protected** – unauthorised handling of information could cause substantial damage or destruction of 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 a negative impact on the company (e.g. previously unpublished information about projects, planned events, etc.).
- **Public** – unauthorised handling of information should not harm anyone and should not have any impact on the company (e.g. publicly available contacts, project presentations, etc.). [11]





In addition to the two classifications mentioned above, there are a number of other classifications that are accepted by organisations or individuals, either on the basis of legislation or at the discretion of the user.

The classifications, provided they are respected and adhered to, can significantly mitigate the impact of a possible cyberattack.

3. Traffic Light Protocol

Within the cybersecurity community, there has been a need in the past to share sensitive information and data (typically about cyberattacks). For this reason, the **TLP (Traffic Light Protocol)** [12] was created in the National Infrastructure Security Coordination Center [13] in early 2000. This protocol aims to speed up the exchange of information between stakeholders and at the same time lays down rules for the handling of transmitted information. The entity that transmits information (the source of the information) always marks the information with a certain colour that determines how the recipient should handle the information.

The TLP protocol is best defined in the following table, which was taken from US-CERT [14]:

Colour	When to use	How to share?
TLP:RED  Not intended for publication, for participants only.	Entities may use TLP: RED in cases where the information does not allow for an effective response by other entities and could lead to implications for the privacy, reputation or operations of those entities if misused.	Recipients may not share information classified in the TLP: RED category with any entity other than the specific exchange, meeting or conversation in which the TLP:RED information was originally disclosed. For example, in a meeting, the TLP: RED information is limited to those who are directly attending the meeting. In most cases, information marked TLP: RED should only be exchanged verbally or in person.
TLP:AMBER  Limited disclosure. Disclosure is possible only in the organisation of participants.	Entities may use TLP: AMBER in cases where information requires an effective response from other entities and poses a risk to privacy, reputation or operations, if it is shared outside the participating organisations.	Recipients may share information classified in the TLP: AMBER category with members of their own organisation and with clients or customers who need to know this information in order to protect or prevent further potential harm. Entities are free to set additional sharing rules, and these must be followed.
TLP:GREEN  Limited disclosure, limited to the community.	Entities may use TLP: GREEN if the information is useful to raise awareness among all participating organisations. It is also possible to share this information with other entities within a wider community or sector.	Recipients may share information classified in the TLP: GREEN category with partners and partner organisations within their sector or community. However, information cannot be shared through publicly accessible channels. Information in this category can be massively disseminated within a given community. Information included in the TLP: GREEN category may not be released outside the community.
TLP:WHITE  Disclosure is not restricted in any way.	Entities may use TLP: WHITE if information contains little or no foreseeable risk of misuse in accordance with applicable disclosure rules and procedures.	In accordance with the rules and copyright protection, information included in the TLP: WHITE category may be distributed without restriction.

"In cybersecurity, unwanted disclosure of certain information is referred to as a breach of its confidentiality or leakage." [\[15\]](#)

4. Confidentiality assessment according to Decree No. 82/2018 Sb., on Security Measures, Cybersecurity Incidents, Reactive Measures, Requirements for Filing in the Field of Cybersecurity and Data Disposal (Decree on Cybersecurity) [\[16\]](#)

The Decree on Cybersecurity largely takes over the Traffic Light Protocol mentioned above for the confidentiality rating scale (see Appendix 1 to the DoCS).

Level	Description	Examples of asset protection requirements
Low	Assets are publicly available or were intended for disclosure. Breach of asset confidentiality does not jeopardise legitimate interests of an obligor. In the case of sharing such an asset with third parties and using the classification according to the Traffic Light Protocol (hereinafter the "TLP"), the TLP:WHITE designation is used.	No protection is required. Liquidation/deletion of the asset at the Low level – see Appendix No. 4.
Medium	Assets are not publicly available and constitute the know-how of an obligor; the protection of assets is not required by any piece of legislation or contractual arrangement. In the case of sharing such an asset with third parties and using the classification according to the TLP, the TLP:GREEN or TLP:AMBER designation is used in particular.	Access control tools are used to protect confidentiality. Liquidation/deletion of the asset at the Medium level – see Appendix No. 4.

High	Assets are not publicly available and their protection is required by legal regulations, other regulations or contractual arrangements (e.g. trade secrets, personal data). In the case of sharing such an asset with third parties and using the classification according to the TLP, the TLP:AMBER designation is used in particular.	Tools to ensure access control and recording are used to protect confidentiality. Transmissions of information over communication networks are protected by cryptographic means. Liquidation/deletion of the asset at the High level – see Appendix No. 4.
Critical	Assets are not publicly available and require an above-standard level of protection beyond the previous category (e.g. strategic trade secrets, special categories of personal data). In the case of sharing such an asset with third parties and using the classification according to the TLP, the TLP:RED or TLP:AMBER designation is used in particular.	Tools to ensure access control and recording are used to protect confidentiality. Furthermore, methods of protection preventing a misuse of assets by administrators. Transmissions of information are protected by cryptographic means. Liquidation/deletion of the asset at the Critical level – see Appendix No. 4.

Integrity

According to the Cybersecurity Glossary [\[17\]](#), **integrity** is defined as *"the property of accuracy and completeness."* **Data integrity** is then defined in the same glossary as *"certainty that data has not been altered. 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-healing codes, redundancy, journaling, etc. In cryptography and information security in general, integrity means data validity."* **System integrity** is then *"a property that the system performs its intended function in an undisturbed manner, without intentional or accidental non-automated manipulation with the system."*

Integrity therefore represents the impossibility of interfering with information, data, computer systems, their settings, etc. by a person other than the one authorised to do so.

At the same time, integrity is a kind of guarantee of the integrity of the system, information or data.

"Unwanted modification (alteration) is therefore referred to in information security as a breach of integrity." [\[18\]](#)

In the event of an integrity violation, be aware that if an unwanted change to the data occurs, the unwanted change may not be detected at all and a considerable amount of time may elapse before the integrity violation is detected.

The Decree on Cybersecurity in Appendix 1 also represents a scale for assessing integrity.

Level	Description	Examples of asset protection requirements
Low	Assets do not require protection in terms of integrity. Breach of asset integrity does not jeopardise the legitimate interests of an obligor.	No protection is required.
Medium	Assets may require protection in terms of integrity. A breach of the integrity of an asset may damage the legitimate interests of an obligor and may have less serious effects on the primary assets.	Standard tools (such as restrictions on write access rights) are used to protect integrity.
High	Assets require protection in terms of integrity. A breach of the integrity of an asset leads to damage to the legitimate interests of an obligor with significant effects on the primary assets.	To protect integrity, special means are used that allow to track the history of changes made and record the identity of the person making the change. Protection of the integrity of information transmitted by communication networks is ensured by cryptographic means.

Critical	Assets require protection in terms of integrity. A breach of integrity leads to very serious damage to the legitimate interests of an obligor with direct and very serious effects on the primary assets.	To protect integrity, special means are used to uniquely identify the person making the change (for example, using digital signature technology).
-----------------	---	---

Availability

According to the Cybersecurity Glossary [\[19\]](#), **availability** is defined as "a property of accessibility and usability at the request of an authorised entity."

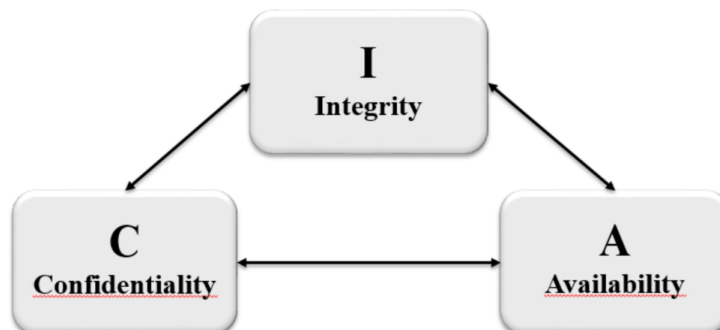
Availability can therefore be defined as a guarantee of access to information, data or a computer system at the moment of need. No matter how system ensuring integrity and allowing access to the system itself, data or information is, it will be unusable if it does not provide reliable access as needed. [\[20\]](#)

"The destruction of certain information is referred to in information security as a violation of its availability." [\[21\]](#)

The Decree on Cybersecurity in Appendix 1 also represents a scale for assessing availability.

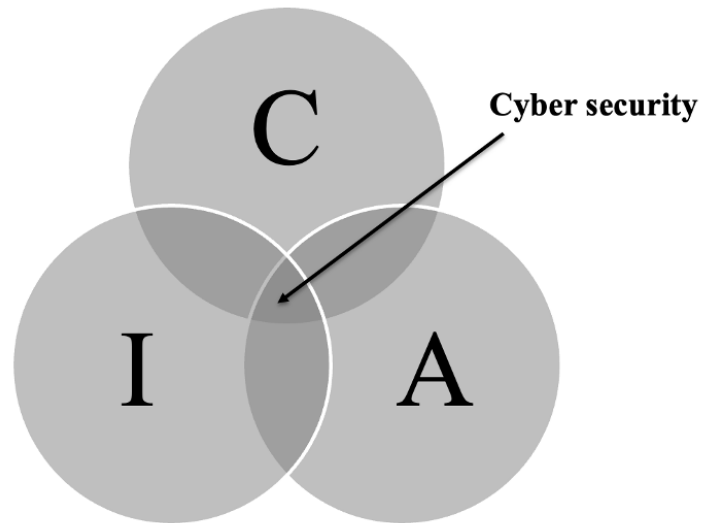
Level	Description	Examples of asset protection requirements
Low	Disruption of asset availability is not important and in the event of an outage, a longer period of correction is usually tolerated (approximately up to 1 week).	Regular backups are sufficient to protect availability.
Medium	Disruption of asset availability should not exceed a working day, a longer-term outage leads to a possible threat to the legitimate interests of an obligor.	Common backup and recovery methods are used to protect availability.
High	Disruption of asset availability should not exceed a period of several hours. Any failure must be addressed immediately as it leads to a direct threat to the legitimate interests of an obligor. Assets are considered to be very important.	Backup systems are used to protect availability, and the resumption of service provision may be conditional on operator intervention or the exchange of technical assets.
Critical	Disruption of asset availability is not permissible and even short-term unavailability (in the order of several minutes) leads to a serious threat to the legitimate interests of an obligor. Assets are considered to be critical.	Backup systems are used to protect availability, and the resumption of service provision is short-term and automated.

The CIA triad is often represented visually to better understand its individual attributes and relationships. For this reason, too, a typical depiction of the CIA triad is shown here. In the next part of this chapter, this triad is supplemented by certain elements (technology, people, processes).



The CIA Triad

If we tried to define the space of cybersecurity within the implementation of the CIA triad, then this space could be displayed as an intersection of individual principles of this triad.



CIA triad and cybersecurity



Parkenian hexad view[22]

1.2.2 Elements of cybersecurity

The following three elements, or their mutual interaction, make it possible to create or establish cybersecurity to a certain extent. These elements are:

- **people,**
- **technologies** and
- **processes.**

We believe that it is utopian to think that it is possible to create absolute cybersecurity or an absolutely secure system in which elements of ICT are used.

Theoretically, it would be possible to conceive of a completely isolated computer system (including a power supply, e.g. by means of an aggregate), enclosed in a Faraday cage, with a clearly defined group of people who are authorised to work on this computer system, ensuring no media (electronic or otherwise) is brought into or removed from this unique environment.

However, the question is what purpose a system secured in this way would serve and how the results of work on this system would be used, or how these results could be brought to life when it is not possible to bring the results of the activity. The counter-argument could then be the claim that the results will be delivered only at the end of the project, until then everything will be protected and access will be subject to the above-mentioned regime.

However, the question is whether such an artificially created and completely isolated system is protected against other threats, which may be the absence of backups, the possibility of physical destruction of the computer system, disclosure of partial information by people working with the system, etc.

Any system is as safe as its weakest link (element).

People

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

Bruce Schneier [\[23\]](#)

People interacting with cybersecurity can be seen as:

- **the author (creator) of this security** (i.e. typically persons who try to enforce and implement individual elements of cybersecurity, either in relation to themselves or in relation to the organisation),
- **recipients of cybersecurity rules** (i.e. persons who have decided or are forced to implement existing cybersecurity rules),
- **entities that need to be protected against cyberattacks,**
- **entities that need to be informed and trained on the rules and principles of cybersecurity,**
- **a risk or threat to the creation and maintenance of cybersecurity.**

If we focus on the role of people in building and maintaining cybersecurity, especially in connection with the AoCS, then it is necessary to define and staff the following positions in an appropriate manner:

- Cybersecurity Committee,
- Cybersecurity Manager,
- Cybersecurity Architect,
- Cybersecurity Auditor,
- Cybersecurity Team,
- Guarantor,
 - of primary assets,
 - of ancillary assets,
- Factual Administrator,
- Technical Administrator,
- Operator (sometimes also referred to as the supplier),
- Administrator,
- User.

People are a key element of any security. In the case of cybersecurity, their role is intensifying, and typically people are the weakest element and at the same time the most common target of attackers.

There are several reasons that lead us to this statement.

The first is the relatively short time we have actually been using computer systems. Most users started using one of the computer systems only after 1990. We started to connect to the Internet more on a large scale around 1995, and we have been using "smart" mobile phones since about 2007. A number of social network sites, which are currently considered a necessary part of life, without which we can't imagine our daily activities, haven't been used by us for more than 10 years.

The second reason lies in the enormous dynamics of the development of both hardware and especially software, which is inextricably linked to our interaction in the digital world. It is the dynamics of software development that do not allow many users to address in more detail the security issues that are inevitably associated with the use of software.

The third and last reason is the fact that life without information and communication technologies is now inconceivable or impossible for our society. ICT and applications associated with these technologies create digital avatars of ourselves, but with a much larger amount of information than we, as individuals, are able to remember or store. In addition to hardware and software vendors, attackers are aware of this fact, and it is for this reason that they are targeting people in cyberspace.

"Amateurs hack systems, professionals hack people."

Bruce Schneier [\[24\]](#)

In our opinion, it is essential that people who use ICT and choose to interact in cyberspace:

- **understand** at least the **basic principles and rules** relating to **cybersecurity,**
- **understand** at least the **basic functions of computer systems** (e.g. PC, laptop, mobile phone, smart TV, etc.) **that they use** for this interaction,
- **analyse the applications that they use** for this interaction and, if necessary, if the activity of these applications or their contractual conditions do not suit them, they did not use the applications,
- **educate themselves** in cybersecurity.

Therefore, in order to facilitate at least the last item from the above list, we decided to create this publication and summarise at least some of the findings that can be used by both lay users and IT professionals who have decided to pay increased attention to cybersecurity.

Technologies

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.“

Bruce Schneier [\[25\]](#)

Technologies are usually a means for users to connect to the Internet, social media, and other applications. It is a tool that uses various office packages when creating documents, sends e-mails, checks video, etc. The average user usually perceives and interacts with end technologies (PC, tablet, mobile phone, etc.), which they themselves use, while they are usually not interested in other the technological layers that are necessary for its operation in cyberspace.

For organisations, technologies represent a whole range of devices from technologies intended for users (desktop, mobile devices, etc.), through a complete network infrastructure (LAN, active elements, Wi-Fi elements, etc.) and services (servers, applications, etc.), to elements that serve to ensure security both on the perimeter (firewall [\[26\]](#), IDS/IPS [\[27\]](#), honeypot [\[28\]](#), etc.) and within the infrastructure (elements designed for authentication and authorisation, monitoring, analysis, etc.).

As part of building and maintaining cybersecurity, it is necessary to analyse existing assets and, on the basis of this analysis, possibly supplement or modify existing systems. Within technologies, the following elements should be an integral part of an ICT organisation, taking into account the specifics of that organisation:

- detection systems – Intrusion Detection System (**IDS**) / Intrusion Prevention System (**IPS**),
- central administration of users and roles,
- centralised management of information classification,
- protection against malicious code (application firewall, antivirus, antispam and other solutions),
- technology for recording the activities of individual elements of ICT, administrators and users (**log system**),
- active and offline backup systems; backups of vital servers, applications and databases (**recovery system**),
- network security management (VLAN, DMZ, firewall, etc.).

Technologies are usually the part of cybersecurity where we, as users or organisations, do not save money. We are willing to pay a large part of the funds for technology, either because we “need the latest phone” or because of a real and justified reason based on obsolescence and further non-support (updating) of the computer system.

Therefore, in order to ensure cybersecurity, it is necessary to keep technologies in such a state that they are able to respond to the changes associated with the development of ICT. In particular, technologies (both hardware and software) should be kept up to date and secure.

Although technologies are certainly an important part of the process of creating and maintaining cybersecurity, they are, in our opinion, the least important part. Much more important elements of cybersecurity are appropriately set up processes and people who can apply or modify the given processes in practice and follow pre-agreed rules.

Processes

*„The mantra of any good security engineer is: **Security is a not a product, but a process.**‘ It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.“*

Bruce Schneier [\[29\]](#)

Processes are activities that need to be done in order for people and technologies to be able to use them.

In terms of the passage of time, it is possible to monitor the processes of:

- asset and risk management,
 - definition and categorisation of assets,
 - risk analysis and categorisation,
- implementation of ICT and applications,
- user and role management,
- authorisation and authentication,
- maintenance (updating) of systems and services,
- security testing of individual computer systems and services,
- analysis of corrective measures,
- implementation of corrective measures,
- cybersecurity audit,
- detection of anomalies or cyberattacks,
- response to cyberattacks or other incidents,
- processes to ensure continuity,
- training and exercises, etc.

The above list of individual processes associated with the creation and maintenance of cybersecurity is certainly not exhaustive, and the outlined processes can be granularised. Individual processes are implemented within the entire life cycle of ICT, information, data and in relation to users. [30]

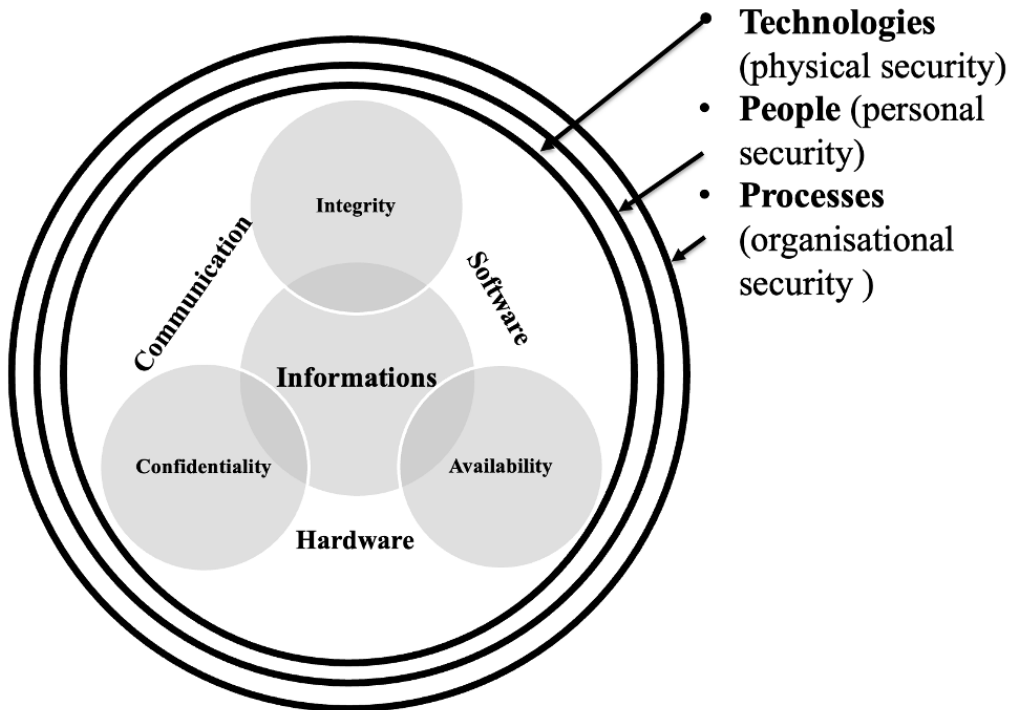
The actual setting of processes, their constant maintenance or modification is the most demanding part of building cybersecurity. At the same time, this activity places the highest demands on the administrators of individual systems.

If the organisation decides to implement the rules of cybersecurity, then it is of course appropriate to keep the hardware and software up to date, follow the rules that are set for access to individual systems, etc.

If possible, it is advisable to perform simulations of typical cyberattacks in the organisation (e.g. phishing, business e-mail compromise, etc.) in order to realistically demonstrate these attacks and possible impacts if a person falls victim to such attacks.

Penetration testing also allows you to find errors in already set processes.

However, when creating and setting cybersecurity rules, the organisation should primarily focus on human resources and their education.

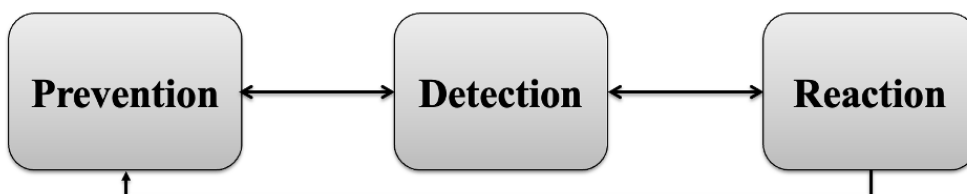


CIA triad supplemented by technologies, people and processes [31]

1.2.3 Cybersecurity life cycle

From the point of view of the passage of time, it is necessary to apply or modify both the CIA triad and partial elements of cybersecurity during the entire life cycle in the implementation of cybersecurity. In particular, it is about prevention, detection and reaction to the attack. [32]

Very often, the cybersecurity life cycle is represented by various diagrams. For clarity, I present some of them.



Simplified representation of the cybersecurity life cycle



Kybernetická bezpečnost životní cyklus

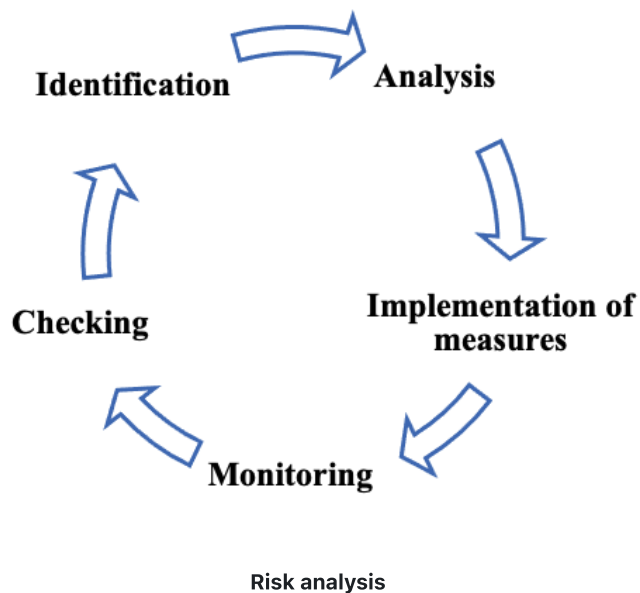
Cybersecurity life cycle according to kybez.cz [33].

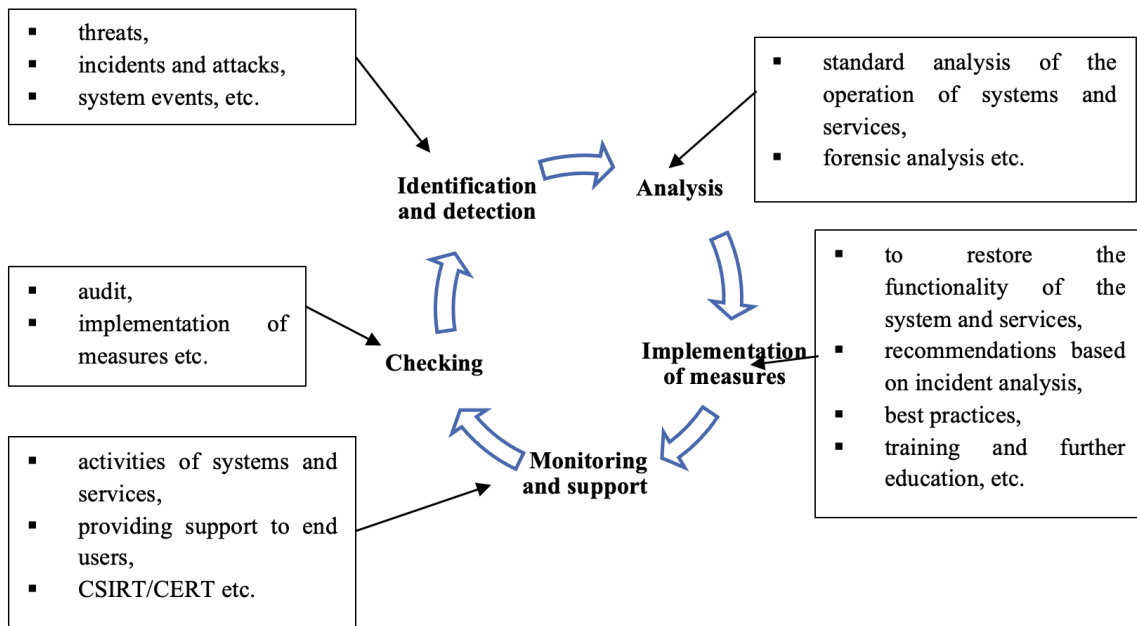
Text on the figure: **Cybersecurity** – life cycle

ADMINISTRATION – AUDIT – RISKS – MEASURES – IMPLEMENTATION

When dealing with cybersecurity, there is no “point of reference” within which it could be said: “*We made it! We are protected against cyberattacks or threats. We are cybernetically secure.*”

Building and maintaining cybersecurity can be compared to a never-ending risk analysis, but this routine analysis needs to be complemented by other support processes that can help increase cybersecurity in the organisation.





Cybersecurity life cycle

The actual depiction of the cybersecurity life cycle can be much more complex. [34]



Example of cybersecurity solution

Evolution of cybersecurity

At the end of this subchapter, it would be possible to ask a simple question: "Why should I (as an individual) or an organisation deal with cybersecurity at all?"

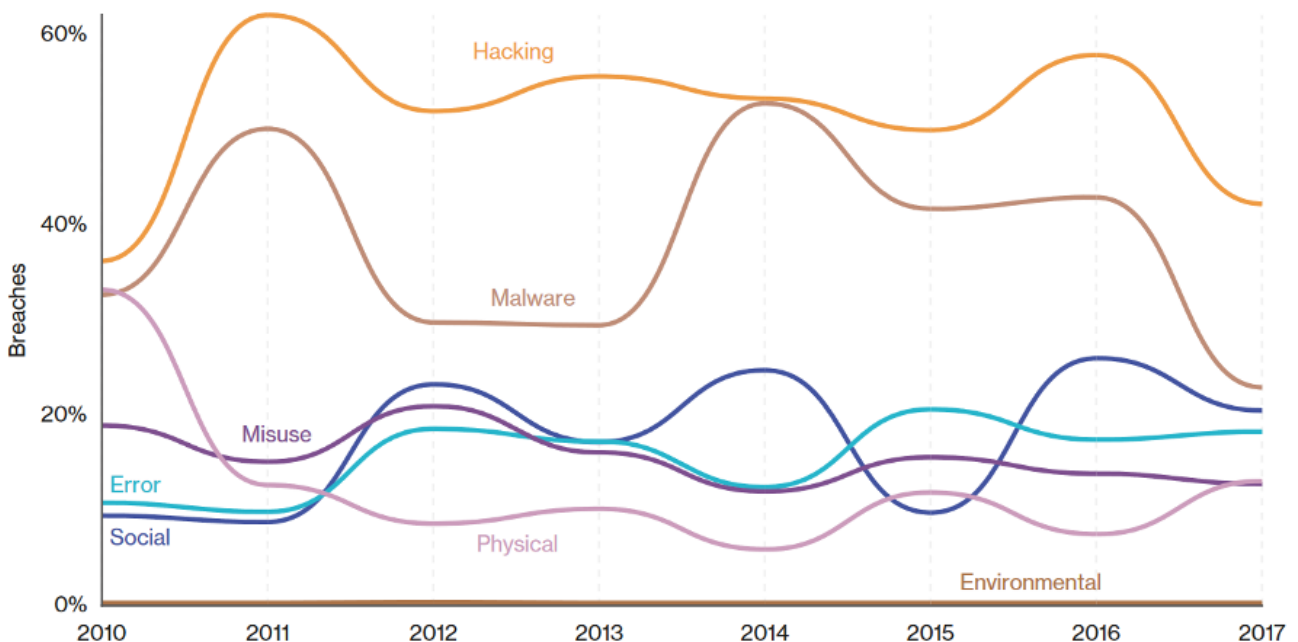
The answer will not be so complicated, although it will be necessary to dispel the often ingrained myth that someone else, whether large organisations such as Microsoft, Google, Apple or providers of cloud services, connectivity, etc., is already addressing the issue of cybersecurity for me.

It is true that these organisations have introduced and applied sub-elements of cybersecurity, but cybersecurity, like any other security, always begins and ends with a specific person or organisation that wants to secure itself, always with regard to the specifics of that person or organisation.

The following facts emerge from the Data Breach Investigations Report [\[35\]](#) for 2017, which deals with security breaches leading to data compromise:

- the attacker was
 - a person outside the organisation – 73%
 - a person within the organisation – 28%
 - an organised crime group – 50%
- a method of the attacks was:
 - hacking – 48%
 - malware – 30%
 - o 49% of the malware was distributed by an attacker and subsequently installed via e-mail
 - social engineering – 43%
 - physical attack – 8% [\[36\]](#)
- victims are organisations operating in:
 - healthcare – 24%
 - public sector (typically state administration and self-government, etc.) – 14%
- motive of attack:
 - enrichment – 76%
 - gain of data and information (espionage) – 13%
- 68% of attacks were detected only after several months or after a longer period

The following graph presents the development of individual attacks from 2010 to the end of 2017.



Types of attacks used to compromise security [\[37\]](#).

According to a report by the National Cyber and Information Security Agency, [\[38\]](#), "a further increase in cyberthreats can be expected in 2018, especially further next-generation phishing attacks, attacks on markets, wallets and cryptocurrency exchanges, file-free variants of ransomware, use of artificial intelligence for cyberattacks, data attacks in Cloud solutions, attacks on the Internet of Things, industrial systems, etc. The share of state or state-supported actors in cyberattacks is expected to increase, and massive leaks of personal data, passwords and access data will continue. That is why it is necessary to build the cybersecurity of information and communication systems important for the operation of the state and its critical infrastructure." [\[39\]](#)

The area of cybersecurity will be one of the most important areas in the future as it can be assumed that the use of ICT and services related to these technologies will not be reduced. Cybersecurity is intended to help identify gaps in the setup of these systems and services.

"Cybersecurity also helps identify, assess and address threats in cyberspace, reduce cyber risks and eliminate the impact of cyberattacks, information crime, cyberterrorism and cyber espionage by strengthening the confidentiality, integrity and availability of data, systems and other information and communication infrastructure elements.

The main purpose of cybersecurity is the protection of the environment to enforce human information rights." [40]

[1] See e.g. HSU, D. Frank and D. MARINUCCI (eds.). *Advances in cybersecurity: technology, operations, and experiences*. New York: Fordham University Press, 2013. 272 p. ISBN 978-0-8232-4456-0. p. 41.

KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti*. [online]. [cit. 21/07/2018]. Available from: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf

[2] For more details, see e.g. *Parkerian Hexad*. [online]. [cit. 20/08/2016]. Available from: <https://vpuhuseeri.wordpress.com/2009/08/16/149/>

[3] Article 1 (b) of the Convention on Cybercrime. *Convention on Cybercrime*. [online]. [cit. 20/08/2016]. Available from: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0>

[4] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, p. 25

[5] For more details, see WIENER, Norbert. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích*. Prague: Státní nakladatelství technické literatury, 1960. 148 p., p. 32 et seq.

[6] ŠÁMAL, Pavel et al. *Trestní zákoník II. § 140 až 421. Komentář*. 2. Publ. Prague: C. H. Beck, 2012, p. 2308

[7] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, p. 25

[8] For more details see: KOLOUCH, Jan. *CyberCrime*. Prague: CZ.NIC, 2016, p. 57 et seq.

[9] For more details, see e.g. 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]. [cit. 10/12/2017]. Available from: <https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf>

ANDRESS, Jason. *The Basics of Information Security*. 2nd Edition. Syngress. ISBN: 9780128007440

HENDERSON, Anthony. *The CIA Triad: Confidentiality, Integrity, availability*. [online]. [cit. 13/01/2018]. Available from: <http://panmore.com/the-cia-triad-confidentiality-integrity-availability>

[10] For more details, see <https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/>

[11] See also: ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. p. 20 et seq.

[12] Currently the Center for Protection of National Infrastructure – CPNI

[13] For more details, see e.g. *Traffic Light Protocol (TLP) Definitions and Usage*. [online]. [cit. 13/01/2018]. Available from: <https://www.us-cert.gov/tlp>

[14] *Traffic Light Protocol (TLP) Definitions and Usage*. [online]. [cit. 13/01/2018]. Available from: <https://www.us-cert.gov/tlp>

[15] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. p. 19

[16] Hereinafter referred to as the Decree on Cybersecurity or **DoCS**.

[17] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 58. [online]. [cit. 10/07/2018]. Available from: http://afcea.cz/wp-content/uploads/2015/03/Slovník_v303.pdf

[18] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. p. 22

[19] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 43. [online]. [cit. 10/07/2018]. Available from: http://afcea.cz/wp-content/uploads/2015/03/Slovník_v303.pdf

- [20] See e.g. 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]. [cit. 10/12/2017]. Available from: <https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf>
- [21] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. p. 24
- [22] *The Parkerian Hexad*. [online]. [cit. 20/08/2016]. Available from: <http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf>
- [23] SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570039>
- [24] SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570035>
- [25] SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570040>
- [26] A firewall is a system containing rules that govern data flows within network technologies.
- [27] **IPS** (Intrusion Prevention System), a device that monitors unwanted (malicious) network activity and/or computer system activity. Hereinafter referred to as the **IPS**.
- IDS** (Intrusion Detection System) is a system designed to detect unusual activities that can potentially lead to breaches of security of computer networks, computer systems, applications, etc. Hereinafter referred to as the **IDS**.
- [28] A honeypot is a system the purpose of which is to detect malware or other unwanted activities, which are then analysed in this artificial environment.
- [29] SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570047>
- [30] The term "user" is used here to express a natural person who is authorised to use elements of ICT, individual systems and applications. From this point of view, the user means both a person with administrator rights and an end user.
- [31] The graph was based on the graph published in: *CIA triad methodology*. [online]. [cit. 10/07/2018]. Available from: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png
- [32] For more details, see SVOBODA, Ivan. *Řešení kybernetické bezpečnosti*. Přednáška v rámci CRIF Academy. (23/ 09/2014)
- [33] *Základní pojmy*. [online]. [cit. 10/07/2018]. Available from: <https://www.kybez.cz/bezpecnost/pojmoslovi>
- [34] *The complete breadth of CGI Cyber Security services*. [online]. [cit. 10/07/2018]. Available from: <https://mss.cgi.com/service-portfolio>
- [35] *2018 Data Breach Investigation Report. 11th Edition*. [online]. [cit. 28/07/2018]. Available from: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf
- [36] Techniques and tools are usually combined as a part of individual attacks.
- [37] *2018 Data Breach Investigation Report. 11th Edition*. [online]. [cit. 28/07/2018]. Available from: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf p. 7
- [38] *Národní úřad pro kybernetickou a informační bezpečnost*. Hereinafter referred to as the **NUKIB**
- [39] *Zpráva o stavu kybernetické bezpečnosti za rok 2017*. [online]. [cit. 29/06/2018]. Available from: <https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf>
- [40] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. [online]. [cit. 01/07/2018]. Available from: <https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf>

1.3. Risk, asset, vulnerability

1.3.1 Risk

Before defining the terms of threat, event, incident and attack, we consider it necessary to define at least a general definition of the term "risk", which is directly related to the subsequently defined terms.

The Cybersecurity Glossary defines risk as: "(1) *Danger, possibility of damage, loss, failure.* (2) *The effect of uncertainty on the achievement of objectives.* (3) *The possibility that a particular threat exploits the vulnerability of an asset or group of assets and causes damage to the organisation.*" [\[1\]](#).

Risk can also be defined as **the potential for a threat to become real and exploit an asset's vulnerability**. According to Article 4 (9) of the NIS, a **risk** is **"any reasonably identifiable circumstance or event that could have a negative impact on the security of networks and information systems"**. In cyberspace, users, as well as computer systems and applications are at risk, as well as other elements of ICT.

The term **"risk"** expresses the probability with which an unwanted event can occur. The degree of probability that this event will occur is expressed through risk analysis. Minimum standard values for methods of identification, analysis, evaluation and treatment of risks are defined in ČSN EN 31010.

Valášek et al [\[2\]](#) state that the risk assessment is usually based on three basic issues:

- **What can go wrong (be unwanted)? What can fail?**
- **What is the possibility/probability that this will happen?**
- **How serious (intensity, size, etc.) can the effects (impacts, consequences) be?**

According to Valášek, however, these questions represent only a basic framework that is able to define its own risk. In addition to these three questions, the following supplementary questions are asked, which relate to significant factors influencing the risk characterisation:

Factor	Question
Time	"How long will we be exposed to risk (threat)?"
Instability	"How close are the estimates of the impacts of a risk event to reality?"
Complexity	"Is it difficult to understand risk?"
Mutual relationships	"How far are the different risks or risk factors related?"
Influence	"Is it possible to manage risk?"
Life cycle	"How does risk change over time?"
Cost effectiveness	"How costly are measures in relation to risk?"

For each risk, the degree of significance of the risk is calculated, which can be expressed as follows:

Significance of risk = **Impacts** of risk * **Probability** of risk occurrence

"The result of the risk analysis is to determine the significance of the defined risks. Each risk, with respect to the assigned task, has different impacts that it can cause. We evaluate the impacts of risk or consequences on a five-point scale, for example, as follows:"

Points	Probability of risk occurrence	Occurrence description
5	SURE	Risk occurs almost always or with a probability of 90–100%.
4	LIKELY	The risk is likely to occur
3	POSSIBLE	Risk may sometimes occur (e.g. under specific conditions).
2	UNLIKELY	Risk may sometimes occur, but it is unlikely.
1	Impossible	Risk occurs only in exceptional cases and under specific conditions.

In addition to the impact, individual risks may or may not occur. Therefore, the probability of risk occurrence is determined. Occurrence is again evaluated on a five-point scale as follows: [\[3\]](#).

Points	Impact of risk	Description of impact
5	CRISIS	The situation will fundamentally reduce or terminate the company's operations (e.g. bankruptcy, loss of life, etc.).
4	SIGNIFICANT	The situation very dangerously affects the internal and external operation of the company (e.g. the occurrence of significant financial losses – 100% over budget, time, the emergence of litigation, injuries, etc.).
3	MEDIUM	The situation will dangerously affect the internal and external operation of the company (e.g. losses will occur, but the company is able to continue to operate, financial losses will occur up to 30% of the budget, etc.).
2	INSIGNIFICANT	The situation limits the internal operation of the company (e.g. there will be time delays of up to 30 days).
1	NEGLIGIBLE	Although the situation negatively limits the operation of the company, it does not cause losses greater than 5%.

In addition to the above, other circumstances must be taken into account in the risk assessment, which are:

§ the very nature (type) of the risk or threat,

§ asset vulnerability,

§ probability that the risk will turn into a security event or incident.

Risk analysis is very difficult and requires knowledge of assets, threats and, in particular, some experience in this area is needed. Based on the risk analysis, measures can be identified to minimise or eliminate the risks.

1.3.2 Asset

An asset is anything that has a certain value for a person, organisation or state.

An asset can be a **tangible object** (building, computer system, networks, energy, goods, etc.) or an **intangible one** (information, knowledge, data, programs, etc.) from the point of view of civil law.

However, an asset can also be a **quality** (e.g. availability and functionality of the system and data, etc.) or a **good name**, reputation, etc. **People** (users, administrators, etc.) and their knowledge and experience are also an asset from the point of view of cybersecurity.

According to Section 2 (f) and (g) of the DoCS, **assets** are divided into **ancillary** and **primary**.

An **ancillary asset** is a technical asset, employees and suppliers involved in the operation, development, administration or security of the information and communication system.

A **primary asset** is information or a service processed or provided by an information and communication system.

1.3.3 Vulnerability

Vulnerability refers to the weakness of an asset, software, security, which is exploited by one or more threats.

Vulnerability, as well as a threat, can be caused by a number of factors grounded in human behaviour, technical failure, and possibly force majeure.

In the field of cybersecurity, vulnerabilities are divided into:

- **known vulnerabilities** (published)
 - **fixed** (treated) – a typical case are software vulnerabilities for which the manufacturer has already issued an update
 - **unfixed** (untreated) – an affected entity (manufacturer, administrator, etc.) knows about the vulnerability, but did not ensure its correction
- **unknown vulnerabilities**
 - hidden
 - undiscovered

In the case of unknown vulnerabilities, it is important whether they are discovered by an attacker, a manufacturer, a security analyst, a penetration tester, or a user. Equally important is the motivation of the person who discovers the vulnerability.

Security vulnerabilities are potential security threats. Security vulnerabilities can be eliminated to some extent by consistently updating and patching all software..[4].

The Decree on Cybersecurity in Appendix 3 lists some of the vulnerabilities as an example. **According to this decree, the vulnerability is:**

1. insufficient maintenance of the information and communication system,
2. obsolescence of the information and communication system,
3. insufficient protection of the outer perimeter,
4. insufficient security awareness of users and administrators,
5. inappropriate setting of access rights,
6. insufficient procedures for identifying and detecting negative security phenomena, cybersecurity events and cybersecurity incidents,
7. insufficient monitoring of the activities of users and administrators and inability to detect their inappropriate or defective behaviour,
8. insufficient setting of security rules, inaccurate or ambiguous definition of rights and obligations of users, administrators and security roles,
9. insufficient protection of assets,
10. inappropriate security architecture,
11. insufficient degree of independent control,
12. inability to detect errors in a timely manner by employees.

[1] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 99. Available from: <https://nukib.cz/download/aktuality/container-nodeid-665/slovník-kb-cz-en-1505.pdf>

[2] VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Krizové řízení při nevojenských krizových situacích*. Prague: Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 01/07/2018]. Available from: <http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx>

ISBN 978-80-86640-93-8 p. 73

[3] *Analýza rizik*. [online]. [cit. 01/07/2018]. Available from: <https://www.vlastnicesta.cz/metody/analýza-rizik-risk/>

[4] Cf. JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 29. Available from: <https://nukib.cz/download/aktuality/container-nodeid-665/slovník-kb-cz-en-1505.pdf>

1.4. Cyber threats, events, incidents and attacks

Dealing with the issue of “negative cyber phenomena” can be somewhat problematic as different scientific literature as well as procedural rules often use different synonyms, which should mean the same thing, to define the specific negative phenomenon.

The reason for the persistence of terminology is, on the one hand, the relatively short time we have been dealing with cyber threats, attacks and incidents, and, on the other hand, the not always identical translation from English, which is used primarily in IT.

1.4.1 Cyberthreat

A threat can most simply be defined as something that is able to disrupt the normal or orderly state of affairs and interfere with the rights of other entities. This is a negative effect that may or may not be brought to completion. It is sufficient for the definition itself that the possibility of a negative state threatens and is real.

According to the Ministry of the Interior of the Czech Republic, *“any phenomenon that has the potential to harm the interests and values protected by the state is considered a threat. The severity of a threat is determined by the magnitude of the possible damage and the time scale (usually expressed in probability or risk) of the possible application of that threat.”*^[1]

The Cybersecurity Glossary defines several terms that are directly related to cyber threats.

Threat is defined as *“the potential cause of an unwanted incident that could result in damage to a system or organisation.”*^[2]

Directly related to this basic concept is the concept of **information security threat**^[3], which is defined as *“a potential cause of an adverse event that may result in damage to the system and its assets, such as destruction, unwanted disclosure (compromise), data modification or unavailability of services.”*^[4]

In addition to the two above-mentioned terms, the authors also define **active threat**, **passive threat** and **advanced** and **permanent** threat in the glossary.^[5]

The Oxford dictionary states that a **cyberthreat is the possibility of a malicious attempt to damage or disrupt a computer network or system.**^[6] In this context, a computer system is considered to be a system.

Cyberthreat can also be defined as an act aimed at changing^[7] information, applications or the system itself.

Jirovský defines four groups of basic threats and at the same time characterises their relationship:^[8]

1. **Leakage of information** is a condition where protected information is leaked to an unauthorised entity.
2. **Integrity violation** represents damage, change or deletion of data.
3. **Suppression of a service** means intentionally obstructing access to information, applications, or the system.^[9]
4. **Unauthorised use** is the use of information by an unauthorised entity or in an unauthorised manner.^[10]

Classification of cyberthreats

There are a number of classifications of cyberthreats, and most often these threats are divided according to:

1. Source of threat

a) **Man-made threats.** In the event that a threat is caused by a person, it is appropriate to focus on the form of fault that led to the initiation of the threat. From this point of view, it is possible to distinguish threats caused:

· **intentionally,**

Intentionally caused cyberthreats include, for example:

- o intentional data deletion, system configuration, etc.,
- o physical damage to a computer system or other element of ICT,
- o data and information theft,
- o cyberattacks (malware, DoS, DDoS, phishing, unauthorised eavesdropping, etc.).^[11]

· **through negligence.**

Cyberthreats caused by negligence include, for example:

- o accidentally deleted data,

- o physical damage to a computer system or other element of ICT (e.g. by falling, tripping over structured cabling, etc.),
 - o damage of data, systems or other elements due to failure to become familiar with internal acts (legal or technical),
 - o other user error.
- b) **Technical errors** (e.g. software or hardware error).
- c) **Force majeure.**

Cyberthreats caused by force majeure include, for example:

- unplanned power failure (unless it is a man-made threat from negligence),
- natural events (lightning strikes, storms, etc.) or disasters (floods, earthquakes, etc.),
- fire (unless it is a man-made threat).

2. Source of action

- a) **internal threats** (the source of the threat is located within the organisation)
- b) **external threats** (the source of the threat is outside the organisation)[\[12\]](#).

3. Target of threat

a) Attack on the CIA triad.

- **Confidentiality** – e.g. theft of data, access data and keys, hardware, 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 any of the elements of cybersecurity.

- **People** – attacks by social engineering (in the real world, but also cyberspace), phishing, malware, theft, etc.
- **Technologies** – all threats listed in point 1 of this classification. Typically, threats can affect:
 - o hardware (endpoint computer systems, servers, network controllers, IoT, etc.),
 - o databases,
 - o network and network infrastructure,
 - o software (operating system or other applications),
 - o information and data stored in computer systems.
- **Processes** – unauthorised testing of security or functionality of processes set up in the organisation, etc.

4. Motivation

If a threat is caused by intentional human behaviour, it is appropriate to deal with its motivation when addressing the threat. Based on the analysis of the motivation for such behaviour, it is possible to create corrective measures within the threat response process so that there is no incentive for this motivation in the future.

Based on motivation, you can monitor:

- threats in order to obtain financial gain,
- threats in order to gain a competitive advantage,
- threats in order to demonstrate somebody's capabilities,
- threats for retaliation,
- threats due to non-fulfilment of obligations.[\[13\]](#)

5. Type of threat

- social engineering,
- botnet,
- malware,
- ransomware,
- spam/scam,

- fraudulent offers,
- phishing, pharming, spear phishing, vishing, smishing,
- hacking,
- sniffing,
- DoS, DDoS, DRDoS attacks,
- distribution of defective content,
- identity theft,
- APT (Advanced Persistent Threat),
- cyberterrorism,
- cyber extortion.

The Decree on Cybersecurity in Appendix 3 lists some of the threats as an example. **According to this decree, a threat is:**

1. a breach of security policy, execution of unauthorised activities, misuse of permissions by users and administrators,
2. damage or failure of hardware or software,
3. identity fraud,
4. use of software in violation of the license conditions,
5. malicious code (such as viruses, spyware, Trojans),
6. violation of physical security,
7. interruption of the provision of electronic communications services or electricity supply,
8. misuse or unauthorised modification of data,
9. loss, theft or damage to an asset,
10. non-compliance with the contractual obligation by a supplier,
11. a fault for reasons attributable to employees,
12. misuse of internal means, sabotage,
13. long-term interruption in the provision of electronic communications services, electricity supply or other important services,
14. shortage of employees with a required professional level,
15. targeted cyberattack using social engineering, use of espionage techniques,
16. misuse of removable electronic data carriers,
17. attack on electronic communication (eavesdropping, modification).

1.4.2 Cybersecurity event

Prošise and Mandiva characterise "**computer security event**" (which can be understood as a computer attack or computer crime), as an illegal, unauthorised, unacceptable action that involves a computer system or computer network. Such an action may focus, for example, on the theft of personal data, spam or other harassment, embezzlement, dissemination or possession of child pornography, etc.^[14]

Jirásek et al. define a security event as: "**an event that may cause or lead to a breach of information systems and technologies and the rules defined for its protection (security policy).**"^[15]

The definition of a security event can also be found in Article 3.5 of ISO/IEC 27001, 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 another situation that previously has not happened that may be important from an information security perspective."

A similar definition can be found in NIST, 800-61 Computer Security Incident Handling Guide, which states that a security event is: "*an unfavourable event with a negative effect, such as system crashes, packet flooding, unauthorised use of system privileges, unauthorised access to sensitive data or execution of malicious code that destroys data.*"^[16]

A cybersecurity event is also defined by the Act on Cybersecurity in Section 7 (1) as "**an event that may cause a breach of information security in information systems or a breach of security of services or security and integrity of electronic communications networks.**"

In fact, **it is an event without a real negative consequence** for a given communication or information system. In essence it is only a threat, but it must be real.

At the same time, the authors use tautologies by explaining an event as an event.

We believe that it would be more appropriate and probably more comprehensible to label and interpret the term "cybersecurity incident" as a **cyberthreat**, because there really is only a potential cause that can cause an adverse event.

Example: *An e-mail message containing malicious code (malware) is delivered to a user's internal company mail. However, this malware is compressed (e.g. using WinZip) and cannot be installed without further user action. Such an event does not necessarily mean a breach of security in itself, but it is in certain circumstances capable of breaching it.*

1.4.3 Cyber (security) incident

Jirásek et al. define a security incident as *"a breach or imminent threat of a breach of security policies, security principles, or standard security rules for the operation of information and communication technology."*^[17]

The ISO/IEC 27001 standard provides its own definition of an **information security incident**. In Article 3.6 of this standard, an information security incident is defined as: *"one or more unwanted or unexpected security events in which there is a high probability of compromising an organisation and compromising information security."*

A very similar definition of a **computer security incident** can also be found in the NIST manual, 800-61 Computer Security Incident Handling Guide, which states that it is *"a violation or imminent threat of violating security policies, acceptable use policies (system, service) or standard security practice."*^[18]

A cybersecurity incident is also defined in Section 7 (2) of the Act on Cybersecurity as *"a breach in the security of information in information systems or a breach in the security of service provision or a breach of security and integrity of electronic communication networks due to a cybersecurity event."*

It follows from the wording of the act that an incident can be caused by both intentional and negligent actions of a person but also by force majeure. It is essential that **the security of information, or services and information and communication systems associated with them, is compromised.**

A cybersecurity incident thus represents a real breach of information security in information systems or a breach of the security of services or the security and integrity of electronic communication networks, i.e. a breach of an information or communication system with a negative impact.

Accidents, hardware and software errors, errors made by administrators during configuration, errors of system users, etc. are also responsible for a certain part of cybersecurity incidents.

Example: *If we build on the previous example, then when the user runs malicious code on the computer, we are already referring to the occurrence of a security incident.*

1.4.4 Cyberattack

Jirásek et al. define a cyberattack as: *"An attack on an 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."*^[19]

Such a definition of a cyberattack would significantly narrow and not affect all the negative activities of cyberspace users^[20], especially because it cumulatively combines the conditions for IT damage and information retrieval. A cyberattack can also include actions in the form of social engineering, where the only goal is to obtain information, or, conversely, a DoS or DDoS attack, where the only goal may be to suppress (i.e. not damage) the functionality of one or more computer systems or services.

The difference between a cybersecurity incident and a cyberattack lies primarily in the question of fault. As mentioned earlier, a cybersecurity incident can be caused by both intentional and negligent human behaviour, or force majeure. However, a cyberattack is an intentional act by a person.

Based on the above, a **cyberattack**^[21] can therefore be defined as **any intentional conduct by an attacker in cyberspace that is directed against the interests of another person.**

A cyberattack can also be defined as the actions of an attacker or group of attackers that use information and communication technology to attack another information and communication infrastructure, whether to compromise the availability, confidentiality, or integrity of data.

1.4.5 Cybercrime

At the end of the discussion of cyber incidents and attacks, we consider it necessary to define, at least in general terms, the relationship between these attacks or incidents and cybercrime.

When defining the content of the concept of **cybercrime**, it is necessary to realise that along with the growth of the possibilities of using information and communication tools, the possibility of their use (abuse) to commit crime is also growing. Therefore, there is virtually no universal, generally accepted definition that would fully affect the scope and depth of this concept.

Most generally, cybercrime can be defined as **conduct directed against a computer system, computer network, data or users, or conduct in which a computer system is used as a tool to commit a crime.** An indispensable criterion for the application of the definition of cybercrime is the fact that the computer network, or cyberspace, is then the environment in which this activity takes place.

Cybercrime represents the broadest set for all crimes that occur in the information and communication technology environment. "Classic crime" is very often transferred to cyberspace, as it is possible to commit crime faster and more effectively there (e.g. fraud, dissemination of child abuse material, etc.). In addition to this transfer of familiar crime, there are new attacks so far often not covered by law.

It should be noted that not every cyberattack must be a crime, but every cybercrime must be a cyberattack at the same time. Many cyberattacks, even due to the absence of a criminal law standard, can be subsumed under conduct that will have the nature of an administrative or civil tort, or it may not be conduct that is punishable by any legal standard (it can be, for example, only an immoral or intolerable conduct).

[1] *Hrozba*. [online]. [cit. 28/07/2018]. Available from: <http://www.mvcr.cz/clanek/hrozba.aspx>

[2] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 52. Available from: <https://nukib.cz/download/aktuality/container-nodeid-665/slovníkcz-cz-en-1505.pdf>

[3] In this case, there is 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, then the correct Czech equivalent is, for example, "hrozba pro bezpečnost informací; hrozba zabezpečení informací" etc.

[4] *Ibidem*, p. 25.

[5] *Ibidem*, p. 16, 81 a 87

[6] *Cyberthreat*. [online]. [cit. 06/07/2018]. Available from: <https://en.oxforddictionaries.com/definition/cyberthreat>

[7] The change also means the theft of information, its destruction, or frustrating its use.

[8] Cf. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Prague: Grada Publishing, a. s., 2007. p. 21 et seq.

[9] These attacks are, for example, **DoS – Denial of Service**, **DDoS – Distributed Denial of Service**, etc. For more details, see KOLOUCH, Jan. *CyberCrime*. Prague: CZ.NIC, 2016, p. 295 et seq.

[10] For example, a charged system will be attacked and its services used without payment for services.

[11] For individual cyberattacks, see for example: KOLOUCH, Jan. *CyberCrime*. Prague: CZ.NIC, 2016, p. 181 et seq.

[12] For more details, see e.g. POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace*. [online]. [cit. 06/07/2018]. Available from: <https://www.cybersecurity.cz/data/pozar2.pdf>

[13] Před čím chránit? – Bezpečnostní hrozby, události, incidenty. [online]. [cit. 06/07/2018]. Available from: <https://www.kybez.cz/bezpecnost/pred-cim-chranit>

[14] PROSISE, Chris and Kevin MANDIVA. *Incident response & computer forensic, second edition*. Emeryville: McGraw-Hill, 2003, p. 13

See also: CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition*. London: Academic Press, 2004, p. 9 et seq.

[15] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 28. Available from: <https://nukib.cz/download/aktuality/container-nodeid-665/slovníkcz-cz-en-1505.pdf>

[16] *Computer Security Incident Handling Guide* [online]. [cit. 13/08/2018], p. 6. Available from: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

[17] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 25. Available from: <https://nukib.cz/download/aktuality/container-nodeid-665/slovníkcz-cz-en-1505.pdf>

[18] *Computer Security Incident Handling Guide* [online]. [cit. 17/02/2018], p. 6. Available from: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

[19] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015. p. 71. Available from: <https://nukib.cz/download/aktuality/container-nodeid-665/slovníkcz-cz-en-1505.pdf>

[20] The above definition especially lacks a definition of any motivation of the attacker other than that... *causing damage or gain to strategically important information*. An example not covered by this definition can be economically motivated attacks, which are dramatically growing at present.

[21] It is necessary to distinguish the concept of cyberattack from the concept of security incident, which represents a breach of IS/IT security and the rules defined for its protection (security policy).

2. CERT/CSIRT teams

The Internet has experienced massive development and commercialisation in the 21st century. The number of users, the number of computer systems connected to the global network and also the number of critical services being operated increased dramatically, both from the commercial sphere (e.g. electronic banking, e-shops, electronic auctions) and from the state sphere (e.g. state information service administration and self-government, registers). Security incidents, cyberattacks, and crime committed through information and communication technologies in the real and virtual worlds are becoming increasingly more serious, and their impacts and consequences are deteriorating.

A significant difference of this cybercrime from other types of crime is its high latency, high level of tolerance by society (including user indifference), anonymity of the perpetrator and its often difficult identification. There is a growing need to streamline defence against these attacks, in particular to improve the environment and means of tracing the perpetrator, to unify and formalise procedures, and to educate users to identify, deal with and ideally prevent threats and risk situations. For this purpose, the infrastructure of the CERT and CSIRT security teams is being built.

2.1. History

The first security incident that negatively affected the operation of the then Internet by shutting down approximately 10% of all connected devices is called the Morris worm. The worm was launched on the Internet in 1988 by Robert Morris, a student at Cornell University in the United States. This incident started an era of creating and spreading computer viruses, worms, Trojan horses and other similar "electronic vermin", collectively referred to as *malware*. And it was this experience that started the discussion on the security of networks and services at the end of the 1980s, in order to subsequently formulate the basic principles of defence, prevention and protection of the transmission of sensitive data.

In response to the Morris worm, the first CERT team was formed at Carnegie Mellon University (CMU) in the USA. This first ad-hoc CERT was designed to examine the Morris worm, find an effective defence, and propose a solution to the predicament. In the end, the most valuable result of the team's work was to find that the most important thing was to be prepared in advance for a security breach and launch a predefined and tested defence and recovery rescue plan at the time of the problem, and not just begin to examine what needs to be done and what steps. The result of the work of this first CERT thus started the era of building a global infrastructure of teams of this type.

Carnegie Mellon University has registered the abbreviation CERT as a trademark, and although it is not opposed to its use by other organisations in this context (an organisation wishing to use the abbreviation on behalf of its team must apply for permission to use the abbreviation and usually receive it), this was the reason for the emergence and introduction of the second concept of CSIRT.

2.2. CERT and CSIRT teams

CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team). Although each of these acronyms has a slightly different meaning and mainly a slightly different historical genesis, both acronyms can in fact today be understood as the same type of team – a team that is in its clearly defined scope of activity responsible for dealing with security incidents and (cyber)threats, from the point of view of users or other teams, the place to which they can turn with the detected security incident, with a request for cooperation, exchange of information, assistance, etc.

CERT/CSIRT teams are created at the level of individual organisations that mediate the operation of the Internet (ISP – Internet Service Providers), as well as organisations that use the Internet environment for their core business (such as IT companies, content providers, banks).

The basic duty of every CSIRT team is to respond to a threat and cooperate in resolving incidents. A CSIRT team usually addresses a problem that occurs in its scope of activity (e.g. its own network infrastructure), i.e. where it has real possibilities to intervene.

A CERT/CSIRT of a given network (organisation) is generally a point of contact that users can turn to with an identified security problem (or just a suspected problem) that concerns a computer network or one of the services operated. A professional CERT/CSIRT team should review each report (including a potential) security incident received and, if possible, remedy the problem.

It is nothing revolutionary which would not exist in practice, every major organisation, internet provider or service provider runs a security team. **The difference between a regular security team and a CERT/CSIRT team is mainly in the involvement in the global security infrastructure, the sharing of information within this infrastructure and the observance of established formal procedures.**

The existence of at least one official CERT/CSIRT team is desirable in every network operated, especially in the large ones (transit, regional, university), i.e. at the level of large ISPs, but also at banks or service providers.

The overarching **top teams** within individual states have a significant and **specific role** – the so-called **national** and **governmental** teams, to which a separate subchapter will be devoted.

Globally, existing CERT/CSIRT teams can be viewed as an infrastructure that addresses Internet security problems. At work, a CERT/CSIRT team draws primarily from its experience, pre-prepared and proven procedures and from cooperation and exchange of information with other CERT/CSIRT teams.

The basic requirement of a community is that the CERT/CSIRT team publicly declares its contact information and rules of activity:

- who is its operator,
- who are its members,
- the way and when it is possible to reach the team,
- what services does it offer,
- scope of activity (AS number^[1], network, domains, services), in which the team is qualified to act and in what way, i.e. defining its powers and responsibilities. Based on the scope of activity, the team is then contacted (e.g. by those attacked) and addresses the issues (incidents) associated with it.

The concept of addressing a security incident can have different specifics depending on the team settings and its internal policy – it can be a simple elimination of an attack (destruction of the source of the problem, e.g. by disconnecting the compromised computer system from the network), tracing the attacker, fast resumption of operation of the infected service/network, etc.

Depending on the team's activities in resolving a security incident, teams can be described as *internal* (institutional) or *coordinating*. The internal type of the team usually has the possibility of direct intervention (disconnect the source of the problem, introduce network traffic filtering, etc.), the coordination type of the team does not have the possibility of direct intervention, its activities focus on communication, cooperation and mediation of information (they are usually *national* teams, which will be discussed below).

In the case of addressing a specific incident, the participants tries to address it directly at the source, i.e. with who is closest to the source or destination of the incident and can intervene as effectively as possible (end network or service administrator). The ideal situation occurs when the source and target are within the scope of a CSIRT team, because it is very easy and fast to find a specific expert at the problem site. The expert can then also address the problem effectively and his/her reactions are predictable, as he/she voluntarily published his/her rules of the game. This communication procedure is very flexible due to the fact that the communication does not go through different levels. It is fast and accurate. Then the reaction can be the same. However, if the victim cannot find a suitable counterpart (whether because he/she does not exist, does not give any usable information about himself/herself, refuses to address the problem or simply does not react), a "leverage" would be appropriate. That can be usually, to some extent, provided by top teams – national and governmental.

[1] **AS – Autonomous System.** An autonomous system is a set of IP networks and routers under common technical management, which represents a common routing policy towards the Internet.

2.3. How a CERT/CSIRT team is formed

An organisation that decides to set up a CERT/CSIRT team must initially define clearly and comprehensively what it wants to achieve by creating the team, what role it requires from the team (i.e. it specifies its scope, powers, responsibilities and services operated) and must also secure it in an appropriate way in the organisation.

Scope of activity

The scope of activity is usually the area of cyberspace in which the team is qualified to act and over which it has the relevant powers and responsibilities defined by the founder. Based on the declared scope of activity, the team is then contacted, for example, by those attacked, and addresses problems in the sphere of their influence. The scope of a team's activity can be defined as a specific network(s), autonomous system(s), name domain(s), but there are also teams that list their expertise, specific service, etc. as the scope of activity.

Services

In order for a team to be officially called a CERT/CSIRT, it needs to primarily offer a security incident resolution or coordination service within its defined scope, thus fulfilling the "response" idea used in CERT/CSIRT acronyms, i.e. this team needs to be able to *respond* to a security incident. However, the team can offer a number of other services from many areas, such as training, warning of current attacks, OS vulnerabilities, security audits, SW consultations, recommendations of basic security rules, development and operation of tools for monitoring network and service traffic and much more.

Team members

The area that has a decisive influence on the quality of the team is its staffing. In each network operated, there is usually a department or group of technicians who are in charge of the operation and development of the network and services and also deal with security aspects (generally "IT staff", "security staff", "administrators", etc.). These are usually the right people to join a CERT/CSIRT team or to be assigned to build it. However, it is advisable to have other types of experts in the team (such as a lawyer, or, in the case of national and government teams, a media liaison officer, a manager, a sociologist, etc. can be useful). It depends on the focus, environment, services offered and the role of the team.

From an "external" point of view, a team becomes a CERT/CSIRT team when it is accepted as such by other existing global CERT/CSIRT teams. The path to obtaining CERT/CSIRT team status is not complicated, at the beginning it is enough to clearly declare the following:

1. **Basic contact information** – name of the team, name of the organisation running the team, e-mail 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 headquarters, names of team members, working hours for which the team can be reached, etc.
2. **Scope of activity of the team** – defines what the team is responsible for and what its role is. This, of course, depends on what team it is. It is possible to set up teams of roughly the following types:
 - **internal** – it serves and is responsible for a specific network (e.g. for a specific range of IP addresses, domains), usually set up by the network operator,
 - **coordinating** – a team whose main task is to coordinate the resolution of security incidents, it does not have to address them in a targeted manner,
 - **vendor** – a team dealing with the resolution of security incidents that affect a specific product (SW),
 - **national, governmental** – special cases based on the principles of the first two mentioned teams (internal and coordination), their scope and role depend on the founder and often also on the legislation of a particular country.
3. **Services offered** – the CERT/CSIRT team must provide at least a security incident resolution service.

Once a newly established CSIRT/CERT team has dealt with the above steps and established a basic team policy for dealing with security incidents, which includes incident severity classification, incident response rules, contactability of team members, rules for communication with the author of the security incident report, etc., it is well on its way to being accepted by the adjacent teams. A natural and necessary part is the need to get acquainted with the basic rules agreed by the CSIRT community and to follow them.

At the very beginning of creating a team of the CERT/CSIRT type is also the creation of its technical and organisational background, without which no team can function effectively.

Technical background means, for example, a tool for effective management of security incident reports, which allows monitoring of its entire life cycle, i.e. when the report was sent, by whom, at what stages of the incident, why, how it proceeded, who asked whom to cooperate, how serious the incident was and what escalation procedures were applied to it, etc. For this area, teams usually use various so-called ticketing systems, e.g. RTIR[1], OTRS[2]. Other important aids in the field of technical tools are various IDS (Intrusion Detection System), systems for security audits of networks and equipment, systems for forensic analysis, network traffic monitoring (netflow), etc.

The **organisational background** represents precisely the mentioned "readiness" for the problem, i.e. defining the basic rules for the operation of the team so that each team member knows his/her role, duties and responsibilities, the policy of security incident resolution, rules for communication, information sharing and exchange, cooperation, etc. The basis in this area is generally well-managed **incident management**.

At the moment when the newly forming team manages the above, i.e. it is able to describe itself and its activities and carry them out. It can participate in cooperation at the national and international level.

[1] **RTIR** – Request **T**acker for Incident **R**esponse. For more details, see e.g.: <http://www.bestpractical.com/rtir/>.

[2] **OTRS** – Open **S**ource **T**icket **R**equest **S**ystem. For more details, see e.g.: <http://www.otrs.org/>.

2.4. CERT/CSIRT infrastructure cooperation

CERT/CSIRT teams are set up on a voluntary basis, and it is in their interest to communicate effectively with each other, exchange important information and knowledge and cooperate. They therefore associate in international organisations. Currently, the best known and most active organisations that deal with this issue and create a suitable environment for the above objectives are the international organisations **GÉANT**[1] and **FIRST** (Forum for Incident Response and Security Teams)[2].

Both of the above organisations initiate and enable regular meetings of members of the security teams, exchange of experience and participate in defining the basic rules of cooperation and communication between the world's CERT/CSIRT teams.

The European organisation GÉANT runs several activities in which the world's CERT/CSIRT teams can participate if interested:

- **TF-CSIRT** (Task Force for CSIRT) is a working group that allows teams to work together in the form of regular two-to-three-day meetings, which take place 3 times a year. (This meeting is usually hosted by a CERT/CSIRT team.) More information can be found at: <https://tf-csirt.org/>.
- **CSIRT Training** – used to train new members of CSIRT/CERT teams, or for those who are going to establish a CERT/CSIRT team. It is usually held twice a year and the trainers are experienced members of renowned CERT/CSIRT teams and other top security experts. More information can be found at: <https://tf-csirt.org/transits/>.
- **Trusted Introducer**[3] – an office whose primary task is to build trust between different CERT/CSIRT teams and to assist in the creation of new ones. More information can be found at: <https://www.trusted-introducer.org/>.

In addition to the large annual conference held every year, FIRST organises a number of training sessions, creates guidelines and standards for the effective work of CERT/CSIRT teams and, of course, cooperates with the TF-CSIRT activity.

Within the global infrastructure of CERT/CSIRT teams, GÉANT and FIRST act as a kind of “guarantee” that the team that claims to be a CERT/CSIRT team is really so, and that the declared pattern of conduct is true. Every new team that wants to join the security infrastructure goes through an entry process that verifies that the team meets community standards, is transparent, and there are no compelling reasons to accept it. In the case of European infrastructure (TF-CSIRT platform), this entry process is provided by the Trusted Introducer and is actually requested by the new team to register in the team list and be granted **listed** status.[4]

Among the existing teams, there must also be at least two teams (so-called sponsors) that will support a new team, and no already established team may object to its acceptance. If all goes well, information about the new team is stored in a list maintained by TI (and some of it is published), the team gets the **listed** status, and the community welcomes the new member.

In the case of FIRST, the entry procedure is very similar, only ending not by granting status, but by gaining **membership**.

Both processes have one thing in common – it is about determining and publicise the maximum amount of information about a given team, describing its conduct and perceiving the issue of resolving security incidents so that it corresponds to the requirements of the community.

In the case of the Trusted Introducer, it is possible to achieve other, more significant, statuses, namely **accredited** and **certified** statuses. The differences are as follows:

- A team with the achieved **listed** status provided basic information about itself, declared a desire to conduct as a CSIRT team and the community accepted it.
- A team with the **accredited** status declares the required level of its procedures to the community and is committed to adhering to common TI policies.
- A team with the **certified** status then proved its “level of maturity” (maturity) within the certification process.

Being an **accredited** or **certified** team requires a continuous effort to maintain the status of the team. Part of this effort is also the obligation to keep the team information up-to-date on the TI's list. If the team does not do so in the long run, it may lose its status and, in the worst case, be expelled by the community. This obligation also applies to **listed** teams, which, if they do not pass the accreditation process within three years of obtaining the listed status, must renew their listed status by demonstrating support from other teams (i.e. a re-listed process). This mechanism ensures a high degree of timeliness of the information in the TI list and thus its credibility.

Another organisation active in the field 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 covers a range of activities including pan-European cybersecurity exercises, the development of national cybersecurity strategies, cooperation between CERT/CSIRT teams and capacity building, addressing data protection issues and working together to create and implement legislation in matters related to Network Information Security (NIS).

All three mentioned organisations have one more common function – they gather know-how from the whole community and enable its sharing (by formulating so-called best-practices documents, instructions, recommendations).

[1] The association was formed by merging TERENA (Trans-European Research and Education Networking Association) and DANTE.

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

[3] Hereinafter also **TI**.

[4] **Listed** – listing the team in the database of all registered teams.

2.5. Hierarchy of CERT/CSIRT teams?

CERT/CSIRT teams have no official hierarchy that would make one team superior to another. All teams are **equal** in terms of functioning, communication, cooperation and exchange of information and are not limited in these areas. The existence of the so-called top *national* and *government* teams somewhat suggests that a hierarchy between teams exists, even though this is not the case. The only "hierarchy", but rather it would be more appropriate to say "greater capacity to act", gives the top team the legislation of the country, which regulates its powers (e.g. in the area of required response to security threats from network and service operators, etc.).

In the world of CERT/CSIRT teams, willingness to share important information about an incident and threats is key. To do this, it is essential that teams trust each other and also that users trust their teams. Gaining the trust of users and the community is a long-term task. Teams must show their qualities in all aspects of their operation and build credibility gradually – not only with the ability to help, but also the ability to ensure confidentiality and fair treatment of shared data, transparency of conduct, etc.

2.6. National and government CERT/CSIRT teams

National and government teams are a special form of CERT/CSIRT teams. They treat other CERT/CSIRT teams as equals, but their role throughout the system is different.

National CERT/CSIRT acts as a kind of last resort where it is possible to request intercession, assistance and intervention. Its goal is (within the state or area where it operates) to mediate contact between a victim and a perpetrator of the problem and help successfully address the problem. National teams (usually) do not control the physical infrastructure, so they do not (unlike internal/institutional teams) have the opportunity to intervene directly. Their role consists in mediating contact, or in coordinating (hence this type of team is called a coordination team) the procedure of individual troubleshooters in the event that the problem is more extensive and its solution requires the cooperation of several components.

From the principle of the functioning of the whole structure, incidents that pass through the system of the national CSIRT are usually only a fraction of the total number. Most incidents are resolved through direct communication, without the need for escalation and mediation. The national team thus receives mostly incidents that cannot be addressed otherwise (those responsible refuse to address them; it is not easy to identify who is responsible for addressing them), very serious or recurring problems, or problems that may have a general impact, etc.

The national CERT/CSIRT usually has training and cooperation in its job description. It is both consciousness raising with regard to the public and an operation within the Internet infrastructure. The aim is to support the creation of additional CERT/CSIRT teams in the country, their introduction to the international scene and support in the implementation of standard procedures and methods. All this significantly increases the transparency of the environment and gives the victims a chance to effectively seek redress.

A Government **CERT/CSIRT** usually focuses on the area of state administration and self-government and on resolving incidents that threaten the security of the state and its services. A government CERT/CSIRT can take the form of an internal team with the possibility of direct intervention in the event of a problem. Its existence is usually supported by legislation.

However, the above is not dogma, and the situation varies from country to country. There are countries where only the national team works (and also serves as the government team); there are countries where the government team works (and plays the role of the national team); there are countries where both exist; there are countries where there is neither and the role of the top team is replaced by one of existing teams, etc.

2.7. Situation in the Czech Republic and in the world

Currently, around 380 CERT/CSIRT security teams are officially constituted worldwide, which are either members of FIRST or the European TF-CSIRT platform (or both).

In the Czech Republic, 39 security teams of the CERT/CSIRT type are currently officially established and recognised by the Trusted Introducer, which makes the Czech Republic almost a world "superpower", with only France, Germany and the United Kingdom competing in numbers. Of course, it is not about quantity, but above all about quality.

The first CERT/CSIRT security team that was established in the Czech Republic is the **CESNET-CERTS** security team (<https://csirt.cesnet.cz/>). It was officially constituted in 2003, and in January 2004 it was officially recognised by the international infrastructure and the Trusted Introducer. It is operated by the CESNET association^[1] and is responsible for addressing and coordinating the resolution of security incidents in the CESNET e-infrastructure. Among other things, it deals with the development of security tools and also provides educational services for users in its sphere of influence.

Other teams were founded in the CZ.NIC association (CZ.NIC-CSIRT) in 2008, at Masaryk University in Brno (CSIRT-MU) in 2009, in the company Active24 (team Active24-CSIRT) in 2012 and within a project supported by the Ministry of the Interior of the Czech Republic CSIRT.CZ team (since 2011 National CSIRT CR).

We can observe a big boom in the field of building security CERT/CSIRT teams in the Czech Republic especially since 2013, when the Czech Republic faced a series of DDoS attacks on public web services. This event subsequently initiated the creation of the Fenix project (<https://fe.nix.cz/>) on the grounds of the Czech peering center NIX.CZ.

The purpose of this project is to enable the availability of Internet services within the entities involved in this activity in the event of a DoS attack. The Fenix project has defined a number of technical and organisational rules that those interested in joining the project must meet, and one of them is also an officially constituted CERT/CSIRT team. This was an impulse for many organisations to formalise their security teams into a CERT/CSIRT team and integrate them into the international infrastructure.

Another motivating impulse that led to the constitution of new teams is the adoption and subsequent effectiveness of the law on cybersecurity. Many organisations have understood that security is worthwhile and that setting up a CERT/CSIRT brings benefits.

The current infrastructure of CERT/CSIRT teams in the Czech Republic, numbering 39 teams, consists of a national and government team, there are teams at the level of large ISPs, several teams in the academic sector, teams in the banking industry, IT companies, domain registrars and last but not least on the ground of the Czech peering center NIX.CZ, on the ground of the CZ.NIC association. Together, this is a very diverse and, as a result, robust and viable infrastructure, which includes experience from various industries.

The current list of Czech CERT/CSIRT teams can be found at: https://tiw.trusted-introducer.org/directory/country_LICSA.html

^[1]The CESNET Association, z. S. P. O., is an industry association of legal entities, founded in 1996 by universities and the Academy of Sciences of the Czech Republic. It operates the national high-speed computer network for science, research, development and education CESNET2. For more details, see: <http://www.cesnet.cz/>.

2.8. National CSIRT of the Czech Republic

In December 2010, the Czech Republic also officially established the National CSIRT of the Czech Republic. The CZ.NIC Association and the Ministry of the Interior signed (on 16 December 2010) a Memorandum according to which the administrator of the Czech national domain of the CZ.NIC Association took over the agenda of the CSIRT.CZ team and since January 2011 has been operating it as the National CSIRT of the CR.

The CSIRT.CZ practice (<http://www.csirt.cz/>) was established within the scope of a grant of the Ministry of the Interior of the Czech Republic "*Cyber threats and Czech Republic's security interests*" (project identification code is VD20072010B013) and was built by CESNET. This practice was referred to as a model and was built to verify the state of the security infrastructure in the Czech Republic and to verify the feasibility of building a distributed hierarchy for a systematic comprehensive solution to security issues in the Czech computer networks through CSIRT teams. The operation of this team was officially launched on 3 April 2008. In May of the same year, it was presented to other European CERT/CSIRT teams at the TF-CSIRT community meeting (which took place in Oslo, Norway) as a CSIRT practice with the role of "*last resort*" for the Czech Republic and as such was accepted by the community.

The CSIRT.CZ practice laid the foundations for the further development of the top level of the CERT/CSIRT infrastructure in the Czech Republic, especially in the area of cooperation. At the same time, it verified and confirmed the assumption that the top CERT/CSIRT teams in the Czech Republic make sense.

The National CSIRT of the Czech Republic also performs other tasks of CS.

2.9. Government CERT of the Czech Republic

On 19 October 2011, the Government of the Czech Republic adopted Resolution No. 781 on the establishment of the National Security Authority (*Národní bezpečnostní úřad – NBU*) as the custodian of cybersecurity issues in the Czech Republic and at the same time the national authority in this area. Since the beginning of its appointment, the NBU has focused on three tasks – writing the law on cybersecurity, building the NCKB (*Národní centrum kybernetické bezpečnosti – National Cyber Security Centre*) and building the Government CERT of the Czech Republic.

The Government CERT of the Czech Republic, the GovCERT.CZ team, was incorporated into the international community in 2012, making the Czech Republic one of the countries that has a National and Government CERT/CSIRT team.

The competence of GovCERT.CZ includes networks of state administration, self-government and critical infrastructure of the Czech Republic. The team also focuses on the development and operation of security services, education and is also involved in national and international cooperation.

The Government CERT of the Czech Republic also performs other tasks.

2.10. Which CERT/CSIRT team to contact?

The title of this subchapter is also a frequent lament of an Internet user who got into trouble (e.g. someone attacks him/her, stole his/her identity, hacked a Facebook profile or e-mail account, or witnessed the spread of child pornography). What should such a user do? Contact the Police of the Czech Republic? Or the Internet service provider, e.g. their helpdesk? Or contact the National Cyber and Information Security Agency when it is responsible for cybersecurity? The [National Safer Internet Center](#) hotline? Or some CSIRT team when they're still being talked about? But which one?

The process of reporting and resolving security incidents (or in other words "who to contact if I want to report or resolve a security incident") **can be viewed from two perspectives**. From the perspective of technicians (network and service administrators, members of security teams) and from the perspective of users.

For technicians (network and service administrators, members of security teams), the answer to the question "who to actually contact with a request for action" is quite clear, but this is due to drill, experience and above all a very good knowledge of the Internet environment and its basic principles, as well as knowledge of where contact information for individual existing networks, services, domains, etc. is available.

For members of CERT/CSIRT teams, the basic sources of contact information are the RIR databases, the database of top-level domain operators and the catalogues of CERT/CSIRT teams.

RIR (Regional Internet Registry) holds and makes available information on to whom a block of IP addresses has been assigned. The world is divided into regions and each RIR (currently RIPE, ARIN, APNIC, LACNIC, AFRINIC) assigns IP addresses for its region. The Europe, Middle East and Asia region is administered by RIPE NCC (<https://www.ripe.net/>). RIRs operate publicly accessible databases that contain data on assigned Internet networks and their administrators. These databases allow you to find information about which organisations and which administrators are responsible for specific IP addresses.

Another source of useful information is data on domains operated and made available by top-level domain administrators; for the TLD domain .cz, it is the CZ.NIC association.

And then there is the area of CERT/CSIRT teams, which usually define their scope using Internet identifiers, name domains, or just verbally. Due to their number, the way they define their scope and especially the differences in their level, it is not always easy to find a team that is able to help. To facilitate orientation between teams, some kinds of "catalogues" have been created, which are taken care of by FIRST and the Trusted Introducer. These catalogues contain basic information about CERT/CSIRTs, contacts, their scope, etc.

The process of reporting and resolving security incidents (**incident handling**) is not an exact process, on the contrary, and a lot depends on the experience and sometimes the creativity of the person who performs this process. The exchange of information between teams usually takes place quickly and efficiently, although even this often does not guarantee a quick solution to the problem, because the whole infrastructure is still relatively "sparse", and unfortunately it must be noted that the level of teams is different.

The optimal state of the infrastructure would be if each IP address were within the scope of an official CSIRT team. This is, however, by far not the situation of the infrastructure of CERT/CSIRT.

From the point of view of a normal user, the situation is very unclear and, in fact, confusing. So what should a user do if a security incident is detected and who should they contact? It is difficult for the user to want to orientate himself/herself in the issues of CERT/CSIRT teams, to be able to find the right one, to study its security incident reporting policy and take action. A user should first contact the administrator of his/her network or services (if he/she has someone like that), or he/she should cooperate with the Internet service provider, i.e. his/her ISP's helpdesk or its user support. On the part of the ISP or service provider, there should be a clearly described entry point (contact) which users could and should contact if they become the target of an attack, detect a security incident, or feel that something is not all right. This is why the environment of ISPs is one of the most important areas where an official CERT/CSIRT team should be constituted and provide security services to the users of their network.

Of course, there may be situations where both a technician and a user do everything right, and the solution to the problem is still not in sight. A person or team does not react to the reported problem, or even refuses to address it (saying that it is not their problem, or it is not so serious), etc. This is the moment when either the Police of the Czech Republic comes in (the user can contact it with the filing of a criminal complaint), or a top team comes in (national or government) that the user can contact as the last resort from which help and response can be expected.

There is a very close cooperation and exchange of information and relevant data between the **national and government team**, and thus the transfer of the reported problem to be addressed from one team to another or directly to the solution.

In general, the national and government team should be a place for network providers, service providers (and, if necessary, users) where, in case of problems, ambiguities, etc., it is possible to ask for help and consultation, e.g. finding a suitable counterpart for communication (foreign CERT/CSIRT team), mediation of communication (yes, sometimes the "leverage" of the top team is useful, the counterpart is then more willing), and a source of know-how and information.

In general, however, it would be desirable for network and service administrators and members of security teams to master and apply the principles of the *incident handling* process and to maximise communication directly (not through top teams). This makes the incident handling process fast and efficient, and other intermediate stages can introduce unpleasant delays and, unfortunately, distortions. But as already mentioned, it depends on the severity of the situation and the problem being addressed.

CERTs/CSIRTs and their infrastructure are generally not omnipotent and do not ensure security "in a nutshell".

Their existence is just one of the little blocks in the field of building Internet security, in which all stakeholders play an important role, i.e. network administrators, service managers, managers who decide on the background for effective network and service security, ISPs, critical service operators, security forces, state, and last but not least we, users.

The current list of CSIRT/CERT teams can be found at:

<https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map>.

2.11. SUMMARY

SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

- The difference between a regular security team and a CERT/CSIRT team is mainly in the involvement in the global security infrastructure, the sharing of information within this infrastructure and the observance of established formal procedures.
- The basic requirement of a community is that the CERT/CSIRT team publicly declares its contact information and rules of activity:
 - who is its operator,
 - who are its members,
 - the way and when it is possible to reach the team,
 - what services does it offer,
 - scope of activity (AS number^[1], network, domains, services), in which the team is qualified to act and in what way, i.e. defining its powers and responsibilities. Based on the scope of activity, the team is then contacted (e.g. by those attacked) and addresses the issues (incidents) associated with it.
- Scope of activity of the team – defines what the team is responsible for and what its role is. This, of course, depends on what team it is. It is possible to set up teams of roughly the following types:
 - internal – it serves and is responsible for a specific network (e.g. for a specific range of IP addresses, domains), usually set up by the network operator,
 - coordinating – a team whose main task is to coordinate the resolution of security incidents, it does not have to address them in a targeted manner,
 - vendor – a team dealing with the resolution of security incidents that affect a specific product (SW),
 - national, government – special cases based on the principles of the first two mentioned teams (internal and coordinating), their scope and role depend on the founder and often also on the legislation of a particular country.
- CERT/CSIRT teams have no official hierarchy that would make one team superior to another. All teams are equal in terms of functioning, communication, cooperation and exchange of information and are not limited in these areas.
- National CERT/CSIRT acts as a kind of last resort – the last instance where it is possible to request intercession, assistance and intervention.
- A government CERT/CSIRT usually focuses on the area of state administration and self-government and on resolving incidents that threaten the security of the state and its services. A government CERT/CSIRT can take the form of an internal team with the possibility of direct intervention in the event of a problem. Its existence is usually supported by legislation.

[1] AS – Autonomous System. An autonomous system is a set of IP networks and routers under common technical management, which represents a common routing policy towards the Internet.

KEY WORDS TO REMEMBER

- CSIRT team
- CERT team
- Incident handling
- Hierarchy of teams
- Scope of activity

KNOWLEDGE CHECK QUESTIONS

- What is a CSIRT/CERT team?
- How is a CSIRT/CERT team created and established?
- What does the national CSIRT team focus on?
- What does the government CSIRT team focus on?
- What are the basic community requirements for a CERT/CSIRT team?

3. Legislative framework of CSIRT/CERT

On 6 July 2016, the 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 of network and information systems across the Union (the NIS Directive) was adopted by the European Parliament.

The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
- a culture of security across sectors that are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and to notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the new Directive.

Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas.

The EU Network and Information Security Directive (NIS Directive) aims to create a CSIRT Network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". The Directive states that each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in the Directive's point (1) of Annex I (requirements), covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process.

The NIS Directive aims at creating a CSIRT Network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". The Directive states that each Member State shall designate one or more CSIRTs that shall comply with a set of defined high-level requirements.^[1]

According to Article 9 of NIS states:

„Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.“

And NISD continues to state that:

- *The CSIRTs have adequate resources to effectively carry out their tasks*
- *Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs*
- *Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level*
- *Member States shall inform the Commission about the remit, as well as the main elements of the incident- handling process, of their CSIRTs*
- *Member States may request the assistance of ENISA in developing national CSIRTs^[2]*

Annex I of NISD is labelled *REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)* and is quoted here in full because of its great relevance for the national/governmental CSIRT community inside the EU:

(1) Requirements for CSIRTs:

(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

(b) CSIRTs' premises and the supporting information systems shall be located in secure sites.

(c) Business continuity:

(i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.

(ii) CSIRTs shall be adequately staffed to ensure availability at all times.

(iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.

(d) CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.

(2) CSIRTs' tasks:

(a) CSIRTs' tasks shall include at least the following:

(i) monitoring incidents at a national level;

(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(iii) responding to incidents;

(iv) providing dynamic risk and incident analysis and situational awareness;

(v) participating in the CSIRTs network.

(b) CSIRTs shall establish cooperation relationships with the private sector.

(c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:

(i) incident and risk-handling procedures;

(ii) incident, risk and information classification schemes.

[1] *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cit. 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. 5-6

[2] *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cit. 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. 11

3.1. Czech Republic

The legislative framework of CSIRT/CERT teams in the Czech Republic is partly set by the Cybersecurity Act. This act sets out the conditions for the existence of the national and government CSIRT/CERT team, but on the other hand does not restrict the establishment and existence of other CSIRT/CERT teams.

Based on the Cybersecurity Act, two CERT/CSIRT teams, **namely national and government, are compulsorily established in the Czech Republic**. Each of these teams has the rights and obligations specified by law (Section 17 et seq. of the AoCS).

Teams whose scope is defined by the Cybersecurity Act are obliged to respect the limits set by this act.

3.1.1 National CERT

The national CERT team is defined in Section 17 of the AoCS. It is also stated that:

(1) The national CERT ensures, to the extent stipulated by this act, sharing of information at the national and international level in the field of cybersecurity.

(2) The operator of the national CERT

- a) receives notifications of contact details from the authorities and persons referred to in Section 3 (a), (b) and records and stores these details,
- b) receives reports of cybersecurity incidents from the authorities and persons referred to in Section 3 (b) and records, stores and protects these data,
- c) evaluates cybersecurity incidents in the case of bodies and persons referred to in Section 3 (b) and
- d) provides the bodies and persons referred to in Section 3 (a), (b) and methodological support, assistance and cooperation in the event of a cybersecurity incident,
- e) acts as a contact point for the bodies and persons referred to in Section 3 (a), (b) and
- f) assesses vulnerabilities in the field of cybersecurity,
- g) transmits to the Office data on cybersecurity incidents reported pursuant to Section 8 (3), without stating the notifier,
- h) transmits data pursuant to Section 16 (5) and (6) upon request to the Office,
- i) act as a CSIRT in accordance with the relevant European Union legislation.[\[1\]](#),
- j) inform the relevant authority of another Member State, without disclosing the identity of the notifier, of a cybersecurity incident with a significant impact on the continuity of basic or digital service in that Member State, while informing the Office and maintaining the notifier's security and business interests,
- k) cooperate with CSIRTs of other Member States; and
- l) receives reports on cybersecurity incidents from authorities and persons not listed in Section 3, and if its capacities allow it, processes them and provides methodological support, assistance and cooperation to the authorities or persons affected by a cybersecurity incident.

(3) The operator of a national CERT may, on behalf of its own name and on its own responsibility, also perform other economic activity in the field of cybersecurity not regulated by this Act, provided that this activity does not interfere with the fulfilment of obligations referred to in paragraph 2.

(4) The operator of the national CERT shall, in fulfilling the obligations referred to in paragraph 2, coordinate its activities with the Office.

(5) The operator of a national CERT must act impartially in fulfilling the obligations under paragraph 2.

This provision defines the institution of the national supervisory body for which the legislative abbreviation national CERT is used and defines its activities. The act assumes that the national CERT will usually be run by a person governed by private law, who will enter into a public contract with the NBU, and will serve in particular as a joint contact and coordination point for obligated persons under private law. Providers of electronic communications services, entities providing electronic communications networks and entities providing significant networks will implement their legal notification obligation towards the national supervisory workplace.

The model of standard private law performance of the functions of the national CERT facilitates communication between the national CERT and the obligors using it as a contact point. These persons will also, as a rule, be of a private law nature. The National CERT will also be able to participate in international networks of similar private national supervisory bodies and benefit from the knowledge that is informally

shared within these networks.

Given the meaning and purpose of the act, the presumed private law character of the national CERT is also appropriate because the operator of the national CERT may, if it is a person governed by private law, take initiatives on the basis of tacit permission, i.e. any activity under their private will not violate legal obligations. The operator of the national CERT will thus be able, for example, to provide methodological and information assistance to entities outside the personal scope of the act, i.e. to persons outside the definition of individual categories of obligors who show interest in it. The National CERT will be able to further develop its own educational, publishing, research or development activities, etc. The condition limiting the activities of the national CERT carried out on the initiative to achieve the purpose of this act is their indisputability with the fulfilment of obligations legally specified in the act.

Concerning Section 17 (2) (a), (b), (d) and (e)

Digital service providers are added to the entities with which the national CERT operator communicates and cooperates.

Concerning Section 17 (2) (c)

Digital service providers are added to the entities with which the national CERT operator cooperates, in this case for which it evaluates cybersecurity incidents. This provision is in reverse guard to the provision that obliges digital service providers to report cybersecurity incidents to the national CERT operator.

Concerning Section 17 (2) (g)

This is a linguistic adjustment of the provisions and the explicit relation of the obligation to provide information to incidents reported by obliged entities.

Concerning Section 17 (2) (h)

The wording of the provision is clarified and the restriction of situations in which the national CERT transmits the contact details of obligors to the Office is removed.

Concerning Section 17 (2) (i) to (l)

The National CERT (Computer Emergency Response Team) acquires new competencies and related obligations under the directive in this provision. This provision is closely linked to Section 8, which, among other things, regulates the reporting of cybersecurity incidents that have affected the information system of a digital service provider. In this respect, the National CERT is determined, inter alia, as one of the CSIRTs (Computer Security Incident Response Team) in the Czech Republic; the government CERT (National Cyber Security Centre, which is part of the NSA) is the second CSIRT within the meaning of the directive on incidents against the security of networks and information systems of designated basic service providers.

CSIRT teams must meet the requirements of Appendix I of the directive, which is fulfilled in the case of a national CERT operated by CZ.NIC by the requirements for the operator of the national CERT set out in Section 18 of the Act and by the content of the public contract which NBU entered into with it pursuant to Section 19. This contract pursuant to paragraph 1 of this provision is intended to ensure the fulfilment of activities pursuant to Section 17, i.e. also the new requirements arising from the directive.

Specifically, the act corresponds to the tasks of the CSIRT under the directive as follows:

National CERT: receives reports on cybersecurity incidents, evaluates them, provides methodological support, assistance and cooperation to the entities concerned, acts as a contact point, assesses vulnerabilities in the field of cybersecurity, transmits incident data to the NSA, acts as a CSIRT under the directive, cooperates with other CSIRTs, communicates with the relevant authorities of other Member States and, last but not least, receives voluntary reports of cybersecurity incidents. By this it meets the requirements of Appendix I to the Directive:

- *Monitoring of incidents at the national level – Section 17 (2) (b), (c), (l)*
- *Issue of early warnings and alerts, notification and dissemination of information on risks and incidents to relevant stakeholders – Section 17 (2) (d), (e), (g), (j)*
- *Response to incidents – Section 17 (2) (c), (d)*
- *Provision of dynamic analysis of risks and incidents and overview of the situation – Section 17 (2) (f)*
- *Participation in the CSIRT network – at the discretion of the national CERT operator, see further commentary on Section 20.*

The obligation to set up at least one CSIRT security team responsible for risk management and incident resolution according to well-defined procedures and meeting the requirements for CSIRT security teams follows from Article 9 (1) of NIS.

The NIS Directive stipulates that this mandatory team must cover at least the sectors listed in Appendix II (types of entities) and the services listed in Appendix III (types of digital services).

Appendix I of the NIS Directive defines the tasks and requirements for CSIRTs. These tasks and responsibilities according to Appendix I of the NIS include:

1. Requirements for CSIRTs

- CSIRTs will ensure that there are no single points of failure in their communication services, so that these services are widely available and have several ways to contact others and which will make it possible to contact them at any time. In addition, communication channels must be clearly specified and well known to the collaborating partners and entities within the scope of the teams.
- CSIRT practices and their support information systems are located in a safe place.
- Continuity of activity:
 - o CSIRTs are equipped with appropriate requirements management and routing systems to facilitate handover,
 - o CSIRTs are properly staffed so that they are available at all times,
 - o CSIRTs must work with infrastructure the continuity of which is guaranteed. Backup systems and workstations must be available for this purpose.
- CSIRTs must be able to participate in international cooperation networks if they wish to be part of them.

2. Tasks of CSIRTs

- The tasks of CSIRTs include at least:
 - o monitoring incidents at the national level,
 - o issuing early warnings and alerts, notifying and disseminating information on risks and incidents to relevant stakeholders,
 - o response to incidents,
 - o providing a dynamic analysis of risks and incidents and an overview of the situation,
 - o participation in the CSIRT network.
- CSIRTs will establish cooperation with the private sector.
- In order to facilitate cooperation, CSIRTs promote the adoption and use of common or standard procedures in the areas of:
 - o incident and risk management,
 - o classification of incidents, risks and information.

The CZ.NIC Association operates the **national CSIRT team of the Czech Republic – CSIRT.CZ** (for more details see <https://csirt.cz/>).

Concerning paragraphs (1), (2) and (4)

According to the Cybersecurity Act, the operator of the national CERT:

- **receives notifications of contact details** from the authorities and persons referred to in Section 3 (a), (b) and of the AoCS and records and stores these details,
- **receives reports of cybersecurity incidents** from the authorities and persons referred to in Section 3 (b) and of the AoCS and records, stores and protects these data,
- **evaluates cybersecurity incidents** at bodies and persons referred to in Section 3 (b) and of the AoCS,
- **provides the bodies and persons** referred to in Section 3 (a), (b) and of the AoCS **methodological support, assistance and cooperation in the event of a cybersecurity incident**,

The scope of activity of the CSIRT.CZ team is the entire address range of the Czech Republic. CSIRT.CZ can be contacted for help by all network administrators who need assistance with resolving an incident that requires coordination of the solution or have a suspicion that the incident could have a nationwide impact. More information and instructions on reporting incidents can be found [here\[2\]](#). **The CSIRT.CZ team does not have executive powers** and in resolving incidents, it acts as a coordinator that can also provide methodological assistance in resolving them.[3]

- **acts as a contact point** for the bodies and persons referred to in Section 3 (a), (b) and of the AoCS,
- **assesses vulnerabilities** in the field of cybersecurity,
- **transmits to the NUKIB data on cybersecurity incidents** reported pursuant to Section 8 (3) of the AoCS without stating the notifier,
- **transmits data** pursuant to Section 16 (5) and (6) of the AoCS **upon request to the NUKIB**,
- **act as a CSIRT in accordance with the NIS Directive**,
- **inform the relevant authority of another Member State**, without disclosing the identity of the notifier, **of a cybersecurity incident with a significant impact** on the continuity of basic or digital service in that Member State, while informing the Office and maintaining the notifier's security and business interests,
- **cooperate with CSIRTs of other Member States**,

- **receives reports on cybersecurity incidents from other persons** not referred to in Section 3 of the AoCS, and if its capacities allow it, processes them and provides methodological support, assistance and cooperation to the authorities or persons affected by a cybersecurity incident.

Pursuant to Section 17 (4) of the AoCS, the **CZ.NIC Association is obliged to coordinate the activities of the national CSIRT team with the activities of NÚKIB.**

In addition to the obligations explicitly set out in the Cybersecurity Act, the national CSIRT has set itself other tasks [\[4\]](#), including:

- **Information about an infection in the .CZ domain**

For the purposes of central monitoring and handling threats in the second-order domain, CSIRT.CZ has developed an open source tracker: [Malicious Domain Manager](#).

The application serves as a central point for collecting and analysing information about malicious URLs in the .CZ domain.

The application supports the history of threats in the domain and direct contact with their holder. Domain holders are contacted from the dedicated address malware@nic.cz.

- **Web scanner**

For the non-profit and public sector, a free website penetration testing service is primarily provided. Testing consists of automatic and manual tests aimed at finding security vulnerabilities in the application. Each safety finding is identified by an estimated level of potential risk and contains a description of recommendations for its possible correction.

For more details, see <https://www.skenerwebu.cz>.

- **Education and lectures**

In cooperation with the CZ.NIC Academy, the courses [Computer Security in Practice](#) and [Fundamentals of CSIRT Team Operation](#) are regularly implemented. CSIRT.CZ also implements specialised courses for security forces, state and educational institutions or ad hoc lectures.

- **Assistance in setting up a CERT/CSIRT team**

- **Working groups**

The CSIRT.CZ team organises regular meetings of security teams and members of the security community in the Czech Republic.

- **Stress tests**

After the DDoS attacks of 2013, which were focused on important services in the Czech Republic, the CZ.NIC Laboratories prepared [stress tests](#) reaching the same and higher intensity as the mentioned DDoS attacks. In cooperation with CSIRT.CZ, this service is provided free of charge for all interested parties that meet the entry conditions.

- **Intrusion Detection System**

In cooperation with [CESNET](#) Association, CSIRT.CZ operates a system that detects suspicious behaviour of systems connected to the Internet.

In case of recording suspicious connection attempts from specific IP addresses, the responsible administrators are immediately informed about such an event (via the e-mail address ids@csirt.cz).

- **Operation of honeypots**

As part of security research, CSIRT.CZ, in cooperation with the CZ.NIC Laboratories, operates a number of honeypots. Within the HoneyNet project, it is possible to find a visualisation of attacks in real time at <https://honeymap.cz>. Newly detected malware samples are analysed.

- **PROKI**

Sending information about security incidents that originate in the range of Czech IP addresses.

Concerning paragraphs (3) and (5)

The provision of Section 17 (2) of the AoCS allows the CZ.NIC Association to carry out other economic activities in the field of cybersecurity on its own behalf and on its own responsibility, which is not directly regulated by the Cybersecurity Act. However, there is a condition that this further economic activity does not interfere with the performance of the tasks of the national CSIRT.

The CZ.NIC Association is obliged to act impartially in fulfilling the obligations of the national CSIRT team.

Pursuant to the provisions of Section 18 of the AoCS, only such a legal entity may become the operator of a national CERT

- a) that satisfies the conditions set out in paragraph 2 and
- b) with that the Office has entered into a public contract pursuant to Section 19.

(2) The operator of a national CERT may only be a legal entity that

- a) does not act or has not acted against the interests of the Czech Republic in the sense of the law regulating the protection of classified information,
- b) operates or manages information systems or services and electronic communications networks [\[5\]](#) or has been participating in their operation and management for at least 5 years,
- c) has technical prerequisites in the field of cybersecurity,
- d) is a member of a supranational organisation operating in the field of cybersecurity,
- e) has no arrears recorded in the tax register of the bodies of the Financial Administration of the Czech Republic or the bodies of the Customs Administration of the Czech Republic or in social security premiums and public health insurance premiums,
- f) has not been convicted of a criminal offence referred to in Section 7 of the Act on Criminal Liability of Legal Entities and Proceedings Against Them,
- g) is not a foreign person under another piece of legislation and
- h) has not been established or set up solely for the purpose of making a profit; this does not affect the possibility for the operator of the national CERT to proceed in accordance with Section 17 (3).

(3) The applicant proves the fulfilment of the conditions by submission of

- a) a sworn statement in the case of paragraph 2 (a) to (d), (g) and (h) and
- b) confirmation from the body of the Financial Administration of the Czech Republic and the Customs Administration of the Czech Republic in the case of paragraph 2 (e).

(4) From the content of the sworn statement according to paragraph 3 (a), it must be clear that the applicant meets the relevant requirements. The confirmation pursuant to paragraph 3 (b) that the applicant has no arrears recorded in the tax register of the bodies of the Financial Administration of the Czech Republic or the bodies of the Customs Administration of the Czech Republic or in social security premiums and public health insurance premiums, may not be older than 30 days. In order to demonstrate the condition referred to in paragraph 2 (f), the Office will request an extract from the Criminal Register in accordance with another legal regulation [\[6\]](#).

(5) The operator of the national CERT performs activities pursuant to Section 17 (2) (a) to (c), (e) and (g) to (l) free of charge. The operator of the national CERT is obliged to incur the necessary costs for the proper and efficient performance of the activities referred to in Section 17 (2).

(6) The Office will publish on its website data on the operator of the national CERT, namely its business name or name, registered office address, entity's identification number, data box identifier and address of its website.

This provision sets out the general conditions for the selection of the national CERT operator. At the same time, the method of establishing its obligation to operate a national CERT is regulated in the form of a public law contract entered into with the NBU. The use of the institute of a public contract corresponds to the assumption that the operator of the national CERT will be a person of private law. Although the obligations of the national CERT operator to perform the activities specified in this Act are mainly of a private nature, in relation to providers of electronic communications services, entities providing electronic communications networks and entities providing significant networks, the national CERT operator will act as an entity through which these obligors perform some of their legal obligations, typically the obligation to report contact details and, in the case of entities providing significant networks, also the obligation to report the occurrence of cybersecurity incidents.

Given that the national CERT is an organisation of great importance for the cybersecurity system of the Czech Republic, its operator is required to have its registered office in the Czech Republic. With regard to the security exposure of the national CERT, it is therefore not possible to perceive this requirement as discriminatory against persons established in other states of the European Union. Integrity, a transparent ownership structure and the absence of due financial obligations to the state are the standard formal conditions required in the case of cooperation between the state and a person governed by private law. The act also formulates the material conditions for the performance of the function of the national CERT operator, requiring the national CERT operator to demonstrate the factual skills, experience and technical capabilities to perform activities imposed on it by this act, as well as the ability to work in cooperation with foreign entities operating in the field of cybersecurity. The act further requires that the operator of a national CERT perform activities entrusted to it impartially by this act, regardless of its possible contractual or other relationship with obligors.

Concerning Section 18 (5)

This provision responds to the extension of the competencies of the national CERT operator in Section 17 and adequately expands the range of activities that the national CERT operator performs free of charge.

Concerning Section 18 (5)

Legislative technical adjustment due to the extension of the competencies of the national CERT operator. In order to ensure the consistent fulfilment of the obligations arising from the Directive and subsequently from the Cybersecurity Act, the obligation of the national CERT is to spend adequate funds on ensuring the exercise of competencies.

Re paragraphs (1) and (2)

The operator of the national CERT team is the CZ.NIC association.

The provisions of Section 18 of the AoCS define the conditions under which an entity may become the operator of the national CERT.

The operator of the national CERT can only be a **legal entity [7], with which NUKIB (or formerly NBU) has entered into a public law contract [8]** (according to Section 19 of the AoCS), and **which meets the following conditions:**

a) does not act or has not acted against the interests of the Czech Republic in the sense of the law regulating the protection of classified information,

According to Section 2 (b) of the Act on the Protection of Classified Information and on Security Competence is *"in the interest of the Czech Republic to preserve its constitutionality, sovereignty and territorial integrity, ensure internal order and security, international obligations and defence, protect the economy and protect the life or health of individuals."*

b) operates or manages information systems or services and electronic communications networks or has been participating in their operation and management **for at least 5 years,**

c) has technical prerequisites in the field of cybersecurity,

d) is a member of a supranational organisation operating in the field of cybersecurity,

The requirement to operate one of the systems referred to in under (c), the existence of technical prerequisites in the field of cybersecurity and membership in a multinational organisation operating in the field of cybersecurity gives the state a guarantee that the person has been involved in cybersecurity, incident resolution etc. It is essentially a demonstration of the factual ability, experience and technical ability to perform the activities imposed on it by the AoCS.

e) has no arrears recorded in the tax register of the bodies of the Financial Administration of the Czech Republic or the bodies of the Customs Administration of the Czech Republic **or in social security premiums and public health insurance premiums,**

f) has not been convicted of a criminal offence referred to in Section 7 of the Act on Criminal Liability of Legal Entities and Proceedings Against Them,

The absence of due financial obligations to the state, as well as proof of integrity, is a standard condition for entering into a contract in the case of cooperation between the state and a person governed by private law.

The Act on Cybersecurity in Section 18 (2) (f) makes a factual inaccuracy caused by the amendment to Act No. 418/2011 Sb., on the Criminal Liability of Legal Persons and Proceedings against them. In this act, Section 7 originally defined those criminal offences which a legal person may commit. In the current effective legal regulation, Section 7 contains a negative definition of criminal offences.

The provision of Section 7 of ACLLE (Act on Criminal Liability of Legal Entities) (effective from 1st December 2016) stipulates that a legal person may be criminally liable for the commission of all criminal offences, with the exception of the criminal offences exhaustively listed in this provision.

In addition to defining the scope of criminal offences, the issue of imputability must also be addressed in the case of criminal liability of legal persons. Although a legal person is a fictitious construct, the law generally recognises, in relation to legal persons, their ability to act legally (and therefore illegally), including by attributing fault to them. Fault as a condition of criminal liability is imputed to a legal person if circumstances have arisen pursuant to Section 8 (2) of the Act on Criminal Liability of Legal Entities.

Pursuant to Section 8 (1) of ACLLE, a criminal offence committed by a legal person means an unlawful act committed in its interest or within the scope of its activities, if it was an action of

a) a statutory body or a member of a statutory body, or another person in a managerial position within a legal person who is entitled to act on behalf of or for a legal person,

b) a person in a management position within a legal person who carries out management or control activities over that legal person, even if he/she/it is not the person referred to in (a),

c) a person who exercises decisive influence over the management of that legal person, if his/her/its conduct was at least one of the conditions for the occurrence of a criminal liability of the legal person, or

d) an employee or person in a similar position (hereinafter referred to as an "employee") in the performance of his/her duties, even if he/she is not the person referred to in (a) to (c),

e) if the actions of the above-mentioned person can be attributed to the legal person according to Section 8 (2) of ACLLE.

g) is not a foreign person under another legal regulation,

According to Section 3024 of the Civil Code, a foreign person is a natural person with a residence or a legal person with a registered office outside the territory of the Czech Republic.

Due to the importance of the national CERT team in the field of cybersecurity in the Czech Republic, it is required that the operator of this team be based in the Czech Republic. This requirement cannot be perceived as discrimination against other persons established in another Member State of the Union.

h) has not been established or set up solely for the purpose of making a profit; this does not affect the possibility for the operator of the national CERT to proceed in accordance with Section 17 (3) of the AoCS.

Concerning paragraphs (3) and (4)

A legal entity wishing to become the operator of a national CERT shall prove the fulfilment of the conditions by submitting a sworn statement [in the case of Section 18 (2) (a) to (d), (g), (h) of the AoCS] and confirmation from the body of the Financial Administration of the Czech Republic and the Customs Administration of the Czech Republic [in the case of Section 18 (2) (e) of the AoCS].

It must be clear from the content of the sworn statement that the applicant meets the relevant requirements. The confirmation that the applicant has no arrears recorded in the tax register of the bodies of the Financial Administration of the Czech Republic or the bodies of the Customs Administration of the Czech Republic or in social security premiums and public health insurance premiums, **may not be older than 30 days.**

In order to **prove the fact that a legal person has not been convicted of a criminal offence, NUKIB will request an extract from the Criminal Register.**

Concerning paragraph (5)

The operator of the national CERT **performs the activities specified in Section 17 (2) of the AoCS free of charge.** Exceptions to the free of charge condition are only the following activities:

- **it provides the bodies and persons** referred to in Section 3 (a), (b) and of the AoCS **methodological support, assistance and cooperation in the event of a cybersecurity incident,**
- **it assesses vulnerabilities** in the field of cybersecurity.

The operator of the national CERT is obliged to incur the necessary costs for the proper and efficient performance of the activities referred to in Section 17 (2) of the AoCS.

Concerning paragraph (6)

Due to the possibility of contacting the operator of the national CERT team, the data on this operator are published on the NÚKIB website. The following information is published: business name or name, registered office address, entity's identification number, data box identifier and address of its website.

3.1.2 Government CERT

Government CERT, as part of the Office,

- a) receives notifications of contact details from the authorities and persons referred to in Section 3 (c) to (g),**
- b) receives reports of cybersecurity incidents from the authorities and persons referred to in Section 3 (c) to (g),**
- c) evaluates data on cybersecurity events and cybersecurity incidents from the critical information infrastructure, the basic service information system, significant information systems and other public administration information systems,**
- d) provides the bodies and persons referred to in Section 3 (c) to (g) with methodological support and assistance,**
- e) provides cooperation to the bodies and persons referred to in Section 3 (c) to (g) in the event of a cybersecurity incident and cybersecurity event,**
- f) receives suggestions and data from the bodies and persons referred to in Section 3 and from other bodies and persons and evaluates these suggestions and data,**
- g) receives data from the operator of the national CERT and evaluates such data,**

- h) receives data from authorities acting in the field of cybersecurity abroad and evaluates such data,**
- i) pursuant to Section 9 (4), provides the operator of the national CERT, bodies acting in the field of cybersecurity abroad and other persons operating in the field of cybersecurity with data from the register of incidents,**
- j) assesses vulnerabilities in the field of cybersecurity,**
- k) informs the relevant authority of another Member State, without disclosing the identity of the notifier, of a cybersecurity incident that has a significant impact on the continuity of basic services in that Member State or affects the provision of digital services in that Member State, while maintaining the notifier's security and business interests,**
- l) receives reports of a cybersecurity incident from authorities and persons not referred to in Section 3; the government CERT processes the reports and, if its capabilities allow it and if it is a cybersecurity incident with a significant impact, it provides methodological support, assistance and cooperation to the authorities or persons affected by the cybersecurity incident,**
- m) act as a CSIRT in accordance with the relevant European Union legislation [\[9\]](#) and**
- n) cooperates with CSIRTs of other Member States.**

The government CERT is a part of the NBU, or the National Centre for Cybersecurity, which is an organisational unit of the NBU, which ensures its activities. The government CERT is conceived as a central public department and a public "single point of contact" for the area of cybersecurity. Its activities include the receipt of contact data from selected obligors, the receipt of information on the cybersecurity situation, in particular the receipt of mandatory and initiative reports of cybersecurity incidents and other data on the cybersecurity situation from domestic and foreign public authorities and cooperating entities and their evaluation. The Government CERT also provides cooperation to selected types of obligors in the event of a cybersecurity incident, ensures cooperation with other bodies and entities ensuring cybersecurity in the Czech Republic and in cooperating or allied states, and also conducts cybersecurity vulnerability evaluations.

Concerning Section 20 (a), (b), (d) and (e)

Among the entities with which the government CERT communicates and cooperates, new obligatory entities are added – operators of basic services and administrators and operators of information systems of basic services.

Concerning Section 20 (c)

Information systems for which government CERT evaluates data on cybersecurity events and cybersecurity incidents are complemented by information systems on the operation of which the provision of basic services depends.

Concerning Section 20 (i)

Legislative technical adjustment resulting from the need to add new letters to this provision.

Concerning Section 20 (j) and (k) to (n)

The government CERT acquires new competencies and related obligations under the directive in this provision. This provision is closely linked to Section 8, which regulates the reporting of cybersecurity incidents.

According to the law, as amended by this proposal, the government CERT: receives reports on cybersecurity incidents, evaluates them, provides methodological support, assistance and cooperation to the entities concerned, acts as a contact point, assesses vulnerabilities in the field of cybersecurity, transmits incident data to the NSA, acts as a CSIRT under the directive, cooperates with other CSIRTs, communicates with the relevant authorities of other Member States and, last but not least, receives voluntary reports of cybersecurity incidents.

By this it meets the requirements of Appendix I to the Directive:

- Monitoring of incidents at the national level – Section 20 (b), (c), (f), (g), (l).*
- Issuing early warnings and alerts, notifying and disseminating information on risks and incidents to relevant stakeholders – Section 20 (d), (e), (i), (n).*
- Response to incidents – Section 20 (d), (e).*
- Providing a dynamic analysis of risks and incidents and an overview of the situation – Section 20 (j).*
- Participation in the CSIRT network – Section 20 (m).*

By fulfilling the role of the CSIRT, the government CERT, which is part of the NBU, will also meet the requirements of the Directive for the participation of the CSIRT team in the CSIRT network pursuant to Article 12 of the Directive. The participation of representatives of the national CERT will be left to their discretion.

Article 9 of the Directive stipulates that each Member State shall set up one or more CSIRTs, but does not address that representatives of all CSIRTs of a Member State should be required to participate in the work of the CSIRT. The full participation of at least one CSIRT team is thus sufficient, which will be fulfilled by representatives of the government CERT. The provision regulates the procedure of the government CERT in the event that the reported cybersecurity incident has a significant impact on the continuity of the provision of basic services, or the impact on the provision of digital services in another Member State of the European Union. In such a case, in accordance with Article 14 (5), and therefore Article 16 (6) of the Directive, the power of a governmental CERT to inform the relevant authorities of other Member States of the incident is enshrined.

Article 20 of the Directive provides for a situation in which an entity which has not been designated as an operator of basic services and is not a provider of digital services detects and seeks to address the security of its information systems. In this case, it may voluntarily report the cybersecurity incident to the government CERT and work with the CERT to resolve the situation. In this case, the government CERT will process the report and, if its capabilities allow it and it is a cybersecurity incident with a significant impact, provide it as adequately as when a cybersecurity incident is reported to it by the basic service provider.

Based on the Cybersecurity Act, two CERT/CSIRT teams, **namely national and government, are compulsorily established in the Czech Republic.**

The operator of the national CERT is a legal entity with which NUKIB (formerly NBU) has entered into a public law contract (see Section 19 of the AoCS).

Government CERT (**GovCERT.CZ** – see <https://www.govcert.cz/>) is established according to law as part of the National Cyber and Information Security Agency (formerly under the responsibility of the NBU).

According to the Cybersecurity Act, the government CERT:

- **receives notifications of contact details** from the authorities and persons referred to in Section 3 (c) to (g) of the AoCS,
- **receives reports of cybersecurity incidents** from the authorities and persons referred to in Section 3 (c) to (g) of the AoCS,
- **evaluates data** on cybersecurity **events** and cybersecurity **incidents** from the critical information infrastructure, the basic service information system, significant information systems and other public administration information systems,
- **provides the bodies and persons** referred to in Section 3 (c) to (g) of the AoCS with **methodological support and assistance**,
- **provides cooperation** to the bodies and persons referred to in Section 3 (c) to (g) of the AoCS **in the event of a cybersecurity incident and cybersecurity event**,

Resolving security incidents is one of the main activities of the government team. When reporting a cybersecurity incident, the government team of GovCERT.CZ is ready to help IT specialists from a technical point of view, including providing advice for further preventive measures. In the event that it is found that one of the incidents targets more than one entity, the government team GovCERT.CZ is ready to coordinate a joint procedure for its resolution. [\[10\]](#)

- **receives suggestions and data** from the bodies and persons referred to in Section 3 of the AoCS and from other bodies and persons and **evaluates** these suggestions and data,
- **receives data from the operator of the national CERT** and evaluates such data,
- **receives data from authorities acting in the field of cybersecurity abroad** and evaluates such data,
- **according to data from the incident register** (see Section 9 (4) of the AoCS), it provides the operator of the national CERT, bodies acting in the field of cybersecurity abroad and other persons operating in the field of cybersecurity with data from the register of incidents,
- **assesses vulnerabilities** in the field of cybersecurity,
- **informs the relevant authority of another Member State, without disclosing the identity of the notifier, of a cybersecurity incident that has a significant impact** on the continuity of basic services in that Member State or affects the provision of digital services in that Member State, while maintaining the notifier's security and business interests,
- **receives reports of a cybersecurity incident from authorities and persons not referred to in Section 3 of the AoCS;** the government CERT processes the reports and, if its capabilities allow it and if it is a cybersecurity incident with a significant impact, it provides methodological support, assistance and cooperation to the authorities or persons affected by the cybersecurity incident,
- **act as a CSIRT** in accordance with Article 9 of the NIS Directive,
- **cooperates with CSIRTs of other Member States.**

In addition to the obligations explicitly set out in the Cybersecurity Act, the government CSIRT has set itself other tasks [\[11\]](#), including:

- **Data sharing** - GovCERT.CZ obtains a number of reports and data concerning potentially infected information systems in the Czech Republic in cooperation with various multinational organisations dealing with cybersecurity. It provides this information to other entities as part of proactive activities. Shared data is divided into the following projects:
- **BotnetFeed** – using this tool, data about end stations connected to botnet networks from C&C servers taken over are processed. To identify a potentially infected computer system, the IP range manager is given an IP address and information about the botnet in which it is integrated.
- **IHAP** (Incident Handling Automation Project), **MDM** (Malicious Domain Manager) – fragments of compromise indicators (IoCs) from various servers are collected within these projects. The most common indicators include phishing, brute force attacks, ids alerts, spam, scanning attempts, exploit vulnerabilities, malware, and many other types. Based on these data, short reports are prepared, which always contain the IP address of the compromised machine and a brief summary of the type of incident.

- **Shadowserver** – the project is focused on the continuous search for relevant information about vulnerabilities in cyberspace and the occurrence of these vulnerabilities at specific IP addresses.
- **Deployment of Honeypots**
- **Penetration testing**

This is a legal attempt to break into the tested systems. The result is a report of the test subject's security vulnerabilities, which is addressed exclusively to its owner, who will take appropriate security action based on the report.

Another option is to perform vulnerability scanning according to the OWASP (Open Web Application Security Project).

- **Information HUB**

On the govcert.cz website it is possible to find information, searches, analyses and articles concerning current threats and vulnerabilities related to systems in the Czech Republic. These documents are supplemented by regular monthly bulletins summarising significant security incidents in the Czech Republic and abroad.

- **Education and research activities**
- **Forensic laboratory and SCADA laboratory**

[1] Article 9 of NIS

[2] *Kdy nás kontaktovat*. [online]. [cit. 07/07/2018]. Available from: <https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/>

[3] *Služby CSIRT.CZ*. [online]. [cit. 07/07/2018]. Available from: <https://csirt.cz/page/2764/sluzby/>

[4] All tasks are taken from: *Služby CSIRT.CZ*. [online]. [cit. 07/07/2018]. Available from: <https://csirt.cz/page/2764/sluzby/>

[5] Act No. 127/2005 Sb., on Electronic Communications and on the Amendment of Certain Related Acts (the Electronic Communications Act), as amended.

[6] Act No. 269/1994 Sb., on the Criminal Register, as amended.

[7] Pursuant to Section 20 (1) of the Civil Code (CC), a legal person means ***“an organised entity that the law stipulates has legal personality or whose legal personality is recognised by law. Regardless of the subject of its activity, a legal person may have rights and obligations which are compatible with its legal nature.”*** The state is considered a legal entity in the field of private law. (Section 21 of the CC).

A legal entity can be a person of private or public law, depending on the interest in which the legal entity is established (Section 144 of the CC). From the point of view of civil law, corporations (see Section 210 et seq. of the CC), foundations (see Section 303 et seq. of the CC) and institutes (see Section 402 et seq.) are legal entities.

[8] The use of the institute of a public contract according to Section 160 et seq. of SŘ corresponds to the assumption that the operator of the national CERT will be a person of private law.

[9] See Article 9 of NIS

[10] *Poskytované služby*. [online]. [cit. 01/08/2018]. Available from: <https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/>

[11] All tasks are taken from: *Poskytované služby*. [online]. [cit. 07/07/2018]. Available from: <https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/>

3.2. Poland

CERT Polska is Computer Emergency Response Team which operates within the structures of Naukowa i Akademicka Sieć Komputerowa (Scientific and Academic Computer Network or NASK) – a research institute which conducts scientific activity, operates the national .pl domain registry and provides advanced IT network services. CERT Polska is the first Polish computer emergency response team. Active since 1996 in the environment of response teams, it became a recognised and experienced entity in the field of computer security. Since its launch, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. It also conducts extensive R&D into security topics.

In 1997, CERT Polska became a member of the international forum of response teams – FIRST, and since 2000 it has been a member of the working group of European response teams – [TERENA](#) TF-CSIRT and an associated organisation Trusted Introducer. In 2005 on the initiative of CERT Polska, a forum of Polish abuse teams was created - Abuse FORUM, while in 2010 CERT Polska joined [Anti-Phishing Working Group](#), an association of companies and institutions which actively fight on-line crime.

The main tasks of CERT Polska include:

- o registration and handling of network security incidents for Poland and the “.pl” domain name space;
- o providing watch & warning services to Internet users in Poland;
- o active response in case of direct threats to users;
- o cooperation with other CERT teams in Poland and worldwide;
- o participation in national and international projects related to IT security;
- o research activity in relation to methods of detecting security incidents, analysis of malware, systems for exchanging information on threats;
- o development of proprietary tools for detection, monitoring, analysis, and correlation of threat;
- o regular publication of CERT Polska Report on security of Polish on-line resources;
- o information/education activities aimed at increasing the awareness in relation to IT security;
- o performing independent analyses and testing solutions related to IT security.

Below is the full description of CERT Polska in accordance with RFC 2350 "Expectations for Computer Security Incident Response":

CSIRT Description for CERT Polska

=====

1. About this document

1.1 Date of Last Update

This is version 2.0, published on 04 March 2019.

1.2 Distribution List for Notifications

Currently CERT Polska does not use any distribution lists to notify about changes in this document.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the CERT Polska WWW site; its URL is

<https://www.cert.pl/wp-content/uploads/2017/12/rfc2350.txt>

Please make sure you are using the latest version.

1.4 Authenticating this document

This document has been signed with the CERT Polska PGP key. The signatures are also on our Web site, under:

<http://www.cert.pl/o-nas>

2. Contact Information

2.1 Name of the Team

CERT Polska

2.2 Address

CERT Polska

NASK

ul. Kolska 12

01-045 Warszawa

Poland

2.3 Time Zone

Central European Time (GMT+0100, GMT+0200 from April to October)

2.4 Telephone Number

+48 22 3808 274

2.5 Facsimile Number

+48 22 3808 399 (note: this is **not** a secure fax)

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

<cert@cert.pl> This is a mail alias that serves the human(s) on duty for CERT Polska.

2.8 Public keys and Other Encryption Information

CERT Polska has a PGP key, which KeyID is 969C0EB8 and which fingerprint is

DC34 CB6E CD73 C0B1 DC8C 8AE7 FD58 C59E 969C 0EB8

The key and its signatures can be found at the usual large public key servers.

2.9 Other Information

General information about CERT Polska, as well as links to various recommended security resources, can be found at <http://www.cert.pl/>

CERT Polska uses the following Facebook page to publish news about current activities <http://www.facebook.com/CERT.Polska>

CERT Polska posts short messages on current events to the following twitter accounts

http://www.twitter.com/cert_polska

http://www.twitter.com/cert_polska_en

2.10 Points of Customer Contact

The preferred method for contacting CERT Polska is via e-mail at <cert@cert.pl>; e-mail sent to this address will be handled by the responsible human. We encourage our customers to use PGP encryption when sending any sensitive information to CERT Polska.

If it is not possible (or not advisable for security reasons) to use e-mail, CERT Polska can be reached by telephone during regular office hours. Off these hours incoming phone calls are transmitted to an answering machine. All messages recorded are checked ASAP.

CERT Polska operates 24 hours a day, every day of the year.

If possible, when submitting your report, use the form mentioned in section 6.

3. Charter

3.1 Mission Statement

The mission of CERT Polska is to identify, analyse and mitigate threats targeting Polish internet users. As an essential part of the national cyber security system, CERT Polska contributes to ensuring cyber security at the national level.

3.2 Constituency

Constituency of CERT Polska is defined in Article 26 (1) of the Act of 5 July 2018 on the national cyber security system.

All legal entities and natural persons in Poland, with the exceptions of:

- entities subordinate to or supervised by the Minister of National Defence, including entities whose ICT systems or ICT networks are covered by a single list of facilities, installations, devices and services included in the critical infrastructure referred to in Article 5b, paragraph 7, subparagraph 1 of the Act of 26 April 2007 on crisis management,*
- companies of significant importance in terms of economy and defence, for whom the authority organising and supervising their performance of tasks for the defence of the state is the Minister of National Defence,*
- public finance sector entities referred to in Article 9, items 1, 8 and 9 of the Act of 27 August 2009 on public finance, with the exception of: research institutes, Office of Technical Supervision, Polish Air Navigation Services Agency, Polish Centre for Accreditation, National Fund for Environmental Protection and Water Management and regional funds for environmental protection and water management,*
- National Bank of Poland,*
- National Development Bank,*
- entities than listed in items 1 to 4 and paragraph 5, whose ICT systems or ICT networks are covered by a single list of facilities, installations, devices and services included in the critical infrastructure referred to in Article 5b,*

paragraph 7, subparagraph 1 of the Act of 26 April 2007 on crisis management.

Note that ANY incident regarding any host, network, legal entity or natural person in Poland MAY be reported to CERT Polska. Reports of incident beyond CERT Polska's constituency will be forwarded without undue delay to the relevant CSIRT, according to Article 26 (8) of the Act of 5 July 2018 on the national cybersecurity system.

3.3 Sponsorship and/or Affiliation

CERT Polska is financially maintained by the National Research Institute NASK which it is formally a part of.

NASK receives a specified-user subsidy from the part of the state budget assigned to the minister competent for digitalisation to fund operations of CERT Polska.

3.4 Authority

The Act of 5 July 2018 on the national cyber security system defines competencies and authority of "CSIRT NASK" - a role assigned to NASK in the national cyber security system.

Parts of that role, specifically addressing operational aspects such as:

- monitoring of cyber security threats at the national level,*
 - incident response,*
 - information sharing,*
 - participation in CSIRTs Network*
- are fulfilled by CERT Polska.*

4. Policies

4.1 Types of Incidents and Level of Support

CERT Polska is authorized to address all types of computer security incidents which occur, or threaten to occur, in its constituency.

The level of support given by CERT Polska will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the availability of CERT Polska's resources at the time, though in all cases some response will be made within two working days.

Incidents will be prioritized according to their apparent severity and extent.

Critical, significant and substantial incidents, as well as incidents in a public entity (as defined in Article 2 of the Act of 5 July on the national cyber security system) are coordinated by respective CSIRTs - including CERT Polska, according to their constituency.

Incident handling is the responsibility of individual entities.

However, under Article 26 of the Act of 5 July on the national cyber security system, in reasonable cases, at the request of operator of essential services, digital service providers, or public entities, CERT Polska may provide support in incident handling.

4.2 Co-operation, Interaction and Disclosure of Information

CERT Polska exchanges all necessary information with other CSIRTs, other entities included in the Polish national cyber security system, as well as with affected parties' administrators. No personal nor overhead data are exchanged unless explicitly authorized.

All sensitive data (such as personal data, system configurations, known vulnerabilities with their locations) are encrypted if they must be transmitted over unsecured environment as stated below.

4.3 Communication and Authentication

In view of the types of information that CERT Polska

deals with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to CERT Polska, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable level of trust. Within NASK, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5. Services

5.1 Incident Response

CERT Polska will provide incident response capabilities in the following areas:

5.1.1 Incident Triage

- Investigating whether indeed an incident occurred.*
- Determining the extent of the incident.*

5.1.2 Incident Coordination

- Determining the initial cause of the incident
(vulnerability exploited)*
- Facilitating contact with other sites which may be*

involved.

- *Facilitating contact with appropriate law enforcement officials, if necessary.*
- *Making reports to other CSIRTs*
- *Composing announcements to users, if applicable*

5.1.3 Incident handling

In some cases, limited support may be provided in technical incident handling, including malware and forensic analysis, threat hunting, evidence collection.

The extent of this support will depend on the type and severity of the incident, and the type of the affected entity.

5.2 Proactive Services

CERT Polska coordinates and maintains the following services to the extent possible depending on its resources:

- *Network security information sharing platform ("n6") available to all network administrators:*

<https://n6.cert.pl/>

- *Information services through the following channels:*

= website: <https://www.cert.pl/>

= Facebook website: <https://facebook.com/CERT.Polska>

= twitter: https://twitter.com/CERT_Polska (PL) and

https://twitter.com/CERT_Polska_en (EN)

- *Training and educational services*

CERT Polska organizes an annual SECURE conference covering current important security issues which is open for all interested parties.

CERT Polska contributes to NASK's activities in the area of awareness rising and education on cyber security.

5.3 Research and Development

CERT Polska provides tools and facilities to monitor and analyze threats.

<https://github.com/CERT-Polska>

<https://www.cert.pl/en/projekty/>

6. Incident Reporting Forms

CERT Polska had created a local form designated for reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out, although this is never required. The current version of the form is available from:

<https://incydent.cert.pl/>

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT Polska assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

3.3. Portugal

FIX IT

3.4. SUMMARY



SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

- 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 of network and information systems across the Union (the NIS Directive) was adopted by the European Parliament.
- The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:
 - Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a relevant national NIS authority,
 - cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
 - a culture of security across sectors that are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.
- The Member States have taken different approaches to implementing NIS.

- **The legislative framework of CSIRT/CERT teams in the Czech Republic** is partly set by the Cybersecurity Act. This act sets out the conditions for the existence of the national and government CSIRT/CERT team, but on the other hand does not restrict the establishment and existence of other CSIRT/CERT teams.
 - Based on the Cybersecurity Act, two CERT/CSIRT teams, namely national and government, are compulsorily established in the Czech Republic. Each of these teams has the rights and obligations specified by law (Section 17 et seq. of the AoCS).

- **The legislative framework of CSIRT/CERT teams in Poland**

The Act of 5 July 2018 on the national cybersecurity system distinguishes 3 national CSIRTs:

- CSIRT GOV - Computer Security Incident Response Team operating at the national level, led by the Head of the Internal Security Agency
- CSIRT MON - Computer Security Incident Response Team operating at the national level, led by the Minister of National Defense
- CSIRT NASK - the Computer Security Incident Response Team operating at the national level, led by the Scientific and Academic Computer Network - National Research Institute

- Other than that the Act mentions the following actors of the national cybersecurity system:
 - operators of essential services;
 - digital service providers;
 - CSIRT MON;
 - CSIRT NASK;
 - CSIRT GOV;
 - sectoral cybersecurity teams;
 - units of the public finance sector, referred to in article 1. 9 points 1-6, 8, 9, 11 and 12 of the Act of 27 August 2009 on public finances (Journal of Laws of 2017, item 2077 and of 2018, items 62, 1000 and 1366);
 - research institutes;
 - the National Bank of Poland;
 - Bank Gospodarstwa Krajowego;
 - the Office of Technical Inspection;
 - Polish Air Navigation Services Agency;
 - Polish Center for Accreditation;

 - The National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management;

- o commercial companies performing public utility tasks within the meaning of Art. 1 clause 2 of the Act of December 20, 1996 on municipal management (Journal of Laws of 2017, item 827 and JoL of 2018, item 1496);
- o entities providing cybersecurity services;
- o cybersecurity competent authorities;
- o Single Contact Point for cybersecurity;
- o the Government Plenipotentiary for Cybersecurity;
- o Cybersecurity College.

- **The legislative framework of CSIRT/CERT teams in Portugal**

FIX IT



KEY WORDS TO REMEMBER

- o cybersecurity
- o CSIRT/CERT
- o NIS directive
- o ENISA
- o Constituency
- o National and government CERT/CSIRT
- o Team collaboration



KNOWLEDGE CHECK QUESTIONS

- o Is there a hierarchy among CSIRT/CERT teams?
- o How is the scope of activity of a CSIRT/CERT team defined?
- o Who is the government CSIRT/CERT team?
- o Who is the national CSIRT/CERT team?
- o What are the roles and tasks of other CSIRT/CERT teams?
- o How about the constituency of CSIRT/CERT teams in your country?

4. Conclusion

We live in a time when information and communication technologies are already inextricably linked to every aspect of our being. A certain paradox is that we essentially do not have the opportunity to avoid this penetration and mutual interaction with ICT, which at the same time makes us more vulnerable.

As the volume of data and information stored in individual ISPs grows, the issues of their effective security, transfer or deletion are increasingly being addressed, not only on the basis of a contract entered into between the service provider and the end user, but also on the basis of emerging legislation.

States, organisations, but also individuals are increasingly aware that information and data represent significant potential, which is increasingly attacked by cyberattacks, whether with the aim of theft, damage, inaccessibility or deletion of data.

If we want to live in today's society and take advantage of its benefits, it is not possible to get rid of ICT and it definitely does not make sense to stop using these technologies. It is necessary to start learning how to use these technologies and services, how to avoid or at least eliminate the consequences of cyberattacks.

Many negative events can be avoided if individuals and organisations respect at least the basic principles of cybersecurity.

In cyberspace, as in the real world, there is no single type of security or protection that can be universally applied to everyone. If we want to address security, we need to address it comprehensively, and we need to tailor it to each individual.

Information and communication technologies are the most dynamically and massively developed field. Areas to which we should pay extreme attention in this context are user safety and education.

5. References

1. 2018 Data Breach Investigation Report. 11th Edition. [online]. [cit. 28/07/2018]. Available from: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf
2. Analýza rizik. [online]. [cit. 01/07/2018]. Available from: <https://www.vlastnicesta.cz/metody/analiza-rizik-risk/>
3. ANDRESS, Jason. *The Basics of Information Security*. 2nd Edition. Syngress. ISBN: 9780128007440
4. CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition*. London: Academic Press, 2004, p. 9 et seq.
5. CIA triad methodology. [online]. [cit. 10/07/2018]. Available from: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png
6. *Computer Security Incident Handling Guide* [online]. [cit. 13/08/2018], p. 6. Available from: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
7. *Cybersecurity*. [online]. [cit. 06/07/2018]. Available from: <https://en.oxforddictionaries.com/definition/cybersecurity>
8. *Cybersecurity*. [online]. [cit. 06/07/2018]. Available from: <https://www.merriam-webster.com/dictionary/cybersecurity>
9. *Cyberthreat*. [online]. [cit. 06/07/2018]. Available from: <https://en.oxforddictionaries.com/definition/cyberthreat>
10. *Definition of Cybersecurity - Gaps and overlaps in standardisation*. [online]. [cit. 10/12/2017]. 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) [cit. 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 Security Categorization of Federal Information and Information Systems*. National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cit. 10/12/2017]. Available from: <https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf>
13. FRANK, Libor. *Bezpečnostní studia*. [online]. [cit. 10/07/2018]. 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]. [cit. 01/07/2018]. 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]. [cit. 13/01/2018]. Available from: <http://panmore.com/the-cia-triad-confidentiality-integrity-availability>
16. *Hrozba*. [online]. [cit. 28/07/2018]. 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 p. ISBN 978-0-8232-4456-0. p. 41.
18. JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3rd updated edition. Prague: AFCEA, 2015, p. 23. [online]. [cit. 10/07/2018]. Available from: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovník-kyberneticke-bezpecnosti---druhe-vydani/>
19. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Prague: Grada Publishing, a. s., 2007. p. 21 et seq
20. KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti*. [online]. [cit. 21/07/2018]. 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. *Kybernetická bezpečnost: Co s tím?* [online]. [cit. 29/06/2018]. Available from: <http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html>
23. *Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma*. [online]. [cit. 29/06/2017]. Available from: http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san
24. MAREŠ, Miroslav. *Bezpečnost*. [online]. [cit. 10/07/2018]. Available from: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

25. MATUROVÁ, Jana a Miroslav VALTA. *Prevence rizik - provádění kontrol technického stavu technických zařízení*. [online]. [cit. 01/07/2018]. Available from: <https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickyh-zarizeni>
26. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. [online]. [cit. 01/07/2018]. Available from: <https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf> p. 5
27. *Parkerian Hexad*. [online]. [cit. 20/08/2016]. Available from: <https://vputhuseeri.wordpress.com/2009/08/16/149/>
28. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, p. 37.
29. POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace*. [online]. [cit. 06/07/2018]. Available from: <https://www.cybersecurity.cz/data/pozar2.pdf>
30. PROSISE, Chris and Kevin MANDIVA. *Incident response & computer forensic, second edition*. Emeryville: McGraw-Hill, 2003, p. 13
31. Před čím chránit? – Bezpečnostní hrozby, události, incidenty. [online]. [cit. 06/07/2018]. Available from: <https://www.kybez.cz/bezpecnost/pred-cim-chranit>
32. *Příchod hackerů: příběh Stuxnetu*. [online]. [cit. 01/07/2018]. Available from: <https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/>
33. RAK, Roman. Homo sapiens versus security. ICT fórum/PERSONALIS 2006. [presented on 27/09/2006]. Prague (a conference presentation).
34. SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570039>
35. SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570035>
36. SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570047>
37. SCHNEIER, Bruce. [online]. [cit. 18/07/2018]. Available from: <https://www.azquotes.com/quote/570040>
38. *Směrnice NIS*. [online]. [cit. 01/07/2018]. Available from: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN>
39. SVOBODA, Ivan. *Řešení kybernetické bezpečnosti*. Přednáška v rámci CRIF Academy. (23/ 09/2014)
40. ŠÁMAL, Pavel et al. *Trestní zákoník II. § 140 až 421. Komentář*. 2. Publ. Prague: C. H. Beck, 2012, p. 2308
41. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. p. 20 et seq.
42. *Tajné služby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin*. [online]. [cit. 29/06/2017]. Available from: <http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin>
43. *The complete breadth of CGI Cyber Security services*. [online]. [cit. 10/07/2018]. Available from: <https://mss.cgi.com/service-portfolio>
44. *Traffic Light Protocol (TLP) Definitions and Usage*. [online]. [cit. 13/01/2018]. Available from: <https://www.us-cert.gov/tlp>
45. VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Krizové řízení při nevojenských krizových situacích*. Prague: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 01/07/2018]. Available from: <http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskyh-krizovych-situacich-pdf.aspx>
46. WAIŠOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0
47. *WannaCry se neměl vůbec rozšířit. Stačilo, abychom používali Windows Update*. [online]. [cit. 27/06/2017]. 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. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích*. Prague: Státní nakladatelství technické literatury, 1960. 148 p.
49. *Základní pojmy*. [online]. [cit. 10/07/2018]. Available from: <https://www.kybez.cz/bezpecnost/pojmoslovi>
50. ZEMAN, Petr et al. *Česká bezpečnostní terminologie: Výklad základních pojmů*. [online]. [cit. 10/07/2018]. Available from: <http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048>. p. 13
- Zpráva o stavu kybernetické bezpečnosti za rok 2017*. [online]. [cit. 29/06/2018]. Available from: <https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf>