# The project "Current cyber threats in the Czech Republic and their elimination"

Petr Hrůza[1], Oldřich Luňáček[1]

[1] University of Defence, Kounicova 65,
62100 Brno, Czech Republic
{petr.hruza, oldrich.lunacek}@unob.cz

**Abstract.** The article describes the current status of the project "Current cyber threats in the Czech Republic and their elimination." The project is focused on the identification of cyber threats and the types of cyber-attacks which are relevant for the Czech Republic and includes a description of the possible consequences of certain real cyber-attacks and is accompanied by a description of possible measures, methodologies and tools to combat the most serious forms of cyber-attacks. The result of the project will be draft of measures of their elimination (both the state and the private sector).

**Keywords:** Cyberspace, cyber-attack, cybercrime, cyber security, critical information infrastructure, management, information system.

## 1 Introduction

Scope and continuously expansion of usage of information and communication system in society increases the company's dependence on their proper function. The success of individual entities (companies, organizations, institutions) is dependent on the protection of these systems, which in its content and meaning may be the target of attacks from various interest groups and individuals whose goal is to gather information, data. Or their aim should be that the organization will be somehow damaged.

## 2 Subject and objectives of the project

The object of the project is the identification of cyber threats and the types of cyber-attacks relevant to the Czech Republic. Attention will also be devoted to describing the potential consequences of some real cyber-attacks. Finally, a description will be made of possible measures, methodologies and tools to combat the most serious forms of cyber-attacks. The project goals also include in particular the proposal to their elimination (both the state and the private sector). The attention will be also focused on the motivation and goals of the attackers in cyberspace, especially focusing on attacks against communication and information systems and elements of the state's critical infrastructure, critical information infrastructure (CII), communications and information infrastructure. Attention will be paid to the security of services which are used by major information systems of the state and elements of the critical infrastructure of the state), and technical and personnel possibilities of potential attackers. One of the major objectives of the project will be the design of a system for sharing of information on national and international levels, and inclusion bodies responsible for combating cyber threats, cyber-terrorism and cyber-crime in this system based on existing or newly defined competencies as National Cyber Security Centre (NCSC).

The project was designed for two years from 2014 to 2015. They are solved intermediate objectives in each year. For each sub-goal were identified basic processes, which will help to fulfil intermediate objectives. Within these processes were identified individual activities and these activities were then assigned to individual researchers.

The project aims for 2014 were:

- Analysis of the Czech Republic's preparedness for the current cyber threats.
- Proposal of the technical, organizational, and legislative or other measures that are required to improve the situation in the fight against cyber threats in the Czech Republic.
- Proposal of the crisis scenarios in the event of a serious disruption of critical information infrastructure.
- Analysis of the weaknesses of CII and possible ways how to detect attacks, including their impact on the extent of primary and secondary damage and description of the possibilities of the fight against these attacks.
- Identification of the appropriate software and describe other measures necessary for the detection, analysis of cyber-attacks on CII.
- Identification of the appropriate software for forensic analysis of elements of CII.

The project objective for 2015 is:

- Description the use of government and the national workplace Computer Emergency Response Team (CERT) / Computer Security Incident Response Team (CSIRT) in the area of the prevention of cyber threats to CII, cyber terrorism and crime.
- Proposal of the most appropriate tool for the popularization and awareness of cyber threats and protection methods to the general public.
- Creation of the knowledge-based cyber protection of CII.
- Research on the psychological profile of the attacker.
- Development and the certification of the methodology "Draft procedures for detecting, monitoring, reflecting, evaluation and documentation of various forms of attacks and their objectives in terms of destabilization of the CII of the Czech Republic."
- Write and publish educational book about cyber security.

## 3 Performed analysis

Within the project were mainly in 2014 conducted several analyses focusing on cyber protection of the Czech Republic:

- Analysis of readiness for the current cyber threats.
- Analysis of vulnerabilities and detect various forms of attacks, including their impact on the extent of primary and secondary damage and description of the possibilities of the fight against these attacks.
- Draft technical, organizational, and possibly other legislative measures needed to improve the situation in the fight against cyber threats in the country.
- Draft a crisis scenario in the event of a serious disruption of CII.
- Possible uses workplace CERT / CIRT.

## 4 Cyber protection knowledge base of critical information infrastructure of the Czech Republic

Cyber protection knowledge base of CII of the Czech Republic is one of the project outputs, which can be the backbone for supporting information / knowledge systems that enable to:

- Create a logically structured content from which you can easily generate documentation for various decisions, such as evaluation of draft legislation and standards, and procedures for dealing with incidents (Who? What? Where? When? How? Why should we do?
- Share and link contents of the documents, information resources and systems at various levels of generalization / abstraction, usage different languages and different terminology. On that basis, it should be identified duplicates, gaps and inconsistencies in terminology, legislation and regulations. By this way it will be created a semantic basis for cooperation and training of experts in the field of cyber and energy security.
- Analyse the effects / impact of actions in the area of cyber security to business affected subjects and create vivid and consistent basis for negotiations cooperating entities and drafting of legislation and standards.
- Evaluate information on incidents and identify new forms and sources of threats (technological, social, economic, environmental, political), new vulnerabilities and gaps or inconsistencies in procedures for the prevention or crisis situations.
- Monitor information from different sources and putting them into the context of possible threats to critical infrastructure and to distribute them to the relevant bodies for evaluation.

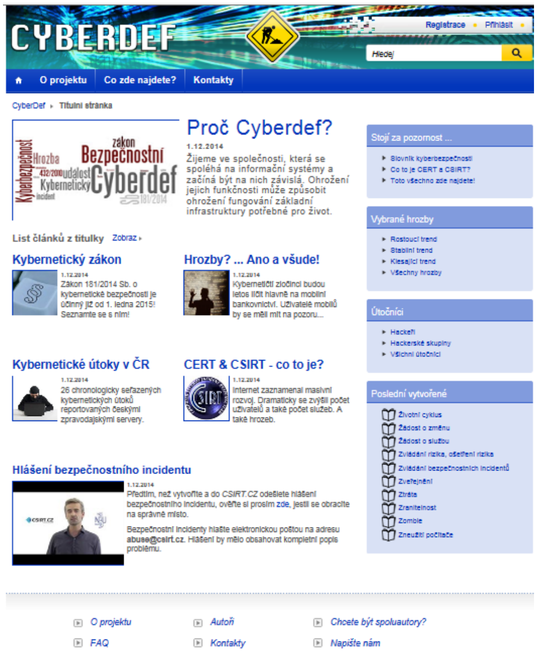
The backbone of the knowledge base will be ontology of CII cybersecurity, which defines the basic concepts and will include links to national and European legislation. Ontology will also include the methodology, and description of the bodies and systems CII, including their vulnerabilities, threats and risks.

Knowledge base will also contain rules as taxonomy for categorizing incidents, events, and other documents (CII documentation systems, procedures averting threats, information about tools for their management, links to service providers CII protection and resolving incidents.

For the purposes of the implementation of this activity was used technology knowledge system ATOM3. As part of this structure was designed knowledge base in the form of ontology and there is gradually filling the knowledge base of the individual outputs of research activities with gradual adjustments of the knowledge base. Into the knowledge base was inserted dictionary of the cybersecurity, in draft mode it was supplemented with new links and concepts. It has been established active link to freely available source of information and vulnerabilities (National Vulnerability Database of www.nist.gov), threats (bulletins and reports from www.govcert.cz and www.csirt.cz) and hacker attacks (Hacking News from www. softpedia.com). These resources are continually updated.

In 2015, has been performing an analysis of documents produced within the project and documents from external sources. Based on this analysis and consultation with the personnel from NCSC was stated focus primarily on the knowledge base glossary of cybersecurity supplemented by connections and relationships between concepts. Selected concepts will be accompanied by specimens or lists (DB hacker groups, APT, etc.). The selected concepts will be supplemented by references to specific examples (law on cybersecurity, legislative documents, and etc.). They were developed following partial results, which will be in the coming months to be further supplemented and developed:

- On the base of consultations with representatives NCSC was expanded number of indexed external sources of information, and continue to have their continuous updating (the date of this report were downloaded and indexed more than 290,000 documents from more than 4,500 Internet resources).
- The database of selected attackers was created (the date of this report contained 119 and 140 hacker groups from more than 20 countries) and rules for automated extraction of these invaders from textual data were created. These rules were applied to selected external sources.
- Rules have been developed for the automatic extraction of known types of vulnerabilities from textual data, and these rules have been applied to selected external sources.
- It was created a prototype of a web interface that allows external users to browse the contents of a knowledge base with an automatically generated link to the documents from external sources, including the highlight of extracted entities (attackers, vulnerability, and others) - www.atom.cyberdef.cz.



Proč Cyberdef?

1.12.2014

Žijeme ve společnosti, která se spoléhá na informační systémy a začíná být na nich závislá. Ohrožení jejich funkčnosti může způsobit ohrožení fungování základní infrastruktury potřebné pro život.

Kybernetický zákon

1.12.2014

Zákon 181/2014 Sb. o kybernetické bezpečnosti je účinný již od 1. ledna 2015! Seznamte se s ním!

Hrozby? ... Ano a všude!

1.12.2014

Kybernetičtí zločinci budou letos ličit hlavně na mobilní bankovnictví. Uživatelé mobilů by se měli mít na pozoru...

Kybernetické útoky v ČR

1.12.2014

26 chronologicky seřazených kybernetických útoků reportovaných českými zpravodajskými servery.

CERT & CSIRT - co to je?

1.12.2014

Internet zaznamenal masivní rozvoj. Dramaticky se zvýšil počet uživatelů a také počet služeb. A také hrozeb.

Hlášení bezpečnostního incidentu

1.12.2014

Předtím, než vytvoříte a do *CSIRT.CZ* odešlete hlášení bezpečnostního incidentu, ověřte si prosím zde, jestli se obracíte na správné místo.

Bezpečnostní incidenty hlašte elektronickou poštou na adresu abuse@csirt.cz. Hlášení by mělo obsahovat kompletní popis problému.

**Fig. 1.** Web application www.atom.cyberdef.cz

## 5 Methodology of finding weaknesses and for the fight against cyber attacks

Within the framework of the project activity was created an analysis of existing approaches, the concept and methodology framework, including the preparation of the initial proposal was designed. Proposal of the methodology was structurally divided into analytical, design and implementation part. Methodical procedure sets out the general structural requirements for each area of security (physical, informational, administrative, personnel security, crisis management and planning / business continuity) and requirements for the management structure system of the cybersecurity that have a major impact on the level of risk and vulnerability in CII and major systems.

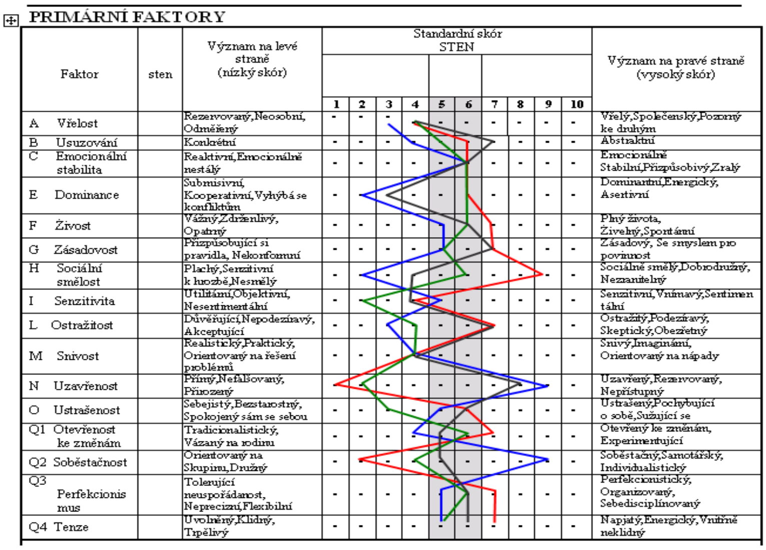
These facts should enable to optimize the practical process of finding vulnerabilities, and detection, response and reaction to cyber-attacks (cyber security incident). In the next phase the draft will be internally commented and supplemented. Subsequently, the guidance document will be confronted with the acceptor and supplemented on the basis of formulated requirements.

# 6 Research on the psychological profile of the attacker

In the area of the psychological profile of the attacker were implemented actions, which were aimed on identification of the psychological aspects of people working in the field of cyber security. These were selected people who can be categorized as professionals-professional hackers, and they agreed with their participation in the investigation. They voluntarily decided to agree with the processing of the results without giving personal data. Inquiries and the results were compared with a random selection of several people who are not professional's workers cyber services, but according to them are able to implement the content of the work of hackers.

We can describe perpetrators from several different perspectives on their personality, structure, and especially from the point of view of their activities motivation. It is usually referred, that hackers are people which committed action with the result and impact in an area of cyber activity. Significance of the hacker has undergone a remarkable evolution over the years. While earlier it was synonymous for the person with whom it looks with reverence, today most people still consider designation for a computer criminal. For true hackers is typical of their social behaviour, used language, the recognition of moral values and of course the actual implementation of hacking.

Within the project was carried out several psychological examinations of people working in the field of cyber security. The examination result of each participant survey was drawn up in tables of results with verbal interpretations and final recommendations by the process and the limiting criteria for the selection of potential employees. Based on the findings we proposed a series of tests for possible recruitment in the area of information security.



PRIMÁRNÍ FAKTORY

| Faktor | sten | Význam na levé straně (nízký skór) | Standardní skór STEN | | | | | | | | | | Význam na pravé straně (vysoký skór) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
| A Vřelost | | Rezervovaný,Neosobní, Odměřený | | | | | | | | | | | Vřelý,Společenský,Pozorný ke druhým |
| B Usuzování | | Konkrétní | | | | | | | | | | | Abstraktní |
| C Emocionální stabilita | | Reaktivní,Emocionálně nestálý | | | | | | | | | | | Emocionálně Stabilní,Přizpůsobivý,Zralý |
| E Dominance | | Submisivní, Kooperativní,Vyhýbá se konfliktům | | | | | | | | | | | Dominantní,Energický, Asertivní |
| F Živost | | Vážný,Zdrženlivý, Opatrný | | | | | | | | | | | Plný života, Živelný,Spontánní |
| G Zásadovost | | Přizpůsobující si pravidla, Nekonformní | | | | | | | | | | | Zásadový, Se smyslem pro povinnost |
| H Sociální smělost | | Plachý,Senzitivní k hrozbě,Nesmělý | | | | | | | | | | | Sociálně smělý,Dobrodružný, Nezranitelný |
| I Senzitivita | | Utilitární,Objektivní, Nesentimentální | | | | | | | | | | | Senzitivní,Vnímavý,Sentimentální |
| L Ostražitost | | Důvěřující,Nepodezíravý, Akceptující | | | | | | | | | | | Ostražitý,Podezíravý, Skeptický,Obezřetný |
| M Snivost | | Realistický,Praktický, Orientovaný na řešení problémů | | | | | | | | | | | Snivý,Imaginární, Orientovaný na nápady |
| N Uzavřenost | | Přímý,Nefalšovaný, Přirozený | | | | | | | | | | | Uzavřený,Rezervovaný, Nepřístupný |
| O Ustrašenost | | Sebejistý,Bezstarostný, Spokojený sám se sebou | | | | | | | | | | | Ustrašený,Pochybující o sobě,Sužující se |
| Q1 Otevřenost ke změnám | | Tradicionalistický, Vázaný na rodinu | | | | | | | | | | | Otevřený ke změnám, Experimentující |
| Q2 Soběstačnost | | Orientovaný na Skupinu,Družný | | | | | | | | | | | Soběstačný,Samotářský, Individualistický |
| Q3 Perfekcionismus | | Tolerující neuspořádanost, Nepreciznı́,Flexibilní | | | | | | | | | | | Perfekcionistický, Organizovaný, Sebedisciplinovaný |
| Q4 Tenze | | Uvolněný,Klidný, Trpělivý | | | | | | | | | | | Napjatý,Energický,Vnitřně neklidný |

**Fig. 2.** Comparison of the results of four tests at probands

Personality manifestations in the questionnaire 16 PF can be summarized into several consecutive factors that create significant values of evidenced manifestations by examined people and represent characters that can be evaluated as identical or in very close relation.

Personality structure of person which is skilled in computer technology is marked by the expression of their personal interests and ambitions to dominate the technique and be myself achieving the objectives of the regulator, which represents a certain uniqueness of its importance and the mission and capabilities. It is necessary to ask the question as to how much the person will be realized only in the field of science and its application in practice, or when this imaginary limit will be exceeded.

One from the possibility manifestations is a personal expression to achieve the general effort in the recognition of detecting the possibility of further qualitative changes in the field that have not been discovered and their presentation brings inner satisfaction and recognition capabilities (altruistic aggression - aggression aimed at protecting other). This may constitute a contribution to the creation of new security features into organization cyber security and the overall process of the system.

The other real possibility is a creation of the personal plan for use as unknown process for the overcoming of barriers within the program and creation of warning and defence. The knowledge and disposition will be used in the opposite intention. Either as an anonymous warning of the system error (inner satisfaction of their abilities and with no harmful consequences), or as cross-border activities of general standards in order to harm the client (organizations, companies, government interest etc.). In this case it is example of the act of aggression angry (angry aggression), leading to damage or destruction of the target objects.

The identification of manifestations of personality in various stages of activity is a complex task that needs to be solved gradually with regard to the hierarchy of their own activities. It must be respected starting skills and knowledge and experience in normal conditions of work and also in critical and extreme situations.

Planning activities and ensuring of the continuity with the fulfilment requirements for cyber security management structure have a major impact on the level of risk and vulnerability, especially in the context of critical information infrastructure and relevant information systems. These facts should allow virtually optimize the process of finding vulnerabilities, detection, feedback and reaction to cyber-attack.

## 7 Conclusion

Cyber security is a very serious problem. Today's society is dependent on the use of information and communication systems. In addition to many benefits, including greater efficiency, speed the transfer of information, revocation time spatial barriers, we must realize the fact that in case of rejection of these systems can be a company, organization or country paralyzed. Cyber security must be a top priority, because there's neglect of the company may feel the dire consequences. Defence needs to start when planning any activity and must move seamlessly into practical measures that ultimately became part of the conduct of each individual. As the above mentioned reasons, a project aimed at solving problems related to cyber security is of great importance. It is very necessary to focus on the identification of cyber threats and the types of cyber-attacks are relevant to the country. Solving this problem is relevant today for all developed countries.

## References

1. DRAPELA, Viktor, J. Přehled teorií osobnosti. Praha: Portál, 1997, 175 pp. ISBN 80-7178-766-3 (1997)
2. CHALUPA, Bohumír. Studie z kognitivní psychologie. Brno: Littera, 2011. 199 pp. ISBN 978-80-85763-65 (2011)
3. ČÍRTKOVÁ, Ludmila. Policejní psychologie. Praha: SUPPORT, 1996. 2.vyd, 304 pp. ISBN 80-902164-0-4 (1996)
4. BELZ, Horst, SIEGRIST, Marco. Klíčové kompetence a jejich rozvíjení. Praha. Portál, 2001. 1.vyd. 376 pp. ISBN 80-7178-479-6 (2001)
5. SMÉKAL, Vladimír. Pozvání do psychologie osobnosti. Brno: BARRISTER PRINCIPAL, 2002, 1.vyd. ISBN 80-85947-80-3 (2002)
6. ŠTIKAR, Jiří, RYMEŠ Milan, RIEGEL, Karel, HOSKOVEC, Jiří. Psychologie ve světě práce. Praha: UK-Karolinum, 2003. ISBN 80-246-0448-5 (2003)
7. HRUZA, Petr, Kybernetická bezpečnost. Univerzita obrany, Brno, Dukase s.r.o, 2012, ISBN 978-80-7231-914-5 (2012)
8. HRUZA, Petr, PITAŠ, Jaromír, ŠANDA, Jaroslav, BRECHTA, Bohumil, Kybernetická bezpečnost II. Univerzita obrany, Brno, Monika Promotion s.r.o, Praha 2013, ISBN 978-80-7231-931-2 (2013)
9. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). [online]. [cit. 2015-06-30]. http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/
10. Deloitte, Tovek, Univerzita obrany: Dílčí studie řešení projektu CYBERDEF, 2014-2015. (2014)