AARMS Vol. 17, No. 3 (2018) 115–130.

Milestones Related to the Development of Organizational Aspects of Cybersecurity and Protection against Cyber-Threats in the Czech Republic

Oldřich KRULÍK[1]

Although the Czech Republic belongs to the most "internetised" countries in the world, its information and communication security policy (as well as the protection of the critical information infrastructure) lagged behind for a relatively long time, when compared to most of the remaining European countries. Building the hierarchy regarding the umbrella teams of the Cybernetic Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT) type (regardless of whether we call them governmental, national or otherwise) was unthinkable without the contribution of the private sector that substituted many functions of the state in this field. The whole process can be understood as an interaction of international and national pressures appealing to the solution of the situation.

Keywords: *CERT/CSIRT, information and communication security policy, critical information infrastructure protection, measures, recommendations*

CERT/CSIRT Teams and their Role

The integral part of the preventive and active protection of cyberspace is a consistent and effective solution of security incidents, including the elimination of their causes and consequences. Network administrators and users must be prepared and must have functional structures, effective procedures, rules and technical resources to minimize the respective damages as quickly as possible. [40]

In many countries, the issue of cyberspace incidents handling is solved by the so-called CERT or CSIRT teams. [25]

The services provided by the CERT/CSIRT teams can include both *reactive* and *proactive services* (training, alerting against attacks, identification of system's weaknesses, security audits, consultations regarding the specific software, traffic monitoring tools and services, many other activities etc.).

The minimum range of such activities is, however, the addressing of respective security incidents to cover the term "response" (or "ability to respond"), contained in the term CERT/CSIRT itself. [8] [42]

The umbrella (national, governmental) CERT/CSIRT team in each country is a focal point for the individual users (firms, citizens, public institutions) to address with a specific problem

[1] Mgr., Ph.D., Police Academy of the Czech Republic in Prague, assignment; e-mail: "krulik@polac.cz

that they cannot handle themselves. In case of a cyber-attack from abroad, communication between top CERT/CSIRT teams in individual countries of the world is often faster and more efficient than police cooperation channels (and is also usable in communicating with countries with no existing mutual police cooperation channels).

CERT/CIRT Teams in the World and in Europe

The situation with regard to the existence of CERT/CSIRT teams in Europe is as follows:

- "At least some" CERT/CSIRT teams exist in each European Union member state, as well as in many other European countries.
- Some teams or institutions of such nature run the non-governmental (academic) subjects (sometimes with some state support). Iceland can serve as an example. [19]
- In many countries, CERT/CSIRT teams provide some form of service for the widest public (awareness, education, alerts etc.). Germany, the German Federal Office for Information Security can serve as an example. [4] [5]
- In a number of countries, there is a number of CERT/CSIRT platforms serving only individual private customers (firms, internet service providers, universities).
- In some countries, CERT/CSIRT teams serve mostly governmental and military structures (e.g. Turkey).
- In some countries, such structures do not exist at all.

It should be also emphasized that a particular platform will become a CERT/CSIRT team only at the moment when other existing CERT/CSIRT teams will accept it and establish channels of basic mutual cooperation.

The way of the status of a CERT/CSIRT team, however, must not be complicated, if the following key information is clearly and truthfully declared:

- Who is the founder and operator of the team?
- Basic contact information (e-mail for immediate communication, phone number, postal address, etc.).
- Scope (scope of responsibility) of the team.
- Overview of the offered services.

To get an idea about the "density" of the CIRT/CSERT teams in Europe, the most suitable are the overviews (maps) created by the European Union Agency for Network and Information Security (in 2007, the only platform for the Czech Republic mentioned was CESNET–CERTS). [7]

One of the key prerequisites for the functionality of national CERT/CSIRT teams is its high-quality and efficient *links to foreign counterparts*, which is typically formalized through "accreditation" in key transnational structures:

- The world-wide association Forum of Incident Response and Security Teams (FIRST, interconnecting about 300 teams). [15] [33]
- Organizational and certification site for the Task Force on Computer Security Incident Response Teams (TF-CSIRT) Europe, associated with Trans-European Research and Education Networking Association (TERENA). [53]

- The European Union Agency for Information Technology (ENISA), which focuses on information security from the point of view of manufacturers and operators. [21]

During the accreditation, the "identity, credibility and functionality" of a particular CERT/CSIRT team is verified. This means, in practice, that the individual team has to document its own work, including all relevant information, as well as to guarantee generally accepted patterns of behaviour and response. Preparation for such a process usually takes several years, the process itself several months (structured usually to three tiers):

- recognition (acceptance) of the entity ("listed" status);
- accreditation;
- certification (according to relevant ISO standards).

Through becoming a member of these organizations, the CERT/CSIRT teams will get the way for important and useful information, exchange and cooperation. The forum of Incident Response and Security Teams organizes a five-day conference once a year, TF-CSIRT meetings are held three times a year. The meetings are always hosted by one of the European teams. In January 2008, for example, this meeting was held in Prague, in the Czech Republic. [24]

It is also necessary to emphasize that the national environment in each country is so specific that no foreign model can be copied for the purposes of another country.

A "Tough Way" to Determine the "Umbrella Hierarchy" of CERT/CSIRT Teams in the Czech Republic

"Prehistoric Times"

The Czech Republic certainly does not belong to the countries that would be understood as pathfinders for a CERT/CSIRT team in Europe. This only illustrates the little emphasis connected to information security issues in the Czech Republic in the recent past. [29] [55]

Although the Czech Republic has been connected to the Internet since 1993 or 1994, for a long time it was impossible to talk about a comprehensive security policy in this area.

The topic of establishing a team (hierarchy of teams) of the CERT/CSIRT-type in the Czech Republic was one of the "chronic" aspects of the efforts related to the information security agenda in the Czech Republic for more than 10 years.

The need to create a CERT/CSIRT team in the Czech Republic was mentioned already in the document called *Crime Reduction Policy in Relation to Information Technologies* adopted by the Ministry of the Interior of the Czech Republic in 2001.[2] Very important is

[2] Task: *"To initiate and support CERT-type activities as a non-governmental association of qualified experts informing other professionals about security issues and responding to ongoing attacks."* Responsible body: Ministry of the Interior of the Czech Republic, in cooperation with the Office for Public Information Systems of the Czech Republic, the Chairman of the Government Council for State Information Policy, Ministry of Justice of the Czech Republic, Ministry of Culture of the Czech Republic, Ministry of Education, Youth and Sport of the Czech Republic and the National Security Authority of the Czech Republic; Deadline: 30 June 2002.

the fact that responsibility for information infrastructure in the Czech Republic has long been the subject of competence struggle (mostly "negative competence struggle", when no institution was willing to take the responsibility for the respective agenda).

Between the years 2003 and 2007, the Czech Republic had the Ministry of Informatics of the Czech Republic that was more or less responsible for the cybersecurity agenda. After the dissolution of this Ministry, the agenda was not completely transmitted to another institution, and it caused a period of disputes that had an impact on the situation in the respective area for many years.

In addition, the Ministry of Informatics of the Czech Republic entrusted itself with important tasks specified in a document called *Action Plan Implementing the National Security Information Security Strategy of the Czech Republic*.[3] [52]

Pilot Teams and its Competitors

In 2006 and 2007, the process of building the National CERT/CSIRT team continued through the Consortium, which won the tender of the Security Research Project of the Ministry of the Interior of the Czech Republic for the period 2007–2010 (project called *Cyber Threats in the Security Interests of the Czech Republic*).[4] [48]

The consortium also included the "academic" CESNET–CERTS team, the first domestic CERT/CSIRT team with relevant practical experience, already connected to the relevant transnational platforms. The process of building a *coordinating model workplace-team of CERT/CSIRT-type* (CSIRT.CZ) within the academic network CESNET started in the mid-2007. Its pilot operation was launched on 3rd April 2008. The team has been continuously organizing methodical education (with the participation of a number of private entities, representatives of the Security Information Service, the Police of the Czech Republic and the National Security Authority). During its existence, CSIRT.CZ has gained a reputation at home and abroad, but its formal international accreditation was blocked due to the uncertainty about its future after the end of the project.

A certain blind alley in this regard was the parallel activity of the private firm Relsie, which concluded in a Memorandum of Understanding with the Ministry of the Interior of the Czech Republic in *February 2007* (describing the vision to build a CERT/CSIRT facility, called CERT.ORG). But this company was, in fact, an unknown player for foreign partners, so it cannot reach its goals. [46]

For foreign counterparts, the situation in the Czech Republic became even more unclear. Two competing "CERT/CSIRT" teams were confusing for them.

---

[3] Task: *"To implement the Early Warning and Response System. Establish a National Center for Management, Monitoring and Analysis of the Security Environment of the Information and Communication Systems of the Czech Republic. Establish a CERT-type team with a cross-national competence."* Responsible authority: originally the Ministry of Informatics of the Czech Republic, later the Ministry of the Interior of the Czech Republic, in cooperation with the Security Information Service of the Czech Republic. Deadline: no later than in 2008. Task: *"To establish monitoring of effectiveness of proposed countermeasures in the CERT team."* Responsible authority: Ministry of the Interior of the Czech Republic. Deadline: no later than in 2008.

[4] The Consortium was formed by the individual faculties of the Charles University, Prague, the Czech Technical University, CESNET (Internet Service Provider for numerous academic institutions) and NESS Czech Company.

In *September 2008*, the security team of NIC.CZ[5] (CZ.NIC-CSIRT) was created. The effectiveness of this team has been so far the most advanced of all teams of this type in the Czech Republic. A number of incidents was vigorously resolved, not only "archived" through this team.

Despite all partial shifts, *political consensus* on practical steps towards building a national CERT/CSIRT-type team *had not been achieved since 2007 until the beginning of 2010*. At a later stage, the responsibilities (and costs) associated with this step were refused by the Ministry of the Interior of the Czech Republic, the Ministry of Defense of the Czech Republic as well as the National Security Authority of the Czech Republic. It is no wonder that these delays caused embarrassment not only in the domestic expert community. [14] [32]

Overcoming the Competence Vacuum

The situation (at least for some time) started to clarify after the introduction of the "caretaker government" in the Czech Republic (June 2009 to July 2010), especially due the Resolution of the National Security Council of *5th January 2010* No. 4, *On the Analysis of the Current Level of Cyber Security of the Czech Republic*. This document imposed the main competences and responsibilities for the next steps regarding the cybersecurity agenda unambiguously on the Ministry of the Interior of the Czech Republic. [50]

Following the aforementioned Resolution of the National Security Council, a new Cyber Security Department was established within the Ministry of the Interior of the Czech Republic at the beginning of 2010. [35] [44] [47]

One of its first registrable activities was the participation at the session of the CSIRT.CZ Working Group on *25th March 2010* (interconnecting representatives of major internet service providers, content providers, state security forces, Czech Telecommunication Office, CZ.NIC, NIX.CZ[6] and the academic sector). [26] [47]

But no tangible steps were then taken by the state (the Ministry of the Interior of the Czech Republic), and the initiative was taken over by the private sector, especially by the administrator of the Czech national domain, CZ.NIC. At its own expenses and responsibility, it created a CERT/CSIRT-type team that used the company's background and served the widest public. [34] This situation continued until 16th December 2010, when a Memorandum on Computer Security Incident Response Team of the Czech Republic was signed between the Ministry of the Interior of the Czech Republic and the CZ.NIC,

[5] CZ.NIC is an association of legal persons founded in 1998 by the leading Internet service providers in the Czech Republic. The main activity of the association is the operation of the domain name register .cz. At present, the association is improving the domain management system, supporting new technologies beneficial to the Internet infrastructure in the Czech Republic. CZ.NIC is a member of international organizations that associate with similar organizations around the world (CENTR, ccNSO and others) and also a member of EURid, a European .eu domain. [43]

[6] NIX.CZ (Neutral Internet Exchange) is a platform that interconnects Internet Service Providers in the Czech Republic to interconnect their Internet networks. This association is formed by telecommunication companies operating in the Czech Republic because they have a common interest in ensuring that their computer networks are mutually interconnected and their customers can quickly communicate via the Internet within the Czech Republic. Members of the platform contribute together to the technologies that can improve the exchange efficiency and securely. [41]

according to which the CZ.NIC temporarily (from the 1st of January 2011) took the agenda of the national security team CSIRT.CZ. [10]

The Memorandum also stated that the Ministry of the Interior of the Czech Republic addressed the status of CERT/CSIRT teams within the state administration and sought to support the inclusion of CSIRT.CZ in international structures, in particular by confirming the status of CSIRT.CZ as a "National CSIRT Team". Furthermore, it coordinates the activities of CSIRT.CZ, evaluates information received from CSIRT.CZ in case CSIRT.CZ suspects that the incident could have an impact on the state or state administration systems. The Ministry of the Interior of the Czech Republic also had the right to request an audit of the performance of CSIRT.CZ activities. [34]

As it was already stated above, CSIRT.CZ was a research project carried out by CESNET that ended on 31st December 2010. As of *1st January 2011*, under the agreement of the Cyber Security Department of the Ministry of the Interior of the Czech Republic, the CESNET and CZ.NIC, took the responsibility for the relevant equipment to be able to maintain the continuity of CSIRT.CZ. [34]

CSIRT.CZ, perceived as a "national CSIRT team" since its creation, became in 2010 a co-worker of the European Union Agency for Information Technology (Point of Contact for the Czech Republic). [54]

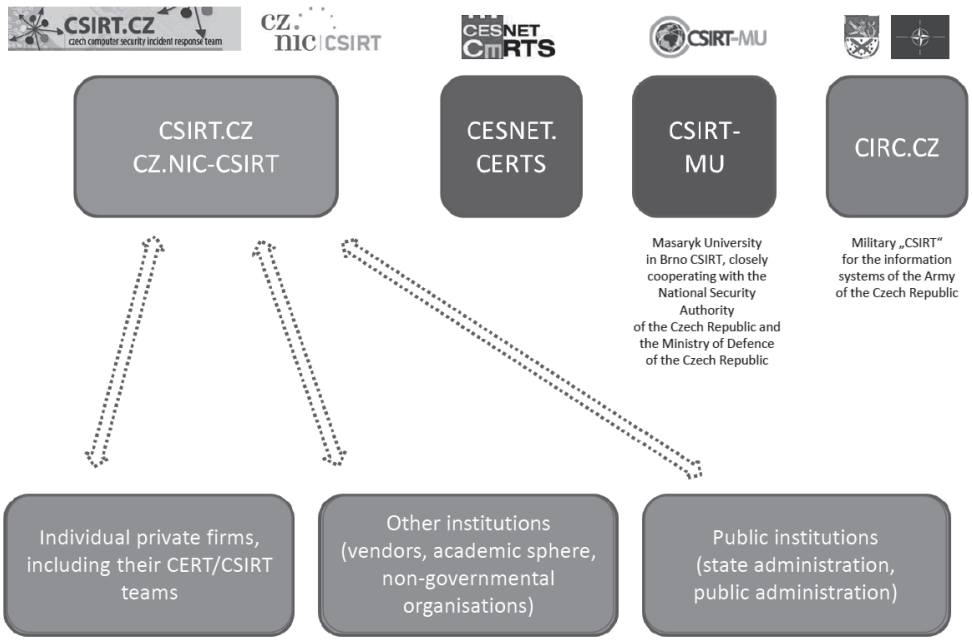

Figure 1. *Perspectives regarding the various stages of possible development of umbrella CERT/CSIRT Teams in the Czech Republic in the years 2010–2011.*
[Edited by the author.]

In connection with the aforementioned facts, the National Security Council of the Czech Republic discussed on *28th February 2011* the document describing the current situation

regarding cyber security issues in the Czech Republic. Due to the importance of the agenda, the Cyber Security Strategy (elaborated by the Ministry of the Interior of the Czech Republic) was submitted to the National Security Council and then to the Government by *30th June 2011.*

The perspectives regarding the various stages of possible development, as expected in the beginning of 2011, are described by the following visualizations (several CERT/CSIRT-type teams, two of them open to the general public questions and proposals). [16]

Transfer of the Agenda to the National Security Authority of the Czech Republic

The "coordination role" of the Ministry of the Interior of the Czech Republic did not last long. On the basis of the Resolution of the Government of *19th October 2011* No. 781, on the Umbrella "National Authority" Responsible for the Area of Information Security Regarding the Public Sector of the Czech Republic, the relevant competence was transferred to the National Security Authority of the Czech Republic. The new administrator was already, whether alone or in co-operation with other stakeholders, very active in many relevant areas. [22]

The Government approved of the establishment of the National Cyber Security Center as a part of the National Security Authority of the Czech Republic. [30]

At the same time, the Government of the Czech Republic set up the Cyber Security Council as a part of the National Security Council and the National Cyber Security Center as a part of the National Security Authority of the Czech Republic. At the same time, the Government imposed a number of specific tasks on the National Security Authority of the Czech Republic. The relevant Cyber Security Strategy for the years *2012 to 2015* was already elaborated also under the coordination of the National Security Authority of the Czech Republic. [49] [36] [37] [38] [49] [58]

In January 2012, CSIRT.CZ reviewed the period of one year of its operation with the following conclusion: The CSIRT.CZ team officially represented the Czech Republic in the world (in the relevant international forums and is also the first contact point for foreign counterparts). In July 2011 it organized the pilot training seminar *The World of Internet and Domains*, intended for employees of the state administration and members of the security forces, especially the Police of the Czech Republic. The team was cooperating with the Internet Service Providers in the Czech Republic. Special attention was paid to the practical issues that should help (especially) the police investigators to orient themselves in the issue of basic forms of cybercrime and to learn to address directly the specific subjects that can support their work. Participants of the pilot course were also the intelligence operations specialists, judges etc. In 2011, CSIRT.CZ was invited to the Law Enforcement Authorities Expert Working Group of the European Union Agency for Information Technology. The work of this expert group resulted in a document, mapping the experience raised from the interconnection of law enforcement and cybersecurity experts, and suggesting a set of recommendations. [6] [12] [20]

This cooperation did not end in 2012. Due to the fact that the National Security Authority of the Czech Republic was not able to launch its Gov-CERT, that was already "under construction" in the former premises of the Ministry of Defense in Brno), the decision was

made to sign another Memorandum, moving this "turning point" until 2015. Until then, the national cyberspace will be dominated by the CZ.NIC. [9] [57]

"The current solution to cyberspace protection is unsatisfactory. CSIRT.CZ *of the CZ. NIC is good and professional, but this fact cannot substitute the absence of the Gov-CERT team, which must be a part of the security system and the protection of cyberspace … The* members of the national CSIRT […] has no powers or responsibilities that are key to handling security threats. *CSIRT has only a consultative role […] Four half-time CZ.NIC specialists are responsible for the security of the Czech cyberspace, but they do not have any competencies as well as the right to handle classified information […] With time, they can be supported and even replaced by the employees of the Gov-CERT in Brno, but without any support in the legislation, it still will be a group of experts with no power to enforce their will."* [27]

Proposal of the Modified Institutional Framework

The proposal, with one of the first drafts of the Act on Cyber Security (February 2012), included the framework for the provision of information security functions in the Czech Republic. It was envisaged to create two umbrella CERT/CSIRT teams in the Czech Republic.

1. The *"National" CERT* will be built on the fundament of the CZ.NIC (CSIRT.CZ), with the use of the experience of the model workplace-team operated by CESNET (CSIRT.CZ), according to the research project of the Ministry of the Interior of the Czech Republic. The "National" CERT will establish or deepen existing links with and among similar teams within the Network Monitoring Cluster and, in the first phase, perhaps, also regarding the public sector. CSIRT.CZ will be involved in resolving cyber-security incidents in networks operated in the Czech Republic. CSIRT.CZ will also provide co-ordination assistance, but not physical support, to resolve individual incidents (but this assistance will not be provided directly to end users). CSIRT.CZ will collect and evaluate data on reported incidents and report respective incidents to those responsible for operating the individual network(s) that is (are) the source(s) of the incident, in accordance with the severity of the incident. CSIRT.CZ will fulfil the role of so-called National Point of Contact (PoC), as well as the center of education and dissemination of cyber security related education. It will also assist to establish the CERT/CSIRT teams in networks operated in the Czech Republic, including help regarding the establishing of co-operation connections with foreign/global security platforms. [34]
2. At the same time (or later) the construction of the *"Government" CERT* team (GovCERT.CZ) would be launched. This team would be primarily designed to monitor government networks and (public) critical information infrastructure, or to coordinate and methodologically run other sub-centers of this type that operate or will operate within specific public institutions.[7]

[7] The National Cyber Security Center will pursue efforts to protect networks primarily within public institutions, such as ministries, energy companies, hospitals or the Czech National Bank. The National Center for Cyber Security (in its embryonic condition) is directly subordinated to the Director of the Office.

In connection with the construction of this workplace-team, it will be especially necessary[8] to interconnect both platforms, as well as ensure their connection to the "military" team of a similar type (CIRC.CZ).

Both teams are to be understood first and foremost as partners who "lighten each other's burden". However, GovCERT would have a veto right in a number of questions, but at the same time it does not possess such technical and human resources (it is reportedly a problem to fill the relevant positions in public institutions), such as the National CERT that was built mainly on the basis of CZ.NIC.

The whole process is planned to go from "more limited" to "more ambitious" goals.

The relevant experts saw this proposal as a shift in the positive direction (compared with many years of inactivity in the past).[9] The limits related to the involved bodies (important and not-important public administration information systems, and "selected" service providers and network operators) were not entirely clear.

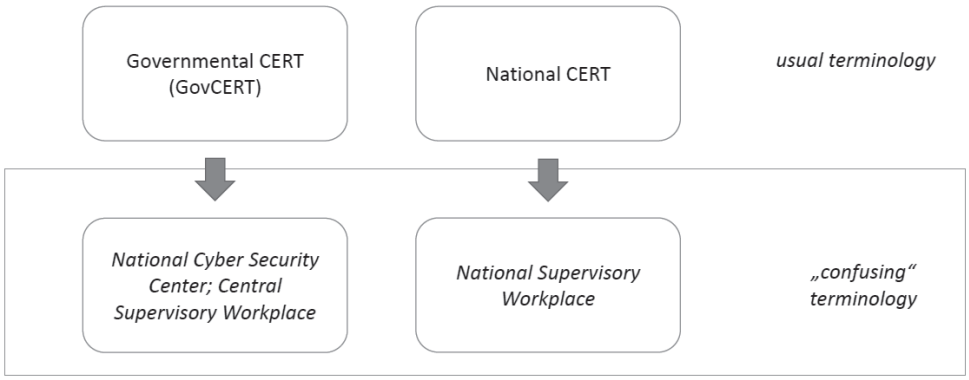

Figure 2. *Mutual ties and connection among individual CERT/CSIRT-like platforms in the Czech Republic, proposal from February 2012.* [Edited by the author.]

This vision has been widely commented by the domestic expert community as somewhat unusual: "In the world of information security, there are certain common terms (see, for example, outputs of the European Union Agency for Information Technology) […] according to which the 'National CERT or CSIRT' is a body, which stands on the top of the whole hierarchy in a particular country, and coordinates the other CERTs/CSIRTs. It is also the primary contact point for communication with CERTs/CSIRTs in other countries, and is also the country's principal representative in cyber-security related international organizations. In addition to 'national' CERTs or CSIRTs, there are still 'governmental' CERT/CSIRT teams that take care of those systems that are serving to the public administration bodies (state and local government) […] Typically, they have somewhat

[8] Due to the fact that there are several platforms in the Czech Republic already bearing the name CERT or CSIRT, it was decided that this "governmental" concept would differentiate (as in other countries) by the prefix "Gov" (derived from the word "government" or "governmental"). In addition, this term indicates the "superiority" of such a platform over the other CERTs (CSIRTs) existing within the state.

[9] At the same time, it is said that this concept could be improved and reshaped according to developments in countries that are more developed in the field of information security (for example, Germany). [3] [5]

different powers (and modes of operation) than the national teams. […] In the Czech Republic, in the proposal of the Cyber Security Act, what is usually 'governmental', on the contrary, refers to 'national' (and what is usually 'national' is referred to as 'central') […] in such a way that the authors of the proposal do not use the 'settled' terminology. […] Let's note one more thing: the 'National Supervisory Workplace' ('governmental' CERT) will be 'plugged in' inside another workplace called National Cyber Security Center (the only contact point for foreign partners). And this National Cyber Security Center is also 'plugged in' the National Security Authority of the Czech Republic as its organizational component." [45]

This begs for a rhetorical question: Will our foreign counterparts understand such an unconventional structure, if a serious incident occurs?

The management of the CSIRT.CZ and NIC.CZ were aware of this situation and tried to "calm down" similar negative or hesitating comments: "Teams designated as governmental and national have a very specific role in the CERT/CSIRT security infrastructure. Teams referred to as government are usually intended to oversee the networks of state administration, self-government and so-called critical infrastructure of the country. National teams usually fulfil the role of the National Point of Contact, sharing information with other teams abroad, and with the entities and organizations of their country […] A similar model is currently being used in the Czech Republic: The National CSIRT of the Czech Republic, fulfils the role of the governmental team, at least temporarily, according to the Memorandum signed in 2012." [6]

Gradual Stabilization, the Way to the National Cyber and Information Security Agency (Years 2012 to 2017)

On *19th December 2014* the regulations implementing Act No. 181/2014 on Cyber Security were published in the Collection of Acts: [51]

- Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures.
- Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria.
- Decision of the Government No. 315/2014 Coll. which amends the Decision of the Government No. 432/2010 Coll. on the Criteria for the Determination of the Elements of the Critical Infrastructure.

Act No. 181/2014 Coll. on Cyber Security and on the Amendments of the Related Acts (Cyber Security Law) after many and many discussions and changes, came into force on *1st January 2015*. The Act on Cyber Security is "based" on two principles: the first principle is to minimize the interference with the rights of private persons; the second is the principle of the individual responsibility for the security of the respective information systems. The Act came into force together with implementing regulations. [1] [2]

August 2017: The National Cyber and Information Security Agency (NCISA) became the central body of state administration for cyber security, including the protection of classified information in the area of information and communication systems and cryptographic protection. It is also in charge of the public regulated service of the Galileo satellite system.

It was created on the basis of Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Act).

National Cyber and Information Security Agency with its 120 employees took over the agenda of the National Security Authority of the Czech Republic that previously fell under the responsibility of the National Cyber Security Center that had been operating since 2011. The National Cyber and Information Security Agency's headquarter in Brno is in offices that previously served the National Cyber Security Center.

The situation in the Czech Republic grew closer to what is considered a standard in advanced European countries.

Main areas of the activity of the *National Cyber and Information Security Agency* are as follows: [39]

- operating of the Government CERT (GovCERT.CZ);
- cooperation with other domestic CERT/CSIRT teams;
- cooperation with international CERT/CSIRT teams;
- drafting of security standards for information system regarding critical information infrastructure and "Important Information Systems" (defined by law);
- support of education in the field of cyber security;
- research and development in the area of cyber security;
- protection of classified information in the field of information and communication systems and cryptographic protection.

The National Cyber and Information Security Agency operates the National Public Regulated Service Center (NCPRS), which fulfils the task of the so-called Competent Public Regulated Service Authority; it is one of the services provided by the European satellite system Galileo.

A new building in the barrack premises in Brno is planned to be built that will serve almost 400 staff members. The new office should be opened in 2023.

Conclusion

The Czech Republic is a relatively highly "internetised" country, where projects such as Data Boxes (state-guaranteed e-mail like communication system) and CzechPoint (offices for dissemination of state-guaranteed data and confirmed documents) are strongly promoted. But the security aspect of the whole issue remained for a long time behind the "edge of interest", and the whole country was in this regard understood by its foreign counterparts as an "untrusted partner".

Public sector institutions within the Czech Republic, for a long time, have only been looking after their own "cyberspace-sections" and the nationwide structure remained rather in the hands of active private sector players.

Only after 2011 the country invested more in a coordinated way of protecting its information infrastructure.

Table 1. *Weak points that took place in the history of the Czech Republic's cybersecurity related effort.* [Edited by the author.]

Weak points that took place in the history of the Czech Republic's effort	Proposals regarding cybersecurity issues
A protracted long-standing negative competence dispute where no resort or authority wanted to accept new costly and complicated agenda.	Resolute political (governmental) decision in this regard.
Only formal and rhetorical "fulfilment" of necessary tasks and demands of the transnational and foreign counterparts.	Efforts realistically meet individual requirements, being aware of their importance.
Non-standard terminology, problematic for both home and foreign/transnational counterparts.	Use of standard terminology as much as possible.
"Waiting tactics" regarding the relevant private actors.	Sincere public-private cooperation, with clearly defined rules.
When co-operation with private players started, its results were bodies without formal competencies.	Delegating unambiguously specified competencies to renowned and trusted private players.
Rigidity in relation to the possible employment of top-level (and adequately paid) experts in the state administration.	Accepting the need to remunerate top experts adequately.
Total underestimation and under-dimensioning of the topic.	Accepting the theme of cyber security as today's major priority, the failure of which would lead to serious and quantifiable negative effects regarding the state and society.

Instead of Conclusion: Recommendations Related to the Issue of Cybersecurity

As part of the "umbrella" cybersecurity institutions in the Czech Republic, it is necessary to address specific aspects of collection and distribution of information about threats from/to participating centers, as well as creation of a register of incidents, threats and vulnerabilities accessible by relevant entities to enhance the active protection of the cyberspace of the Czech Republic. [17] [18] [28]

It is also necessary to clarify the relevant communication and competence flows set within the Czech Republic as well as regarding the communication abroad. [56]

In addition to building a hierarchy at the national level, a clear hierarchy of responsibility for information security within the Police of the Czech Republic should be built. The qualified interconnection of the professional and strong team with sufficient equipment and staff cannot be perceived only in terms of the structure of the Police, but it is necessary to point out the existing need for co-operation with other bodies of state administration and commercial sphere.

Outside the Police of the Czech Republic, it is necessary to establish the links of the direct cooperation with the intelligence services, the critical infrastructure elements and the IT security specialist in the private sphere.

In all concerned public institutions, unambiguous contact points should be created regarding the topic of information security (which should remain stable regardless any personnel and organisational turbulence). Stakeholders from each institution need to exchange relevant experience on a regular basis (or even daily), or even create a joint "knowledge fund".

References

[1] *On Cyber Security and Change of Related Acts (Act on Cyber Security).* https://nukib.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf (Downloaded: 27.06.2018)

[2] *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* Praha: National Cyber and Information Security Agency, 2015. www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf (Downloaded: 27.06.2018)

[3] *Bundesamt für Sicherheit in der Informationstechnik*. www.bsi.bund.de (Downloaded: 20.06.2018)

[4] *Bundesamt für Sicherheit in der Informationstechnik.* www.bsi.bund.de/EN/Home/home_node.html (Downloaded: 20.06.2018)

[5] *Bundesamt für Sicherheit in der Informationstechnik.* www.buerger-cert.de/ (Downloaded: 20.06.2018)

[6] *CSIRT.CZ a jeho první rok fungování v roli Národního CSIRT České republiky.* 12. 1. 2012. http://csirt.cz/page/992/csirt.cz--a--jeho-prvni-rok-fungovani-v-roli-narodniho-csirt-ceske-republiky/ (Downloaded: 20.06.2018)

[7] *CSIRTs by Country – Interactive Map*. Attiki: European Union Agency for Network and Information Security, s.d. www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (Downloaded: 24.06.2018)

[8] *CSIRTs in Europe.* Attiki: European Union Agency for Network and Information Security, s.d. www.enisa.europa.eu/topics/csirts-in-europe (Downloaded: 24.06.2018)

[9] *CZ.NIC a Národní bezepčnostní úřad podepsali nové memorandum o spolupráci.* 19.12.2012. www.nic.cz/page/1308/cz.nic-a-nbu-podepsali-nove-memorandum-o-spolupraci/ (Downloaded: 20.06.2018)

[10] *CZ.NIC ohlídá kybernetickou bezpečnost České republiky.* 16.12.2010. www.nic.cz/page/830/cz.nic-will-watch-over-cybernetic-security-of-the-czech-republic/ (Downloaded: 20.06.2018)

[11] CZ.NIC převezme systém řešení bezpečnostních incidentů CSIRT. *České noviny* (online), 16.12.2010. www.monitoruji.cz/it-pocitace/349997/cz-nic-prevezme-system-reseni-bezpecnostnich-incidentu-csirt (Downloaded: 20.06.2018)

[12] Česká kybernetická jednotka CSIRT bojuje proti Anonymous. *Živě.cz* (online), 02.02.2012. www.monitoruji.cz/it-pocitace/565556/ceska-kyberneticka-jednotka-csirt-bojuje-proti-anonymous (Downloaded: 20.06.2018)

[13] Českou republiku střeží před kyberútokem čtyři lidé na půl úvazku. *Aktuálně.cz* (online), 21.12.2011. www.monitoruji.cz/it-pocitace/523094/cr-strezi-pred-kyberutokem-ctyri-lide-na-pul-uvazku (Downloaded: 20.06.2018)

[14] DOČEKAL, D.: CSIRT.cz přichází. Kyberzločincům navzdory. *Lupa.cz* (online), 04.04.2008. www.lupa.cz/clanky/csirt-cz-prichazi-kyberzlocincum-navzdory/ (Downloaded: 20.06.2018)

[15] *Forum of Incident Response and Security Teams.* www.first.org/ (Downloaded: 20.06.2018)

[16] HNÍK, V., KRULÍK, O.: *Okolnosti, související s budováním pracoviště typu CERT v České republice.* (Unpublished document for the purposes of the Cybersecurity Department of

the Ministry of the Interior of the Czech Republic). Prague: Cybersecurity Department of the Ministry of the Interior of the Czech Republic, 2010.

[17] HNÍK, V., KRULÍK, O., POŽÁR, J.: Česká republika na rozcestí (I). *Security World*, 1 (2011), 44–47.

[18] HNÍK, V., KRULÍK, O., POŽÁR, J. Česká republika na rozcestí (II). *Security World*, 2 (2011), 44–47.

[19] HNÍK, V., KRULÍK, O., POŽÁR, J.: Zajišťování informační bezpečnosti na Islandu jako inspirace pro Českou republiku. In. JIRÁSEK, P. (ed.): *Kybernetické útoky na informační systémy.* Prague: AFCEA, 2012. www.cybersecurity.cz/data/hnik.pdf (Downloaded: 20.06.2018)

[20] HOŠT, O.: Trendy v bezpečnosti 2012: soukromí, Facebook, mobilní platby a stará dobrá havěť. *Lupa.cz* (online), 02.03.2012. www.lupa.cz/clanky/trendy-v-bezpecnosti-2012-soukromi-facebook-mobilni-platby-a-stara-dobra-havet/ (Downloaded: 20.06.2018)

[21] *Index Inventory. European Union Agency for Network and Information Security.* Attiki: European Union Agency for Network and Information Security, s.d. www.enisa.europa.eu/cert_yinventory/index_inventory.htm (Downloaded: 24.06.2018)

[22] *Informace k usnesení vlády České republiky č. 781 ze dne 19. října 2011*. Praha: Národní bezpečnostní úřad České republiky, 2011. www.nbu.cz/cs/aktuality/994-informace-k-usneseni-vlady-ceske-republiky-ze-dne-19-rijna-2011-c-781/ (Downloaded: 20.06.2018)

[23] Jak CSIRT.CZ došel k akreditaci. *Lupa.cz* (online), 01.11.2011. www.monitoruji.cz/it-pocitace/510651/jak-csirt-cz-dosel-k-akreditaci (Downloaded: 20.06.2018)

[24] January 2008 FIRST Technical Colloquium. *Forum of Incident Response and Security Teams.* Prague, 27–31 January, 2008. www.first.org/events/colloquia/jan2008 (Downloaded: 20.06.2018)

[25] JIROVSKÝ, V., HNÍK, V., KRULÍK, O.: Základní definice, vztahující se k tématu kybernetické bezpečnosti. *Security Magazine*, 03–04 (2007), 46–49.

[26] KHUDHUR, P.: Ministerstvo vnitra chce zřídit CSIRT, vládní pracoviště pro bezpečnost IT. *Security World* (online), 21.05.2007. http://securityworld.cz/aktuality/ministerstvo-vnitra-chce-zridit-csirt-vladni-pracoviste-pro-bezpecnost-it-2498 (Downloaded: 20.06.2018)

[27] KOVALÍK, J.: Česko se začne před kyberútoky bránit až v roce 2015. *DataRama* (online), 06.12.2011. http://datarama.aktualne.centrum.cz/clanek.phtml?id=723306 (Downloaded: 20.06.2018)

[28] KRULÍK, O.: Návrhy a doporučení pro oblast informační bezpečnosti. *Bezpečnostní situace v České republice*. (CD-ROM) Praha: Ministerstvo vnitra České republiky, 2012. (ISBN 978-80-260-3275-5)

[29] KRULÍK, O, HNÍK, V.: Zahraniční inspirace, související s tématem kybernetických hrozeb. *Policista*, 10 (2007), annex, I–XII.

[30] *Legislation.* Praha: National Cyber and Information Security Agency, s.d. https://nukib.cz/en/legislation/legislation/ (Downloaded: 27.06.2018)

[31] MACÍCH, J.: CZ.NIC od ledna přebírá agendu CSIRT.CZ. *Lupa* (online), 17.12.2010. www.lupa.cz/zpravicky/cz-nic-od-ledna-prebira-agendu-csirt-cz/ (Downloaded: 20.06.2018)

[32] MALÝ, O.: Stát chce bojovat s kyberzločinem. *Lidové noviny* (online), 10.02.2010. www.cesnet.cz/sdruzeni/napsali-o-nas/2010/02/20100210_Lidove_noviny.html (Downloaded: 20.06.2018)

[33] *Members around the World.* Forum of Incident Response and Security Teams (FIRST), s.d. www.first.org/members/map (Downloaded: 20.06.2018)
[34] Memorandum on Computer Security Incident Response Team České republiky. *CSIRT.CZ* (online), 27.05.2011. www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf (Downloaded: 20.06.2018)
[35] Ministerstvo vnitra představí návrh řešení kybernetické bezpečnosti České republiky. *Český rozhlas* (online), 15.03.2010. www.rozhlas.cz/zpravy/spolecnost/_zprava/706944 (Downloaded: 20.06.2018)
[36] *Národní bezpečnostní úřad České republiky.* www.nbu.cz/cs/ (Downloaded: 20.06.2018)
[37] *Národní centrum kybernetické bezpečnosti se představuje a nabízí zajímavé pracovní příležitosti*. Praha: České vysoké učení technické, 2011. http://oi.fel.cvut.cz/en/node/621 (Downloaded: 20.06.2018)
[38] *Národní centrum kybernetické bezpečnosti*. www.govcert.cz/cs/ (Downloaded: 20.06.2015)
[39] *National Cyber and Information Security Agency.* https://nukib.cz/en/ (Downloaded: 27.06.2018)
[40] NĚMEČKOVÁ, K., KRULÍK, O., POŽÁR, J., HNÍK, V.: Vývoj, související s budováním pracovišť typu CSIRT/CERT v České republice. *Ochrana & Bezpečnost*, 3 (2012), 1–42. http://ochab.ezin.cz/O-a-B_2012_C/2012_C_09_nemeckova.pdf (Downloaded: 20.06.2018)
[41] *Neutral Internet eXchange.* www.nix.cz/cs (Downloaded: 20.06.2018)
[42] *New Guide on Cyber Security Incident Management to Support the Fight against Cyber Attacks.* Attaki: European Union Agency for Network and Information Security, 2011. www.enisa.europa.eu/news/enisa-news/new-guide-on-cyber-security-incident-management-to-support-the-fight-against-cyber-attacks (Downloaded: 20.06.2018)
[43] O sdružení. *CZ.NIC* (online) www.nic.cz/page/351/ (Downloaded: 20.06.2018)
[44] *Odbor kybernetické bezpečnosti.* Praha: Ministerstvo vnitra České republiky, s.d. www.mvcr.cz/clanek/odbor-kyberneticke-bezpecnosti.aspx (Downloaded: 20.06.2018)
[45] PETERKA, J.: Jaký bude zákon o kybernetické bezpečnosti. *Lupa.cz* (online), 22.02.2012. www.lupa.cz/clanky/jaky-bude-zakon-o-kyberneticke-bezpecnosti/ (Downloaded: 20.06.2018)
[46] Pilotní kurz CERT – TERENA. *relsie.cz* (onlie), 2010. www.relsie.cz/rj/pilotni-kurz-cert-terena (Downloaded: 10.02.2013)
[47] *Pracovní skupina CSIRT.CZ o vládním bezpečnostním pracovišti CSIRT.* CESNET, 30.02.2010. www.cesnet.cz/doc/tisk/2010/tz100330.html (Downloaded: 20.06.2018)
[48] *Problematika kybernetických hrozeb.* Praha: Ministerstvo vnitra České republiky, 2009. www.mvcr.cz/clanek/vysledky-projektu.aspx (Downloaded: 20.06.2018)
[49] *Rada na svém zasedání dne 23. XI. 2011 mimo jiné přijala usnesení o harmonogramu budování Národního centra kybernetické bezpečnosti.* Brno: Rada pro kybernetickou bezpečnost a Národní centrum kybernetické bezpečnosti, 2011. www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/ (Downloaded: 20.06.2018)
[50] *Report from the National Security Council Session of 5th January 2010 (Záznam ze schůze Bezpečnostní rady státu ze dne 5. ledna 2020).* Praha: Government of the Czech Republic, 2010. www.vlada.cz/cz/ppov/brs/cinnost/zaznamy-z-jednani/zaznam-ze-schuze-brs-konane-dne-5--ledna-2010-66950/ (Downloaded: 20.06.2018)

[51] ROHEL, V.: *Kybernetická bezpečnost z pohledu státu*. Brno: Národní centrum kybernetické bezpečnosti, 2014. https://konferencesecurity.cz/images/archiv/2014/for-download/Security-2014---M4-2---Rohel.pdf (Downloaded: 27.06.2018)

[52] SVOBODOVÁ, M.: Realizace Národní strategie informační bezpečnosti České republiky. *ISSS Conference 2006.* Hradec Králové: Ministerstvo informatiky České republiky. http://slideplayer.cz/slide/3295272/ (Downloaded: 25.06.2018)

[53] *TF-CSIRT Membership*. Amsterdam: Trans-European Research and Education Networking Association, 2012. www.terena.org/activities/tf-csirt/membership.html (Downloaded: 20.06.2018)

[54] *The Czech Republic*. Attiki: European Union Agency for Information Security. www.enisa.europa.eu/activities/cert/security-month/pilots/czech-republic (Downloaded: 20.06.2018)

[55] *TRANSITS: CSIRT Training.* Amsterdam: Trans-European Research and Education Networking Association, s.d. www.terena.org/activities/transits/ (Downloaded: 20.06.2018)

[56] *Trusted Introducer for CSIRTs in Europe*. www.trusted-introducer.org/ (Downloaded: 20.06.2018)

[57] *Vládní CERT.* Praha: Národní bezpečnostní úřad České republiky, s.d. www.govcert.cz/cs/govcert/ (Downloaded: 20.06.2015)

[58] *Zprávy Ministerstva vnitra o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky.* (Statistiky kriminality – dokumenty) Praha: Ministerstvo vnitra České republiky, s.d. www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx (Downloaded: 20.06.2018)