CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC
FOR THE 2011 – 2015 PERIOD

The 2011 – 2015 Cyber Security Strategy of the Czech Republic is linked to the Security Strategy of the Czech Republic and reflects challenges of a modern information society. The Strategy represents an institutional framework, which constitutes a part of the Czech Republic's security system. The framework document marks the beginning of an active national cyber defense policy, which must be continuously evaluated and updated. The awareness of ICT security challenges on the part of every individual, operator, administrator, university, company or institution is a fundamental prerequisite of being able to keep the cyberspace reliable and secure. The Czech Republic regards cyber security as an essential part of everyday use of ICT and is committed to taking measures needed to guarantee it.

Contents

Introduction

The Cyber Security Strategy of the Czech Republic (hereinafter "CR") for the 2011 – 2015 period has been prepared taking the directions and principles set forth in the Security Strategy of the Czech Republic into account. It defines interests and intentions of the Czech Republic in the field of cyber security needed to build up a credible information society with solid legal foundations, which is committed to a secure cyber transmission and processing of information in all domains of human activities and makes sure that the information can be used and shared freely and safely.

Essential objectives of the cyber security policy include protection against threats which information and communication systems and technologies (hereinafter "ICTs") are exposed to, and mitigation of potential consequences in the event of an attack against ICTs.

The present "Strategy" is a keynote document, designed to be used as a basis of every ICT security-related policy, legal standard, directive, methodological instruction, rule, principle, manual, operating mode, plan, recommendation etc.

The implementation, operation and security of credible information and communication systems is a duty of the Czech Republic and a responsibility of all levels of government and administration, the private sector and the general public, the objective being to maintain a safe, secure, resistant and credible environment that makes use of available opportunities offered by the digital age. The strategy focuses mainly on unimpeded access to services, data integrity and confidentiality of the Czech Republic's cyberspace and is coordinated with other related strategies and concepts.

I. Background

ICTs have a major effect on the functioning of advanced societies and economies

1. Safe, secure and reliable operation of ICTs is necessary for the functioning of government and public structures and is an indispensable prerequisite for prosperity and a sustainable economic growth. The number of human activities and production operations directly or indirectly depending on ICTs is incessantly growing. The Czech Republic has an ambition to rank among advanced nations in this respect. Online services and networks must be not only secure and sturdy, but also reliable. The whole society must step up its activities in the field of security and reliability of ICTs.

ICTs and ICT-dependent societies are vulnerable

2. The incessant and speedy progress of ICTs keeps bringing new opportunities for the society, but also new security challenges. Combined with a technical defect, human error or intentional damage, the increasing dependence on ICTs makes it difficult to minimize any consequences resulting from a break through a weak spot of the whole ICT system. While the advent of new technologies offers new opportunities of the development of our society, it also brings new requirements concerning the security of ICTs and the whole society.

3. The growing dependence on information and communication technologies increases the vulnerability of the state and its citizens to cyber attacks. Such attacks may be a new type of warfare, or may have a criminal, economic, or terroristic motive and be launched to destabilize the society. Leaks of strategic information and intrusions of ICTs of government agencies or strategic enterprises and companies providing essential functions of the state may endanger strategic interests of the Czech Republic. There are many examples showing how fast and diversified developments in the field of cyber security are. Attacks against ICT structures are increasingly sophisticated and more comprehensive. They make use of many different methods and are aimed against various targets. Their nature and motives of the attackers also change. Well-organized attacks are more and more often aimed at elements of critical infrastructure (hereinafter “CI”), which are vital for the functioning of the state. As ICTs have found their way into many important areas of everyday life, they themselves have become a critical infrastructure element.

II. Essential Principles

4. Cyber security issues cannot be viewed as an isolated problem of the Czech Republic or just one or several segments of our society. They do not represent just an international, interdepartmental, private- or public-sphere problem, but rather a problem of the whole society. This is why cyber security merits a high level of priority.

Interlinking of and Strengthening of Cooperation among all Sectors of Society

5. It is highly desirable to network all initiatives, be they of the state (civilian, police, military) or of commercial or academic sectors, which have already accomplished a lot in the field of cyber security. Such joint efforts have led to improved cyber security and in many cases prevented dispersion of resources and unnecessary duplication. Much of the ICT infrastructure and many related products and services are provided by the private sector. Mutual trust and sharing of information are essential conditions of successful cooperation between the private and the public sectors.

Individual Responsibility

6. It is in the interest of the state that ICT security rules are in place. Every citizen, business, organization or institution should be responsible for the systems they own and operate. All operators and administrators (but also citizens, businesses and institutions) must take appropriate measures to make sure their ICT systems and networks are safe, secure and reliable.

Responsibility of the Business Sector

7. It is in the interest of the state and of the business sector to define minimum cyber security standards, implement them in day-to-day operations and activities, and require that they are strictly complied with.

Interdepartmental Cooperation

8. Pursuant to the Resolution of the Government No. 205, dated March 15, 2010, the institution with overall responsibility for and the national authority in the field of cyber security issues is the Ministry of Interior of the Czech Republic. In this respect, an important role belongs to the Interdepartmental Coordination Board for Cyber Security (hereinafter “ICBCS”), which will continue to initiate cooperation among government institutions and agencies. In accordance with its statutes, the

Board will establish working groups composed of relevant experts, which will jointly discuss cyber security issues of the public sector, but also of the banking sector, supply of energies and utilities etc.

International Cooperation

9. The Czech Republic will become involved in international cooperation in the field of cyber and information security. Within the European Union (hereinafter “EU”) and the North Atlantic Treaty Organization (hereinafter “NATO”), it will participate in the drafting of standards and international policies, as well as in activities of joint institutions, and, at the same time, adequately apply the standards and relevant mechanisms in its own national cyber security legislation. When fulfilling the requirements outlined above, the Czech Republic will abide by principles of a democratic society and duly consider legitimate interests of its citizens, business sector and public administration institutions and agencies in relation to the citizens.

Adequacy of Measures

10. Using risk analyses and relevant international recommendations, the government of the Czech Republic will adopt necessary measures to protect and guarantee national cyber security. These measures will respect privacy, fundamental rights and liberties, free access to information and other democratic principles. The Czech Republic will focus on their adequacy, balancing the need to guarantee security against respect for fundamental rights and liberties.

III. Strategic Objectives and Measures

Legislative Framework

11. New legislation will determine what the relevant public authority responsible for the coordination of measures in the field of cyber security will do, duties of entities producing, providing or making use of ICT services, and forms (procedures) and frameworks (scopes) of cooperation with the private sector and general public.

12. The Czech Republic will create an appropriate legislative framework for the purpose of ensuring cyber security, which will not impose any restrictions on rights to freedom of speech, access to information for all population segments, protection of privacy and confidentiality of information guaranteed by the Constitution, taking into account international commitments of the Czech Republic, in particular to EU and NATO.

13. The Czech Republic will regularly evaluate and assess international legislation, agreements, trends and recommendations in the fields of cyber and information security, electronic trade and electronic transactions, and use the results to draw conclusions and apply appropriate recommendations in the Czech environment. The Czech Republic will actively participate in the drafting of legal acts and standards, and other forms of cooperation in the field of cyber security in the framework of EU and other international organizations.

14. The Czech Republic will improve legislative and procedural steps so that the cyber security field ultimately comprises prevention, detection, reaction and measures designed to identify and combat cyber crime.

Strengthening of Cyber Security of Public Administration and CI ITCs

15. The introduction and implementation of security standards in information systems of public administration authorities and critical infrastructure elements is one of the key prerequisites of the strengthening of cyber security of information systems. Effective cyber security requires a mandatory implementation of, and strict compliance with, the security standards, including thorough periodical compliance audits of all public administration bodies and elements of the critical national infrastructure. Many of the latter are not owned by the state; consequently, a thorough analysis of ICT-related risks arising from the abovementioned fact and a legal enactment of binding rules applying to such systems are needed.

16. Methodological documents defining the required basic cyber security standard (directives and recommended procedures) will be prepared. The Czech Republic will support and promote a convergence of security measures and processes based on recommended procedures and employed both by state institutions and by the private sector. One of the tools of improving the information security level is the Information Security Management System (ISMS).

17. The Czech Republic will develop new methodologies and define procedures and ways of handling and protecting unclassified confidential information (i.e. the information the protection of which is not governed by the Classified Information Act), which is stored in information systems operated and used by public administration authorities and, above all, information systems needed to run and operate elements of the critical national infrastructure. The Czech Republic will also define standardized methodologies for categorizing information and information and communication systems.

Establishment of a National CERT Agency

18. Because of threats faced by ICTs, security and reliability of information and communication systems of the critical national infrastructure ranks among top priorities of the Czech government. To this end, the government intends to establish a government coordination agency that could immediately response to computer incidents, namely a Computer Emergency Response Team (hereinafter “CERT”). The agency will be a part of both the national and international cyber threat early warning systems. The Czech Republic will prefer and promote systems capable of both minimizing impacts of a cyber attack and of restoring the functionality of affected systems as soon as possible.

19. The CERT centre will optimize options used to identify potential cyber attacks and coordinate countermeasures and remedial actions. In cooperation with other relevant government agencies, the centre will coordinate and propose preventive measures to avert or thwart a potential attacks against information and communication systems of the state and elements of the critical national infrastructure. The agency will also identify, record, and evaluate security incidents. The CERT government agency will cooperate with the national centre and other public, commercial and academic facilities with a similar orientation, and provide them methodological assistance and support needed to handle and deal with security incidents.

20. The Czech Republic will develop a national cyber threat early warning system, which will also feature response options and an exchange of information reducing the risks that such threats pose to elements of information and communication systems, and will strive to make it a part of the international cyber threat early warning system. Mutual communication of security elements responsible for protecting CI information and communication systems against attacks will be continuously improved.

21. The Czech Republic will implement and regularly update plans designed to deal with operating and security incidents in the field of cyber security and to subsequently restore the functionality of all public administration and CI-related information systems.

22. The Czech Republic will introduce monitoring and testing of the efficiency of processes designed to deal with security risks and proposed countermeasures as parts of the Information Security Management System. The

capabilities will be verified by regular national and international cyber defence exercises.

International Cooperation

23. Coordinated international cooperation is an essential prerequisite of a global dimension and comparable levels of cyberspace security.

24. The Czech Republic actively participates and will continue to participate in the development of measures against cyber threats and in cooperation in the framework of international organizations, in particular EU, NATO and others. The Czech Republic is also involved in an intensive international exchange of information and lessons learnt through its membership in relevant international institutions, and will continue to do so.

25. The Czech Republic supports stronger and more extensive international judicial and police cooperation to apprehend perpetrators of cyber attacks, and will continue to do so.

26. The Czech Republic should join effective and promising initiatives advocating the development of international legal standards dealing with cyber and information security issues.

Cooperation of the State, Private Sector and Academia

27. The dynamic nature of the development of ICTs requires incessant cooperation among the public, private and academic sectors. If the cooperation did not exist, it would be impossible to strengthen the Czech Republic’s cyber security, to minimize any damage caused by cyber attacks, or to quickly restore the functionality of affected ICT systems. An important element of the cooperation is an official platform for the purpose of sharing cyber security information and lessons learnt.

28. The Czech Republic will support both national-scale and international cooperation of public administration authorities, private entities and academia on information exchange/sharing and best practice cyber security projects.

29. The Czech Republic supports research and development efforts focused on both current and potential cyber security issues (in particular intensified cooperation of the state, private sector and academia).

30. The Czech Republic makes use of results of international cooperation, including availability of information about cyber security-related problems, solutions, trends, legislation, standards and international initiatives.

Increased Cyber Security Awareness

31. Information on ICT-related security challenges is available in the public domain; still, it is necessary to increase the cyber space security awareness of end users, system administrators, IT developers, public contracting authorities, public servants, auditors and managers. Insufficient information on ICT security poses great risks to critical infrastructure elements even in cases the systems are not a part of the critical infrastructure itself. Lack of properly trained and well-informed personnel and absence of a continuous training and education programme or a personnel certification system increase the systems´ vulnerability and potential damage.

32. The Czech Republic will increase the cyber and information security awareness of its citizens through disseminating relevant information in cooperation with the media. It will increase the awareness of the necessity of a security certification of ICT products and services, and it will build a platform ensuring effective communication in the field of cyber security.

33. The Czech Republic will include cyber security in education programmes of public servants and promote this education in the private sector as well. The objective is to achieve the target level of knowledge for each of the players in the field of cyber and information security.

34. The Czech Republic will methodologically cooperate with the private sector in the implementation of training programmes focusing on cyber and information security.

35. The Czech Republic will continuously analyze qualification needs of Czech ICT users in the field of cyber and information security and of school and extra-curricular training, and will integrate cyber and information security in relevant methodologies at all levels of education.