STRATEGY
OF THE CZECH REPUBLIC IN THE FIELD OF CYBERNETIC SECURITY FOR 2012 - 2015

Content

Introduction

Strategy of the Czech Republic in the field of cybernetic security for 2012 – 2015 (hereinafter referred to as “Strategy”) is one of the steps of the Government of the Czech Republic in reaction to worldwide rise of cybernetic threats. The Strategy stems from efforts of governmental and non-governmental entities to raise level of cybernetic security. It brings initiatives to enhance cybernetic security for state bodies, critical infrastructure and commercial sphere as well as for citizens.

The Strategy defines aims and interests of the Czech Republic in the field of cybernetic security for building of reliable information society and is in line with the Security Strategy of the Czech Republic.

This Strategy is the basic document for the creation of legal acts, security policies of information and communication systems, standards, rules, operation measures, maintenance plans, recommendations and other tools for cybernetic security.

The Strategy is divided into three parts. The first one describes foundations determining necessity to deal with this problem. The second one brings analysis and basic principles of cybernetic security. The third states goals and describes activities crucial for enhancing cybernetic security – activities implemented by the Government of the Czech Republic and activities in cooperation with partners.

I. Foundations

Attacks on critical information infrastructure have become more often, complex and sophisticated as the perpetrators are more professional in the recent years. Possibilities for timely reaction and arrests of perpetrators are very limited and demanding. The trend of the development of ISs for industrial use connected to the internet brings new vulnerabilities of those systems. Experience with Stuxnet virus shows that important industrial facilities are not immune to cybernetic attacks. Cyber security shall remain crucial for maintaining functioning state in the future.

Information and communication technologies and their impact on modern society and economics

Safe and sound functioning if information and communication technologies (hereinafter "ICT") is necessary for operations of state and public entities and is one of the basic preconditions of prosperity and sustainable economic growth. The share of human activity dependent directly or indirectly on ICT is steadily growing. The Czech Republic has ambitions to belong among developed countries in this field. Networks and online services have to be not only secure but also reliable. The whole society has to enhance its activities towards the security and reliability of ICT.

ICT and societies dependent on them are vulnerable

Constant and rapid progress in the field of ICT brings new opportunities for the society but also new security challenges. Combination of increased dependence on ICT which is not flawless with human failure or intentional damage makes mitigation of damages more complicated. The emergence of new technologies brings new opportunities for the development of the society but also new vulnerabilities and new demands for the security of ICT and whole society.

Increased dependence on ICT enhances vulnerability of the state and its citizens to the cybernetic attacks. These attacks may be motivated by crime, economic profit or terrorism and may be used to destabilise society. Leaks of strategic information, infringements into ICT of state institutions or strategic companies may endanger interests of the Czech Republic. Examples show rapid and diverse development in the field of cybernetic security. Attacks against ICT are more complex and sophisticated. These attacks are aimed against various targets and waged by various means. Also the nature of attackers and their motives are changing. Parts of the critical infrastructure, crucial for functioning of the state, are becoming target of attacks more and more often.

Considering the fact that digital society is globalised and cybernetic attack are crossing state, cultural and legislative boundaries, it is often not obvious which jurisdiction should be applied to them. Close international cooperation is therefore needed also in the area of legislation.

II. Basic principles of strategy of cybernetic security

Investment into cybernetic security means investing into our future and our economic growth. The level of cybernetic security comprises from all measures, both national and international, adopted to protect availability of ICT and integrity, authenticity and confidentiality of data in the cyberspace. Cyber security has to be based on complex approach demanding information sharing and coordination of activities. The cooperation between military and civilian, public and private and international and national spheres is to be ensured while building the system of cybernetic security. Only such approach ensures sound operation of ICT infrastructure in critical areas, rapid and effective reaction to cybernetic attacks and legal protection in the digital world. The issue of cybernetic security cannot be seen as an isolated problem of the Czech Republic or several parts of our society. It's not only international, inter-ministerial public or private sphere issue but the problem of whole society. Therefore, ensuring of cybernetic security deserves the highest priority.

Interconnection and strengthening cooperation of all parts of society

It is desirable to coordinate all initiatives of state (civilian, police, military), commercial and academic entities, those which have done a lot of good work in their areas of responsibility and those which weren't very active so far. Only coordinated effort leads towards enhancing of cybernetic security without dispersion and useless doubling of efforts and growth of costs. ICT infrastructure, goods and services are from largest part provided by the private sector. Mutual trust and information sharing are thus basic precondition for successful cooperation between public and private sector.

Individual responsibility

It is the basic interest of the state to establish the ICT security rules in a way to be accepted by all users of cyberspace (state bodies, critical infrastructure entities, public entities, commercial companies and citizens) and service providers in order to adopt in their ICT systems appropriate measures to protect the system against internal and external attacks and not to pose a threat for other systems.

Inter-ministerial cooperation

According to the decision of the Government of the Czech Republic no. 781 from 19th October 2011 the body responsible for the field of cybernetic security is the national Security Authority (hereinafter "NSA"). The Council for Cybernetic Security (hereinafter "Council") plays a key role in the inter-ministerial coordination. It will, among other tasks, initiate cooperation of state bodies. In line with its statute, the Council will establish working groups comprised of relevant experts. The working groups will draft documents dealing with specific issues of cybernetic security for the Council.

International Cooperation

Bearing in mind that a measure could be effective only if implemented or coordinated on an international level the Czech Republic will actively support through common bodies and working groups the efforts of the European Union (hereinafter "EU") and North Atlantic Treaty Organisation (hereinafter "NATO") to create international policies, standards and norms and adequately implement those policies, standards and norms into national legislation dealing with cybernetic security.

Adequacy of adopted measures

There is no way how to achieve absolute cybernetic security. The Czech Republic will adopt measures based on realistic evaluation of risks and shall be appropriate to such risks. They will respect protection of privacy and basic rights as free access to information, freedom of speech and others. The measures shall be appropriate to the necessity to ensure security on one side and to respect basic rights and freedoms on the other side.

III. Strategic goals and measures

Strategy adopts measures against current threats and is a basis for the Action Plan which defines particular steps and identifies those responsible for their achievement. The following areas shall be prioritised:

Creation of legislative framework

The NSA shall draft a specialised law on cybernetic security which will determine responsibilities of the national Centre for Cybernetic Security (hereinafter "NCCS"). The law shall define obligations of entities offering and/or using services in the cyberspace. It shall further determine means and scope of cooperation with private sector, public and international institutions.

International laws, agreements, trends and recommendation in the field of cybernetic security e-commerce and electronic transactions shall be regularly evaluated and the conclusions and recommendations stemming from such evaluation shall be implemented. The Czech Republic shall actively participate in

drafting of laws, norms and other cooperation associated with cybernetic security in the framework of EU, NATO and other international organisations.

Establishing National Centre for Cybernetic Security and Governmental CERT

The NCCS shall be established within NSA to optimize cooperation between state bodies and improve coordination of protection and implementation of counter-measures. Governmental CERT (Computer Emergency Response Team) will be part of the NCCS. The NCCS shall actively cooperate with other state bodies, academic institutions and commercial entities on the basis of cooperation agreements. Quick and effective sharing of information about vulnerabilities of ICT, forms of cybernetic attacks profiles and motivation of the perpetrators will enable NCCS to analyse security incidents and draft recommendations of counter-measures. It is in the best interest of the private sphere to cooperate with NCCS in protection of their own ICT systems against attack through cybernetic attacks. Bearing in mind that the best way to ensure security is through proper preparation and prevention, the NCCS shall establish a system of early warning and shall provide recommendations how to protect against cybernetic attacks.

NCCS shall push for the system of testing of handling security risks and proposed counter-measures as a part of risk management system. Such capabilities shall be subject to regular testing through cybernetic defence exercises (also on international level).

Protection of critical information infrastructure

Protection of critical information infrastructure is one of the main priorities in cybernetic security. This infrastructure poses main part of almost all parts of critical infrastructure and is becoming more and more important. Both private and public spheres have to create conditions for closer cooperation based on information sharing. It will be properly evaluated where the security measures will be fully implemented and where shall be additional powers in case of specific attacks and threats.

Strengthening of cybernetic security of information and communication systems of public governance

Users of ICT need to be provided with relevant and consistent information about risks and safe ways how to utilize the cyberspace. NCCS shall provide such information on GovCERT.cz portal. Also information about available security products and services will be provided on the portal.

Implementation of security rules and standards in information systems whose secure operation is crucial for the functioning of the state is one of the preconditions for enhancing cybernetic security of those systems. Effective cybernetic security

demands obligatory implementation and proper adherence to those rules and standards and regular inspections of their implementation in the public governance bodies.

Methodical documents (regulations and recommended practices) shall be prepared. Enhancing of level of information security will be done through implementation of the ISMS (Information Security Management System).

Effectiveness of fighting crime in the cyberspace

NCCS shall contribute to fight against cybernetic criminality by cooperating with law enforcement bodies and shall use their experience during development of means and measures against cybernetic attacks.

Coordination of activities to ensure cybernetic security in Europe

Global cyberspace security may be achieved only through coordination on national and international level.

The NSA shall support appropriate measures based on European Action Plan for Protection of Critical Information Infrastructure in the framework of the EU. Further, the cooperation with the European Network and Information Security Agency (ENISA) shall commence in the field of training and information sharing. The ideas for future activities may be found in „EU Internal Security Strategy“ and in „Digital Agenda for Europe“ as well as in the new „NATO Policy on Cyber Defence“. The cooperation in the areas under NSA responsibility shall be also established with the newly established European Agency for Management of Large-Scale IT Systems and with the EU Centre for Cybernetic Criminality.

Using of reliable IT

Availability of reliable ICT systems to public governance users has to be ensured. Research and development of means for protection of ICT systems of public governance and critical infrastructure facilities shall be supported. The aim will be to use technical and software means accredited according to international standards in areas critical for the security of the state.

Raising awareness about cybernetic security

Establishing cybernetic security cannot rely on technical means only. Proper care has to be given also to end-users and administrators of ICT systems, development workers, public contract awarders, auditors and managers. Insufficient information about security of ICT systems brings serious risks. Lack of trained and informed personnel and further education raise vulnerability and damages.

Awareness of citizens about cybernetic security shall be risen through spreading of relevant information in cooperation with media. Cybernetic security shall part of training of public employees and will be supported in the private sphere as well. The aim is to reach sufficient level of knowledge for each position in the area of cybernetic security.

Cooperation aimed at creating training programmes focusing on cybernetic security shall be started with the academic and private spheres. Needs for qualification in cybernetic security, opportunities of school and other education shall be evaluated on a regular basis. The issue of cybernetic security will be implemented into all levels of education.

Response to cybernetic attacks

Bearing in mind that the cybernetic attacks against the systems of public governance and critical infrastructure cannot be avoided the state has to prepared for such attacks. Complex set of measures to be implemented in the event of cybernetic attack has to be created in cooperation with all competent state bodies. Necessity and adequacy of such measures has to be taken in mind.

Strategy in the Field of Cybernetic Security for 2012 – 2015 follows up to the Security Strategy of The Czech Republic and reflects the challenges of modern information society. The Strategy provides institutional framework contributing to the security system of the Czech Republic. This framework constitutes beginning of active policy of cybernetic protection of the state which is to be permanently evaluated and amended. Awareness of every individual, operator, administrator, university or company about security challenges of ICT is a basic precondition to ensure reliability and security of the cyberspace. The Czech Republic considers the issue of cybernetic security to be an important part of daily use of ICT and shall further work to ensure it.