Aims fulfillment of the National Strategy for Information Security in the Slovak Republic

Jan Hochmann, Ministry of Finance of the Slovak Republic
Petra Hochmannová, CSIRT.SK/DataCentrum

Abstract

Information and communication technologies (ICT) influence the everyday lives of our society and create new form of behavior of its members in the social, economic and political sphere. Simultaneously with the development and use of ICT, it is necessary to solve the problem connected with privacy and valuable state asset protection and set the border of what is allowed. In the Slovak Republic (SR), the initial document dealing with this area is the National Strategy for Information Security in the SR (NSIS), adopted by Resolution No. 570/2008 of the Government of the SR creating wide platform for dealing with legislative, institutional and executive issues. The key aim of this document is to create suitable conditions for consistent implementation of directives, regulations and international agreements such as United Nations Security Council resolutions, regulations and general decisions of international institutions especially EU and particular states. Aforementioned document creates condition for basic problem solving in the area of coordination and cooperation of key subjects along with increasing the awareness, competence and education in the area of information security, creating the secure environment and encouraging international cooperation. Special attention is paid to the development of suitable legislative environment, standardization activities and organization of national exercises as a protection against cyber threats and assuring the security and protection of citizens and businesses in the on-line environment. NSIS is defined as a summary strategic document involving strategic aims, priorities and specific tasks with defined responsible subjects and deadlines. The actual tasks resulting from the strategic aims and priorities of information security in the SR are described more in detail in further documents focused on particular areas. The most important of them are involved in the resolutions with the time horizon 2008 – 2013. Further strategic tasks are developed in the document "Action plan for National Strategy for Information Security in the SR" for years 2009 – 2013 and Digital Agenda for Europe approved in 2010.The solution results from the development of international security situation, activities of international institutions, implementation of legal measures of individual ministries and other public bodies of the state government.

1. Global environment and framework

In the existing environment, information is widely processed in the electronic form by the use of information and communication technologies (hereinafter ICT). As a result there are many different factors that can jeopardize the functionality or cause the dysfunction of ICT and alter

information that is processed. In general, there are natural disasters, technological failures, human errors and omissions, malicious code, sabotage, cyber crime and terrorism that can cause significant security problems. Especially dangerous are the plans of terroristic groups, trafficking on human beings and personal data, financial and economic crime, anarchy etc. The priority is to prevent the access of unauthorized persons to sensitive information. Very dangerous are also the attacks aimed at national critical infrastructure committed through expanding networks and the Internet and new methods connected with the use of RFID technology (Radio Frequency Identification). It involves barcodes, biometric authentication, chip cards, monitoring systems, voice identification and others based on this principle. These technologies have long been used to protect objects and goods, they have been also used for access control and identification systems, entrances to buildings, toll systems, entrances to sport and cultural events, and more recently in a personal identification card, bank cards, and passports, medical cards, manufacturing and logistics, automotive industry, public archive and data processing in the field of telecommunications, eVoting, eCensus etc. It is difficult to set clear border between positive and negative impact of aforementioned technologies. From the geopolitical point of view new sophisticated forms of crime has emerged. ICT are misused for political, economic and military dominance known as “cyber warfare” and “cyber terrorism”. In Mediterranean area[(1)] there are countries which are prepared to block the access to ICT for political reasons to avoid the internet and mobile communication which may threaten the economy and security in other locations around the world. The misuse of ICT is becoming a dangerous tool for manipulation, lucrative form of investment and illegal source of money with minimum initial investment. Additionally, this form of criminal activity is committed to long distances often crossing state borders demanding minimum amount of time. As a result of global interconnection, threats are coming from different places on earth. The local approach to respond to this situation seems to be inefficient. Global approach of international community and mutual cooperation with countries of the Third World is deemed to be inevitable. The acceleration of technological, information, cultural a political interconnection of countries and continents brings other threats that negatively influence the control of individual governments. They can be source of disharmony within and among countries.

2. Information Security analysis in the SR from 2008

Despite the fact that there are common features among the existing challenges and problems, measures and ways to ensure the security and resilience, as well as the level of basic awareness, competence, professionalism and willingness to solve this global problem differs significantly across Member State. Separated national approaches and disrespect of common international procedures by some of the Member States, including the Slovak Republic, are bringing the risk of incompatibility and inefficiency for Europe.

According to information security survey, the Slovak Republic is currently one of the weakest members of the EU in this area. The reasons came from insufficient and inconsistent legislation, lack of proficiency and poor technical knowledge of system administrators, users and employees in the managerial position. The security awareness can be perceived as a understanding of the need and the nature of information security of all users with the

[(1)] COM(2011)200 final on Partnership for democracy and shared prosperity within the southern Mediterranean

following transformation of the security awareness into competence. It means understanding and application of own responsibility. Information security awareness does not reach the required level in the Slovak Republic. As a result of the information security survey carried out by the Ministry of Finance of the SR in December 2008 shown, to this area has not been given sufficient attention yet. Incident management processes are underdeveloped, there is a lack of methodology and training, in some areas related to ICT education is provided by unqualified lecturers. Results of the survey are publicly available on the website of the Ministry of Finance of the SR www.informatizácia.sk/prieskum. Significantly negative is the fact, that private companies have access to personal and sensitive data while managing different projects and implementing information systems what is often misused. This is also closely related to an inappropriate outsourcing of IS administration by public institutions. The problem is also the fragmentation of responsibilities, duplication of processes and the issue of double standards, their mutual incompatibility and lack of foreign cooperation in the process of their adoption. Statistics show that e-learning is used three times less in the Slovak Republic than in the EU average.

Despite the existing common challenges and problems, there is a significant improvement from the year 2008, but some major weaknesses still persist. These undesirable differences in approaches and lack of systematic internal and cross-border cooperation obviously reduce the effectiveness of national countermeasure among other also because there are requirements for interoperability of individual sectors located in the Member States. Different level of security in one country increases the vulnerability and risks in other countries.

3. Activities on the national level

The Slovak Republic responded to the negative situation in the country and the requirements of the EU by the elaboration and implementation of strategic documents such as “National Strategy for Information Security in the SR” (Gov. Decree No. 570/2008) and “Action Plan for the National Strategy for Information Security in the SR” (Gov. Decree No. 46/2006) involving strategic aims and priorities in this area. Among others important related documents belong “Proposal of the System of Information Security Education in the SR” (Gov. Decree No. 391/2009), “Proposal of organizational, personnel, material, technical a financial provision concerning the creation of a Computer Security Incident Response Team (CSIRT.SK) in the SR” (Gov. Decree No. 479/2009) and the others arising from the EU directives, regulations and recommendations. [(2), (3), (4)]

3.1 National Point of Contact - CSIRT.SK

In the area of prevention and preparedness at the national level, minimum standards were adopted and Computer Security Incident Response Team Slovakia (hereinafter CSIRT.SK) operating under the auspices of the Ministry of Finance of the SR was created (Gov. Decree

---

[(2)] COM(2009) 149 final on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancingpreparedness, security and resilience".

[(3)] COM(2010) 245final, A Digital Agenda for Europe.

[(4)] COM(2010) 517 final on attacks against information systems and repealing Council Framework Decision.

No. 479/2009). The main aim of CSIRT.SK is to provide adequate level of information and communication infrastructure protection and protection of critical information infrastructure. According to the conception, CSIRT.SK is in the last phase of its development. Incident reporting is applied by national as well as international institutions and counterparts. National point of contact for early warning and incident reporting created by the CSIRT.SK will be launched in the 2nd half of 2012. On the web portal www.csirt.gov.sk are published other important activities and information about the team.

3.2 Act on Critical Infrastructure

Positively perceived in the area of "Criteria of European Critical Infrastructures in the ICT sector" was the adoption of "Act No. 45/2011 coll. on Critical Infrastructure" under the auspices of the Ministry of Interior of the SR.
The Act defines critical infrastructure sectors and determines the public bodies of the state government responsible for the protection of its elements. Cross-sectoral criteria for determining the elements were approved by the Governmental Decree No. 356/2011. Subsequently, the draft of elements of critical infrastructure in all sectors was approved by the Governmental Decree No. 751/2011. The specific tasks of each sub-program are managed within "Inter-ministerial program on critical infrastructure protection in the SR" approved by the Slovak Government in the year 2010.

Sector	Subsector	Organization
1. Transport	Road, air, water, rail	MTCRD SR
2. Electronic Communication	Satelite communication, Networks and stable and mobile services of electronic communications	MTCRD SR
3. Energetics	Mining, Electricity, Gas, Crude oil	ME SR
4. Information and Communication Technologies	Information Systems and Networks, Internet	MF SR
5. Post	Post services, system of payments and procurement activities	MTCRD SR
6. Industry	Pharmaceutical, metallurgical, chemical,	ME SR
7. Water and atmosphere	Meteorology, water construction, drinking water	ME SR
8. Health		MH SR

3.3 Legislative intent – Act on Information Security

The main aim of the state is to provide adequate level of protection of whole ICT systems administrated by public bodies and municipalities. The future Act on Information Security will create coordinated and effective system of protection of public administration information systems (hereinafter PAIS) in the Slovak Republic. Since PAIS are the part of

wider digital space in the Slovak Republic, a large proportion is owned by the private sector. The future legislation must create the conditions for raising the level of information security across the digital space in the Slovak Republic by supporting the interoperability and standardization of information security. In general, this law will solve two problematic areas. Firstly, it will ensure the protection of the public administration information systems as a whole and secondly it will create a general legal framework for protecting the whole digital space in the Slovak Republic. The scope of the Act will apply to PAIS and it will set mandatory and basic safety requirements for other ICT systems in the digital space that communicate with PAIS to the extent necessary for ensuring their safe operation.
The paragraph wording of the aforementioned act will cover the area of information security in the SR and lay down stricter rules in the information security environment. It will determine the basic structure and adequate level of protection of whole digital space in the SR. The proposal takes into account the interests and needs of the owners and users of ICT, as well as the rights of natural persons and legal person whose data are processed in the systems and need to be protected. There is an absence of the process of information security management (hereinafter ISMS) in public administration and classification of PAIS in terms of requirements for information security in the SR. The new legislation will also solve this issue. The Act further provides minimum safety requirements for eGovernment and internet security as a key part of the national critical infrastructure. A special section will be devoted to new identification technologies, working on the principle of radio frequency identification of persons and goods and legal protection against spam. Submission of the Act on Information Security in the legislative process is expected by the end of 2012.

3.4 Education, awareness and competence in the area of information security

The main objective was firstly to identify groups of users in the digital space and divide them into the group of laics, managers, informatics, IT specialists, teachers and the researchers. Secondly, it was necessary to estimate their qualification needs in the Slovak environment and finally propose appropriate level of education for these categories. The document involves also the proposal of the system of education based on the current situation in the Slovak Republic and in the world. The proposed system of education in the information security is designed as an open system that can be continuously updated and augmented by new features and procedures. The outcome of this important strategic document is the establishment of basic objectives, tasks and activities in the field of education in the information security and the draft of measures, which is reflected in the tasks defined governmental decree. As a part of an integrated “Proposal of the System of Information Security Education in the SR" approved by Governmental Decree No. 391/2009, which forms the core of the learning process, the Ministry of Finance prepared the complete process of implementation, including the pilot project and public procurement. Before the contract had been signed, the Office for Public Procurement in the SR, issued on 22 August 2011on its own initiative, decision to cancel the procurement process. Ministry

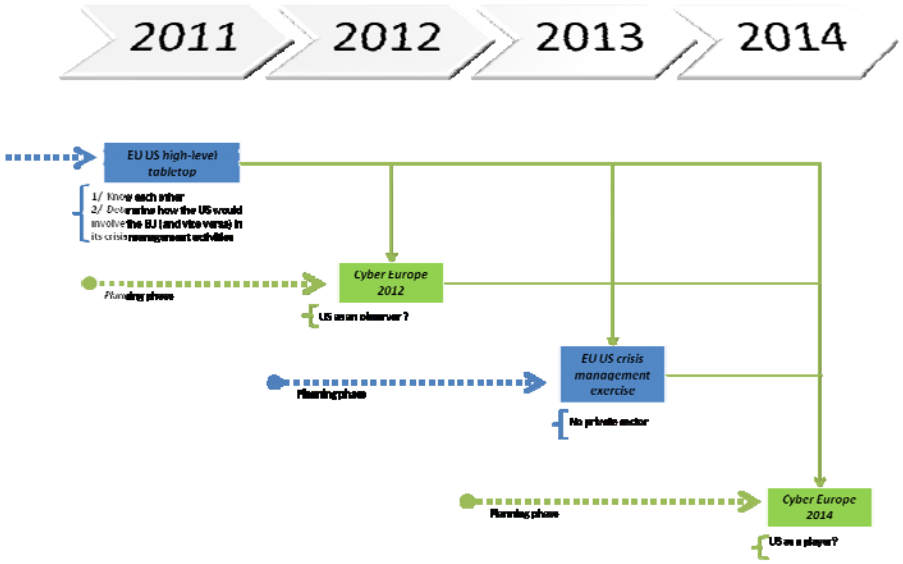
of Finance of the SR decided to sue the Office for Public Procurement in the SR for the inappropriate intervention. The case is currently under the trial. Despite the highest priority of this task, for unknown reasons, nothing significant has happened in this case till now.

4. International activities

The activities in the area of international cooperation are focused on active participation on international exercises on critical infrastructure protection. After the successful representation of the SR on the first Paneuropean exercise - Cyber Europe 2010 in the year 2010 in Athens, Ministry of Finance of the SR together with CSIRT.SK actively supported also other activities.

In the of 2011, the Slovak Republic participated actively on the first joint cyber security exercise between the EU and US – Cyber Atlantic 2011 in Brussels, with the support of the EU's cyber security Agency ENISA and the US Department of Homeland Security. It was the day-long table-top exercise with the experts from 16 countries. Exercise simulated two cyber-crisis scenarios to explore how the EU and US would engage each other and cooperate in the event of cyber-attacks on their critical information infrastructures.

In the first scenario, a targeted stealthy cyber-attack (Advanced Persistent Threat – APT) attempts to infiltrate and publish online, secret information from EU Member States' cyber security agencies on the simulated portal called „Euroleaks". The second simulation was focused on the disruption of supervisory control and data acquisition (SCADA) systems in power generation infrastructures. The main aim of participating Member States was to respond to the situation by forming crisis teams, organizing teleconferences, information Exchange, coordinating activities and minimizing impact based on European Standard Operating Procedures. Cyber Atlantic 2011 is part of an EU-US commitment to cyber security which was made at the EU-US summit in Lisbon on 20 November 2010.



On 23 November 2011, the first national exercise on critical information infrastructure protection – „SISE 2011" (Slovak Information Security Exercise 2011) organized by the Ministry of Finance of the SR and CSIRT.SK was held. Besides these two, institutions

actively participating in the exercise involved Ministry of Interior of the SR, Government Office of the SR, Telecommunications Regulatory Authority of the SR and DataCentrum together with foreign counterparts CERT.at (Computer Emergency Response Team Austria) and CSIRT.CZ (Computer Security Incident Response Team Czech Republic). Ministry of Defense of the SR and academic CESNET-CERTS (CESNET Computer Security Incident Response Team) performed the role of observer. The main aim of the exercise was to verify the reaction of participating institutions on large-scale security incidents and other related activities such as mutual communication and functionality of internal processes and procedures (disaster recovery and business continuity plans). Among other partial objectives belonged trust building at the national level and the examination of internal processes of CSIRT.SK as a national coordinator and contact point for large-scale security incidents. Final report from the exercise is a part of „Task fulfillment report to Action plan for the National Strategy for Information Security in the SR“.

5. Conclusion

One of the most valuable assets of each state is a human potential, streaming from the knowledge level of citizens, non-commercial and commercial organizations, public institutions, from the risks associated with the use of ICT and ways how to protect against threats on the Internet, media and eGovernment services. Our priority is therefore to create awareness and competence in the information security, to develop standards for basic knowledge, expand and implement a system of education for target groups and include it in all educational programs of formal and informal education. One part of the project related to the implementation of „ Inter-ministerial program on critical infrastructure protection“ is to create a description of the information security qualifications within the national system of qualifications. The main challenge however is to create the high quality human potential based on moral principles and to enhance the knowledge of citizens in such sensitive area as information security. It should be noted that successful implementation of this horizontal priority requires not only highly professional and organizational work, but especially strong political will.