

I Feasibility study for the establishment of the National CERT

INTRODUCTION

The Law on Information Security („Official Gazette of RS“, No. 6/2016) stipulates measures for the protection from security risks in information and communication systems, regulates the liability of legal entities during management and use of information and communication systems, designates competent authorities responsible for the execution of protection measures, defines coordination between protection factors and monitors proper application of the prescribed protection measures. Pursuant to the provisions of this Law, the tasks of the National Centre for the Prevention of Security Risks in ICT Systems (National CERT; CERT – *Computer Emergency Response Teams*) are assigned to the Regulatory Agency for Electronic Communications and Postal Services (RATEL). The National Center for the Prevention of Security Risks shall perform the tasks of coordination, prevention and protection from security risks in information and communication systems in the Republic of Serbia on a national level.

The Regulatory Agency for Electronic Communications and Postal Services, established by the Law on Electronic Communications („Official Gazette of RS“, Nos. 44/10, 60/13 – CC and 62/14), is an independent regulatory organization acting as a legal entity, performing public authorizations for an efficient implementation of the set policies in the domain of electronic communications, in the aim of fostering competition of electronic communications networks and services, improving their capacity, quality, participating in the development of the electronic communications market and protection of interests of the users of electronic communications, in line with provisions of the Law and its regulations, as well as other tasks in accordance with the special law regulating postal services.

Pursuant to Article 8 of the Law on Electronic Communications, the Agency RATEL shall:

1. adopt by-laws;
2. decide on the rights and obligations of operators and users;
3. cooperate with agencies and organizations in charge of broadcasting, competition protection, consumer protection, personal data protection and other agencies and organizations on issues relevant for the electronic communications sector;
4. cooperate with the relevant regulatory and expert bodies of the European Union Member States and other states for the purpose of harmonizing the practice of implementing the electronic communications sector regulations and promoting the development of cross-border electronic communications networks and services;
5. participate in the work of international organizations and institutions within the electronic communications sector in the capacity of the national regulatory authority within the electronic communications sector;
- 5a) perform regulatory and other activities pertaining to the postal sector, in accordance with the special law governing the domain of postal services.
6. perform other activities in accordance with this law.

Furthermore, the Agency is obliged to perform the above activities as entrusted tasks, impartially and publicly.

Having in mind types of duties RATEL has performed as part of its current tasks, as well as the achieved quality of performance regarding the execution of these activities, it is clear that RATEL has a great potential for a successful realization of the National CERT.

Based on the obligation prescribed by the Law, the Regulatory Agency for Electronic Communications and Postal Services launched the project on the establishment of a separate organizational unit with the role of National CERT. The first step in this process is the elaboration of the National CERT Feasibility Study, which is also the topic of this project. The Feasibility Study on the National CERT establishment must be able to explain organization, structure, functions, required resources, processes and budget (cost estimate) of the future National CERT, and also present an Action Plan for the establishment of the National CERT over a 5-year period.

CONCLUSION

Global informatization of society brought the issue of information security into the spotlight. A compromised ICT system may paralyze the modern world in its entirety. This problem has been recognised in our country too, which resulted in passing the Law on Information Security („Official Gazette of RS“, No. 6/2016). Article 14 of this Law stipulates establishment of a National Centre for the Prevention of Security Risks in ICT Systems (National CERT). In line with the same Article, the National CERT is to be founded by the Regulatory Agency for Electronic Communications and Postal Services. Having in mind types of activities performed by RATEL within its legal authorization so far, as well as the achieved quality of performance regarding the execution of these tasks, it is clear that RATEL has a great potential for a successful realization of the National CERT.

Main tasks of National CERT are to collect and exchange data on ICT system security risks, as well as on the events threatening ICT systems security, based on which it shall inform, warn and advise persons managing ICT systems in the Republic of Serbia and the public accordingly. To be up to this task, the National CERT must employ trained experts in the domain of information security. Beside the collection and exchange of data on ICT systems security risks, experts employed at the National CERT will be able to assist special interest ICT systems' operators with their advice and recommendations. The solution of the National CERT's organizational structure and manner of functioning proposed in this study, projects the National CERT to become the hub of information security knowledge in the Republic of Serbia. The National CERT shall form an information system which will collect all the data on security incidents, including the ways of overcoming and preventing these incidents. The National CERT's technical infrastructure should enable the Ministry of Trade, Tourism and Telecommunications (MTTT) to perform its own tasks, prescribed by Law, in the domain of collection and processing of security incidents data on the territory of the Republic of Serbia. Mutual relations and manner of cooperation between the MTTT, as a competent authority, and the National CERT will be arranged in a special agreement.

The proposed solution from the study foresees 14 employees on a permanent basis at the National CERT by the end of its fifth year of existence. This number includes one position for director, one position for business assistant and one position for marketing expert. The remaining 11 positions are to be filled by engineers – experts in the domain of information security. This type of employee structure in the National CERT demonstrates a clear commitment to the establishment of a highly professional organization tasked with the provision of adequate expert assistance in the domain of information security to all special interest ICT systems' operators and other ICT system operators in the Republic of Serbia. Taking into account that, both locally and globally, the domain of information security lacks highly specialized experts, the initial five-year plan foresees a very intensive training of all the employees in the National CERT. After the completion of the initial five-year plan, the National CERT will have a highly specialized CERT team that will be able to respond to all kinds of challenges which can arise in the field of information security. During the initial years of the National CERT's activities, the focus will be on building the necessary infrastructure, training of employees, defining the totality of the necessary work procedures and communicating with relevant bodies in the country and abroad. From the third year, the National CERT should have enough knowledge to respond to ever-sharper challenges in the domain of information security. During the fourth year, when the number of employees reaches the planned level, National CERT will switch to a 24/7 operation mode, ensuring the

provision of continuous assistance in case of potential problems in the domain of information security, for the entire territory of the Republic of Serbia.

The proposed solution for the National CERT foresees a five-year budget in the amount of slightly above 3.1 million Euro. This figure is justified by the fact that a very specific organization is being created and that RATEL, at the moment, does not dispose of an adequate expert pool for the execution of this type of work. This practically means that it is necessary to buy and realize the complete National CERT's technical infrastructure and train the experts so that they can tackle these specific issues. The domain of information security is one of the most dynamic areas of the modern society, which requires continuous vocational training of experts who perform their tasks professionally. The same requirements are therefore expected to be fulfilled by the National CERT experts. One should however take into account that the National CERT is not conceived as a profitable organization. As a result, the financing of the National CERT will have to be realized through the budget of an umbrella organization, which is, in this case, RATEL. Due to the specificity of the tasks and issues the National CERT is assigned to resolve, it is not possible to justify the refund of the invested resources by classical methods. By comparing the importance of the existence and quality and professional work of a National CERT in modern society, one can put this organization in the same line with the military, police and other authorities ensuring protection and unhindered development of the society. Damages caused in modern information society by potentially compromised ICT systems can amount to billions of Euro. The National CERT is one of the key organizations which should provide prevention and protection of the modern society from such unwanted events. If we suppose that professional activities and actions of the National CERT reduce damage to the modern society by at least 10% (in reality this figure being considerably higher), it is clear that possible savings surpass manyfold the required budget needed for this organization's functioning.