Elements of cyber security in public territorial administration of Slovakia in regional self-governments

Jana Béreš Furmanová [*] [A]; Dominik Béreš [A]

[*] **Corresponding author:** Doctoral Student, e-mail: jana.furmanova@vsbm.sk
Doctoral Student, e-mail: dominik.beres@vsbm.sk

[A] The University of Safety Management in Košice, Slovakia

Received: June 9, 2023 | Revised: June 26, 2023 | Accepted: June 30, 2023

DOI: 10.5281/zenodo.8336008

Abstract

The article is interested in describing the basic legislative procedures for the creation of effective protection of the level of public administration – a self-governing region against incidents of the current modern infrastructure in the field of information and cyber systems. Among the most important steps in the preparation and implementation of an appropriate security directive and the introduction of measures in information and cyber security are the role and position of the cyber security manager, the advisory body – the security committee of the self-governing region, as well as the significant importance of the audit of critical threats and rules in the field of information and cyber security. The creation of suitable security rules is increasingly coming to the fore even in relatively non-progressive public administration.

Key words: cyber security, security manager, security committee, audit of cyber security, self-government, region.

Introduction

The necessity of introducing modern elements of cyber security is becoming more and more evident in public administration components, especially in the regional (county) establishment, with increasing threats of cyber incidents. The article sets itself the task of proposing optimal technical, organizational and personnel measures, the implementation of which the regional self-government will declare the goal of achieving compliance with the legislative requirements arising from the relevant legislation on cyber security at least at the level of 80%. At the same time, the article presents the possibilities of approaching from the point of view of cyber security in public administration to the operational program integrated infrastructure, in priority axis 7 – Information society, with a focus on "Development of governance and the level of information and cyber security in the sub-sector of the Security Service" and, last but not least, the fulfillment of the requirements of the National Security Office in the current situation of the ongoing conflict in Ukraine.

In the following lines, we will describe the basic legislative procedures for the creation of effective protection of the level of public administration – a self-governing region against incidents of the current modern infrastructure in the field of information and cyber systems. Among the most important steps in the preparation and implementation of an appropriate security directive and the introduction of measures in information and cyber security are the role and position of the cyber security manager, the advisory body – the security committee of the self-governing region, as well as the significant importance of the audit of critical threats and rules in the field of information and cyber security. The creation of suitable security rules is increasingly coming to the fore even in relatively non-progressive public administration, compared to the private sector

and large ICT corporations, which are advancing by leaps and bounds when it comes to cyber security.

Result and Discussion

Manager of cyber security of the self-governing region

The cyber security manager is a management job position in the self-governing region, for which the abbreviation "CISO" (from the English "Chief Information Security Officer") is often given. It should be able to communicate and submit proposals and report information in the field of cyber security directly to the statutory body of the self-governing body. The cyber security manager must not be "deeply embedded" in the structure of the organization. However, in complicated and extensive organizational structures, such as the structure of a self-governing region (or its office), it is acceptable if the power of direct access to the statutory body is regulated procedurally, for example by internal regulations. The position of the cyber security manager must be independent from the department ensuring the operation of information and communication technologies. The role of the cyber security manager is mainly to ensure the organization's resistance to cyber security threats, manage related risks and resolve security incidents. The cyber security manager is often the "security counterweight" to the development and operation of information and communication technologies. He significantly participates in the protection of the assets of the self-governing region, sometimes he even has to decide on stopping the risky activity of the region, of course, depending on his competences. If the cyber security manager were dependent on the operation and development of technological services, there is a risk that even in crisis situations, decisions in the field of cyber security will be influenced mainly by the goals of the departments responsible for information and communication technologies and the operation of the self-governing region. Other tasks of the cyber security manager of the self-governing region are in the area of security management. The strategic management of information and cyber security of the region mainly includes the development and presentation of a security strategy and concept, the implementation of information and cyber security processes in accordance with generally binding legal regulations and other internal governing acts, as well as ensuring the development, maintenance and updating of security documentation of information and cyber security or the proposal budget requirements and other resources related to the financing of security measures and processes. The personnel point of view is also important – methodical guidance of administrators and managers of information and communication technologies, process owners, asset owners, senior employees and other responsible employees in relation to achieving the security goals of the self-governing region, providing information to the security committee and the statutory body about the state of information and cyber security or about serious security risks, incidents and significant security events. In the field of threat and risk management, the tasks of the cyber security manager mainly include the identification, analysis and monitoring of security threats and risks, the proposal of measures to prevent the impact of security events, ensuring the assessment of the technical vulnerability of systems, detection, recording and prevention of cyber incidents, or the processing of a functional continuity plan and recovery of regional activities (the so-called Business Continuity Management), including planning the recovery of systems after a disaster (the so-called Disaster Recovery Planning).

In the area of the application of security measures, the security manager mainly manages the processing of proposals, their implementation, changes and optimization of security solutions with a vision of their trouble-free operation, as well as management of the security architecture and submission of expert opinions on new changes in the IT infrastructure that may have a potential impact on the security of information assets self-governing region. This manager has the task of leading a team of employees of the information and cyber security department, if such an

organizational department is established. The partial tasks also include ensuring the sustainability of organizational measures, including the maturity of security processes, ensuring the application of the principle of separation of powers and responsibilities in the entire organizational structure of the region so that so that the same person is not responsible for carrying out and at the same time approving or controlling safety-relevant activities and activities. In the field of compliance management, it plays a role in processes of guaranteeing compliance (so-called Compliance Management) in the field of information and cyber security, ensuring regular review of the state of cyber and information security, evaluating compliance with internal regulations related to cyber security management, providing cooperation to internal and external audits of information and cyber security, designing metrics and key indicators for monitoring the development and status of security and the development of security risks, ensuring employee training in the field of cyber security and information security, ensuring continuous education for work roles relevant from the point of view of cyber security, ensuring the building of security awareness in the field of information and cyber security and personal data protection and cooperation with public authorities and law enforcement authorities.

Committee for security in the self-governing region

Pursuant to the Decree of the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization (2020), which establishes the method of categorization and the content of security measures of public administration information technology, there is a need to establish a security committee of the self-governing region for the field of information and cyber security as its permanent advisory body to ensure professional management in the field of information and cyber security, which will be established by the chairman of the self-governing region. The committee is an advisory body to the chairman of the self-governing region in the area of information and cyber security, especially in relation to the fulfillment of legislative requirements defined by the Act on Cyber Security, the Act on Personal Data Protection, as well as in relation to the requirements of the STN ISO/IEC 27001 standard – information security management system.

The committee needs to be defined in a processed document that will regulate the position, scope, composition and tasks of the security committee of the self-governing region. The security committee of the self-governing region is mainly to fulfill the tasks initiated by the cyber security manager, assess the adequacy of technical, organizational and personnel measures formulated by the cyber security manager, verify proposals for revision of the security policy and subsequent security guidelines of the self-governing region. The committee also assesses the effects on data protection, as well as other documents related to information and cyber security, personal data protection and ensuring compliance with the requirements of the Regulation of the European Parliament and the Council of the EU (2016), as well as the Act on Information Technologies in Public Administration (2019), decrees of the National Security Office (2018, 2019), or the decree of the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization (2020, 2020).

On the basis of the adopted resolution from the meeting, the security committee submits to the chairman of the self-governing region for approval a proposal for responsibility for the implementation and application of individual cyber security and information security measures and procedures in the conditions of the self-governing region. At the same time, the committee of the self-governing region provides support to the cyber security manager in the coordination and methodical management of the fulfillment of established measures and requirements in the field of information and cyber security arising from the security policy, legislation and guidelines in the conditions of the region. Reminds the measures and procedures proposed by the cyber security manager to increase and maintain adequate information security and ensure compliance with security legislation, especially in the case of fundamental changes in the information system, which

he presents to the chairman. The committee coordinates and discusses processes, roles, strategies and technologies in the organizational, personnel and technical areas, the aim of which is to ensure cyber security during the life cycle of networks and information systems. Discusses activities related to information security, suspicious events and makes recommendations to the chairman on potential cyber and security incidents. Methodologically, the committee directs the updating and finalization of internal documentation for the management of information and cyber security, proposes and discusses related documents and recommendations as well as directives for the protection of personal data, and also adopts procedures proposed by the cyber security manager to build security awareness and educate employees of the regional office. personnel and technical areas, the aim of which is to ensure cyber security during the life cycle of networks and information systems. Discusses activities related to information security, suspicious events and makes recommendations to the chairman on possible cyber and security incidents. Methodologically, the committee directs the updating and finalization of internal documentation for the management of information and cyber security, proposes and discusses related documents and recommendations as well as directives for the protection of personal data, and also adopts procedures proposed by the cyber security manager to build security awareness and educate employees of the regional office. personnel and technical areas, the aim of which is to ensure cyber security during the life cycle of networks and information systems. Discusses activities related to information security, suspicious events and makes recommendations to the chairman on possible cyber and security incidents. Methodologically, the committee directs the updating and finalization of internal documentation for the management of information and cyber security, proposes and discusses related documents and recommendations as well as directives for the protection of personal data, and also adopts procedures proposed by the cyber security manager to build security awareness and educate employees of the regional office. Discusses activities related to information security, suspicious events and makes recommendations to the chairman on possible cyber and security incidents. Methodologically, the committee directs the updating and finalization of internal documentation for the management of information and cyber security, proposes and discusses related documents and recommendations as well as directives for the protection of personal data, and also adopts procedures proposed by the cyber security manager to build security awareness and educate employees of the regional office. Discusses activities related to information security, suspicious events and makes recommendations to the chairman on possible cyber and security incidents. Methodologically, the committee directs the updating and finalization of internal documentation for the management of information and cyber security, proposes and discusses related documents and recommendations as well as directives for the protection of personal data, and also adopts procedures proposed by the cyber security manager to build security awareness and educate employees of the regional office.

The security committee of the self-governing region is usually composed of permanent members – employees of the self-governing region resulting from their job position. The chairman of the committee is at the head, and other persons invited by the chairman can also participate in its meetings. However, invited persons have only an advisory role and do not have voting rights. Committee meetings are closed to the public.

Audit of cyber security in the self-governing region

We consider a cyber security audit to be a method of obtaining evidence about the state of security in a self-governing region. The task of this audit is to assess the compliance of the adopted security measures with the requirements of the Cyber Security Act (2018). The audit determines the effectiveness of the implemented measures and the manner of their operation as well as implementation in the environment of the self-governing region. Based on this, it is possible to take

measures to eliminate undetected risks and remedial action, thus preventing the risk of cyber security incidents. The result of the audit is the final report on the results of the cyber security audit of the self-governing region. After preparing the final report on the results of the cyber security audit, which is submitted to the National Security Office. The proposed measures resulting from this report can be divided according to their nature into technical, organizational and personnel. By implementing them, the self-governing region will declare the goal of achieving compliance with legislative requirements at least at the level of 80% within two years from the last audit. The active participation of the management of the self-governing region is a necessary prerequisite for the successful implementation of the measures, especially when approving the resources needed to implement the measures and ensuring the necessary support for security measures. This procedure is also a transposition of the directive of the European Parliament and the Council of the EU (2016) on measures to ensure a high common level of security of networks and information systems in the EU. namely achieving compliance with legislative requirements at least at the level of 80% within two years from the last audit. The active participation of the management of the self-governing region is a necessary prerequisite for the successful implementation of the measures, especially when approving the resources needed to implement the measures and ensuring the necessary support for security measures. This procedure is also a transposition of the directive of the European Parliament and the Council of the EU (2016) on measures to ensure a high common level of security of networks and information systems in the EU. namely achieving compliance with legislative requirements at least at the level of 80% within two years from the last audit. The active participation of the management of the self-governing region is a necessary prerequisite for the successful implementation of the measures, especially when approving the resources needed to implement the measures and ensuring the necessary support for security measures. This procedure is also a transposition of the directive of the European Parliament and the Council of the EU (2016) on measures to ensure a high common level of security of networks and information systems in the EU. especially when approving the resources needed to implement the measures and ensuring the necessary support for security measures. This procedure is also a transposition of the directive of the European Parliament and the Council of the EU (2016) on measures to ensure a high common level of security of networks and information systems in the EU. especially when approving the resources needed to implement the measures and ensuring the necessary support for security measures. This procedure is also a transposition of the directive of the European Parliament and the Council of the EU (2016) on measures to ensure a high common level of security of networks and information systems in the EU.

The measures can help prevent threats to the self-governing region, reduce its known vulnerabilities, protect its system from cyber threats, even if the threat has already been implemented and a harmful event has occurred. The task of applied preventive security measures is to detect such events in time and limit their negative impact. The aim of the subsequent reactive measures is also to guarantee compensation for losses caused by a harmful event or to obtain evidence for the continuation of legal proceedings aimed at punishing the perpetrators, recovering damages or inferring responsibility within the framework of the employment relationship. The achieved security goals allow to obtain a guarantee that the components of the information architecture can be considered trustworthy and reliable. The reliability of information is determined by its three basic security attributes: confidentiality, availability and integrity. It follows that the measures guaranteeing the security and reliability of the components of the information architecture should mainly aim to ensure confidentiality, availability and integrity. Security architecture is an interdisciplinary issue that extends across the entire enterprise architecture. It can be described as a comprehensive set of views and artifacts of information and cyber security, privacy and operational risk, including security objectives and security services. Even after its

amendment, the Cyber Security Act (2018) continues to preserve the principle of technical neutrality. It is therefore solely up to the decision of the leadership of the self-governing region, what range of security measures it decides to implement in its environment. The essence of the later assessment by the auditor is the effectiveness of security measures, i.e. in the end the assessment of the level of achieved capabilities, i.e. tasks, processes, roles and technologies in the organizational, personnel and technical areas, the aim of which is to ensure cyber security during the life cycle of networks and information systems. The Decree of the National Security Office (2018) understands that security measures are either general, establishing the content of security measures and the structure of security documentation, or sectoral, which are implemented on the basis of certain specifics of the categorization of networks and information systems. The reason for their existence and the effect of generally binding regulations is the legislator's intention to solve the real specifics of some industries, for example energy, air transport, healthcare or industrial production. The problem at the level of the self-governing region is the fact that the relevant decree of the Office of the Deputy Prime Minister for Investments and Informatization (2020) does not effectively define any specifics of the public administration sector and thus, compared to the NBU decree, it does not introduce any additional requirements for security measures.

Conclusions

The period of recent years bears witnesses to intensifying information and cyber-attacks in the functioning of regional self-government. Currently, an enormous vulnerability of systems in municipalities is critical, which is also indicated by codes such as CVE-2022-42856, and such a vulnerability is actively exploited by attackers. The vulnerability is given in the so-called numerical expressions “CVSS score”, the highest of which in the case of multiple vulnerabilities reaches the value of 9.8 out of 10 numerical points. For illustration, the Apple iOS operating system in a version older than 12.5.7 is also in such a critical vulnerability. If a cyber security incident is detected in the municipality, the attack must be immediately reported to the National Cyber Security Center “SK-CERT” (incident@nbu.gov.sk). Currently, the National Security Office often issues warnings about the increased risk of cyber security incidents by pro-Russian oriented community hacker groups on Slovak targets in relation to the security of networks and information systems of public administration, including elements of critical infrastructure and other organizations. The NBU issues such warnings mainly on the basis of information it has obtained through its own activities and cooperation with other state security agencies. To protect against attacks, organizations are immediately recommended to create backup sites of systems and services, or their redundancy, to publish static websites to the Internet, ideally in an external hosting company (the editorial system, installed in an internal network inaccessible from the Internet, generates HTML files, images and styles, which are subsequently transferred to the hosting service), strictly separate sensitive data and operationally critical assets from public websites, implement a security infrastructure capable of filtering the attacker's IP addresses in large volume with options for setting “geofencing” – limiting the countries from which incoming connections are allowed, setting firewall rules and allowing only selected IP addresses, etc. At the same time, it is necessary to enforce multi-factor authentication and use a VPN for remote access, disable all ports and protocols that are not necessary for the operation of networks, systems and services, map all public services of the self-governing region exposed to the Internet and then completely shut down unnecessary and unused systems. update outdated systems, delete old accounts and configure the mail server to so that harmful and suspicious emails do not reach users' or employees' mailboxes. Update the password policy to prohibit the use of the same password for different services and to enforce the use of strong passwords or passphrases. It is recommended to avoid SMS verification and social engineering (physical tokens). Cloud services cannot be used as a repository for critical information

assets, such as trade secrets, personal data, infrastructure plans, classified information, and the like. It is also important that every employee knows who to contact in the event of a suspected information and cyber incident, as well as the 24/7 availability of the region's key cybersecurity operations and management personnel. Even in the organizational platform of the self-governing region, there is a need to educate its employees about the risks of cyber security incidents and to inform them about the increased risk of attacks. Educational activities need to be done in a targeted manner, according to the roles and responsibilities of individual employees – ordinary users (principles of social engineering), administrators (rules of secure infrastructure), cyber security specialists (specialized security education).

References

REGULATION of the European Parliament and the EU Council no. 2016/679 on the protection of natural persons in the processing of personal data and on the free movement of such data.

DECREE no. 436/2019 Coll. National Security Office on Cyber Security Audit and Auditor Knowledge Standard.

DECREE no. 362/2018 Coll. of the National Security Office, which establishes the content of security measures, the content and structure of security documentation and the scope of general security measures.

DECREE no. 179/2020 Coll. Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization, which establishes the method of categorization and the content of security measures of public administration information technologies.

DECREE no. 78/2020 Coll. Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization on standards for public administration information systems.

DECREE no. 85/2020 Coll. Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization on Project Management.

LAW no. 69/2018 Coll. on cyber security and amendments to some laws.

LAW no. 18/2018 Coll. on the protection of personal data and the amendment of some laws.

LAW no. 95/2019 Coll. on information technologies in public administration and on the amendment of some laws.