NATIONAL CYBERSECURITY STRATEGY ACTION PLAN FOR CYBER RESILIENCE: QUALITATIVE DATA AND ACHIEVEMENTS

William Steingartner, Darko Galinec

Technical University of Košice (Slovakia), Zagreb University of Applied Sciences (Croatia)

william.steingartner@tuke.sk; darko.galinec@tvz.hr

EXTENDED ABSTRACT

Cyber issues of importance to the state and the global environment represent a much wider area than the field of cybersecurity and are closely related to several traditional departments of public administration. Cybersecurity in these matters is the basis for their smooth development in the virtual dimension of modern society. Cybersecurity is a part of all public administration processes, as all processes rely on the proper functioning of communication and information systems, either directly, through data processing, storage, and transmission, or in directly through the management of basic services (e.g., electricity distribution, transport, etc.). Given the widespread dispersion of responsibilities of state bodies in cyberspace, the establishment of the National Council for Cybersecurity, Operational and Technical Coordination for Cybersecurity and the development of the National Cyber Security Strategy and Action Plan for its implementation establishes a mechanism for sharing information and harmonizing public administration professional and political/administrative level. This paper presents a qualitative assessment of the implementation of the Action Plan of the Strategy based on the outcomes of reporting to the holders and co-carriers of the implementation of the Action Plan's measures at the state level.

In the development of the National Cybersecurity Strategy and Action Plan for its implementation comprehensive approach to cybersecurity by covering cyberspace and infrastructure and users that fall under the jurisdiction of the Republic of Croatia (citizenship, registration, domain, address) is used as well as integration and harmonization of activities and measures arising from various aspects of cybersecurity and falling under the competence of various organizations and their complementarity in order to create a safer common cyberspace.

A proactive approach by constantly adapting the activities and measures applied in cyberspace and by occasionally adapting the relevant strategic frameworks was needed for strengthening the resilience, reliability, and adaptability of information systems by implementing certification, accreditation, and security protocols (Szymoniak, 2021a; Szymoniak, 2021b), especially taking into account the specific requirements of data, services and other business processes on information systems. Using probabilistic techniques, various parameters and behaviors of security protocols embedded in the authentication systems can be thoroughly examined (Siedlecka-Lamch, 2020). The basic principles on which modern society is based (Cesarec, 2020; Gálik & Tolnaiová, 2019) are also applied in the cyberspace that makes up the virtual dimension of society:

- Application of the law for the purpose of protection of human rights and freedoms, especially privacy and the right to expression, property, and all other essential features of an organized modern society.

- Harmonized legislative framework and continuous improvement of regulatory mechanisms through harmonized initiatives of all sectors of society, i.e., bodies and legal entities.
- The principle of subsidiarity through the systematic elaboration of the power to decide and inform on cybersecurity issues to the body whose competence largely covers the problem to be solved, whether the problem relates to the organization, coordination and cooperation, or technical capabilities to respond to computer communication threats and information infrastructure.
- The principle of proportionality between the increase of protection measures and responsibilities and decreasing negative consequences (Tokarčíková et al., 2014) and accompanying costs and reduction of associated risks, i.e., greater possibilities to limit the threats that cause them.

Adopting a national cybersecurity strategy is one of the most important first steps in securing the national cyber infrastructure and services upon which the digital future and economic wellbeing of a modern nation depend (Spidalieri, 2017). Due to the ever-increasing availability and variety of sophisticated malicious digital tools and the ease with which these tools can be deployed, cybersecurity is now a crucial element of national security. Within this larger context, the concept of cyber defense, with its implicit military connotation, has also gained significantly more prominence (Dewar, 2018). In the following parts, we focus on countries which, in view of our best knowledge, we have found to have clear explanations key policy principles on cybersecurity, cyber defense and cyber resilience as essential concepts.

Cybersecurity and cyber defense are constantly shifting and evolving topics. The technology used to carry out cyber-attacks, and the tools required to mitigate or deter those attacks, is in a constant state of development and innovation. As a result, national policy relating to these topics also undergoes periodic shifts and changes, depending on national priorities (Dewar, 2018).

The National Cybersecurity Strategy planning and the Action Plan for its implementation development have been created and executed based on integration, inclusiveness and integrity principles by drafting strategic guidelines, concept development, plan development and plan assessment to achieve situational awareness at the national level. Furthermore, one of the main principles of the strategy was strengthening resilience, reliability and adjustability by applying universal criteria of confidentiality, integrity and availability of certain groups of information and recognized social values, in addition to complying with the appropriate obligations related to the protection of privacy, as well as confidentiality, integrity and availability for certain groups of information, including the implementation of appropriate certification and accreditation of different kinds of devices and systems, and also business processes in which such information is used (Dewar, 2018).

According to Gartner in (Top Priorities, 2020), security and risk management leaders are key enablers of digital business and are accountable for helping the enterprise balance the associated risks and benefits. By 2023, 30% of chief information security officers' effectiveness will be directly measured on the role's ability to create value for the business.

Three trends are making the highest impact for security and risk management leaders to be effective in their role and deliver business value to their organizations (Top Priorities, 2020):

- Citizen computing accelerates. Citizen computing is when a user creates new business applications using development and run time environments approved by IT. However, it's generally outside of IT visibility and traditional enforcement, which creates complexities for security and risk leaders tasked with protecting the organization.
- New digital initiatives create challenges. The security team is often not consulted until digital plans for the organization are well underway. In addition to reorienting the security program to address new technologies, effective security leaders are working with the board and business leaders to manage cyber-risk control expectations.
- Cybersecurity mesh emerges as the preferred delivery model for security services. This cloud-based and highly modular architecture makes it much more practical to control the uncontrollable. Cybersecurity mesh is the most efficient and effective way to extend security policy to digital assets that are outside of the traditional enterprise.

The main goal of this paper is to present the results of the implementation of the National Cyber Security Strategy because of research by qualitative analysis based on reports of sectoral bodies as responsible bodies for the implementation of action plan measures and implementation of the strategy.

KEYWORDS: Action plan, cyber attack, cyber defense, cyber resilience, national cybersecurity strategy, qualitative assessment.

REFERENCES

Arias-Oliva, M., Pelegrín-Borondo, J., & Matías-Clavero, G. (2019). Variables Influencing Cryptocurrency Use: A Technology Acceptance Model in Spain. *Frontiers in Psychology*, 10. https://doi.org/10.3389/fpsyg.2019.00475

Cesarec, I. (2020). Beyond physical threats: Cyber-attacks on critical infrastructure as a challenge of changing security environment – overview of cyber-security legislation and implementation in SEE countries. *Annals of Disaster Risk Sciences*, 3(1), 2020.

Dewar, R.S. (2018). National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1. Center for Security Studies (CSS), ETH Zürich.

Gálik, S., & Tolnaiová, S.G. (2019). Cyberspace as a New Existential Dimension of Man, Cyberspace, Eds. E. Abu-Taieh, A. E. Mouatasim, and I. H. A. Hadid. IntechOpen, Rijeka, 2019, chap 2.

Siedlecka-Lamch, O. (2020). Probabilistic and Timed Analysis of Security Protocols. 13th International Conference on Computational Intelligence in Security for Informa tion Systems (CISIS 2020). Advances in Intelligent Systems and Computing, vol 1267, Eds. Herrero, Á., Cambra, C., Urda, D., Sedano, J., Quintián, H., & Corchado, E. Springer, 2021, p. 142–151.

Spidalieri, F. (2017). Italy: Building a Cyber Resilient Society, available online (accessed on 2022-04-19). Retrieved from https://www.ispionline.it/it/pubblicazione/italy-building-cyber-resilient-society-18229

Szymoniak, S. (2021a). Using A Security Protocol To Protect Against False Links, Moving technology ethics at the forefront of society, organisations and governments ETHICOMP

Book Series, Eds. Jorge Pelegrín Borondo, Mario Arias Oliva, Kiyoshi Murata, Ana María Lara Palma, pp. 513-525.

Szymoniak, S. (2021b). Security protocols analysis including various time parameters. *Mathematical Biosciences and Engineering,* 18(2): 1136-1153. http://doi.org/10.3934/mbe.2021061

Tokarčíková, E., et al. (2014). Automotive Company's social responsibility in Slovakia, Proceedings of the 24th International Business Information Management Association Conference – Crafting Global Competitive Economies: 2020 Vision Strategic Planning and Smart Implementation, pp. 2118-2127.

Top Priorities for IT: Leadership Vision for 2021 (2020). Gartner, Inc.