INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGIES, ENGINEERING AND MANAGEMENT SCIENCE

Managing Cybersecurity at National Level

Martin Mazúch[1], Boris Bučko, Roland Kelemen[2], Adam Farkas[2]
[1]University of Žilina, Žilina, Slovakia,
[2]Széchenyi István University, Hungary
martin.mazuch@fri.uniza.sk, boris.bucko@gmail.com,
kelemen.roland@ga.sze.hu, dradamfarkas@gmail.com

Abstract

A comprehensive and flexible national cybersecurity policy is necessary to guarantee the safety and security of citizens in a democracy. This plan must effectively tackle the ever-changing and progressive nature of cyber threats posed by nation-states, criminal syndicates, and individual hackers. This article explores the critical role of a robust cybersecurity framework in safeguarding a nation's digital infrastructure. It delves into the key components and principles that underpin effective cybersecurity management at the national level. By providing a comprehensive overview, this article aims to contribute to informed policymaking and the development of resilient national cybersecurity strategies.

Keywords: cybersecurity strategy, national security, digital resilience, cyber threats

Introduction

One of the fundamental responsibilities of the state in a democratic society is to guarantee the security and safeguard the rights, freedoms, and property of its citizens. To successfully do this mission, it is necessary to continuously enhance the state's readiness to confront security issues, threats, and emergencies. Additionally, it is imperative to actively participate in upholding global peace and security, proactively address circumstances that jeopardize the safety of the nation and its inhabitants, and possess sufficient resources, tools, and strategies.

The world is in a perpetual state of flux, with periods of increasing instability, unpredictability, and thus diminished security. Due to ongoing changes in the social landscape and rapid advancements in information technology, society is increasingly susceptible to many forms of dangers. This is subject to dynamic changes based on the prevailing circumstances and advancements in technology.

This scenario presents a chance to strategically assess and establish the security policy of the state. The development of the state's Security Strategy is a direct response to the continuous shifts in the security landscape and the requirement for a comprehensive strategy to ensuring our security, given our membership in the North Atlantic Alliance and the European Union.

The security plan is focused on the state level, however, the security of the state also has a substantial impact on the security of neighboring states. Given the European Union's global perspective, it is crucial to align with other countries in pursuing shared security goals and policies, taking into account their unique national or historical circumstances.

Creating an Effective National Cybersecurity Strategy

Like many other countries, the European Union countries is facing an increasing amount of cyber threats. The dangers originate from diverse sources, encompassing state entities, criminal syndicates, and individual hackers. Cyber-attacks have the potential to interrupt vital infrastructure, pilfer confidential information, and result in substantial financial harm.

EU Member States must consistently enhance and adapt their cybersecurity plans to combat novel and emerging cybersecurity threats. National cybersecurity strategy (NCSS) are the main documents utilized by national governments to set strategic goals, norms, and objectives. They also outline specific actions to mitigate cybersecurity risks in certain circumstances. Directive (EU) 2022/2555, known as NIS2, replaced Directive (EU) 2016/1148 on January 16, 2023. As to the findings of The European Union Agency for Cybersecurity - ENISA, NIS2 improves the existing level of cybersecurity in multiple ways across the European Union. The objective of NIS2 is to enhance cybersecurity across the European Union. ENISA is working in collaboration with Member States to identify and establish best practices throughout the European Union, with the aim of assisting in the implementation of the Directive.[1]

Every country must have a comprehensive national cybersecurity policy because cyber threats are ever-evolving. This strategy will function as a definitive and exact blueprint, guiding national efforts to protect essential infrastructure, ensure the security and accuracy of data, and foster a robust and flexible digital ecosystem. Creating an effective cybersecurity strategy is a complex undertaking that requires careful consideration of key strategic elements, incorporation of established cybersecurity plans and best practices, and seeking guidance from specialized cybersecurity organizations.

An effective cybersecurity plan must recognize cyberspace as a crucial component of contemporary society, intricately intertwined with sectors such as healthcare, finance, manufacturing, education, military, and social media. The policy should prioritize cybersecurity as essential for maintaining economic stability, protecting critical infrastructure, preserving democratic integrity, safeguarding data privacy, and ensuring national defense, given the widespread influence of technology.

In light of the increasing prevalence of state-sponsored cyber warfare and cyberterrorism, which have the potential to disrupt global economy and democratic societies, it is imperative to develop a policy that promotes prompt international cooperation between states and cyber defense teams in order to effectively address and minimize these risks. This strategy of collective defense guarantees constant watchfulness and prompt action against cyber threats that endanger both national and global interests.

In order to tackle the intricate nature of modern cyber threats, the strategy should promote a fundamental change in the mindset of cybersecurity. This transition entails adopting a shared duty for cyber accountability and individual cyber protection. This highlights the importance of implementing programs and forming partnerships between industry and government to promote efficient coordination and tackle market failures, therefore reducing the consequences of cyber disasters.

Moreover, the approach should readjust incentives to encourage long-term investments in cybersecurity infrastructure. This involves making use of all accessible resources to modify incentive programs, promoting proactive actions to strengthen cybersecurity resilience.

To redefine the approach to cybersecurity, the plan should incorporate new foundational principles to enhance cyber protection. The pillars encompass the following:

1. Safeguarding Critical Infrastructure.
2. Countering and dismantling threat actors.
3. Shaping Market Forces.
4. Investing in a Resilient Future.
5. Forging International Partnerships.

These factors together create a strong and effective cybersecurity policy, enabling governments to confidently and resiliently handle the changing landscape of cyber threats.

As previously stated, a recommended method for developing a country's cybersecurity strategy is to utilize an existing strategy, enhance it, and adapt it to the specific requirements of the country. This should be done in consultation with the author of the original strategy and dedicated cybersecurity institutions such as ENISA. This approach can yield significant advantages, particularly in a cohesive geographic region such as the European Union, where countries collaborate closely, face similar cybersecurity concerns, and strive to accomplish shared objectives in the digital realm.

In the subsequent sections, we aim to provide and analyze crucial elements for the effective formulation of a comprehensive national cybersecurity plan. We are referencing established plan from the Slovak Republic, which has formulated a comprehensive National Cyber Security plan 2021-2025. This strategy aims to protect the cyberspace of the Slovak Republic and guarantee a secure digital environment for its residents and enterprises. In general, a comprehensive NCSS should:

1. Strengthen national cybersecurity resilience.
2. Protect critical infrastructure.
3. Enhance public awareness of cyber threats.
4. Promote international cooperation on cybersecurity.

There are also four strategic pillars which should be covered: prevention, detection, response, recovery.

Each pillar is supported by a number of specific measures that are designed to achieve the overall objectives of the strategy.

Principles

The cybersecurity of the Slovak Republic is overseen through a comprehensive framework that includes regulations, risk management, detection and response to cybersecurity incidents, system recovery, education, security awareness, and research and development of cybersecurity tools and processes. In order to guarantee the efficiency of a system on a large scale and encourage cooperation among those responsible for its upkeep and advancement, it is essential to follow basic principles based on democratic values, the rule of law, and a modern outlook on national cybersecurity and international collaboration in this field.

Cyberspace is a domain where an increasing number of individuals engage in ongoing digital metamorphosis. It is a location where individuals not only fulfill their needs, but also share a part of their identity and privacy. The Internet is employed for various objectives, such as communicating with our relatives and friends, purchasing consumer products, making bill payments, and managing our smart homes. The North Atlantic Treaty Organization recognizes cyberspace as a distinct operational realm, in addition to its official designation as such.

Similar to the real world, cyberspace is additionally imperfect. In the last two decades, there has been a rise in the frequency of cyberattacks, an escalation in the sophistication of the attackers, and an upsurge in the financial losses suffered by the victims.

In order to ensure the protection of basic human rights and freedoms, such as the right to privacy, it is crucial to establish explicit regulations that mirror those outlined in the constitution. Additionally, it is important to view cyberspace as equivalent to the real world. This will guarantee that the online realm is not only secure, but also unrestricted, liberated, and available to all individuals who are concerned. The preservation of the digital sovereignty of the member states of the European Union is essential for ensuring the protection of fundamental human rights and freedoms in the digital realm. This also guarantees the preservation of the governments' autonomy and sovereignty in the realm of cyberspace. The security of cyberspace must be intrinsically linked to its liberty.[2]

The strategic objectives of cybersecurity

Efficiently overseeing a cybersecurity system requires more than just creating extensive regulations and installing necessary security measures. At the national level, cybersecurity should be recognized as a vital national interest that protects not only government assets, but also as one of the fundamental services that the government provides to its citizens and businesses. The implementation of the State's cybersecurity activities should be based on fundamental strategic concepts, while also effectively tackling the existing and prospective future cybersecurity threats and the national governance structure.

In order to guarantee the successful execution of cyber security strategic principles and an adequate reaction to threats, it is imperative to define unambiguous and quantifiable strategic objectives. By attaining these goals, it will be feasible to impartially assess their influence on improving the cyber security system in the particular country where the NCSS is created and executed.

Based on the strategic principles and recognized threats, the subsequent strategic objectives have been established.

State prepared for cyberthreats

Establishing national mechanisms is crucial for implementing effective security measures. These mechanisms should focus on defining cybersecurity policies, managing the system, detecting and resolving issues, enhancing professional skills, and promoting situational and security awareness. Furthermore, in order to build trust, the state must carry out the aforementioned measures in accordance with the Constitution and other legal requirements, while only encroaching upon fundamental human rights and freedoms to the extent that is absolutely necessary.

Efficient identification of cybercriminal activities

The incidence rate of cyber security breaches, which are also categorized as cybercrime offenses, is steadily increasing. As adversaries have become more sophisticated, it has become more difficult to identify and detect their attacks. Victims endure substantial damage, often putting their financial survival at risk. Cyber-attacks are carefully planned and executed, with the culprits skilled at hiding their operations and avoiding discovery. Identifying culprits is an extremely difficult task that requires an adequate quantity of proficient staff and defined protocols.

Resilience within the private sector

Commercial sector providers play a vital role in providing a diverse range of services to individuals, as well as to the commercial sector and governmental agencies. As per the Cybersecurity Act and the Critical Infrastructure Act, critical infrastructure components are classified as vital automated services. The individuals responsible for operating these pieces are categorized as essential service operators. These services and their operators are crucial in guaranteeing the effective operation of society. These companies have a large number of customers and have a significant impact on the economy. Additionally, they play a significant role in ensuring the protection of human life and well-being, as well as influencing public order, safety, and the transportation of individuals and goods. Ensuring their security is vital since it not only enables the continuous provision of important services but also promotes their expansion and progress.

Building strong partnerships

For any democratic state governed by the rule of law, security is a primary priority. The field of cyber security is not immune to this phenomenon, and it is extensively globalized, as cyber-attacks ignore national borders and the culprits may not necessarily be residents of the country being targeted. Therefore, it is imperative for a state to build strong international alliances in order to share experiences, skills, and information, and then apply them within its own borders. The advancement of cybersecurity is guaranteed by collaborative efforts and the establishment of trust among government agencies, businesses, and academia.

Truly educated professionals and general public

Education is essential for improving the creation and capabilities of intricate cybersecurity systems. Cultivating situational and security awareness among ordinary users functions as a proactive strategy to avert cybersecurity incidents. Users that possess a high level of knowledge and awareness are better equipped to effectively address and mitigate security threats and dangers in the digital domain. Moreover, they are more inclined to behave properly and refrain from being targets of successful attacks due to their lack of awareness. Understanding the importance of security awareness raising is essential as a comprehensive educational process, in which the student not only comprehends the subject matter but also establishes a connection with it.

Research and development capabilities in cybersecurity

The perils and vulnerabilities in the online realm are in a constant state of flux as technology progresses and society becomes increasingly digitized. Engaging in cybersecurity research and development is a proactive and efficient strategy to tackle the ever-changing security environment. It enables the implementation of essential measures to minimize assaults, address vulnerabilities, and promptly identify and handle cybersecurity problems.

Any nation needs a cybersecurity policy for various reasons:

- Protecting Critical Infrastructure: Power grids, banking institutions, and communication networks in modern societies depend on interconnected digital systems. Cyberattacks on key facilities can interrupt services, damage the economy, and endanger lives. The vulnerabilities and security measures are identified and prioritized by a national cybersecurity plan.
- Protecting Data and Privacy: Digital technologies generate massive volumes of personal and sensitive data. Cyberattacks on sensitive data can cause identity theft, financial losses, and reputational harm. A strong cybersecurity plan protects citizens' data.
- Economic Growth and Innovation: A secure digital environment inspires company investment and innovation. Cyberattacks impair business operations and damage customer trust, stifling economic progress.
- Maintaining National Security: Cyberattacks can target national security assets and secret data. A cybersecurity strategy protects critical data and national security from cyber espionage and sabotage.
- Protecting Global Stability: Cyberattacks can affect nations worldwide. A global cybersecurity plan allows countries to share threat intelligence and coordinate response operations to mitigate cyber threats and secure the digital environment for all.

In the digital age, a strong national cybersecurity policy shields a nation's key infrastructure, data, economy, and security. It creates a durable and secure digital environment, boosting national economy and stability.

Conclusion

Safeguarding the security and safeguarding the rights, freedoms, and property of citizens is a fundamental obligation of the state in a democratic society. This mission requires a constant improvement of the state's readiness to confront security problems, threats, and emergencies. The ever-changing and progressive global security landscape, influenced by societal shifts and technological progress, necessitates a comprehensive and flexible national security plan. In this context, it is crucial to establish a national cybersecurity policy, especially for EU Member States that are more vulnerable to cyber-attacks from state actors, criminal organizations, and individual hackers.

An effective national cybersecurity policy should function as a well-defined blueprint to protect vital infrastructure, guarantee the security and accuracy of data, and foster a strong and adaptable digital ecosystem. The key elements encompass safeguarding vital infrastructure, impeding malicious actors, influencing market dynamics to promote security, allocating resources towards building resilience for the future, and establishing international alliances. Engaging in partnerships with specialized cybersecurity organizations like ENISA and drawing insights from established approaches, such as Slovakia's National Cyber Security Strategy 2021-2025, can play a crucial role in formulating a successful policy.

References

[1] National Cybersecurity Strategies Guidelines & tools (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools).

[2] National Cybersecurity Strategy of the Slovak Republic for years 2021-2025 (https://www.nbu.gov.sk/national-cybersecurity-strategy-of-the-slovak-republic-for-years-2021-2025/).