РОЗДІЛ 2
ІНСТИТУЦІЙНІ НА ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Rychlik Andrzej
Lodz University of Technology
PhD, associate professor at the Institute of Information Technology,
Faculty of Technical Physics, Information Technology and Applied Mathematics
University of Technology and Humanities in Radom
PhD, associate professor at the Department of Computer Science and Teleinformatics
Faculty of Transport, Electrical Engineering and Computer Science

THE NEED TO AMEND THE ACT ON THE NATIONAL CYBERSECURITY SYSTEM IN POLAND

From August 28, 2018, the Act on the national cybersecurity system [2] is in force in Poland, implementing the Directive of the European Parliament and of the Council (EU) on measures for a high common level of security of network and information systems in the territory of the European Union (Directive 2016/1148) , the so-called the NIS Directive. [5] This act was adopted by the Polish parliament with an overwhelming majority of votes, although the work on it and public consultations were full of contradictions and doubts.

Figure 1 shows the architecture of the national cybersecurity system built on the basis of the applicable act. The national cybersecurity system aims to ensure cybersecurity at the national level, in particular:

- uninterrupted delivery of essential digital services,
- achieving a sufficiently high level of security of ICT systems used to provide these services.

Although two years have passed since the adoption of the law, a complete national cybersecurity system based on the architecture shown in the figure has not yet been

built. The act defines an incident as an event that has or may have an adverse impact on cybersecurity. Based on it we are obliged to report each incident to the appropriate Computer Security Incident Response Team. The Cybersecurity College is a consultative and advisory body on planning, supervising and coordinating the activities of CSIRTs, sectoral cybersecurity teams and competent authorities.

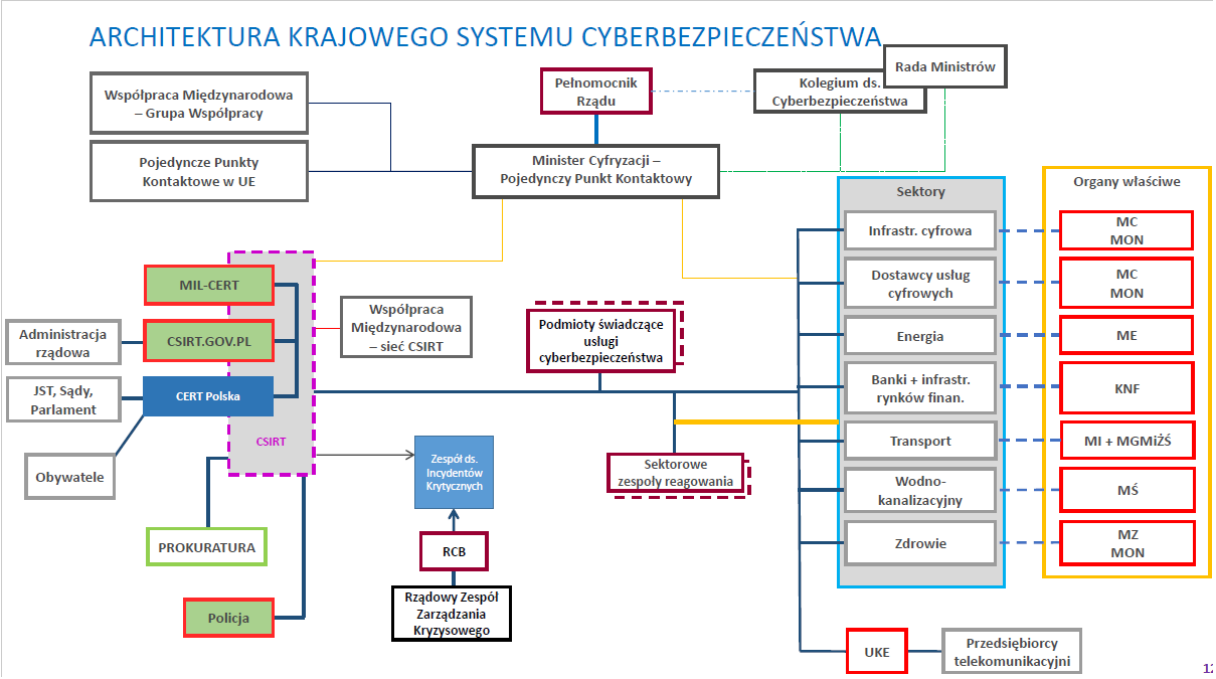

Fig. 1. Architecture of the national cybersecurity system [6]

Despite the statutory possibility, all sectoral cybersecurity teams have not been established so far. So far, only one such team has been established - the Polish Financial Supervision Authority's CSIRT for the financial sector at the Polish Financial Supervision Authority. The team was created based on internal resources and human resources of the Office of the Polish Financial Supervision Authority. In order to increase the effectiveness of responding to incidents, it is necessary to establish sectoral CSIRTs for each of the key sectors of the Polish economy. As a result, operators of essential services will be able to deal with incidents faster and more effectively, as they will receive direct support in responding to incidents. The College also issues opinions on cybersecurity requirements regarding the decisions of the President of the Office of Electronic Communications on frequency reservations. Due to the development of information and communication technologies, the transforming telecommunications infrastructure, the changing international political situation, user preferences, the

national cybersecurity system of 2018 did not stand the test of time and therefore needs to be reconfigured.

On July 24, 2020, the European Commission, with the support of ENISA and EU Member States, published the 5G Toolbox Implementation Report describing progress in implementing the EU toolbox and strengthening 5G network security measures. Toolbox was published in January 2020. It sets out a number of measures and actions to effectively reduce risk and ensure the implementation of secure 5G networks throughout Europe. 5G Toolbox provides standards-compliant features and reference examples for modelling, simulating and verifying 5G New Radio (NR) communication systems. Currently, Member States are gradually introducing these provisions.

On September 2, 2019, the US-Poland Joint Declaration on 5G was signed, in which we read: Taking into account that secure fifth generation wireless communications networks (5G) will be vital to both prosperity and national security in the near future, Poland and the United States declare their desire to strengthen our cooperation on 5G. Therefore, Poland and the United States endorse the Prague Proposals, the Chair's statement from the Prague 5G Security Conference, [3] as an important step toward developing a common approach to 5G network security and ensuring a secure and vibrant 5G ecosystem. Poland and the United States note that as part of a robust and comprehensive approach to network security, a careful and complete evaluation of 5G component and software providers is essential. [4]

On October 12, 2021, the government of the Republic of Poland noticed the delay of the legal system in the field of cybersecurity to the current ecosystem and sent a draft amendment to the act of July 5, 2019 to public consulations. The amendment made it possible to start work on the further development of the national cybersecurity system, and the experience gained over the two years of the system's operation in Poland indicated the need for changes at the statutory level. One of the most common problems is the lack of appropriate structures at operators of key services responsible for cybersecurity or the scope of their qualifications (including human resources) and the availability of information on cyber threats, which makes it difficult to effectively respond to incidents. The issue of access to expert knowledge on cyber threats is a key issue. The amendment also introduces certification in the field of cybersecurity.

The solutions adopted also serve to implement the Cybersecurity Strategy of the Republic of Poland for 2019-2024. A Cybersecurity Fund will be created from which activities aimed at ensuring cybersecurity in Poland will be financed. Resilience to cyber threats is highly dependent on the security of your hardware, software, and services. This applies to both ICT systems, telecommunications networks and industrial control systems. Therefore, the amendment provides for the introduction of a procedure for recognizing a supplier of hardware or software for entities of the national cybersecurity system as a high-risk supplier. Proceedings in this matter will be conducted by the minister responsible for computerization. The procedure will be based on transparent procedures specified in the Code of Administrative Procedure. It should be emphasized that the assessment of supplier risk profiles is one of the strategic tools (Strategic Measure - SM03) agreed by the Member States of the European Union, the European Commission and ENISA in the 5G Toolbox. [1]

The author proposes supplementing the governmental draft amendment with articles obliging operators of critical infrastructure to ensure energy independence for this structure. This is especially important in times of natural disasters, wars and revolutions. The second proposal is to ensure a high level of security of digital data transmission for the general public by educating it to use encryption and electronic signing of transmitted documents.

References

1. Commission Recommendation (EU) 2019/534 on the Cybersecurity of 5G networks, 26 March 2019

2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz. U. z 2020 r. poz. 1369

3. The Prague Proposals, The Chairman Statement on cyber security of communication networks in a globally digitalized world, Prague 5G Security Conference

4. U.S.-Poland Joint Declaration on 5G, Signed in Warsaw, Poland, on September 2, 2019

5. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems within the territory of the Union (Journal of Laws of the EU 2016 No. 194)

6. Szyszko A., Department of Safety and Crisis Management, Ministry of Energy, Meeting of the LTE working group

Ключові слова: кібербезпека, 5G Toolbox, інцидент, критична інфраструктура, сертифікація

Ключевые слова: кибербезопасность, 5G Toolbox, инцидент, критическая инфраструктура, сертификация

Keywords: cybersecurity, 5G Toolbox, incident, critical infrastructure, certification

Dykyi Oleh Viktorovych

National University «Odesa Law Academy»,

Dean of the Faculty of Cybersecurity and Information Technologies, Candidate of Law, Associate Professor

MODERN METHODOLOGICAL APPROACHES TO THE STUDY OF CYBER CRIMES

The XIX century was an era of total informatization and cybernation of all spheres of life in most countries. On the one hand, it has improved and simplified people's lives, and on the other, it has created new challenges, such as cybercrime.

In recent years, cybercrime has reached alarming proportions not only in Ukraine but in the world. This is largely due to the lack of proper international cooperation and the rapid processes that are taking place in the cyber environment. Every year, technologies change, new data systems are created, new software is used by criminals,