Jarosław Kostrubiec*

The position of the Computer Security Incidents Response Teams in the national cybersecurity system

Abstract

The purpose of the Computer Security Incident Response Teams is to ensure a coherent and complete system of risk management at the national level and, therefore, they have been obliged to perform tasks to counter cybersecurity threats of cross-sectoral and cross-border nature, as well as to ensure coordination of handling of reported incidents, i.e. events that have or may harm cybersecurity.

Key words: cybersecurity, incident, risk management

* Assoc. Prof. Jarosław Kostrubiec, PhD, Maria Curie-Skłodowska University in Lublin, Faculty of Law and Administration, e-mail: jaroslaw.kostrubiec@mail.umcs.pl, ORCID: 0000-0003-1379-9846.

Introduction

Security of networks and information systems (cybersecurity), in Art. 4 item 2 of the NIS Directive[1], is understood to mean the resilience of networks and information systems, with a given level of confidence, to any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or related services offered or accessible through those networks and information systems. Cybersecurity is a specific, specialized branch of security that includes the protection of information systems from threats[2].

In terms of entities, the national cybersecurity system is primarily made up of public entities, including some units of the public finance sector[3], and therefore also includes the Computer Security Incident Response Teams (CSIRTs). The legislator has included in this system those entities which, according to them, play an important role within the cybersecurity system, and which are also important from the point of view of the strategic interests of the state, including in the field of telecommunications[4]. An important place in the sphere of responsibilities of public entities is occupied by incident handling, which should be understood as activities that enable detecting, recording, analyzing, classifying, prioritizing, taking corrective actions, and reducing the effects of an incident[5].

Cybersecurity is one of the tasks of both government administration and local government, as well as other entities entrusted with the competence

1 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 across the Union (Official Journal of the European Union 2016, L 194, p. 1).

2 M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2, p. 42.

3 Public finance sector entities that make up the national cybersecurity system include the local government. It is a decentralized entity acting for the benefit of the local (or regional) community, equipped with legal personality as well as material, financial and personal resources to meet the needs of residents. More on the position of the local government in the (cyber)security space: M. Karpiuk, *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2; M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

4 M. Karpiuk, *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2, p. 237.

5 M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2, p. 57.

in this area. The legislator understands cybersecurity to mean the resilience of information systems to actions that compromise the confidentiality, integrity, availability, and authenticity of the data being processed or the related services offered by those systems. This definition arises under Art. 2 item 4 of the Act on the National Cybersecurity System[6]. National cybersecurity system entities have been required to protect against cybersecurity threats, therefore, against potential and actual causes of an incident perceived as an event that has or may harm cybersecurity[7]. It is important to emphasize that cybersecurity while having several characteristics that individualize it, constitutes an element of state security[8].

Competences of the Computer Security Incident Response Teams

The legislator defines the various CSIRTs in Art. 2 items 1–3 of the Act on the National Cybersecurity System. CSIRT GOV is a computer security incident response team operating at the national level and led by the Head of the Internal Security Agency; CSIRT MON, in turn, is a computer security incident response team operating at the national level and led by the Minister of National Defense, and CSIRT NASK is a computer security incident response team operating at the national level and led by the Research and Academic Computer Network (NASK) – National Research Institute.

Within the national cybersecurity system, special attention should be paid to the tasks of individual CSIRTs. According to Art. 26 sec. 1–2 of the

6 Act dated 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws 2020, item 1369, as amended).

7 K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021, p. 1.

8 Security is one of the basic human needs, which can be satisfied by both public and non-public entities, as well as by the interested parties themselves, to the extent that they are able to satisfy it. M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2, p. 67. Security is the domain which is very important for the state as a public institution, as well as for society or its individual members, and therefore should be considered in the category of common good. M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, no. 3, p. 15. More on the state security: M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3; M. Czuryk, *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, „Roczniki Nauk Społecznych" 2013, no. 3.

Act on the National Cybersecurity System, CSIRT MON, CSIRT NASK, and CSIRT GOV teams cooperate with each other, with the authorities responsible for cybersecurity, the minister in charge of computerization, and the Plenipotentiary, ensuring a coherent and complete risk management system at the national level, performing tasks to counter cybersecurity threats of cross-sectoral and cross-border nature, as well as ensuring coordination of handling of the reported incidents. When reasonably requested by critical service operators, digital service providers, public entities, sectoral cybersecurity teams, or the owners, owner-like possessors, or dependent possessors of facilities, installations, equipment, or services that are part of critical infrastructure[9], they may provide support in incident handling. Thus, the purpose of CSIRTs is, among others, to ensure the coordination of the handling of reported incidents, which means incidents that have or may have an adverse impact on cybersecurity.

The supportive role of CSIRTs during incident handling should be emphasized. The team does not directly step in to handle an incident at a specific entity, except in exceptional situations. Incident handling is the responsibility of the key service operator, the CSIRT has a supporting role. Handling an incident in a particular system requires in-depth knowledge of how the system works, how it is structured, what changes it has undergone, and what its weaknesses are. This is often internal knowledge that people outside the organization do not have. Therefore, the role of the CSIRT relies on analytical and investigative capabilities as well as the ability to share information with other entities that may already have a solution to the problem[10].

To avoid competence disputes, the legislator has defined the competences of the CSIRTs in Art. 26 of the Act on the National Cybersecurity System. Their tasks take into account the responsibilities assigned to each CSIRT to manage the state's cybersecurity. A directory of supported entities making

9 The Director of the Government Center for Security shall draw up, based on detailed criteria, in cooperation with the relevant ministries responsible for the systems, a uniform list of facilities, installations, equipment and services constituting critical infrastructure divided by systems. The list also distinguishes European critical infrastructure located on the territory of the Republic of Poland and European critical infrastructure located on the territory of other Member States of the European Union that may have a significant impact on the Republic of Poland. The list is classified, Art. 5b sec. 7 item 1 of the Act of 26 April 2007 on the Crisis Management (consolidated text, Journal of Laws 2020, item 1856, as amended).

10 J. Dysarz, *Komentarz do art. 26* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. A. Besiekierska, Warszawa 2019.

up the national cybersecurity system has also been established[11]. The tasks of CSIRT MON, CSIRT NASK and CSIRT GOV teams, in accordance with their respective competences, include (Art. 26 sec. 3–7 of the Act on the National Cybersecurity System): 1) monitoring cybersecurity threats and incidents at the national level; 2) estimating risks associated with disclosed cybersecurity threats and incidents, including conducting dynamic risk analysis; 3) communicating information on incidents and risks to national cybersecurity system entities; 4) issuing messages on identified cybersecurity threats; 5) responding to reported incidents; 6) classifying incidents, including major incidents and significant incidents, as critical incidents and coordinating the handling of critical incidents; 7) reclassifying major incidents and significant incidents; 8) submitting to the relevant team (CSIRT MON, CSIRT NASK or CSIRT GOV) technical information pertaining to the incident, the coordination of which requires cooperation of the CSIRT; 9) examining, in justified cases, the IT device or software to identify vulnerabilities, the use of which may threaten, in particular, the integrity, confidentiality, accountability, authenticity or availability of the processed data, which may have an impact on public security or a significant interest of state security, and submitting proposals on recommendations for the entities of the national cybersecurity system regarding the use of IT devices or software, in particular, with regard to the impact on public security or a significant interest of state security; 10) cooperating with sectoral cybersecurity teams in coordinating handling of major incidents, including those involving two or more European Union Member States, and critical incidents and in sharing information to counter cybersecurity threats; 11) forwarding to and receiving from other states, including European Union Member States, information on major incidents and critical incidents involving two or more European Union Member States, as well as forwarding to the Single Point of Contact notification of major and critical incidents involving two or more European Union Member States 12) submitting to the Single Point of Contact, by 30 May each year, a list of serious incidents reported in the previous calendar year by operators of key services, affecting the continuity of providing key services by them in the Republic of Poland and continuity of providing key services by them in the Member States of the European Union, as well as a list of significant incidents

11 M. Nowikowska, *Komentarz do art. 26* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 199–200.

reported in the previous calendar year by digital service providers, including those concerning two or more Member States of the European Union; 13) jointly developing and submitting to the minister in charge of computerization of the cybersecurity part of the report on threats to national security; 14) providing analytical as well as research and development facilities, which in particular: a) conduct advanced malware and vulnerability analyses, b) monitor cybersecurity threat indicators, c) develop tools and methods to detect and combat cybersecurity threats, d) conduct analyses and develop cybersecurity standards, recommendations, and good practices, e) support entities of the national cybersecurity system in building cybersecurity capabilities and capacities, f) conduct cybersecurity awareness building activities, g) collaborate on cybersecurity education solutions; 15) ensuring the possibility of making reports and providing information, as well as providing and operating means of communication allowing for making such reports; 16) participating in the CSIRT Network consisting of representatives of the competent CSIRT of the European Union Member States, the CSIRT competent for the institutions of the European Union, the European Commission and the European Union Agency for Cybersecurity (ENISA). The CSIRT MON, CSIRT NASK, and CSIRT GOV teams shall jointly develop the main elements of procedures for dealing with an incident, the handling coordination of which requires cooperation with the CSIRT and shall determine, in cooperation with the sectoral cybersecurity teams how to interact with those teams, including how to coordinate the handling of the incident. At the same time, the tasks of the CSIRT MON include coordination of handling incidents reported by: 1) entities subordinate to the Minister of National Defense or supervised by them, including entities whose information and communication systems or networks are covered by the uniform list of objects, installations, devices, and services included in the critical infrastructure; 2) enterprises of special economic and defense importance, in relation to which the organizing and supervising body for the execution of tasks for national defense is the Minister of National Defense. The tasks of the NASK CSIRT include: 1) coordinating the handling of incidents reported by: a) specified units of the public finance sector, b) units subordinate to government administration bodies or supervised by them, c) research institutes, d) Office of Technical Inspection, e) Polish Air Navigation Services Agency, f) Polish Centre for Accreditation, g) National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management, h) commercial law companies performing public utility tasks,

i) digital service providers, j) key service operators, k) individuals; 2) creating and providing tools for voluntary cooperation and exchange of information on cybersecurity threats and incidents; 3) providing a telephone line or internet service conducting activities in the field of reporting and analysis of cases of distribution, dissemination or transmission of child pornography through information and communication technologies. The tasks of CSIRT GOV include coordinating the handling of incidents reported by: 1) specified units of the public finance sector; 2) units subordinated to the Prime Minister or supervised by them; 3) the National Bank of Poland; 4) Bank Gospodarstwa Krajowego; 5) other entities whose information and communication systems or networks are covered by the uniform list of facilities, installations, devices and services constituting critical infrastructure. Importantly, the CSIRT MON, CSIRT NASK, or CSIRT GOV team that has received an incident report, and is not competent to coordinate its handling, shall immediately forward that report to the appropriate CSIRT along with the received information[12].

At the national level, in the operational and technical domain, the Act on the National Cybersecurity System decided to adopt a deconcentrated approach, according to which three equivalent CSIRTs operate within the national cybersecurity system. CSIRT teams are the technical level of incident handling coordination. The adoption of a deconcentrated solution for the operational and technical level is justified by the benefits that arise from the possibility of using experience, before the entry into force of the law[13].

According to Article 27 of the Act on the National Cybersecurity System, the CSIRT GOV team is competent with regard to incidents related to terrorist incidents, which should be understood as a situation suspected to have arisen as a result of a terrorist crime[14] or a threat of such a crime occurring, and the

12 See also K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, op. cit., p. 41–43.

13 K. Prusak-Górniak, K. Silicki, *Komentarz do art. 26* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

14 A crime of a terrorist nature is an offense, punishable by imprisonment with a maximum of at least 5 years, committed towards: 1) serious intimidation of many people; 2) forcing a public authority of the Republic of Poland or another state or an authority of an international organization to take or refrain from taking certain actions; 3) causing serious disturbances in the system or economy of the Republic of Poland, another state or an international organization – as well as threats to commit such an act, Art. 115 § 20 of the Act of 6 June 1997 – Penal Code (consolidated text, Journal of Laws 2020, item 1444, as amended).

CSIRT MON team is competent with regard to incidents related to terrorist incidents detrimental to the security of the national defense potential, the Polish Armed Forces and organizational units of the Ministry of Defense.

Conclusion

Cybersecurity is a common good that must be protected by law; therefore, it has special contemporary importance, it is very important for the normal functioning of the state, as well as the information society[15]. The common good is a fundamental element of public order and the system of a democratic state under the rule of law; thus it is the goal of public authorities' pursuit, and therefore public entities are responsible for it[16].

As part of the protection of cybersecurity (as a common good), individual CSIRTs are to ensure coordination of the handling of reported incidents, including their classification, indication of whether we are dealing with a critical incident, which is defined in Art. 2 sec. 6 of the Act on the National Cybersecurity System as an incident resulting in significant damage to public security or order, international interests, economic interests, operation of public institutions, civil rights and freedoms, or human life and health, classified by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV team.

CSIRTs have the expertise to handle incidents, so they have a supporting role. Nevertheless, their position in the national cybersecurity system is significant, because the analytical activities they undertake and their ability to share information significantly support the protection of cybersecurity.

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, no. 3.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, „Roczniki Nauk Społecznych" 2013, no. 3.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

15 M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2, p. 87.

16 M. Czuryk, *Bezpieczeństwo jako dobro*..., p. 15.

Dysarz J., *Komentarz do art. 26* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. A. Besiekierska, Warszawa 2019.
Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2.
Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Karpiuk M., *The Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2.
Nowikowska M., *Komentarz do art. 26* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.
Prusak-Górniak K., Silicki K., *Komentarz do art. 26* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

Miejsce zespołów reagowania na incydenty bezpieczeństwa komputerowego w krajowym systemie cyberbezpieczeństwa

Streszczenie

Celem działania zespołów reagowania na incydenty bezpieczeństwa komputerowego jest zapewnienie spójnego oraz kompletnego systemu zarządzania ryzykiem na poziomie krajowym. W związku z powyższym zostały one zobowiązane do realizacji zadań na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także w celu zapewnienia koordynacji obsługi zgłoszonych incydentów, czyli zdarzeń, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo.

Słowa kluczowe: cyberbezpieczeństwo, incydent, zarządzanie ryzykiem