The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland

Monika Nowikowska

Abstract Computer Security Incident Response Teams (CSIRTs) are specialised entities established to handle network and information system security incidents and cooperate with similar entities around the world, both in terms of operational, as well as research and implementation activities. The main tasks of CSIRTs include: recognition, prevention, recording and handling of events that breach network security, active response in the event of direct threats, cooperation with other CSIRT teams, and, finally, participation in national and international projects related to information security and research activities on the scope of methods for detecting security incidents. The article analyses the detailed tasks established on the basis of the Act of 5 July 2018 on the National Cybersecurity System of three CSIRTs operating in Poland: CSIRT MON, CSIRT NASK and CSIRT GOV.

Subsequent to the adoption on 6 July 2016 by the European Parliament and by the Council of the European Union of Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) all Member States were required to adopt a national strategy for the security of network and information systems, including the establishment of networks of Computer Security Incident Response Teams, known as CSIRT networks. The Preamble to the NIS Directive indicates that network and information systems and services play an important role in society. Their reliability and security are essential for economic and social activities, in particular for the functioning of the internal market.

The scale, frequency, and impact of security incidents are increasing, and constitute a serious threat to the functioning of network and information systems. These systems can also become the object of intentional harmful operations designed to

M. Nowikowska (✉)
Instytut Prawa/Institute of Law, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: m.nowikowska@akademia.mil.pl

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_15

damage or interrupt their performance. Such incidents can hamper business activities, cause significant financial losses, undermine user confidence and result in serious damage to the Union's economy.

In view of the differences between national management structures, the Member States were authorised to designate responsible national authorities (more than one) to be in charge of implementing tasks related to the security of network and information systems belonging to operators of essential services and digital service providers. Furthermore, for the purpose of facilitating cross-border cooperation and communication, each Member State is required to designate a national single point of contact responsible for coordinating issues relating to the security of network and information systems and cross-border cooperation at the Union level. The NIS Directive therefore provided the states with the flexibility to determine the number of CSIRTs, with the reservation that operators of essential services and digital service providers will have a designated CSIRT to which they will report. The Polish legislators have designated three national-level CSIRTs: the CSIRT MON, CSIRT NASK, and CSIRT GOV.

In the National Cybersecurity System Act the legislators established the CSIRT structure and the responsibilities of individual CSIRTs. The CSIRT MON, CSIRT NASK, and CSIRT GOV are obliged to cooperate with each other, with the authorities competent for cybersecurity matters, the Minister competent for computerisation, and the Plenipotentiary, ensuring a cohesive and complete system at the national level, performing tasks for counteracting cybersecurity threats of a cross-sectoral and cross-border nature, as well as ensuring the coordination of handling reported incidents. The entities have been obligated to jointly develop a procedure for dealing with incidents, the coordination of which requires CSIRT cooperation. Chapter 6 of the National Cybersecurity System Act implements Articles 9 and 10 of the NIS Directive.

Pursuant to Article 9 of the NIS Directive, each Member State shall designate one or more CSIRTs, which shall comply with the requirements set out in point (1) of Annex I covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. CSIRTs may be established within a competent authority. The Polish legislators adopted the second option, indicating three parallel CSIRTs. CSIRTs, also known as CERTs, are computer emergency response teams which comply with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks, and to ensure efficient cooperation at the Union level. The CSIRTs are expected to contribute to developing trust and confidence between the Member States, and to promote prompt and effective operational cooperation. The CSIRTs should be able to instruct the single point of contact to forward incident reports to the single points of contact in other Member States affected by the incident.

The states are required to ensure that the competent authorities and the single points of contact are adequately equipped in terms of both technical and organisational capabilities. It is intended to ensure the effective and efficient prevention, detection, response, and mitigation of network and information system incidents and risks.

In Poland, a model based on three CSIRTs has been adopted: CSIRT GOV—a Computer Security Incident Response Team operating at the national level, managed by the Head of the Internal Security Agency, CSIRT MON—a Computer Security Incident Response Team operating at the national level, managed by the Minister of National Defence, and CSIRT NASK—a Computer Security Incident Response Team operating at the national level, managed by the Research and Academic Computer Network—the National Research Institute. These designated CSIRTs cover all the sectors referred to in Annex II of the NIS Directive.

The three parallel CSIRTs represent the technical level of coordination of incident handling, and demonstrate that the Polish legislators have adopted a de-centralised system for the functioning of the CSIRTs. For the purpose of avoiding conflicts of competence, the legislators have defined the briefs of computer incident response teams. The tasks of CSIRTs take into consideration the responsibilities assigned to each CSIRT for the management of the state's cybersecurity, and include directories of the entities supported forming the national cybersecurity system. The competence scope is of a subjective and objective nature.

Among the tasks of the CSIRT MON is the coordination of handling incidents reported by the entities subordinate to or supervised by the Minister of National Defence, including those whose information and communication systems or networks are covered by the uniform list of facilities, installations, devices, and services constituting the critical infrastructure, as drawn up by the Director of the Government Centre for Security, pursuant to the Act on Crisis Management. The tasks of the CSIRT MON also involve coordinating the handling of incidents reported by enterprises of particular economic and defence significance, in relation to which the Minister of National Defence is the authority organising and supervising the performance of tasks for national defence, as well as in the field of incidents related to events of a terrorist nature which undermine the security of the defence potential of the state, the Polish Armed Forces, and the organisational units of the Ministry of National Defence.

The CSIRT GOV operates within the structures of the Internal Security Agency. The CSIRT GOV's tasks encompass the coordination of incident handling in the sphere of government administration and critical infrastructure.

The CSIRT NASK operates within the Research and Academic Computer Network—the National Research Institute, supervised by the Minister competent for computerisation. NASK operates in accordance with the Act of 30 April 2010 on Research Institutes.[1] The tasks of CSIRT NASK are a continuation of CERT Polska, which was established in 1996 as the first incident response team in Poland.

The first set of tasks of CSIRTs is to cooperate with each other, with the authorities competent for cybersecurity, the Minister competent for computerisation, and the Plenipotentiary, ensuring a cohesive and complete risk-management system at the national level.

[1] Act of 30 April 2010 on Research Institutes, consolidated text, Polish Journal of Laws of 2020, item 1383, as amended.

The second group of responsibilities is to implement measures to counteract threats to cybersecurity. The CSIRTs operate to counter cybersecurity threats of a cross-sectoral and cross-border nature. Cybersecurity hazards of a cross-sectoral nature are those which go beyond a single sector listed in the Act. For the prevention of threats of a cross-border nature, CSIRTs shall cooperate within the framework of the CSIRT network, consisting of representatives of CSIRTs of the European Union Member States. Under this cooperation, the Single Point of Contact provides information on cross-border incidents.

The Single Point of Contact is required to submit summary reports to the Cooperation Group, which should be anonymised in order to preserve the confidentiality of the notifications and the identity of the operators of essential services and digital service providers. It is indicated that information on the identity of the notifying entities is not required for the exchange of best practices within the Cooperation Group. The summary report should therefore include information on the number of notifications received, as well as information on the nature of the reported incidents, such as the types of security breaches, their seriousness, and their duration. The Single Points of Contact should not receive any incident notifications directly, unless they also function as a competent authority or a CSIRT.

CSIRTs are obligated to receive, analyse and coordinate incident notifications. The CSIRT MON, CSIRT GOV, and CSIRT NASK obtain incident reports from operators of essential services, digital service providers, and public entities, according to their competence. Pursuant to Article 26(2) of the NCSA, CSIRTs, in justified cases, are also obligated to provide incident-handling support at the request of operators of essential services, digital service providers, public entities, sectoral cybersecurity teams or owners, owner-like possessors, or holders bound by obligations towards owners, of facilities, installations, and equipment or services forming part of the critical infrastructure. Therefore, the principle should be that the incident must be handled by persons connected with the affected entity, or working for it. The reliable handling of incidents requires knowledge of the specific system under attack, and its functionality and design, which their administrators have. The operators of essential services should not expect the appropriate CSIRT team to provide support in every case. The granting of support might depend on the scale of the threat, the degree of impact, and other relevant factors. It should be emphasised that the CSIRT support or its handling of serious incidents which have affected operators of essential services and other entities can occur under two conditions: in justified cases, and at the request of these entities.

The coordination of incidents is the primary task of the CSIRT teams. This is essential for the proper performance of tasks, in particular when the incident is of a cross-sectoral nature. Under this cooperation, the CSIRT teams exchange information concerning threats. In Article 26(3) of the NCSA, the legislators defined the responsibilities shared by all three national-level CSIRTs. The monitoring of cybersecurity threats and incidents at the national level is listed as the first task. Incident management involves responding to a reported incident. Incident handling involves verification and classification, collection of information, documentation, coordination, and, if incident management requires CSIRT cooperation, reporting or

communication with the media. As part of incident management, the CSIRT classifies incidents, including those which are serious and significant, as critical incidents, and coordinates the handling of critical situations, as well as reclassifies serious and significant ones. Serious and significant incidents involving two or more countries shall be forwarded to the Single Point of Contact for further transmission to the relevant Member States.

The common responsibilities of CSIRTs include the assessment of the risks associated with identified cybersecurity threats and incidents, including dynamic risk analysis. The analysis of the incident is one of the crucial steps in dealing with the occurrence. Its proper implementation can and should serve to draw conclusions and tighten the security of systems. The proceedings during this stage should include securing evidence and preparing documentation on the event, on the basis of which further actual analysis of the incident will be performed.

CSIRTs have been obligated to report incidents and risks to the national cybersecurity system, and to issue communications about identified cybersecurity threats.

For cross-sectoral incidents, the legislators have ordered that technical information concerning the incident, the coordination of which requires CSIRT cooperation, must be transmitted to the appropriate CSIRT.

Where appropriate, CSIRTs have been required to conduct examinations of IT devices or software in order to identify the vulnerabilities whose exploitation can threaten, in particular, the integrity, confidentiality, accountability, authenticity, or availability of the data processed, and which can affect public security or the essential interests of national security; they must also submit proposals or recommendations to the entities of the national cybersecurity system in respect of the use of IT equipment or software, in particular with regard to the impact on public security or essential interests of national security. The concept of accountability is understood as ensuring that the actions of an entity can be unambiguously attributed only to that entity. Data integrity means confirmation that the data transmitted, received, or stored is complete and unaltered. Data confidentiality relates to the protection of communications or stored data against interception and reading by unauthorised persons. Furthermore, it should be noted that the legal regulations strictly define the basic safety conditions to be met by IT devices and software.

The Polish legislators have obligated CSIRTs to provide, by 30 May each year, to the Single Point of Contact, a list of serious incidents notified in the previous calendar year by operators of essential services which have affected the continuity of their essential services in the Republic of Poland and the continuity of their provision of essential services in the Member States of the European Union, as well as a summary of significant incidents notified by digital service providers in the previous calendar year, including those involving two or more Member States of the European Union. Moreover, the CSIRT teams must collectively prepare and submit to the Minister competent for digital affairs the part of the report on national security threats referred to in the Act on Crisis Management concerning cybersecurity.

National-level CSIRTs provide analytical and R&D facilities for the national cybersecurity system. This involves conducting advanced malware and vulnerability analyses, monitoring cyber threat indicators, developing tools and methods for

detecting and combating cyber threats, conducting analyses and developing standards, recommendations, and good practices in the field of cybersecurity, supporting entities of the national cybersecurity system in building cybersecurity capacities and capabilities, and conducting awareness-building activities in the sphere of cybersecurity.

The CSIRT tasks defined in the NCSA are compliant with the requirements for Computer Security Incident Response Teams as defined in Annex I to the NIS Directive. The EU legislature has included among these tasks monitoring incidents at the national level, providing early warnings to the relevant stakeholders, issuing alerts, publishing announcements and disseminating information to the stakeholders regarding risks and incidents, responding to incidents, providing dynamic risk and incident analysis and situational awareness, participating in the CSIRT network, and establishing cooperation with the private sector.

The Polish legislators, in Article 26(8) of the NCSA, also regulated the rules for forwarding incident notifications by the inappropriate CSIRT according to competence. The CSIRT MON, CSIRT NASK, or CSIRT GOV which has received an incident notification, but is not responsible for coordinating its handling, shall immediately forward this notification to the competent CSIRT, along with the information received. These entities may also entrust each other with the performance of tasks in respect of certain types of entity on the basis of an agreement. Should such an agreement be made, the CSIRT shall inform the entity in respect of which there has been a change of subsidiarity. Additionally, the announcement of the conclusion of the agreement shall be published in the Official Journal of the Minister of National Defence, the Minister for Digital Affairs, or the Internal Security Agency, respectively, indicating the address of the website on which the content of the agreement is published, and the date from which the agreement is binding. Whenever it is determined that the incident, the handling of which is coordinated by the responsible CSIRT MON, CSIRT NASK, or CSIRT GOV, is related to an event of a terrorist nature or to a terrorist act detrimental to the security of the state's defence capabilities, the Polish Armed Forces and the organisational units of the Ministry of National Defence, the coordination of incident handling is assumed by the responsible CSIRT MON or CSIRT GOV.

It is important to note that information regarding incidents is becoming increasingly valuable to the general public and businesses. Therefore, it is important that such information should not only be focused on incidents and events with a national range, but must also be provided in an aggregated form at the Union level. This is due to the fact that small and medium-sized enterprises in particular are increasingly operating across borders and the citizens are using online services. The EU legislators encourage CSIRTs to provide, on a voluntary basis, information to be published on websites, without including confidential or sensitive information. When information is considered confidential according to national laws, it must be kept confidential. At the same time, the authorities are obligated to devote due attention to safeguarding informal and trusted channels of information-sharing. Decisions concerning the provision of information to the public about incidents should be taken with a reasonable balance between the public interest, according to which the

public should be informed of the threats, and the risk of the reputational and commercial damage to which the operators of essential services and digital service providers reporting incidents are exposed. While fulfilling their incident-notification obligations, the competent authorities and the CSIRTs should pay particular attention to the need to maintain strict confidentiality with regard to information relating to product vulnerabilities until the appropriate security fixes are released.

In identifying the right CSIRT, priority shall be given to examining whether an entity belongs to the category of entities for which the CSIRT MON is appropriate. The NCSA identifies two entity categories. First, entities subordinate to or supervised by the Minister of National Defence, including those whose communication and information systems or networks are covered by the uniform list of facilities, installations, devices, and services included in the critical infrastructure, referred to in Article 5b(7)(1) of the Act of 26 April 2007 on Crisis Management; Second, the enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence within the meaning of Article 5(3) of the Act of 23 August 2001 on the Organisation of Tasks for State Defence Performed by Enterprises.[2] If a given entity is part of one of these two groups, it is obligated to report to, or liaise with, the CSIRT MON response team. The CSIRT MON is exclusively responsible for implementing the tasks laid down in the NCSA in relation to the entities listed below. The scope of the entities subordinate to or supervised by the Minister of National Defence was defined in the Notice of the Minister of National Defence of 16 January 2019.[3] Furthermore, it should be indicated that the CSIRT MON's jurisdiction *ratione personae* extends to critical-infrastructure entities which are also subsidiary to the Minister of National Defence. Essentially, the CSIRT GOV will be the responsible entity for critical infrastructure. The legislators have thus decided that, as far as critical infrastructure is concerned, entities under the authority of the Minister of National Defence, and supervised by him or her, would be covered by the CSIRT MON's responsibility. The second group of entities within the responsibility of the CSIRT MON includes enterprises of particular economic and defence importance, in respect of which the Minister of National Defence is the authority organising and supervising the performance of tasks for state defence.

Within the scope of the CSIRT NASK's responsibilities, the legislators have adopted both a subjective and an objective scope. In addition to the category of entities which are within the responsibility of the CSIRT NASK, two functions have been identified, which remain within the exclusive ambit of the CSIRT NASK. In the subjective aspect, the tasks of the CSIRT NASK include the coordination of handling incidents reported by units subsidiary to or supervised by

[2]Act of 23 August 2001 on the Organisation of Tasks for State Defence Performed by Enterprises, consolidated text, Polish Journal of Laws of 2020, item 1669.

[3]Notice of the Minister of National Defence of 16 January 2019, The Official Gazette of the Government of the Republic of Poland of 2019, item 48.

government-administration authorities, except for units subsidiary to or supervised by the Prime Minister, research institutes, the Office of Technical Inspection, the Polish Air Navigation Services Agency, the Polish Centre for Accreditation, the National Fund for Environmental Protection and Water Management, and provincial funds for environmental protection and water management, commercial law companies performing public service tasks intended to meet, on an ongoing and continuous basis, the collective needs of the population through the provision of open services, natural persons, digital service providers, in so far as they are not critical infrastructure operators, the operators of essential services, with the exception of those operators which are assigned to the CSIRT MON and the CSIRT GOV, and other entities which are outside the responsibility of the CSIRT MON and the CSIRT GOV. Therefore, incidents may be reported to the CSIRT NASK by all entities not classified in any of the above-mentioned categories of entity. This means that anyone can report incidents to the CSIRT NASK.

Among the additionally indicated exclusive tasks of the CSIRT NASK are the creation and provision of tools for voluntary cooperation, and the exchange of information on cybersecurity threats and incidents. The EU legislators encourage the creation by other organisations of their own informal cooperation mechanisms to ensure the security of network and information systems, recognising the need for cooperation between the public and the private sectors. The Cooperation Group should invite relevant stakeholders for discussion. In order to effectively encourage the sharing of information and best practices, it is necessary to ensure that operators of essential services and digital service providers participating in such exchanges do not bear the consequences arising from the mere fact of cooperating. Moreover, it should be stressed that the CSIRT NASK's activities are financed in the form of an earmarked subsidy from the part of the state budget at the disposal of the Minister competent for computerisation.

The second function of the CSIRT NASK is to provide a telephone or Internet service for those who are active in reporting and analysing the distribution, dissemination, or transmission of child pornography through information and communication technologies. This task is performed on the basis of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.[4]

The categories of content covered by the CSIRT NASK response procedure include child sexual abuse material, hard pornography, racism, and xenophobia, but also other illegal content which does not relate to either of these categories. All materials (photos and videos) displaying the sexual abuses of children are transferred to the ICCAM database to identify the victims and perpetrators. ICCAM is an integrated database for the exchange of information on CSAM (child sexual abuse materials). The legislators, in the discussed provision, explicitly indicated that the

[4]Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ EU 2011 L 335/1.

task of the CSIRT NASK was to undertake activities in the field of the analysis of cases of the distribution, dissemination, or transmission of child pornography by means of information and communication technologies. In order to fulfil this obligation, employees are allowed to be in possession of pornographic content. It should be stressed that the CSIRT NASK's activities will be within the limits of its statutory entitlements and obligations, and will not constitute a breach of Article 202 § 4a and 4b of the Penal Code. If the material featuring the sexual abuse of a child is on a server located in Poland, the information is forwarded to the National Police Headquarters. If the child sexual abuse material is located in a country covered by the operations of INHOPE Association, the information is forwarded to the response team of the country where the server is located, as well as to Interpol. If the child sexual abuse material is out of the reach of INHOPE, the information is forwarded to the National Police Headquarters and to Interpol.

This task is implemented by the CSIRT NASK through Dyżurnet.pl, a team of CSIRT NASK experts. This team belongs to the International Association of Internet Hotlines (INHOPE). More than 50 response teams from all over the world are members of the Association. The operations of all response teams and the law-enforcement agencies cooperating with them aim to identify the perpetrator and victim of sexual abuse as quickly as possible. The notification by the user and immediate action by the administrator facilitates a significant reduction in the dissemination of the material and a reduction in secondary victimisation.

The Polish legislators have defined the categories of entities and specific, named, entities for which the CSIRT GOV is competent. The tasks of the CSIRT GOV include the coordination of handling incidents reported by selected public finance sector entities: public authorities, including government-administration bodies, state control and law protection institutions and courts and tribunals, the Social Insurance Institution and funds managed by it, the Agricultural Social Insurance Fund and funds managed by the President of the Agricultural Social Insurance Fund, and the National Health Fund. Additionally, the CSIRT GOV is responsible for entities subordinate to or supervised by the Prime Minister, the National Bank of Poland, Bank Gospodarstwa Krajowego, and other entities whose communication and information systems or networks are covered by the uniform list of facilities, systems, equipment, and services included in the critical infrastructure prepared by the Director of the Government Centre for Security pursuant to the Act on Crisis Management, with the exception of entities whose incident handling is performed by the CSIRT MON.

The CSIRT GOV has jurisdiction over all critical infrastructures. The legislators have indicated that the entities whose incident handling is coordinated by the CSIRT NASK, if the incident involves information and communication systems or networks covered by the uniform list of facilities, systems, equipment, or services which are part of the critical infrastructure, prepared by the Director of the Government Centre for Security under the Crisis Management Act, fall within the competence of the CSIRT GOV. When determining the scope of the CSIRT GOV's competence in relation to critical infrastructure entities, it should be stressed that the principle is the

CSIRT GOV's competence, excluding entities subject to or supervised by the Minister of National Defence.

The legislators have obligated CSIRT teams to respect the range of their competence. In the event that the CSIRT MON, CSIRT NASK, or CSIRT GOV receives an incident notification from an entity for which it does not have an assigned coordination capability, it shall immediately forward that notification to the appropriate CSIRT, along with any information received. The notifier should also be informed of the transmission of the notification by virtue of the obligations incumbent on them. The National Cybersecurity System Act also provides for the possibility of the CSIRTs' entering into agreements under which the general responsibility of an individual CSIRT can be modified. These entities may also entrust each other with the performance of tasks in relation to certain entity types by agreement. When such an agreement is made, the CSIRT shall inform the entity in respect of which there has been a change of subordination. The notification should contain, in particular, the parties to the agreement, a list of entities in relation to which the CSIRT has been changed, and the effective date of the agreement, the obligation for the CSIRT to inform the entities concerned that the agreement has been made, and the address of the website on which the text of the agreement will be published.

Pursuant to Article 27 of the National Cybersecurity System Act, the CSIRT GOV and CSIRT MON are exclusive in relation to incidents linked to terrorist acts. The statement of reasons to the Act indicates that the purpose of introducing the provision was to maintain the consistency of the provisions of the NCSA with the provisions of the Act on Anti-Terrorism. Incidents associated with a terrorist act have been treated in a unique way, due to the seriousness of the threat. **The primary objective of the regulation is to increase the effectiveness of the Polish cybersecurity system, and thus to increase the security of all Polish citizens, by strengthening the mechanisms for coordinating actions, clarifying the tasks and responsibilities of the various CSIRTs and the rules of cooperation between them, and ensuring that effective action can be taken in the event of an incident related to a terrorist act.**

Whether a specific incident is related to terrorist activities might be difficult to identify during the notification phase. Here it is important to analyse in detail the causes of the incident and to exchange information between the CSIRT teams. In fact, only the CSIRT to which the incident has been reported may conduct an analysis of the incident, and it is the one which remains responsible for the correct classification. The CSIRT GOV is competent for incidents related to terrorist activities. The event of a terrorist nature is a situation which is suspected to have arisen as a result of an offence as specified in Article 115(20) of the Act of 6 June 1997—the Penal Code.[5] Pursuant to Article 115(20) of the Penal Code, a terrorist offence is a prohibited act with the aim of seriously intimidating a large number of people, to compel a public authority of the Republic of Poland or another state or an

[5] Act of 6 June 1997—the Penal Code, consolidated text, Polish Journal of Laws of 2020, item 1444, as amended.

authority of an international organisation to undertake or refrain from undertaking any specific act, or to cause any serious disruption to the system or the economy of the Republic of Poland or another state or international organisation, or threaten to commit any such act.[6] It is punishable by a maximum term of imprisonment of at least five years.

The CSIRT MON is competent for incidents related to events of a terrorist nature which compromise the security of the state's defence capabilities, the Armed Forces of the Republic of Poland, and organisational units of the Ministry of National Defence. Whenever an incident, the handling of which is coordinated by the responsible CSIRT MON, CSIRT NASK, or CSIRT GOV, is related to events of a terrorist nature, the coordination of incident handling will be assumed by the responsible CSIRT MON or CSIRT GOV, depending on the nature of the incident.

The Polish legislators have imposed an obligation on CSIRT MON, CSIRT NASK, and CSIRT GOV teams to inform other European Union Member States of incidents which affect them. This obligation relates to serious incidents reported by the operators of essential services. The information is transmitted through the Single Point of Contact, which is used for communication within the European Union. The exchange of information between EU Member States contributes to the objectives of the NIS Directive to achieve a high common level of security of network and information systems in the EU. The Single Point of Contact shall forward, at the request of the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV, notifications of a serious incident or an incident involving two or more Member States of the European Union to Single Points of Contact in other Member States of the European Union. It is also obligated to receive notifications of a serious incident involving two or more Member States of the European Union from the Single Points of Contact in other Member States of the European Union, followed by the transmission of these notifications to the CSIRT MON, CSIRT NASK, CSIRT GOV, or sectoral cybersecurity teams. A serious incident, reported by an operator of essential services, will be one associated with a serious deterioration or disruption to the provision of an essential service.

The appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV may request from the Single Point of Contact that a report of a serious incident be forwarded to the Single Points of Contact in the other Member States of the European Union affected by such an incident. This obligation relates to serious incidents. The information is transmitted through the Minister for Digital Affairs, who performs the tasks of the Single Point of Contact.

Article 29 of the NCSA establishes the obligation for the responsible CSIRT to inform other EU Member States of incidents involving two or more Member States. This obligation has been imposed on all CSIRTs. Article 29 reflects the provisions laid down in Article 16(6) of the NIS Directive. In accordance with this Article, when a significant incident involves two or more Member States, the appropriate authority or CSIRT shall inform the other affected Member States. In so doing, the

[6] Węglowski (2018).

competent authorities, CSIRT, and Single Points of Contact shall protect the security and commercial interests of the digital service provider, as well as the confidentiality of the information transmitted. This obligation concerns significant incidents. A significant incident is an incident which has a substantial impact on the provision of a digital service. These are incidents which are reported by digital service providers. Digital service providers shall, without undue delay, report to the appropriate CSIRT any incident having a significant impact on the provision of a service afforded by those providers in the Union. These notifications must contain information enabling the appropriate CSIRT to determine the significance of the cross-border impact. The notification must not expose the notifying party to increased liability.

Digital service providers should ensure a level of security commensurate with the level of risk to which the security of their digital services is exposed, considering the importance of those services for the activities of other businesses in the Union. This article is applicable to digital service providers. The EU legislators have noted that the degree of risk to the operators of essential services—which are often crucial for maintaining critical societal and economic activities—is higher than for digital service providers. The security requirements for digital service providers should therefore be reduced. Digital service providers should be permitted to adopt measures they consider appropriate to manage the risks to which the security of their network and information systems might be exposed. The CSIRT MON, CSIRT NASK, or CSIRT GOV shall inform the other Member States of the European Union about the incident via the Single Point of Contact.

The NCSA also defines the rules for incident notification to the CSIRT NASK by entities other than operators of essential services and digital service providers, including individuals. For the purpose of receiving voluntary incident notifications, the CSIRT NASK is the responsible entity. Entities not identified as operators of essential services and which are not digital service providers may, on a voluntary basis, report incidents which have a significant impact on the continuity of the services they provide. A voluntary notification may not result in the imposition of any obligations on the notifying party to which they would not be subject if they had not done this notification. The entity which voluntarily reports an incident to the CSIRT NASK is required to provide its name, or details of the information system in which the incident occurred. Secondly, it should describe the incident, which must be an event which has an adverse effect on cybersecurity. The notification is made by filling in the form available on incydent.cert.pl, and specifying the category. These categories are grouped into (1) suspicious e-mails (suspicious attachments, phishing, blackmail), (2) attempts at fraud (fake online shops and other attempts at impersonation), (3) malware (virus samples or ransomware-encrypted files), (4) vulnerabilities (errors in software or web applications), (5) illegal content (notifications intended for the Dyżurnet.pl team), (6) and other (all incidents not matching the previous categories).

The notification shall contain all the appropriate information on the incident. This information should be useful for the CSIRT. As an example, the source from which the applicant learned about the site, and the bank account number for transferring

money may be mentioned. Information which is legally protected, including trade secrets, should be clearly identified in the notification. The legislators, in Article 30 (2) of the NCSA, stipulated that the CSIRT NASK should deal with incident reports from operators of essential services and digital service providers, i.e. mandatory notifications as a priority over voluntary notifications. Voluntary notifications are examined only if such an examination does not impose a disproportionate or excessive burden on the Member States involved. In this context, it should be recognised that anyone who is concerned about a specific cybersecurity incident may report the incident to the CSIRT NASK.

The Polish legislators have granted individual CSIRTs the responsibility to determine how notifications should be submitted. It should be noted that the CSIRT MON, CSIRT NASK, and CSIRT GOV have been responding to incidents for several years, maintaining cybersecurity. The legislators have recognised that the solutions developed by individual CSIRTs in the field of incident notification and communication with their entities, taking into consideration the specificity of each entity's operations, may still be implemented. Pursuant to Article 31, it is possible to determine the manner in which notifications are to be made and information provided in electronic form.

The independence of a CSIRT in respect of the entities for which it is responsible concerns

(1) serious incidents which must be reported by the operators of essential services
(2) significant incidents which must be reported by digital service providers
(3) incidents in a public entity, to be reported by the public entities
(4) information from the operators of essential services, digital service providers, and public entities on other serious incidents, cyber threats, risk estimation, vulnerabilities and technologies used
(5) other than the above-mentioned incidents, which may be reported by entities not covered by the obligation to notify of incidents, on a voluntary basis.

The legislators reserve within the ambit of the CSIRT MON, CSIRT NASK, and CSIRT GOV the technical issues of notifications. These notifications may be submitted by electronic means as well as by other communication media where it is not possible to submit the notification or to transmit it by electronic means. The manner of notification and communication should be specified in the communication. The notice is published on the website of the Public Information Bulletin of the Minister of National Defence, Research and Academic Computer Network—the National Research Institute, or the Internal Security Agency, respectively.

Electronic incident notification for the CSIRT MON is made by filling in the Incident Notification Form. As regards the CSIRT NASK, the electronic incident notification takes place using the form available on the incydent.cert.pl website. The form is completed under one of these categories: (1) suspicious e-mails, (suspicious attachments, phishing, blackmail), (2) attempts at fraud (fake online shops and other attempts at impersonation), (3) malware (virus samples or ransomware-encrypted files), (4) vulnerabilities (errors in software or web applications), (5) illegal content (notifications intended for the Dyżurnet.pl team), (6) other (all incidents not falling

into the previous categories). The electronic reporting of an incident in the case of the CSIRT GOV is made via the form available on csirt.gov.pl.

The Polish legislators have introduced the principle that the CSIRT MON, CSIRT NASK, or CSIRT GOV may conduct an inspection of an IT device or software to identify vulnerabilities, the use of which might, in particular, jeopardise the integrity, confidentiality, accountability, authenticity, or availability of the data processed, and which may affect public security or vital national security interests. The subject of the inspection may be an IT device or software. The purpose of the investigation is to identify vulnerabilities which, in particular, can jeopardise the integrity, confidentiality, accountability, authenticity, or availability of the data processed, where such vulnerability might affect public security or a substantial national security interest.

Data integrity is the confirmation that the data sent, received, or stored are complete and in an unaltered state, and that the resources of the information system have not been unlawfully modified. Data confidentiality is a property which ensures that information is not disclosed to unauthorised persons. It means protecting communications or stored data against interception and reading by unauthorised persons. Accountability means the property of a system which allows specific activities to be assigned to a person or process and placed in time. Authenticity refers to the feature that the data content or origin is as declared. The last feature, the availability of the processed data, is the property determining that the data may be used on request, within the assumed period of time, by an entity authorised to work in a communication and information system.

The legislators have established in Article 33(2) of the NCSA an obligation to declare the fact of undertaking an inspection of an IT device or software. If one of the CSIRTs initiates an inspection of an IT device or software, it shall inform the other CSIRTs. The information should indicate which specific IT device or software is being tested. This solution is designed to prevent the duplication of activities by the individual CSIRT teams. The CSIRT MON, CSIRT NASK, or CSIRT GOV informs the other CSIRTs of the results.

Following the testing of an IT device or software, the CSIRT should prepare a report which includes its findings and conclusions. Where it is established that there is a vulnerability whose use can have an impact on public security or a substantial national security interest, the CSIRT shall request a recommendation for the use of a given IT device or software. The request is addressed to the Plenipotentiary for Cybersecurity.

Recommendations shall be issued by the Plenipotentiary after obtaining the approval of the College for Cybersecurity. The Plenipotentiary is also entitled to change and cancel the recommendation concerning the use of IT devices or software. Both the amendment and the withdrawal of the recommendation require the approval of the College. Recommendations are not administrative decisions. The statement of reasons to the Act indicates that recommendations are a positive measure, which means that they may recommend the software in question or consider it undesirable. Recommendations should also be a voluntary measure, which means that they cannot bind private entities. It is designed to raise user awareness, supporting the safe use of hardware and software. Recommendations are of an abstract nature,

which means that the Plenipotentiary should inform all entities of the national cybersecurity system which might be affected by the vulnerability when the recommendation is issued.

An entity of the national cybersecurity system may raise objections to the Plenipotentiary's recommendations concerning the use of IT devices or software, on the grounds of their negative impact on the service provided, or the public task being performed, no later than within 7 days of the receipt of the recommendation. The Plenipotentiary should address the concerns received from the national cybersecurity system operator without delay, but no later than 14 days after receipt. As a result of examining the objections, the Plenipotentiary may uphold the recommendations concerning the use of IT equipment or software, or issue amended recommendations. If the objections are deemed justified, the amended content of the recommendation shall be subject to the approval of the College. If the recommendations concerning the use of IT equipment or software are not taken into consideration, the Plenipotentiary is entitled to apply to the authority supervising the entity to which the recommendation relates for them to be disregarded. The supervisory authority, within the scope of its responsibilities, may take supervisory measures.

The NCSA has established the principle of cooperation between the CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams and service providers, with law enforcement authorities, as well as with the justice and intelligence services, in the performance of their statutory tasks. The legislators have thus highlighted that the CSIRT teams play an extremely significant role in counteracting cybercrime. This might arise from the fact that these entities have knowledge and experience in incident analysis. The CSIRT MON, CSIRT NASK, and CSIRT GOV, while coordinating incident handling, are obligated to determine whether an incident involves personal data. If the incident is found to have resulted in a personal data breach, the CSIRT is required to cooperate with the authority responsible for personal data protection.

Operators of essential services, digital service providers, and public entities, in the case of an incident resulting in a personal data breach, in addition to the obligation to notify the appropriate CSIRT of the incident, pursuant to the GDPR regulation, are also obligated to report such a violation to the President of the Personal Data Protection Office.

According to Article 31 of the GDPR, the controller and processor shall cooperate with the supervisory authority in the performance of their tasks. In the case of a personal data breach, the controller shall, without undue delay, where possible not later than 72 h after having established the breach, report it to the supervisory authority, unless the breach is unlikely to result in a risk of jeopardising the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 h, it shall be accompanied by reasons for the delay (Article 33 (1) of GDPR).

Under Article 35 of the NCSA, the legislators provided for a specific category of incidents, i.e. critical incidents. These are incidents with the most significant importance, resulting in considerable damage to public safety or order, international

interests, economic interests, the operation of public institutions, civil rights and freedoms, or the lives and health of people. Each time an incident is classified as critical by the CSIRT team, and the identification of such an incident by each CSIRT is related to the requirement to inform the other CSIRTs about the incident and to notify the Government Centre for Security. The information should include a preliminary analysis of the potential effects of the incident. This analysis should identify the number of users affected by the incident (especially if it disrupts the provision of an essential service), the moment when the incident occurred and was detected, and its duration, as well as the geographical coverage of the affected area. The information should include a description of the incident, specifying its nature, course, and technical characteristics.

The information may include a recommendation to establish a Government Crisis Management Team. It is a consultative and advisory authority responsible for initiating and coordinating crisis management activities, operating within the structures of the Council of Ministers. The team is composed of the Prime Minister, as the Chairperson, the Minister of National Defence and the Minister competent for public administration, the Minister of Foreign Affairs and the Minister Coordinator of Special Services. The tasks of the Government Crisis Management Team include preparing proposals for the use of the forces and resources necessary to manage a crisis situation, and advising on the coordination of actions by government administration authorities, state institutions and services in crisis situations, as well as providing opinions on the final reports on actions taken regarding crisis management.

The Act also provides for the possibility of including in the information a request to convene a Critical Incidents Team. Apparently, a critical incident event may be qualified as a crisis situation as referred to in the Act on Crisis Management. A crisis situation is defined as any situation which adversely affects the level of security of individuals, property of substantial size, or the environment, causing significant constraints on the operation of the responsible public authorities due to the inadequacy of the forces and the resources available. Immediate cooperation, together with the exchange of information and the coordination of actions, are essential elements in the event of a critical incident. The CSIRT which has classified an incident as critical transfers information to the other CSIRT teams. All CSIRT teams are authorised to inform each other in the event of intelligence on cybersecurity threats. These are potential sources of incidents. Moreover, this appears to refer to cybersecurity threats that might contribute to a critical incident. Therefore, it would be inappropriate to communicate all the threats identified by individual CSIRTs. The CSIRT may also inform the Government Centre for Security on these threats. The Government Centre for Security is the state entity established under Article 10 of the Act on Crisis Management. It reports to the Prime Minister. One of the tasks of the Government Centre for Security is to support the Critical Incidents Team.

All CSIRTs have also been authorised to publish on the website of the Public Information Bulletin of, respectively, the Minister of National Defence—the CSIRT MON, the Research and Academic Computer Network—the National Research

Institute—the CSIRT NASK, or the Internal Security Agency—the CSIRT GOV, information, to the extent necessary, on vulnerabilities, critical incidents, and threats to cybersecurity, provided that the provision of the information contributes to increasing the cybersecurity of the information systems used by citizens and businesses, or to ensuring the safe use of those systems. The information disclosed may not violate the regulations on the protection of classified information and other legally protected secrets, or the regulations on personal data protection. The publication of information on vulnerabilities, critical incidents, and threats to cybersecurity should contribute to increasing the security of systems and public awareness of the hazards. Such publication may be accompanied by information relating to risk prevention and advice.

The adoption by the Polish legislators of several entities responsible for performing duties related to the security of networks and IT systems owned by operators of essential services and digital service providers—three national level CSIRTs: the CSIRT MON, CSIRT NASK, and CSIRT GOV—resulted in the obligation to establish a team which would coordinate the activities undertaken by the CSIRT MON, CSIRT NASK, CSIRT GOV, and the Government Centre for Security. In the article discussed, the legislators appointed the Critical Incidents Team, which coordinates the activities of the three CSIRTs, and exchanges information in the event of a critical incident.

It is composed of representatives of the CSIRT MON, the CSIRT NASK, the Head of the Internal Security Agency implementing the tasks of the CSIRT GOV, and the Government Centre for Security. The Team's work is managed by the Director of the Government Centre for Security. The Centre also supports the operations of the Team. According to the statement of reasons for the Act, this is an auxiliary body which should provide organisational and technical assistance for critical incidents. This Team is therefore not a decision-making unit. The work of the Team is convened by the Director of the Government Centre for Security. The Director is obligated to convene the Team on his or her own initiative after being notified of the occurrence of a critical incident, at the request of a Team member, and if the request to call the Team results from CSIRT information on the occurrence of the said incident. The Director of the Government Centre for Security shall immediately notify the members of the Team of the date and venue of the Team's meeting. Participation in the meeting of the Group may take place by electronic means of communication. Electronic-communication means shall be understood not only as technical solutions, but also as information and communication devices and associated software tools enabling individual communication at a distance using data transmission between communication and information systems, in particular e-mail.

The actions taken by the Team at meetings include unanimously designating the CSIRT coordinating critical incident handling, and defining the roles of the other CSIRTs and the Government Centre for Security in dealing with the incident. The designation of the leading entity enables all information to be gathered in one place. The Team also determines the manner in which technical information on the critical incident shall be exchanged between the CSIRT MON, CSIRT NASK, or CSIRT GOV. The Team's responsibility also includes adopting decisions requiring the

Director of the Government Centre for Security to submit a request to the Prime Minister to convene the Government Crisis Management Team. The decision to call the Government Crisis Management Team relates to situations in which such critical incidents might result in crisis situations within the meaning of the Act on Crisis Management. Where a critical incident might result in the threat of a terrorist act involving the information and communication systems of public authorities, or information and communication systems which form a critical infrastructure, the Team prepares information and conclusions on such an incident for the Minister competent for the Interior and the Head of the Internal Security Agency. According to the information provided, CRP alert levels (alerts related to threats in the cyber-space) may be announced.

CRP alert levels are introduced pursuant to Article 15(2) of the Act of 10 June 2016 on Anti-Terrorism. There are four CRP alert levels. Where there is a threat of a terrorist incident involving information and communication systems of public administrations, or information and communication systems which are part of the critical infrastructure, or where such an event occurs, one of the four CRP alert levels may be introduced.

(1) First CRP alert level (ALFA-CRP level);
(2) Second CRP alert level (BRAVO-CRP level);
(3) Third CRP alert level (CHARLIE-CRP level);
(4) Fourth CRP alert level (DELTA-CRP level).

The first alert level may be introduced when there is intelligence on the possibility of a terrorist event, the type and extent of which is difficult to predict. The second alert level may be introduced in the event of an increased and foreseeable threat of a terrorist act, although the specific target of the attack has not been identified. The third alert level may be introduced in the event of an occurrence of incidents confirming the probable target of a terrorist attack which is detrimental to the security or public order or safety of the Republic of Poland, or the security of another state or international organisation, and poses a potential threat to the Republic of Poland; or in the event of obtaining reliable and confirmed information about a planned terrorist event on the territory of the Republic of Poland; or in the event of obtaining reliable and confirmed evidence of a planned terrorist act, the consequences of which might affect Polish citizens residing abroad or Polish institutions or Polish infrastructure located outside the Republic of Poland. The fourth level may be introduced in the event of the occurrence of any event of a terrorist nature which causes a threat to public security or order, or to the security of the Republic of Poland, or to the security of another country or international organisation, and poses a threat to the Republic of Poland intelligence being obtained indicating an advanced stage of preparation for a terrorist event on the territory of the Republic of Poland, intelligence being obtained indicating an advanced stage of preparation for a terrorist event which is to be targeted at Polish citizens residing abroad, or at Polish institutions or Polish infrastructure located outside the borders of the Republic of Poland, whereas the information obtained indicates the inevitability of such an event.

The alert levels are introduced, modified, or cancelled by way of an Order—depending on the type of threat posed by the terrorist event—by the Prime Minister, following consultation with the Minister competent for internal affairs and the Head of the Internal Security Agency, and, in urgent cases, by the Minister competent for internal affairs after consulting the Head of the Internal Security Agency, informing the Prime Minister promptly.

Reference

Węglowski MG (2018) Działania antyterrorystyczne. Komentarz, Warsaw

Monika Nowikowska PhD, adjunct at the Department of Cybersecurity Law and New Technologies of the Institute of Law of the War Studies University. Author of several dozen scientific publications in the field of intellectual property law and the media. He also specializes in issues related to security, such as audit, protection of classified information and personal data. Internal auditor, legal advisor.