www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2020, VOL. 66, NO. 2, PP. 321-326
Manuscript received March 26, 2020; revised April, 2020. DOI: 10.24425/ijet.2020.131881

Towards Building National Cybersecurity Awareness

Marek Amanowicz

***Abstract*—The paper depicts a complex, distributed information system aimed at promoting cybersecurity awareness at the national level. The system, that is built in accordance with the Act on National Cybersecurity, passed by the Polish Parliament, enables collecting and processing in near-real time available information on the security status of essential services and digital services and, also, provides for assessment of negative impact of the identified threats concerned with the provision of those services. Advanced access control and dissemination mechanisms, for secure information sharing within the system, are provided in order to aggregate distributed knowledge and use this information for on-line security risk analysis and for generation and distribution of early warnings.**

***Keywords*—cybersecurity awareness, service interdependencies, on-line risk analysis, threats propagation**

I. Introduction

We currently observe an increasing number of more and more sophisticated, and growing in complexity, cyber-attacks. They pose serious threats to functioning the network and information systems, especially those being important from the point of view of reliable and secure business and social activities. They can lead to violation of continuous provision and/or to deterioration of the quality of essential and digital services. This, in consequence, may bring significant damage to state, in particular to state security, public and economic order, functioning of public institutions, civil rights and freedoms, and, finally, to human life and health.

The situation is complicated by strong interdependence of the services, presented for instance in [1-4], as well as by the shared use of ICT resources; both significantly extend the area of impact of existing threats and create new channels for attacks. This means that effective identification of threats in cyberspace, an assessment of their impact on the services rendered or tasks performed, and response to actual demand are not possible without the cooperation of teams responsible for IT security analysis and management [5]. Obtaining a reliable situational picture of the cyberspace and ensuring a high level of protection against threats at the national level requires development of the procedures enabling exchange of experience and effective cooperation of all entities being responsible for ICT security. It is also necessary to create technical solutions enabling effective acquisition, processing, and distribution of the verified information on the existing threats and their potential effects.

Recently, much research effort and case studies have been undertaken with an objective to develop methods and technical skills and solutions enabling the effective sharing of information on threats and their potential detrimental effects. For example, the CS-AWARE project (https://cs-aware.eu/), launched under the H2020 Program, focuses on creating solutions dedicated to local public administration bodies, non-governmental organizations, and small and medium-sized enterprises. The developed tools enable for automatic detection, classification, and visualization of computer incidents in near-real time, supporting the prevention or mitigation of the effects of such events. The solutions, created within this project, are based on mechanisms for information sharing, concerning actual threats and on using the advanced methods of big data analysis and processing.

A number of new solutions, focused on increasing awareness to cyber threats and improving the level of security of networks and information systems, are also available. For example, an interesting approach for building a common cybersecurity awareness of critical infrastructure is presented in [6]. By aggregating and analysing the data, obtained from security management systems and their correlation, a global cybersecurity picture is created that also allows – due to the links between critical infrastructure elements – for anticipating the risks of threat propagation. An interesting proposal of information system for collaborative cyber incident management for the European interconnected critical infrastructure is presented in [7].

The actions, taken in Poland, aimed at providing legal, organizational and technical foundations for obtaining a high level of protection against computer threats, also fall under this trend. They were and are being stimulated by the Directive of the European Parliament and the Council of the European Union [8] of the 6th July 2016 on the measures for a high level of security of network and information systems on the territory of the Union, colloquially referred as the NIS Directive. This Directive imposed, on the member states, an obligation to implement several regulations, related, for instance, to:

- development and adoption of the strategies for security of networks and information systems at the national level,
- establishing requirements and procedures for reporting cybersecurity incidents by essential service providers and main core operators of digital services,
- creating a network of national Computer Security Incident Response Teams (CSIRTs).

Several initiatives have been undertaken by EU and at a state level of EU states to implement the NIS Directive. In 2017, in particular, ETSI launched the document [9] that provides guidance on the available and being developed technical specifications designed to meet the legal measures and

This work was done as part of CYBERSECIDENT/369195/I/NCBR/2017 project, supported by the National Centre of Research and Development, in the frame of CyberSecIdent Programme

Author is with NASK-National Research Institute, Warsaw, Poland (e-mail: marek.amanowicz@nask.pl)

requirements regarding sharing the information on the network-based risks and incidents. An overview of the state-of-the-art of the implementation on NIS Directive within Europe is available at (https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive).

On the 5th July 2018, the Polish Parliament passed the Bill on the National Cybersecurity System (NCS), which specifies the frame of the organization of this system, the tasks and responsibilities of all entities involved in this system, the manner of exercising supervision and control on application of the Act, as well as determines the scope of the Cybersecurity Strategy of the Republic of Poland. The Act is also accompanied by several implementing provisions, which define specific requirements concerning sectors of economy and important individual institutions.

The regulations are aimed at creating both efficient and secure system that should increase the level of protection against computer threats in Poland and they enable effective cooperation with the EU Member States. The system includes essential service operators, digital service providers, and the public entities (i.e. institutions that perform public tasks or dispose of public property). It is to be managed at the operational level by three Computer Security Incident Response Teams (CSIRT GOV, CSIRT MON, CSIRT NASK), and – at the central level – by the Governmental Representative for Cybersecurity and the Board for Cybersecurity.

The Act imposes a number of obligations on NCS components and entities. In particular, essential service operators are required to implement security management tools within their information systems enabling the provision of the services concerned. Also, they have an obligation to:

- exercise permanent risk analysis and incident management,
- implement technical and organizational measures as appropriate and proportionate to the estimated risks,
- gather information on cyber threats and vulnerabilities of the information system supporting provision of a given service,
- report serious incidents to the appropriate CSIRT no later than 24 hours from its detection,
- use appropriate measures to prevent and limit the detrimental impact of the detected cyber incidents on the rendered services, including removal of the identified vulnerabilities.

The CSIRT teams are required to ensure coherent and complete risk management system at the national level and to implement the measures to mitigate cyber threats of cross-sectoral and cross-border nature, as well as to coordinate the handling of reported incidents. Each CSIRT has a clearly defined scope of responsibility and a set of supervised entities. The tasks of the CSIRTs include, among others:

- monitoring cyber threats and incidents at the national level,
- estimation of risks, related to the disclosed cyber threats, and the occurring incidents, including a dynamic risk analysis,
- providing information on incidents and risks to the entities of the NCS,
- responding to the reported incidents and issuing messages informing about the identified cyber threats,
- classification of incidents and coordination of their handling.

The Act on NCS also imposes on the cabinet minister responsible for developing and maintaining an ICT system being able to:

- support the cooperation of all the national cybersecurity system entities,
- report and handle incidents,
- perform risk analysis at the national level, and disseminate warnings relevant to the considered entities.

The rest of the paper is organized as follows. Section II presents architectural and functional features of the National Platform for Cybersecurity (NPC) – an ICT system enabling collecting and processing of the current available information on a security status of essential and digital services. NPC is designed to assess the possible detrimental impacts of the identified threats on the services. Some solutions, supporting secure information sharing and risk analysis at the national level, are presented in Section III. Section IV describes the concept of NPC system implementation in the operational environment. In the conclusion section, possible limitations related to promoting and achieving the cybersecurity awareness at the national level are discussed.

II. National Platform for Cybersecurity

An important component of the ICT system, that meets the requirements of the Act on NCS, is the research project entitled "*National Platform for Cybersecurity*" (NPC) carried out within the framework of the CybeSecIdent Program on "*Cybersecurity and e-Identity*", supported by the National Centre for Research and Development. The main goal of the project is to develop a prototype of a comprehensive, integrated system for continuous monitoring, detection, depicting the threats and risks and disseminating the warnings that concern the threats actually affecting or likely to affect in the near future, both the quality and continuity of essential and digital services and the tasks performed by public entities, in particular those services and tasks, the deterioration of which may cause significant damage to security, public order, international relations, and to broadly understood economic interests.

To achieve this goal, it was necessary to create the mechanisms for integration of the security management systems used by various institutions and companies, and an aggregation of a distributed knowledge from numerous databases. In addition, it was necessary to develop procedural and technical solutions to ensure secure sharing and dissemination of the information about events that could adversely affect the cybersecurity.

The NPC ecosystem, shown in Figure 1, includes essential services operators (ESO), digital service providers (DSP), Computer Security Incident Response Team (CSIRT), other NCS entities, NPC Backbone Network and external sources of threat data. The external sources of threat data, available to the NPC entities, are collected and verified at the CSIRT level, which provides integrated and updated online threat database for the service providers.

A partnership cooperation model of the NCS entities was adopted. This means that the service providers are free to make decisions on joining the Platform and complying with mutually accepted principles of cooperation, especially in terms of protection the shared data.

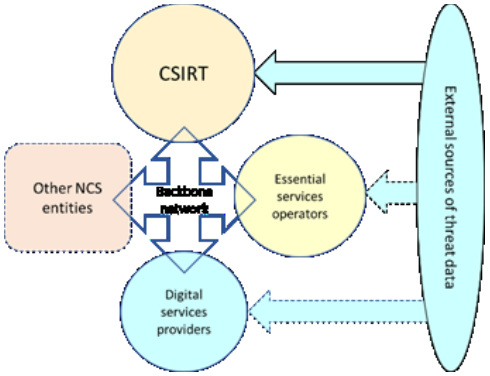

Fig.1. NPC ecosystem

The Platform supports secure exchange of several types of data between CSIRT and the Security Operation Centers (SOC) of the service providers, like for instance:

- information on the rendered services and the conditions for their provisioning (including, but not limited to service interdependencies) and the possible consequences related to disruptions of service continuity and/or quality),
- information on the identified security incidents together with the incident descriptions and possible consequences (i.e. impact on the rendered services),
- information on the identified vulnerabilities along with their potential impact on the exploitation of those vulnerabilities on the security of the rendered services,
- reports on newly discovered vulnerabilities and the indicators of compromise (IoC),
- information on security breaching events,
- reports concerning suspicious data and raw data requiring detailed analysis,
- results of technical analyses related to cybersecurity,
- recommendations and conclusions resulting from performed analyses,
- possible hazard warnings,
- results of risk analysis in relation to rendered services,
- recommendations regarding the desired actions to mitigate the effects of incidents and possible threats.

The National Platform for Cybersecurity, as shown in Figure 2, consists of four functional system component types, i.e.: Operations Centre System (OCS), Edge System (ES), Management System (MS), and Backbone Network (BN).

The OCS is an application system that supports building situational awareness.

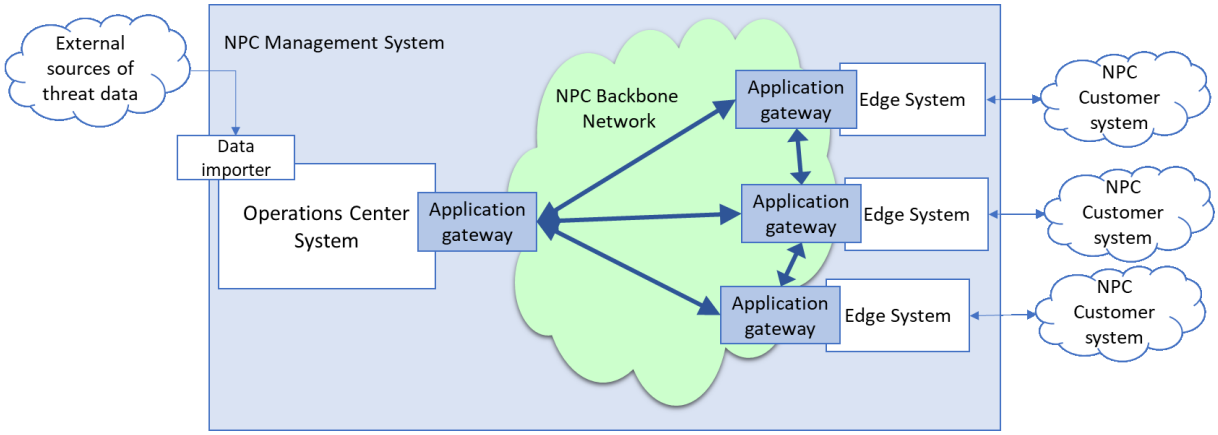

Fig.2. NPC systems

It is a central place for exchange of the cybersecurity information. It integrates the data about threads obtained from external sources, collects information from the ESs, relevant to the security and continuity of rendered essential and digital services, and it provides its own information resources necessary for quick and effective response to existing or potential threats. The OCS is a part of the CSIRT system preforming an outstanding role in execution of several essential processes that include:

- provision of information on the present status of cybersecurity concerning essential and digital services, both at the local and national level,
- management of incident reporting,
- aggregation of vulnerability data available from the external sources and sharing the integrated vulnerability database with the NPC customers[1],
- modelling of the service interdependencies and threats propagation,
- security risk analysis at the national level,
- exchange of knowledge supporting technical analysis of threats,
- dissemination of security warnings.

To ensure reliable operation, the OCS is deployed in broadly available configuration (Dual Modular Redundancy). The Edge System is a customer portal enabling access to the Platform resources. It provides a graphical user interface (GUI) and application programming interface (API) for integration with security management systems used by the customer. The system also performs the tasks related to monitoring and recording the customer activity and ensures accountability and non-repudiation of the exchanged information.

Application gateways perform the functions related to secure sharing of resources between the NPC system in accordance

[1]Customer is an entity that provides essential and/or digital services and participates in exchanging the cybersecurity data over the Edge System

with the adopted security policy. The Backbone Network connects the NPC system components using encrypted virtual tunnels (VPN) created in the existing telecommunications networks. The Management System performs the tasks related to management of the certificates, system devices, system components, and application configurations, as well as of monitoring the security status of all NPC systems.

III. SELECTED SOLUTIONS

A. *Assessment of the services' interdependencies*

A necessary condition for safe and reliable provision of an essential or a digital service is to ensure a high level of protection of the network and information systems upon which its operation is conditioned. However, due to existing dependencies and interdependencies of the services, a malfunction of a single service may cause cascading, negative impact on other services provision, as it was discussed for instance in [10,11,12,13].

For this reason, an important part of NPC is a mechanism supporting identification and assessment of impact of potential threats that can lead to violation of continuity and deterioration of the quality of essential and digital services due to their complexity and interrelation. It supports:

- creation of the network of services rendered by different providers and the services' interdependencies,
- dissemination of the information on incidents that could violate the stability and security of the services,
- dynamic risk assessment of the services and modelling risk propagation in the cybersphere,
- selection of specific security recommendations and their distribution to service providers to improve safety of rendering the services.

A network of the services' interdependencies is obtained by conducting surveys, in which service operators answer a number of questions. The survey collects the information in three sections:

- a set of data that uniquely identifies the operator,
- description of attributes of each essential/digital service being reported,
- description of the supporting services.

The network of interdependent services is presented in the form of weighted graph, where the vertices (V) represent services and the edges (E) reflect the dependency of the services. The edge E_i is described by the vector:

$$E_i = \left(V_m, V_n, \boldsymbol{K}^{(m,n)}\right) \tag{1}$$

where $\boldsymbol{K}^{(m,n)}$ is the matrix of criticalities describing impact of V_n on V_m regarding the aspects of availability (a), integrity (i), and confidentiality (c), i.e.:

$$\boldsymbol{K}^{(m,n)} = \begin{bmatrix} k_{aa}^{(m,n)} & k_{ai}^{(m,n)} & k_{ac}^{(m,n)} \\ k_{ia}^{(m,n)} & k_{ii}^{(m,n)} & k_{ic}^{(m,n)} \\ k_{ca}^{(m,n)} & k_{ci}^{(m,n)} & k_{cc}^{(m,n)} \end{bmatrix} \tag{2}$$

The graph structure and the criticality matrices determine the importance of services, i.e., the impact on safe and reliable operation of other services. This impact can be expressed in terms of scope and intensity that a given service malfunction has or may have on the other services. Taking into account (1) and (2), the importance of service V_m may be expressed by security triad, i.e.: availability, integrity, and confidentiality:

$$\boldsymbol{q}^{(m)} = \begin{bmatrix} q_a^{(m)} \\ q_i^{(m)} \\ q_c^{(m)} \end{bmatrix} \tag{3}$$

A number of metrics are discussed in the literature, for instance in [14], to express the criticality of a service impact. For the purpose of this work, the recursive maximum availability degree was adopted, which is based on the highest value of the metric for the service directly dependent on V_m:

$$q_a^{(m)} = min\left(10, 1 + \frac{1}{10} max_n\left\{k_{aa}^{(m,n)}\right\}\right), n \in \mathcal{E}^{(0ut;1)}(V_m) \tag{4}$$

A detailed presentation of the mechanism and description of procedures used for identification and security management of the services are presented in [15]. A comparative study on sensitivity of various centrality indexes to measure each service vulnerability, combined with various aggregation methods to errors in edge weights, reported by service operators presented in [14] confirmed the value of the proposed formulas.

B. *Application gateway*

The application gateways create closed and centrally configured set of devices that perform basic functions ensuring the secure sharing of resources between NPC entities, i.e.:

- data transfer in accordance with the distribution rules,
- hiding information about the sender and recipient of the message,
- anonymous acknowledgment of the receipt of a message,
- anonymization of the sensitive data,
- message encryption.

The NPC security policy assumes that an individual customer cannot know the names and physical addresses of the other customers. The full list of NPC customers and configuration data of the Backbone Network is known only to the NPC management system. Only the identity of the OCS is known, by default, to all NPC customers.

All messages from any customer system are forwarded to the OCS. If a given message should be sent to some other customers, it is addressed using a symbolic name of that group corresponding to a defined number of proper names. The symbolic name may correspond, for example, to industry sector or community to which a customer belongs. The full list of NPC customers, grouped under the symbolic names, is known to the NPC management system only.

Camouflage of the message sender relies on changing the value of the selected fields in its header to the constant value "*anonymous*". The sender's anonymization is not carried out in case of the message exchange with OCS. The recipient's concealment procedure is also used for anonymous acknowledgment of the messages receipt. A full acknowledgement is made by the OCS only.

If a customer message contains the sensitive data, the broad disclosure of which may threaten the security or reputation of this customer, then these data are anonymized. The data are marked by the sender in a specific way, which makes the application gateway to replace them by a string of characters "*xxx*" of the same length as the original text whenever this message is sent to the other customer. Anonymization is not performed for the messages transferred to OCS.

The application gateways are authenticated with the X.509 certificate. Certificates are generated for each functional system and signed with the CA root certificate of the NPC. Each of them contains the name of the functional system, its public key, and the certificate's validity period. The message sent by the application gateway is accompanied by the signature of the sending system.

Messages, shared within the NPC, are encrypted both at the network and the application layers of OSI model. Standard IPSec protocol is used for securing VPN connections between the NPC entities. In addition, the elliptic curves cryptography is used at the application layer for encryption of the data transferred between NPC system components.

C. Risk analysis at the national level

Obtaining awareness of cyber security, both at the level of the organization and on a global scale required elaboration of a methodological basis for assessing the type and scale of the identified or likely threats in cyberspace, their propagation and consequences for the provision of key and digital services. Achieving a coherent and reliable global image requires a uniform - by all NCS entities - approach to assessing cyber threats. Karbowski et al. in [16] propose using Markov chain model, for assessing the risk of unfavourable events through calculation of an indicator concerning availability of interdependent services, which is a function of the current state of the system. A hierarchical approach to on-line risk assessment at the national level, taking into account cyber threats and vulnerabilities as identified at a local level of the services' providers is shown in [17].

As a part of the NPC, proprietary risk analysis methodology has been developed, covering both the dynamic risk analysis procedure, carried out by service providers (so-called own risk), and the static and dynamic risk analysis procedures carried out by the Operations Centre System.

It was assumed that the own risk results from the possibility of violating confidentiality, integrity, and availability of the service by using the vulnerabilities of the ICT infrastructure (hardware and software) used to provide it identified by the service provider. The results of the analysis carried out by the customer are reported to OCS.

The risk analysis, performed at the Operations Centre, depicted in some details in [18], is based on a map of service interdependencies and takes into account the threats resulting, among others:

- known vulnerabilities identified by the Platform's customers in their ICT infrastructure,
- preparing the customer's organization for effective cyber security management,
- incidents reported by customers and obtained from external sources.

The impact of these threats is estimated using the adopted measure of criticality of the impact of services, and then the value of the so-called aggregate risk is calculated.

On this basis, the aggregate risk is determined for a set of services (rendered by a single entity or a set of entities, within the sector, between the sectors or in the whole space).

In the event of incident, whose consequence is a violation of the security of service provision, there is a temporary (until removal of the effects of the incident) increase in the value of aggregate risk, according to the effects caused by it, and determination of new risk values for other services. The effects of the incident are estimated on the basis of criticality of the service's impact on a given entity, sector or geographical area, which enables determination of the scale of the threat and an extent of its impact.

By appropriately linking the results of analyses, carried out by the Operation Centre System, a global picture of the state of cyber security is created. Elements of the situational picture available to NCS entities - to the extent and degree of detail resulting from their role - deliver the necessary data enabling rapid response already at the stage of emergence of threat symptoms and the selection of appropriate measures to eliminate or limit their scope and consequences.

IV. NPC IMPLEMENTATION

A software layer of the NPC consists of several application systems that can operate independently. Edge Systems can exchange data without an OCS being present. In case of the complete or a partial network outage, all application systems are able to operate and store data. Data that have not been sent due to network outage or a remote system unavailability are stored locally until the problem is resolved. The NPC applications were deployed on a self-hosted Kubernetes platform that provides, among others, horizontal auto scalability and high level of availability. Each NPC application system is divided into a set of domain-specific, interconnected applications, called microservices, (Figure 3).

Microservices form a business logic layer that communicates with database backends and serves data to the front-end application for the interaction with the user. The Angular front-end application implements all views and exchanges only the data to the business logic layer. Application systems can be deployed in a highly available or stand-alone mode, according to end-user needs. All application systems share such architecture which allows for a unified approach to their implementation, deployment of security policy management mechanisms, interchangeable use of software components, both in edge and centre systems, as well as for secure and scalable communication between particular systems. The prototype of NPC was installed and tested in the demonstration environment of the Research and Academic Network Institute – National Research Institute (NASK) in Poland. Several operators of essential and digital services representing different economy sectors were connected via the NPC Backbone Network to the Operations Centre System that enabled individual users (institutions) to verify the basic NPC functionalities.

The underway works are focused on installation and integration of the system with the CSIRT operational environment and on execution of complete functional and validation tests.

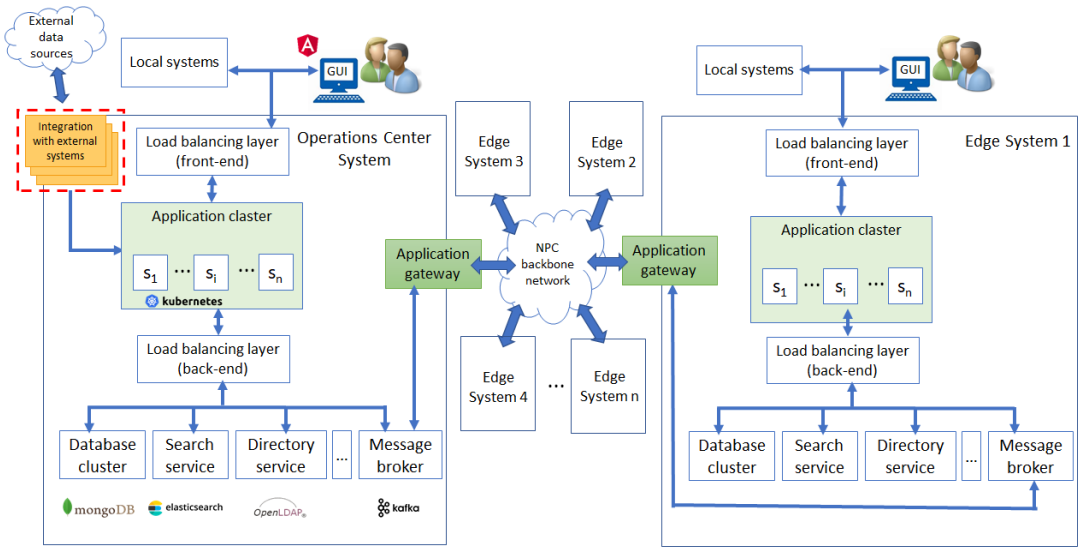

Fig.3. NPC application systems

CONCLUSION

Lessons, learned from the NPC implementation, indicate a need to overcome a number of procedural and technical issues for obtaining reliable and complete cybersecurity picture at the national level. The scope and degree of details of such a picture depends on the ability of all entities involved to providing essential and digital services to effectively detect and successfully react to cyber threats originating or being maliciously installed in their technical infrastructure as well as on their readiness to share the information on security breach events. Lack of sufficiently strong and widely accepted mechanisms, ensuring the expected level of trust of these entities in mutual and/or external relations, as well as insufficient awareness of the benefits of such collaboration can seriously decrease the cybersecurity level. Additionally, a significant number of entities still does not have highly qualified and experienced cybersecurity specialists and some of them also do not have the effective tools for configuration management (i.e. CMDB), which dramatically limits their ability to protect their utilities and information systems from cyber threats. Also, the rules and the procedures, related to the cooperation between the CSIRTs, remain an open and a very complex problem to be solved. The same refers to elaboration of effective procedures and mechanisms enabling creation of a consistent and reliable cybersecurity evaluation and presentation at a national level when based upon the data obtained from the partial images created by different CSIRTs.

ACKNOWLEDGEMENTS

The author thanks prof. Krzysztof Malinowski for interesting discussions and valuable suggestions, which helped to structure this work.

REFERENCES

[1] S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, 2001, pp. 11 – 25.

[2] R. Zimmerman, "Decision-making and the vulnerability of interdependent critical infrastructure", in: *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics* , vol. 5, The Hague, 2004, pp. 4059 – 4063

[3] F. Petit et al., "Analysis of critical infrastructure dependencies and interdependencies", Technical Report, Agronne National Laboratory, ANL/GSS-15/4, 2015.

[4] J. Banerjee, A. Das, A. Sen, "A Survey of Interdependency Models for Critical Infrastructure Networks", Cornell University, arXiv:1702.05407v1 [physics.soc-ph], 2017.

[5] Skopik, G. Settanni, R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defence through security information sharing", *Computers & Security* vol. 60, 2016, pp. 154 – 176.

[6] S. Puuska et al., "Nationwide critical infrastructure monitoring using a common operating picture framework", *International Journal of Critical Infrastructure Protection,* vol.20, 2018, pp. 28 – 47.

[7] G. Settanni et al., "A collaborative cyber incident management system for European interconnected critical infrastructure", *Journal of Information Security and Applications*, vol. 34, 2017, pp. 166 – 182.

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, (https://eur-lex.europa.eu/eli/dir/2016/1148/oj).

[9] ETSI, Implementation of the Network and Information Security (NIS) Directive, Technical Report 103 456 v1.1.1 (2017-10).

[10] R. Wróbel, "Dependencies of elements recognized as critical infrastructure of the state:, in: *Transportation and Research Procedia*, vol. 40, 2019, pp. 1625 – 1632.

[11] B. Wu, A. Tang, J. Wu, "Modeling cascading failures in interdependent infrastructures under terrorist attacks," *Reliability Engineering & System Safety*, vol. 147, 2016, pp. 1 – 8.

[12] M. Ouyang, "Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks," *Reliability Engineering & System Safety*, vol. 154, 2016, pp. 106 – 116.

[13] R. Zimmerman, C. Restrepo, "Analyzing cascading effects within infrastructure sectors for consequence reduction", in: *Proceedings of the IEEE Conference on Technologies for Homeland Security*, Boston, 2009, pp. 165 – 170.

[14] M. Kamola, "Sensitivity of Importance Metrics for Critical Digital Services Graph to Service Operators' Self-Assessment Errors*"*, *Security and Communication Networks*, 2019, doi.org/10.1155/2019/7510809.

[15] M. Kamola et al., "Decision Support System for Identification and Security Management of Essential and Digital Services", in: *Proceedings* of *International Conference on Military Communications and Information Systems*, Budva, 2019, DOI: 10.1109/ICMCIS.2019.8842769.

[16] A. Karbowski et al., "Critical Infrastructure Risk Assessment Using Markov Chain Model", *Journal of Telecommunications and Information Technology,* No.2, 2019, pp. 15 – 20.

[17] K. Malinowski, A. Karbowski, "Hierarchical On-line Risk Assessment at National Level*"*, in: *Proceedings* of *International Conference on Military Communications and Information Systems*, Budva, 2019, DOI: 10.1109/ICMCIS.2019.8842769, DOI:10.1109/ICMCIS.2019.8842731.

[18] M. Janiszewski, A. Felkner, P. Lewandowski, "A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Detection", *Journal of Telecommunications and Information Technology*, No 2, 2019, pp. 5 – 14.