

A Shared Cybersecurity Awareness Platform

Marek Amanowicz

NASK National Research Institute, Warsaw, Poland

<https://doi.org/10.26636/jtit.2021.154421>

Abstract—Ensuring a good level of cybersecurity of global IT systems requires that specific procedures and cooperation frameworks be adopted for reporting threats and for coordinating the activities undertaken by individual entities. Technical infrastructure enabling safe and reliable online collaboration between all teams responsible for security is an important element of the system as well. With the above taken into consideration, the paper presents a comprehensive distributed solution for continuous monitoring and detection of threats that may affect services that provision is essential to security and broadly understood the state's economic interests. The said solution allows to collect, process and share distributed knowledge on hazard events. The partnership-based model of cooperation between the system's users allows the teams to undertake specific activities at the central level, facilitates global cyber threat awareness, and enhances the process of predicting and assessing cyber risks in order to ensure a near-real-time response. The paper presents an overview of the system's architecture, its main components, features, and threat intelligence tools supporting the safe sharing of information concerning specific events. It also offers a brief overview of the system's deployment and its testing in an operational environment of NASK's Computer Security Incident Response Team (CSIRT) and Security Operation Center (SOC) of essential services operators.

Keywords—*cybersecurity awareness, risk and threat propagation, threat intelligence.*

1. Introduction

An increasing number of ever more sophisticated and complex cyberattacks may be observed. For instance, the Computer Emergency Response Team being a part of the NASK – National Research Institute registered 10,447 such incidents in 2020. The said number was the largest recorded in history and represented the fastest year-on-year increase. Phishing was the most common type of attack accounting for proximately 67.2% of all incidents. The use of malicious software was the second most common type of threads, with its share equaling approximately 7.1%. Such attacks pose a serious threat to information technology (IT) systems supporting services that are of critical importance for the society. They may lead to the disruption in the provision of such services, breaching national security, impacting public

and economic order, violating civil rights and freedoms, as well as endangering human life.

In order to protect IT systems, new functionalities must be implemented to enable early detection of threats, to assess their negative impact and to prevent them. Good level of situational cyberspace awareness needs to be achieved as well in order to collect, in real-time, information on threats and risks identified and on their impact on the behavior of systems, as well as on the related processes and services. Achievement of global cybersecurity of IT systems requires that procedures and cooperation networks be established to facilitate the reporting of incidents and to coordinate the actions undertaken. It is also recommended to create a technical infrastructure allowing a safe and reliable online collaboration of all teams responsible for cybersecurity. Detailed identification of vulnerabilities of information and operational technologies (IT/OT) and of the impact that cyber threat events exert on the related processes and services is important as well.

However, as presented in [1], [2], the achievement of such a goal is difficult due to the considerable level of interdependence of the systems and the fact that they share the same information and communications technology (ICT) resources. The interrelations between individual services are of a diverse and complex nature [3], and yet they need to be determined precisely in order to identify threats in cyberspace and to assess their impact on the level of security. Many works devoted to this issue, such as [4]–[6], confirm the need of modeling the network of interdependent infrastructures in order to identify its critical components and to better understand the scale and scope of potential threats. Such an approach enables early identification of threats and triggers alerts allowing to take preemptive actions in order to mitigate the risk encountered. However, in order to create a network of services that reliably reflects the actual condition of and the interrelations between its components, it is necessary to obtain detailed and verifiable data from service providers. Furthermore, an effective threat response requires close cooperation between IT security analysis and management teams from all interdependent entities.

The procedures of cooperation between all entities responsible for IT security needs to be developed as well, in order to ensure a clear situational awareness picture and the highest level of protection. It is also desirable to establish spe-

cific solutions encouraging cooperation and ensuring that the vital interests of all cooperating parties are protected. These activities should be supported by technical systems enabling efficient acquisition, processing and distribution of information concerning threats and their potential impacts. This paper presents an innovative and scalable solution that allows organizations to collect, process and share threat-related information in order to predict and assess the risk involved, and to share distributed knowledge in order to provide a near-real-time response. The said solution focuses on procedural and technical aspects of service network modeling, as well as on processes related to aggregation of knowledge distributed across multiple databases, assessment of risk, propagation of threats, building a common operational picture and sharing threat-related information. A brief overview of the process of deploying the system and testing it in a real-life environment is given as well. The main contributions of this paper are:

- presentation of a novel collaborative distributed system facilitating online cyber threat awareness;
- presentation of an innovative concept for building a network of interdependent services and for relying on such a network in assessing the threats and the related risks.

The remaining part of the paper is organized as follows. Section 2 gives a brief review of the initiatives aiming to improve the level of IT security. Section 3 describes the system's architecture, its main components, features and properties in terms of flexibility, extensibility and scalability. Selected solutions enabling to assess the impact of potential threats on the provision of services, as well as those enabling to collect, process, and secure information related to hazardous events between all National Platform for Cybersecurity (NPC) users are presented in Section 4. The paper concludes with an overview of the system's deployment and with proposals concerning future work.

2. Related Work

Many international and national initiatives have been undertaken recently to boost the security of IT systems in order to improve reliability and availability of services. The Directive of the European Parliament and of the Council [8] on security of network and information systems (NIS) of 6 July 2016 (hereinafter referred to as the NIS Directive) encourages a number of such initiatives. The NIS Directive imposes, on the Member States, the obligation to implement several legal measures, including by establishing national strategies for the security of networks and information systems, and sets forth requirements and procedures for reporting cybersecurity incidents by service operators and providers. In response to this, the European Telecommunications Standard Institutes (ETSI) [9] and many European

countries established their strategies to implement the requirements of the NIS Directive¹.

For example, the CS-AWARE project [10], launched under the Horizon 2020 program, focuses on creating solutions targeted for local public administration authorities, non-governmental organizations, as well as small- and medium-sized companies. The tools developed enable 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 are based on mechanisms for sharing information about actual threats, relying on big data analysis and processing. By leveraging the existing processes of sharing cybersecurity-related information, CS-AWARE enables and improves incident detection and meets the information sharing-related requirements of the NIS Directive.

Another interesting approach to improve an organization's ongoing awareness of the risk posed to its business by cybersecurity attacks has been developed as part of the PROTECTIVE project [11]. The said approach allows to raise the level of situational awareness by enhancing the correlation and prioritization of security alerts, therefore pinpointing the relevance of the organization's assets to its business. Using the context-awareness approach, any organization may identify its key business goals and may define the relationships between such goals, simultaneously determining information and computer assets of critical importance. This data is combined with near-real-time scoring of the assets' vulnerability levels. This helps rank alerts based on their potential damage to the threatened assets and business.

Many new solutions focus on increasing the awareness of cyber threats and on improving the level network and information system security. For example, an interesting approach to the problem of building common cybersecurity awareness by critical infrastructure operators is presented in [12]. By aggregating, analyzing and correlating data obtained from security management systems, a global cybersecurity picture is created allowing also, due to the links between critical infrastructure elements, to anticipate threat propagation-related risks. An inspiring proposal of an IT system for collaborative cyber incident management for the European interconnected critical infrastructure is presented in [7].

The Polish Parliament passed the Act on the National Cybersecurity System (NCS) [13] which specifies the following: organizational framework of the system, tasks and responsibilities of all entities involved, the manner in which supervision and control over the implementation of the Act is exercised, as well as the scope of the cybersecurity strategy. This aims to create a comprehensive solution for boosting protection against threats in Poland and for enabling effective cooperation with other Member States. The Act is building on service operators, digital service

¹more information on status of NIS Directive implementation in EU countries is available at <https://www.digitaleurope.org/resources/nis-implementation-tracker/>

providers and public entities. The NCS 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, the Governmental Representative for Cybersecurity and the Board for Cybersecurity. The NCS concept requires its components and the related entities to assume responsibility for several aspects. In particular, essential service operators are required to implement security management tools within their information systems to support the provision of services. They are obliged, inter alia, to perform risk assessment and to manage incidents on an on-going basis, to collect information on cyber threats and vulnerabilities of the information system supporting the provision of a given service, and to report serious incidents, to the appropriate CSIRT, within 24 hours at the latest. CSIRT teams are required to implement a coherent and comprehensive risk management system at the national level, to undertake actions to mitigate cyber threats of cross-sectoral and cross-border character, and to coordinate the handling of the reported incidents. Each CSIRT has a clearly defined scope of responsibilities and a set of entities it supervises. CSIRT tasks include monitoring cyber threats and estimating risks related to the disclosed cyber threats, including by performing dynamic risk assessment at the national level, classifying incidents and coordinating the process of handling such incidents. The CyberSecIdent research program focusing on “Cybersecurity and e-Identity” was launched for the purpose of implementing the NIS Directive. The research project titled “National Platform for Cybersecurity” (NPC) was conducted between 2017 and 2020 within the framework of the program. Its aim was to develop a prototype integrated system used for continuous monitoring, detection of and warning about threats and risks affecting or likely to affect the quality and continuity of services whose deterioration may cause significant damage to the overall security level.

3. NPC System Overview

3.1. System Architecture

The NPC consists of four systems (Fig. 1):

- Edge systems (ES) located within the customers’² infrastructure, serving as the NPC’s portals to the platform resources,
- Operations center system (OCS), i.e. an application system supporting situational cyberspace awareness and constituting a central point for exchanging information on cybersecurity. By default, there is one OCS instance within the platform, but the architecture allows for the existence of more centers that exchange data with each other,
- Management system (MS) which manages both the application and network layers of the NPC,

²Customer is an entity that provides essential and/or digital services and participates in exchanging cybersecurity data over the edge system

- NPC backbone network (BN), i.e. dedicated communication infrastructure that enables secure information exchange between the platform systems (mainly OCS and ES) in wide area networks.

The operations center and the edge systems ensure integration with the user’s systems that, as a rule, are located in the operator’s private networks and may initiate data exchange with the platform systems, such as the malware information sharing platform (MISP), security information and event management (SIEM) system or incident management (IM) system.

The OCS retrieves and aggregates data from external sources assumed to be located in untrusted networks. These include, for instance, network security incident exchange database (n6), national vulnerability database (NVD) or vulnerability database (vulners.com). The OCS initiates communication and retrieves the data, but the source cannot initiate communication with the OCS.

The management system includes a set of tools and services such as:

- managing a public key infrastructure,
- managing the configuration of systems and applications,
- managing the configuration of network devices of the NPC backbone network,
- monitoring the security status of the platform and all system components,
- maintaining a replica of the system directory.

The key functions of the platform are performed by application systems (i.e. OCS and ES). The system architecture developed is universal (Fig. 2) and enables to implement specific OCS and ES solutions.

The application system architecture includes:

- front-end load-balancing layer for HTTP/HTTPS protocols, designed to provide the users and local systems with a simplified interface for highly available applications,
- application layer implemented by a highly available cluster containing domain-specific, interconnected applications, called microservices, responsible for the system’s business logic. The following applications within this cluster operate in special security zones:
 - application gateway ensuring the secure sharing of resources between the NPC systems,
 - data importer for data acquisition from external sources deployed only in the OCS,
- back-end load balancing layer for various protocols ensuring unified interfaces with the services provided for the applications,

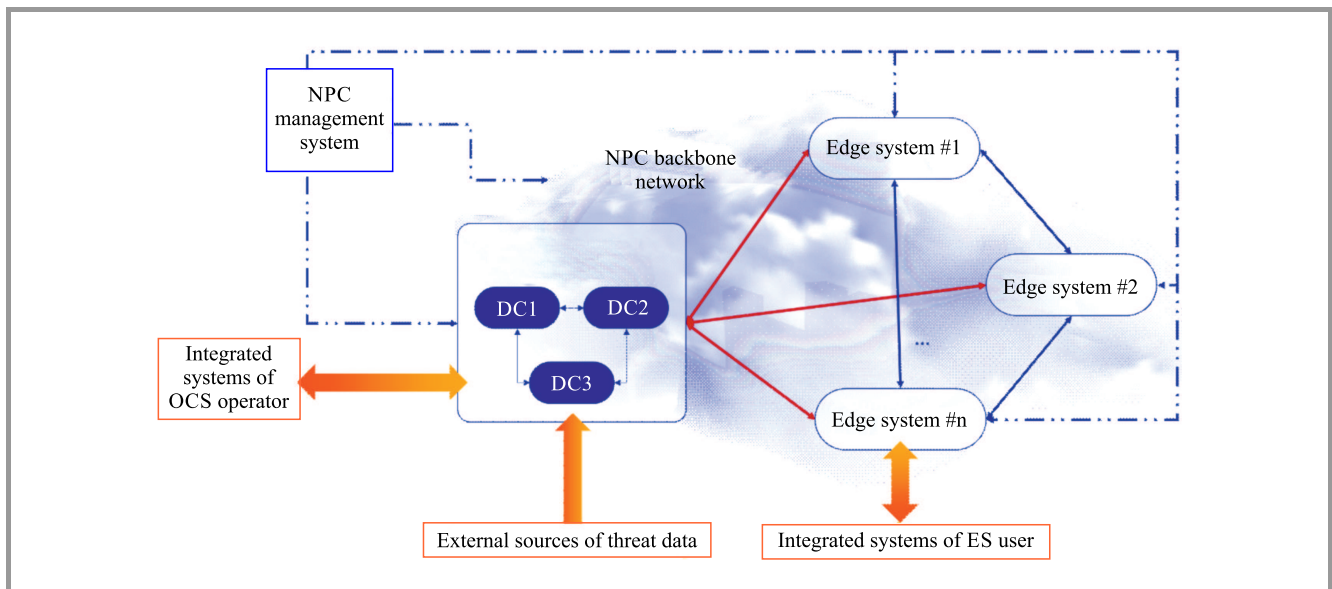


Fig. 1. NPC architecture.

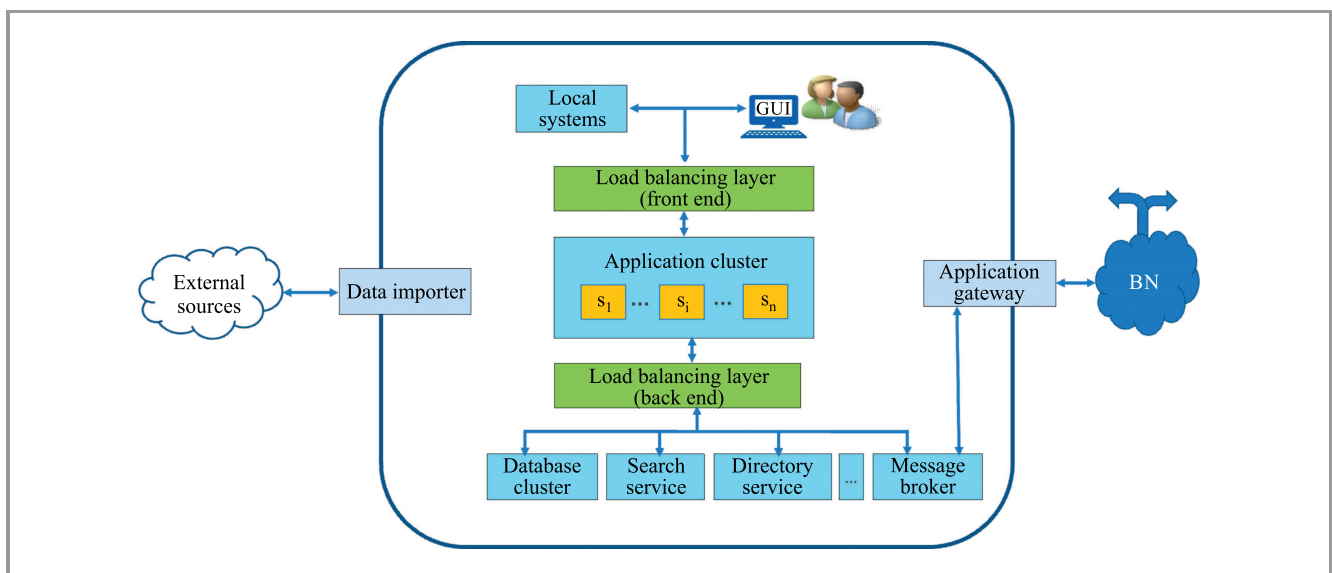


Fig. 2. Application system architecture.

- database back-end layer containing the services provided for the application, such as, for instance:
 - database cluster that stores operational data,
 - directory service, i.e. a database of the NPC users and their permissions,
 - search service enabling full text searches covering the operational data,
 - message broker providing asynchronous message exchange between applications.

The application system may run in a stand-alone or high-availability configuration, and its components, services, and service layers are developed in a high availability configuration, i.e. are distributed over many physical resources. The ES may exchange data without the OCS being present.

In the case of a complete or partial network outage, all application systems are capable of operating properly. Data that have not been sent due to network failure or unavailability of the system are stored locally until the problem is resolved. The NPC applications were deployed on a self-hosted Kubernetes platform that provides scalability and a high level of availability.

3.2. Information Processes

Operation of the NPC system relies on a partner-like collaboration between its users, meaning that service providers are free to decide whether to join the platform and comply with mutually accepted cooperation principles, especially those pertaining to the protection of the data shared.

The security-specific data are exchanged between CSIRT and the related service provider. There is also a possibility of sharing some data between a group of users in compliance with the applicable security requirements. Such an exchange may occur, for instance, when OCS is temporarily unavailable or if the user wants to deliver urgent data to a group of users, such as those belonging to the same business group or sector. It should be stressed that all data exchanged directly between the users have to be submitted to the OCS as well.

The exchange of information is carried out within the functional processes, i.e. when surveying the service providers, handling incident reports, assessing the risk, exchanging information on security events, providing warnings about threats and risks, sharing information on vulnerabilities, and issuing recommendations.

The service providers (ES users) are obliged to provide the following types of data to the OCS:

- detailed information on the services rendered, on the conditions for providing such services and on the potential consequences related to disruptions of their continuity or quality,
- notification of incidents that would exert a significant disruptive effect on the provision of services, including detailed incident descriptions and their potential consequences (i.e. impact on the services rendered),
- outcomes of risk assessment processes associated with the services rendered.

In addition, they may provide the OCS with reports on newly discovered vulnerabilities and the indicators of compromise (IoC), the results of their analysis, information on suspicious data, raw data requiring for detailed studies, and information about the technologies used.

The OCS processes and analyses data collected from external threat sources, as well as those submitted by ES users and shares its own information resources in order to ensure a quick and effective response to existing or potential threats. The OCS performs a significant role in the providing crucial processes that include:

- providing information on the present cybersecurity status of the services, at local and national level,
- managing incident reporting,
- gathering vulnerability data from external sources and sharing the integrated vulnerability database with NPC users,
- modeling the interdependencies between services,
- predicting threats and risks propagation and their impact on cyberspace security,
- analyzing security risks at the national level,
- sharing knowledge supporting technical analysis of threats,

- distributing security warnings,
- providing NPC users with recommendations regarding the desired actions to increase the protection of their information infrastructure.

Data are transferred from the ES in unicast mode, while the OCS may transmit data in unicast or broadcast/multicast mode.

3.3. System Features

The NPC system is based on a universal architecture that relies on the NPC technology stack. The application architecture is based on microservices, ensuring a high degree of system flexibility and allowing the implementation of selected components. It also reduces the need to modify specific services or applications, keeping the system-related costs low. Consequently, the applications used at one place may be easily modified and used in other parts of the system.

The NPC is a scalable and distributed system that may be deployed on a large scale or scaled down to a single rack unit or even less. It is also possible to distribute the system components and functions between multiple physical locations.

The solution ensures low deployment and maintenance costs due to the fact that the ES and the applications may be developed and installed without maintenance downtime and, what's more, implementations are automatically executed in a way imperceptible to the user. It is worth noticing that all applications are managed within the Kubernetes cluster.

Good interoperability of the NPC system is achieved thanks to the availability of all relevant data through:

- documented REST API,
- custom integration with security platforms, such as TAXII, MISP and SIEM, with a potential extension to other platforms as well,
- dedicated API for creating new applications, adding new vulnerability data sources or threat data integration.

The management system enables automated deployment of applications throughout the platform, which is particularly important when adding new entities or upgrading the applications. The system ensures:

- complete control of the entire software supply chain,
- backups and quick data restore for ESs,
- consistency of timescales throughout the NPC,
- monitoring the entire NPC and all its components,
- central analytics of logs from all NPC systems and devices.

It should also be noticed that management functions may be split between the NPC application and the backbone network, for instance, if BN management needs to be performed by a separate entity.

4. Selected Solutions

4.1. Network of Interdependent Services

An expert subsystem supporting decision-making processes and ensuring the safe provision of services by NPC users is an essential part of the platform. It supports the identification of interdependencies between NPC users, their services and the ICT infrastructure used. It also allows to determine the potential impact of incidents (scale, geographic reach, duration), and to obtain the input data required to assess their significance (spread of threats and assessment of their outcomes).

The decision support subsystem is made up of four components, as shown in Fig. 3. All service providers are surveyed before they start the operational use of the system in order to collect the required input data.

Ensuring the consistency of data obtained from the surveys allows to create a network of interdependencies services. The attributes of the network components reflect the criticality (impact on other services) of the individual services and the relationship between them [14]. The process of managing the network of interdependent services allows to conduct several operations, including network upgrades and reconfigurations, depending on the needs of the system analyst.

In order to ensure coherent and reliable security awareness at the national level, a uniform approach to assessing cyber threats by all NPC users is required. A concept of evaluating the risk of unfavorable events by relying on the Markov chain model to calculate an indicator concerning the availability of interdependent services is presented in [15]. Malinowski and Karbowski in [16] adopt a hierarchical approach to risk assessment at the national level, considering cyber threats and vulnerabilities identified by service providers at a local level. The NPC system uses its proprietary risk assessment methodology covering both

the dynamic risk analysis procedure carried out by service providers (the so-called “own risk”) and the static and dynamic risk analysis procedures performed by the OCS [17]. It was assumed that an 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 NPC users are reported to OCS.

The risk assessment performed at the OCS is based on mapping service interdependencies and takes into account threats resulting, inter alia, from the following:

- vulnerabilities identified by service providers in their ICT infrastructure,
- criticality of the services and their interdependencies,
- the extent to which the NPC customer organization ensures the safe rendering of the services,
- reported incidents, IoCs and other security events,
- information on security issues, obtained from various sources, concerning the ICT infrastructure supporting the services reported by NPC users.

Results of the risk assessment procedure are visualized using a network of interdependent services presented in Fig. 4. The node colors correspond to the risk values assigned to the specific services. The width of the lines indicates the strength of specific impacts. More information about a given service and the related risks may be obtained by clicking on the selected node. The panel on the right-hand side of Fig. 4 shows the details of the service chosen (with a blue border), including the risk value and its trend.

By linking the results obtained by OCS, a global cybersecurity awareness picture is created based on a configurable panel with data about the current and predicted state of service in cyberspace. The example presented in Fig. 5 shows the current status of service-related risks, statistical data concerning incidents reported and vulnerabilities identified, the most exposed services, service threshold risk

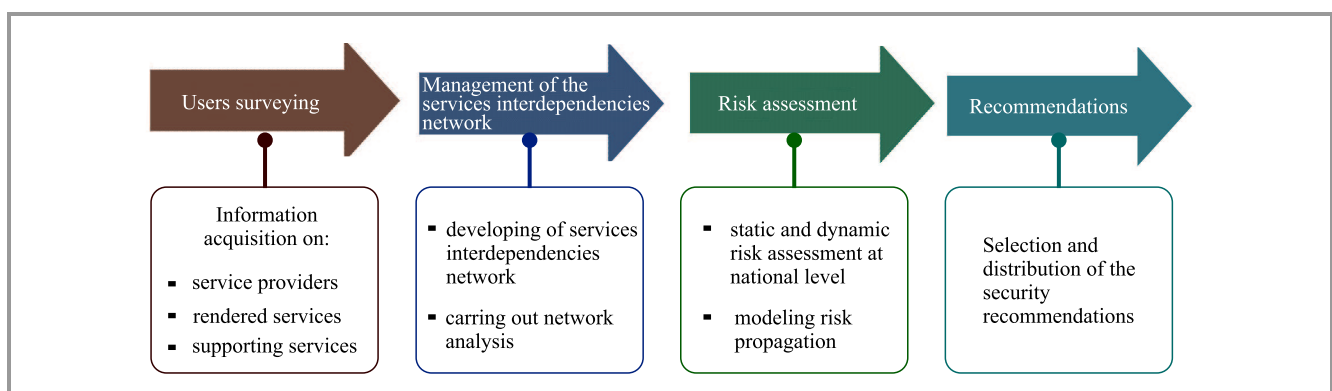


Fig. 3. Components of the decision support subsystem.

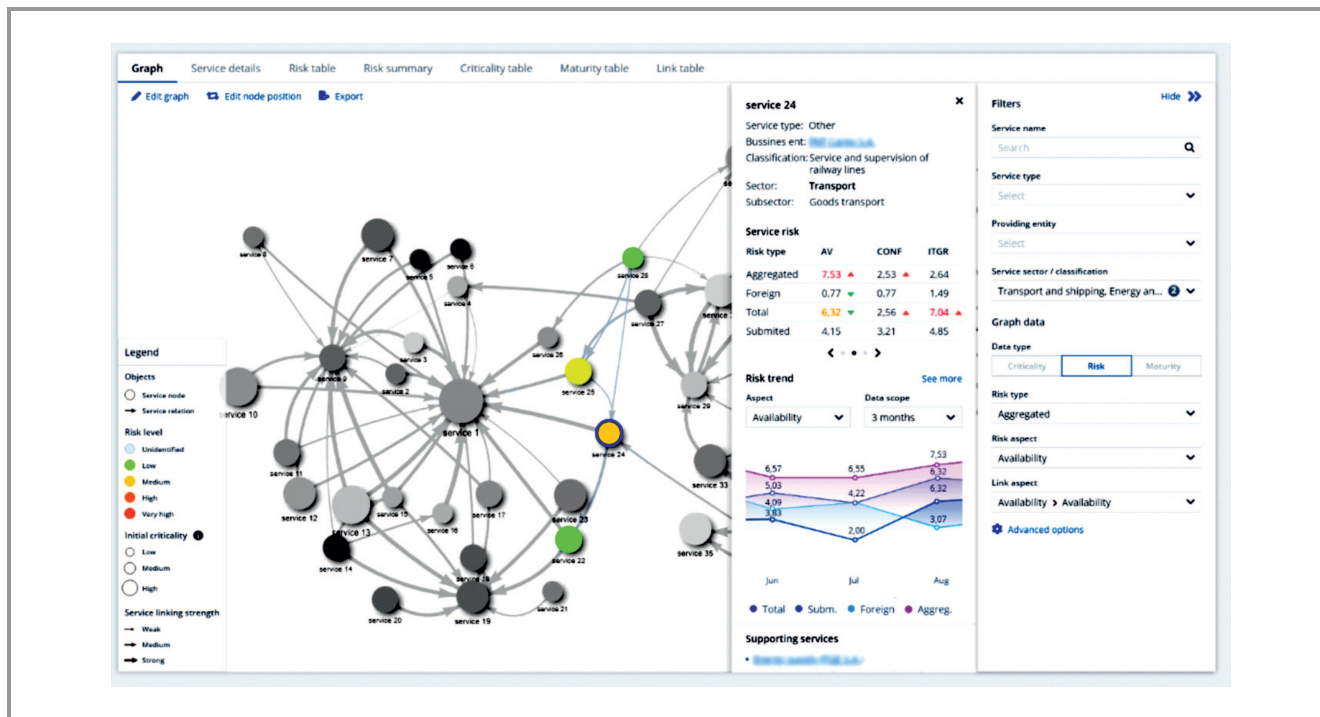


Fig. 4. Results of the risk assessment procedure carried out by OCS in an exemplary network of interdependent services. (see the digital version for color images)

values, and sectoral risks. The supervising analyst is capable of customizing the layout and the content to meet the current needs.

The situational awareness data are shared with NPC users – to the extent and degree of detail resulting from their role, the enabling them to respond quickly and select appropriate measures to eliminate or limit any potential consequences.

The analysis, provided by OCS, contains input data supplied to the rule-based engine that is tasked with selecting appropriate recommendations in order to ensure a high level of security of the services rendered. A dedicated tool is used for the distribution of the recommendations to service providers.

4.2. Threat Intelligence Mechanisms

A set of threat intelligence tools is used to efficiently exchange information on cyber events that enable a coordinated response to the threats that have been identified.

The malware information sharing protocol (MISP) is relied upon to exchange information about network security events and indicators of compromise (IoC). Application services, installed in central and edge systems, perform tasks related to MISP integration, synchronization of the databases, and data distribution within the system. For users who do not have their own MISP instances, a dedicated tool was developed to make this data available. The NPC ensures also integration with the n6 platform designed to collect, process and share information about network events and potential security incident (IoCs). The n6 was created by CERT (Poland) and contains information about sources of the attack, i.e. URL, domain, IP, and name of malicious software as well as other unique information if available.

The application service implemented in the OCS collects and aggregates data on IT/OT systems' vulnerabilities from external public sources and converts these into the format required by the NPC. The aggregated data and source vulnerabilities (i.e. before aggregation) and several related in-

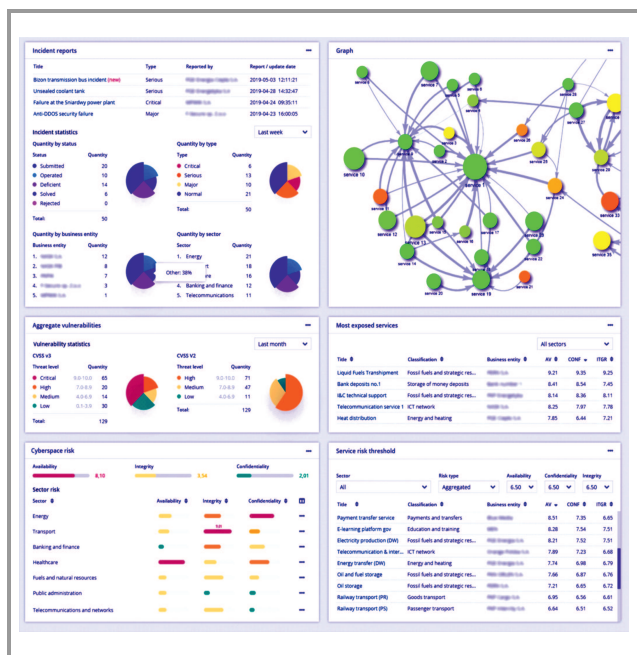


Fig. 5. Example of a situational picture.

formation resources, e.g. technical bulletins, risky products, vulnerability relationships with other objects, are available to all platform users. The tools used for database management ensure the OCS analyst is able to constantly update its contents and allow all users to search the database quickly according to selected criteria. The database enables service providers to identify potential threats and quickly implement the mitigation solutions required.

The NPC users are able to share their knowledge and experiences related to the specific incidents and other security events by using a dedicated application. They can exchange observations and conclusions from their own technical analysis. Such an analysis may also be performed by OCS and ES analysts and may be made available in accordance with the applicable distribution rules. The ES is capable of delivering sensitive data, e.g. malware code, to the OCS. The warning feature is activated when predefined security events occur, enabling the OCS analyst to send a warning message. The operator may also support the recipient's actions taken by adding attachments to the message. Moreover, all threat intelligence tools used have a built-in chat mechanism that supports online communication.

4.3. Security Measures

The NPC incorporates a set of built-in security features for secure sharing of sensitive information and protecting the vital interest of the NPC users, including:

- encrypted end-to-end communications,
- marking sensitive data and configurable anonymization,
- auditing of user actions and extensive logging, assuring non-repudiation and accountability of exchanged data.

The data shared within NPC users are encrypted at the network and application layers of the OSI model. The 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 data transferred between the NPC system's components. The system of X.509 certificates is applied for authentication of the system users and signing the shared data, which ensures its credibility.

The NPC security policy assumes that an ES user is not capable of obtaining the names and physical addresses of the other users. The configuration data of the backbone network and a list of NPC users are available only to the management system. Only the identity of the OCS is known, by default, to all NPC users. All data sent from the ES are forwarded to the OCS. Data targeted for other edge systems are addressed using a symbolic recipient name. The complete list of symbolic names is known to the management system only. Unavailability of the data sender relies on changing the value of the selected fields in its header to the constant value anonymous. Sender anonymization is not performed

when messages are exchanged with the OCS. The recipient concealment procedure is used also for "anonymous" data receipt acknowledgement. Full confirmation is made by the OCS only.

The system incorporates a security feature that allows the message sender to hide sensitive data. This type of data is marked by the user, meaning the anonymization feature replaces the selected fragment with a "xxx" of the same length as the original text before sending the message. Anonymization is not performed for messages sent to the OCS. The application system guarantees that the tagged fragment will not be retransferred to the platform users.

Additionally, an audit service is performed to ensure accountability and non-repudiation of user actions and system functionalities. The system acquires and stores information about all events, i.e.:

- time stamp,
- user login data,
- address of the host on which the action was performed,
- name of the acted module,
- action type (e.g. create, update, send),
- subject to which the action relates (e.g. incident, vulnerability),
- optional additional data.

An API for the web application is used for analyzing the collected data, enabling the search function of users' and system actions with the activities filtering, sorting, and correlation finding.

5. System Deployment

The prototype of the NPC was developed in an operational environment of CSIRT NASK with the participation of four service providers from different sectors of the market (financial, transport, energy) and an entity providing cybersecurity services. Three spatially distributed data centers of CSIRT NASK were connected, via the backbone network, with edge systems located within the service providers' IT infrastructure (Fig. 6). The OCS was deployed in a configuration characterized by a high degree of availability, known as dual modular redundancy, where data center number 3 acts as an arbitrator.

A full range of tests was performed to verify the functionality of the system and the results obtained confirmed the system's usability. That enables CSIRT analysts and a number of service providers to perform a trial using a prototype of the system. The scenarios verified included user activities related to the development of a network of services,

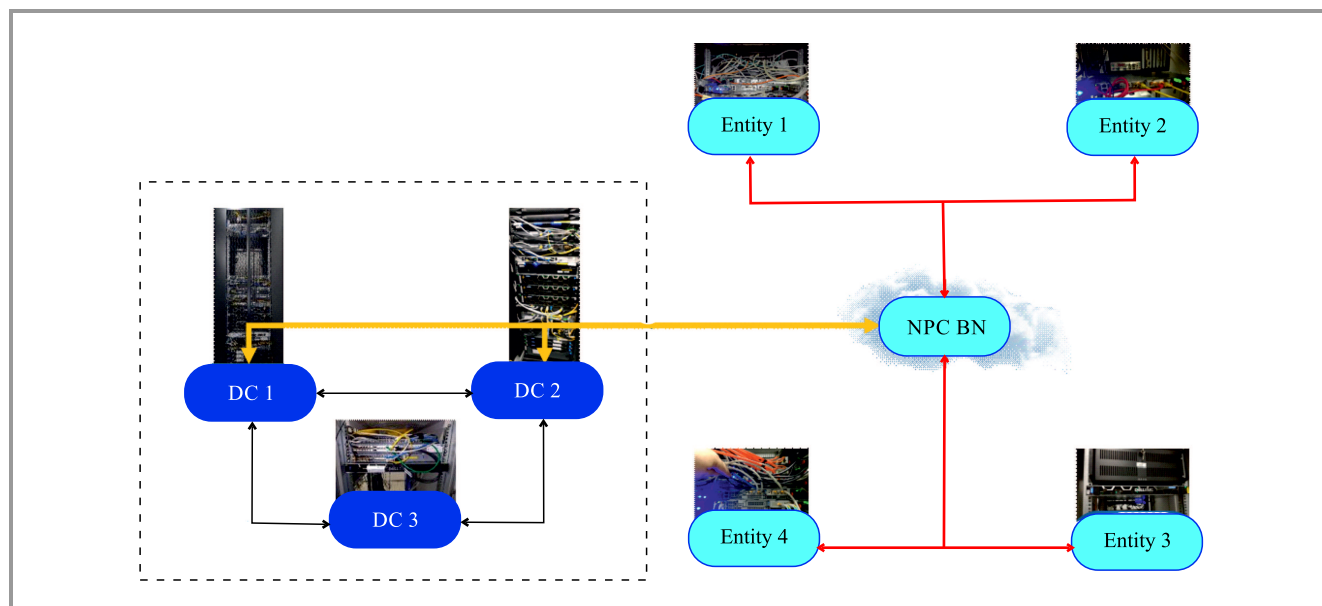


Fig. 6. NPC deployment in an operational environment.

reporting and handling incidents, sharing and using an aggregated vulnerability database, sharing knowledge, using threat intelligence features, assessing the risk and assessing cyberspace security.

All this allowed the users to better understand the functionalities of the NPC system and its operational value. The test results confirmed suitability of the prototype that may serve as a technological foundation for a full-scale implementation of a solution that meets all applicable legal requirements. The system architecture was expanded to incorporate three (instead of one) OCSs and to make the system accessible for all NCS entities.

The lessons learned from the deployment of NPC confirm that the actual level of cyber threat awareness depends on all parties involved in detecting and reacting to cyber threats originating or maliciously installed in their technical infrastructure, as well as on their readiness to share cyber threat-related information. The NPC system presented offers effective features ensuring a high level of trust of the service providers in mutual and/or external relations. It delivers tools for improving the user collaboration, supports secure threat data sharing and allows to develop a shared cybersecurity picture. All these features lead to increasing the level of cyberspace awareness and help react to the actual or potential cyber threats in a more coordinated manner.

Future work needs to be focused on implementing the recommendations formulated based on prototype tests and should lead to developing an operational NPC version for the Polish Cyber Security System. The features of the presented solution rely on the universality and flexibility of the system architecture, support quick and effective implementation of the NPC for use cases (other than NCS) requiring safe sharing of information about threats, creating shared situational awareness and coordinated responses. The pre-

sented system may act as an ICT infrastructure for the Security Incidents Response Teams (SIRTs) or Information Sharing and Analysis Centers (ISACs). In particular, it can be adapted for the safe sharing of information and building a global situational awareness picture for security management in complex and dispersed structure organizations.

6. Acknowledgements

This work was performed under the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Centre for Research and Development (CyberSecIdent Program).

The author would like to thank a large group of his highly committed associates from NASK, National Centre for Nuclear Research, National Institute of Telecommunications and Warsaw University of Technology, contributing their extensive expertise to the process of designing and deploying the system in question.

References


- [1] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies", *IEEE Control Syst.*, vol. 21, no. 6, pp. 11–25, 2001 (DOI: 10.1109/37.969131).
- [2] R. Zimmerman, "Decision-making and the vulnerability of interdependent critical infrastructure", in *Proc. IEEE Int. Conf. on Systems, Man and Cybernetics (IEEE Cat. No. 04CH37583)*, The Hague, Netherlands, vol. 5, 2004, pp. 4059–4063 (DOI: 10.1109/ICSMC.2004.1401166).
- [3] F. Petit and L. P. Lewis, "Incorporating logical dependencies and interdependencies into infrastructure analyses", *George Mason University*, 2016 [Online]. Available: <https://cip.gmu.edu/2016/02/17/incorporating-logical-dependencies-and-interdependencies-into-infrastructure-analyses/>

- [4] A. Nieuwenhuijs, E. Luijff, and M. Klaver, "Modeling dependencies in critical infrastructures", in *Proc. IFIP Int. Federation for Informat. Process.*, 2008, pp. 205–213 (DOI: 10.1007/978-0-387-88523-0_15).
- [5] R. Setola, V. Rosato, E. Kyriakides, and E. Rome, "Managing the complexity of critical infrastructures", vol. 90, *Springer Int. Publishing*, 2016 (DOI: 10.1007/978-3-319-51043-9).
- [6] C.-H. Han, S.-T. Park, and S.-J. Lee, "The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system", *Int. J. Crit. Infrastruct. Prot.*, vol. 26, 2019, (DOI: 10.1016/j.ijcip.2019.100312).
- [7] G. Settanni *et al.*, "A collaborative cyber incident management system for European interconnected critical infrastructures", *J. Inf. Secur. Appl.*, vol. 34, pp. 166–182, 2017 (DOI: 10.1016/j.jisa.2016.05.005).
- [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" [Online]. Available: <http://data.europa.eu/eli/dir/2016/1148/oj>
- [9] ETSI TR 103 456 v1.1.1, "Implementation of the Network and Information Security (NIS) Directive", 2017 [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
- [10] CS-AWARE Project, *Horizon 2020 Programme* [Online]. Available: <https://cs-aware.eu>
- [11] PROTECTIVE Project, *Horizon 2020 Programme* [Online]. Available: <https://protective-h2020.eu>
- [12] S. Puuska *et al.*, "Nationwide critical infrastructure monitoring using a common operating picture framework", *Int. J. Crit. Infrastruct. Prot.*, vol. 20, pp. 28–47, 2018 (DOI: 10.1016/j.ijcip.2017.11.005).
- [13] "Act on the National Cybersecurity System", *J. of Laws*, item 1560, 2018, [Online]. Available: <https://uodo.gov.pl/en/file/307>
- [14] M. Kamola *et al.*, "Decision support system for identification and security management of essential and digital services", in *Proc. Int. Conf. on Military Commun. and Informat. Systems (ICMCIS)*, Budva, Montenegro, 2019, pp. 1–7 (DOI: 10.1109/ICMCIS.2019.8842769).
- [15] A. Karbowski *et al.*, "Critical infrastructure risk assessment using Markov chain model", *J. Telecommun. Inf. Technol.*, vol. 2, pp. 15–20, 2019 (DOI: 10.26636/jtit.2019.130819).
- [16] K. Malinowski, A. Karbowski, "Hierarchical online risk assessment at national level", in *Proc. Int. Conf. on Military Commun. and Informat. Systems (ICMCIS)*, Budva, Montenegro, 2019, pp. 1–5 (DOI: 10.1109/ICMCIS.2019.8842731).
- [17] M. Janiszewski *et al.*, "A novel approach to national-level cyber risk assessment based on vulnerability management and threat intelligence", *J. Telecommun. Inf. Technol.*, vol. 2, pp. 5–14, 2019 (DOI: 10.26636/jtit.2019.130919).



Marek Amanowicz graduated from the Military University of Technology, Warsaw, Poland, where he held several positions, including that of a faculty dean and Vice Rector for R&D. He was a Deputy Chairman of the Polish National Committee of the International Union of Radio Science. He served as the head national representative to

the Information Systems Technology Panel of the NATO Scientific and Technology Organization. He worked at TAC ONE, an international company in Paris, as a systems V&V manager. In 2017, he joined the NASK – National Research Institute, assuming the position of professor. He is an elected member of the Electronics and Telecommunications Committee of the Polish Academy of Sciences. He has led many national and international research projects focusing on systems engineering, mobile communications, modeling and simulation. He is the author or co-author of more than 200 papers published in scientific journals or at national and international scientific conferences. His current research interests focus on communication systems engineering and information security of complex technical systems.

 <https://orcid.org/0000-0002-9132-5788>

E-mail: marek.amanowicz@nask.pl
 NASK – National Research Institute
 ul. Kolska 12
 Warsaw, Poland