Advances in Reliability, Safety and Security, Part 4 – Kołowrocki, Dąbrowska (eds.)
 ISBN 978-83-68136-16-6 (printed), ISBN 978-83-68136-03-6 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Cybersecurity Awareness Provision: Case Study

Marek Amanowicz

NASK – National Research Institute, Warsaw, Poland

Abstract

The paper presents a conceptual and practical approach to achieving cybersecurity awareness at the state and enterprise level. It stresses that ensuring cybersecurity awareness requires, among other things, the precise identification and understanding of the multilateral interdependence of services and tasks provided by enterprises and public institutions caused by strong interrelations of critical infrastructure sectors and the sharing of information and communication technology resources. The attention is paid to describing cyberspace modelling methodology, risk assessment procedures, and its propagation within cyberspace. The suitability of the proposed approach and the effectiveness of cybersecurity awareness provision are evaluated by a case study established in collaboration with the Polish essential services operator. The paper concludes with some remarks on the preliminary outcomes of the case study execution.

Keywords: cybersecurity, situational awareness, cyberspace modelling, risk assessment

1. Introduction

The critical dependence of government and corporate organizations on information technology (IT) means that cyber threats can significantly affect operational efficiency, causing significant economic and social consequences on both local and global scales. With the substantial increase in cyber threats, cybersecurity awareness is vital to ensure the safety of employees and organizations and limit the negative impacts of hazard events in accomplishing business objectives. It provides perception and understanding of the cyberspace state, its determinants and consequences and enables acting responsibly to avoid potential risks. The effectiveness of protection against threats requires cybersecurity awareness at all levels of the organization and on a national and global scale.

Ensuring cybersecurity awareness requires, among other things, the precise identification and understanding of multilateral interdependence of services and tasks provided by enterprises and public institutions, as presented in (Rinaldi et al., 2001) or in (Petit et al., 2017), caused by strong interrelations of critical infrastructure sectors and the sharing of information and communication technology (ICT) resources. It significantly expands the area of influence of cyber threats and creates new channels for attacks. Consequently, it can substantially damage security, public and economic order, the functioning of public institutions, civil rights and freedoms, and human life and health.

On the positive side, there is growing community awareness of cyber issues, general awareness within organizations of the risks involved, and using existing knowledge to create and implement procedures to ensure comprehensive ICT security management. Many enterprises and institutions are establishing Security Operations Centres (SOCs) equipped with capabilities and resources to monitor and respond to computer incidents. However, relatively few qualified and sufficiently experienced cybersecurity professionals significantly limit their evolution and effectiveness. As a result, smaller entities, in particular, are forced to rely on external security services provided by organizations that do not have the necessary knowledge of internal business conditions and the consequences of a security breach for executed operations. It should also be noted that SOC operations focus mainly on the infrastructure layer, with little attention paid to the business processes layer. It is also clear that effective identification and analysis of cyber threats, assessment of their impact on critical business objectives or ongoing tasks, and effective response are impossible without the collaboration of all teams or individuals

responsible for security management (Skopik et al., 2016). Obtaining a reliable situational picture across cyberspace, whether at the state or individual entity level and ensuring a high level of protection against threats requires the elaboration of procedures that enable the exchange of experiences and support the practical cooperation of such teams. Another challenge is overcoming the complexity and interrelations of cyberspace components and the diversity of cybersecurity awareness determinants. It leads to the necessity of elaborating procedural and technical solutions for effectively acquiring, processing and distributing verified information on hazards and their potential impacts and providing cybersecurity awareness at the national level and all levels of individual organizations.

The rest of the paper is arranged as follows. Section 2 presents a global approach to cybersecurity awareness and its implementation at the national level. Exploiting the experience gained from the design and operational use of the National Platform for Cybersecurity (NPC) and lessons learned from critical infrastructure entities, a Situation Awareness Management System (SAMS) was developed to support an individual entity in gaining awareness of cyber threats within cyberspace at all organization levels. A description of the approach used is provided in Section 3. Referring to the methodology described in (Amanowicz and Kamola, 2022), new methods, namely dynamic risk assessment and identification of critical paths of hazard propagation within cyberspace, are presented. It also gives examples of the SAMS application widgets used for cybersecurity awareness management. The paper concludes with some remarks on the preliminary outcomes of the case study execution.

2. National Platform for Cybersecurity

The elaboration of the ICT system, which meets national and European requirements for ensuring a high level of resilience and security of networks and information systems (NIS Directive), was carried out under the project entitled National Platform for Cybersecurity, implemented under the CybeSecIdent programme sponsored by the Polish National Centre for Research and Development. Its main objective was to develop a prototype of a comprehensive, integrated system for the continuous monitoring, detection, imaging and warning of threats that affect or could affect the quality and continuity of critical services, digital services and tasks performed by public entities, which deterioration may cause significant damage to security and to broadly understood economic interests of the state. For its achievement, it was necessary to create mechanisms to integrate the protection systems used in different institutions and sectors of the state's critical infrastructure and to aggregate the distributed knowledge collected in numerous databases, as well as procedural and technical solutions to ensure the secure sharing and accessibility of information on events affecting cybersecurity.

The Platform ecosystem, shown in Figure 1, includes operators and service providers, the Computer Security Incident Response Team (CSIRT), stakeholders, public and telecom entities, Information Sharing and Analysis Centers (ISAC), the IT network and external sources of data on threats and hazard events that may affect cybersecurity assessment on a state level.

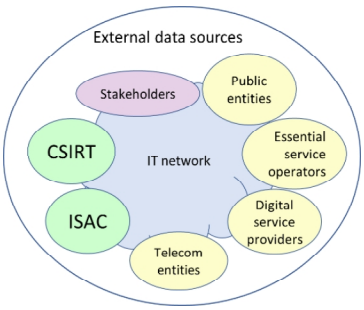

Fig. 1. NPC ecosystem.

The system architecture is based on a partnership model of cooperation between entities in exchanging information on cyber threats. It means that the service providers are free to decide on joining the Platform and comply with mutually accepted principles of cooperation, especially regarding shared data protection. The scope of exchanged data collected by both the CSIRT and the security management teams of essential service operators and digital service providers and also obtained from external sources (e.g. NVD, MISP, n6) includes, among others:

- information on the services provided and the conditions for their provision (including their interconnections and the consequences of a breach in their continuity);
- identified security incidents with their description and effects of occurrence (including impact on services provided);
- Indicators of Compromise (IoC);
- suspicious and raw data requiring detailed analysis;
- results of the dynamic risk assessment related to the services provided;
- recommendations on desirable actions to mitigate the effects of incidents.

Some of these data can be directly exchanged between entities in compliance with the security requirements adopted by a sender.

The data obtained from users are analyzed and processed in the Operational Centre. The results, like:

- updated value of risk related to the rendered services that take into account the impact of threats resulting from services interdependencies;
- recommendations and conclusions from analysis related to the improvement of the security mechanisms;
- warnings on identified threats that may impact the service;

are delivered to the entities for their internal use. Users also have online access to an integrated vulnerability database that is constantly updated.

NPC comprises four functional systems (Figure 2), e.g., Edge Systems (ES) located within the entities' infrastructure, Operations Centre System (OCS) and, Management System (MS) located at CSIRT facilities and backbone communication network (NPCnet). The Operations Centre System that retrieves and aggregates data from external sources is spatially distributed, which ensures its high availability. A centralized management system manages the NPC's application and network layers.

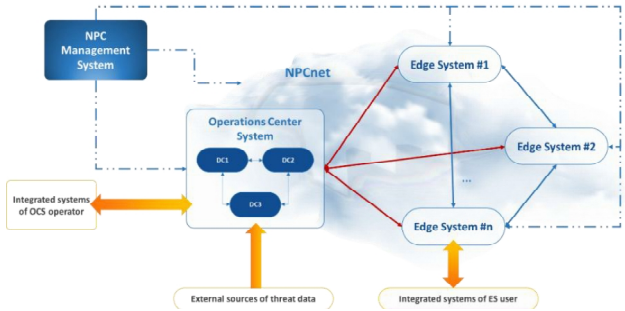

Fig. 2. NPC architecture.

The architectural model is based on microservices, which ensures high flexibility of the system, enables the selection of appropriate functions for implementation in individual components, including adding, removing or dividing, and also reduces the impact of particular service modification on other applications, which in turn ensures low system evolution costs. As a result, the applications used in one place can be easily modified and used in other parts of the system.

The Edge System is a portal to OCS resources. It provides an application programming interface (API) for integrating the NPC with the security management systems used by the service operator and a graphical user interface for its interaction with the OCS. It also performs tasks related to monitoring and recording the users' activity, ensuring accountability and non-repudiation of the information exchanged. The task of the NPCnet is to interconnect the system's components using encrypted VPN tunnels established over existing telecommunications networks. The Management System performs tasks related to certificate management, configuration of devices, systems and applications, and monitoring of the NPC security status, including host and network intrusion detection and behavioural and signature protection of workstations.

Achieving cybersecurity awareness at the state level requires establishing a methodological basis for assessing the type and scale of cyber threats identified or likely to occur, their proliferation and the consequences for rendering the services. Accomplishing a consistent and reliable situational awareness picture requires using a unified approach - by all entities - to assess cyber threats. For this purpose, a proprietary dynamic risk assessment methodology (Janiszewski et al., 2019) has been developed and implemented in the OC system. It was assumed that risk arises from the possibility that the service confidentiality, integrity or availability could be compromised by exploiting vulnerabilities in the ICT infrastructure (hardware and software) used for its

provision. The service operator performs the risk assessment for each rendered service and reports the results to the OC.

A state-level risk assessment is carried out by the Operations Center, taking into account the interdependences of the services provided by the various operators and the threats posed by, among others, identified vulnerabilities and reported incidents. 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 operator or a set of operators within and between the sectors or in cyberspace). A global cybersecurity awareness picture of the state (Figure 3) is created by appropriately linking the results of analyses. It makes it possible to assess the current and projected status of critical infrastructure components, the impact of reported incidents on national security, and to take actions to prevent the propagation of threats. Elements of such view available to service providers - to the extent and degree of detail resulting from their role - deliver the necessary data enabling rapid response already at the emergence stage of threat symptoms and the selection of appropriate measures to eliminate or limit their scope and consequences.

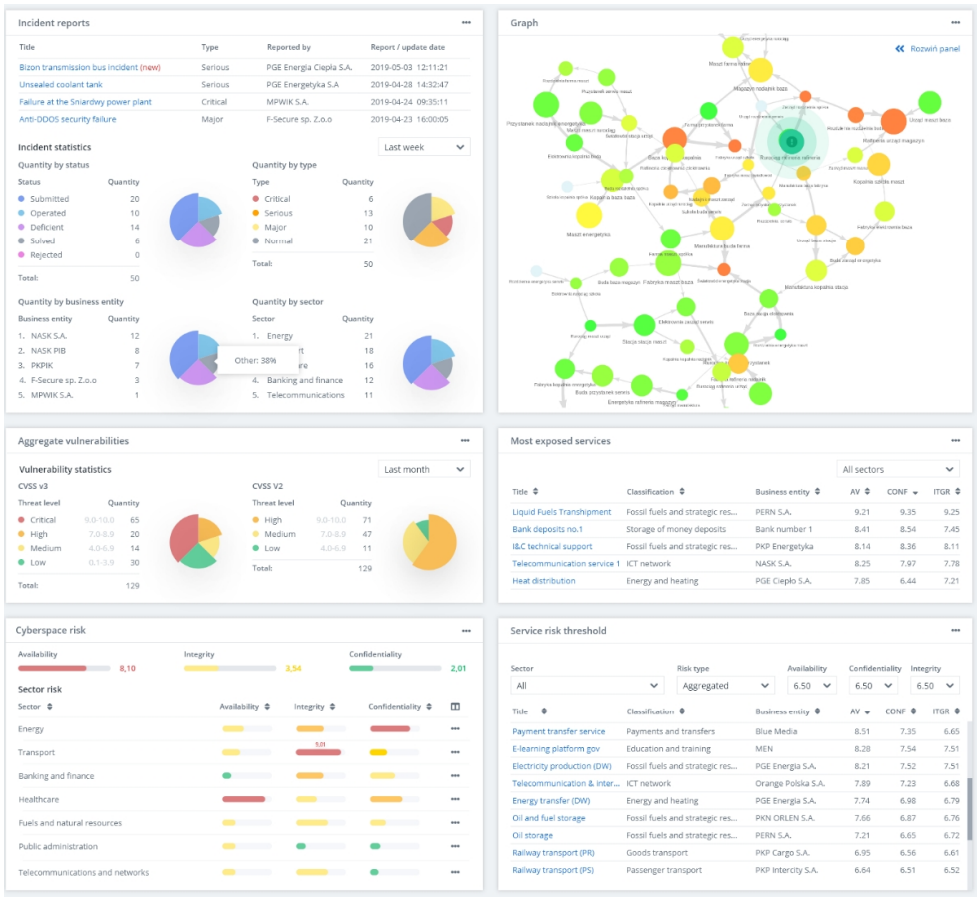

Fig. 3. A sample picture of cybersecurity awareness at the state level.

The prototype of the NPC system was implemented and successfully tested by CSIRT NASK. Several operators of essential and digital services representing different economic sectors were connected to the OCS via the NPCnet, enabling them to assess the basic NPC functionalities. The NPC prototype was the basis for implementing a fully functional version of the system, which has been installed at the national level in Poland and is now used operationally by three CSIRTs.

3. Cybersecurity awareness provision at the entity level

3.1. Modelling of an entity domain

It should be noted that the NPC system does not equip critical infrastructure entities with effective mechanisms and tools to build local cybersecurity awareness, enabling them to analyze online cyber threats and risks that impact rendered services and essential business processes. The lessons learned from implementing the NPC system and experiences from straight collaboration with the critical infrastructure entities allowed for elaborating a solution to fill this gap.

Cybersecurity awareness provision at the company level requires gathering real-time data on potential threats, their scope and scale, and enabling the assessment of the impact of vulnerabilities of software and hardware information infrastructure on the business objectives. It also requires an in-depth expert knowledge of complex interrelations of business processes and information infrastructure caused by complicated and often entangled functional relationships and the scale and importance of their impact on the security and continuity of executed business objectives. Furthermore, information infrastructures do not exist in isolation. The disruption of a single component can have a cascading effect, leading to wide-scale outages with significant consequences for a single entity, industry sector, or even an entire country.

Consider a critical infrastructure entity that provides essential services crucial to maintaining important social or economic activity. Figure 4 shows the main components of the operator's domain and its external interrelations. The business processes, service, IT/OT infrastructures, and technical and security management systems are networked, reflecting interdependencies.

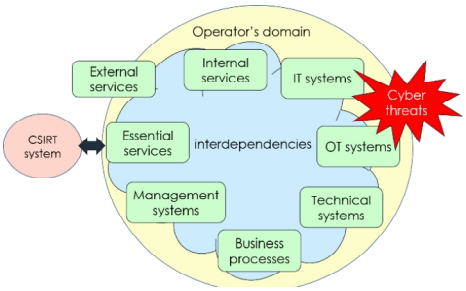

Fig. 4. Essential services operator domain.

From now on, each element of the operator domain will be referred to by the more general term business object (abbreviated as object), which represents, depending on the context considered, a service, a process, and a system or its element. So, the operator's domain can be modelled as a network of interdependent objects, from now on referred to as the network of objects or network for short:

$$\mathcal{N} = \langle \boldsymbol{G},\ \boldsymbol{F}, \boldsymbol{f} \rangle \tag{1}$$

where: $\boldsymbol{G} = \langle \boldsymbol{V},\ \boldsymbol{E} \rangle$ – digraph, $\boldsymbol{V}$ – set of vertices representing objects, $\boldsymbol{E}$ – set of arcs representing objects interdependencies, $\boldsymbol{F}$ – set of functions defined at vertices of graph, $\boldsymbol{f}$ - set of functions defined at arcs of graph.

The functions defined at arcs represent the criticality of impact, i.e., the level of impact of threats resulting from the degradation of confidentiality (c), integrity (i), availability (a) of the object on the security attributes of the related object and the propagation time of degradation. The functions defined at vertices characterize, among others, the level of object exposure to degradation of security and continuity of its operations and the risk posed by the possibility of materializing threats.

The process of the network definition is based on the *AnalyticHierarchyProcess (AHP)* method proposed by (Saaty, 2008). It is performed in two sequential phases, i.e., elaborating a database of business objects with their attributes and establishing objects' interdependence (impact) with their characteristics and relevance regarding the consequences of a security breach. At least two static metrics characterize each object:

- *relative criticality* characterizing the significance of the object's impact on a dependent one;
- *business criticality* describing the importance of the object in accomplishing business objectives

and two dynamic metrics:

- *security status* of the object in terms of confidentiality, integrity, and availability;
- *security risk* concerning confidentiality, integrity, and availability.

The relative criticality of object V_n that takes into account the impact of all P objects interdependent with object V_j is calculated from (2):

$$\omega_{nj} = \frac{s_{nj}}{\sum_{x=1}^{P} s_{xj}} \tag{2}$$

where: s_{nj} – the level of impact of threats resulting from the degradation of security attributes of the object V_n on the security attributes of the related object V_j.

The business criticality υ_n of object V_n is calculated from (3):

$$\upsilon_n = \sum_{z=1}^{Z} s_{nz} \cdot \upsilon_z \tag{3}$$

The object's criticality enables the operator to prepare and implement prevention measures to reduce the impact of threats on its strategic objectives. It also allows it to conduct in-depth analysis to seek technical and procedural solutions that can mitigate business risks arising from the propagation of threats within the operator's domain. Dynamic attributes are calculated based on the acquired data on detected events affecting the current and predicted status of the objects. Interested readers can find (Amanowicz and Kamola, 2022) more information on the operator's domain modelling process and analysis examples to assess the impact of threat propagation within the network of interdependent objects.

3.2. Security risk assessment procedure

Consider the following types of security risks associated with each network's component:

- intrinsic risk resulting from technical and procedural features of the object;
- external (contributed) risk resulting from the propagation of risk in a network;
- overall risk, i.e. a composite of intrinsic and external (contributed) risks.

Each IT/OT infrastructure element is associated with a numerical value of intrinsic risk resulting from its potential exposure to cyberattack, disruption due to technical unreliability and business criticality. The values of the intrinsic risk of external services derive from the agreed conditions of their provision. The values of the intrinsic risk of other objects (business processes, internal services) derive from their exposure to degradation arising from the adopted technical, organizational and procedural solutions for ensuring security, business continuity, and business criticality.

The intrinsic, extrinsic and overall risk values will be assumed to be real numbers in the interval [0,10]. Any change in the value of an object's intrinsic risk resulting, for example, from a change in its level of exposure and resulting from the materialization of an object-related hazard, will automatically recalculate the values of the overall risks of all objects of the network.

For each IT/OT infrastructure element V_n, the numerical values of the potential exposure to attack resulting from its identified vulnerabilities can be determined from a modified equation proposed by (Kim et al., 2014):

$$E(V_n) = min\left[10, \left(IC_{cia}(V_n) \cdot (10 - y) \cdot MI_{cia}^{w_{MI}}(V_n) \cdot MV^{w_{MV}}(V_n) \cdot ACA^{w_{ACA}}(V_n) + ATT(V_n, x, y)\right)\right] \tag{4}$$

where:
$IC_{cia}(V_n)$ – is an *Initial Compromise* level that reflects the object's potential level of compromise due to exploiting some combination of the existing vulnerabilities impacting confidentiality (c), integrity (i), and availability (a);
$MI(V_n)$ – depicts the maximum impact of detected vulnerabilities on (c, i, a);
$MV(V_n)$ – indicates the vulnerability representing the greatest threat to the object V_n;
$ACA(V_n)$ – is a combined parameter of maximum access and access complexity;
$ATT(V_n, x, y)$ – depicts the attack surface, which is a function of the number of vulnerabilities concerning the object V_n and the threat that they present;
w_{MI}, w_{MV}, w_{ACA} – are the weights of relevant parameters.

The value of the security risk resulting from the exposure of an infrastructure object V_n on the accomplishing business objectives is determined from (5):

$$R_{cia}^{\upsilon}(V_n) = [E_{cia}(V_N)]^{\upsilon_n} \tag{5}$$

The level of exposure of the infrastructure object V_n arising from its technical unreliability is determined according to (6):

$$N(V_n) = 1 - K_g(V_n) \tag{6}$$

where: $K_g(V_n)$ – is a likelihood that the object performs correctly.

Thus, the value of risk resulting from the unreliability of the object V_n is calculated from (7) and its intrinsic risk of security and continuity degradation from (8).

$$R^r_{cia}(V_n) = [N(V_N) \cdot 10]^{v_n} \tag{7}$$

$$R^w_{cia}(V_n) = min\{[R^v_{cia}(V_n) + R^r_{cia}(V_n)], 10\} \tag{8}$$

The intrinsic risk of an object representing an internal service or business process derives from its level of exposure to degradation in terms of ensuring security and business continuity and from its business criticality. It was assumed that the exposure to degradation of such objects would be assessed by evaluating the organization's maturity level resulting from the degree of implementation of procedures and mechanisms required by security standards. Thus, the intrinsic risk of the process or service should be determined from (9):

$$R^w_{cia}(V_{p/s}) = \left[10 - \frac{D(V_{p/s})}{100} \cdot 9\right]^{v_{p/s}} \tag{9}$$

where: $D(V_{p/s})$ – is the percentage index of the implementation of security measures, standards and procedures related to process V_p or service V_s .

For the object V_n, which action is not conditioned by any other ones in the network (no incoming relations) should be assumed that its overall risk equals intrinsic risk:

$$R^o_{cia}(V_n) = R^w_{cia}(V_n) \tag{10}$$

The overall risk of an object on which security and continuity impact a set of X other ones is expressed by Eg.(11):

$$R^o_{cia}(V_j^X) = \min\{10, [R^w_{cia}(V_j) + \frac{\sum_{i=1}^{X} R^o_{cia}(V_i) \cdot s_{ij}}{\sum_{i=1}^{X} s_{ij}}]\} \tag{11}$$

where: s_{ij} – the level of impact of threats resulting from the degradation of security attributes of the object V_n on the security attributes of the related object V_j.

3.3. Critical paths assessment

Degradation of confidentiality, integrity or availability of an object caused by a security incident or technical failure causes the event to propagate through the network of interdependent objects along paths leading from the degraded object to objects representing high-level business objectives. There are two attributes associated with each such path:

- threat propagation time, and
- the significance of the impact.

Since there may be multiple paths in the network with the same or similar value of the threat propagation time but with varying impact significance, it is reasonable to determine k>1 of such critical paths. Each path $\mathcal{R}_s^d$ in the network from an object V_s to object V_d is an alternating sequence of objects and their relations, i.e.:

$$\mathcal{R}_s^d: V_s, (V_s, V_{i_1}), V_{i_1}, (V_{i_1}, V_{i_2}), V_{i_2}, \dots, V_{i_{n-1}}, (V_{i_{n-1}}, V_{i_n}), V_{i_n}, (V_{i_n}, V_d), V_d \tag{12}$$

Let us assume that for each relationship (V_i, V_j), the threat propagation delay time τ_{ij} is known, i.e., the time after an object V_j, suffers the effect of the degradation of an object V_i. Thus, the threat propagation time from the degraded object V_s to the object V_d equals:

$$T_{sd} = \sum_{(V_i, V_j) \in \mathcal{R}_s^d} \tau_{ij} \tag{13}$$

The significance of the impact of a threat propagating along the path $\mathcal{R}_s^d$ can be determined as follows:

$$\mathcal{S}_{sd} = \sum_{(V_i, V_j) \in \mathcal{R}_s^d} \frac{s_{ij}}{r(\mathcal{R}_s^d)} \tag{14}$$

where: $r(\mathcal{R}_s^d)$ is the number of relations on the path $\mathcal{R}_s^d$.

For example, Yen's algorithm (Yen, 1971) can be used to determine the k-shortest paths from a degraded object, and the results of the calculations can be presented in the form shown in Figure 5.

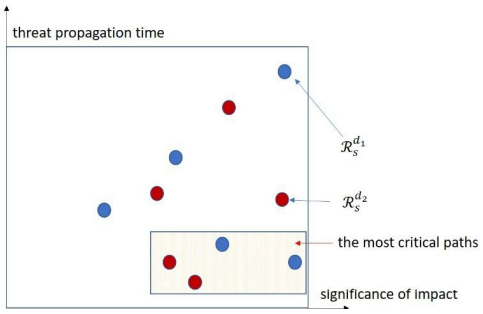

Fig. 5. Example of calculations results, where: $\mathcal{R}_s^{d_1}$ - represent paths from the degraded object V_s to object V_{d_1} $\mathcal{R}_s^{d_2}$ - represent paths from the degraded object V_s to object V_{d_2}.

This example shows that particular attention should be devoted to the paths marked as the most critical since the threat spreads along them at the fastest and greatest severity.

3.4. A case study

The above concept of the operator's domain modelling and analysis of cyber threats' impact on accomplishing the business objectives provided the theoretical basis for implementing a security awareness management system (SAMS) dedicated to critical infrastructure entities. Its primary functions are:

- supporting the process of building and maintaining a network of interdependent services, i.e., provided by the operator, internal and external ones, critical business processes, IT/OT systems and their elements, determining the achievement of business objectives using data obtained from security management systems utilized by the operator. An example of a network of interdependent objects is shown in Figure 6;
- visualization of the current and predicted security status of all network elements and the results of dynamic risk assessment and its propagation within the network;
- predicting the impact of security incidents on the performance of network elements;
- supporting carrying out in-depth analysis, including the "what-if" type.

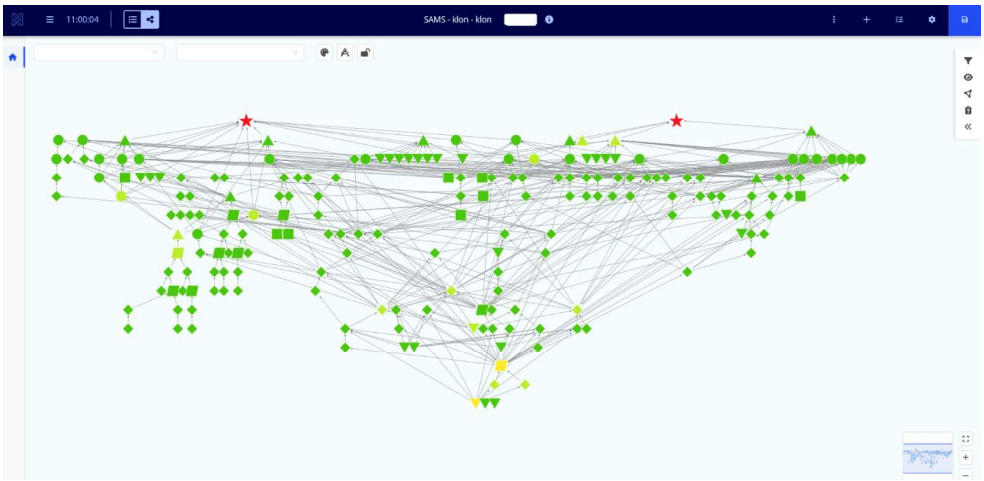

Fig. 6. A screenshot of the SAMS application showing the network structure of interdependent objects. The shape of an object indicates its type, and its color corresponds to its level of business relevance.

The SAMS system's suitability for the operator and the effectiveness of providing cyber security awareness will be evaluated through a case study. As a result of the established cooperation with the essential services operator in Poland, the SAMS system was placed in the operator's environment, as shown in Figure 7.

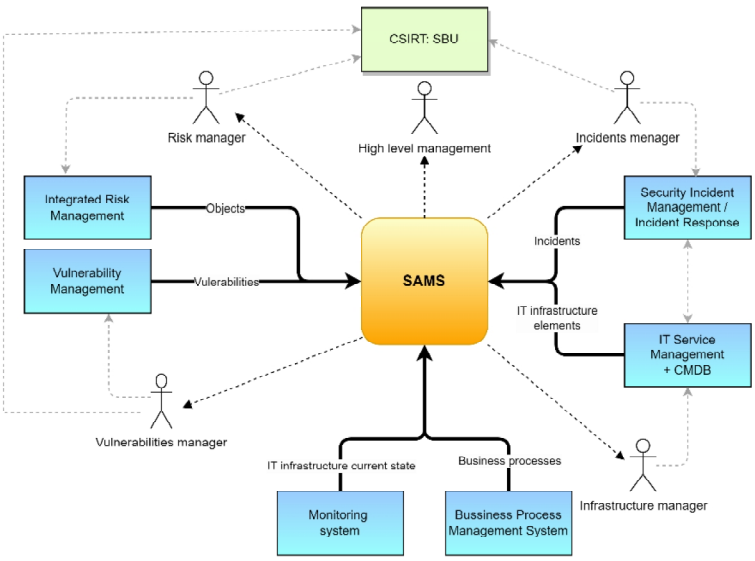

Fig. 7. SAMS in the operator's environment.

The SAMS has interfaces to the management systems, shown in Figure 7, from which it obtains the data necessary to build and manage the network of interconnected objects. Due to the complexity of the building and description of the network, it was assumed that it should be created as automatically as possible, with possible manual completion of missing data. Of course, it is possible to manually enter the entire network if any of the systems is unavailable.

The SAMS provides the key managers identified in Figure 7 with interfaces to perform in-depth analysis related to their tasks and return the results. For example, they can analyze the current structure of the network to identify the critical path of threat propagation, as presented in Figure 5, enabling them to undertake mitigation measures on time. They can also determine the most critical vulnerabilities regarding their impact on business objectives, location, etc. Risk and incident managers are responsible for reporting data to the CSIRT, which is required to provide cybersecurity awareness at the state level.

The successful validation of the proposed concept of providing cybersecurity awareness and further development of the SAMS system is expected to enable its practical use by critical infrastructure entities.

4. Summary

The preliminary results of the case study provide stimulating conclusions regarding the usefulness of the proposed approach and indicate areas for further development. It is pointed out that the domain modelling process creates significant added value, enabling the complete identification of the resources needed to accomplish the main business processes and discover their interdependencies, which are not always obvious. One of the first insights is that SAMS functionalities can effectively support business impact analysis (BIA) by providing objectified data to predict the consequences of security disruptions and the information needed to develop recovery strategies.

Acknowledgement

The paper presents the results of the research project supported by the National Centre of Research and Development in the frame of the CyberSecIdent programme and research project SMAS granted by NASK – National Research Institute.

References

Amanowicz, M., Kamola, 2022. M. Building SecurityAwareness in Cyberspace of Interdependent Services, Business Processes and Systems. Electronics 11, 3835.

Janiszewski, M., Felkner, A., Lewandowski, P. 2019. A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence. Journal of Telecommunications and Information Technology 2, 5 – 14.

Kim, A., Kang, M.H., Luo, J.Z.,Velasquez, A., 2014. A Framework for Event Prioritization in Cyber Network Defense, Technical Report. US Dept. of the Navy. Arlington County, VA, USA.

Petit F., et al., 2015.Analysis of critical infrastructure dependencies and interdependencies, Technical Report ANL/GSS-15/4, Argonne National Laboratory, Lemont, IL, USA

Rinaldi, S.M., Peerenboom, J.P., Kelly T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine 21(6), 11 – 25.

Saaty, T., 2008. Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process. RACSAM Rev. R. Acad. Cien. Serie A. Mat. 102, 251–318.

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

Yen, Jin Y., 1971. Finding the k Shortest Loopless Paths in a Network. Management Science 17 (11), 712 – 716.