https://doi.org/10.32056/KOMAG2024.2.5

Cybersecurity of IT/OT systems in key functional areas of a mining plant operating on the basis of the idea of INDUSTRY 4.0

Received: 15.05.2024

Accepted: 25.06.2024

Published online: 08.07.2024

Author's affiliations and addresses:

[1]Mineral and Energy Economy Research Institute, Polish Academy of Sciences, J. Wybickiego str. 7A, Krakow, PL-31261, Poland

***Correspondence:**

e-mail: arturdyczko@gmail.com

Artur DYCZKO [1*]

Abstract:

The article is based on practical experience and research, presenting the author's concept of applying the principles of cybersecurity of IT/OT systems in key functional areas of a mining plant operating based on the idea of INDUSTRY 4.0.

In recent years, cyberspace has become a new security environment, which has introduced significant changes in both the practical, and legal and organizational aspects of the operation of global security systems. In this context, it is particularly important to understand the dynamics of this environmental change (both in the provisions of the NIS 2 directive and the KSC Act) [1]. Building a legal system as a national response to the opportunities and challenges related to its presence in cyberspace was an extremely complex task. This results not only from the pace of technological change, but also from the specificity of the environment and its "interactivity". The trend in international law that has emerged during COVID-19 and the current geopolitical situation is to treat organizations from the mining and energy sector as one of the important actors in national and international relations [2].

The new regulations introduce and expand international cooperation between individual entities and regulate security strategies and policies, which should take into account the recommendations of the Ministry of Climate and Environment, with particular emphasis on, among others, ensuring the continuity of system operation, handling security incidents and constantly increasing awareness of cybersecurity and cyber threats. It should not be forgotten that threats in cyberspace represent a different class of organizational challenges, largely similar to those posed by other asymmetric threats such as terrorism. Their common feature is that they require less hierarchical and more flexible solutions on state structures. Cybersecurity, both socially and technologically, with all its consequences, emerges as one of the most important concepts of the security paradigm at the national and international level [3].

Keywords: Industry 4.0, mining, IT/OT, cybersecurity, data processing, AI in mining, economic parameters.

1. Introduction

The second decade of the 21st century brought the events that led to a re-evaluation of the current thinking about security management in many domains, brutally verified additionally by the COVID-19 pandemic and the outbreak of the war in Ukraine.

Both of these events are equally important, considering that the armed conflict in Ukraine continues to negatively affect the level of security in neighboring countries, which have automatically become an arena of hybrid operations. This applies in particular to the Baltic states and Poland. As Microsoft reports show, in the contemporary hybrid war model, information influence operations based on social engineering techniques and supported by digital technology are becoming particularly important. Various events, including those taking place in the country, show that information operations can be as effective as complex attacks on industrial infrastructure, while being much cheaper. Currently, false information introduced into public space can be used to cause disruptions in the functioning of a sector that is important from the point of view of the security of an organization, community or state. For example, effective disruptions in the fuel sector can be achieved by causing social hysteria by introducing false information into the media about a significant increase in fuel prices or its limited stocks. A society susceptible to disinformation, subject to panic, will destabilize the situation on the fuel market. Such an operation will be much cheaper than the sophisticated actions of highly respected hackers. Examples of this type of activities make us look at the security of office computers, mobile devices, as well as industrial automation in a broader context [4].

The pandemic forced ICT system administrators to use solutions enabling remote work and learning in those areas where it was possible. A side effect of these then desirable actions was the emergence of new types of risk, related to the level of digital skills of the user who is outside the secure company network and uses important company data as part of his professional activity. In these circumstances, the issue of identity protection and the philosophy of authentication of IT system users become particularly important. During the epidemic, a similar situation was observed in industry. Pandemic restrictions on the movement of personnel, including service technicians, forced many companies to compromise in the area of OT security by allowing remote service and maintenance activities. Unfortunately, this meant additional system vulnerabilities and a potential threat to the continuity of operation of the infrastructure. As a result of these changes, certain risks have moved from the business layer to lower layers, exposing OT to threats in a greater extent than before [5].

Cyberspace protection has become one of the most frequently discussed security topics. Countries, international organizations and other non-state entities understand that the stable functioning and development of the global information society depends on an open, reliable and, above all, safe cyberspace. The growing awareness in this area goes hand in hand with a sharp increase in the number of computer incidents and the emergence of new types of threats.

Poland faces technological, environmental, but also social challenges related to the supply of raw materials that underlie our industrial activities. The civilizational transformation of our economy cannot take place without ensuring the monitoring and safety of industrial processes, these processes cannot be supervised without efficient exchange of information and access to the latest technologies, ICT, automation and control systems, the construction and operation of which is already the subject of routine activities of specialized services [3].

Analyzes of events and vulnerabilities - both reported by the energy sector to the competent authority and included in subsequent reports of consulting and auditing companies, show that a new approach to managing security, resilience and business continuity is needed. This is expressed, among others, by: recent legislative work at the European Union forum, as part of which, on December 27, 2022, amendments to two key directives were published, regarding the resilience of critical entities and measures for a common level of cybersecurity within the territory of the European Union.

The European legislative offensive, which cumulated at the end of 2022, led to the creation of a package of new directives and regulations that are extremely important for the regulated market that

Publisher: **KOMAG Institute of Mining Technology, Poland**

makes extensive use of digital technology. This is particularly important in the case of the NIS 2 Directive (Directive on measures for a high common level of cybersecurity across the EU) and the CER Directive (Critical Entity Resilience Directive). Both directives were created in response to new types of risks in cyberspace, which are based not only on events such as the pandemic or the war in Ukraine, but in particular on the models of functioning of modern supply chains. Nowadays, simple sequences of business processes are becoming less common. Modern supply chains are often complicated connections of smaller or larger sub-processes, the interruption of which may lead to a cascading effect and pose negative consequences unknown in advance. This prompts us to re-examine the areas that should be protected, what protection model should be used and whether an object-oriented or process approach should be used [3].

Unlike the existing legal solutions, the need to cover an entity with the NIS 2 directive will not be signaled by a notification or the issuance of an administrative decision - the interested entrepreneur himself should check whether the subjective scope of the regulation applies to him. The obligations that will be associated with the implementation of directives into national law will mainly concern the application of an approach to security based on risk analysis and the design of risk mitigating measures based on the zero-trust rule. In practice, this will mean giving up on the current principle according to which all resources should be locked in a safe network in favor of protecting these resources under one central policy. This approach significantly hinders the penetration of company resources, typical of today's attack vectors, by obtaining subsequent credentials as part of the so-called lateral movements. The resources that should be constantly protected include identity, data, applications, networks, devices and digital infrastructure. Effective strengthening of resilience in this area is only possible with the involvement of all possible stakeholders - from the management board and administrators to serial users of end devices.

2. Cybersecurity system in key functional areas of the JSW Group is a means to ensure business continuity

In the JSW Capital Group, a systemic approach to managing the security of IT/OT systems began to be created in mid-2017, when the "Strategy for the development of IT/OT systems of the JSW Group" was developed, in which the " Cybersecurity Program " was established. The next stage of strengthening the cybersecurity system being built was the adoption on March 6, 2018 by the Management Board of JSW SA of the "Model for management and supervision of the IT/OT area" in the Group, containing a security strategy along with a roadmap for further work [6]. These activities were intensified with the recognition of the JSW Group as a Key Service Operator in accordance with the provisions of the Act of 5/07/2018 (Dz.U. 2018, poz. 1560) on the national cybersecurity system [7], which led to JSW IT Systems launching on October 10, 2019 a support for JSW Group in implementing the obligations arising from the Act on the national cybersecurity system by introducing the "Model of management and supervision over the IT/OT area" adopted in 2018 and implementing [6]:

- antivirus system with the EDR module to detect and respond to suspicious activities on end devices; thanks to advanced technology that detects cyber-attacks at an early stage, it is an effective weapon against hackers, detecting suspicious activities at their initial stage,
- MDM class system combining the functionality of comprehensive security and the Enterprise Mobility Management (EMM) tool, including traditional mobile application management (MAM) and a mobile content management tool (MCM),
- Log Management system for centralized storage, monitoring, visualization and analysis of server/application/machine logs.

These activities preceded the decision on November 27, 2019 by the JSW Group to launch a strategic project entitled: "Expansion of IT/OT cybersecurity systems in key functional areas."

The historical context of the creation and supervision of the systemic security management of IT/OT systems by the author, along with the idea of establishing the Cybersecurity Information

Publisher: **KOMAG Institute of Mining Technology, Poland**

Exchange and Analysis Center for the mining sector, over the years 2017÷2023, is presented in Figure 1 [3].

The above-mentioned Act of 5/07/2018 on the national cybersecurity system-imposed obligations on operators of essential services [8]:

- systematically assessing the risk of incidents and managing this risk,
- implementation of appropriate technical and organizational measures proportional to the assessed risk, taking into account the latest state of knowledge,
- collecting information about cybersecurity threats and vulnerabilities to information system incidents,
- incydent management,
- applying measures to prevent and limit the impact of incidents on the security of the information system,
- using means of communication enabling correct and safe communication in within the national cybersecurity system.

Taking the above into account, in November 2020, the Company performed a security audit of information systems used to provide the Key Service - mineral extraction. Its aim was to confirm the compliance of the security of the information system used to provide Key Services with the requirements of the Act on the National Cybersecurity System [3].

Publisher: **KOMAG Institute of Mining Technology, Poland**

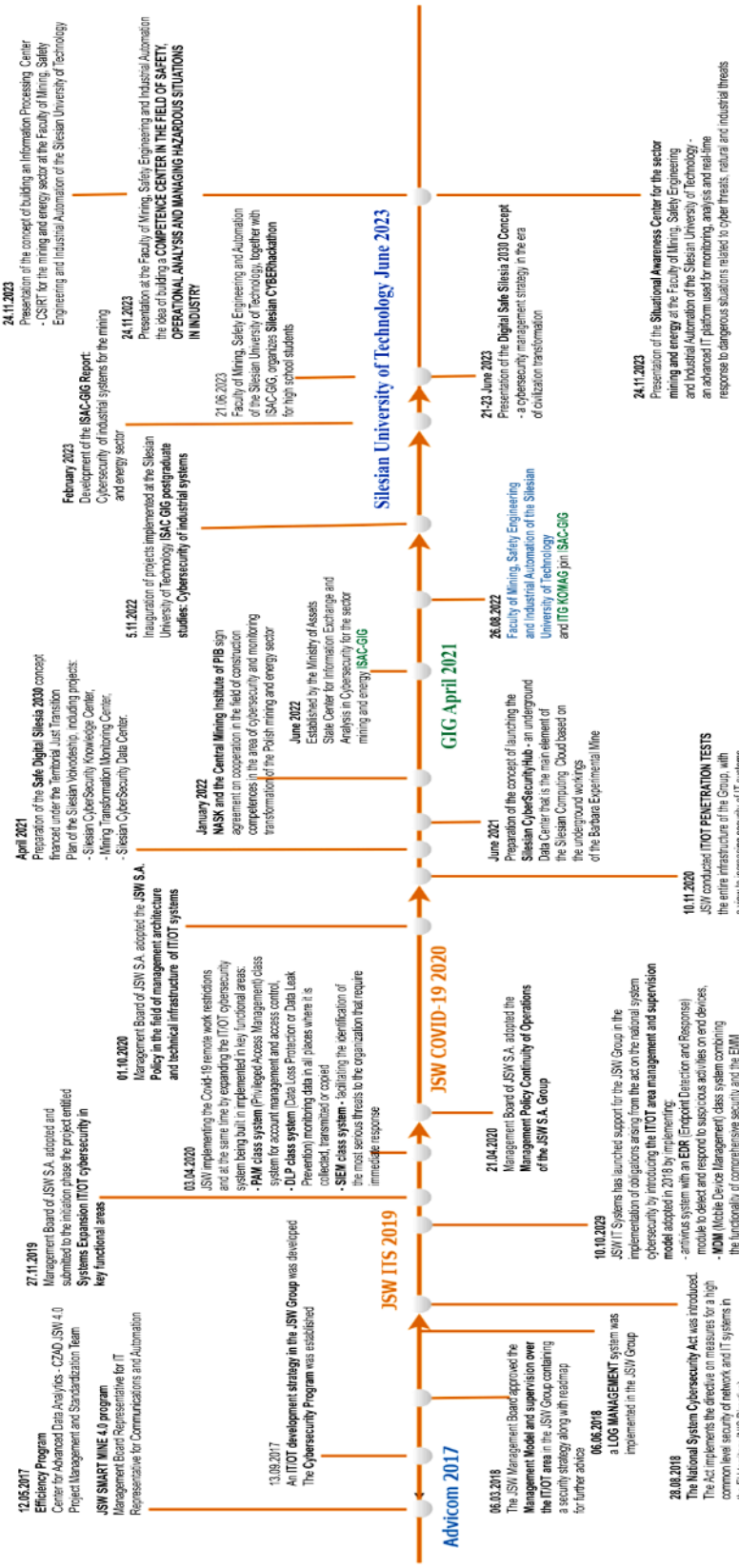


Fig. 1. Historical context of the author's creation and supervision of the systemic security management of IT/OT systems in the JSW Group, along with the development of the idea of establishing the Cybersecurity Information Exchange and Analysis Center for the mining sector, over the years 2017÷2023 [3]

The audit consisted of sampling the implementation of system maintenance processes with the support of external suppliers (including software updates, change management, vulnerability testing, system monitoring, ensuring the continuity of system operation, making backup copies and testing their correctness, controlling access to systems, documenting service activities, etc.). The scope of work included:

- understanding the context of the organization's operation, including the impact of IT and OT Systems (SI_OUK) on Key Services;
- confirmation of the fulfillment of the obligations of the Key Service Operator in accordance with articles 8-16 of the Act on the National Cybersecurity System;
- analysis of documentation regarding cybersecurity of the information system used to provide Key Services;
- tests of the effectiveness of control mechanisms;
- preparation of a report containing a description of identified non-compliances along with recommendations;
- presenting the results of the Audit to the Top Management.

The results of the audit allowed for the issuance of a positive opinion and the identification of a number of recommendations, the most important of which included the implementation of the following tools in the Company:

- PAM class for managing privileged accounts, which allows for effective monitoring of activities carried out using accounts with "super user" rights, e.g. admin, root, accounts with elevated rights in databases, servers, etc. (Fig. 2) [9].

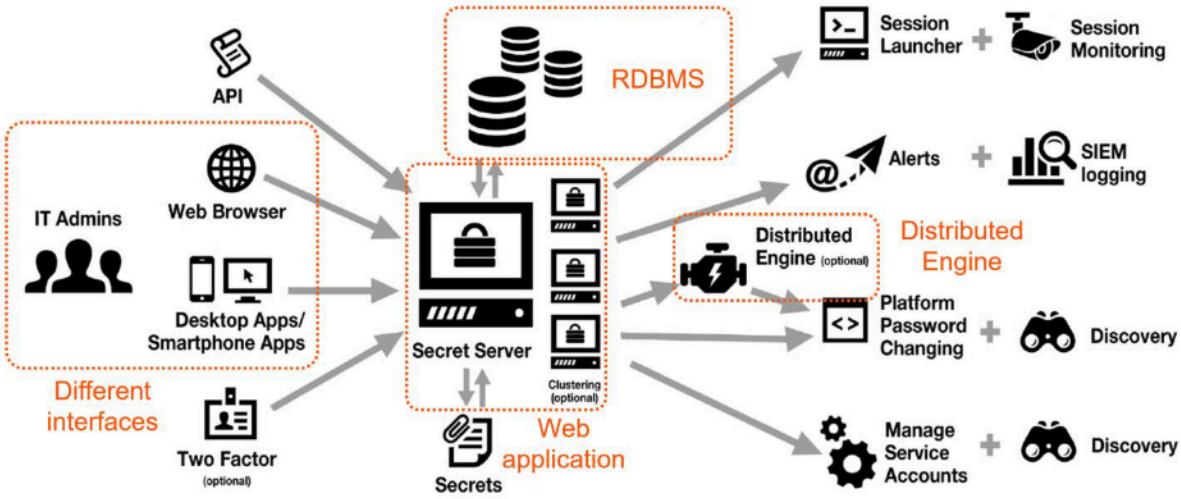


Fig. 2. Sample Privileged Access Management (PAM) System Architecture [9]

- SIEM systems provide comprehensive insight into what is happening on the network in real time and help IT teams actively fight threats. The uniqueness of SIEM solutions lies in the combination of security incident management with information management about the monitored environment (Fig. 3) [10].

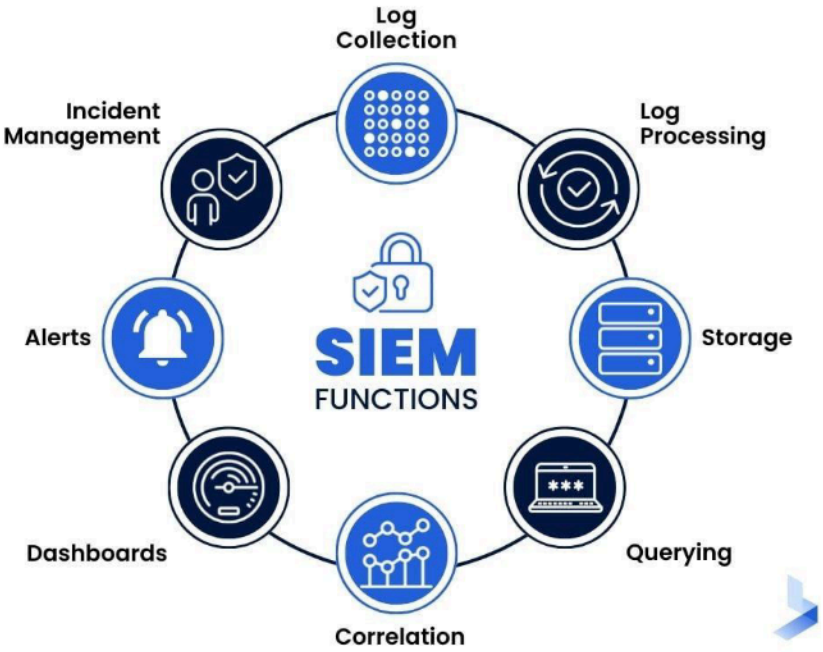


Fig. 3. Features of security information and event management (SIEM) systems, which are platforms that provide insight into the company's IT environment and help detect and respond to threats [10]

The tools used as a result of the implementation of the audit recommendations allowed the Company to provide a level of security adequate to the requirements and risk, ensuring that the protection of processed data is maintained at the highest possible level. They also allowed us to develop an optimal model of cooperation between the Privileged Access Management and Security Information and Event Management systems (Fig. 4 and Fig. 5) [3].

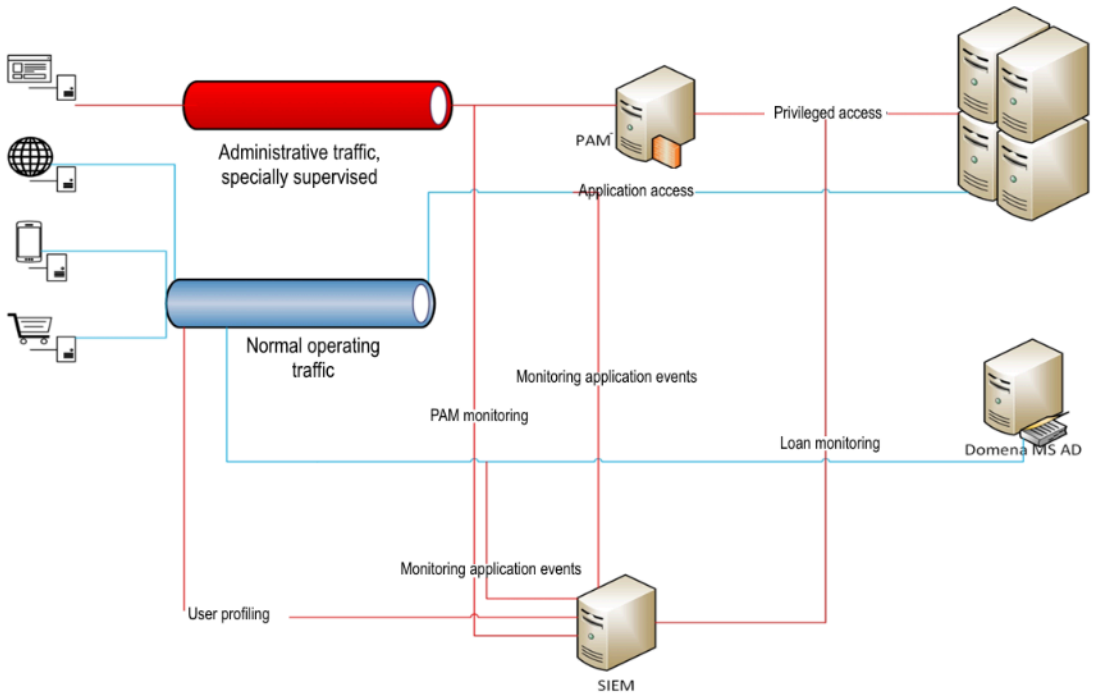


Fig. 4. Model approach for cooperation between SIEM and PAM class systems [3]

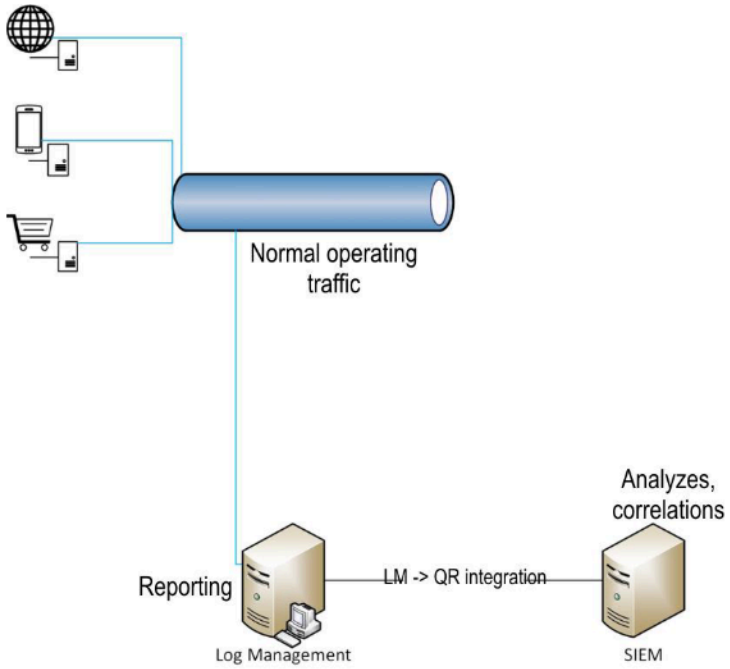


Fig. 5. Log Management SIEM model approach [3]

– DLP class system - monitoring data, searching data patterns, and in the event of an attempt to send or copy documents containing sensitive data (defined by the DLP System Administrator), blocking this action and notifying the administrator about irregularities. It is a tool that was created to tighten the information processing processes in the company. They effectively support business and security departments in understanding how, where and by whom critical data is processed - Fig. 6 [11].

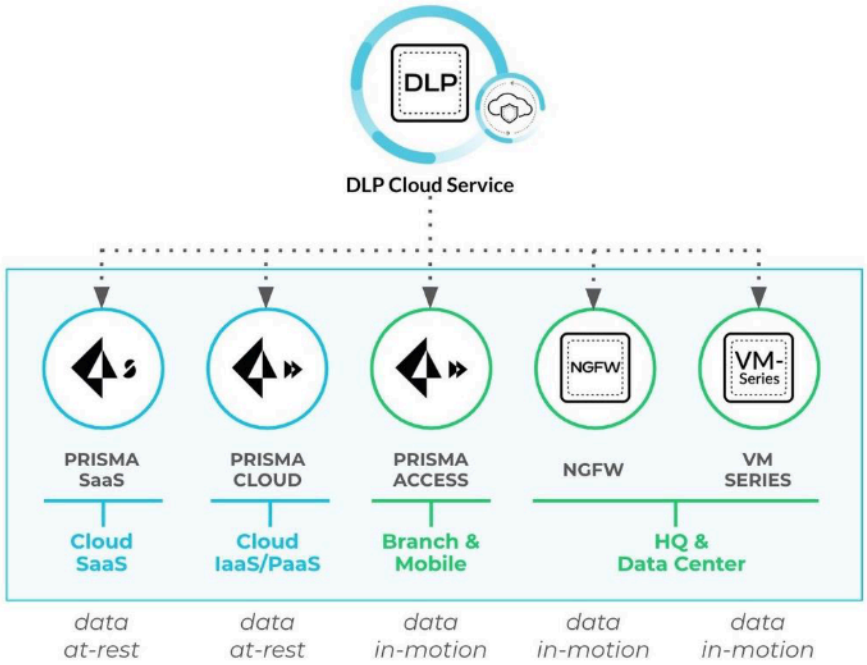


Fig. 6. Sample architecture of the Data Loss class system Protection DLP by Palo Alto Networks [11]

Publisher: **KOMAG Institute of Mining Technology, Poland**

IT/OT cybersecurity system built in the years 2017÷2020 in key functional areas of the JSW Group allowed in 2020 alone to block approximately 900 domains that regularly harass the Company's IT network with phishing attacks, at the same time, the farms of JSW SA anti-spam and anti-phishing systems scanned and rejected approximately 1.3 million messages. Phishing currently accounts for approximately 49% of all cyberattacks and is sometimes difficult for an employee to identify. That is why it is so important to raise awareness and constantly train employees.

The year 2020 will always be associated with the COVID-19 pandemic. The Crisis Team at Jastrzębska Spółka Węglowa, established in March of that year, decided to start remote work for a significant number of employees, which created new challenges for the IT and OT services in the Company, forcing increased protection of the Company's IT infrastructure and blocking numerous attempts to infect workstations. Suffice it to say that in the second half of 2020 alone, JSW SA recorded approximately 8,000. domains showing "Malware behavior" and over 10,000 attempts to inject malicious code into workstations. These attacks were treated very seriously, bearing in mind the experience from December 2019, when the Ostrava-Karviná mines (OKD) were attacked by hackers, as a result of which, for security reasons, the entire OKD Company was interrupted in mining for almost a month. As it turned out, the hackers skillfully infiltrated the OT networks of Czech mines from the office network, using unsecured and infected end-user workstations for this purpose. The experience of the Czech OKD mines had a significant impact on the preparation of Polish mines for face attacks related to the CYBER area. An important activity was to conduct a continuous inventory of resources, IT/OT architecture, identify areas susceptible to threats and appropriate security. An essential element was to conduct cybersecurity training, which allowed a wide group of employees to be aware of the threats on the one hand and, on the other hand, allow us to operate in accordance with the adopted standards and Security Policies [3].

Currently, JSW SA together with JSW IT Systems is conducting a number of projects and implementations of systems that increase safety at work. The foundation of these projects is to increase the level of safety of crews and IT/OT processes and technologies. The cybersecurity strategy developed by JSW IT Systems in 2016÷2020 is based on stopping attacks (prevention), monitoring and determining undesirable events (detection), as well as implementing corrective actions (reaction). This is considered in relation to resources identified in the prism of protection of an extensive maturity model, extending the requirements of ISO 27001. Projects are implemented in cooperation with technological leaders in the field of IT/OT security on the market. The activities carried out strengthen the technical area of prevention by hardening the environment, controlling the tasks performed by employees and limiting the propagation of vulnerabilities in the internal network. In order to properly manage this infrastructure, the JSW SA Automation and IT Office was established at the Company's Headquarters, reporting directly to the President of the Management Board for Technical and Operational Affairs, which included the Automation and Teletransmission Team and the Advanced Data Analytics Team, closely cooperating with JSW IT Systems. This allowed the development and implementation on April 21, 2020 of the "Business Continuity Management Policy of JSW SA" and on October 1, 2020 of the "Policy of Jastrzębska Spółka Węglowa SA regarding the management of the architecture and technical infrastructure of IT/OT systems", including: "Conditions of access to separate networks in JSW SA plants" and "Guidelines for IT/OT solutions for the created Specifications of Essential Procurement Terms at JSW SA".

3. Ensuring business continuity

From the point of view of mining companies, it is critical to maintain business continuity and rebuild service continuity after a failure. Therefore, it is recommended to follow the Recommendations on actions aimed at strengthening cybersecurity in the energy sector and the sectoral guidelines on reporting incidents prepared by the Ministry of Climate and Environment in the field of cybersecurity for the Polish energy sector. Business continuity management is an activity whose aim is, among others, to: ensuring the operation of a given entity by protecting critical, key processes against the effects of incidents in the technological process area, as well as protecting information assets necessary to implement these processes. Business continuity itself can be defined as the ability of an

enterprise to anticipate and respond to business process disruptions in order to maintain its operations at an acceptable, established level. Business continuity management should be a priority for every company. Therefore, it is recommended that the organization develops methodologies for maintaining business continuity, taking into account aspects that, according to the organizational specificity of a given enterprise, may affect this continuity, understood as maintaining key processes enabling the provision of a key service. It is recommended that a business continuity plan be developed for each type of threat that may occur according to the risk analysis, as shown in Figure 7 [12].

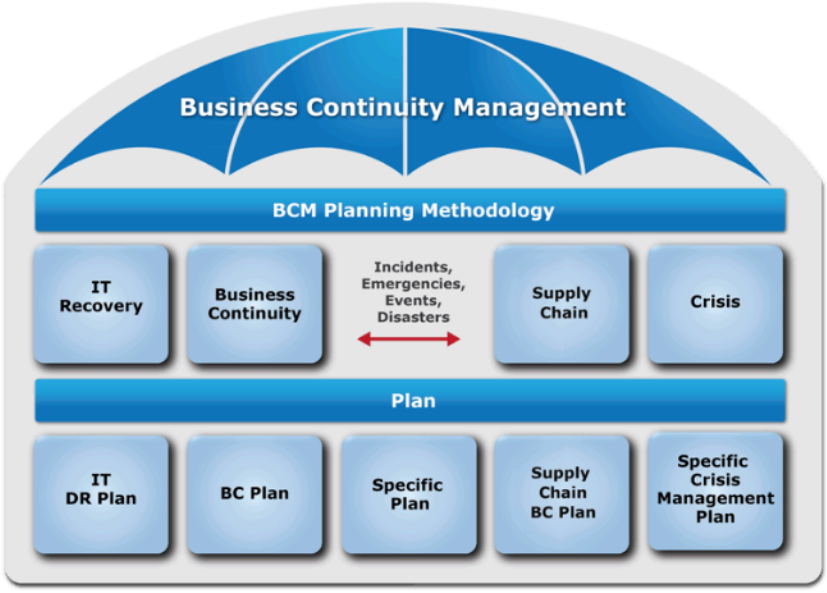


Fig. 7. Methodology for planning and managing business continuity in an enterprise according to the Business Continuity Management Institute [12]

Business continuity management is a holistic management process aimed at identifying the potential effects of threats and developing response plans. The key goal here is to increase the organization's resilience to business disruptions and minimize their effects. The definition of business continuity management includes not only business continuity (BC), but also crisis management (CM), crisis communication (CC), IT disaster recovery planning (DRP) and operational resilience (OR).

In the Jastrzębie mines, the "Business Continuity Management Policy of JSW SA" was adopted on April 21, 2020. It is generally a set of procedures and information developed to assess risk and plan business continuity in the event of any business disruptions and minimize their effects to an acceptable level [13].

The primary goal of business continuity management in the JSW Group is to protect the Company as effectively as possible against the negative consequences of critical events and to enable the restoration of original efficiency in the shortest possible time. By implementing the principles described in the Policy, the Company's Management Board expected to achieve the following goals:

- integration and coherence of contingency plans in the event of catastrophic disruptions in Critical Business Processes,
- ensuring supervision over the effectiveness and adequacy of maintained emergency plans,
- providing policies and tools to support BCP Plan Owners in their development and maintenance.

The policy applies to all issues related to the identification, analysis and development of rules of conduct in the events that have a strong impact on the course of Critical Business Processes. Business continuity management is presented in two perspectives: the efficiency of the Company's Critical Business Processes and the passage of time counted from the occurrence of events that result in a critical drop in this efficiency. The principles of conduct adopted in the Policy enable the

development of effective response plans to the occurrence of an Extraordinary Event. The business continuity management model in the JSW SA Group is presented in Figure 8 [13].

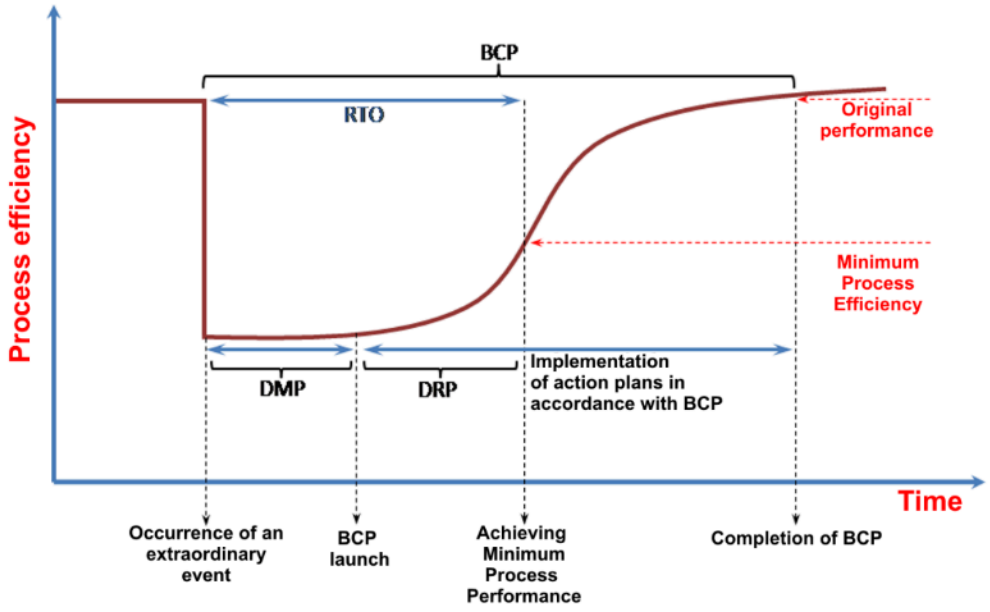


Fig. 8. Procedure diagram and main elements of the business continuity management system in the JSW Group [13]

The occurrence of an event that is considered in the context of loss of business continuity causes a sharp decline in the efficiency of the entire process. In order to be able to restore the lost efficiency in an optimal time, it is necessary to plan actions that will be taken immediately after the occurrence of an Extraordinary Event. The procedure is divided into three stages:

- activities from the moment of occurrence of an Emergency Event to the moment of formal establishment of a business continuity plan (DMP),
- activities undertaken as part of the announced and applicable business continuity plan and leading to the restoration of the minimum expected efficiency of interrupted Critical Business Processes (DRP), or the introduction of a maintenance mode,
- activities undertaken as part of the announced and applicable business continuity plan leading to the restoration of lost performance (BCP).

The first step after an Emergency Event occurs is to take steps to formally announce and implement the BCP. The procedure defined as DMP is described directly in the BCP plan. The essence of DMP is to use the shortest possible communication and decision path so that it is possible to effectively take actions aimed at maintaining Critical Business Processes.

After establishing the BCP, which includes a course of action taking into account assigned roles, rights and responsibilities, the Company begins to operate in an emergency mode. The first actions are aimed at achieving the minimum efficiency of interrupted processes that will enable it to survive, or establishing a maintenance mode. The activities that are performed at this stage are described in the DRP, which is part of the BCP plan. DRP is constructed taking into account the critical time during which the lost efficiency must be partially restored, thus enabling the company to maintain its operations. The time counted from the moment of occurrence of an Extraordinary Event to the moment of achieving minimum survival efficiency is defined as RTO.

After the Company achieves efficiency at a level that guarantees the resumption of Critical Business Processes or the introduction of the maintenance mode, activities related to restoring the state

before the Extraordinary Event are carried out. In special cases, the nature of the disruption or the effectiveness of the solutions used so far justify making changes and restoring the lost functionality by using other methods.

After the loss of efficiency is achieved, the BCP operation is terminated, which is equivalent to the cancellation of the emergency mode. As in the case of introducing the BCP, in accordance with the described DMP procedure, the procedure for its cancellation must result from specific and described rules. The rules for canceling the BCP are described in each of the BCP plans prepared and adopted for use.

In the years 2020÷2023, Polish Ministry of Climate and Environment recommended mining enterprises to develop procedures for dealing with emergency situations, including [3]:

- action plans in the event of a sudden loss of operational capabilities caused by the unavailability of a large number of employees at one time,
- establishing methods of communication between people involved,
- developing procedures for training employees with similar competences and transferring them, if necessary, to provide higher priority services, the aim of which should be to maintain the provision of the key service.
- developing shift work mechanisms, maintaining continuous monitoring of key systems,
- developing mechanisms for notifying key employees in the event of a serious failure or event related to CRP alert levels,
- developing remote work mechanisms, purchasing equipment enabling remote work and delegating employees (who can perform this type of work) to perform it at their place of residence,
- limiting access to the organization's headquarters by third parties, taking into account exceptions, such as people from CSIRT-type teams,
- controlling and monitoring third parties supporting the operation of key systems.

Integral to an organization’s ability to maintain business continuity is the development of Disaster Recovery Plan (DRP). Developing such a plan is the process of formulating a strategy detailing the key actions required to restore IT services within the established recovery goals to be achieved following business interruption due to a disaster.

For the key services provided, dependent on information systems, it is extremely important to include these systems in the post-disaster reconstruction plan. Taking the above into account, the possible threats leading to a disaster in their context include [3]:

- criminal activity/cyber-attack/abuse,
- wiretapping/intercepting the session,
- physical attack,
- accidental damage (accident),
- malfunction/failure,
- interruption in supply (e.g. electricity),
- legal threats,
- natural disasters.

An important recommendation is also to raise awareness of employees in the field of cybersecurity, continuous training and education in the field of service continuity, and above all, OT/IT cybersecurity, with particular emphasis on the layering of security and implemented systems. One of the best means of protecting an organization's assets are employees who are aware of the threats and

the importance of the information processed. An employee who is not fully aware of the consequences, such as disclosing certain information, may inadvertently take actions that negatively impact the organization. The process of periodic awareness and training can be a mean of creating preventive protection against such events. Training for new and existing employees should include at least relevant information on information security within the organization, as well as information specific to a particular job position. It is advisable to organize the training itself in a form that is interesting for the listener, which will not only enable passive acquisition of knowledge in a given area, but will also provide an opportunity for discussion. Additionally, where possible, examples of violations should be provided along with an indication of the consequences that occurred or could occur.

4. Responding to incidents

With the increasing likelihood of incidents and attacks on small and large organizations in the mining and energy sectors, it is essential to prepare the organization's ability to respond to incidents in order to secure the provision of services that are crucial to maintaining critical social or economic activities. Cybersecurity regulations, including: The Act on the National Cybersecurity System enforces the requirement to be able to respond to incidents.

Incident response requires thorough preparation as well as the ability to identify, contain and recover from cyberattacks. There are standards and guidelines for responding to incidents, e.g. ISO 27035:2016, SANS Incident Response in a Security Operation Center and NIST 800-61 Rev. 2 Computer Security Incident Handling Guide. The ISO 27035 standard proposes five phases of the incident management process. These are [3]:

1. Planning and preparation.
2. Detection and reporting.
3. Assessment and decision.
4. Reaction.
5. Drawing conclusions.

NIST Guideline 800-61 Rev. 2, are one of the most detailed publicly available standards that describe in detail the process of responding to IT security incidents. According to the NIST document, there are four main steps in incident response:

1. Preparation.
2. Detection and analysis.
3. Reduction, elimination and recovery.
4. Post-incident actions.

In 2022, the Report "Cybersecurity in mining - 2022" prepared by the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology, ISAC-GIG Information Exchange and Analysis Center for the mining and energy sector proposed the necessary guidelines and supplements to improve cybersecurity conditions in 2023 (Fig. 9) [14].

Fig. 9. Principles influencing the improvement of enterprise cybersecurity conditions developed basing on the experience of the JSW IT Systems Ltd. [14]

Incident response requires a holistic approach to analyzing the situation and mitigating hostile actions taken against organizational assets. Threat analysis helps you realize how important it is to maintain constant dialogue and cooperation between IT and OT departments, cybersecurity and physical security experts, market entities and auditors. Therefore, in order to support active, early warning and rapid response to critical incidents, it is recommended to create a permanent and multidisciplinary task force within the organization, which must be able to select an appropriate strategy to mitigate the effects of incidents in order to minimize the impact on the continuity of key service.

To achieve this goal, the multidisciplinary task force should include:

- operational business line experts who know the consequences of shutting down a system or communication channel,
- IT/OT experts who know the business continuity specifications of the organization's infrastructure and who are in contact with suppliers and other partners during major incidents,
- incident response experts who are responsible for making decisions regarding actions determining the level of severity,
- analysts who can understand attack patterns and malware behavior, who should identify possible countermeasures.

Current practice shows that an incident may be various events, but in order for them to be considered a serious or critical incident, they must meet appropriate conditions. The Polish government regulated the issue of recognizing a given incident as serious by specifying these premises by way of a regulation on the thresholds for recognizing an incident as serious, according to the types of events in individual sectors and subsectors specified in Annex No. 1 to the KSC Act. Based on the thresholds indicated in this document relating to the effects that a given incident may cause, the following are listed [15]:

- the number of users affected by the disruption of the provision of an essential service,
- time of impact of the incident on the key service provided,
- geographical scope of the area affected by the incident, other factors specific to a given subsector, i.e. circumstances such as: death of a person, serious damage to health, other serious damage to the health of more than one-person, financial losses exceeding PLN 250,000. zloty.

Publisher: **KOMAG Institute of Mining Technology, Poland**

The key service operator classifies the incident as serious and then, no later than within 24 hours from its detection, reports its occurrence to the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV. When an incident occurs, the responsibility for appropriately classifying the incident as serious rests with the operator of the essential service. It should appropriately analyze the thresholds contained in the relevant regulation for a given essential service and, on this basis, submit the notification to the appropriate national level CSIRT.

5. Information Sharing and Analysis Center (ISAC) in the mining and energy sector

Information Sharing and Analysis Center (ISAC) are non-profit organizations that provide the opportunity to exchange information about threats in the CYBER area. They enable the exchange of information on threats and vulnerabilities of IT systems and automation between enterprises, research institutes and local government units. This is especially important now that there is an armed conflict so close to our country's borders and the use of IT systems and the Internet in enterprises and offices has significantly increased as a result of the COVID-19 pandemic. It is the greater use of IT in the operation of industrial enterprises that has translated into a very large increase in related risks [3].

In counteracting CYBER threats, the key issue is access to expert knowledge. Therefore, enabling the exchange of experiences between people dealing with cybersecurity in different enterprises is particularly important and valuable, especially today, when there is such a shortage of specialists in this field. Cooperation within ISAC provides this opportunity and enables the education of new specialists, contributing to increasing resistance to all types of threats related to IT and automation systems.

The first Center for the exchange of knowledge and experience regarding cybersecurity incidents (ISAC) was established in the 1990s after the terrorist attacks in New York and Oklahoma City, when President Bill Clinton established the Presidential Commission for Securing Critical Infrastructure. The commission's task was to prepare a report recommending actions to secure American critical infrastructure in the future. In the report, the committee indicated the Internet and ICT systems as one of the greatest threats. The experts primarily recommended strengthening cooperation between government agencies and critical infrastructure operators and sharing information on potential threats. This recommendation was to be implemented through the establishment of the ISAC Center for the exchange of knowledge and experience regarding cybersecurity incidents. The Commission also emphasized the need to invest in research and development of modern technologies. In response to the Commission's recommendations, the first ISAC centers were created, and two years later, in accordance with the presidential recommendation, the obligation to create ISACs in each critical infrastructure sector was passed. The organization bringing together ISAC teams from all sectors in the USA is the National Council of ISACs. Its responsibilities include strengthening cooperation and exchanging cross-sectoral information [3].

There are currently over 20 ISAC organizations in the United States. In Europe, the first ISACs were established in the financial and energy sectors. It is worth emphasizing that European organizations have different specifics than their American counterparts. They were created later, were built on a different cultural basis and are much more focused on government support, not just sector cooperation. This results from the belief deeply rooted in European culture that the state should ensure the security of both the public and private sectors.

European ISACs, compared to their American counterparts, are much more formalized, mainly due to the greater influence of government bodies on their functioning. They focus primarily on building partnership and trust. According to the nomenclature adopted by the European Network and Information Security Agency (ENISA), there are three ISAC models in Europe: national, sectoral and international. Each of these models has its own characteristics and specifics. Currently, there are over 20 ISACs operating in Europe, including: in Spain, Portugal, Poland, the Netherlands, Lithuania, Hungary, Greece, Ireland, France, Estonia, Austria, Belgium. ISAC-GIG is the first center for the exchange of information, experience and knowledge in the field of cybersecurity in the mining and energy sector in Poland and even in Europe.

Publisher: **KOMAG Institute of Mining Technology, Poland**

The rapid development of technologies used in the energy and mining industries has increased the number of dangers that may disrupt its smooth functioning. Effective cooperation, based on mutual trust between the public and private sectors, is necessary to ensure effective protection against new threats.

The idea of building an ISAC Center for the Exchange of Knowledge and Experience regarding cybersecurity incidents for the mining and energy sector appeared for the first time in March 2020 during consultations between the heads of the crisis teams of JSW SA, Artur Dyczko, author of this exempt, and of KGHM Polska Miedź SA, Radosław Stach, vice-president responsible for copper production. Crisis teams were established to prevent, counteract and combat the threat of the SARS-CoV-2 virus. The editor of this monograph, organizing the work of the crisis team, which he then headed until March 2021, appointed as the team member, in addition to the directors of key production plants of the JSW Group, the President of JSW IT SYSTEMS Ltd., providing comprehensive IT services for Jastrzębie mines. It is this fact that led to intensive discussions until June 2020 at the level of the JSW SA and KGHM Polska Miedź SA crisis teams on the necessary procedures to ensure the Business Continuity of the Mining Plants, also requiring the construction of the Knowledge and Experience Exchange Center regarding ISAC cybersecurity incidents [14].

It should be emphasized that the idea of creating ISAC, formulated in March 2020, during the work of the JSW SA Crisis Team for the mining and energy sector was born from the need to exchange knowledge, information, experience, but above all, good practices in securing the Business Continuity of Mining Plants. The past three years have clearly demonstrated the relevance and reasonableness of our idea. Today, no one disputes the thesis that cybersecurity of the entire mining and energy sector depends on the security of individual entities, especially the smallest ones.

Currently, ISACs are becoming an increasingly popular cooperation model because they help improve the competences of operators in key sectors and build trust between the stakeholders of the cybersecurity system. Learning from each other, reducing costs and improving the level of cybersecurity - these are just some of the benefits of launching ISAC. Such knowledge exchange centers are built around various sectors of the economy (e.g. financial, aviation or energy). Their main task is to bring together institutions and enable an exchange of experiences about threats. ISAC is a form of public-private partnership (PPP) that is particularly effective in the area of cybersecurity. Operators of key services are private or public enterprises, and ICT threats rarely concern only one institution or even one sector. Therefore, good cooperation and proper exchange of knowledge can significantly increase the level of cybersecurity. The data collected by ENISA shows that the creation of ISAC significantly contributed to increasing the level of knowledge about threats in a given country and to increasing the competence of companies and institutions in counteracting these threats.

As life has shown, despite several attempts and interventions of the Ministry of Climate, establishing the Knowledge and Experience Exchange Center regarding ISAC cybersecurity incidents by the State Treasury companies themselves was extremely difficult and fraught with the risk of divergent strategic goals - which consequently causes economically strong companies to operate alone, not taking advantage of the opportunities offered by working in a group, generating at the same time the costs of lost development opportunities that could be achieved by using the available resources more effectively. Not being discouraged by these problems, the author of this monograph, after almost a year of objective difficulties, in April 2021, together with several enthusiasts of the topic, proposed the organization of the Knowledge and Experience Exchange Center regarding ISAC cybersecurity incidents for the mining and energy sector at the Central Mining Institute (GIG), where the Institute's management, with great enthusiasm and ingenuity, took to create the necessary formal ISAC structures.

Formally, the agreements between the Central Mining Institute and most representatives of State Treasury companies, playing a key role in the Polish mining sector, were signed in January 2022, while the ceremonial signing of the declaration of launching ISAC-GIG took place on June 3, 2022 at the Ministry of State Assets (Fig. 10) [17].

Publisher: **KOMAG Institute of Mining Technology, Poland**

Fig. 10. Signing of an agreement between the Central Mining Institute and representatives of most State Treasury companies that play a key role in the Polish mining sector. Piotr Toś from JSW SA was appointed as the first Managing Director of ISAC-GIG. – Warsaw June 3, 2022 [17]

The signatories of the agreement on cooperation within ISAC-GIG are currently [17]:

- Central Mining Institute,
- Jastrzębska Spółka Węglowa SA,
- JSW IT Systems Sp. z o. o.,
- KGHM Polska Miedź SA,
- TAURON Polska Energia SA,
- TAURON Wydobycie SA,
- Polska Grupa Górnicza SA,
- Lubelski Węgiel "Bogdanka" SA,
- Węglokoks Kraj SA,
- ITG KOMAG,
- Silesian University of Technology, Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology.

In August 2022, in the presence of the Undersecretary of State at the Ministry of State Assets, Minister Piotr Pyzik, the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology and ITG KOMAG solemnly signed an agreement on joining the Information Exchange and Analysis Center in the field of cybersecurity for the mining and energy sector ISAC - GiG. The accession of ITG KOMAG and the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology to ISAC GIG is the next step after the launch of elite postgraduate studies at the Faculty of Mining, Safety Engineering and Industrial

Publisher: **KOMAG Institute of Mining Technology, Poland**

Automation from October 2022 together with ITG KOMAG entitled: "Cybersecurity of industrial systems" (Fig. 11) [16].

Fig. 11. Accession of the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology and ITG KOMAG to ISAC- GiG – Gliwice, August 2022 [16]

ISAC-GIG is one of the first projects of this type in the country, the first to bring together companies that play a key role in energy security. So far, only two such centers have been launched in Poland, i.e. ISAC-Kolej in the railway sector and the Reputation Center for Electronic Communications (ISAC-UKE) in the telecommunications sector. The idea of creating ISAC-GIG was born from the need to exchange knowledge, information, experience and good practices in the use of IT system security. The aim of ISAC-GIG Center is to, in accordance with the adopted principles, develop and promote standards and recommendations for the mining and energy sector, as well as cooperate in handling security incidents and cyberattacks affecting entities in this sector.

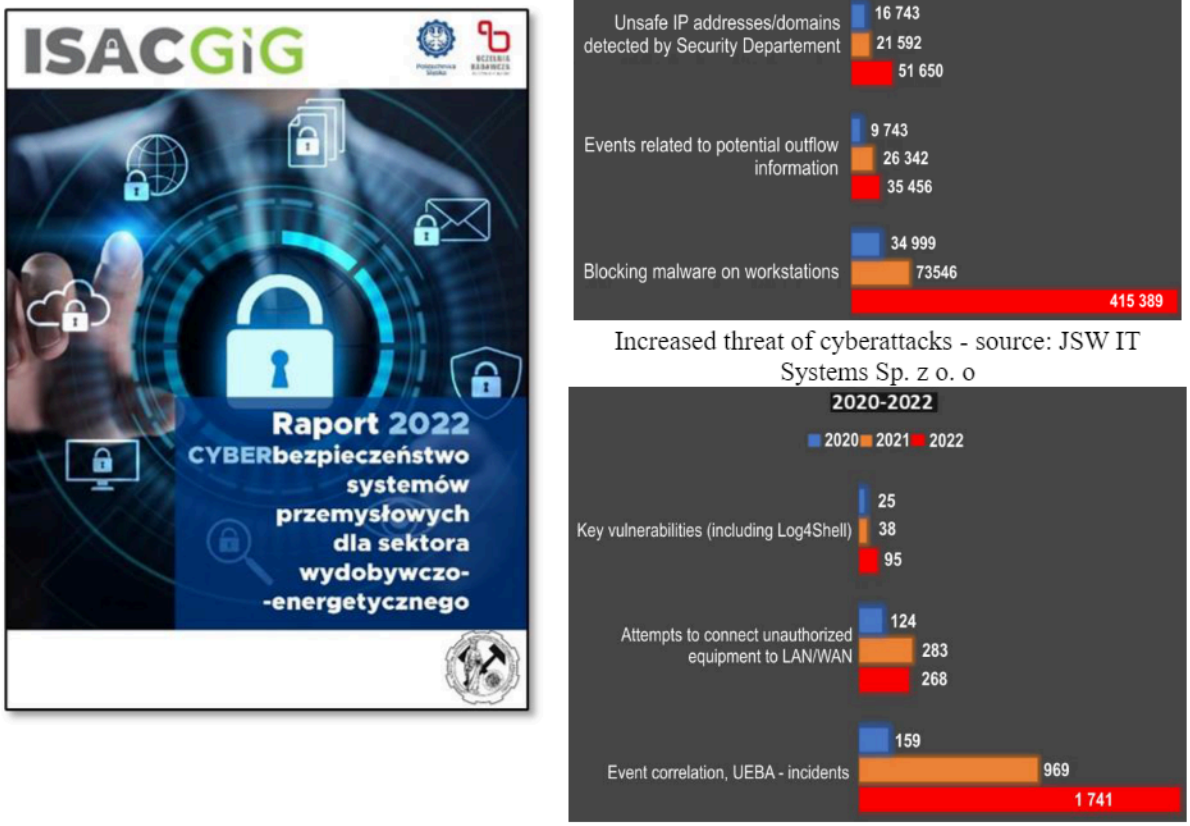
The joint effort of each participant is to constantly analyze and share information about threats and incidents that occur in cyberspace. The main tasks of ISAC-GIG include:

- exchange and analysis of threat data in real time,
- creating reports on security incidents,
- exchange of technical and operational experiences along with the solutions used,
- sharing conclusions and experiences from incidents and threats.

One of ISAC-GIG's cyclical initiatives is the preparation of the Report " Cybersecurity of industrial systems for the mining and energy sector for 2022". This document is an element of the Center's larger strategy related to conducting postgraduate studies entitled " Cybersecurity of industrial systems" at the Silesian University of Technology by the Faculty of Mining, Safety Engineering and Industrial Automation together with the KOMAG Institute of Mining Technology (Fig. 13, Fig. 12) [16].

Publisher: **KOMAG Institute of Mining Technology, Poland**

Fig. 12. The architects of the creation of postgraduate studies entitled: " Cybersecurity of industrial systems" at the Silesian University of Technology, Dean of the Faculty of Mining, Safety Engineering and Industrial Automation, prof. Franciszek Plewa PhD Eng. and the head of ISAC GIG, the CEO of JSW ITS Sp. z o.o. Piotr Toś – Gliwice, October 2022 [16]



Increased threat of cyberattacks - source: JSW IT Systems Sp. z o. o

Fig. 13. Report " Cybersecurity of industrial systems for the mining and energy sector for 2022" [17]

The report (Fig. 13) is ultimately intended to be an important element of ISAC-GIG's activities in the field of promoting and developing cooperation in the area of cybersecurity between science and business, constituting a kind of alliance of innovative projects and research programs, disseminating

Publisher: **KOMAG Institute of Mining Technology, Poland**

their results in order to raise awareness of the management of the entire cybersecurity ecosystem for mining and energy sector [17].

Learning from each other, reducing costs and improving the level of cybersecurity - these are just some of the benefits that come from reading the document, which will allow you to turn the data, observations and recommendations contained therein into actions that can ultimately improve security, among others, by building a new potential and capabilities in the area of the national cybersecurity system. The report, presenting the achieved goals and improvements that have been developed as part of developing a higher level of maturity and resilience of cybersecurity in the mining and energy sector, also includes the effects of the amendment to the KSC Act, as well as proposals for the NIS 2 Directive introducing a number of challenges for entities of the national cybersecurity system in all sectors [15].

6. Silesians CyberSecurity Hub - a new way to build digital awareness and develop cybersecurity competences

As mentioned above, the idea of building the ISAC Center for the Exchange of Knowledge and Experience regarding cybersecurity incidents for the mining and energy sector appeared for the first time in March 2020 during consultations of the heads of the JSW SA and KGHM Polska Miedź SA crisis teams. A little later, in April 2021. As a result of developing this idea, the main assumptions of the strategic research program entitled "Safe Digital Silesia 2030" were developed, an extremely ambitious initiative aimed at ensuring digital security for the inhabitants of Silesia in the era of civilization transformation [3].

The entire concept was based on the assumption that the primary goal of the "Safe Digital Silesia 2030" program will be the construction, in the "Barbara" Experimental Mine in Mikołów, belonging to the Central Mining Institute, of the Center for the Development of Innovative Digital Competencies, whose task in the coming years will be:

- creation of the Center for the Exchange and Analysis of Information on vulnerabilities, threats and incidents to support entities of the national cybersecurity system, currently ISAC GIG,
- development of digital competences, especially in the field of cybersecurity, of local government units, large, small and medium-sized enterprises, construction of a training base in the field of cybersecurity, along with the launch of a program for discovering and training the most talented students of Cybersecurity Talent Identification and Assessment Program - CTIAP
- creating technological security measures ensuring the continuity of operation of industrial IT/OT systems, enabling coordination and active response to incidents in cyberspace, creation of the Regional Transformation Monitoring Center based on obtaining source production and environmental data from mines undergoing the transformation process.

All this so that ISAC GIG, thanks to published reports, analyzes and training, becomes an opinion leader and creator of ecosystems that increase resistance to cyberattacks.

All the author's ideas were strongly confronted with the prose of life, and especially with the financial reality of Polish science, in order to finally discuss the assumptions of the program with the Marshal's Office, which, after familiarizing itself with the proposed concept, included them in the Territorial Plan for the Just Transformation of the Silesian Voivodeship up to 2030, supporting activities aimed at increasing the level of innovation of the economy, developing new competences related to the need to adapt employees in the mining and mining-related industries to ongoing changes, and an effective and socially responsible transformation management system.

The finally prepared projects constituting the "Safe Digital Silesia 2030" research program were incorporated into the Territorial Just Transformation Plan of the Silesian Voivodeship, forming three main pillars (Fig. 14.) [3]:

- Digital competence center – Silesian CyberSecurity Knowledge Center,

– Regional transformation monitoring center – Mining Transformation Monitoring Center,
– Technological security center – Silesian CyberSecurity Data Center.

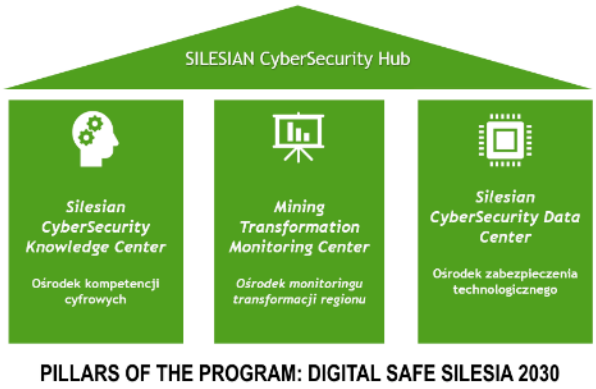


Fig. 14. The idea of transforming the Barbara Experimental Mine into Silesian CyberSecurity Hub [17]

The process of transforming the "Barbara" Experimental Mine, which had conducted normal mining activities in the past, into a modern IT center with a modern data processing center located underground, which will become a good example of the digital transformation not only of Silesia, but of the entire raw materials industry, has already been planned and financed in the National Reconstruction Plan of the Silesian Voivodeship.

The main advantage of locating the Data Center in underground mines is maintaining a high degree of security of stored data in an easier way than when using traditional server rooms. Data center customers demand server reliability and full availability. All IT and support devices located underground are not exposed to bad weather conditions or other random situations, not to mention war.

Internet service providers around the world have been cooperating with underground data processing centers for years. The most energy-efficient server room in Europe is located in Lefdal, Norway. It is located 150 m underground, in the workings of a former olivine mine, and has been operating since 2017 (Fig. 15) [18].

Fig. 15. The most energy-efficient server room in Europe located in the Norwegian Lefdal olivine mine 150 m underground [18]

In the American city of Springfield, Missouri, in an old underground limestone mine, approximately 25 m underground, a data processing center with an area of over 7 500 m^2 was located. Similar underground server rooms operate in Pennsylvania and Kansas City. The Kansas City center is located 34 m below the surface and the Pennsylvania center is located 70 m below the ground (Figure 16) [10].

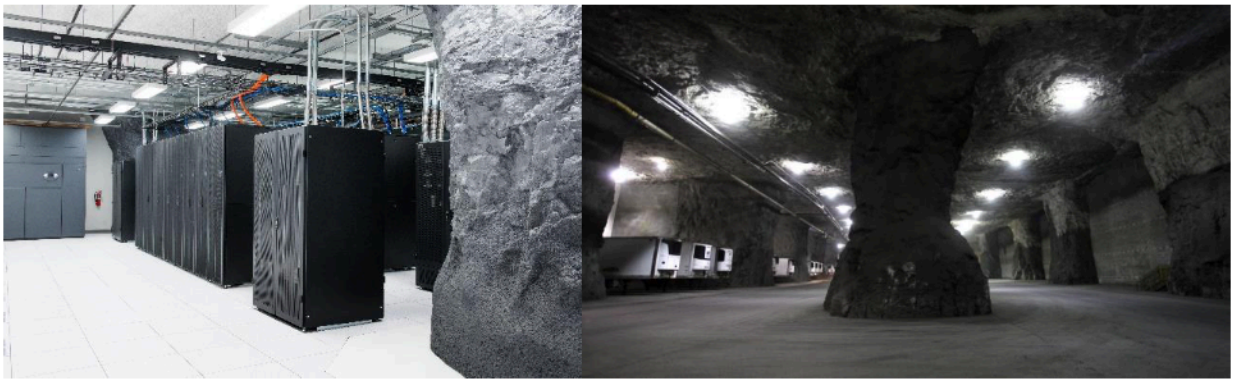


Fig. 16. Data processing center in the American Springfield, Missouri in an old underground limestone mine - DATA CENTER COMPANY EXPANDS UNDERGROUND IN MISSOURI [10]

Data Center KD Barbara, through the use of existing underground workings, will help reduce the costs of data processing center operators, as it will not be necessary to build an entire server room building or rent expensive space. There will also be no huge costs associated with cooling the devices, because there is no sunlight underground and the temperature and air humidity are constant there.

According to the author of this chapter of the monograph, who is one of the creators of the concept of "Safe Digital Silesia 2030", Silesian CyberSecurity Hub can not only be an element of the Silesian Computing Cloud built, among others, based on the KD "Barbara" Data Center, but ultimately it should become an important element of the Government Computing Cloud in the area of monitoring the transformation of the national mining and energy sector [17].

Fig. 17. A modern IT center in the "Barbara" Experimental Mine [17]

As the reality around us shows, the "Safe Digital Silesia 2030" program prepared in April 2021 has not lost any of its attractiveness and relevance, and the war in Ukraine only confirmed the validity of the theses formulated by the authors a year before its outbreak, giving them additional meaning.

Publisher: **KOMAG Institute of Mining Technology, Poland**

7. Conclusion

The past is in our heads and the future is in our hands - as folk wisdom says, the truth of these words was clearly confirmed by the past year 2022. This was the first year of operation of the Information Exchange and Analysis Center for the mining and energy sector (ISAC GIG).

ISAC GIG works actively, integrating the entire environment of the Polish raw materials sector to raise awareness and digital responsibility, which is the foundation of the new face of the mining and energy industry in our country.

The writer of these words is particularly pleased that currently Silesian CyberSecurity Hub is not only GIG and the idea of building a Center for the Development of Innovative Digital Competencies in the "Barbara" Experimental Mine with the only modern server room in Poland located in underground mines. Today, after a year of operation, ISAC GIG, Silesian CyberSecurity Hub is primarily an ALLIANCE between the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology, the Central Mining Institute and the KOMAG Institute of Mining Technology for the benefit of State Treasury companies playing a key role in the Polish mining and energy sector.

Today Silesian CyberSecurity Hub is also, and perhaps above all, an agreement between the worlds of science and industry - an industry that is exceptionally important for the security of our country's functioning - to permanently secure an elementary node of concentration of the main data streams of our critical infrastructure in many fields. As Piotr Toś, Chairman of the Management Committee of the Information Exchange and Analysis Center ISAC-GIG, said: *"... today Silesian CyberSecurity Hub is working to create a training base to support all existing and emerging new ISACs throughout Poland. We have experience and great achievements in building efficiently operating Information Exchange and Analysis Centers in the field of cybersecurity, we want to become an important element of the Government Computing Cloud in the area of monitoring the transformation of the Polish energy industry, we want to launch, together with the Silesian University of Technology, a program for searching and training the most talented students Cybersecurity Talent Identification and Assessment Program - CTIAP, we want, together with the KOMAG Institute, to build a fast certification path in the field of cybersecurity of IT/OT products that will be recognized in Europe. I believe that our cooperation in Silesia will bring a new quality. There is no doubt that we play as one team, and our team is not a group of people who just work together! Our team is a group of people who trust each other in the context of science, new and innovative ideas, research projects and initiatives that are aimed at developing and modernizing the Polish scientific sector...* " [16].

THE ALLIANCE of the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology, the Central Mining Institute and the KOMAG Institute of Mining Technology breathed life into the idea of building Silesian CyberSecurity Hub! Through organized postgraduate studies, training and information exchange, as well as ensuring an appropriate response to emerging threats, it has made it possible to build and develop new competences in the field of cybersecurity for State Treasury Companies, Local Government Units and other participants of the National Cybersecurity System.

This alliance also focused the efforts of the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology around the idea proposed by the Author to launch six laboratories at the Faculty by 2025, constituting a COMPETENCE CENTER IN THE FIELD OF SAFETY, OPERATIONAL ANALYTICS AND MANAGING HAZARDOUS SITUATIONS IN INDUSTRY [16].

The Alliance for building a DIGITAL ECONOMY as a factor in the technological development of the mineral resources sector and a fair energy transformation of Silesia was established on December 11, 2023 in Gliwice.

The Silesian University of Technology and the Mineral and Energy Economy Research Institute of the Polish Academy of Sciences from Krakow have concluded an agreement on cooperation in the

Publisher: **KOMAG Institute of Mining Technology, Poland**

implementation of research programs, project initiatives and commissioned works aimed at improving innovation, technical and economic efficiency of the mineral resources management in Europe.

The agreement was solemnly signed by the Silesian University of Technology - Vice-Rector for Science and Development, prof. Eng. Marek Pawełczyk PhD, and on the part of the Mineral and Energy Economy Research Institute of the Polish Academy of Sciences - Prof. eng. Krzysztof Galos PhD, Director of the Institute (Fig. 18) [16].

Fig. 18. Signing an agreement on cooperation between the Silesian University of Technology and the Mineral and Energy Economy Research Institute of the Polish Academy of Sciences in Krakow by the Vice-Rector for Science and Development, prof. Eng. Marek Pawełczyk PhD and prof. Eng. Krzysztof Galos PhD, Director of the Institute [16]

The CENTER, based on the latest achievements in automation and IT using artificial intelligence, will enable simulation of industrial and technological processes and crisis situations, as well as connecting distributed monitoring, control and security systems responsible for the operation of the enterprise (Fig. 18) [16].

Fig.19. The construction of the CENTER will be managed by the Dean, prof. Eng Franciszek Plewa PhD and Dr. Eng. Artur Dyczko [16]

Publisher: **KOMAG Institute of Mining Technology, Poland**

AI, OPERATIONAL ANALYTICS AND INFORMATION PROCESSING Laboratory - will constitute the heart of the CENTER being built, serving as a research ground for ensuring the security and cybersecurity of industrial automation systems in the mining and energy sector. This will fill the gap in testing the cyber resistance of automation systems and devices used in industry. A complement to the activities presented by the Author, originator and initiator of activities aimed at involving the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology around the idea of: Digital Economy as a Factor in the Technological Development of the Mineral Sector, will be the creation of a SITUATIONAL AWARENESS SYSTEM - constituting, as it were, the brain of the CENTER being built. The situational awareness system for industry is an advanced platform for real-time monitoring, analysis and response in an industrial environment. The main assumptions of this system include, among others, the integration of data from various sources, such as sensors, monitoring systems, databases and measuring devices, which will allow to obtain a comprehensive picture of the situation. This knowledge provides the opportunity to counteract and respond appropriately to emergency situations [16].

The author of this chapter of the monograph believes that the COMPETENCE CENTER IN THE FIELD OF SAFETY, OPERATIONAL ANALYTICS AND MANAGEMENT OF HAZARDOUS SITUATIONS IN INDUSTRIES being built at the Faculty of Mining, Safety Engineering and Industrial Automation of the Silesian University of Technology will be an excellent development and complement to the Silesian concept of CyberSecurity Hub, at the same time becoming a new quality on a European scale in the field of research and training, using simulation and virtualization in laboratory conditions of dangerous situations related to cyber threats, natural and industrial threats.

References

[1] [Online:] https://www.gov.pl Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 w zakresie opracowania i wdrożenia Narodowych Standardów Cyberbezpieczeństwa [dostęp: 21.03.2024].

[2] Dyczko A., 2023: Production management system in a modern coal and coke company based on the demand and quality of the exploited raw material in the aspect of building a service-oriented architecture. Journal of Sustainable Mining: Vol. 22: Iss. 1, Article 1. https://doi.org/10.46873/2300-3960.1371.

[3] Dyczko A., 2023: Automatyzacja i monitorowanie procesu produkcyjnego w kopalniach podziemnych – polskie doświadczenia we wdrażaniu paradygmatu PRZEMYSŁU 4.0" Monografia. Wyd. Instytut Techniki Górniczej KOMAG, ul. Pszczyńska 37, 44-101 Gliwice ISBN 978-83-65593-30-6. https://doi.org/10.32056/KOMAG/Monograph2023

[4] Dyczko A. 2021: Construction of a heuristic architecture of a production line management system in the JSW SA Mining Group in the context of output stabilization, quality improvement and the maximization of economic effects. Mineral Resources Management 37(4), 219–238. Kraków, Poland. DOI: 10.24425/gsm.2021.139746.

[5] Kicki J., Dyczko A. 2010: The concept of automation and monitoring of the production process in an underground mine. Publisher: Taylor & Francis Group, London. Journal: New Techniques and Technologies in Mining-Proceedings of the School of Underground Mining, R. Dychkovskyy (eds.), Volume R. 72, Issue nr 8, str.245-253 London 2010. ISBN 978-0-415-59864-4.

[6] Ozon D. i Dyczko A., 2019 – Strategia IT/OT w GK JSW – NOWE WYZWANIA. Materiały konferencyjne International Mining forum 2019: Safety and efficiency of exploitation against the challenges of industry 4.0.

[7] EMC. (Ustawa EMC). Dyrektywa 2014/30/UE Parlamentu Europejskiego i Rady z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej (wersja przekształcona). Dz. Urz. UE z 29.03.2014 (L96) USTAWA z dnia 13 kwietnia 2007 r. o kompatybilności elektromagnetycznej. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 lutego 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy o kompatybilności elektromagnetycznej. Dz.U. 2018 poz. 397.

[8] Ozon D., Dyczko A., 2017: W kierunku inteligentnej kopani przyszłości – JSW 4.0. Materiały konferencyjne XXXI Konferencji z cyklu: Zagadnienia Surowców Energetycznych i Energii w Gospodarce Krajowej. Instytut Gospodarki Surowcami Mineralnymi i Energią PAN, Zakopane 15-18 października 2017.

[9] [Online:] IBM Redbooks, 2021, Privileged Access Management for Secure Storage Administration. https://www.redbooks.ibm.com/redpapers/pdfs/redp5625.pdf [Dostęp: 23.03.2023].

[10] [Online:] SIEM, https://www.bitlyft.com/security-information-and-event-management [Dostęp: 27.07.2023].

[11] [Online:] Palo Alto Networks, 2020. https://www.paloaltonetworks.com [Dostęp: 27.03.2024].

[12] [Online:] BCM Institute Courses, https://blog.bcm-institute.org/bcm/what-exactly-is-business-continuity-management [Dostęp: 27.03.2024].

[13] Hereźniak W., Dyczko A. 2020: Działania podejmowane w celu ograniczenia rozprzestrzeniania się zakażenia wirusem SARS-COV-2 w Jastrzębskiej Spółce Węglowej S.A., [w:] Monografia: Zagrożenie wirusem SARS-CoV-2 w kopalniach podziemnych – wybrane zagadnienia. GIG, 2020.

[14] [Online:] ISAC-GIG https://isac.gig.eu/plan-cyberpoligonu-oraz-konferencji-cyfrowy-bezpieczny-slask-2030-strategia-zarzadzania-cyberbezpieczenstwem-w-dobie-transformacji-cywilizacyjnej [Dostęp: 27.03.2024].

[15] [Online:] KSC, 2018. Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa. Dz. U. 2018 poz. 1560 z późniejszymi zmianami.

[16] [Online:] https://www.polsl.pl/rg/centrum-kompetencji [dostęp: 21.03.2024].

[17] [Online:] ISAC-GIG https://isac.gig.eu/biuletyn-cyberbezpieczenstwo-isac-gig-cenna-lektura-dla-bezpieczenstwa [Dostęp: 27.03.2024].

[18] [Online:] Centrum Przetwarzania Danych Lefdal https://www.lefdalmine.com [dostęp: 21.03.2024].

Publisher: **KOMAG Institute of Mining Technology, Poland**