SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 204

SECURITY MANAGEMENT OF GEOINFORMATIC SYSTEMS – CASE STUDY

Anna BLUSZCZ[1]*, Anna MANOWSKA[2], Martin BOROŠ[3], Katarzyna TOBÓR-OSADNIK[4]

[1] Department of Safety Engineering, Silesian University of Technology; anna.bluszcz@polsl.pl,
ORCID: 0000-0001-9724-5706
[2] Department of Automatics and Industrial Informatics, Silesian University of Technology;
anna.manowska@polsl.pl, ORCID: 0000-0001-9300-215X
[3] University of Žilina, Faculty of Security Engineering, Department of Security Management, Žilina, Slovakia;
martin.boros@uniza.sk, ORCID: 0000-0003-0705-0556
[4] Department of Safety Engineering, Silesian University of Technology; katarzyna.tobot-osadnik@polsl.pl,
ORCID: 0000-0003-4568-3485
* Correspondence author

Purpose: The aim of this article is to identify methods for securing data developed in geo-information systems and published on websites where data is stored in the cloud.

Design/methodology/approach: The study used GIS tools to identify the level of selected natural hazards. The PHA method was then used to determine the magnitude of the emergency risk. The functionality of GibHub for secure cloud storage was then analysed.

Findings: The result of the analysis presents a selected IT tool for geodata cybersecurity.

Practical implications: The article presents the most important functionalities of the QGIS software, such as the process of generating web maps. It has been shown that IT tools are currently an integral part of critical infrastructure management processes. The most important issue of publishing confidential information is ensuring an appropriate level of security of IT systems. These aspects were also presented extensively in the work in the form of strongly developing tools based on biometric authentication.

Originality/value: The article is a valuable material both for theoreticians in the field of security engineering and computer science, as well as for practitioners who come into contact with the issues of geoinformatics tools and cybersecurity in their daily work. The article is addressed to people dealing with the area of knowledge related to crisis management, IT and cybersecurity.

Keywords: critical infrastructure, cybersecurity, crisis management, IT tools.

Category of the paper: research paper**.**

http://dx.doi.org/10.29119/1641-3466.2024.204.1

1. Introduction

The instability of national security due to the dynamic geopolitical situation poses a number of challenges for crisis management in European countries (Bluszcz et al., 2023). Stable economic development of European countries is possible if, among other things, it is ensured:

- national security (Van Damme, 2022), which is based on securing critical infrastructure, including networks communication, energy networks (Xiao et al., 2019) or transport systems and many others,
- cybersecurity to protect critical infrastructure against cyber-attacks, which is crucial as such attacks can disrupt services and threaten national security (Mead, 2022),
- economic stability (Levytska, 2023), which can only function when financial institutions and markets operate on a safe and reliable infrastructure for transactions, trade and banking services (Zwiech, 2024; Bluszcz, 2017),
- stability in the trade area, where infrastructure such as ports (Żywucka-Kozłowska, Broniecka, 2024), railways and highways support the flow of goods and services, facilitating domestic and international trade,
- the sustainability of public health and safety (Gourevitch et al., 2022), where health care systems such as hospitals, emergency and pharmaceutical services,
- and supply chains, as well as reliable water supply and waste management systems (Tzanakakis et al., 2020), depend on resilient infrastructure to provide health care and protect health public.

All these aspects of society are exposed to dynamic and unpredictable crisis situations. These include, for example, dynamic weather changes, snow storms, floods, tornadoes or pandemics, population migrations (Bluszcz et al., 2023) or cyberattacks (Manowska et al., 2024). All such unpredictable events create crisis situations, causing chaos in the functioning of many sectors of the economy and having drastic consequences for the population and the economy. Crisis situations often cannot be completely eliminated. The only way is preventive action, which can be prepared in many areas at the same time in order to minimize losses for society.

Geographical information systems (GIS) play a key role in emergency management, providing essential spatial data that improves decision-making and resource allocation in emergencies. GIS record and analyse geographic data, enabling authorities to understand the spatial dynamics of crises, such as natural disasters or public health threats (Greenough, Nelson, 2024).

Using GIS tools makes it easier to manage critical infrastructures, such as transport and utilities, by providing real-time data to aid response (Alhaj, Abdalla, 2022). Using GIS data, stakeholders can develop early warning systems and standardised protocols for better preparedness for adverse events (Boumahdi et al., 2020).

While GIS offers significant benefits in emergency management, challenges such as data integration and privacy issues remain. Addressing these issues is essential to maximise the effectiveness of GIS in future emergency scenarios.

The aim of this article is to identify methods for securing data developed in geo-information systems and published on websites where data is stored in the cloud. The process of achieving the objective was carried out in successive stages. First, the use of geoinformatics tools such as QGIS was presented to identify examples of critical infrastructure objects in Poland. In the next stage, the methodology of risk analysis for the selected type of threat for the surveyed objects was presented. In the next step, a method was presented whereby, with the help of a web map plugin, it is possible to generate files representing input data to a website containing compiled critical infrastructure data together with a risk assessment. In order to publish such maps, it is common to use, among other things, repositories in the Git Hub service, which allow multiple users to access such elaborated data in QGIS. In the Git Hub service, the data is stored in the cloud. Due to this fact, publishing confidential data in particular requires the use of selected database security measures.

Security is based on methods that combine encryption, access control and data integrity measures. Encryption techniques include:

- Hybrid cryptography: combining AES with code-based cryptography, such as the McEliece cryptosystem, increases security against quantum threats while providing efficient data encryption (Peng et al., 2023).
- Advanced encryption protocols: The use of hyperchaotic encryption and hash functions can greatly enhance the confidentiality and integrity of data, making it resistant to various attacks (Jain, Singhal, 2024).

Access control and authentication is achieved through:

- Precise access control: Techniques such as identity-based and attribute-based encryption enable secure data sharing, ensuring that only authorised users have access to sensitive information (Mishra, Verma, 2020).
- User authentication: The implementation of robust authentication protocols is crucial to verify legitimate users before granting access to data stored in the cloud (Zargar et al., 2021).

At the same time, data integrity and auditing are important:

- Integrity protocols: Digital signatures and hash functions facilitate data authentication, allowing users to verify the integrity of their data (Mahida, 2024).
- Auditing mechanisms: Third-party auditing allows data owners to periodically check the integrity of their data without having to download it altogether (Garg et al., 2020).

While these strategies greatly enhance the security of data in the cloud, challenges remain, especially when it comes to balancing usability and security. As cloud environments evolve, security measures will need to be continually adapted to counter emerging threats.

The article describes the importance of the critical infrastructure identification process for the risk classification process for individual systems in relation to various threats. Then, the IT tools used were indicated, as well as selected IT tools to protect confidential data.

2. Critical infrastructure review

Critical infrastructures (CI) are the real and cyber systems (facilities, equipment or installations) necessary for the minimum functioning of the economy and the state (Petersen, 2020).

There is a variety of critical infrastructure. The article presents selected critical infrastructure facilities in Poland, which include, among others:

- Energy Sector: Bełchatów Power Station: One of the largest thermal power plants in Europe, crucial for Poland’s electricity supply, Polskie Sieci Elektroenergetyczne (PSE): The national electricity transmission system operator, Gdańsk Refinery: Operated by Grupa Lotos, a key refinery for petroleum products, LNG Terminal in Świnoujście: Vital for natural gas imports and energy security.
- Water Supply and Management: Włocławek Dam: Important for water management, hydroelectric power, and flood control on the Vistula River, Warsaw Waterworks: Ensuring the water supply for the capital city and its metropolitan area.
- Transportation: Frederic Chopin Airport (Warsaw): The largest and busiest airport in Poland, a key hub for international and domestic flights, Port of Gdańsk: One of the largest seaports in the Baltic Sea region, critical for trade and transportation, A4 Motorway: A major east-west highway connecting the German border to Ukraine, facilitating transportation and logistics.
- PKP Intercity: National railway operator providing long-distance passenger rail services.

Due to the fundamental importance of critical infrastructure for the stable economic functioning of European countries, all measures are necessary to protect identified critical infrastructure facilities (Chowdhury, Gkioulos, 2021).

Critical Infrastructure Protection (CIP) involves the measures and strategies necessary to safeguard essential systems, assets, and networks from threats and ensure their resilience and reliability (Yigit, 2024). Here's a detailed overview of CIP:

- Identification and Prioritization.
    - Asset Identification: Determine which assets are critical to national security, public health and safety, economic stability, and public confidence.
    - Risk Assessment: Evaluate the risks to these assets from natural disasters, cyber-attacks, terrorism, and other threats.
    - Prioritization: Rank critical assets based on their importance and the severity of potential impacts from their disruption.
- Risk Management.
    - Threat Analysis: Continuously monitor and analyze potential threats to infrastructure.
    - Vulnerability Assessment: Identify weaknesses that could be exploited by these threats.
    - Mitigation Strategies: Develop and implement strategies to reduce vulnerabilities and manage risks.
- Security Measures.
    - Physical Security: Install barriers, surveillance systems, access controls, and other physical security measures to protect critical infrastructure.
    - Cybersecurity: Deploy firewalls, intrusion detection systems, encryption, and other cybersecurity tools to protect against cyber threats.
    - Personnel Security: Conduct background checks, training, and other measures to ensure that employees do not pose a security risk.
- Resilience and Recovery.
    - Continuity Planning: Develop and maintain business continuity and disaster recovery plans to ensure that critical services can be maintained or quickly restored after a disruption.
    - Redundancy: Implement redundant systems and networks to provide backup in case of failure.
    - Response and Recovery: Establish protocols for rapid response and recovery efforts following an incident.
- Information Sharing.
    - Public-Private Partnerships: Foster collaboration between government agencies and private sector stakeholders to share information and resources.
    - Intelligence Sharing: Share threat intelligence and best practices among different sectors and organizations.
    - Public Awareness: Educate the public about the importance of critical infrastructure and ways to contribute to its protection.

- Policy and Regulation.
  - Legislation: Enact laws and regulations to mandate the protection of critical infrastructure and establish standards.
  - Compliance and Enforcement: Ensure compliance with regulations through inspections, audits, and penalties for non-compliance.
  - Funding and Incentives: Provide funding and incentives for infrastructure protection initiatives.

3. Results

3.1. Identification selected objects of critical infrastructure in Poland using QGIS

Identification of critical infrastructure facilities is possible using many different IT programs. The study used the available free version of the QGIS program, which is an excellent geoinformatics tool (Flenniken, 2022). The article presents layer views in which exemplary critical infrastructure facilities in Poland were identified. It should be noted that this is the first stage of preventive measures to protect critical infrastructure.

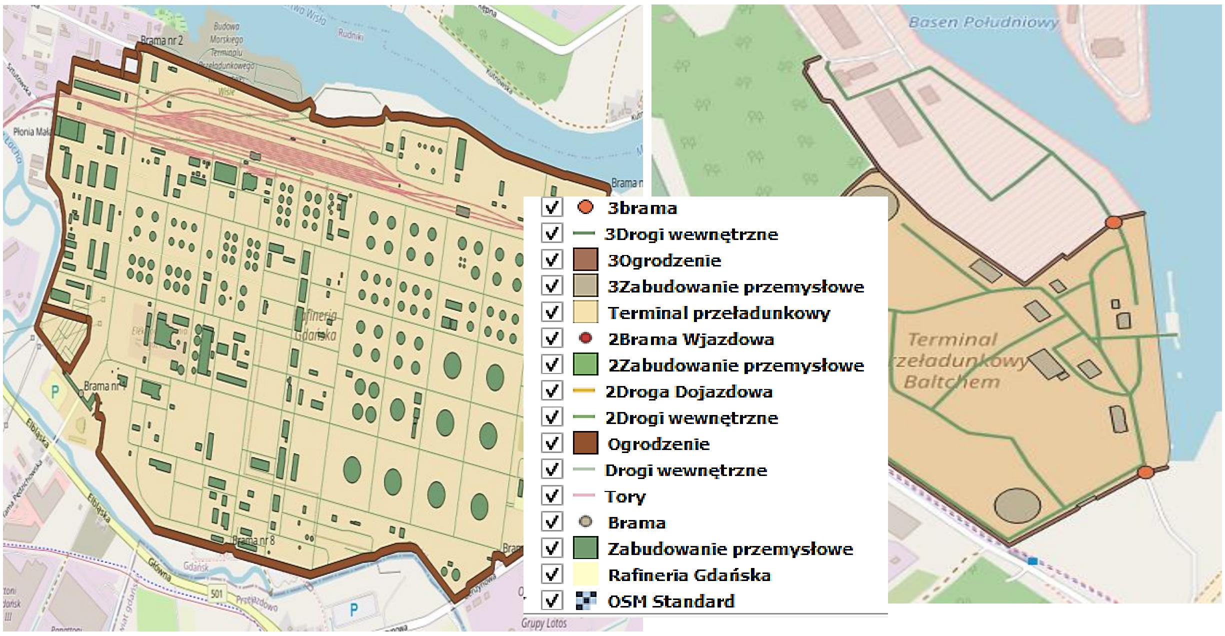


Figure 1. Energy critical infrastructure in Poland: Gdańsk Rafinery and the Baltchem Transhipment terminal.

Source: own elaboration using QGIS program.

Refineries, such as the one in Gdańsk are crucial for processing crude oil into valuable products like gasoline and diesel. They contribute to energy security, economic stability, and job creation in strategic locations. The significance of a refinery lies in its impact on the local and international supply chain, logistical efficiency, and its role in a country's critical energy infrastructure. Advanced technologies and environmentally friendly practices in refineries can also drive innovation and sustainability in the industry. For the latest information on the importance of the Gdańsk refinery, it is recommended to check recent and reliable sources. Second examples of energy critical infrastructures in Poland is the Baltchem Transhipment Terminal which holds significance for several reasons. Firstly, strategically located in a key port, it facilitates efficient transshipment of goods, enhancing regional and international trade. Secondly, the terminal's handling capacity contributes to the smooth flow of bulk commodities, including chemicals, fostering economic growth. Thirdly, its advanced infrastructure and equipment promote operational efficiency, reducing turnaround times for vessels. Additionally, the terminal's adherence to environmental standards and safety protocols ensures responsible handling of goods.

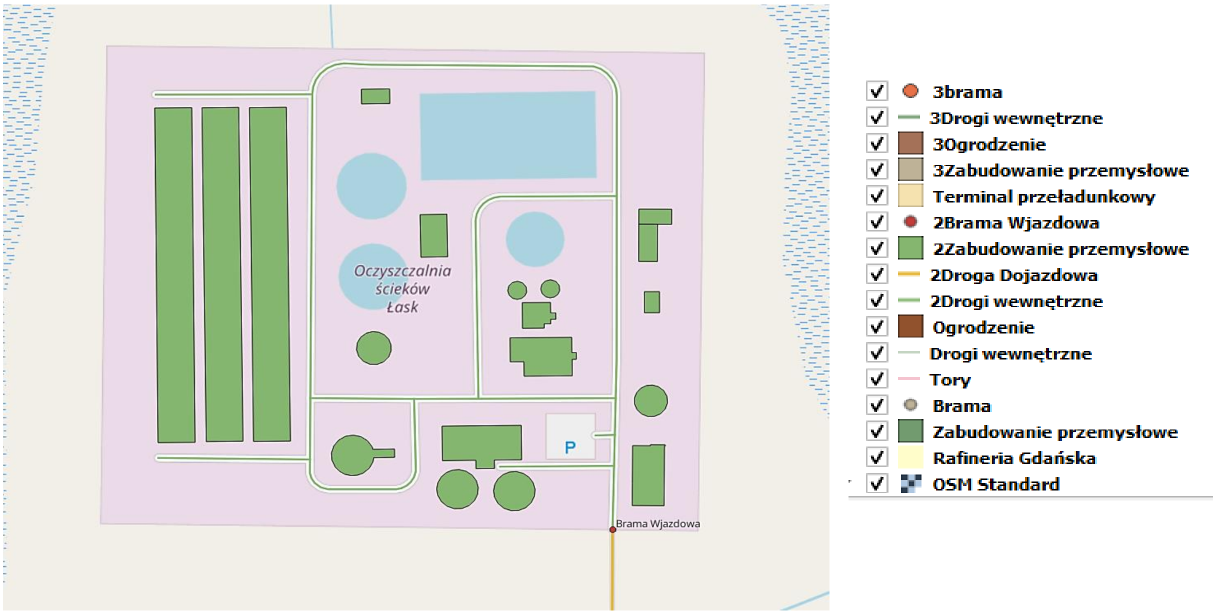


Figure 2. Public health protection systems as an example of critical infrastructure in Poland: Łask Sewage Treatment Plant.

Source: own elaboration using QGIS program.

The Łask Sewage Treatment Plant holds crucial importance for several reasons. Firstly, it plays a pivotal role in environmental conservation by treating wastewater, preventing pollution, and safeguarding local water bodies. Secondly, its operation ensures public health by treating sewage before its discharge, minimizing the risk of waterborne diseases. Thirdly, the plant's adherence to strict environmental standards contributes to sustainable water management practices in the region. Moreover, the Łask Sewage Treatment Plant supports urban development by providing essential infrastructure for growing communities. In summary, the plant's functions extend beyond wastewater treatment, encompassing environmental protection, public health, and sustainable urban planning.

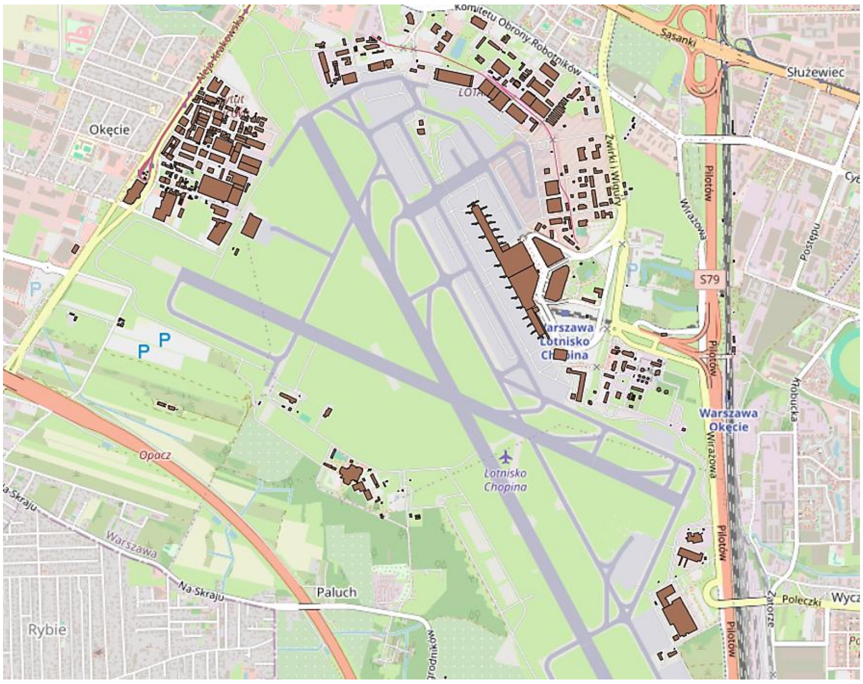


Figure 3. Transports systems as an example of critical infrastructure in Poland: Warsaw Chopin Airport. Source: own elaboration using QGIS program.

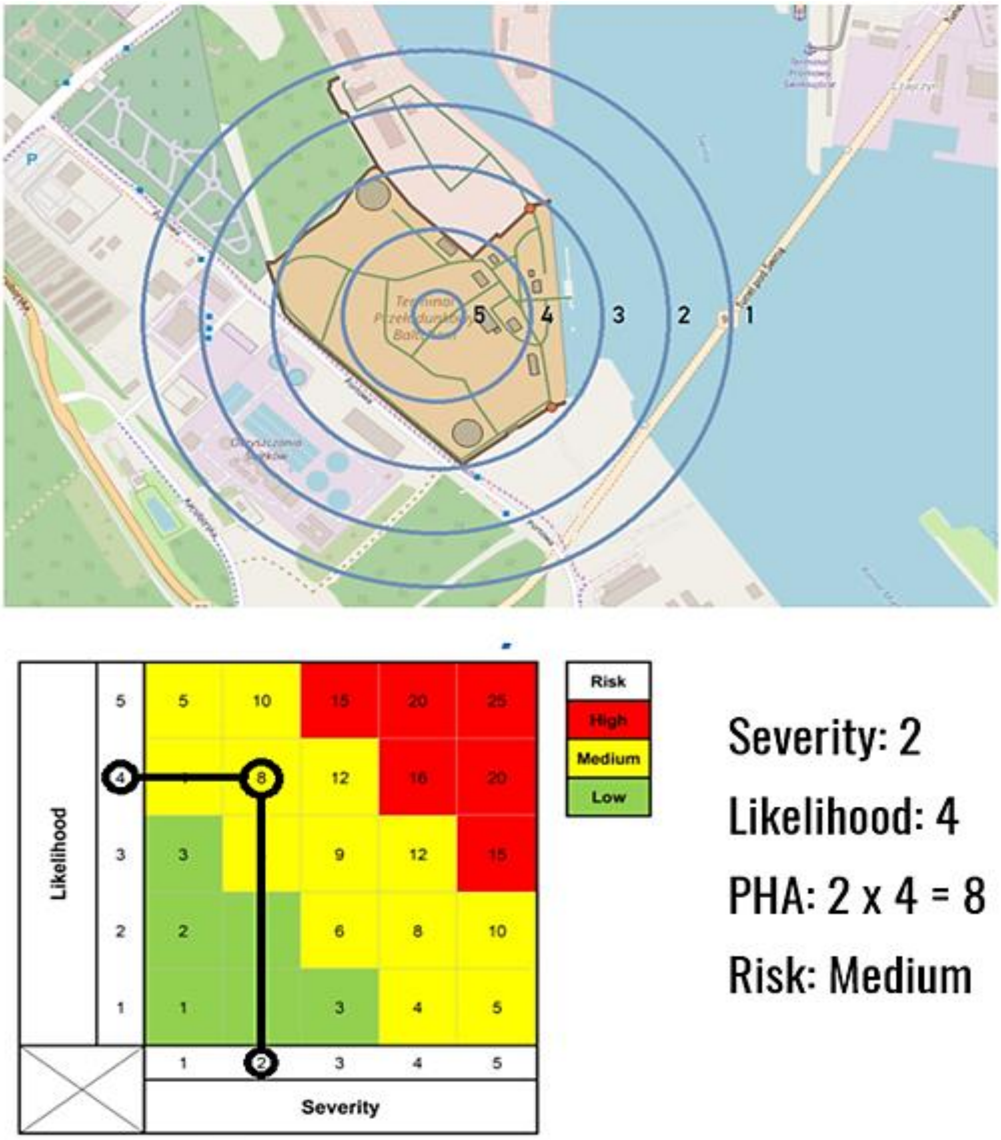
Warsaw Chopin Airport holds significant importance for various reasons. Firstly, as Poland's largest and busiest airport, it serves as a crucial international gateway, connecting the country to a wide array of global destinations. Secondly, it plays a pivotal role in supporting the nation's economy by facilitating business travel, tourism, and trade. The airport's strategic location within Europe positions it as a key transportation hub, contributing to regional connectivity and economic growth. Thirdly, Warsaw Chopin Airport is a vital asset for the capital city, serving as a major transportation center for governmental, diplomatic, and cultural exchanges. Additionally, its modern facilities and services contribute to Poland's overall competitiveness in the global aviation industry. Lastly, the airport's role in cargo transportation enhances trade and commerce, facilitating the movement of goods and strengthening Poland's economic ties with the rest of the world.

3.2. Risk assessment

The next stage of the research was a risk assessment for selected threats to the examined critical infrastructure facilities categorized for the corresponding risk scale. Risk, according to the Polish standard ISO 31000:2012, means the influence of internal and external factors on the uncertainty of achieving the set goals (Olkiewicz, 2020). In relation to emergencies, risk can be defined as an identified undesirable event that may occur with a certain probability. To quantify risk (the probability of a specific effect occurring at a specific time or in a specific situation) in crisis management, the formula is used (Ładysz, 2015):

$$R = P \times S \tag{1}$$

where:
R – risk,
P – probability of occurrence of a crisis situation,
S – value of potential losses, estimated destruction after the occurrence of a crisis situation.



Likelihood	1	2	3	4	5
5	5	10	15	20	25
4		8	12	16	20
3	3		9	12	15
2	2		6	8	10
1	1		3	4	5

Risk
🟥 High
🟨 Medium
🟩 Low

Severity: 2
Likelihood: 4
PHA: 2 x 4 = 8
Risk: Medium

Figure 4. Risk assessment using PHA methodology for liquid fuel base Świnoujście.
Source: own elaboration using QGIS program.

As an example of risk analysis, the PHA method was used to calculate flood risk for a critical infrastructure facility. When building crisis management scenarios, dedicated actions are planned for a specific level of risk. IT tools for crisis management services provide wide opportunities to create specifications in the examined area and work on selected data layers. Attribute tables for data additionally constitute a database of information that can be displayed on maps and managed accordingly.

3.3. Cyber security tools

Critical infrastructure facilities may be exposed to various types of threats, which include:

- natural hazards (floods, strong winds, drought, intense snowfall, epidemics),
- technical hazards (breakdown of equipment and damage to structures),
- terrorism (direct attacks, cyber-terrorism).

Based on the completed risk assessment stage, taking into account selected threats to the assessed critical infrastructure facilities, it is possible to select adequate measures to protect these facilities.

Effective cyber security management requires the implementation of advanced technologies and strategies that minimize the risk of attacks and ensure continuity of systems. These include:

- Advanced Threat Detection and Response Systems (SIEM): A SIEM system integrates data from a variety of sources, enabling the detection of anomalies and potential threats in real time. An example of the application of SIEM in power grids can be found in research on power grid security monitoring and analysis (Zhang et al., 2018).
- Applications of Artificial Intelligence (AI) and Machine Learning (ML): AI and ML can be used to predict and prevent threats. An example of the use of AI and ML in analysing network traffic patterns and identifying threats can be found in the literature on critical infrastructure cyber security (Hodo et al., 2017).
- Multi-Factor Authentication (MFA) mechanisms: MFA adds additional layers of protection by requiring users to confirm their identities with more than one factor. An example of the use of MFA in healthcare infrastructure can be found in research on securing patient data (Gomathi et al., 2020).
- Data Encryption: Encryption provides protection for sensitive information stored and transmitted within critical infrastructure. An example of the use of encryption in water systems can be found in the literature on data security in SCADA systems (Fernandez et al., 2014).
- Regular Penetration Tests and Security Audits: Regular penetration tests and security audits help identify vulnerabilities in information systems. An example of the use of penetration testing in the financial sector can be found in the literature on security assessment of banking systems (Jouini et al., 2014).
- Incident Management and Disaster Recovery Plans (DRPs): The preparation of disaster recovery and business continuity plans is crucial for the rapid restoration of critical system functions after an incident. An example of the application of DRP in energy systems can be found in the research on incident management (Wang, 2016).

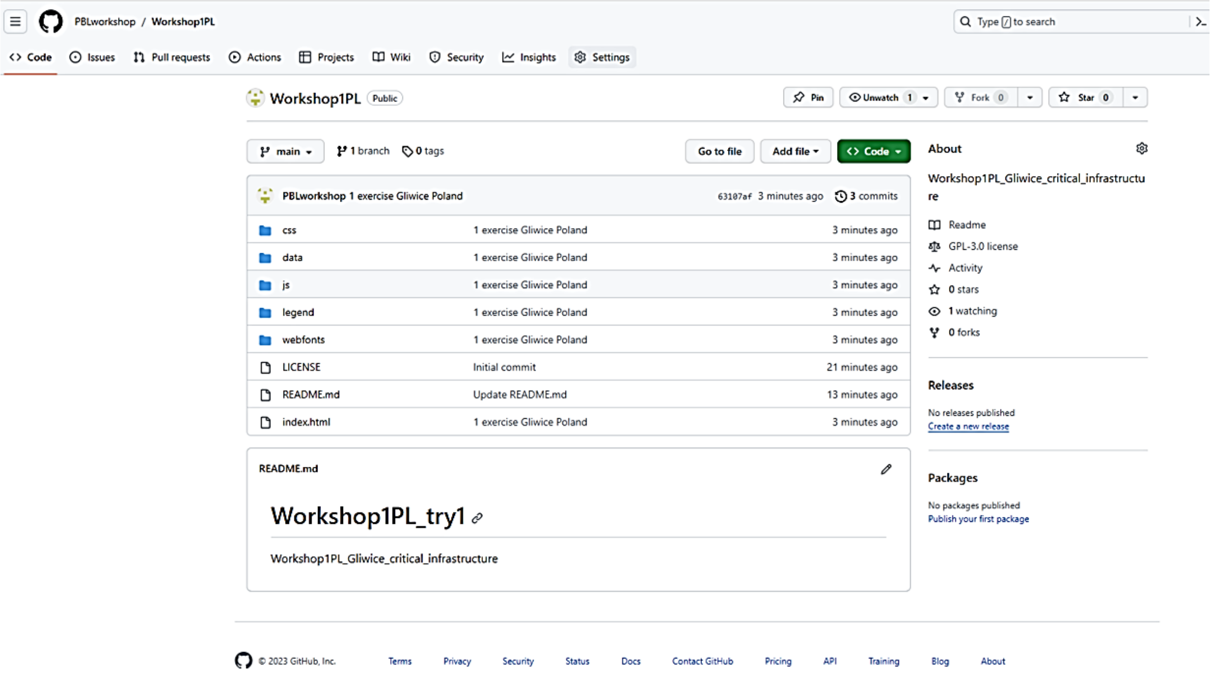
As an example of preventive activities that concern information published on various websites available via the Internet, the article focuses on selected aspects of cybersecurity of geoinformatic data.

In one well-documented case, there was a cyber-attack on navigation systems in the Black Sea in 2017. Ships equipped with GPS systems began to report navigation problems, resulting in their locations being incorrectly indicated. This incident attracted the attention of security experts, who suspected that this was the result of GPS signal interference (GPS spoofing).

Attack Methodology: Attackers used a technique known as ‘GPS spoofing’, which involves sending false GPS signals that interfere with the correct signals coming from satellites. As a result, the GPS receivers on the ships received false information about their position, leading to erroneous navigation. This type of attack can be carried out using relatively cheap hardware and software available on the market, making it a serious threat to the safety of maritime navigation.

Nowadays, geo-information data plays a key role in critical infrastructure management, spatial planning and emergency response. Their availability and accuracy are important, but the publication of this data on various online platforms is associated with a number of cyber threats. Selected aspects of cyber security that are key to protecting geoinformatics data are discussed below.

Figures 5 and 6 show examples of geoinformatics data publications on GitHub, presenting a web map data repository covering sample critical infrastructure data along with risk assessments of selected sites. Such repositories require the identification of a strict group of users and their access levels to the data. The use of tools in data protection, data encryption, data integrity protection, incident management and threat response therefore becomes essential.



PBLworkshop 1 exercise Gliwice Poland		63107af 3 minutes ago 3 commits
css	1 exercise Gliwice Poland	3 minutes ago
data	1 exercise Gliwice Poland	3 minutes ago
js	1 exercise Gliwice Poland	3 minutes ago
legend	1 exercise Gliwice Poland	3 minutes ago
webfonts	1 exercise Gliwice Poland	3 minutes ago
LICENSE	Initial commit	21 minutes ago
README.md	Update README.md	13 minutes ago
index.html	1 exercise Gliwice Poland	3 minutes ago

README.md

Workshop1PL_try1

Workshop1PL_Gliwice_critical_infrastructure

About

Workshop1PL_Gliwice_critical_infrastructure

Readme
GPL-3.0 license
Activity
0 stars
1 watching
0 forks

Releases

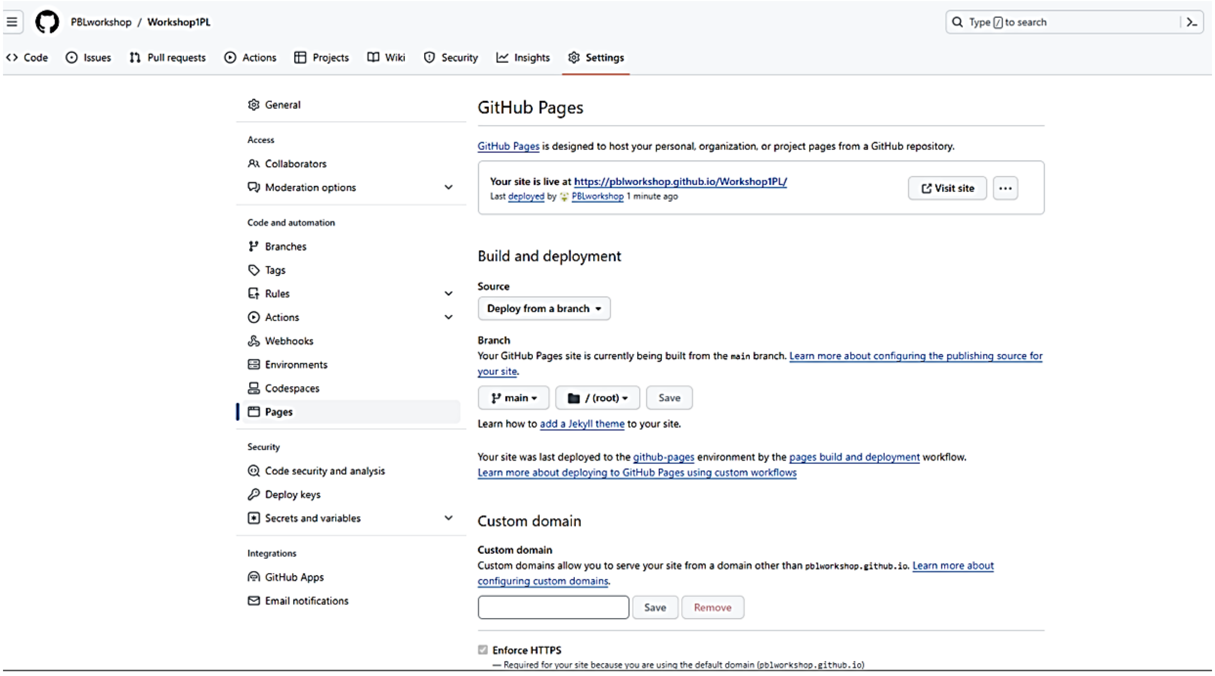
No releases published
Create a new release

Packages

No packages published
Publish your first package

Figure 5. Creation of a new repository for data on identified critical infrastructure facilities along with risk assessment on GitHub.

Source: own elaboration using GitHub.



GitHub Pages

GitHub Pages is designed to host your personal, organization, or project pages from a GitHub repository.

Your site is live at https://pblworkshop.github.io/Workshop1PL/
Last deployed by PBLworkshop 1 minute ago

Build and deployment

Source
Deploy from a branch

Branch
Your GitHub Pages site is currently being built from the `main` branch. Learn more about configuring the publishing source for your site.

main / (root)

Learn how to add a Jekyll theme to your site.

Your site was last deployed to the github-pages environment by the pages build and deployment workflow.
Learn more about deploying to GitHub Pages using custom workflows

Custom domain

Custom domain
Custom domains allow you to serve your site from a domain other than `pblworkshop.github.io`. Learn more about configuring custom domains.

☑ Enforce HTTPS
— Required for your site because you are using the default domain (`pblworkshop.github.io`)

Figure 6. Creation of a new link for web map with identified critical infrastructure facilities along with risk assessment on GitHub.

Source: own elaboration using GitHub.

In order to secure data on the Git Hub service, it is essential to follow key security principles which include:

- Data Access Protection: Geoinformatics data are often used by a variety of institutions and users. To protect this data from unauthorized access, multi-factor authentication (MFA) mechanisms are used. MFA increases the level of security by requiring users to confirm their identity with more than one factor, such as a password and a one-time code sent to a mobile phone. This ensures that even if a third party gains access to the password, access to the data will still be protected.
- Data Encryption: Encryption is a fundamental part of geoinformatics data protection. This process involves converting data into a form that is unreadable by those without the appropriate decryption key. Encryption should be used both when data is being transmitted over networks and when it is stored on servers. The use of strong encryption algorithms, such as AES (Advanced Encryption Standard), ensures that even if data is intercepted by cyber criminals, it will remain unreadable and unusable.
- Protecting Data Integrity: The integrity of geo-information data is crucial to ensure its accuracy and reliability. Techniques such as digital signatures and hash functions can be used to ensure that data has not been modified since its creation. Digital signatures make it possible to verify the authenticity of data and identify its author, which is particularly important in the context of critical data.

- Incident Management and Threat Response: Effective management of cyber security incidents requires the development of attack response plans. These plans should include procedures for detecting, analysing and responding to incidents such as data breaches or DDoS (Distributed Denial of Service) attacks. The implementation of disaster recovery procedures and business continuity plans (DRPs and BCPs) ensures the rapid restoration of critical systems functions and minimises the impact of incidents on the organisation's operations.

Adherence to these principles significantly enhances the security of geo-information data on popular sites including GitHub.

4. Discussion

Data security risks in the cloud are multifaceted, arising from data vulnerabilities, unauthorised access and inadequate encryption practices. Understanding these risks is critical for organisations using cloud services.

Key cloud data security risks include:

- Unauthorised access: cloud environments are vulnerable to breaches where unauthorised users can access sensitive data. This risk is exacerbated by weak authentication mechanisms and poor access management practices (Basha et al., 2023).
- Data leakage: The potential for data leakage is significant, especially when users share files without proper encryption. This can lead to the exposure of critical information to unintended parties (Roobini et al., 2024).
- Inadequate encryption: while encryption is a primary defence, many cloud services do not implement robust encryption protocols. The Advanced Encryption Standard (AES) is recommended, but its effectiveness depends on proper implementation (Basha et al., 2023).
- Security vulnerabilities in mobile cloud computing: The growth of mobile cloud computing poses additional risks, as mobile devices may not have the same security measures as traditional computing environments, making them more vulnerable to attacks (Waseem et al., 2016).

Despite these risks, organisations can mitigate them through stringent security protocols, regular audits and the use of advanced encryption techniques to protect data integrity and confidentiality. In order to secure GIS data, the authors proposed a number of methods to limit access by unwanted parties.

5. Conclusions

Security is an aspect that determines stable social development. The dynamic course of technological development, including the development of IT and communication systems, the volume and diversity of types of available data, is characterized by both many advantages and very important threats.

The article attempts to discuss selected aspects of crisis management in terms of critical infrastructure protection. Selected issues were discussed regarding selected IT tools that can provide excellent support for anti-crisis services. The work shows the effects of work in the QGIS program, which used, among others, the open street map plugin to identify critical infrastructure facilities in Poland. Next, the usefulness of generating a web map directly in the software was demonstrated. This method of data preparation has one drawback – it is only available on a specific computer. In order to publish specific data for a wider group of recipients, it is possible to place files regarding the created website on GitHub. This solution, using a new repository, allows you to generate a direct link to the data. This tool, of course, allows to publishing data in an open mode, available to all users or selected ones. The presented material contains many important cognitive aspects that clearly confirm the importance of IT systems in the protection of critical infrastructure.

The results of the research conducted are:

1. Demonstration of QGIS functionality in emergency management:
   - Implementation of vector layers from OpenStreetMap.
   - Geoprocessing tools in the form of multi-level buffers.
   - Webmap plugin.
2. Identification of methods for securing data shared in the cloud:
   - multi-factor authentication (MFA),
   - use of key decryption,
   - digital signatures for access verification,
   - procedures for detecting, analysing and responding to incidents such as data breaches or DDoS (Distributed Denial of Service) attacks.

The article provides practical examples that can be applied to Cyber Security management.

Acknowledgements

Author Contributions: Conceptualization: A.B. and A.M.; methodology: A.B. and A.M.; validation: A.B., A. M. and K.T-O.; formal analysis: M.B., K.T-O., A.M. and A.B. investigation: M.B., A.M. and K.T-O.; resources: A.B.; data curation: K.T-O.; writing—

original draft preparation: A.B., A.M., M.B. and K.T-O.; writing—review and editing: A.B., A.M., M.B. and K.T-O.; visualization: A.M., M.B., A.B. and K.T-O.; supervision: A.B. and A.M.; project administration: A.M. and M.B.; funding acquisition: A.M. and M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded as part of the Excellence Initiative – Research University program of Silesian University of Technology (PBL).

References

1. Alhaj, M.K., Abdalla, A.G.E. (2022). Usage of GIS in system planning and management of infrastructures projects. *European Journal of Computer Science and Information Technology, 10*(4), 33-51.
2. Basha, S.M., Rishik, V., Krishna, V.J.N., Kavitha, S. (2023). Data security in cloud using advanced encryption standard. *International Conference on Inventive Computation Technologies (ICICT), IEEE,* 1108-1112.
3. Bluszcz, A. (2018). Conditions for maintaining the sustainable development level of EU member states. *Social Indicators Research, Vol. 139, 2,* 679-693. doi:10.1007/s11205-017-1746-6
4. Bluszcz, A., Tobór-Osadnik K., Manowska A., Kelisek, A. (2023). *The use of web maps in managing crises caused by climate change*. Proceedings of 23rd International Multidisciplinary Scientific GeoConference SGEM 2023 / Trofymchuk Oleksandr, Rivza Baiba (red.), International Multidisciplinary Scientific GeoConference & EXPO SGEM, 2023, vol. 23, nr 4.2, STEF92 Technology, 1-10, ISBN 978-619-7603-65-1.
5. Bluszcz, A., Tobór-Osadnik, K., Tomiczek, K., Mansor, S., Awang, H. (2023). The use of geomatics tools in critical infrastructure management. *Journal of the Polish Mineral Engineering Society, 1,* 169-174. http://doi.org/10.29227/IM-2023-01-21
6. Boumahdi, A., El Hamlaoui, M., Nassar, M. (2020). Crisis Management Systems: Big Data and Machine Learning Approach. *ENASE,* 603-610.
7. Chowdhury, N., Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review, 40,* 100361.
8. Fernandez, J., Simões, J., Santos, H. (2014). *Survey of ICS SCADA security related incidents in the energy sector*. Proceedings of the International Conference on Critical Information Infrastructures Security (CRITIS). doi: 10.1007/978-3-319-25225-6_2
9. Flenniken, J.M., Stuglik, S., Iannone, B.V. 2020. Quantum GIS (QGIS): An introduction to a free alternative to more costly GIS platforms: FOR359/FR428. *Edis, 2,* 7-7.
10. Garg, N., Bawa, S., Kumar, N. (2020). An efficient data integrity auditing protocol for cloud computing. *Future Generation Computer Systems*, *109*, 306-316.

11. Gomathi, S., Vimal, S., Muthusamy, K. (2020). A review on multi-factor authentication mechanisms for e-healthcare applications. *International Journal of Advanced Science and Technology, 29(3),* 2852-2861. doi: 10.30534/ijatcse/2020/127932020
12. Gourevitch, M.N., Kleiman, N., Falco, K.B. (2022). Public Health and Public Safety: Converging Upstream. *American Journal Of Public Health*, *112*(5), 716-718.
13. Greenough, P.G., Nelson, E.L. (2024). *52 - Use of Geographical Information Systems in Crises.* In: G.R. Ciottone, *Ciottone's Disaster Medicine* (Third Edition). Elsevier, 341-346, doi: 10.1016/B978-0-323-80932-0.00052-5.2024.
14. Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., Atkinson, R. (2017). *Machine learning approach to anomaly-based intrusion detection system for software-defined network*. Proceedings of the International Conference on Wireless Networks and Mobile Communications (WINCOM). doi: 10.1109/WINCOM.2017.8238164
15. Jain, N., Singhal, P. (2024). Securely Cloud Data Storage and Sharing. *Journal of Informatics Electrical and Electronics Engineering (JIEEE), 5(1),* 1-12.
16. Jouini, M., Rabai, L.B.A., Aissa, A.B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32,* 489-496. doi: 10.1016/j.procs.2014.05.451
17. Ładysz, J. (2015). *GIS technology in security engineering.* Wroclaw, Poland.
18. Levytska, S., Osadcha, O., Tykhonchuk, L. (2023). Security of economic potential for critical infrastructure subjects. *Scientific Notes of Ostroh Academy National University, Economics Series*, *31(59),* 4-12.
19. Mahida, A. (2024). Secure Data Outsourcing Techniques for Cloud Storage. *International Journal of Science and Research (IJSR), 13(4),* 181-184.
20. Manowska, A., Boroš, M., Bluszcz, A., Tobór-Osadnik, K. (2024). The use of the command line interface in the verification and management of the security of IT systems and the analysis of the potential of integrating biometric data in cryptographic mechanisms. *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 198*, 289-308. doi:10.29119/1641-3466.2024.198.16
21. Manowska, A., Boroš, M., Hassan Muhammad Waqar, Bluszcz, A., Tobór-Osadnik, K. (2024). A modern approach to securing critical infrastructure in energy transmission networks: integration of cryptographic mechanisms and biometric data. *Electronics (Switzerland), vol. 13-14,* 2849, 1-19. doi:10.3390/electronics13142849.
22. Mead, N.R. (2022, August). *Critical infrastructure protection and supply chain risk management*. IEEE 30th International Requirements Engineering Conference Workshops (REW), 215-218.
23. Mishra, P., Verma, V. (2020). Study of identity-based encryption for cloud data security. *Decision analytics applications in industry*, 401-408.
24. Olkiewicz, M. (2020). The role of the stakeholder in the quality improvement of an organization. *Zeszyty Naukowe Organizacja i Zarządzanie*. Politechnika Śląska, 235-245.

25. Peng, L., Yan, Z., Liang, X., Yu, X. (2023). SecDedup: Secure data deduplication with dynamic auditing in the cloud. *Information Sciences, 644*, 119279.
26. Petersen, L., Lange, D., Theocharidou, M. (2020). Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators. *Reliability Engineering & System Safety*, *199*, 106872.
27. Roobini, M.S., TejaSatyanrayana, B., SaiVenkataGirish, B., Sridevi, N., Pothumani, S. (2024). Threat-Specific Security Risk Evaluation in the Cloud. *International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 1-10.
28. Tzanakakis, V.A., Paranychianakis, N.V., Angelakis, A.N. (2020). Water supply and water scarcity. *Water*, *12*(9), 2347.
29. Van Damme, I. (2022). *National security.* [in:] Bethlehem D., and others (eds), The Oxford Handbook of International Trade Law (2e), Oxford Handbooks (Oxford, 2022; online edn, Oxford Academic, doi: 10.1093/oxfordhb/ 9780192868381.013.28
30. Wang, Y., Yang, J., Lin, H. (2016). *Research on emergency response management of power grid.* Proceedings of the International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC). doi: 10.1109/IHMSC.2016.19
31. Waseem, M., Lakhan, A., Jamali, I.A. (2016). Data security of mobile cloud computing on cloud server. *Open Access Library Journal*, *3*(4), 1-11.
32. Xiao, Z., Wu, X., Li, P., Liu, Z., Yang, H., Zhou, Z., Zhang, L. (2019). Power communication network design considering global information fusion part two applications and explorations. *Procedia Computer Science*, *155*, 768-773.
33. Yigit, Y., Ferrag, M.A., Sarker, I.H., Maglaras, L.A., Chrysoulas, C., Moradpoor, N., Janicke, H. (2024). Critical infrastructure protection: Generative ai, challenges, and opportunities. *arXiv preprint arXiv:2405.04874*.
34. Zargar, S., Shahidinejad, A., Ghobaei-Arani, M. (2021). A lightweight authentication protocol for IoT-based cloud environment. *International Journal of Communication Systems*, *34*(11), e4849.
35. Zhang, J., Li, Y., Wang, J., Ma, L. (2018). A survey on cybersecurity in smart grid. *Energy Reports*, *4*, 181-189. doi: 10.1016/j.egyr.2018.06.001
36. Zwiech, P. (2022). Approaches to Socio-Economic Inequality in Economic Theory, *Scientific Papers Of Silesian University Of Technology, Organization And Management Series*, *164*, 565-572, doi: 10.29119/1641-3466.2022.164.43
37. Żywucka-Kozłowska, E., Broniecka, R. (2024). Security Threats to Port Critical Infrastructure. *Cybersecurity and Law, 12(2)*, 273-281.