GIS Odyssey Journal

2022 • Volume 2 • Number 2

https://doi.org/10.57599/gisoj.2022.2.2.23

Agnieszka Besiekierska[1], Kamil Czaplicki[2]

CYBERSECURITY OF SPATIAL INFORMATION

Abstract: Services related to the broadly understood spatial information are subject to constant and intensive digitization. In addition to many positive sides, such as broad access to services, digitization also brings negative phenomena such as cyber attacks, which have intensified in recent years. Responsibilities in the area of cybersecurity are subject to legal provisions, including the act on the national cybersecurity system. Unfortunately, these obligations are still not sufficiently fulfilled, which is reflected in the results of the Supreme Audit Office (NIK). Advice on safety measures can be found in the letter of the Surveyor General of Poland dated 24 February 2022. The measures indicated in the letter should be considered insufficient.

Keywords: spatial information, cybersecurity, Surveyor General, GIS

Received: 31 October 2022; accepted: 12 November 2022

[1] Cardinal Stefan Wyszyński University, Faculty of Law and Administration, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-1223-1442, email: a.besiekierska@uksw.edu.pl
[2] Cardinal Stefan Wyszyński University, Faculty of Law and Administration, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-3777-4339, email: k.czaplicki@uksw.edu.pl

Introduction

Entities dealing with broadly understood spatial information, including in particular public administration bodies such as surveying offices, are subject to constant and dynamic digitization. One of the most popular terms in recent years, if not decades, is the word transformation – initially referring to political, economic or systemic transformation. Currently, the term is more and more often associated with digital transformation. This term can be understood as the use of technology to transform analog into digital processes. It is an integration of digital technology in all areas of operation. It influences the change of existing behaviors and processes through the increased use of information technologies (Szpor et al., 2021).

From transformation digital one should distinguish between the concepts of computerization and digitization. In the case of computerization, the emphasis was mainly on the increased use of computers as tools supporting human work. Digitization emphasized the transfer of processes to the virtual world, the creation of new digital services and efforts to create a new communication tool. The digital transformation emphasizes the increased use of supporting technologies, such as Big Data, the Internet of Things, artificial intelligence or data analytics. Digital transformation is often equated with business – the term economy 4.0 as the embodiment of digital transformation in industry is becoming more and more popular. This approach is not entirely correct. Digital transformation goes beyond the sphere of business, it affects every area of social activity, including public administration (Kaczyńska et al., 2021). Entities dealing with spatial information are among the most computerized entities. Spatial information is based, among others, on the analysis of huge amounts of data and the use of information technologies supporting their analysis.

This article introduces the importance of cybersecurity in the field of spatial information, presents the legal requirements and threats related to the provision of spatial information access services, as well as assesses the effectiveness of their implementation, pointing to areas for improvement.

Relevant terms: spatial data services, cybersecurity and cyberthreats

The principles of creating and using the infrastructure for spatial information are specified in the Act of March 4, 2010 on the infrastructure for spatial information. The Act defines two key terms in this area: spatial data and spatial data services (art. 3 points 1 and 10). Spatial data means data relating directly or indirectly to a specific location or geographical area. The concept of spatial data services is related to spatial data, understood as services that are operations that can be performed with the use of computer software on data contained in spatial data sets or on related metadata.

The Act does not use the term "geographic information system" (GIS), which is commonly used in practice and is defined in the literature as "a system for acquiring, processing and sharing data containing spatial information and accompanying descriptive information about objects distinguished in the part of the space covered by the system's operation" (Ładysz, 2015). Pursuant to the Act, administrative bodies keep

public registers that contain collections related to spatial data, create and maintain, within the scope of their competence, a network of services related to spatial data sets and services. spatial data sets and services include searching for spatial data sets and services, viewing sets, downloading, copies of sets or parts thereof, and transforming sets in order to achieve the interoperability of spatial data sets and services (Article 9 (1)). The most important portal enabling access to spatial data services is the Geoportal, which is created and maintained by the Surveyor General of Poland. In Poland, the construction of GIS systems is dominated by administrative units – provinces and cities, for which it is one of the most important elements in the development and functioning of the local community, being at the same time a rich source of information for potential investors and tourists. Administrative bodies report sets and spatial data services to the Surveyor General of Poland.

"Cybersecurity" means actions necessary to protect networks and information systems, users of such systems and other persons against cyber threats"(Article 2 point 1 of the Regulation (EU) 2019/881 – Cybersecurity Act). In the Act of July 5, 2018. on the national cybersecurity system "cybersecurity" is defined as the resistance of information systems to activities violating the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these systems.

Unfortunately, technological development, including digital transformation, is not free from threats. Cyberattacks are becoming more common and then more and more dangerous - that is, attacks made by digital means through cyberspace with the intention of causing damage, blocking access, destroying or taking over data (Szpor et al., 2021). The Cybersecurity Act, in Art. 2 point 8, defines a cyber threat as any potential circumstances, events or activities that may cause harm, disrupt or otherwise adversely affect network and information systems, users of such systems and other persons.

Legal obligations related to the cybersecurity

The role of entities dealing with spatial information is to ensure the security and integrity of data. The first legal act that imposed obligations in this area of data security, obliging them to ensure confidentiality, integrity, availability and resilience of IT systems, was the Regulation on the Protection of Personal Data. GDPR obliges both data controllers as well as data processors to ensure a level of security of data processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The proper level of security must be ensured through implementation of adequate technical, organizational and procedural measures (Art. 32 of the GDPR) (Czaplicki, 2018).

In accordance with the Act on the national cybersecurity system, public entities that have IT systems containing spatial information have obligations related to ensuring cybersecurity, such as appointing a person responsible for maintaining contact with the entities of the national cybersecurity system (Art. 21), managing incidents in a public

entity (Article 22 (1) point 1), reporting incidents (Article 22 (1) point 2) and publishing information about cybersecurity on the website (Article 22 (1) point 4).

The Act on the national cybersecurity system is not the only legal act that imposes cybersecurity obligations on public entities (Besiekierska, 2019). Further obligations result from the Act on computerization of the activities of entities performing public tasks and more precisely from § 20 of Regulation of the Council of Ministers on the National Interoperability Framework,, issued on the basis of that Act. The Regulation requires the entity performing public tasks to maintain an information security management system. This system should include, inter alia, internal regulations, inventorying equipment, ensuring an appropriate level of security in the ICT system, minimizing the risk of information loss as a result of a failure, periodic risk analyzes, trainings, annual audits. The Regulation does not answer the question on how to perform individual obligations. A certain hint is provided in § 20.3, according to which the cybersecurity requirements resulting from the Regulation are deemed to be met if the information security management system has been developed on the basis of the Polish Standard PN-ISO / IEC 27001, and establishing security, risk management and auditing are carried out on the basis of Polish Standards related to this standard, including PN-ISO / IEC 27002, PN-ISO / IEC 27005 and PN-ISO / IEC 24762.

Materials and methods

The following materials were used in the study:

- Informacja o wynikach kontroli NIK, Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP (2021) (*Information on the results of the NIK audit, Implementation of public services for citizens using the ePUAP platform*), source: https://www.nik.gov.pl/kontrole/P/20/004/.
- Informacja o wynikach kontroli NIK, Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego (2019) (*Information on the results of the NIK audit, Information security management in local government units*), source: https://www.nik.gov.pl/kontrole/P/18/006/.
- Informacja o wynikach kontroli NIK, Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych (2022) (*Information on the results of the NIK audit, Information security at remote work and mobile data processing*), source: https://www.nik.gov.pl/kontrole/P/21/081/LOL/.

The research was based on the following methods: literature review, analysis of the materials above, quantitative research and internal surveys.

The article uses quantitative research on training in cybersecurity carried out as part of the Project Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym (*Regulatory Model of Disclosure and its Limitations in a Democratic State of Law*), as well as internal surveys conducted during training courses organized by the Cardinal Stefan Wyszyński University in Warsaw and partners supporting the university, including Naukowe Centrum Prawno-Informatyczne (*the Scientific Center Legal and IT*).

Results and discussion

Despite the binding legal obligations to ensure the security and integrity of data, many entities still do not comply with basic security principles and are exposed to cyberattacks. This is indicated by the information published in recent years on the audit results of the Supreme Audit Office (Polish "NIK"). NIK assessed negatively the performance of tasks related to ensuring the security of the processed information, indicating that the offices lacked a systemic approach to ensuring information security. The offices did not have information about their IT resources, did not perform risk assessments, did not carry out an annual audit, and the system access policy was affected by irregularities. In 48% of offices, irregularities were found, consisting in failure to make backups, improper storage of backups and failure to check the correctness of the copies made (Information security management in local government units, 2019). Similarly, in the information on the results of the inspection carried out in 2020, it was indicated that most of the inspected units did not ensure proper organization of information security, which may pose a threat to the security of data processing and ensuring the continuity of the office's work. In particular, 57% of the controlled units lacked an Information Security Management System, and 39% of offices lacked complete and up-to-date information about their IT resources for data processing. In 57% of them, mandatory information security audits were not carried out (Implementation of public services for citizens using the ePUAP platform, 2021).

There is no information available in the media as to whether and to what extent the attacks concerned spatial data services. There is a known attack on the IT systems of the Aleksandrów Municipal Office in the spring of 2021, as a result of which databases were encrypted, which were also used by the Commune Social Welfare Center. It was the week before Easter, when some of the inhabitants of the commune were waiting impatiently for the payment of their benefits (Laurisz, 2022). The cyber criminals demanded a ransom. Other municipalities that have been attacked by cybercriminals are the Kościerzyna Municipal Office, Tuczna Municipal Office, Małopolska Marshal's Office, Poviat Starosty in Oświęcim, Kościerzyna Municipal Office (Municipalities targeted by criminals, 2022).

A consequence of the increasing scale of threats was a letter sent by the Surveyor General of Poland to starosts and mayors of cities regarding cybersecurity of data and related services (Letter of the Surveyor General of Poland dated 24.02.2022). In this letter, the Surveyor General drew attention to the statutory obligations to secure data and the consequences that may result from inadequate protection of spatial data. The letter pays particular attention to the necessity to make electronic backup copies of the geodetic resource. According to the Regulation of the Minister of Development, Labor and Technology on the organization and procedure of the state geodetic and cartographic resource, it is necessary to back up the resource at least once a quarter. In the current situation, it has been suggested to increase the frequency of backups and make them on a weekly basis. The suggestion of the Surveyor General should be assessed moderately positively. It seems that making a 3-month backup (once a quarter)

was dictated only by staff shortages and relieving offices from employing additional specialized IT specialists. The resource of spatial data is crucial for administration, citizens and business. Performing a backup once a quarter means that in the event of a failure or cyberattack, we may lose data from the previous backup (in the worst case it will take up to 3 months). In the case of processing such sensitive data, the scope of lost data seems to be enormous. Recommendation of the Surveyor General shortening this period to 7 days, although positive, does not solve the problem for several reasons. First, the loss of 7-day data is also enormous and difficult to make up for in a short period of time. Second, it's not just the backup itself that counts, but making an effective backup. For the case, it is worth giving the example of the office in Krakow, where despite the backups, in the event of a failure, it turned out that they were not performed correctly and ultimately were not usable (One month after the cyberattack, the IT system in the Małopolska Marshal's Office is still not operational, 2021). Third, backing up is defensive. It is a possible response to an attack or failure, but not an attack defense tool in itself. Not every attack is related to e.g. data deletion. A large proportion of attacks focus on data theft. Therefore, it seems that the Surveyor General, in cooperation with CERT ABW or CERT NASK, should promote methods of offensive resource protection.

Further, the security of the processed data is not only the responsibility of IT departments (or more often one person acting as an IT specialist), but each employed employee. Cybersecurity training must be common and cyclical. Training seems to be a key element of security, however, because usually human is the weakest element of security and effective attacks are often a consequence of human error. Unfortunately, the practice based on own research conducted during the training shows that most of the employees are not trained, and those who attended the training in cybersecurity very often did not understand much of it. This is also confirmed by the results of the NIK audit, where it was indicated that in the audited units the training took place by providing training materials for self-familiarization (Information security at remote work and mobile data processing, 2022). However, this form of knowledge transfer also turned out to be insufficient in the event of a breach of personal data protection. The Polish supervisory authority, the Office for Personal Data Protection, decided that the mere provision of information by the Court as the administrator of personal data about the need to encrypt portable drives, without implementing this security measure, does not satisfy the obligations resulting from the Regulation on the Protection of Personal Data (Decision of UODO of 13 July 2021)

Conclusion

Subsequent audits of the Supreme Audit Office, as well as the authors' own observations, indicate that organizational and technical measures implemented by public entities to protect broadly understood spatial information are insufficient, which means that they are kept at a minimum level (e.g. backup at least once for seven days) or they are not present at all (the lack of information security management systems in some local government units indicated during the audit). In light of the increasing

number of cyberattacks, issues related to cybersecurity should be treated as a priority by all stakeholders.

References

Act of 5 July 2018 on national cybersecurity system Dz. U. (*Journal of Laws*) of 2018, item 1560.

Act of 4 March 2010 on spatial information infrastructure. Dz. U. (*Journal of Laws*) of 2021, item 214.

Act of 17 February 2005 on computerization of the activities of entities performing public tasks Dz.U. (Journal of Laws) of Dz. U. of 2017, item 570, with changes.

Besiekierska A. (2019). Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz (Act on cybersecurity system. Commentary). C.H. Beck, Warsaw.

Czaplicki K. (2018). Security of geographical information systems – how to ensure their confidentiality, integrity, availability and resilience. 25th Anniversary Conference, Geographic Information Systems Conference and Exhibition GIS Odyssey 2018.

Decision of UODO of 13 July 2021, https://uodo.gov.pl/pl/138/2130 [access: 28.10.2022].

Gminy na celowniku przestępców (*Municipalities targeted by criminals*), https://wartowiedziec.pl/serwis-glowny/aktualnosci/62785-gminy-na-celowniku-cyberprzestepcow [access: 28.10.2022].

Gryszczyńska A., Szpor G. (2020). Internet, Cyberpandemia. Cyberpandemic. C.H. Beck, Warsaw.

Informacja o wynikach kontroli NIK, Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP (2021) (*Information on the results of the NIK audit, Implementation of public services for citizens using the ePUAP platform*), https://www.nik.gov.pl/kontrole/P/20/004/ [access: 28.10.2022].

Informacja o wynikach kontroli NIK, Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego (2019) (*Information on the results of the NIK audit, Information security management in local government units*), https://www.nik.gov.pl/kontrole/P/18/006/ [access: 28.10.2022].

Informacja o wynikach kontroli NIK, Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych (2022) (*Information on the results of the NIK audit, Information security at remote work and mobile data processing*), https://www.nik.gov.pl/kontrole/P/21/081/LOL/ [access: 28.10.2022].

Kaczyńska A., Kanduła S., Przybylska J. (2021). Transformacja cyfrowa z punktu widzenia samorządu terytorialnego – wybrane zagadnienia (*Digital transformation from the point of view of local government – selected issues*). Nierówności Społeczne a Wzrost Gospodarczy, 65 (1/2021).

Laurisz M., Gmina która padła ofiarą cyber-ataku dzieli się doświadczeniami i radzi innym samorządowcom, jak i gdzie szukać pomocy (*A municipality that has fallen victim to a cyber-attack shares its experience and advises other local government officials on how and where to seek help*) 5.01.2022, https://itreseller.com.pl/gmina-

ktora-padla-ofiara-cyber-ataku-dzieli-sie-doswiadczeniami-i-radzi-innym-samorzadowcom-jak-i-gdzie-szukac-pomocy/ [access: 28.10.2022].

Letter of Surveyor General of Poland dated 24.02.2022, https://www.geoportal.gov.pl/documents/10179/1113443/zabezpieczenie+danych+w+powiatach.pdf/28071ba3-9af4-4956-99a4-3d089243299a [access: 28.10.2022].

Ladysz J. (2015). Technologia GIS w inżynierii bezpieczeństwa (*GIS technology in security engineering*). Wrocław.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal of the European Union L 151/15.

Regulation of the Council of Ministers on the National Interoperability Framework, minimum requirements for public registers and electronic information exchange and minimum requirements for ICT systems, Dz.U. (*Journal of Laws*) of 2017, item 2247.

Regulation of the Minister of Development, Labor and Technology of 2 April 2 2021 on the organization and management of the state geodetic and cartographic resource, Dz.U. (*Journal of Laws*) 2021, item 820.

Szpor G., Grochowski L., Fischer B. (2021). Tom XXII – Prawo Informatyczne (*Volume XXII – Informatics Law*). Fundacja Ubi societas, Ibi Ius, Warsaw.

W miesiąc od cyberataku w małopolskim urzędzie marszałkowskim wciąż nie działa system informatyczny (*One month after the cyberattack, the IT system in the Małopolska Marshal's Office is still not operational*), 10.03.2021, https://samorzad.pap.pl/kategoria/e-urzad/w-miesiac-od-cyberataku-w-malopolskim-urzedzie-marszalkowskim-wciaz-nie-dziala [access: 28.10.2022].