European Research Studies Journal
Volume XXVIII, Issue 2, 2025

pp. 150-162

The Impact of Cyberthreats on the Security of Important Sectors of the Economy on the Example of the Healthcare Sector

Submitted 06/03/25, 1st revision 23/03/25, 2nd revision 18/04/25, accepted 10/05/25

Sławomir Żurawski[1], Marta Chodyka[2], Julia Nowicka[3], Grudniewski Tomasz Marek[4], Radosław Dawidziuk[5], Katarzyna Gralak[6]

Abstract:

Purpose: *The aim of this study is to demonstrate the impact of cyberthreats on the functioning of key sectors of the economy, with particular emphasis on the healthcare sector, as well as to present effective strategies for counteracting these threats.*
Design/Methodology/Approach: *In the first part of the article, the most common cyberattacks in sectors of the economy based on digital technologies are characterized, with particular emphasis on healthcare as one of the most vulnerable areas. Next, the impact of cyberattacks on the functioning of medical facilities is analysed, focusing on the consequences related to ransomware attacks, data breaches, and threats to medical devices. The following section presents strategies for counteracting threats, legal regulations, and prospects for the development of cybersecurity in the healthcare sector. The research problem is formulated as follows: Which cyberthreats pose the greatest risk to the healthcare sector and what strategies can effectively minimize their impact on the functioning of institutions? The hypothesis assumes that the increasing digitization of the healthcare sector makes medical facilities targets for cyberattacks, and effective protection against them requires the implementation of comprehensive strategies encompassing security technologies, legal regulations, and the education of medical staff. The study is based on theoretical methods, including the analysis of subject literature, cybersecurity reports, and case studies of attacks on healthcare institutions.*

[1]*State Academy of Applied Sciences in Chełm, Poland,*
ORCID: 0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl;
[2]*John Paul II University of Applied Sciences in Biala Podlaska, Poland,*
ORCID: 0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl;
[3]*War Studies University, Poland, ORCID: 0000-0002-0778-0519,*
e-mail: j.nowicka@akademia.mil.pl;
[4]*John Paul II University of Applied Sciences in Biala Podlaska, Poland,*
ORCID: 0000-0003-3394-8992, e-mail: gisbourne2@gmail.com;
[5]*Warsaw Management University, Poland, ORCID: 0009-0004-8818-5691,*
e-mail: radoslaw.dawidziuk@mans.org.pl;
[6]*Warsaw University of Life Sciences, Institute of Economics and Finance, Poland,*
ORCID: 0000-0001-7317-7833; e-mail: katarzyna_gralak@sggw.edu.pl;

Findings: *The main conclusion drawn from the research material is that effective protection of the healthcare sector against cyberthreats requires a multifaceted approach, which includes investments in modern technologies, the implementation of legal regulations, and raising cybersecurity awareness among medical personnel.*
Practical implications: *The study results are of significant importance for organizations in the medical sector. Health must be protected, and awareness of cyberthreats among medical staff should be raised. Those responsible for the security of systems face a major task not only to properly secure data but also to respond effectively when problems arise.*
Originality / value: *This paper examines the impact of cyberthrets on the healthcare sector as a part of critical infastructure. It identifies specific risks of cyberattacts on healthcare institution and offers practical solutions to enhance the sector's cybersecurity resilience.*

Keywords: *Cybersecurity, healthcare, cyberthreats, ransomware, critical infrastructure*

JEL codes: *I18, L86, O33, D80.*

Paper type: *Research article.*

1. Introduction

The contemporary economy is based on modern digital technologies that enable the automation of processes, optimization of services, and improvement of the functioning of key sectors. The healthcare sector, as one of the most important areas of critical infrastructure, uses advanced IT systems to manage patient data, conduct diagnostics, and coordinate treatment. However, growing digitization also brings serious challenges related to cybersecurity.

Cyberthreats such as ransomware attacks, data theft, and disruptions to medical system operations pose a real risk to patient safety and the stability of the healthcare sector. Medical facilities, which are frequent targets of cybercriminals, are often inadequately prepared to effectively defend against such attacks. This leads to serious consequences including data loss, interruptions in hospital operations, and even threats to patients' lives (Makuch and Guziak, 2021, p. 91).

The purpose of this article is to demonstrate the impact of cyberthreats on the security of critical economic sectors, with a particular focus on the healthcare sector. Key threats, their consequences, and strategies for countering cyberattacks will be discussed. The article will also present examples of real incidents as well as possible scenarios for the development of security measures in the future.

2. Characteristics of Cyberthreats in Key Economic Sectors

Contemporary economic sectors increasingly rely on digital technology, which brings numerous benefits such as process automation, improved communication, rapid access to data, and enhanced management efficiency. However, alongside

advancing digitalization, the risk of cyberattacks also grows (Żurawski and Ciekanowski, 2023, p. 13), potentially causing serious disruptions in the operations of enterprises and institutions.

It is worth noting the growth dynamics of individual economies, where most do not exceed 3%, while cybercrime shows a 15% year-on-year increase, which means that in 2025 the world will face a "bill" exceeding 10 trillion dollars (OVERSEC, 2025). Figure 1 is a comparison of the GDP of the world's largest economies, Poland, and cyberthreats.

Figure 1. *Cybercrime as the world's third largest economy*

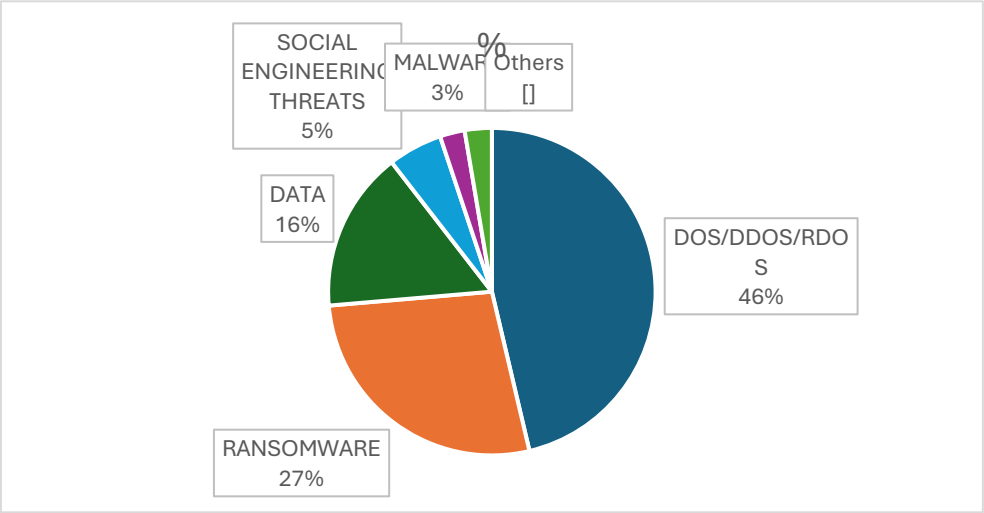
Source: *Cybercrime as the world's third largest economy – Oversec. https://oversec.pl/cyberprzestepczosc-trzecia-co-do-wielkosci-gospodarka-swiata/*

Critical sectors such as energy, finance, transport, and healthcare are particularly vulnerable to cyberthreats because their operations are crucial for socio-economic stability (Ciekanowski, Gruchelski, Nowicka, Żurawski, and Pauliuchuk, 2023, p. 790). Cybercrime takes various forms, with the most commonly used attack methods including ransomware, phishing, DDoS (Distributed Denial of Service) attacks, and advanced social engineering techniques.

Ransomware attacks involve encrypting the victim's data and demanding a ransom for its recovery. This is one of the most dangerous types of cyberattacks (Połowin, 2024, p. 124) because it can completely paralyze an organization's operations, which in the case of critical infrastructure can have catastrophic consequences.

Phishing attacks rely on manipulating users through fake emails or websites to steal authentication data, potentially leading to unauthorized access to IT systems. DDoS attacks overwhelm servers and systems with a massive number of simultaneous requests, causing temporary or permanent shutdowns. As shown in Figure 2, ransomware and DDoS remain the two main threats to the EU.

Figure 2. *Share of number of threats in the EU according to threat group.*



Source: *ENISA Threat Landscape 2024.*

A particularly concerning phenomenon is the rise in advanced, targeted attacks known as APTs (Advanced Persistent Threats). These threats are often carried out by well-organized cybercriminal groups or state-sponsored actors, aiming at long-term infiltration of organizational systems to steal data, conduct economic espionage, or sabotage. In sectors like finance or the energy infrastructure, such attacks can lead to massive financial losses and threaten economic stability.

One of the sectors that has become particularly attractive to cybercriminals in recent years is the healthcare sector. Medical facilities store vast amounts of sensitive patient data, including health status information, treatment histories, test results, and financial data. Additionally, hospital systems are often integrated with networks of medical devices such as CT scanners, ECG machines, and infusion pumps, which increases the attack surface.

Since the operation of medical facilities directly affects patients' health and lives, cyberattacks on this sector can lead to especially dangerous consequences, such as treatment delays, diagnostic errors, or even direct threats to life. Moreover, sensitive elements of identity, such as electronic identity documents, electronic health records, e-prescriptions, and medical leave certificates containing sensitive personal data, are also at risk (Billewicz, 2014, p. 1-2).

It is also worth noting that the healthcare sector often struggles with the problem of outdated IT infrastructure and insufficient security measures. Many facilities use software that is not regularly updated, which makes them vulnerable to attacks. Moreover, healthcare workers, although highly trained in medicine, often lack

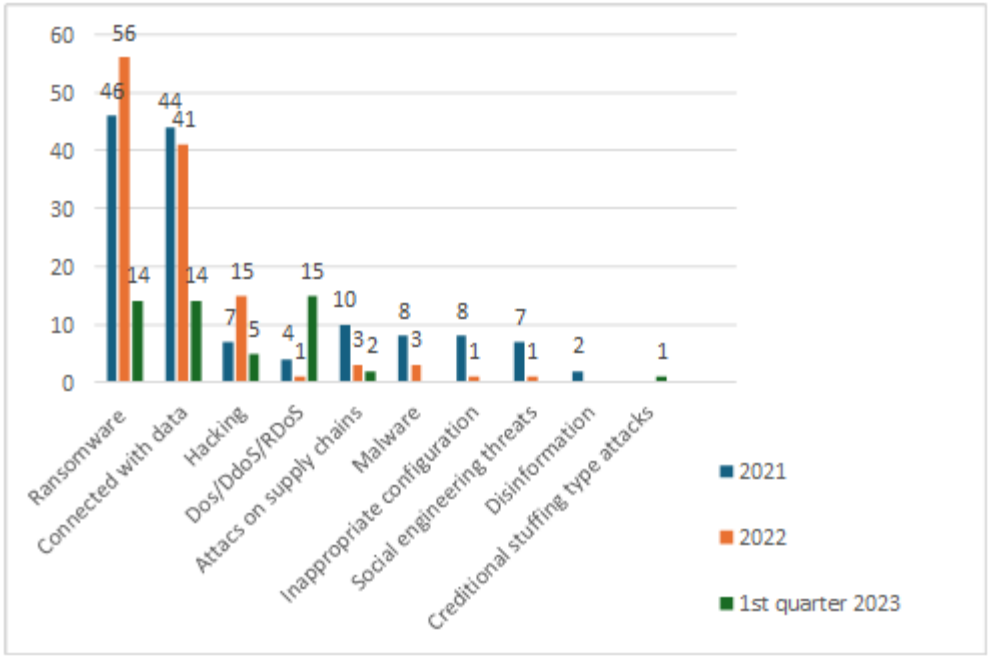
sufficient knowledge in cybersecurity, which increases the risk of successful phishing attacks or other forms of social engineering.

Cyberthreats pose a serious risk to many sectors of the economy, but they are particularly dangerous for the healthcare sector, where the effectiveness of IT systems has a direct impact on human lives. In the following sections of the article, specific cases of cyberattacks on medical facilities will be analysed in detail, along with strategies aimed at increasing the resilience of IT systems in healthcare.

3. The Influence of Cyberattacks on the Health Sector

Cyberattacks on the healthcare sector represent one of the most serious threats to patient safety and the stability of medical facilities. In 2024, approximately 15-18% of all cyberattacks worldwide targeted the healthcare sector (Businessinsider, 2025). These attacks can lead to the loss or leakage of confidential data, disruption of hospital system operations, and in extreme cases, even threaten patients' lives. Due to the increasing reliance of hospitals and other medical institutions on digital systems, the effectiveness and scale of cyberattacks in this sector have significantly increased in recent years. The types of attacks in healthcare are illustrated in Figure 3.

Figure 3. *Types of Attacks On the Health Sector.*



Source: *ENISA Threat Landscape 2023.*

One of the most destructive types of attacks in healthcare security are ransomware attacks. They involve encrypting an institution's data and demanding a ransom for its decryption (Guziak and Ziarnik, 2024, p. 112).

In the case of medical facilities, this means a complete shutdown of IT systems, resulting in halted access to medical records, patient data, test results, and surgery schedules. Without access to this information, medical staff may face serious difficulties in providing proper patient care, which can lead to incorrect diagnoses, treatment delays, and even life-threatening situations.

An example of such an incident is the ransomware attack on a German hospital in Düsseldorf in 2020, which led to the death of a patient. Due to the paralysis of the hospital's systems, a woman in an emergency condition was redirected to another facility, which significantly extended the time it took for her to receive assistance (Securak, 2025).

It was one of the first cases where a cyberattack was directly linked to the loss of a patient's life. There is also no shortage of attacks on hospitals in 2025. Hospitals and a university in Taiwan fell victim to a new group of cybercriminals.

The incident was caused by the "Crazyhunter team" which, so far, has listed five organizations from Taiwan (cyberdefence24.pl). In Poland, similar incidents have also occurred, such as a cyberattack (cyberdefence24.pl) on the MSWiA Hospital in Krakow. Protecting patient data is a key aspect of cybersecurity in healthcare.

Medical facilities store highly valuable information like personal data, medical history, test results, and financial details, which cybercriminals can exploit for identity theft, financial fraud, or blackmail. One of the largest healthcare data breaches occurred in 2015 when the American company Anthem was attacked, exposing data of 78.8 million patients.

The leaked information included social security numbers, addresses, medical data, and other sensitive details, putting victims at risk of identity theft and financial fraud (CEO, 2025). Such incidents highlight the critical importance of properly securing healthcare databases. Lack of adequate security measures-such as data encryption, monitoring systems for suspicious activities, and access controls based on least privilege can lead to catastrophic consequences (Tyagi *et al.,* 2023).

Modern hospitals and medical facilities increasingly use network-connected devices (IoT), such as infusion pumps, patient monitors, ventilators, and surgical robots. Cybercriminals can take control of these devices, causing disruptions in their operation or manipulating data, which can lead to treatment errors.

In 2017, security researchers demonstrated that it was possible to take control of an insulin pump and alter the insulin dosage delivered to a patient, which in extreme cases could lead to death.

Additionally, cybercriminals can exploit poorly secured IoT devices as entry points into a hospital's broader IT infrastructure, enabling them to launch attacks on data storage systems or communication networks. Insufficient access control for devices and a lack of regular security updates increase the susceptibility of medical facilities to such threats.

Cyberattacks on the healthcare sector pose a serious threat to patient safety, the stability of hospital systems, and the protection of medical data (Nawrocki, 2021, p. 108). Cases of ransomware attacks, data breaches, and disruptions to medical devices highlight the critical need to implement effective cybersecurity strategies. The next section of the article will discuss risk mitigation methods, as well as modern technologies and procedures to enhance the healthcare sector's resilience against cyberthreats.

4. Strategies for Counteracting Cyberthreats and the Future of Cybersecurity in Healthcare

In light of an increasing number of cyberattacks targeting the healthcare sector, implementing effective cybersecurity strategies becomes critical (Zamroczyńska, 2021, p. 39). Appropriate protective measures can minimize the risk of incidents, safeguard sensitive patient data, and ensure the operational stability of medical facilities.

A strategy to counter cyberthreats should encompass technological, organizational, and regulatory aspects. In the future, automation, artificial intelligence, and innovative security solutions will play an increasingly vital role in protecting medical systems (Javaid *et al.,* 2023).

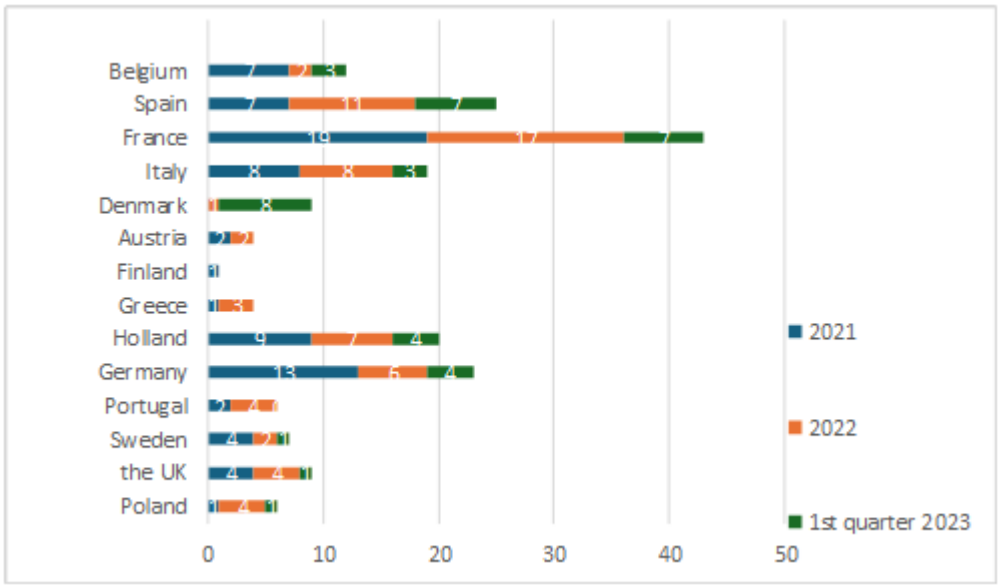
One of the key actions in cybersecurity is the proper protection of IT infrastructure and the regular updating of information systems. Medical facilities often use outdated software that lacks the latest security features, making them vulnerable to attacks.

Implementing modern protection systems such as firewalls, data encryption, and advanced intrusion detection mechanisms allows for more effective counteraction against cyberthreats. Moreover, it is essential to train medical staff in cybersecurity because human errors are one of the most common causes of successful attacks. Employees should be aware of risks related to phishing, social engineering, and using weak passwords. Regular training helps develop appropriate habits and increases the organization's resilience to cyberattacks (Velinov *et al.,* 2023).

Patient data protection also requires the application of the principle of least privilege and strict access control to medical systems. Healthcare facilities should implement multi-factor authentication and limit the number of individuals with access to critical information.

Restricting user privileges minimizes the risk of unauthorized data access and reduces the impact of potential attacks. Equally critical is the creation of regular system backups and the development of effective contingency plans. In the event of a ransomware attack or other cyber incident, the ability to quickly restore access to data can prevent serious disruptions to medical facilities. Figure 4 illustrates cyber incidents in healthcare across European countries.

Figure 4. *Cyber incidents in healthcare in European countries*

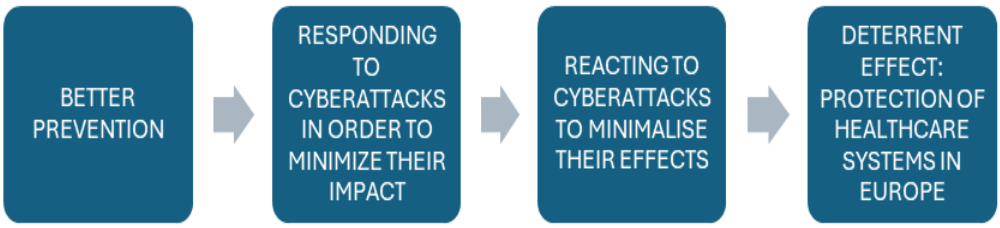


Source: *ENISA Threat Landcape: Health Sector 2023, p. 9*

In 2023, CSIRT NASK handled 2,184 incidents related to public entities. Among these, incidents classified as occurring within the healthcare sector accounted for 231 cases (CERT, 2023, p. 104). Hospitals were the most frequently targeted type of organization by cybercriminals within this sector. To counter these threats, the European Union is implementing initiatives aimed at securing the healthcare sector as a critical infrastructure element.

The new European strategy focuses on strengthening the resilience of medical systems, institutions, and connected medical devices against cyberthreats (KO, 2025). The goal of these actions is to ensure patient safety and increase their trust in modern digital technologies used in healthcare (Zalewska, 2021, p. 334). The European action plan is based on four priorities, which are illustrated in Figure 5.

Figure 5. *The four priorities of the European action plan.*



Source: *https://commission.europa.eu/cybersecurity-healthcare_pl.*

Besides technological and organizational measures, legal regulations play a significant role in ensuring cybersecurity. In the European Union, the GDPR regulation imposes on medical facilities the obligation to adequately secure patient data and to report any breaches within 72 hours.

In the United States, a similar role is played by the HIPAA Act, which sets standards for the protection of medical information and rules for its processing. With the development of cyberthreats, new regulations such as the NIS 2 Directive are increasingly important in ensuring security; this directive imposes additional requirements on healthcare facilities regarding the protection of IT systems and incident reporting.

The ENISA agency, analysing the development of the situation and the most common incidents since the beginning of the pandemic, recommends that the medical sector undertake a series of actions aimed at increasing resilience to cyberthreats. Below are some of the recommendations:

- first and foremost, it is important to systematically inform medical personnel about potential threats and to build their awareness regarding cybersecurity. In the event of detecting an attack, employees should immediately disconnect from the network to prevent further spread of malicious software;
- in the event of a system security breach, it is necessary to halt all ongoing operations within the system and isolate the infected devices both from other elements of the IT infrastructure and from external media or medical equipment. A crucial step is also to switch to offline mode and immediately contact the national cyber incident response team;
- medical facilities should also implement effective backup and system recovery procedures to quickly restore functionality in case of a failure. Business continuity plans should always be available, especially when a system failure could impact critical services provided by the hospital;
- in the event of a cyberattack on medical devices, it is essential to take action in close cooperation with their manufacturer. Collaboration with suppliers should include not only incident response but also the implementation of

appropriate protective measures for medical equipment and IT systems used in hospitals;

- the next important element of a cybersecurity strategy is the implementation of network segmentation, which allows for isolating and filtering network traffic. This enables effectively limiting or completely preventing unauthorized access to specific zones of the IT infrastructure, significantly increasing the protection level of medical systems against cyberattacks (Ezdrowie, 2025).

In the future, cybersecurity in the healthcare sector will increasingly rely on artificial intelligence (AI) and automation. Advanced machine learning algorithms will enable rapid detection of anomalies in network traffic and real-time identification of threats. Threat analysis systems will be capable of predicting potential attacks and automatically responding to suspicious activities before they cause serious damage.

Additionally, blockchain technology may play a key role in protecting patient data. Thanks to its decentralized structure, blockchain allows secure storage of information, minimizing the risk of manipulation and unauthorized access (Peve Herrera, Mendoza Valcarcel, Diaz, Herrera Salazar, and Andrade-Arenas, 2023).

Automation of incident management processes will become an essential element of cybersecurity strategy in the healthcare sector. Modern incident response systems will enable rapid identification and neutralization of threats, minimizing the time needed to restore system functionality.

Moreover, increasing attention must be paid to securing network-connected medical devices such as ventilators, infusion pumps, and patient monitoring systems. With the growing number of IoT devices in medical facilities, it will become necessary to introduce more stringent security standards and more effective methods of device authentication.

Many countries are already investing in the development of cyber incident response centres, which focus on threat monitoring, incident analysis, and supporting medical facilities in data protection. Thanks to international cooperation, it will be possible to more effectively counter cyberthreats and exchange information about new attack methods.

Cybersecurity in healthcare requires a multidimensional approach that includes technological, organizational, and regulatory measures. Effective protection against cyberattacks involves implementing modern security systems, training personnel, and complying with applicable legal regulations.

In the future, technologies such as artificial intelligence, blockchain, and automated incident response systems will play an increasingly important role in ensuring security. Through a comprehensive approach, the healthcare sector can effectively

minimize the risk of attacks and provide patients with safe and uninterrupted medical care.

5. Conclusions

Cyberthreats in the healthcare sector represent one of the greatest challenges of the modern world, and their consequences can be catastrophic both for patients and the stability of medical facilities. With ongoing digitalization, the number of attacks is increasing, which can lead to disruptions in hospital operations, theft of sensitive data, or takeover of medical devices.

Analysing current threats and past incidents shows that the healthcare sector requires a comprehensive cybersecurity approach, encompassing protective technologies, legal regulations, and staff education.

The analysis showed that one of the most common threats are ransomware attacks, which can effectively paralyze the operation of medical facilities and lead to delays in patient treatment. Equally serious is the problem of medical data leaks, which can be exploited for identity theft or blackmail.

Additionally, threats related to medical devices connected to the internet demonstrate that IT system protection in healthcare cannot be limited solely to securing databases – effective management of medical infrastructure and IoT devices is also necessary.

In the context of the future of the healthcare sector, implementing effective cybersecurity strategies is of key importance. There is an urgent need for further investment in modern protective technologies, such as artificial intelligence for threat monitoring and blockchain for secure patient data storage.

Medical facilities should also develop incident response procedures and implement network segmentation to limit the spread of malware in the event of an attack.

An important conclusion drawn from the analysis is also the necessity of continuously raising the awareness of medical personnel regarding cyberthreats. Educating employees is an essential element of effective protection against phishing attacks and social engineering, which often constitute the first step in gaining control over the healthcare facility's IT systems.

Legal regulations, such as GDPR and NIS 2, play a crucial role in ensuring the protection of patient data and medical systems; however, it is necessary to further adapt the regulations to the rapidly changing threat landscape. National authorities and international organizations should cooperate more closely to develop consistent cybersecurity standards for the healthcare sector.

In conclusion, while the healthcare sector is taking increasing measures to enhance cybersecurity, numerous challenges still require effective solutions. Continued investment in modern protective technologies, the development of security policies, and improved awareness among medical staff remain essential.

Only through a comprehensive approach can threats be effectively countered, ensuring patients receive secure and uninterrupted medical care in the digital era.

References:

Billewicz, K. 2014. Ochrona danych osobowych – teoria i fikcja. Wiadomości Elektrotechniczne, no. 7, pp. 12-15.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., Pauliuchuk, Y. 2023. Cyberspace as a Source of New Threats to the Security of the European Union. European Research Studies Journal, Volume XXVI, Issue 3, pp. 782-797.

ENISA Threat Landscape 2023.

ENISA Threat Landcape: Health Sector 2023.

Guziak, M., Ziarnik, K. 2024. Przegląd naruszeń cyberbezpieczeństwa danych medycznych w polskim sektorze ochrony zdrowia w 2023 roku. Rocznik Bezpieczeństwa Międzynarodowego, no. 2, vol. 18, pp. 109-123.

Javaid, M., Haleem, A., Pratap Singh, R., Suman, R. 2023. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, Volume 1, pp. 1-13.

Makuch, J., Guziak, M. 2021. Cyberbezpieczeństwo sektora ochrony zdrowia. Przypadek Polski na tle tendencji światowych. Rocznik Bezpieczeństwa Międzynarodowego, no. 2, pp. 86-102.

Nawrocki, S. 2021. Cyberzagrożenia w sektorze ochrony zdrowia, w tym w anestezjologii i ratownictwie. Charakterystyka wybranych zagrożeń i sposoby zapobiegania. Anestezjologia i Ratownictwo, no. 15, pp. 102-109.

Peve Herrera, C., Mendoza Valcarcel, J., Díaz, M., Herrera Salazar, J., Andrade-Arenas, L. 2023. Cybersecurity in health sector: a systematic review of the literature. Institute of Advanced Engineering and Science, pp. 1099-1108.

Połowin, A. 2024. Cyberzagrożenia w internecie – analiza przypadków. Cybersecurity and Law, 12(2), pp. 117-130.

Raport roczny z działalności CERT 2023.

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E.I. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

Velinov, E., Kadłubek, M., Thalassinos, E., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 147-158). Emerald Publishing Limited.

Zamroczyńska, M. 2021. Cyberbezpieczeństwo w ochronie zdrowia a udzielanie świadczeń telemedycznych. Medyczna Wokanda, no. 16, pp. 41-49.

Zalewska, E. 2021. Cyberbezpieczeństwo aparatury medycznej jako wspólne zadanie inżynierów klinicznych i specjalistów IT. Inżynier i Fizyk Medyczny, 10(4), pp. 333-335.

Żurawski, S., Ciekanowski, Z. 2023. Wpływ zagrożeń w cyberprzestrzeni na bezpieczeństwo państwa. In: Współczesne wyzwania dla bezpieczeństwa państwa, red. D. Brążkiewicz, J. Nowicka, Z. Ciekanowski, L. Elak, Wydawnictwo im. Prof. Leszka Krzyżanowskiego Menadżerskiej Akademii Nauk Stosowanych w Warszawie, Warszawa.

Online sources:

Amerykański ubezpieczyciel zaatakowany przez hakerów. https://ceo.com.pl/amerykanski-ubezpieczyciel-zaatakowany-przez-hakerow-42721.

Businessinsider. 2024. Prawie co piąty cyberatak skierowany w podmioty sektora zdrowia. Czego szukają tam hakerzy? https://businessinsider.com.pl/gospodarka/prawie-co-piaty-cyberatak-skierowany-w-podmioty-sektora-zdrowia-czego-szukaja-tam/ccf38cm.

Cyberbezpieczeństwo w sektorze opieki zdrowotnej - Komisja Europejska. https://commission.europa.eu/cybersecurity-healthcare_pl.

Cyberbezpieczeństwo w ochronie zdrowia – kluczowe dla zdrowia i życia pacjentów - ezdrowie.gov.pl. https://ezdrowie.gov.pl/portal/artykul/cyberbezpieczenstwo-w-ochronie-zdrowia-kluczowe-dla-zdrowia-i-zycia-pacjentow.

CyberDefence24. 2025. Pobrano z: CyberDefence24. https://cyberdefence24.pl/cyberbezpieczenstwo/szpitale-i-uniwersytet-na-tajwanie-ofiarami-nowej-grupy.

CyberDefence24. 2025. Pobrano z: CyberDefence24. https://cyberdefence24.pl/cyberbezpieczenstwo/zhakowano-szpital-mswia-w-krakowie-sluzby-wspieraja-placowke.

Oversec. 2025. Cyberprzestępczość trzecią co do wielkości gospodarką świata – Oversec. https://oversec.pl/cyberprzestepczosc-trzecia-co-do-wielkosci-gospodarka-swiata/.

Sekurak. 2025. Niemiecki szpital został zainfekowany ransomware. Pacjentka została przekierowana, a zbyt późna pomoc prawdopodobnie przyczyniła się do jej śmierci. https://sekurak.pl/niemiecki-szpital-zostal-zainfekowany-ransomware-pacjentka-zostala-przekierowana-a-zbyt-pozna-pomoc-prawdopodobnie-przyczynila-sie-do-jej-smierci/.