eauditor

Cybersecurity in the **medical industry**

Learn about actions ensuring an increase in the level of cybersecurity

1. DISCUSSION OF TRENDS AND ISSUES RELATED TO CYBERSECURITY

Cybersecurity is constantly evolving. Its changing nature, combined with high risks and weak protection, makes it highly uncertain. In theory, it should provide protection to users and computer systems, but increasingly, cybersecurity professionals are facing challenges.

The number of phishing attacks compared to the previous year has increased by 196%. Moreover, hackers are employing increasingly sophisticated methods, the consequences of which can impact business processes. Organizations not only lose trust but also significant amounts of money. For instance, a ransomware attack costs a Polish company an average of 1.5 million złotych.

196%

the number of attacks increased by 196%

1.5 million PLN

this is the average cost of a ransomware attack

3.5 million

a shortage of approximately 3.5 million cybersecurity specialists worldwide is a significant gap to fill

17,5 K

the shortage of around 17,5 K cybersecurity specialists in Poland is quite a substantial gap to address

In the face of an upcoming recession, entities are seeking ways to cut costs. Unfortunately, the budget for cybersecurity is often one of the first to undergo reductions. This leads to a decrease in expenditures on employment. Currently, there is a shortage of about 3.5 million cybersecurity specialists worldwide, and in Poland, the shortage is 17,500.

According to forecasts, in 2023, the number of attacks on critical infrastructure will increase. This implies that cybersecurity measures should be treated as a priority at both the national and organizational levels.

This year is likely to bring attacks on public and private healthcare facilities, government offices, and public institutions providing healthcare services. This will not only lead to chaos and financial losses but also have direct consequences for society, including a threat to human health and life.

[1] https://blog.sagenso.com/cyberbezpieczenstwo-w-2023-roku-prognozy-i-trendy, [accessed: 18.01.2023].

dr Adam Józefiok, assistant professor at the Silesian University of Technology, computer network administrator

www.linkedin.com/in/adamjozefiok

Firstly, we can expect a significant increase in attacks from Russia. Ransomware will lead the trend decisively. It's essential to note that the market for services related to hacking into IT systems is continually growing. Currently, there are 'companies' in the darknet offering subscription-based models, payable in bitcoins, allowing for programmed attacks on specific systems of particular enterprises. Undoubtedly, 2023 will be abundant in such attacks. The second challenge is the significant shortage of specialized personnel. At the beginning of last year, shortages were estimated at over 25,000 employees; unfortunately, the trend is not optimistic now. Another aspect is the considerable growth in attacks on IoT infrastructure and all cloud services. Specialized attacks will also increase, conducted not chaotically but precisely. The growing computational capabilities of computers allow for precise and impactful attacks. These attacks will primarily target the weaker points in the infrastructure. We are facing an open war for 'cyber positions,' especially concerning experienced employees with dozens of projects and thousands of hours at the console.

2. ANALYSIS OF THE CURRENT LEVEL OF CYBERSECURITY IN THE MEDICAL INDUSTRY

Hospitals and healthcare organizations are one of the main targets of cybercriminals. Healthcare organizations deal with a large amount of personal data, which is highly valuable to hacker groups. Almost all healthcare organizations are vulnerable to cybersecurity incidents. The question is not whether a particular facility will be attacked, but when it will happen.

Statistics don't lie: **89% of healthcare organizations** reported an average of **43 cyberattacks per year,** almost one attack per week[2]. From 2018 to 2021 alone, there was an **84% increase** in the number of breaches in the healthcare industry[3], and forecasts indicate that the number of attacks will continue to rise[4].

64% of healthcare organizations report feeling **threatened,** but **only 48%** of them have **a plan to counteract** this threat[5]. Alarmingly, **41% of healthcare organizations** that **haven't experienced** an attack yet **believe they will likely fall victim to cybercriminals in the future[6].**

3% of hospitals show a weak level, **63%** of hospitals show a moderate level, and only **20%** show a good or very good level of cybersecurity. Unfortunately, it is true that the level of cybersecurity in public medical facilities is determined by the hospital with the l**owest level of security.**

I think the biggest challenge for hospitals will be the amendment to the national cybersecurity system law (KSC/NIS2). This means that the healthcare system will be subject to new regulations. Independent public healthcare facilities will have obligations imposed on them by the EU directive and the mentioned national law, which should appear soon. In addition to the need to conduct a risk analysis and implement procedures, there will be a necessity to implement solutions to enhance the level of cybersecurity. Another challenge faced by entities in the healthcare sector is the lack of cybersecurity specialists (which is not unique to this industry). This increases the difficulty of implementing changes resulting from the new law.

Przemysław Kucharzewski, Managing Director,
a producer of cybersecurity solutions

www.linkedin.com/in/przemyslawkucharzewski

3. POTENTIAL THREATS AND RISKS FOR THE MEDICAL INDUSTRY

Incidents related to cybersecurity can pose a threat to network-connected medical devices and data systems crucial for the safe and effective delivery of healthcare. Consequences may include rescheduling appointments or surgeries, redirecting emergency vehicles, or even shutting down healthcare units and entire organizations. Insufficient security measures can also expose patients to serious risks.

A significant portion of incidents can be thwarted or their consequences minimized, but it requires the implementation of appropriate measures. Managing the cybersecurity risk in a healthcare environment is, however, challenging.

Responding to cyber threats necessitates a comprehensive security program to prevent attacks on critical devices and systems. Finding suitable professionals and IT staff also poses a challenge

[1] https://blog.sagenso.com/cyberbezpieczenstwo-w-2023-roku-prognozy-i-trendy, [accessed: 18.01.2023].
[2] https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/, [accessed: 18.01.2023].
[3] https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/, [accessed: 18.01.2023].
[4] Healthcare Cybersecurity Report Q4 2021, Herjavec Group, 2021.
[5] https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/, [accessed: 18.01.2023].
[6] https://expertinsights.com/insights/healthcare-cyber-attack-statistics/, [accessed: 18.01.2023].

4. CYBERSECURITY AS THE KEY TO PROTECTING THE MEDICAL INDUSTRY

Given the significant risks affecting the continuity of medical facilities, it's crucial to strive for risk minimization. A proper response can prevent potential threats from cybercriminals.

Based on the 6th edition of the "Study of the Level of Informatization of Entities Performing Medical Activity," we have prepared a set of guidelines that can significantly enhance the cybersecurity level in your hospital. The most commonly identified needs by surveyed institutions include resilience to cyberattacks (68.9%), increased protection of personal data (65.9%), and improvement of knowledge about IT threats among employees/management of the unit (59.4%).

What actions should be taken in this area?

1. enhance the resilience of IT infrastructure against cyberattacks	68,9%
2. ensure adequate protection of personal data of patients and employees	65,9%
3. increase awareness and knowledge about cybersecurity threats among employees	59,4%
4. improve the continuity of information systems	58,7%
5. raise awareness among employees and management about the risks associated with the use of systems	55,8%
6. enhance the protection of email used in the hospital	49,8%

Source: VI Edition "Study on the Degree of Informatization of Entities Performing Medical Activities 2022"

Maciej Kaczyński, Founder and CEO of BTC LLC, System Architect

www.linkedin.com/in/maciej-kaczyński

The key to ensuring IT security is the implementation of IT infrastructure management systems and data protection elements (DLP - Data Loss Prevention systems). While purchasing and implementing infrastructure management systems is relatively simple and quick, the development and implementation of security policies must be well thought out and properly planned. Too strict security policies will hinder the organization's operations, while too lenient policies will lead to vulnerability and apparent protection. The implementation time for DLP policies is relatively long and can take up to 10 months. The human factor is also crucial – without the right, stable IT team, effective security cannot be guaranteed. In Poland, we have many outstanding IT security specialists, often enthusiasts, who are worth engaging in such projects. And remember, there are no 100% effective safeguards, no systems that are perfect and flawless. But if we don't start implementing security assurance processes, we certainly won't be safe. That's for sure.

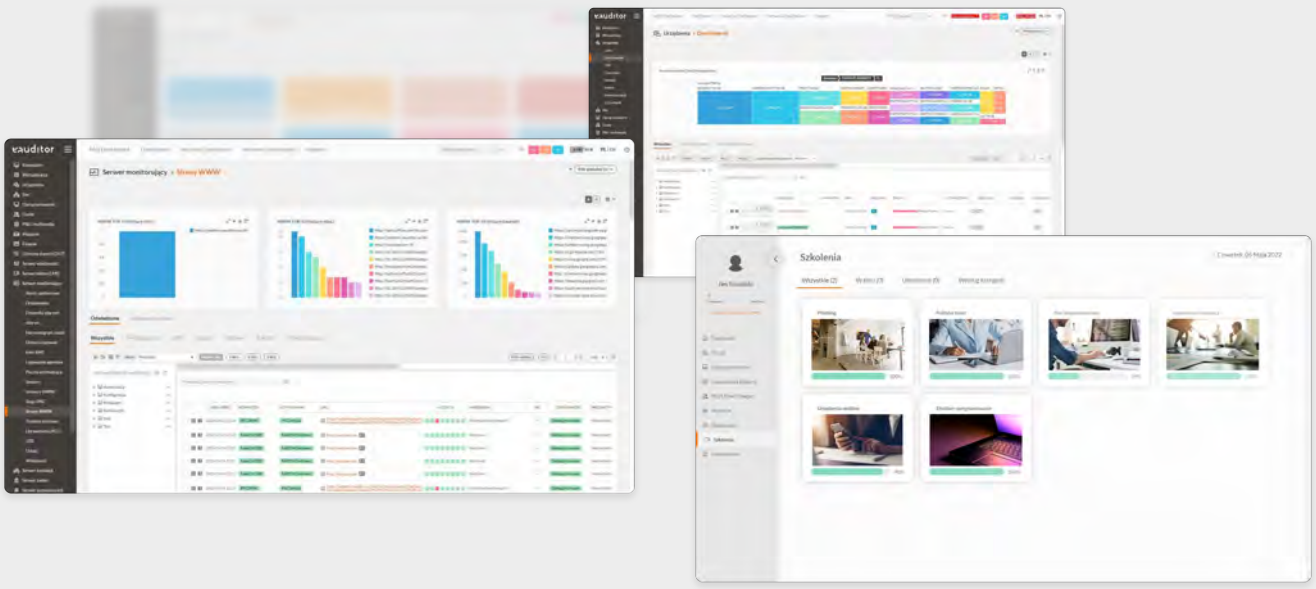
5. SOLUTIONS SUPPORTING THE INCREASE OF CYBERSECURITY LEVEL IN THE MEDICAL INDUSTRY

4 key actions that will ensure an increase in the level of cybersecurity in the medical industry:

- Implementation of advanced IT systems to ensure cybersecurity.
- Implementation of solutions aimed at encrypting data and monitoring user activities on company devices to protect against data loss.
- Educating employees through regular training and information campaigns to increase awareness of cybersecurity threats.
- Conducting security audits to identify infrastructure weaknesses and potential threats.

eauditor

A system ensuring the highest level of protection for medical data



Analysis of IT Security Key Indicators (SOC)

Remote and mass encryption of internal and external (USB) drives

Advanced DLP policies for comprehensive protection against data leaks

Regular training processes on IT security policies for medical staff

Mass blocking of unauthorized USB devices

Blocking access to websites (BTC Website Classification) and running processes (BTC Process Classification)

Visit our website **eauditor.eu**

WHAT AREAS DOES THE EAUDITOR SYSTEM SUPPORT?

Computer Management	Users	Device Monitoring	Security	Education and communication
Dashboard – information about IT infrastructure	Informaton o about online users	Time of turning on, turning off, or putting to sleep	Remote disk encryption (Bitlocker)	Remote employee training
Remote installation / uninstallation	Login and logout time	Computer location by IP (computer behind NAT)	BitLocker USB encryption	Defining your own training materials
Remote desktop (RDP, RTC, VNC, UVNC)	Monitoring work (activity time, inactivity)	External USB devices connected	Blocking unauthorized external USB devices	Ready-made instructional videos on security
Remote management Intel VPro / AMT	Monitoring of launched applications	Monitoring and managing services	Blocking processes (HV)	Automatic communication with users
Remote configuration	Monitoring launched processes	Monitoring performance (RAM, HDD, CPU)	Blocking printers and printouts (HV)	Displaying urgent messages to users (Alert)
Remote restart	Monitoring printers and printouts	Monitoring event logs	Blocking launched websites	Displaying massages to users
Remote execution of CMD scripts (dozens built-in	Monitoring websites based on content (machine learning)	Employee process monitoring	Monitoring / blocking opened documents (HV)	
Remote execution of PowerShell scripts (dozens of built-in)	Monitoring outgoing email and attachments		Blocking access to unauthorized WIFI networks (HV)	
Technical support	Remote employee training and monitoring training progress		Monitoring and blocking access to cloud data storage (HV)	

Summary

The statistics are alarming: the number of cyber attacks on hospitals i**s growing and will continue to rise.** Healthcare organizations are projected to spend $125 billion on cybersecurity between 2020 and 2025[7]. These figures cannot be underestimated. While a strong preventive strategy and program will still be crucial, investing in cyber resilience is no longer an option but a true necessity.

[7] https://expertinsights.com/insights/healthcare-cyber-attack-statistics/, [accessed: 18.01.2023].

As cybersecurity experts highlight, **the primary defense against cyber attacks involves monitoring and raising user awareness about emerging variants of previously identified threats.** A collective system resilience approach proves to be the most effective way to thwart cybercriminals.

One avenue to establish an adequate level of cybersecurity in medical institutions is through the acquisition of an IT system. This approach not only serves as an efficient means to prevent cyber threats within IT infrastructure but also contributes to enhancing the overall organizational operational efficiency.

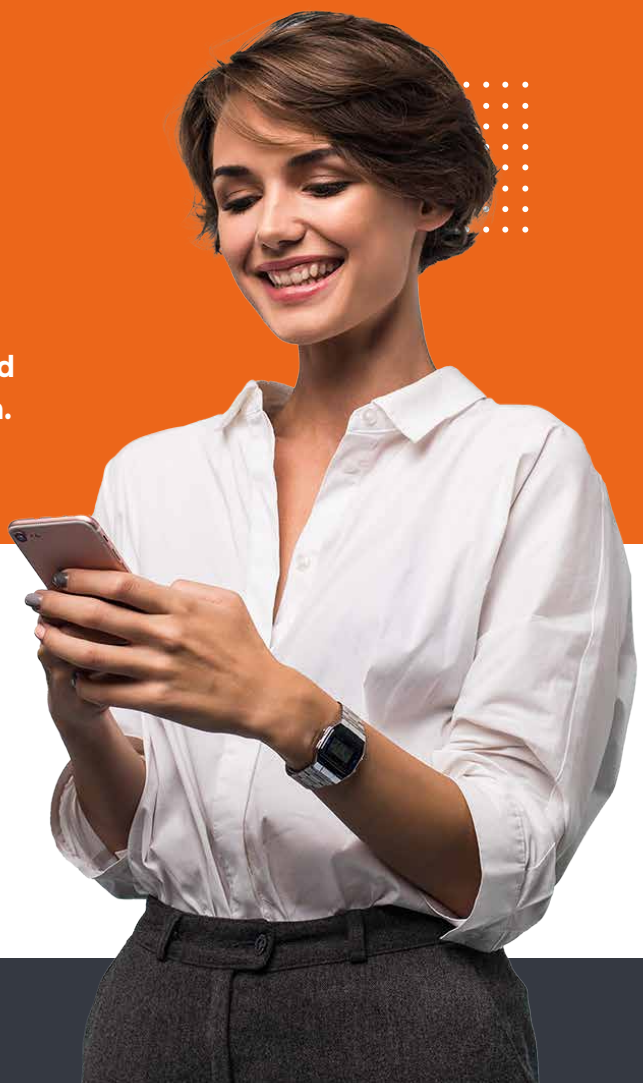
Currently, **the National Health Fund (NHF) is accepting applications for the implementation of teleinformatics systems** and associated services. This initiative seeks to bolster cybersecurity in medical facilities, with a focus on procuring IT software that meets essential requirements for ensuring a sufficient level of IT security.

Call for applications for the implementation of teleinformatics systems under the National Health Fund (NHF)

Application deadline:
October 31, 2023

Grant amount:
PLN 240,000 - 900,000

Do you want to learn more about how the eAuditor system works? **Fill out the form and schedule a free, no-obligation presentation.**



Contact

Form

info@btc.com.pl

+48 91 48 17 204