Mgr. Michal Černý
Police of the Czech Republic
National Counterterrorism, Extremism and Cybercrime Agency
Criminal Police and Investigation Service
Czech Technical University in Prague
Faculty of Biomedical Engineering
Ph.D. student
e-mail: michal.cerny@pcr.cz
ORCID: 0009-0002-1268-2187

Cybersecurity in Healthcare: Challenges and Recommendations

Kybernetická bezpečnost ve zdravotnictví: Výzvy a doporučení

Abstract

The article addresses current threats to cybersecurity in the healthcare sector, based on recommendations from the Czech Ministry of Health and NÚKIB. It focuses on real-life attacks, their impacts on healthcare facility operations, and measures to strengthen the resilience of hospitals and clinics. Special attention is given to staff training, password management, network segmentation, and data backup.

Keywords: cybersecurity, healthcare, ransomware, phishing, hospital, IT security.

Abstrakt

Článek se zabývá aktuálními hrozbami v oblasti kybernetické bezpečnosti ve zdravotnictví, přičemž vychází z doporučení Ministerstva zdravotnictví ČR a NÚKIB. Zaměřuje se na reálné útoky, dopady na provoz zdravotnických zařízení a opatření ke zvýšení odolnosti nemocnic a ordinací. Zvláštní pozornost je věnována školení personálu, správě hesel, segmentaci sítí a zálohování dat.

Klíčová slova: kybernetická bezpečnost, zdravotnictví, ransomware, phishing, nemocnice, IT bezpečnost.

Introduction

Cybersecurity in healthcare is a key area of growing importance, driven by the increasing volume of digitised medical data. Healthcare organisations, hospitals, and private practices are frequent targets of various cyberattacks, primarily due to the sensitivity of the information they store. Medical data rank among the most valuable commodities and their leakage can lead to serious legal as well as ethical consequences. This article focuses on current cyber threats, their potential impacts, and recommendations for strengthening cybersecurity in the healthcare sector.

According to the *"Kybernetická příručka pro lékaře" (Cybersecurity Handbook for Physicians),* published in 2023 by the Ministry of Health of the Czech Republic, the level of cybersecurity in general practitioner's offices and smaller healthcare facilities is largely insufficient. The handbook outlines a set of recommended security measures, including staff training, proper configuration of access rights, data backup, network protection, and physical security. Its objective is to provide physicians with practical guidance on protecting healthcare information systems and preventing cyber threats.[1]

Another important source used in this article is the document "*Doporučení poskytovatelům zdravotních služeb ke snížení kybernetických hrozeb" (Recommendations for Healthcare Providers to Mitigate Cyber Threats)*, published in 2022 by the National Cyber and Information Security Agency of the Czech Republic (NÚKIB), in cooperation with the Ministry of Health of the Czech Republic. The document was issued in response to cyberattacks associated with the armed conflict between the Russian Federation and Ukraine. NÚKIB recommends that healthcare organisations adopt preventive measures such as blocking suspicious network traffic, switching to isolated operating modes, warning employees about phishing attacks, and regularly testing their data backups.[2]

Healthcare is also explicitly addressed in *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (Act No. 181/2014 Coll., on cybersecurity)*, Section 2. The act defines healthcare as an essential service the provision of which depends on electronic communication networks or information systems and the disruption of which could significantly affect the security of social and economic activities. Section 2 thereof further defines the information system of an essential service as a system which the provision of the essential service depends on. This implies that healthcare organisations fall within the scope of the Cybersecurity Act, either as operators or as administrators and operators of essential service information systems. These entities are therefore obliged to implement organisational and technical measures to ensure cybersecurity.

Cybersecurity in healthcare thus represents not only a technological challenge but also a pressing issue of public health and national security. Attacks on hospitals and medical practices can have fatal consequences, including the postponement of surgeries, failures of electronic prescription (eRecept) systems, and the disruption of life-supporting medical devices. This article therefore analyses the most common cyber threats in healthcare and offers practical recommendations based on available methodologies, while aiming to update and expand upon them.

This study is based on a qualitative analysis of professional documents and legal regulations related to cybersecurity in healthcare. The primary sources include methodological materials published by the Ministry of Health of the Czech Republic

[1] MINISTERSTVO ZDRAVOTNICTVÍ. *Kybernetická příručka pro lékaře*. Online. 2023. Available from: https://www.lkcr.cz/doc/cms_library/prirucka-pro-lekare_v10-101802.pdf [cit. 2025-05-15].

[2] NÚKIB. *Doporučení ke snížení kybernetických hrozeb spojených se současným ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou*. Online. 2022. Available from: https://nukib.gov.cz/download/aktuality/2022-02-25_doporuceni-poskytovatele-zdravotnich-sluzeb-UkrajinaA.pdf [cit. 2025-05-15].

and the National Cyber and Information Security Agency (NÚKIB). In addition, case studies of actual cyber incidents in both the Czech Republic and abroad were examined. The legal framework is primarily derived from Act No. 181/2014 Coll., on cybersecurity. The methodological aim of this research was to summarise and assess current threats, describe the concrete impacts of cyberattacks, and propose validated preventive and reactive measures to strengthen the resilience of healthcare organisations.

Current Threats in Healthcare

Cyberattacks targeting healthcare organisations are becoming increasingly sophisticated, with diverse forms and far-reaching consequences that extend beyond financial losses.

In 2019, the Rudolf and Stefanie Benešov Hospital in the Czech Republic was struck by a ransomware attack that disabled its systems for several days, forcing the suspension of medical procedures. The hospital estimated damages exceeding CZK 59 million, with additional costs required for the implementation of a new security system, restoration of information systems, and staff training.[3]

Similar ransomware attacks were reported in hospitals and other healthcare institutions abroad, where they rendered patient electronic records inaccessible, resulting in postponed surgeries and significant disruption of healthcare services.[4]

Ransomware Attacks

One of the most severe cybersecurity threats in healthcare is ransomware. Ransomware is malicious software that, once it infiltrates the target device, restricts access to the system or encrypts user data in such a way that it cannot be restored without a specific decryption key. The attacker then leaves a ransom note demanding payment, usually in cryptocurrency, in exchange for the decryption key or for restoring access to the encrypted data. According to NÚKIB recommendations, maintaining a robust backup system and strong defences against phishing are essential, as phishing attacks often serve as the entry point for subsequent ransomware deployment.

The primary motivation of ransomware attackers is economic. Ransomware represents a form of digital extortion through which perpetrators coerce victims into paying a ransom. Although some attacks may have political, ideological, or destructive motives – such as those carried out by state-sponsored groups or hacktivists –majority of them are driven by the pursuit of quick financial gain. In this regard, ransomware constitutes one of the most effective tools of modern cybercrime.

[3] POLICIE ČESKÉ REPUBLIKY. *Středočeští kriminalisté ukončili vyšetřování Ransomware útoku na benešovskou nemocnici*. Online. 2020. Available from: https://policie.gov.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx [cit. 2025-05-05].

[4] AMERICAN HOSPITAL ASSOCIATION. *Ransomware Attacks on Hospitals Have Changed*. Online. 2020. Available from: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed [cit. 2025-05-06].

Today, ransomware has evolved into a highly sophisticated threat frequently operated within organised groups.[5] The criminal business model known as Ransomware-as-a-Service (RaaS) allows attackers without advanced technical expertise to exploit malicious tools provided by professionals, in exchange for a share of the ransom—typically 20–25 %, as revealed in leaked documentation from the LockBit 3.0 RaaS Affiliate Program. The ransomware economy is based on low operational costs and high returns. This model fosters an extensive criminal ecosystem in which ransomware developers, distributors, and operators are interconnected within an illicit cyber industry. The combination of low entry costs, anonymous financial systems, and global reach makes ransomware highly attractive to both individuals and organised crime groups.[6]

Phishing and Social Engineering

Phishing and social engineering rank among the most common and effective attack vectors in healthcare. Attackers employ manipulative tactics to obtain sensitive data or to install malware within healthcare systems. These methods are particularly dangerous because they do not require advanced hacking techniques, while they rely on exploiting human error instead.

Social engineering exploits psychological vulnerabilities to circumvent security measures. In healthcare, victims may include physicians, nurses, IT staff, or administrative personnel. Hospital and clinic employees must therefore be trained to recognise such attacks, while IT departments should deploy advanced security technologies. Prevention remains the key to safeguarding healthcare systems and sensitive patient information.

The psychological dimension also plays a role in the initial stages of ransomware distribution, which frequently relies on social engineering techniques. Emails with malicious attachments, links to fraudulent websites imitating trusted services, or personalised spear-phishing messages exploit human trust and inattention. These attacks are often carefully planned, highly targeted, and extremely effective – frequently determining whether the cyberattack will succeed.[7]

DDoS Attacks

A Distributed Denial of Service (DDoS) attack overwhelms the hospital network or web server with massive volumes of illegitimate traffic, rendering them unable to

[5] Cyber-attacks. Online. In: *EU Serious and Organised Crime Threat Assessment*. Europol, 2025, p. 38–41. ISBN 978-92-9414-000-5 Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [cit. 2025-05-22].

[6] Sizing up the ransomware ecosystem. Online. In: *The 2023 Crypto Crime Report*. Chainalysis, 2023, p. 30. Available from: https://hkibfa.io/wp-content/uploads/2023/02/Crypto_Crime_Report_2023.pdf [cit. 2025-05-18].

[7] Cyber-attacks. Online. In: *EU Serious and Organised Crime Threat Assessment*. Europol, 2025, pp. 38–41. ISBN 978-92-9414-000-5 Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [cit. 2025-05-22].

operate normally.[8] While this type of attack does not involve data theft, it causes system outages that can severely impact both patients and staff. DDoS attacks typically leverage botnets – networks of compromised devices, IoT equipment, or servers – remotely controlled by attackers to flood the target infrastructure with requests.

Layer 3/4 (network and transport layer) attacks overload hospital networks with large volumes of packets, disrupting internet connectivity. Layer 7 (application layer) attacks target specific services, such as hospital web portals or database servers. DNS-based attacks prevent hospitals from accessing online services and may redirect patients to fraudulent or spoofed websites.

By overwhelming servers with illegitimate traffic, DDoS attacks can cripple access to healthcare systems and paralyse the delivery of essential medical services.

Data Breaches and Misuse of Access Privileges

Unsecured information systems may be exploited not only by external attackers, but also by insiders. Weak passwords, the absence of multi-factor authentication (2FA), or improperly configured access rights represent common vulnerabilities.

Data breaches in healthcare constitute another critical cyber threat, as hospitals, clinics, and private practices store highly sensitive personal and medical information. Such data is extremely valuable to malicious actors, who can monetise it, exploit it for fraud, or use it for extortion against patients or healthcare providers.

Recommendations for Ensuring Cybersecurity

Based on the handbook of the Ministry of Health of the Czech Republic and the recommendations of NÚKIB, several measures have been identified to strengthen cybersecurity in healthcare.

Staff Training

The human factor remains the weakest link in cybersecurity. Physicians, nurses, and administrative personnel should undergo regular cybersecurity training. One recommended resource is the online course *"Stay Cyber-Safe! Basics of Cybersecurity"* published by NÚKIB.[9]

Case studies show that the majority of cyber incidents are caused by human error – whether through accidentally clicking a malicious link, using weak passwords, or carelessly sharing sensitive information. Healthcare staff are often prime targets for attackers, given their access to critical data.

Regular cybersecurity training raises awareness of current threats, reduces the likelihood of human error, and enhances the protection of sensitive data against

[8] Distributed Denial of Service. Online. In: *EU Serious and Organised Crime Threat Assessment*. Europol, 2021, p. 41. ISBN 978-92-95220-22-5. Available from: https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021 [cit. 2025-05-22].

[9] NÚKIB. "*Dávej kyber!*". Online. 2025. Available from: https://osveta.nukib.gov.cz/course/view.php?id=221#section-11 [cit. 2025-07-19].

unauthorised access. Employees also develop safe IT practices that help minimise security incidents. Repeated training additionally increases preparedness for unexpected crisis situations. As an extension of these preventive activities, beyond the recommendations included in the analysed documents, it is advisable to conduct simulated cyberattacks (e.g., testing with fake emails or SMS messages to evaluate staff responses). Such exercises prepare personnel to respond appropriately and help minimise potential damage.

Password Management

Passwords form the first line of defence against unauthorised access to healthcare information systems. Unfortunately, weak or reused passwords remain among the most common security vulnerabilities.

In healthcare, secure authentication is paramount, as the leakage of patient data can have fatal consequences. Medical records contain valuable personal information that can easily be misused for identity theft, fraud, or extortion against patients and healthcare institutions.

The *Cybersecurity Handbook for Physicians* published by the Ministry of Health of the Czech Republic emphasises the correct configuration and management of passwords to minimise the risk of unauthorised access to sensitive data.

Common Password Mistakes

- Use of weak passwords – Common choices include short, easily guessed passwords such as “123456”, “password”, or “admin123”.
- Reusing the same password across multiple accounts – Employees often use a single password for both professional and personal accounts, significantly increasing the risk of compromise.
- Storing passwords in insecure locations – Writing down passwords on sticky notes or in notebooks poses a critical security risk.
- Sharing passwords among staff – Some practices use a single password for an entire team, preventing user identification and increasing the risk of unauthorised access.
- Ignoring multi-factor authentication (2FA) – When available, two-factor authentication should always be enabled.
- Using old or compromised passwords – Some systems still allow passwords previously exposed in data breaches and made publicly available on the dark web.

Recommended Characteristics of a Secure Password

- Unique for each system.
- At least 12–16 characters in length.
- Combination of uppercase and lowercase letters, numbers, and special characters (e.g., @, #, $).
- Should not contain personal information (e.g., name, date of birth, or hospital name).

- Should not be easily guessable (e.g., “Password123”).
- Use of multi-factor authentication (2FA) wherever possible.

In addition to the guidance contained in the analysed documents, the following preventive measures are further recommended:

- Password renewal during personnel changes – for example, when a key employee leaves, including the reset of administrator credentials for information systems.
- Password renewal following cyber incidents – after any security breach, access credentials should be reset as part of the organisation’s crisis management plan.
- Prohibition of shared passwords – each system must enforce unique user identities to ensure full accountability and auditability of access.

Securing Healthcare Information Systems

Healthcare information systems form the core technological infrastructure of medical institutions. Therefore, their protection must be a priority for every hospital, clinic, and private practice. These systems enable the management of patient records, medication orders, communication among physicians, access to laboratory results, and the issuance of electronic prescriptions (*eRecept*). Any disruption of their functionality may lead to serious health-related as well as economic consequences.

According to the *Cybersecurity Handbook for Physicians* and the recommendations of the NÚKIB, particular attention must be paid to security measures that protect healthcare systems against cyberattacks, insider threats, and technical failures.

Key Threats to Healthcare Information Systems

As mentioned above, ransomware is among the most dangerous cyber threats in healthcare. Phishing emails are one of the most common attack vectors. Attackers distribute fraudulent messages that appear to originate from trusted institutions, such as a hospital’s IT department or the *Ministry of Health of the Czech Republic*. These emails often contain malicious attachments or links to fraudulent websites prompting users to enter login credentials or download infected files. Once an employee clicks a malicious link or opens an infected attachment, ransomware can spread across the hospital network and encrypt sensitive data.

Many healthcare institutions continue to rely on outdated operating systems and unpatched software containing exploitable security vulnerabilities. Hackers can exploit these known weaknesses if systems are not regularly updated with security patches. For example, attackers may take advantage of improperly configured Remote Desktop Protocol (RDP) access or deploy exploit kits that automatically search for vulnerabilities. Once ransomware is installed, it can rapidly spread across the hospital’s network and infect connected systems.

Another common vector of attack involves infected USB drives, external hard drives, or laptops connected to hospital networks. Attackers may deliberately leave compromised USB devices in public areas such as reception desks, anticipating that staff will connect them to workstations. Once connected, the ransomware activates automatically and begins encrypting data.[10] This type of attack is particularly dangerous in clinics and hospitals where shared workstations are common.

Attackers may also compromise legitimate healthcare websites or create fraudulent sites resembling official portals. When employees access such sites, malware can be automatically downloaded to their devices without any user interaction. This technique, known as a *drive-by download attack*, exploits vulnerabilities in outdated browsers or plugins such as Java, Adobe Flash, or older versions of Microsoft Office.[11] Once installed, the ransomware spreads through the hospital system, attempting to infect as many devices as possible.

Ransomware can also infiltrate hospital systems through compromised third-party software. Attackers target healthcare software vendors, medical device providers, or cloud service operators that have access to hospital data. If a supplier's system is compromised, malware may enter hospital IT systems during updates or software installations. This type of attack is particularly dangerous, as it can simultaneously affect multiple healthcare institutions.

Hospitals and clinics frequently allow physicians and IT staff to access hospital systems remotely via RDP. If these connections are not adequately secured with strong passwords, multi-factor authentication (2FA), and restrictions to trusted IP addresses, they may become easy targets. Hackers can launch brute-force attacks to guess credentials or use stolen login data to gain unauthorised access. Once inside, attackers may manually install ransomware and trigger it to cause maximum disruption.

Based on the above, the main identified threats to healthcare information systems include ransomware, phishing and social engineering, unauthorised system access, unauthorised interference with IT systems or data carriers, outdated operating systems, and human error.

Data Backup

Data backup is a critical safeguard for protecting healthcare information systems against cyber threats such as ransomware attacks, technical failures, human error, and natural disasters. Healthcare organisations manage highly sensitive data, the loss or corruption of which could severely disrupt the provision of medical care and lead to significant legal and financial repercussions. Healthcare systems store large volumes of sensitive information that may be irretrievably lost due to technical malfunctions, hardware failures, fires, or user mistakes. Medical records possess long-term value, making their secure preservation essential.

According to recommendations from the Ministry of Health of the Czech Republic and NÚKIB, healthcare organisations should back up all key and critical systems and data, regularly test recovery capabilities, and ensure that backups are inaccessible to attackers. Cyberattacks on hospitals are not merely theoretical, they represent

[10] (UBC) UNIVERSITY OF BRITISH COLUMBIA. *The Hidden Dangers of Unknown USB Drives*. Online. 2025. Available from: https://privacymatters.ubc.ca/i-want/hidden-dangers-unknown-usb-drives [cit. 2025-07-19].

[11] BITDEFENDER. *What are drive-by download attacks and how do you prevent them?* Online. 2021. Available from: https://www.bitdefender.com/en-us/blog/hotforsecurity/what-are-drive-by-download-attacks-and-how-do-you-prevent-them [cit. 2025-07-19].

a tangible threat capable of paralysing entire institutions. Hackers often attempt to infiltrate hospital networks, delete or manipulate data, and thereby disrupt operations. For example, if a hospital or clinic lacks current backups during a ransomware attack, it may lose all patient records, potentially compromising medical care or even endangering patients' lives. Institutions are frequently forced into the dilemma of paying substantial ransoms or risking irreversible data loss. Regular data backups enable immediate restoration, preventing the interruption of operations, patient treatment, and overall healthcare delivery.

Critical systems and data that must be backed up include patient records (electronic health records, medical histories, diagnoses, and test results), hospital information systems (HIS, PACS, LIS, *eRecept*, *eNeschopenka*), as well as other essential systems without which healthcare facilities cannot function. In addition, financial and administrative data (billing, insurance records, supplier contracts), email communications and databases (employee information and correspondence), and server configurations with IT system settings should be backed up to ensure rapid recovery of hospital infrastructure after an attack.

An effective approach to data backup is the *"3-2-1 rule"*, which significantly minimises the risk of data loss. This principle entails maintaining three copies of backup data (one primary and two backups) stored on two different media (e.g., a local server and a cloud repository), with one copy kept offline. The offline backup ensures that even in the event of an online cyberattack, not all copies are compromised. A simple example of applying the 3-2-1 rule would be a hospital storing essential data on an internal server, saving a copy in an encrypted cloud repository, and maintaining an additional offline backup securely on an external drive.

It should be emphasised that backups are only useful if they can be reliably and quickly restored. Many organisations assume that having regular backups guarantees protection against data loss. Unfortunately, without systematic testing, backups may be incomplete, corrupted, or improperly stored – such problems are often discovered only in critical situations. For instance, if a hospital under ransomware attack attempts to restore data from untested backups, it may find that files are missing, damaged, or infected with the same malware as the primary system. Therefore, it is essential not only to regularly verify the backup process itself but, above all, to test the ability to restore data rapidly and completely.

Backups of critical systems should be tested at least once a month. Less critical data (e.g., older administrative records or archived documentation) should be tested at least quarterly. Following any major changes in IT infrastructure – such as software updates, server migrations, or security incidents – immediate verification of backup recovery is necessary. Regular testing can reveal critical errors that would otherwise remain unnoticed. Common problems include incomplete backups, corrupted or unreadable files, slow recovery speeds, missing encryption keys (which make data decryption impossible if lost), or malware-infected backups stored within compromised systems.

Therefore, testing backup recovery is not just a recommended practice, but an essential component of cybersecurity for healthcare organisations. Without regular verification, backups may prove unusable, incomplete, or infected, rendering institutions unable to protect vital data in the event of a cyberattack or system failure.

Every hospital should have a clearly defined backup testing plan to ensure rapid data recovery and uninterrupted healthcare service delivery.

Network Security

Ensuring network security in healthcare is essential for protecting sensitive data and maintaining uninterrupted operation of medical systems. Hospital networks typically rely on complex infrastructures that interconnect a wide range of devices, including hospital information systems (HIS), laboratory systems, electronic health records (EHR), medical Internet of Things (IoT) devices, mobile equipment, and even public Wi-Fi networks. Due to this high level of interconnectivity, they are prime targets for cyberattacks such as DDoS, unauthorised intrusions, malware, and phishing. Therefore, network security in healthcare must be carefully designed to safeguard critical data from attackers while ensuring smooth functioning of all connected systems. Healthcare organisations should combine technical measures, continuous monitoring, and staff training to minimise risks associated with network infrastructures.

One of the most important strategies is the segmentation of hospital networks. This approach helps to isolate sensitive systems from less secure devices and minimises the potential impact of a security breach. Key segments within a hospital network include:

- Hospital information systems, which represent a critical component and should only be accessible to authorised staff.
- Medical IoT networks (connected medical devices, patient monitors, infusion pumps, CT scanners), which must be properly secured since compromising them could endanger patient lives.
- Employee computers and mobile devices, which should be accessible exclusively to healthcare personnel and separated from critical databases.
- Public Wi-Fi networks for patients and visitors, which must be fully isolated from internal hospital systems to prevent attackers from exploiting open access points.

A good practice in network segmentation is the implementation of separate VLANs for different device categories, combined with strict firewall rules that permit communication only between explicitly authorised devices.

Use of Firewalls and Network Traffic Monitoring

Firewalls constitute the first line of defence against attacks originating from the internet. Hospitals should deploy advanced firewalls capable of managing network traffic and preventing unauthorised access. Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) assist in identifying suspicious network activity and blocking attacks before they can cause damage. A practical example is the implementation of a next-generation firewall (NGFW), which monitors traffic in real time and immediately blocks attempts at unauthorised access or malicious communication.

Securing Hospital Wi-Fi Networks

Hospital Wi-Fi networks must be properly secured to prevent unauthorised access to critical systems. Key measures include the implementation of WPA3 encryption for maximum connection security, prohibition of shared passwords (each employee should have unique login credentials), restrictions on unknown device connections (medical equipment and staff computers must be protected from patient or visitor access), and strict separation of staff and patient networks.

It is important to note, however, that many medical IoT devices and older client systems do not yet support WPA3 encryption, which makes a full transition currently unrealistic. Consequently, WPA3 encryption should be prioritised, but in cases where it cannot be implemented, at minimum WPA2-Enterprise with 802.1x authentication should be enforced.

Protection Against DDoS Attacks

In April 2014, the hacktivist group *Anonymous* launched a Distributed Denial of Service (DDoS) attack against the Boston Children's Hospital in the United States. The attack was motivated by the hospital's recommendation that a fourteen-year-old patient be placed under state custody, thereby removing her from her parents' guardianship. Members of *Anonymous* perceived this decision as a violation of the girl's personal rights and responded with a series of DDoS attacks targeting the hospital's network. As a result, other institutions connected to the same network – such as Harvard University – also lost internet access. The network outages lasted for nearly a week, during which some patients and healthcare staff were unable to use online systems to check appointments, test results, or other critical information. The hospital ultimately incurred costs exceeding USD 300,000 as a consequence of the attack.[12]

To minimise the risks associated with DDoS attacks, healthcare organisations are advised to employ cloud-based protection services (e.g., Cloudflare, Akamai), implement network traffic filtering and block suspicious IP addresses, and ensure sufficient network infrastructure capacity to withstand heavy traffic loads. The use of firewalls and continuous monitoring of network traffic is also recommended. Furthermore, cooperation with an Internet Service Provider (ISP) can play a crucial role in DDoS mitigation. ISPs are able to filter malicious traffic at the network level before it reaches hospital servers, reroute traffic through specialised anti-DDoS servers that eliminate illegitimate requests, and monitor network flows in real time to detect unusual attack patterns.

In the event of a DDoS attack, immediate measures must be taken to reduce potential damage. These include isolating critical systems and switching them to offline mode, if feasible; contacting the ISP to assist with filtering unwanted traffic; activating DDoS protection to reroute traffic through cloud-based mitigation servers; informing the IT department and initiating attack analysis as well as emergency response procedures. After the attack subsides, an audit should be conducted to assess and verify the extent of the damage. Finally, a comprehensive post-incident analysis should be prepared, including recommendations to improve the institution's security posture and readiness for potential future DDoS waves.

[12] (CIS) CENTER FOR INTERNET SECURITY. *DDoS Attacks: In the Healthcare Sector*. Online. C2025. Available from: https://www.cisecurity.org/insights/blog/ddos-attacks-in-the-healthcare-sector [cit. 2025-07-19].

Conclusion

Cybersecurity in healthcare represents a multidisciplinary challenge that integrates technological, organisational, legal, and ethical dimensions. With the growing digitalisation of healthcare services, medical institutions have become increasingly attractive targets for cybercriminals – primarily due to the high value of sensitive data and their reliance on digital systems. The most common threats include ransomware, phishing, DDoS attacks, misuse of access rights, and vulnerabilities arising from human error.

This article demonstrates that prevention constitutes a critical component of cybersecurity in healthcare organisations. Priority should be given to staff training, the management of strong passwords, regular data backups, network segmentation, and continuous monitoring and evaluation of network traffic. Equally essential are the secure configuration of IT systems, timely software updates, and the implementation of multi-factor authentication. The legal framework – most notably *Act No. 181/2014 Coll., on cybersecurity* – clearly defines the obligations of healthcare organisations and underscores the importance of healthcare as a provider of essential services.

Real-world case studies (e.g., the attacks on *Rudolf and Stefanie Benešov Hospital* and *Boston Children's Hospital*) illustrate that cyber incidents can have severe consequences for the provision of healthcare, resulting not only in financial losses, but also leading to direct threats to patient safety. Therefore, healthcare institutions should regard cybersecurity as an integral part of crisis management and as a strategic investment in ensuring operational continuity.

In conclusion, protecting healthcare information systems is not just a technical issue; it is a fundamental prerequisite for providing medical care safely, effectively and trustingly.

List of References

Legislation

Czech Republic. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Sbírka zákonů České republiky.*

Websites and Documents

MINISTERSTVO ZDRAVOTNICTVÍ. *Kybernetická příručka pro lékaře*. Online. 2023. Available from: https://www.lkcr.cz/doc/cms_library/prirucka-pro-lekare_v10-101802.pdf [cit. 2025-05-15].

NÚKIB. *Doporučení ke snížení kybernetických hrozeb spojených se současným ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou*. Online. 2022. Available from: https://nukib.gov.cz/download/aktuality/2022-02-25_doporuceni-poskytovatele-zdravotnich-sluzeb-UkrajinaA.pdf [cit. 2025-05-15].

POLICIE ČESKÉ REPUBLIKY. *Středočeští kriminalisté ukončili vyšetřování Ransomware útoku na benešovskou nemocnici*. Online. 2020. Available from: https://policie.gov.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx [cit. 2025-05-05].

AMERICAN HOSPITAL ASSOCIATION. *Ransomware Attacks on Hospitals Have Changed*. Online. 2020. Available from:

https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed [cit. 2025-05-06].

Cyber-attacks. Online. In: *EU Serious and Organised Crime Threat Assessment*. Europol, 2025, pp. 38–41. ISBN 978-92-9414-000-5. Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [cit. 2025-05-22].

Sizing up the ransomware ecosystem. Online. In: *The 2023 Crypto Crime Report*. Chainalysis, 2023, p. 30. Available from: https://hkibfa.io/wp-content/uploads/2023/02/Crypto_Crime_Report_2023.pdf [cit. 2025-05-18].

Cyber-attacks. Online. In: *EU Serious and Organised Crime Threat Assessment*. Europol, 2025, pp. 38–41. ISBN 978-92-9414-000-5. Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [cit. 2025-05-22].

Distributed Denial of Service. Online. In: *EU Serious and Organised Crime Threat Assessment*. Europol, 2021, p. 41. ISBN 978-92-95220-22-5. Available afrom: https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021 [cit. 2025-05-22].

NÚKIB. “*Dávej kyber!”*. Online. 2025. Available from: https://osveta.nukib.gov.cz/course/view.php?id=221#section-11 [cit. 2025-07-19].

(UBC) UNIVERSITY OF BRITISH COLUMBIA. *The Hidden Dangers of Unknown USB Drives*. Online. 2025. Available from: https://privacymatters.ubc.ca/i-want/hidden-dangers-unknown-usb-drives [cit. 2025-07-19].

BITDEFENDER. *What are drive-by download attacks and how do you prevent them?* Online. 2021. Available from: https://www.bitdefender.com/en-us/blog/hotforsecurity/what-are-drive-by-download-attacks-and-how-do-you-prevent-them [cit. 2025-07-19].

(CIS) CENTER FOR INTERNET SECURITY. *DdoS Attacks: In the Healthcare Sector.* Online. C2025. Available from: https://www.cisecurity.org/insights/blog/ddos-attacks-in-the-healthcare-sector [cit. 2025-07-19].

Mgr. Michal Černý (*1985)

The author of the article is a member of the Police of the Czech Republic, National Counterterrorism, Extremism and Cybercrime Agency of the Criminal Police and Investigation Service. He has been fully dedicated to investigating virtual currencies since 2018. He is currently a Ph.D. student at the Czech Technical University in Prague, Faculty of Biomedical Engineering.