WRITTEN BY

MICHAL ČÁBELA
Director, Risk Advisory | Cyber Risk
Deloitte Czech Republic

Deloitte.

ADDRESSING CYBER THREATS IN HEALTHCARE

In recent years, cyber-attacks have become more sophisticated, and cybercriminals are constantly finding new ways to exploit vulnerabilities in the IT systems of healthcare facilities. The rise of connected medical devices, such as pacemakers and insulin pumps, has created new entry points for attackers to gain access to healthcare networks.

These devices are often connected to the internet or hospital networks, making them vulnerable to attacks. Moreover, healthcare organizations are not immune to insider threats. Incidents can also be due to the intentional or unintentional actions of disgruntled employees or contractors with access to sensitive data. This makes it important for organizations to have robust security measures in place to prevent and detect insider threats.

Healthcare facilities must comply with a number of regulatory standards, such as the Cyber Security Act and the Health Insurance Portability and Accountability Act (HIPAA), which mandate the protection of patient data. Failure to comply with these regulations can result in large fines and legal action.

The importance of cybersecurity in healthcare cannot be overstated. The consequences of a cyber-attack can be devastating for the affected patients and the healthcare organization concerned. It is crucial for organizations to take proactive measures to safeguard their IT systems and protect sensitive data. Investment in cybersecurity is essential in the long run to prevent costly data breaches and reputational damage.

The EU has been working on strengthening cybersecurity across its member states in recent years. The NIS2 directive is a significant step towards achieving this goal. The directive aims to improve the overall level of cybersecurity of EU Member States by ensuring companies operating in essential sectors have a minimum level of cybersecurity in place. The NIS2 directive covers a wide range of sectors, including energy, transportation, finance, health, and digital infrastructure. The directive is intended to harmonize the approach to cybersecurity across the EU and ensure a consistent level of protection for citizens and organizations.

In the Czech Republic, the NIS2 directive will apply to approximately 6,000 companies from the second half of next year, in addition to the current 350 companies that are already required to meet the minimum cybersecurity requirements. This means that many organizations will need to reassess their current cybersecurity measures and make significant changes to comply with the new law.

The NIS2 directive requires companies to implement risk management and incident response plans, as well as technical and organizational measures to ensure the security of their networks and information systems. This includes the establishment of cybersecurity policies and procedures, regular vulnerability assessments, and the use of security tools and techniques to detect and prevent cyber threats. The new law will also require companies to report security incidents that could have a significant impact on their operations and the security of their customers' data. This means that companies will need to have processes in place to rapidly detect and respond to security incidents, and to report them to the relevant authorities.

> Investment in cybersecurity is essential in the long run to prevent costly data breaches and reputational damage.

To comply with the NIS2 directive, companies will need to make significant changes to their internal control systems, affecting the technical, process, and organizational aspects of IT management. This includes investing in new cybersecurity technologies, hiring cybersecurity experts, and implementing new policies and procedures to ensure compliance with the law. In addition to technical measures, healthcare organizations will also need to address the human factor in cybersecurity. This includes training employees on cybersecurity best practices and establishing clear policies and procedures for handling sensitive data.

Healthcare organizations are likely to be amongst the most affected as the NIS2 directive is implemented across the EU. The healthcare sector has traditionally lagged behind other industries as regards cybersecurity, making it an attractive target for cybercriminals. With the increasing digitization of healthcare, the amount of sensitive data being processed and stored electronically has grown exponentially, further increasing the potential impact of cyber-attacks.

Many healthcare organizations have already taken the first steps towards compliance and are working on differential analyses to understand the changes needed in the coming months. This includes identifying gaps in their current cybersecurity measures and developing a roadmap to achieve compliance.

To address the cybersecurity challenges facing healthcare organizations, it will be important to adopt a proactive approach to cybersecurity. This includes investing in new cybersecurity technologies, such as intrusion detection and prevention systems, firewalls, and data encryption tools. It also means establishing partnerships with cybersecurity experts and vendors to stay up-to-date with the latest threats and best practices.

The motivation for complying with these regulations is not just to avoid potential sanctions or reputational damage, but primarily to ensure the security of services provided to patients. Recent attacks on hospitals in the Czech Republic have shown the vulnerability of healthcare organizations to cyber threats. With the increasing number of cyber-attacks, investing in cybersecurity is becoming increasingly critical to mitigate risks and secure sensitive data.

In conclusion, the implementation of the NIS2 directive in the Czech Republic is a significant step towards improving cybersecurity. Healthcare organizations must act proactively to prepare for compliance with the new regulations and secure their IT infrastructure and patient data. By investing in cybersecurity, healthcare facilities can ensure the security of their services, avoid reputational damage, and maintain the trust of patients.