WRITTEN BY

BORIS KUČERA
Director
FIPRA Slovakia

SLOVAKIA'S DIGITAL INFRASTRUC-TURE

The recent cyberattack on the Geodesy, Cartography, and Cadastre Authority (UGKK) demonstrated how vulnerable the state's critical IT systems can still be. Whilst undoubtedly inconvenient, the attack did not present a direct threat to human lives. With acts of terrorism on the rise, we may not be so lucky the next time. How can we prevent this from happening?

In response to the evolving cyber threat landscape and in alignment with the European Union's Network and Information Security Directive 2 (NIS2), Slovakia enacted a comprehensive amendment to its Cybersecurity Act in November 2024. This legislative overhaul aimed to fortify the nation's cyber resilience through several key provisions.
Firstly, the scope of regulation was expanded as the amendment broadened the definition of essential services to encompass sectors beyond traditional critical infrastructures, including digital service providers and public administration entities. This expansion ensures that a wider array of organizations adhere to stringent cybersecurity standards.

Secondly, the amendment brought enhanced security obligations. Entities falling under the Act's purview are now mandated to implement robust security measures, conduct regular risk assessments, and establish incident response protocols. These obligations are designed to proactively mitigate potential cyber threats.

In order to streamline incident reporting, the amendment introduced standardized procedures for incident notification, requiring affected entities to report significant cybersecurity incidents to the National Security Authority (Národný bezpečnostný úrad, NBÚ) within 24 hours. This prompt reporting facilitates timely responses and coordination. Last but not least the amendment strengthened enforcement mechanisms. To ensure compliance, the amendment imposed substantial penalties for non-adherence, including fines and corrective measures.

RECENT CYBERATTACKS AND THEIR IMPLICATIONS

Despite legislative advancements, recent cyberattacks have exposed vulnerabilities within Slovakia's key state institutions, raising concerns about the adequacy of existing cybersecurity measures.

In early January 2025, Slovakia experienced a large-scale cyberattack originating from abroad on the Geodesy, Cartography, and Cadastre Authority (UGKK), leading to a complete shutdown of its information systems. This incident disrupted the management of land and property records, highlighting the susceptibility of critical national infrastructure to cyber threats.

Around the same period, Všeobecná zdravotná poisťovňa (VšZP), Slovakia's largest health insurance provider, suffered a cyber intrusion with the aim to obtain sensitive personal and medical data of millions of citizens.

PLANNED LEGISLATIVE CHANGES FOR 2025

According to the Plan of Legislative Tasks of the Government for 2025, another amendment of the Cybersecurity Act is planned for September this year to secure implementation of the new Cyber Resilience Act (CRA) of the EU adopted last October, which aims to strengthen cybersecurity across the EU, particularly in products with digital components. While it primarily targets manufacturers and suppliers of hardware and software, its provisions also have important implications for public institutions that rely on such technologies to operate essential services.

Public institutions rely heavily on software, hardware, and connected devices to deliver essential services such as healthcare, law enforcement, public administration, and infrastructure management. The Cyber Resilience Act impacts these institutions in several key ways.

CRA strengthens the security of public IT systems by enforcing secure-by-design principles, which means that the hardware and software used by government agencies have built-in cybersecurity protections. CRA will also bring increased responsibility in public procurement, whereby contracts will require compliance verification from technology providers. Also, risk assessments must be conducted before purchasing software and connected devices. Since public institutions often depend on external vendors for critical digital services (e.g., cloud computing, software applications, and IoT devices), the CRA ensures that vendors meet cybersecurity standards before their products can be used by government agencies. The CRA should also ensure faster response to cyber incidents. Under CRA, manufacturers must immediately notify customers, including public institutions, about security vulnerabilities and breaches in their products. This allows the government to take quick action to mitigate security risks (e.g., applying patches, isolating affected systems), improve incident response coordination and, as a result, reduce downtime and service disruptions caused by cyberattacks. The biggest challenges for public institutions in the implementation process will be the need to upgrade outdated systems to meet CRA security requirements, adapting the procurement processes to verify vendor compliance and providing the necessary training to employees to understand and implement CRA guidelines.

HOW CAN WE MITIGATE THE RISKS OF FUTURE ATTACKS?

Moving forward, we must focus on strengthening cybersecurity at every level of the public sector, ensuring that institutions responsible for critical infrastructure are resilient against sophisticated cyber threats. Investments in workforce training, public-private partnerships, advanced cybersecurity technologies, and robust incident response protocols will be key to protecting both government systems and citizens' personal data.

Additionally, public awareness and education must become a priority, as human error remains one of the most common causes of security breaches. Cyber hygiene campaigns and best-practice training for government employees will significantly reduce the risk of attacks.

Finally, Slovakia must continue to cooperate internationally with EU cybersecurity agencies, NATO cyber defense programs, and global security organizations to leverage shared intelligence and defensive strategies. Cyber threats do not recognize national borders, and a coordinated European approach to cybersecurity will be essential in ensuring Slovakia's resilience against future attacks.

In an era where cyber threats are increasingly sophisticated and state-sponsored cyber warfare is a growing concern, Slovakia's ability to proactively defend its digital infrastructure will be crucial for maintaining national security, economic stability, and public trust in government institutions. The progress made with recent legislative reforms is commendable, but the work is far from over. A long-term commitment to cybersecurity investment, innovation, and collaboration will determine how well Slovakia can safeguard its critical IT systems in the years to come.