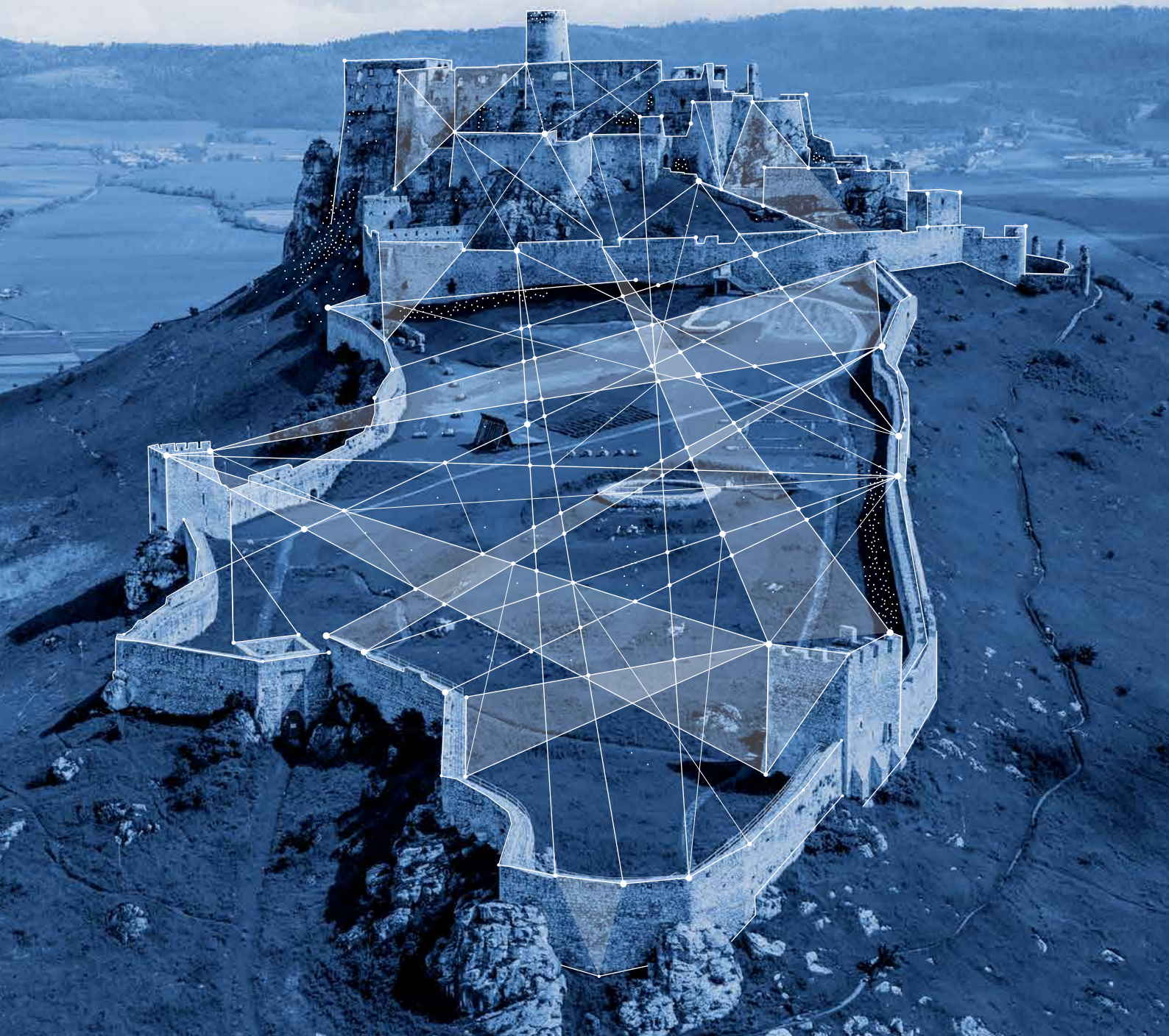
NATIONAL SECURITY AUTHORITY

CYBERSECURITY REPORT

in the Slovak Republic in 2023



NATIONAL SECURITY AUTHORITY

CYBERSECURITY REPORT

in the Slovak Republic in 2023

CONTENTS

1 OVERVIEW OF THREATS FOR 2023 6

1.1 Global Trends 6

1.2 The Most Significant Threats in the Slovak Republic for 2023 9

2 STATISTICAL OVERVIEW OF INCIDENTS FOR 2023 12

3 OVERVIEW OF THE STATE OF CYBERCRIME IN THE SLOVAK REPUBLIC FOR 2023 15

4 SECTORAL PERSPECTIVE 17

4.1 Sanctions 18

4.2 Audits and Self-Assessments 18

4.3 Banking 20

4.4 Transportation 22

4.5 Digital Infrastructure 24

4.6 Electronic Communications 26

4.7 Energy 27

4.8 Postal Services 29

4.9 Industry 29

4.10 Water and Atmosphere 31

4.11 Public Administration 32

4.12 Healthcare 37

5 IMPLEMENTATION OF THE ACTION PLAN FOR THE NATIONAL CYBERSECURITY STRATEGY FOR 2021 – 2025 40

6 ACTIVITIES AND MEASURES 41

6.1 National Legislation 41

6.2 European Union 42

6.3 NATO 44

6.4 Regional Cooperation 44

6.5 Bilateral Relations 45

6.6 Issuing Warnings and Bulletins 46

6.7 Cybergame 46

6.8 Raising Awareness Among the General Public 47

6.9 CSCCC Activities 47

1. Threat Overview for 2023

1.1 Global Trends

Several factors influenced the events in cyberspace in 2023. The cyber dimension of Russia's war against Ukraine remained prevalent, with the sophistication and intensity of cyberattacks not significantly diminishing. This military conflict continues to be a crucial element impacting combat operations, intelligence activities, and cybersecurity on both sides. The experiences gained from cybersecurity and defense in this conflict will serve as valuable lessons for the warring parties and others in the future.

Geopolitical rivalries between states in cyberspace were reflected in the espionage activities of several state-sponsored Advanced Persistent Threat (APT) groups. The United States and the United Kingdom repeatedly accused Russia and China of such malicious activities. State-sponsored groups from Iran and North Korea also remained active. The October attack by the terrorist group Hamas on Israeli civilian targets, followed by Israel's retaliation, was another instance where kinetic actions quickly transitioned into the cyber domain. Directly involved actors or allied groups conducted multiple DDoS campaigns and other malicious activities against both Israeli and Palestinian targets in connection with the aggression.

Cybercriminal activities were also a significant factor influencing the cyber landscape, with ransomware attacks continuing to surpass previous records in terms of the number of victims and financial damage.

1.1.1 SERVICE DISRUPTION

Disabling services through DDoS attacks remained a popular form of malicious activity among attackers with varying levels of knowledge and sophistication. The most frequent targets of this technique included EU and NATO institutions, critical infrastructure, banks, and large companies. Compared to previous years, 2023 saw a marked increase in the intensity of DDoS attacks. A new type of DDoS attack was also observed, which actively exploited vulnerabilities using the HTTP/2 Rapid Reset technique.

Hacktivist groups involved in Russia's war against Ukraine were among the most frequent users of DDoS attacks. These attacks were their primary agenda due to the relative simplicity compared to attempts to breach infrastructure. Their activities mirrored the developments in the Ukrainian conflict. On the Russian side, these activities targeted the infrastructure of states, particularly those supporting Ukraine, while on the opposite side, the targets primarily included Russian institutions.

The most active hacktivist groups included Anonymous Russia, DDoSia, NoName057(16), National Hackers Russia, Killnet, Revil, and Anonymous Sudan. These groups actively promoted their activities on social media, especially Telegram.

In such incidents, it is essential to distinguish between service unavailability caused by direct actor involvement and that caused by unforeseen events. In the case of service disruption, it often occurs due to unforeseen circumstances, such as failed updates, power outages, etc.

1.1.2 RANSOMWARE

The year 2023 was marked by an increase in ransomware attacks, significantly impacting the operations of institutions, companies, and individuals. In this area, professional gangs providing Ransomware as a Service (RaaS) were predominant. Ransomware gangs continued to improve their methods and tools, for example, by speeding up data encryption and streamlining data exfiltration processes.

The ability to carry out ransomware attacks is expanding, partly due to the increasing number of RaaS providers. Leaks of source codes from well-known ransomware groups enable new actors to easily modify and adopt proven tools. Additionally, leaks of ransomware attack manuals allow attackers to increase their efficiency.

The primary vectors for system and device breaches remain credential leaks (directly into infrastructure, services, or VPNs), obtaining access credentials through social engineering, security vulnerabilities, and system misconfigurations, as well as deploying malicious code via phishing activities.

Security forces also achieved success by dismantling several cybercriminal groups through international cooperation, including LockerGoga, MegaCortex, HIVE, and Dharma ransomware.

1.1.3 PHISHING

The motivation for attackers to engage in phishing activities can be divided into two categories. The first involves obtaining sensitive data, which is then sold to third parties. The second category is conducting phishing activities to spread malware, which ultimately may also serve to collect sensitive data.

Phishing campaigns remained the most popular and successful method of acquiring sensitive data. A significant increase in amateur malicious actors was observed, likely due to the ease of acquiring phishing tools that are developed and then sold or offered as a service (Phishing as a Service). Some of these tools are even freely available on the internet, making them accessible to virtually anyone.

The most widespread campaigns continue to be those that exploit the identities of banks and financial institutions, postal and courier services, popular online services, and high-profile social media users (e.g., politicians). Activities exploiting geopolitically relevant events, such as the war in Ukraine or the conflict in Israel, were also recorded.

Attackers frequently use URL shorteners and multiple redirects to mask their activities and bypass security features. In 2023, malwaretisement campaigns continued to spread trojanized versions of frequently used software. The primary issue remains people's habit of automatically clicking on ads that appear among the top search engine results.

Search engine optimization (SEO) was often employed by attackers. It works by optimizing the technical configuration of a website, content relevance, and link popularity. This allows fake versions of websites to more easily penetrate the top positions in search engines. Attackers also took advantage of paid advertising.

1.1.4 ATTACKS EXPLOITING INATTENTION AND INSUFFICIENT SECURITY

Last year, there were again cases related to the lack of secure access to information technologies by both users and administrators of information systems. This includes mainly incorrect configurations and insufficient system security, with poor cyber hygiene and best security practices.

Deficiencies appeared in the form of a large number of devices and services (such as network storage, IP cameras, remote access services) that were freely accessible from the internet, weak passwords, repeated use of the same passwords across different services, and unimplemented two-factor authentication.

Other noted trends include the presence of fraudulent libraries. These have similar-sounding names to their legitimate counterparts (so-called library typosquatting). Their goal is to spread malicious code, benefiting from typos or the inattention of programmers. If such a product is used in other services, the entire supply chain is at risk of being infected.

1.1.5 VULNERABILITIES

Globally, the number of disclosed and reported vulnerabilities increased. The overall risk and relevance of vulnerabilities are assessed not only based on the objective evaluation of severity through the CVSS metric but also based on the availability of a proof of concept (PoC) for exploiting the vulnerability and whether the vulnerability is actively exploited by attackers.

Compared to 2022, which was dominated by several large and visible vulnerabilities, 2023 saw the discovery of multiple critical vulnerabilities with significant impact, although these did not receive as much media attention individually.

In 2023, the most severe vulnerabilities globally were exploited in products such as Forta GoAnywhere (CVE-2023-0669), Barracuda Email Security Gateway (CVE-2023-2868), Progress Software Moveit Transfer (CVE-2023-34362), MS Windows and Office solutions (CVE-2023-23397, CVE-2023-36884, CVE-22336584), WebP/Libwebp (CVE-2023-4863), Cisco XE (CVE-2023-20198), VMware ESXi (CVE-2023-20867), Apple iOS and iPadOS (CVE-2023-41992, CVE-2023-41993), Atlassian Confluence (CVE-2023-22515), and Citrix NetScaler and Netscaler Gateway (CVE-2023-4966).

These vulnerabilities allowed attackers to gain unauthorized access to sensitive data, unauthorized access to systems, and the execution of malicious code, resulting in the complete compromise of the confidentiality, integrity, and availability of vulnerable systems.

1.1.6 NEGATIVE IMPACT OF AI MODELS ON CYBERSECURITY

The rise in popularity of artificial intelligence (AI) tools and the availability of language models such as ChatGPT, MS Copilot, and Grok opened new opportunities for attackers and provided them with a wide range of tools to enhance their activities. These tools allow them to generate higher-quality translations and phishing email texts, as well as automate various tasks performed throughout the lifecycle of a phishing campaign, not just content generation in different languages. The higher sophistication of attacks was also due to the use of custom generative models specifically designed for malicious actors, such as WormGPT, which lacks security restrictions and safeguards against misuse for illegal purposes.

The most common trends in using AI for malicious purposes also included modifying and generating malicious code using AI, automated permutations of code versions to evade detection, and further opening doors for amateur attackers into the world of illegal activities.

1.2 Most Significant Threats in the Slovak Republic in 2023

1.2.1 SOCIAL ENGINEERING

Phishing campaigns continued to leverage social engineering to more effectively achieve their goals. Trends in obtaining sensitive information did not differ significantly from the previous year.

In 2023, phishing in Slovakia predominantly involved impersonating delivery services (e.g., DHL, DPD, Slovenská pošta, Packeta, etc.), internet service providers, banks and financial institutions, the police and Interpol, as well as central government authorities (e.g., the Financial Administration and the Ministry of Investment, Regional Development, and Informatization). These cases were repeatedly publicized throughout the year by state authorities and affected entities.

Fraudulent activities exploiting well-known online sales platforms and forums also persisted, with attackers attempting to extract sensitive information, particularly payment card details or internet banking credentials, from their victims. The phenomenon of sextortion also remained prevalent, wherein attackers blackmail victims without necessarily having access to sensitive materials.

The year 2023 was notable for campaigns based on cryptocurrency scams (various services and pyramid schemes related to cryptocurrency investments). Attackers would initially gain victims' trust by paying out commissions, only to stop payments at a certain point. These scams often involved significant PR efforts, including promotions on Telegram and other social networks, as well as the organization of physical meetings.

Another type of social engineering, known as whaling, remained relevant despite lower frequency. This often involved impersonating a company director to request account balances or payments, urging the victim to urgently transfer funds to the supposed superior or supplier.

Contrary to predictions from the previous year, minimal phishing content was observed on decentralized peer-to-peer platforms (e.g., IPFS). Despite widespread disabling of macro execution in MS Office, attackers continued to use Office documents for spreading malicious content (albeit to a lesser extent). These documents could include malicious URLs or employ alternative techniques like OLE template injection, wherein parts containing malicious content are downloaded to the device during file opening, unaffected by the macro restrictions.

Actors in phishing campaigns also utilized email attachments with file types such as .lnk, .iso, .rar, and others to distribute malicious content.

Interactive forms of social engineering, often linked to phishing attacks, saw an increase. In some cases, phishing websites included interactive chat features where attackers guided victims through remote management services or navigated them during phone calls while pretending to provide technical support.

Fraudulent campaigns on social networks also increased. Attackers sought access to business accounts or accounts with a large following to distribute malicious content, modify paid advertisement content, share fraudulent posts (e.g., related to cryptocurrencies), or disseminate illegal content.

A newly observed trend involved the abuse of SMS payment gateways. In such scams, attackers create an SMS payment request directed at the victim's number and then persuade the victim to send an SMS to a specific short code, thereby confirming the payment. Using this method, attackers purchase items like game unlock keys or other easily resellable products, which they subsequently monetize.

1.2.2 SERVICE UNAVAILABILITY AND DDOS ATTACKS

The year 2023 was marked by numerous DDoS attacks targeting critical infrastructure, the banking sector, and transportation. Additionally, several categorized incidents were reported.

A positive development was the increasing resilience of victims' infrastructure both after attacks and in prevention efforts. This included a high number of publicized successful attack mitigations and the impact of awareness campaigns conducted by security authorities (nationwide alerts and targeted/sector-specific warnings for organizations identified as potential targets by hacktivists). In most cases, operations were successfully restored after the attacks concluded.

A continuing trend involved attacks originating from TOR IP addresses, VPNs, Open Proxies, and compromised devices, often from botnets rented as a service by other hacker groups, which attackers used to obscure their activity.

However, system outages and unavailability were not always caused by malicious third-party actions. They were sometimes the result of systems being unprepared for a high influx of legitimate visitors, poorly executed system maintenance, improperly implemented or untested updates, or the introduction of new, untested elements, among other factors.

1.2.3 MALWARE

In Slovakia, numerous device infections by various malware families were recorded, including SystemBC, IcedID, Ursnif, Trickbot, JS.Agent.USU, QuakBot, Qbot, Redline, Raccoon Stealer, and Amadey. Ransomware infections were also significant, linked to the activities of groups such as Lockbit, Vice Society, Underground Team, and Medusalocker.

The most notable intrusion vectors included social engineering, poor security policies (e.g., using personal devices and service accounts for private purposes), visiting compromised websites, or installing trojanized software (e.g., paid software with compromised add-ons installed).

1.2.4 VULNERABILITIES AND ATTEMPTS TO BREACH SYSTEMS

The most common intrusion vector in 2023 was phishing attacks, representing the most effective way for attackers to bypass system security settings.

This was followed by vulnerabilities and improper device configurations, particularly publicly accessible remote access and data exchange services (e.g., RDP, FTP, SSH, SMB)

and login interfaces for industrial control systems with default factory settings and passwords, or even without authentication or with weak password policies.

A frequent cause of system breaches was the compromise of email accounts as a result of phishing, leading to chain distribution of phishing messages to the contacts of the compromised account.

In the area of vulnerabilities, the National Security Authority (NBÚ) issued numerous targeted warnings, such as those related to vulnerabilities in SYNOLOGY SRM, QNAP NAS, MS Exchange, Barracuda Networks Spam Firewall, Citrix, Jusnos OS, Apache HTTP Server, ZIMBRA, Atlassian Confluence, CISCO IOS XE, Roundcube, TeamCity JetBrains, and others.

It was observed that companies often failed in monitoring and managing vulnerabilities, which prevented them from responding to potential threats in a timely manner.

Another frequently observed issue was the neglect of maintaining outdated and unsupported devices, as they represent a significant financial and personnel burden. This often led to inadequate management of updates or appropriate mitigation measures.

1.2.5 RISK OF CYBER INCIDENTS ARISING FROM INSUFFICIENT SECURITY MEASURES

The human factor and security negligence continued to play a significant role in the occurrence of cyber incidents. In Slovakia, the improper configuration of systems, lack of regular updates, weak passwords, and other security deficiencies contributed to the vulnerability of organizations to cyberattacks.

For example, several incidents in Slovakia involved the compromise of systems due to unpatched vulnerabilities or the use of default passwords. These weaknesses allowed attackers to gain unauthorized access to sensitive data or disrupt the availability of services.

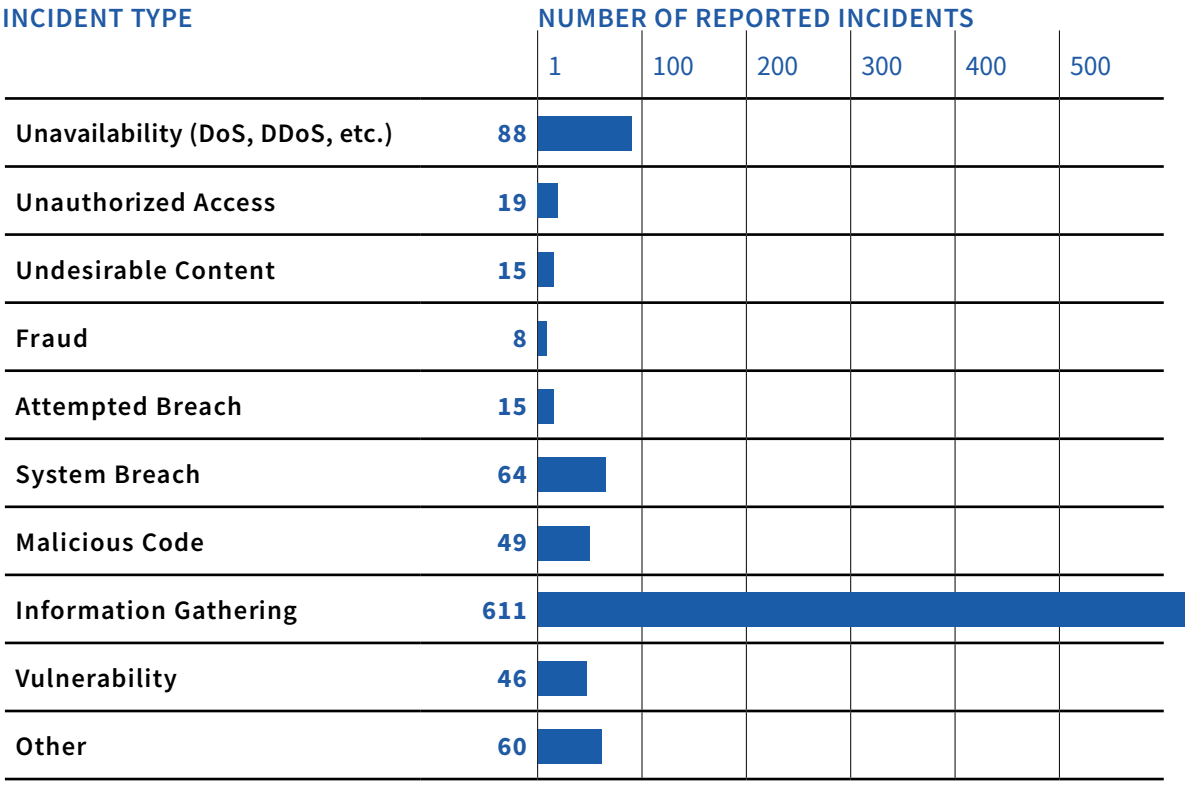
The human factor was also exploited in phishing attacks, where attackers took advantage of users' lack of awareness and poor security habits to gain access to critical systems. The spread of phishing emails and social engineering tactics remained a significant challenge for organizations in Slovakia.

To mitigate these risks, it is essential for organizations to continuously improve their cyber hygiene, implement proper security configurations, conduct regular security assessments, and provide ongoing education and training for employees.

2. Statistical Overview of Incidents in 2023

The National Cyber Security Centre fulfilled its tasks in monitoring the Slovak cyberspace. It worked on gathering and analyzing information from received reports of cybersecurity incidents.

Compared to previous years, there was a change in the statistical evaluation of recorded incidents, which now only includes data on incidents reported to the NCSC.

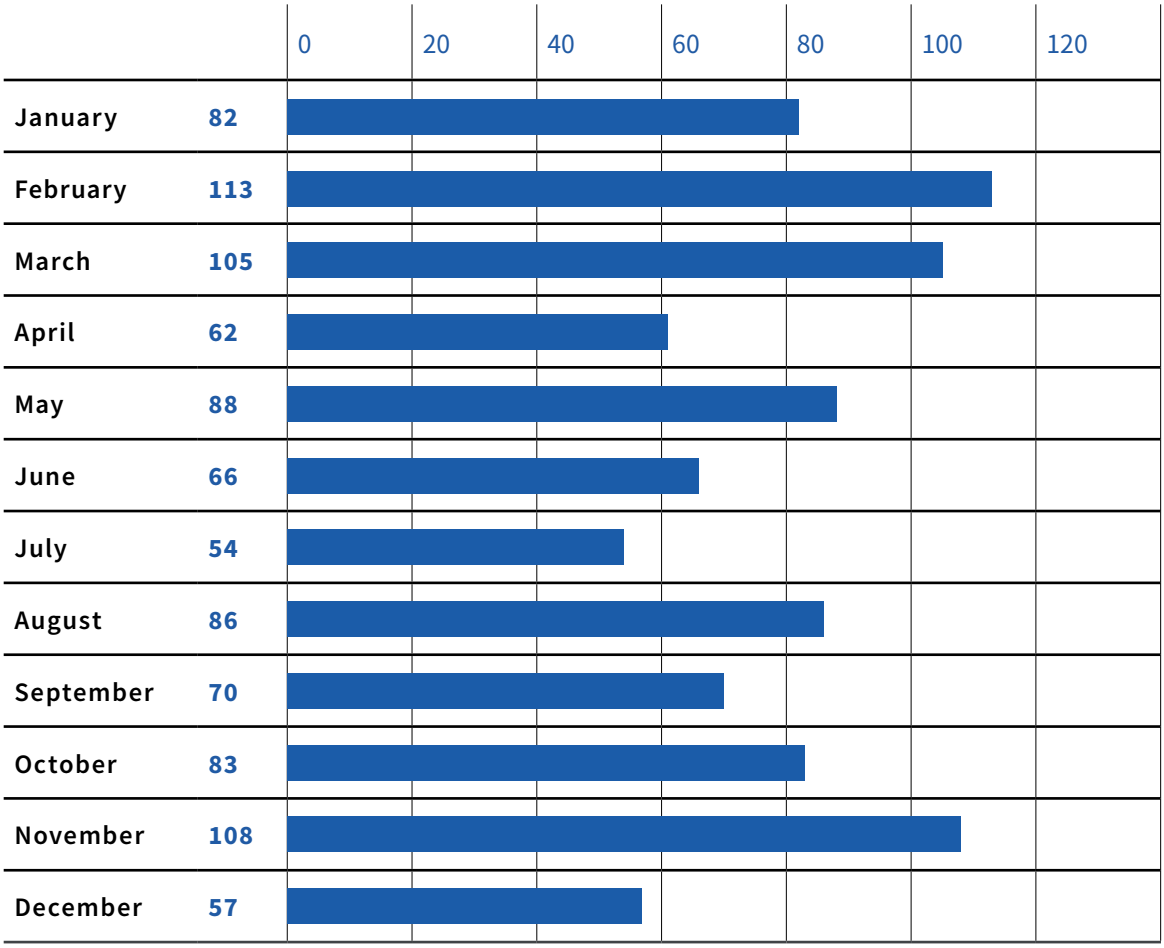


In 2023, technical types of attacks, such as information gathering, unavailability, system breaches, malicious code, and vulnerabilities, were dominant.

Phishing remained the most widespread and successful method of obtaining sensitive data and spreading malicious content. Unavailability also includes system outages that are not the result of a cyber attack (see above). Compared to the previous year, we observed an increase in ransomware and malware activities.

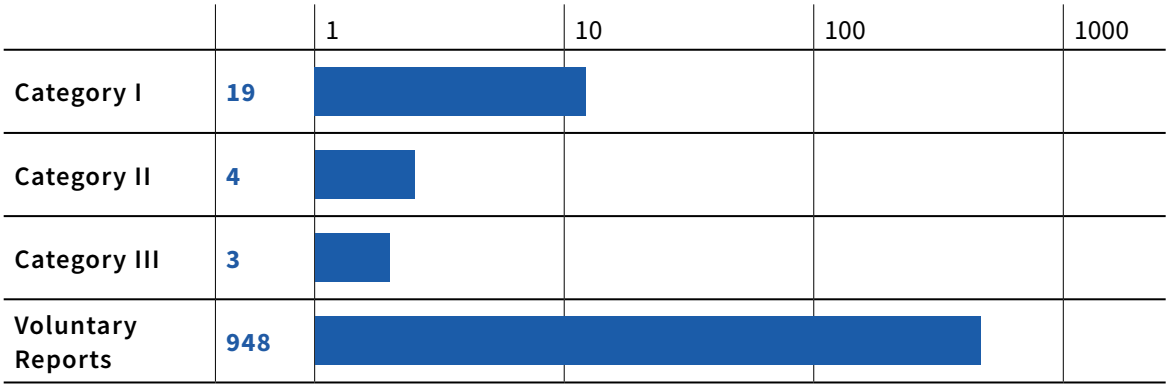
In 2023, the majority of cybersecurity incident reports were received in the first half of the year. SK-CERT received 196 fewer reports in 2023 than in the previous year. However, this does not necessarily imply that Slovak cyberspace has become safer. It is necessary to consider the ongoing lack of awareness among operators of essential services and providers of digital services about reporting incidents, as well as the increasing sophistication of malicious actors, whose activities may be harder to detect, or a combination of both factors.

NUMBER OF REPORTED INCIDENTS



Voluntary reports significantly outnumbered mandatory categorized reports. The most commonly observed reason for not reporting incidents was a lack of knowledge about legal norms—entities are unaware of the reporting obligation. There was also a varied level of maturity and awareness among entities in Slovakia—many entities, for example, fear sanctions or other negative consequences.

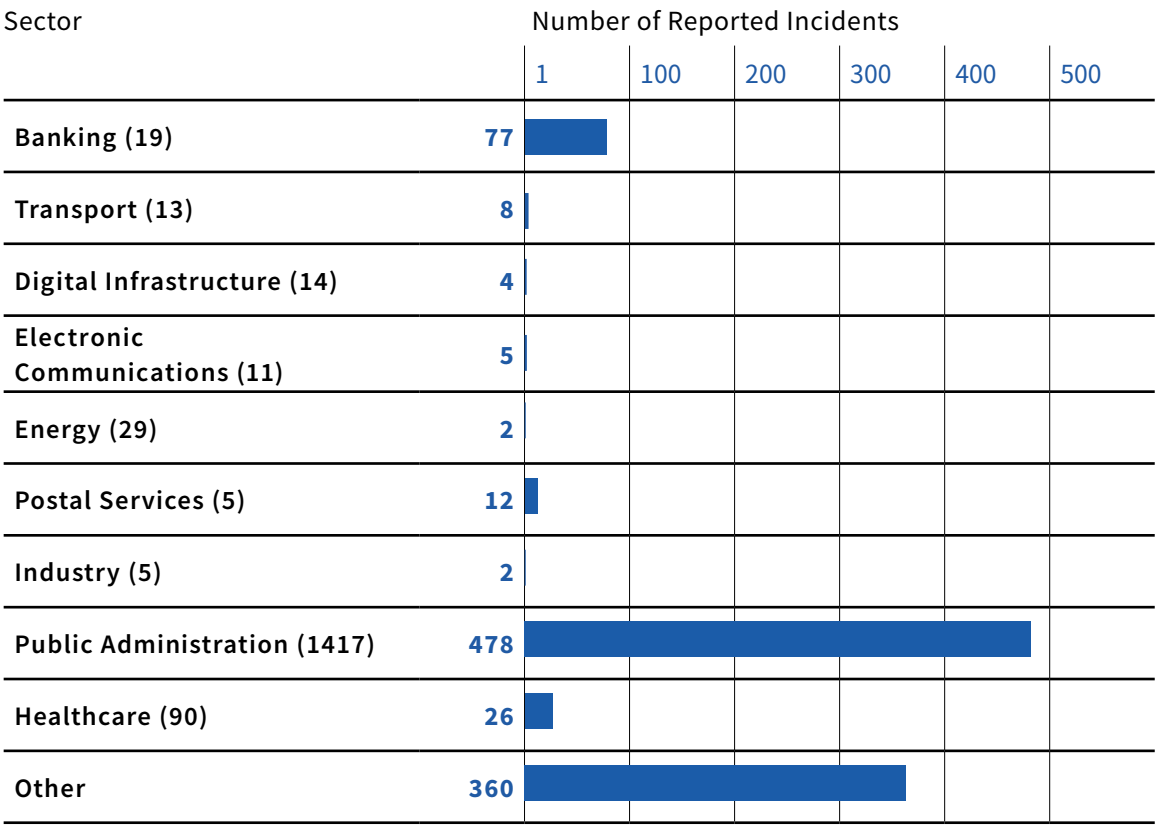
TYPES OF REPORTED INCIDENTS



In 2023, the most reports came from the public administration, banking, and healthcare sectors.

A higher number of reports implies more incidents in the sector and a higher level of maturity and awareness of the reporting entity (not afraid to report, communicates, also reports voluntarily, etc.). However, it is necessary to consider the different numbers of entities in each sector and the attractiveness of potential gains from malicious actor activities. Additionally, with the upcoming amendment to the law in connection with NIS 2, an increase in reports is expected in the coming years, as the amendment will extend the scope to additional entities.

NUMBER OF REPORTED CYBERSECURITY INCIDENTS OVER TIME



3. Overview of Computer Crime Status in the Slovak Republic for 2023

The police force only maintains general data on criminal offenses related to computer crime.

Criminal Offense (Section, Title)	Detected	Solved	% Solved	Damage (€)
§ 201a Sexual Abuse	6	2	33,33	
§ 219 Unauthorized Production and Use of Payment Instruments, Electronic Money, or Other Payment Cards	2116	457	21,65	5 953 000
§ 226 Unjust Enrichment	9	2	22,22	76 000
§ 247 Unauthorized Access to Computer System	23	1	4,35	600 000
§ 247a Unauthorized Intervention in Computer System	8	–	0	15 000
§ 247b Unauthorized Intervention in Computer Data	5	–	0	10 000
§ 247c Unauthorized Access to Computer System	2	1	50	–
§ 247d Unauthorized Capture of Computer Data	–	–	–	–
§ 283 Copyright Infringement	44	9	20,45	1 848 000
§ 368 Production of Child Pornography	33	16	48,48	7 000
§ 369 Distribution of Child Pornography	201	56	27,86	30 000
§ 370 Possession of Child Pornography and Participation in Child Pornographic Performance	37	23	62,16	13 000
Total	**2 447**	**567**	**23,17**	**8 552 000**

MONITORING THE DEVELOPMENT OF CRIMINAL ACTIVITY IN THE FIELD OF COMPUTER CRIME

The only tool available for monitoring the development of criminal activity in the field of computer crime within the Police Force is the Evidence and Statistical System of Crime (EŠSK) in accordance with the Ministry of Interior of the Slovak Republic Regulation No. 83/2014 on the Use of Information Systems of the Police Force, the Evidence and Statistical System of Crime, and the System of Concurrently Prosecuted Persons.

Computer crime is a specific type of criminal activity that can only be committed using computing technology (which serves as the perpetrator's tool for committing the crime), or computing technology is the object of the crime.

Detecting and documenting this type of crime requires a high level of expertise and high-quality computer equipment because crimes related to the damage and misuse of information on storage media are primarily committed via the internet.

The low rate of resolution for computer crime is closely related to the proliferation of new information technologies and services involving various sophisticated methods in P2P/TOR networks, among others. This results in consistently low resolution rates for crimes involving unauthorized access/intervention into computer systems/data or the capture of computer data.

The overall number of crimes related to child pornography is influenced by the information sent regarding child pornography from the National Center for Missing and Exploited Children (NCMEC) in the USA through EUROPOL, and the National Unit of the Europol International Police Cooperation Office to the department as suspicions of production, possession, and distribution of child pornography.

The information is evaluated and sorted in the department, and criminal investigation referrals are sent to the relevant units of the Police Force. In 2023, the department received a total of 41 SIENA packages from NCMEC through Europol, containing 9,601 NCMEC reports. This represents a 20% increase compared to 2022, when 7,627 NCMEC reports were received.

Individual NCMEC reports were analyzed for the presence of child pornography and the relevance of their referral as information for initiating criminal proceedings. A total of 420 referrals/information for initiating criminal proceedings were processed and forwarded to the relevant units of the Police Force. The distribution of materials containing child pornography is most frequently recorded on internet communication platforms and internet forums.

In preventing various online frauds and fraudulent campaigns, the department also collaborates with the Communication and Prevention Department of the Police Force. The department provides information on new methods of committing crimes in the online space, which are published on the official Facebook page Police Force, to ensure that the public is informed as quickly as possible.

4. SECTORAL PERSPECTIVE

The perspective on cybersecurity across different sectors is shaped by two pillars: the results of audit reports and the assessment of activities by central authorities. It is possible to state that the level of cybersecurity varies significantly depending on the sector.

The banking sector has long been ahead in the field of cybersecurity. Operators in this sector OES approach the issue responsibly, both in implementing security requirements and in communication with the National Security Authority (NSA). In the case of incidents or other problems, they respond promptly and without delay. Representatives of OES in the banking sector also actively participate in building a community focused on cybersecurity.

In the healthcare sector, there is a gradual increase in awareness of the importance of cybersecurity. This trend is also supported by the improving work of the central authority. The perception of responsibility for data protection and the functionality of systems and services, upon which human lives depend, is gradually strengthening.

The energy sector exhibits the most significant differences among sub-sectors and within their internal structures. The gas sector achieves the best audit results among all sectors and sub-sectors. In the electricity sector, there are notable differences between individual operators.

Conversely, the thermal energy sector suffers from extremely poor audit results, despite the importance of the sub-sector. Its operation has a significant impact on the daily lives of citizens. Restrictions or outages in this sector can have serious consequences for the life and health of the population.

In the financial market infrastructure, industry, and postal sectors, there is a lack of a clear picture of the state of cybersecurity. This is due to a lack of relevant information from the central authorities responsible for these sectors. They have not provided specific details on cybersecurity in these areas, and there is also a lack of sufficient audit reports to create an anonymized statistical sample.

In the public administration sector, specifically in the sub-sector of public administration information systems, cybersecurity has remained unchanged for a long time despite the largest number of operators. In some cases, it is neglected to a critical degree. Local governments and smaller operators, in particular, do not realize its importance.

They approach the issue superficially and focus on formal actions such as purchasing generic documents. They often try to shift responsibility to external companies, including non-transferable responsibilities of the statutory representative. The overall management of cybersecurity is lacking, chaotic, or incomplete. The problems are not limited to local governments but also affect some large operators in this sub-sector, including state institutions.

When obtaining information from central authorities under Act No. 69/2018 on cybersecurity, there was often a misunderstanding of the role and tasks of the central authority by the competent ministries. Responses were frequently framed in a way that described the situation at the ministry as an operator of a basic service, rather than as an entity responsible for a particular sector or sub-sector. From this perspective, it is essential for central authorities, in particular, to better understand their roles and responsibilities according to § 9.

4.1 Sanctions

In accordance with the Cybersecurity Act, the National Security Authority NSA is authorized to impose fines if an operator of essential services violates (OES) its legal obligations. In 2023, the NSA conducted cybersecurity inspections of 18 operators of essential services, finding deficiencies in 17 of the inspected entities, resulting in a total of 67 findings, which can be categorized into the following areas:

- Cybersecurity and information security management in relation to third parties – 11 violations,
- Event logging and monitoring of networks and information systems – 7 violations,
- Risk management – 12 violations,
- Asset management – 5 violations,
- Identification of technical vulnerabilities – 7 violations,
- Handling of cybersecurity incidents – 6 violations,
- Information classification and categorization of networks and information systems – 6 violations,
- Content and structure of security documentation – 2 violations,
- Security management of network and information systems operations – 4 violations,
- Personnel security – 2 violations,
- Network and communication security – 1 violation,
- Management of personnel access to networks and information systems – 1 violation,
- Appointment of a cybersecurity manager – 1 violation,
- Signing contracts for the implementation of security measures and notification obligations under the law – 1 violation,
- Non-submission of a cybersecurity audit – 1 violation.

4.2 Audits and Self-Assessments

Cybersecurity audits are conducted to verify the effectiveness of the implementation of measures, the execution of actions, and any deficiencies in the measures implemented within the ICT and cybersecurity environments of OES, in line with the applicable regulations and security framework. In 2023, a total of 135 audit reports were submitted to the National Security Authority.

AUDITS

Sector	Number of OES	Number of OES Required to Audit in 2023
Banking	19	19
Digital Infrastructure	15	9
Transport	13	7
Electronic Communications	11	8
Energy	28	17
Financial Market Infrastructure	1	1
Postal Services	5	1
Industry	7	4
Public Administration	1 400	122
Water and Atmosphere	18	15
Healthcare	94	69
Total	**1 611**	**272**

SELF-ASSESSMENTS

Sector	Number of Self-Assessments Submitted
Public Administration	307
Healthcare	6
Transport	2
Postal Services	2
Water and Atmosphere	6
Energy	1
Industry	1
Total	**325**

4.3 Banking

Central Authority: Ministry of Finance of the Slovak Republic (MF SR)

Number of OES: 19

Number of OES Required to Audit in 2023: 19
(can also be fulfilled by self-assessment according to §34a para. 2 ZoKB) Cybersecurity Act

Number of Submitted Audit Reports: 9

Number of Submitted Self-Assessments: 0

Subsectors: None

4.3.1 ASSESSMENT OF CYBERSECURITY STATUS FOR 2023 BY THE CENTRAL AUTHORITY

Critical Threats:

The most significant threats highlighted to the Ministry of Finance in the cyberspace were sophisticated techniques for gaining unauthorized access to organizational systems, ransomware attacks, cloud security threats, social engineering, and vulnerabilities in IT products.

Legal Activities:

The MF SR maintains a Security Operations Center (SOC) as a department within the ministry. The SOC was established as part of the project "Enhancing Information and Cybersecurity at the MF SR" and was successfully implemented in November 2023. Currently, the project is in its sustainability phase. The MF SR is a member of the international TF CSIRT association under "Listed team" status. Throughout 2023, the MF SR was in regular contact with the National Security Authority (NSA) for the implementation of an MF SR access point into the Joint Information System on Cybersecurity, as required by the cybersecurity law.

Activities Beyond Legal Requirements:

The MF SR continues to operate a mechanism for training department staff in combating cyber threats (e-learning portal LMS, internal staff training, raising employee security awareness). Additionally, a generic email address, podozrivaposta@mfsr.sk, is maintained for reporting suspicious and potentially harmful electronic communications. For investigating and handling cybersecurity incidents, a generic email address, incident@mfsr.sk, is designated.

Planned Activities:

The central authority plans to continue operating the training mechanism for department staff in preventing cyber threats; to accredit the SOC security monitoring department within the international TF CSIRT association; and to launch a project funded by the EU aimed at expanding the SOC security monitoring services for the ministry's subordinate organizations.

Planned Strategy:

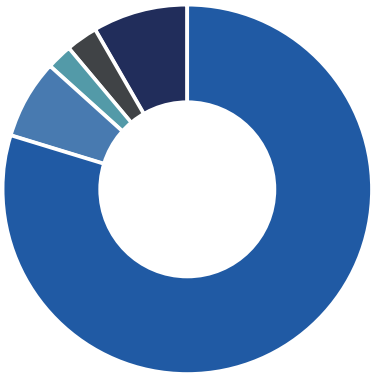
In December 2023, the draft of a new Information and Cybersecurity Strategy was finalized, but it did not specify the sectors under the ministry's jurisdiction as per the cybersecurity law. A specific cybersecurity strategy for the sectors under its jurisdiction is not currently planned.

Human Resources in Cybersecurity:
The MF SR has established a Security Operations Center (SOC) as a security monitoring department within the Information and Cybersecurity Department, part of the Information Technology Section, since 2022, but it is only broadly operational for ministry activities. External entities in sectors under the MF SR's jurisdiction (e.g., banks, insurance companies, the State Treasury) are not covered by these activities. The ministry plans to expand the SOC security monitoring services to its subordinate organizations.

Cybersecurity Cooperation:
There is cooperation with the international TF CSIRT organization. The MF SR communicates with the NATO Computer Incident Response Capability Technical Center, receives their security warnings and informational bulletins directly, and participates in professional symposiums and conferences organized under their auspices. The ministry also communicates with the Cybersecurity Center of Excellence (CCDCOE) in Tallinn, Estonia, where its representatives attended the international Cyber Conflict – CyCon 2023 conference in 2023.

4.3.2 AUDIT RESULTS IN THE BANKING SECTOR

As of December 31, 2023, the National Security Authority received a total of 9 audit reports from the banking sector. Based on compliance statistics with audit requirements, the average percentage of compliance in the banking sector is as follows:



AVERAGE PERCENTAGE COMPLIANCE (YEAR 2023)	
COMPLIANCE	79 %
PARTIAL COMPLIANCE	7 %
NON-COMPLIANCE	2 %
NOT APPLICABLE	3 %
VERIFIED ELSEWHERE	8 %
NOT EVALUATED BY AUDITOR	0 %

When looking at individual Essential Service Operators (OES) in the banking sector, there is a consistently high level of compliance with audit requirements across all operators, with only a very low incidence of non-compliance.

4.3.3 MOST COMMON AUDIT FINDINGS IN THE BANKING SECTOR

Among the most common audit findings in the banking sector are:

- Contracts with all suppliers are not up-to-date and signed according to § 19(2).
- There is no formalized cybersecurity strategy.
- The company has not conducted a comprehensive risk analysis.
- Processes and procedures for asset, threat, and risk management are not established and formalized.
- Procedures for transferring rights, obligations, and responsibilities related to cybersecurity to another entity are not defined.

4.4 Transportation

Central Authority: Ministry of Transport of the Slovak Republic (MT SR)

Number of OES (Essential Service Providers): 13

Number of OES Required to Conduct an Audit in 2023: 7
(Can also be fulfilled by self-assessment according to §34a para. 2 of the Cybersecurity Act)

Number of Submitted Audit Reports: 5

Number of Submitted Self-Assessments: 2

Subsectors: Road Transport, Air Transport, Water Transport, Rail Transport

4.4.1 CYBERSECURITY STATUS ASSESSMENT FOR 2023 BY THE CENTRAL AUTHORITY

Critical Threats:

In the transportation sector, no significant cybersecurity incidents were reported in 2023. However, to ensure compliance with current legislation and the upcoming transposition of the NIS2 Directive, it is necessary to address the technological and investment debt in cybersecurity. The sector faces challenges due to the lack of centralized security oversight, limited funding, and a shortage of qualified personnel capable of performing regular preventive activities related to monitoring, cybersecurity protection, and risk mitigation.

Legal Activities:

The ministry continuously monitors and analyzes needs and requirements relevant to the transportation sector. In line with these tasks, it is actively working on the implementation of the NIS2 Directive, which represents a key legislative framework of the European Union in the field of cybersecurity.

In the context of the NIS2SK project, the MT SR is conducting preparatory work for transposing this directive into national law, considering the specificities and needs identified during market consultations with relevant sector entities.

This process ensures that the adopted standards and regulations adequately and effectively respond to current challenges in cybersecurity. Upon completing the analytical and consultation process, the ministry will issue sector-specific decrees. These will explicitly define the security measures that must be implemented by entities operating within the various sectors to enhance the protection of critical information infrastructures and ensure a higher level of cybersecurity in the Slovak Republic.

As part of the “Development of Governance and the Level of Information and Cybersecurity in the Transport Subsector – Ministry of Transport and Construction of the Slovak Republic” project, the ministry has conducted activities related to securing documentation for the processing and updating of essential documents in the field of information and cybersecurity, and the introduction of software tools for the process-organizational management of information and cybersecurity.

Based on recent attacks, the ministry has begun implementing 2FA/MFA on its information systems. It also ensured MS ATA monitoring for DDoS attacks, which were carried out on its web services (webmail, OA, EWS).

Activities Beyond Legal Requirements:
The Ministry of Transport, in collaboration with the National Security Authority (NSA) and the Competence and Certification Center for Cybersecurity (CSCCC), actively participated in the preparation and implementation of a joint project focused on implementing the NIS2 Directive, funded by the European Commission.

The project is a significant step towards strengthening cybersecurity and protecting critical information infrastructures at the national level, not only in the sectors under the ministry's jurisdiction. The project emphasizes active participation and involvement of market entities through market consultations. This approach allows for valuable insights and suggestions from experts and stakeholders directly affected by the new legislation. Due to this inclusive process, the project has received widespread recognition and positive evaluation.

The joint efforts of the ministry and its partners aim to ensure a smooth transition to the new regulatory framework, aligned with European standards while reflecting the specific needs and challenges of the transportation sector in cybersecurity.

The implementation of the NIS2 Directive in the sectors under the purview of the Ministry of Transport represents a strategic commitment to increase the resilience of information systems and infrastructures against cyber threats and support the secure development of the digital environment.

Planned Activities:
MT SR plans to implement activities that will raise awareness of the planned measures in the sector—through various communication channels, it will clearly and explicitly inform about obligations and practical experiences on how to meet the expected measures. These will be in the form of workshops, webinars, podcasts, and through the ministry's website.

Planned Strategy:
MT SR has implemented a cybersecurity strategy as a strategic document applicable to its office. If required and based on feedback from the transportation sector, the ministry will consider issuing a cybersecurity strategy for the transportation sector or issuing a sector-specific decree.

Human Resources in Cybersecurity:
The transport department has established a department of IT strategy and cybersecurity in its organizational structure. However, it does not have dedicated personnel to fulfill the role of the central authority.

Collaboration in Cybersecurity:
MT SR collaborates on cybersecurity issues with partners in public administration — NSA and CSIRT.

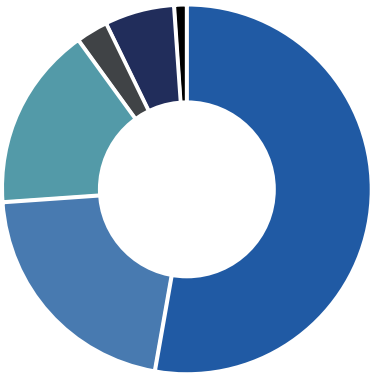
4.4.2 AUDIT RESULTS OF OES IN THE TRANSPORTATION SECTOR

As of December 31, 2023, a total of 5 audit reports and 2 self-assessments from the transportation sector were submitted to the National Security Authority. The average compliance rate in the transportation sector is over 50%, showing a slight improvement compared to previous years. The number of non-compliances with audit requirements is 16%, indicating room for improvement.

4.4.3 MOST COMMON AUDIT FINDINGS IN THE TRANSPORTATION SECTOR

Among the most frequent audit findings in the transportation sector are:

- Insufficiently defined roles and responsibilities in the field of cybersecurity.
- Lack of defined and implemented information classification and network and information system categorization according to the Cybersecurity Act.
- The cybersecurity manager is not appointed, principles of least privilege and segregation of duties are not formalized.
- Personnel security management processes are not formally established, and there is no plan for the development of security awareness and training.
- The operator of essential services (OES) does not have a plan for the development of security awareness.
- Software vulnerabilities and vulnerabilities in technical resources are not systematically monitored and addressed.
- The capability to monitor and analyze events at the OES is at a weak level.



COMPLIANCE RATES FOR 2023

COMPLIANCE	53 %
PARTIAL COMPLIANCE	21 %
NON-COMPLIANCE	16 %
NOT APPLICABLE	3 %
VERIFIED ELSEWHERE	6 %
NOT EVALUATED BY AUDITOR	1 %

4.5 Digital Infrastructure

Central Authority: National Security Authority (NSA)

Number of OES: 15

Number of OES Required to Conduct an Audit in 2023: 9
(Can also be fulfilled by self-assessment according to §34a para. 2 of the Cybersecurity Act)

Number of Submitted Audit Reports: 7

Number of Submitted Self-Assessments: 0

Subsectors: None

4.5.1 CYBERSECURITY STATUS ASSESSMENT FOR 2023 BY THE CENTRAL AUTHORITY

Critical Threats:

In the digital infrastructure sector, we face significant cybersecurity threats. The NSA has identified the most significant threats frequently encountered in the Slovak cyber environment. These include:

- Attacks utilizing social engineering, particularly phishing and vishing.
- Distribution of malicious code and exploitation of vulnerabilities.
- Abuse of compromised infrastructure of OES for executing various attacks. Attackers can use such infrastructure to manage botnet networks, launch DDoS attacks, and spread phishing and malicious code.

In addition to these threats, the NSA also highlights the increasing sophistication of cyber attacks, insufficient levels of cybersecurity in some organizations, and inadequate awareness of cybersecurity threats among users.

Activities:
The NSA actively combats cybersecurity threats in the digital infrastructure sector. Its key activities include:

- Coordinating responses to cybersecurity incidents, guiding and directing the response to cyber incidents in the sector, and providing assistance to affected entities.
- Performing preventive activities, issuing warnings about threats, and providing relevant information to Essential Service Providers. The NSA also offers regular expert consultations on cybersecurity to enhance the sector's cybersecurity level and protect Slovakia's critical infrastructure.

Planned Activities:
The NSA is committed to continuously improving cybersecurity in the sector. It plans to maintain ongoing activities and gradually enhance the services provided to OES. The authority also plans to regularly reassess the situation in the sector and respond to new threats and challenges as needed, aiming to keep pace with the latest trends in cybersecurity.

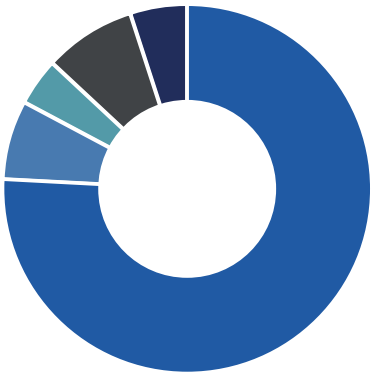
Planned Strategy:
The NSA is responsible for developing and implementing the National Cybersecurity Strategy, with several tasks outlined in the action plan for this strategy. These tasks relate to cybersecurity at the national level, including digital infrastructure.

Human Resources in Cybersecurity:
The NSA is continuously building its personnel capacity in cybersecurity. However, it faces challenges due to the shortage of experts in the labor market and the ongoing underestimation of cybersecurity education. Currently, the situation is stable, but with the increasing responsibilities of the NSA in cybersecurity, more competent staff will be required.

Collaboration in Cybersecurity:
The authority's collaboration is mandated by Act No. 69/2018 on cybersecurity. A comprehensive view of the area of cooperation can be found in this report in the section "Measures and Activities."

4.5.2 AUDIT RESULTS OF OES IN THE DIGITAL INFRASTRUCTURE SECTOR

As of December 31, 2023, a total of 7 audit reports from the digital infrastructure sector were submitted to the National Security Authority. In the digital infrastructure sector, a 75% compliance rate with audit requirements is consistent across most operators, which is also reflected in the overall sector compliance rate. This sector has significantly improved its ratings compared to previous years.



AVERAGE PERCENTAGE COMPLIANCE (YEAR 2023)	
COMPLIANCE	76 %
PARTIAL COMPLIANCE	7 %
NON-COMPLIANCE	4 %
NOT APPLICABLE	8 %
VERIFIED ELSEWHERE	5 %
UNASSESSED BY AUDITOR	0 %

4.5.3 MOST COMMON AUDIT FINDINGS IN THE DIGITAL INFRASTRUCTURE SECTOR

The most common audit findings in the digital infrastructure sector are:

- Details of implemented technical measures are not listed in the existing record of adopted security measures.
- The entity does not carry out and has not implemented information classification in practice.
- The company does not have a clearly defined internal control environment.
- Access/control matrices and role conflicts are not clearly defined.
- Contracts with suppliers do not include mandatory requirements according to the Cybersecurity Act.
- The company has a minimal number of users relative to the number of end customers.
- The access management tool is not implemented within the company.
- Local administrative access approaches are used within the company without justification

4.6 Electronic Communications

Central Authority: Ministry of Transport of the Slovak Republic (MT SR)

Number of Operators: 11

Number of Operators Required to Audit in 2023: 8
(possibly fulfilled by self-assessment according to §34a para. 2 of the Cybersecurity Act)

Number of Audit Reports Submitted: 2

Number of Self-Assessments Submitted: 0

Subsectors: Satellite Communication, Fixed and Mobile Electronic Communications Networks and Services

4. 6. 1 ASSESSMENT OF CYBERSECURITY STATUS FOR THE YEAR 2023 BY THE CENTRAL AUTHORITY

The assessment of the central authority for this sector does not differ from that for the transport sector. In addition to these threats, the National Security Authority (NSA) also highlights the increase in the sophistication of cyberattacks, inadequate levels of cybersecurity in some organizations, and insufficient awareness of cybersecurity threats among users.

4. 6. 2 RESULTS OF AUDITS FOR THE ELECTRONIC COMMUNICATIONS SECTOR

In the electronic communications sector, only two audit reports were submitted, so it is not possible to create an anonymized assessment of the audit results in the sector.

4. 7 Energy Sector

Central Authority: Ministry of Economy of the Slovak Republic (ME SR)

Number of Operators: 28

Number of Operators Required to Audit in 2023: 17
(possibly fulfilled by self-assessment according to §34a para. 2 of the Cybersecurity Act)

Number of Audit Reports Submitted: 13

Number of Self-Assessments Submitted: 1

Subsectors: Mining, Power Engineering, Gas Industry, Oil and Petroleum Products, Thermal Energy

4. 7. 1 ASSESSMENT OF CYBERSECURITY STATUS FOR THE YEAR 2023 BY THE CENTRAL AUTHORITY

Critical Threats:

Due to insufficient personnel capacities, the Ministry of Economy did not assess any threats in its sectors for 2023. However, upon request, the Ministry provided assistance in addressing cybersecurity incidents.

Legal Activities:

The Ministry of Economy methodically and upon request collaborated with operators of subordinate organizations (e.g., answering questions and requests related to cybersecurity, commenting on internal management acts related to cybersecurity and operational IT security, methodically assisting in the preparation of cybersecurity audits, and providing entry-level training for new employees as part of the sectoral cybersecurity pilot project). It also provided professional assistance to some subordinate organizations in implementing new firewall solutions. In collaboration with CSIRT MIRRI, it provided assistance in addressing a cybersecurity incident.

Activities Beyond the Law:

Due to insufficient personnel capacities in 2023, no additional activities beyond § 9 para. 1(c) were carried out.

Activities Beyond the Law
In 2023, due to insufficient personnel capacities, no additional activities beyond those stipulated in § 9 para. 1(c) were carried out.

Planned Activities
The primary plan is to strengthen personnel capacities by at least adding a position for a coordinator of sectoral and departmental cybersecurity.

Planned Strategy
The Ministry plans to issue a cybersecurity strategy, which will be one of the responsibilities of the coordinator for sectoral and departmental cybersecurity.

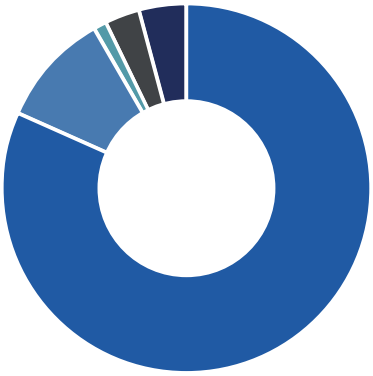
Human Resources in Cybersecurity
The central authority does not have positions dedicated to cybersecurity within its organizational structure. It also lacks sufficient personnel capacities to collaborate on cybersecurity issues with other sectoral authorities and international partners.

The Ministry of Economy has not provided any additional information on the aforementioned areas.

4.7.2 AUDIT RESULTS FOR THE ENERGY SECTOR

By December 31, 2023, the National Security Authority received a total of 13 audit reports from the energy sector.

In the energy sector, the compliance rate exceeds 80%, with 10% partial compliance, demonstrating an improvement in service quality. However, significant discrepancies in compliance levels persist among different sub-sectors, particularly between the thermal energy sub-sector and the others.



AVERAGE PERCENTAGE COMPLIANCE (YEAR 2023)

COMPLIANCE	81 %
PARTIAL COMPLIANCE	10 %
NON-COMPLIANCE	1 %
NOT APPLICABLE	3 %
VERIFIED ELSEWHERE	4 %
NOT ASSESSED BY AUDITOR	0 %

4.7.3 MOST COMMON AUDIT FINDINGS IN THE ENERGY SECTOR

Among the most common audit findings in the energy sector are:

- The list of control activities within the company is not defined. Additionally, there is no method for storing the results of performed control activities.
- Information systems currently in development are not classified or categorized until they go into production.
- A central configuration database is neither established nor complete, including in the IT service tool ASET.

- The defined development plan is not yet regularly implemented, and the effectiveness of employee training is not evaluated.
- Rules and procedures for IT operations management are not established or formalized.
- The company does not test continuity management processes, as this obligation is entirely new.
- While there are recovery plans for central control systems from an operational perspective, they do not consider the rest of the company's environment.

4.8 Postal Services

Central Authority: Ministry of Transport of the Slovak Republic (MT SR)

Number of OES (Operators of Essential Services): 5

Number of OES Required to Undergo Audit in 2022: 1
(Audit can also be fulfilled by self-assessment according to §34a, paragraph 2 of the Cybersecurity Act)

Number of Audit Reports Submitted: 2

Number of Self-Assessments Submitted: 2

Subsectors: Provision of postal services, postal payment services, and procurement activities

4.8.1 EVALUATION OF CYBERSECURITY STATUS FOR 2023 BY THE CENTRAL AUTHORITY

The evaluation of the status by the central authority for this sector is consistent with the statements made by the Ministry of Transport in the transport sector.

4.8.2 RESULTS OF AUDITS OF OES IN THE POSTAL SECTOR

Only one audit report has been submitted for the postal sector, so it is not possible to create an anonymized assessment of audit results for this sector.

4.9 Industry

Central Authority: Ministry of Economy of the Slovak Republic (ME SR)

Number of OES: 7

Number of OES Required to Conduct an Audit in 2023: 4
(possibly fulfilled through self-assessment according to §34a paragraph 2 of the Cybersecurity Act)

Number of Submitted Audit Reports: 3

Number of Submitted Self-Assessments: 1

Subsectors: Pharmaceutical Industry, Metallurgical Industry, Chemical Industry, Intelligent Industry

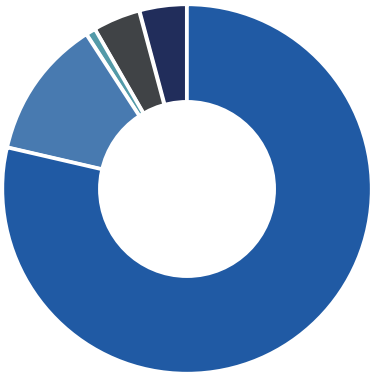
4.9.1 EVALUATION OF THE STATE OF CYBERSECURITY FOR 2023 BY THE CENTRAL AUTHORITY

The evaluation of the state for this sector does not differ from the statement by the Ministry of Economy in the energy sector, as it was not divided into individual subsectors.

4.9.2 RESULTS OF AUDITS OF OES IN THE INDUSTRY SECTOR

By December 31, 2023, the National Security Authority received a total of 3 audit reports and 1 self-assessment from the industry sector.

The sector reports 78% compliance and 12% partial compliance, with only 1% of audited items showing non-compliance.



AVERAGE PERCENTAGE COMPLIANCE (YEAR 2023)

COMPLIANCE	72 %
PARTIAL COMPLIANCE	12 %
NON-COMPLIANCE	1 %
NOT APPLICABLE	4 %
VERIFIED ELSEWHERE	4 %
NOT EVALUATED BY AUDITOR	0 %

4.9.3 MOST COMMON AUDIT FINDINGS IN THE INDUSTRIAL SECTOR

The most frequent audit findings in the industrial sector include:

- Lack of Functional Impact Analysis: There is no analysis being performed to assess the functional impact of disruptions.
- No Documentation of Security Measures: There is no record-keeping for implemented cybersecurity measures.
- Absence of Regular Risk Analysis: The organization does not conduct regular risk analyses for the information systems providing essential services.
- Undefined List of Control Activities: There is no defined list of control activities within the company. Additionally, there is no method for documenting the control activities performed and their outcomes.
- Inconsistent and Irregular Processes: The process is not consistently implemented according to documentation and is not performed regularly. The probability of threat impacts is not identified.
- No Functional Impact Analysis for Essential Services: The company has not conducted a functional impact analysis for essential services according to the criteria for identifying severe cybersecurity incidents as outlined in § 24 of the Cybersecurity Act.

4.10 Water and Atmosphere

Central Authority: Ministry of Environment of the Slovak Republic

Number of OES (Operators of Essential Services): 18

Number of OES with Audit Obligation for 2022: 20
(can also be fulfilled through self-assessment according to §34a, paragraph 2 of the Cybersecurity Act)

Number of Audit Reports Submitted: 6

Number of Self-Assessments Submitted: 6

Subsectors: Meteorological Service, Waterworks, Drinking Water Provision

4.10.1 ASSESSMENT OF THE CYBERSECURITY STATUS FOR 2023 BY THE CENTRAL AUTHORITY

Critical Threats:
The Ministry of Environment considers phishing campaigns to be the most significant threat, aiming to obtain sensitive information or money from users.

Legal Activities:
The ministry participated in cybersecurity training activities organized by MIRRI under the "Training and Security Center for IT Operation and Management for the Public Sector" project.

Activities Beyond Legal Requirements:
The sector manager did not perform any additional activities beyond the legal requirements.

Planned Activities:
The ministry plans to continue improving the level of information and cybersecurity within the ministry in 2024 and will further enhance preventive measures to increase the speed of incident detection and resolution.

Planned Strategy:
The ministry has an approved cybersecurity strategy and continuously works on improving security documentation.

Human Resources in Cybersecurity:
The institution has roles related to cybersecurity throughout the organizational structure. However, there is no separate department dedicated solely to cybersecurity.

Collaboration in Cybersecurity:
The Ministry of Environment does not have interdepartmental or international collaboration.

4.10.2 AUDIT RESULTS FOR OES IN THE WATER AND ATMOSPHERE SECTOR

As of December 31, 2023, the National Security Authority received a total of 6 audit reports and self-assessments from the Water and Atmosphere sector.

AVERAGE PERCENTAGE COMPLIANCE (YEAR 2023)

COMPLIANCE	70 %
PARTIAL COMPLIANCE	15 %
NON-COMPLIANCE	5 %
NOT APPLICABLE	6 %
VERIFIED ELSEWHERE	4 %
NOT EVALUATED BY AUDITOR	0 %

4.10.3 MOST COMMON AUDIT FINDINGS IN THE WATER AND ATMOSPHERE SECTOR

The most common audit findings in the Water and Atmosphere sector are:

- **Security Documentation:** The content of security documentation is often not fully implemented or does not reflect the actual state of conducted activities.
- **Process Consistency:** The process is not implemented consistently with documentation and is not performed regularly. The likelihood of threat impacts is not identified.
- **Employee Awareness and Compliance:** There is no record of employee awareness of cybersecurity policies, and no process for monitoring compliance with these policies is established.
- **Change Management:** Change management is not documented. Patch management is not formalized and is carried out on an ad hoc basis.
- **Event Monitoring:** A central tool for network event monitoring is not implemented, and operational logs are not recorded.
- **Communication and Recovery Plans:** There is no communication plan for implementing contingency plans. Contingency plans and recovery plans are not tested.

4.11 Public Administration

Central Authorities:
Ministry of Investments, Regional Development, and Informatization of the Slovak Republic (MIRRI SR)
Ministry of Defense of the Slovak Republic (MD SR)
Ministry of Interior of the Slovak Republic (MI SR)
National Security Authority (NSA)

Number of Entities (OES): 1,400

Number of Entities Required to Undergo Audit in 2023: 122
(possible to fulfill through self-assessment according to §34a, section 2 of the Act on Cybersecurity)

Number of Audit Reports Submitted: 53

Number of Self-Assessments Submitted: 307

Subsectors: Security, Public Administration Information Systems, Defense, Classified Information

4. 11. 1 EVALUATION OF CYBERSECURITY STATUS FOR 2023 BY THE CENTRAL AUTHORITIES

MINISTRY OF DEFENSE

Critical Threats:

From the defense sector's perspective, Slovakia, as a NATO and EU member, has been a target for state actors conducting cyber operations that threaten both national interests and the security interests of the Alliance and the Union. In addition to traditional threat sources from state actors, the significant threat in 2023 was the armed conflict in Ukraine, as Slovakia provided political, economic, and military-technical support to Ukraine. During the assessed period, the Ministry of Defense encountered various cyberattacks, including phishing attacks, DDoS attacks, "hack and leak" attacks, user account compromises, APT group campaigns, and notably, ransomware attacks.

Legal Activities:

The Slovak Republic's Cyber Defense Center advanced cooperation with the national cybersecurity authority, relevant actors, and other central authorities and essential service operators. The goal was to enhance the resilience of the national cyber space and strengthen Slovakia's cybersecurity.

Key activities in 2023 included:

- Participation in the preparation and amendment of national cybersecurity legislation and internal regulations.
- Conducting penetration testing.
- Addressing cybersecurity incidents in information and communication infrastructure.
- Providing expert advice.
- Sharing information with the national cybersecurity authority and other relevant national and international actors.
- Distributing security alerts.
- Providing expert training and education.
- Participating in national and international cybersecurity exercises.

The Cyber Defense Center also collaborated with the national authority on cryptographic protection, focusing on ensuring information confidentiality. This cooperation involved certifying cryptographic protection tools and updating security standards for cryptographic systems. This standard sets the conditions for assessing the ability to protect information using new cryptographic tools developed by the Cyber Defense Center.

Activities Beyond Legal Requirements

In addition to legal cybersecurity activities under § 9, paragraph 1, letter c) of Act No. 69/2018 on Cybersecurity, the center and national authority also worked on tasks arising from Act No. 500/2022 on military intelligence. These tasks included performing relevant cyber operations to ensure the country's defense and fulfilling Slovakia's international commitments for collective defense and other defense-related agreements.

Planned Activities

In 2024, the Cyber Defense Center will continue its activities as required by national legislation and existing contractual obligations. Key activities will include:

- Enhancing security oversight of the defense sector's information and communication infrastructure.
- Addressing cybersecurity incidents within the defense sector's infrastructure.

- Providing expert advice within the defense sector.
- Strengthening collaboration with public administration, private, and academic sectors.
- Sharing information with the national cybersecurity authority and other relevant national and international actors.
- Distributing security alerts within the defense sector and among partners.
- Providing expert training and education.
- Participating in national and international cybersecurity exercises.
- Ensuring audits of cybersecurity for essential service operators within the defense sector.
- Enhancing cybersecurity capabilities.

Strategy

In 2022, the Ministry of Defense developed and the Slovak government approved the Strategy for Cyber Defense of Slovakia. Its implementation is detailed in the Action Plan for Implementing the Cyber Defense Strategy, which was also approved by the government in 2022. One task is to develop an internal regulation applicable to all organizational components and entities under the Ministry of Defense, covering areas defined in Annex 1 of the NSA Decree No. 362/2018.

Human Resources in Cybersecurity:

The Ministry of Defense has established a dedicated cybersecurity authority, the Cyber Defense Center of Slovakia, as part of the Military Intelligence Service. This unit has comprehensive responsibility for cybersecurity in the defense sector and includes an accredited unit for handling cybersecurity incidents in the defense sector – CSIRT.MIL.SK.

Collaboration in Cybersecurity

The Cyber Defense Center places a strong emphasis on collaboration at both national and international levels. National collaboration involves public administration, the private sector, and academia, while international cooperation takes place multilaterally and bilaterally. Multilateral collaboration focuses on key international and regional organizations such as the EU, V4, NATO, EDA, and CCDCOE. Bilateral cooperation includes working with NATO and EU countries as well as third countries outside the Euro-Atlantic region.

MINISTRY OF INTERIOR

Critical Threats:

Increased activities and threats targeted the ministry's infrastructure and information systems. The rise in harmful activities is related to the conflict in Ukraine and technological advancements in artificial intelligence. In 2023, the ministry did not record any major cybersecurity incidents but noted several potential threats to critical infrastructure, primarily DDoS attacks. Overall, 25 DDoS attacks were recorded, considered less significant incidents. The sources of these attacks are rarely identified, and no successful cases involving phishing or other social engineering methods were reported.

Legal Activities

The ministry enhanced its monitoring of the cyber space, increasing surveillance of illegal websites, social media, and communication platforms to track hacker groups and hacktivist movements. It responded to security alerts from SK-CERT and addressed vulnerabilities in its infrastructure. The ministry focused on raising cybersecurity awareness among employees through drills, training, and informational campaigns. A 24/7 support line was available for incident response, with over 1,800 suspicious emails investigated in 2023. The ministry also conducted several cybersecurity audits in accordance with § 29, paragraph 1 of Act No. 69/2018 on Cybersecurity.

Activities Beyond Legal Requirements

Beyond the requirements of § 9, paragraph 1, letter c) of Act No. 69/2018 on Cybersecurity, the ministry increased monitoring of illegal websites and hacker activities, especially those supported by the Russian government and its allied countries. This heightened monitoring was driven by the ongoing conflict between Russia and Ukraine, which exerted cyber pressure on Slovak government institutions, critical infrastructure, and strategic enterprises.

Planned Activities

In 2024, the Ministry of Interior plans to establish a forensic laboratory for law enforcement to secure evidence in cybercrime cases. A Security Operations Center will monitor critical infrastructure and essential services, funded by the Slovak Recovery and Resilience Plan. The ministry aims to increase the number of qualified cybersecurity professionals and implement an automated training system to enhance security awareness.

Planned Strategy:

In 2024, the Ministry plans to issue the **"Cybersecurity Development Strategy for the Ministry for the period 2024 – 2028"** in accordance with the government's program statement adapted to the Ministry's conditions.

Human Resources in Cybersecurity:

Within the Ministry's organizational structure, there is a **cybersecurity department** that:

- **Manages, coordinates, and controls** cybersecurity within the Ministry.
- **Acts as the single point of contact** for reporting cybersecurity incidents.
- **Provides incident management services** and subsequent system recovery.
- **Conducts preventive campaigns** to raise awareness about cybersecurity.

Cybersecurity Cooperation:

The Ministry works closely in the field of cybersecurity with:

- National Security Authority (NSA)
- CSIRT (Computer Security Incident Response Team)
- NASES (National Agency for Network and Electronic Services)
- NCISA (The National Cyber and Information Security Agency)
- Ministry of the Interior of the Czech Republic

The goal is to enhance defense against cyberattacks, share information on current threats, and coordinate the resolution of cybersecurity incidents at both national and international levels.

MINISTRY OF INVESTMENT, REGIONAL DEVELOPMENT AND INFORMATIZATION

Critical Threats:

The most significant threats in the sector include:

- Inadequate implementation of processes for timely detection and remediation of vulnerabilities.
- Frequent absence of data backup processes.
- Lack of security monitoring.
- Cyberattacks heavily exploiting social engineering.

In 2023, CSIRT recorded **1,012 incidents** in the public administration sector. The trend of threats has remained nearly unchanged from 2022, with a notable exception being a decrease in the use of malicious code. The vulnerability assessment service revealed **750 vulnerabilities** last year, of which **374 were critical**.

Legal Activities

The Cybersecurity Section has published materials for cybersecurity and information security in the public administration information systems sector. These materials serve as methodological preparation documentation for minimum security measures of categories I, II, and III, in accordance with the information technology in the public administration and cybersecurity laws. Templates and samples are not mandatory but are freely available and free of charge for organizations in the public administration information systems sector. They can also be used for training employees in cybersecurity and information security.

Activities Beyond Legal Requirements

The Cybersecurity Section of MIRRI SR actively enhances the cybersecurity resilience of public administration. It implements early warning systems and establishes security monitoring centers. In education, it expands the Cyber Arena and supports the creation of competence centers at universities. The catalog of public authorities and the unified methodological framework of documents strengthen compliance with the cybersecurity law. The Central Cybersecurity Portal will serve as a central gateway to information for public administration entities.

Planned Activities

In 2024, the Cybersecurity Section will continue fulfilling its legal duties in the field of cybersecurity. It plans to respond to legislative proposals, specifically amendments to Law No. 69/2018 on cybersecurity and related necessary amendments to subordinate legal regulations. The Cybersecurity Section will also address and amend the **Regulation No. 179/2020**, which establishes the method of categorization and the content of security measures for information technologies in public administration. This regulation will be revised in the near future to reflect all current legal requirements and address newly identified deficiencies.

The Cybersecurity Section of MIRRI SR will continue finalizing the aforementioned and ongoing projects and plans to oversee new projects in this area.

Planned Strategy

In its cybersecurity strategy, the Cybersecurity Section of MIRRI SR plans to develop a **Unified Methodological Framework (UMF)**. This framework will primarily assist public administration entities in fulfilling their legal obligations in cybersecurity and information security. It will include form templates to help these entities meet their requirements.

Human Resources in Cybersecurity

The Cybersecurity Section of MIRRI SR consists of the Department of Cyber and Information Security Management and the Government CSIRT Unit. Future plans include expanding with additional departments, such as those for monitoring cybersecurity and information security, among others.

Cooperation in Cybersecurity

The Cybersecurity Section of MIRRI SR currently collaborates with other ministries, central state authorities, and additional public administration entities, particularly in legislative areas related to various departments. It also plans to work with regional chambers of the Slovak Chamber of Commerce and Industry and other entities engaged in activities related to cybersecurity.

4. 11. 2 AUDIT RESULTS FOR THE PUBLIC ADMINISTRATION SECTOR

As of December 31, 2023, the National Security Authority received a total of 53 audit reports and 307 self-assessments from the public administration sector.

The public administration sector has the lowest audit ratings among all sectors. The sector reports 47% compliance and 16% partial compliance, with 26% of audited items being non-compliant.

AVERAGE PERCENTAGE COMPLIANCE (YEAR 2023)	
COMPLIANCE	47 %
PARTIAL COMPLIANCE	16 %
NON-COMPLIANCE	26 %
NOT APPLICABLE	5 %
VERIFIED ELSEWHERE	6 %
NOT EVALUATED BY AUDITOR	0 %

4. 11. 3 MOST COMMON AUDIT FINDINGS IN THE PUBLIC ADMINISTRATION SECTOR

Among the most common audit findings in the public administration sector are:

- **Contracts:** The entity does not have amendments to contracts reflecting the obligations under the Cybersecurity Act.
- **Cybersecurity Strategy:** There is no developed cybersecurity strategy with defined cybersecurity goals.
- **Information Classification:** Rules and procedures for information classification are not implemented.
- **Cybersecurity Management:** The cybersecurity manager is not formally designated and authorized according to the Cybersecurity Act and related regulations.
- **Risk and Impact Analysis:** Risk and impact analyses are not conducted on a regular basis.
- **Network Security Management:** Rules, procedures, and responsibilities for network security management are not formalized.
- **Access Control Policy:** An access control policy is not defined and implemented.

4. 12 Healthcare

Central Authority: Ministry of Health of the Slovak Republic (MZ SR)

Number of Entities: 94

Number of Entities Required to Audit in 2022: 69
(possibly fulfilled through self-assessment according to §34a, paragraph 2 of the Cybersecurity Act)

Number of Audit Reports Submitted: 34

Number of Self-Assessments Submitted: 6

Subsectors: Healthcare Facilities (including hospitals and private clinics)

4. 12. 1 ASSESSMENT OF CYBERSECURITY STATUS FOR 2023 FROM THE CENTRAL AUTHORITY'S PERSPECTIVE

Critical Threats

- **Insufficient Funding and Outdated Technology:** These factors endanger cybersecurity in healthcare.
- **Low Staff Awareness:** Limited understanding of cybersecurity threats and vulnerabilities increases the risk of attacks.
- **Sophisticated AI Attacks:** Cyberattacks leveraging artificial intelligence are becoming more advanced, threatening the continuity of care.
- **Lack of Recovery Plans and Information Asset Management:** The absence of recovery plans and management of information assets complicates incident handling and can have severe consequences.

Legal Activities

- **Coordination and Support:** In response to growing cybersecurity threats, MH SR organized meetings with selected operators of essential services in the healthcare sector.
- **Objective:** These meetings aimed to establish functional processes to support and coordinate information and cybersecurity within the organizations under its jurisdiction.
- **Expected Outcomes:** Increased cybersecurity in the healthcare sector is anticipated to lead to better protection of patient data and a reduction in the risk of disruption to healthcare services due to cyberattacks.

Activities Beyond Legal Requirements:

Collaboration with National Security Authority: The Ministry of Health has assisted the National Security Authority in organizing regional workshops titled "Cybersecurity in Healthcare."

Planned Activities

Strategy Preparation and Planning: Developing and planning a cybersecurity strategy for the sector under the Ministry of Health's jurisdiction.

Planned Strategy

Cybersecurity Strategy: The Ministry of Health plans to release a Cybersecurity Strategy in the near future. The goal is to enhance the sector's resilience to cyber threats and protect sensitive patient data. The strategy will include measures to improve prevention, detection, and response to cybersecurity incidents.

Human Resources in Cybersecurity:

Information and Cybersecurity Department: The Information and Cybersecurity Department at the Ministry of Health is responsible for protecting information systems and data from cyber threats. It implements security strategies, manages incidents, and supports cybersecurity resilience in the sector.

Collaboration in Cybersecurity:

- Domestic Collaboration: The Ministry of Health collaborates as needed with other authorities in the field of cybersecurity.
- International Collaboration: To date, there has been no collaboration with foreign partners in this area.

4.12.2 AUDIT RESULTS FOR HEALTHCARE SECTOR

As of December 31, 2023, the National Security Authority received a total of 34 audit reports and 6 self-assessments from the healthcare sector.

As of December 31, 2023, the compliance metrics for the healthcare sector are as follows:

AVERAGE PERCENTAGE COMPLIANCE (YEAR 2023)	
COMPLIANCE	61 %
PARTIAL COMPLIANCE	10 %
NON-COMPLIANCE	17 %
NOT APPLICABLE	6 %
REVIEWED ELSEWHERE	6 %
NOT EVALUATED BY AUDITOR	0 %

4.12.3 MOST COMMON AUDIT FINDINGS IN THE PUBLIC ADMINISTRATION SECTOR

Among the most common audit findings in the healthcare sector are:

- **Lack of Documentation:** There is no documented scope and method for implementing all security measures.
- **Missing Cybersecurity Strategy:** A cybersecurity strategy defining cybersecurity goals has not been developed.
- **Undefined System Boundaries:** Boundaries and interfaces of the information system are not specified.
- **Undefined Security Management Structure:** There is no defined structure for management, performance, and control in the area of cybersecurity.
- **Unestablished Rules and Responsibilities:** Rules and responsibilities for implementing measures resulting from risk analysis are not defined, and there is no responsibility assigned for identifying and documenting assets.
- The transfer of rights, obligations, and responsibilities is not formalized, and procedures for internal controls and audits are not established.
- **Lack of Two-Factor Authentication:** Two-factor authentication is not required for remote connections to the internal network.
- **Insufficient Resources for Continuity Management:** Adequate resources for managing business continuity are not allocated, and processes related to business continuity management and related documentation are not implemented.

5 IMPLEMENTATION OF THE ACTION PLAN FOR THE NATIONAL CYBERSECURITY STRATEGY FOR YEARS 2021 TO 2025

To evaluate the Action Plan for the National Cybersecurity Strategy for 2021 to 2025, the National Security Authority (NSA) established a permanent Monitoring Committee for the implementation of the Action Plan.

The committee acts as an independent advisory body to the director of the authority. Its role is to monitor and coordinate the implementation of the tasks outlined in the action plan. The Monitoring Committee meets regularly to assess the progress of each task. The committee is chaired by a member of the authority, and its members include representatives from all entities with at least one task assigned in the action plan.

One of the committee's responsibilities is to prepare an annual report on the completion of tasks. This report is prepared for the previous year, and the report for 2023 will be a separate document.

Entities regularly report on their tasks to facilitate evaluation in the following manner:

1. **Completed Tasks:** Entities must demonstrate how the task was completed.
2. **Ongoing Tasks:** Entities must provide a description of the current status of the task and the anticipated completion date.
3. **Uncompleted Tas ks:** Entities must provide a reason for the task not being completed.

The progress of the action plan's tasks varies by area. Some entities have many uncompleted tasks, and some did not submit their reports for 2023. Several tasks remain under development. The area with the lowest level of task completion is education. The entity with the most tasks in this area—the Ministry of Education, Science, Research, and Sports of the Slovak Republic—has marked many tasks as incomplete.

Compared to the previous year, there has been a slight improvement in task completion. Despite being one of the most critical areas in cybersecurity, the responsible entities do not attach adequate importance to it. Delays in individual tasks are hindering the achievement of the strategic goals identified in the National Cybersecurity Strategy for 2021 to 2025.

6 ACTIVITIES AND MEASURES

The NSA has reaffirmed its commitment to building a security environment aligned with the principles outlined in the European Union Security Union Strategy for 2020 to 2025 and the EU Cybersecurity Strategy for the Digital Decade. The priorities remain enhancing the resilience of cybersecurity infrastructure, improving cybersecurity, and establishing processes to ensure safety in both physical and digital environments.

The Authority's members have contributed to the development of international relations through ongoing representation in the EU and NATO, expanding additional international activities, bilateral relationships, and regional cooperation.

6.1 National Legislation

The Authority continued its efforts in gathering, analyzing, and evaluating information from its divisions, feedback from the expert community during presentations, or requests for professional opinions, with the aim of incorporating this information into the refinement of legally binding regulations.

Additionally, the Authority harmonized national legal provisions with internationally recognized legal sources to address discrepancies in approaches within European conditions and to enhance the stability of professional activities.

In 2023, the Authority initiated the legislative process for two implementing regulations related to Act No. 69/2018 on Cybersecurity:

1. **First Regulation:** An amendment to the National Security Authority Decree No. 165/2018 Coll., which specifies identification criteria for various categories of serious cybersecurity incidents and details for reporting these incidents. The aim of this amendment is to clearly define the criteria for identifying serious cybersecurity incidents. The decree introduces a standardized vulnerability assessment system, providing a unified method for representing the technical characteristics of vulnerabilities in hardware, software, firmware, and numerical assessment of their severity. The draft amendment is currently undergoing internal review.
2. **Second Regulation:** The amendment to the National Security Authority Decree No. 362/2018 Coll., which establishes the content of security measures, the content and structure of security documentation, and the scope of general security measures. The new decree (No. 264/2023 Coll.) came into effect on September 1, 2023. The aim of this amendment is to create a functional legislative framework essential for the effective implementation of key measures for the security of the national cybersecurity space, incorporating priorities and requirements established at the European level. This framework focuses on expanding the content of security measures, the content and structure of security documentation, and the scope of general security measures.

6.2 The European Union

In 2023, the NSA participated in regular meetings of the EU Council Security Committee (CSC), the European Commission Security Policy Experts Group (ComSEG), the Security Committee of the European External Action Service (EEAS), the Security Committee of the European Union Agency for the Space Programme (EUSPA), the TEMPEST Implementation Task Force (ITTF), and the European Union Agency for Cybersecurity (ENISA).

At the EU Council, a revision of security rules continued with the goal of addressing deficiencies identified in application practice and improving the compliance experience for recipients of these rules. The Authority actively engaged in the preparation of security standards to ensure the protection of classified information.

The year 2023 was particularly active in legislative matters within the EU Council and the European Parliament (EP). Legally, the legislative process for three key proposals was completed:

1. **First Proposal:** Regulation EP and Council 2023/2841, establishing measures to ensure a high common level of cybersecurity across EU institutions, bodies, offices, and agencies (EU Cybersecurity Regulations for EU Institutions and Bodies).
2. **Second Proposal:** Regulation EP and Council concerning horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act, CRA).
3. **Third Proposal:** Regulation EP and Council amending the eIDAS Regulation to establish a framework for European digital identity (eIDAS2). Slovakia actively supported the objectives of these proposals.

The adoption of these legislations is expected to enhance the level of cybersecurity within European institutions, improve consumer protection when purchasing and using various software and hardware products with digital elements, and facilitate simple, EU-wide verification of identity for citizens using electronic services.

In April 2023, the European Commission (EC) published a cybersecurity package consisting of two legislative proposals and one non-legislative document:

1. **Proposal for a Regulation:** To enhance solidarity and capacity in the Union for detecting cybersecurity threats and incidents, preparing for and responding to them (CySOLa).
2. **Proposal for a Regulation:** Amending Regulation (EU) 2019/881 regarding managed security services (CSA+).
3. **Communication:** Establishing a Cybersecurity Skills Academy.

Special attention was given to the development of EU cybersecurity certification schemes, including the EUCC (Common Criteria) and EUCS (Cloud Schemes).

The Horizontal Working Party on Cyber Issues (HWPCI) focused on other strategic elements of cyber diplomacy in its non-legislative activities. In 2023, it updated the Cyber Diplomacy Toolbox framework, which will enable the Council to respond more effectively to harmful cyber activities, including sanctions. This framework also included expanded implementation guidelines, taking into account the conflict in Ukraine, the impact of new technologies, and the deteriorating geopolitical security situation. Additionally, in May 2023, the Council adopted conclusions on EU cyber defense policy based on the work of HWPCI, and in June 2023, the Council adopted conclusions on digital diplomacy. Representatives of the Authority participated in the meeting of the European Union Cybersecurity Certification Group (ECCG). The main topic of this group was

the preparation of the final version of the European Commission regulation regarding the implementation of a horizontal certification scheme for cybersecurity products and protective documents, the addition of references to existing national schemes, and the agreement that mutual recognition among member states should be comprehensive.

The representatives of the National Security Authority (NSA) were involved in the European Commission's working formats as:

- **NIS Cooperation Group:** Their main task is to ensure and intensify mutual strategic and analytical cooperation and to share information between the authorities responsible for cybersecurity in member states and their units.
- **National Strategies Evaluation Working Group:** This group focuses on evaluating and improving national cybersecurity strategies.

A key priority for the NIS Cooperation Group was preparing for the implementation of Directive (EU) 2022/2555 of December 14, 2022, on measures for ensuring a high common level of security of network and information systems across the European Union (NIS 2 Directive). This includes applying new tools related to risk assessment and scenarios, as well as addressing issues related to the conclusions of the Council on the development of the EU's approach to cybersecurity.

New sub-platforms were created within the Cooperation Group, including:

- **Work Stream on Risk Evaluation**
- **Work Stream on Supervision**
- **Work Stream on WHOIS**

These work streams aim to address topics such as risk evaluation, oversight, control, and support for internet security and stability.

In the second half of 2023, the NIS Cooperation Group also focused on "Discussion on Submarine Infrastructure (data cables, pipelines, and their termination points)" due to incidents in the Baltic Sea. Additionally, there was a notable development in the relationship between the Cooperation Group and the Critical Infrastructure Resilience Group, as they held their first joint meeting.

ENISA (European Union Agency for Cybersecurity) implemented a roadmap for cybersecurity exercises. Member states shared their experiences regarding the most severe incidents and threats in cybersecurity that impacted them throughout the year, with ransomware being a prominent issue. ENISA also prepared a presentation focusing on its new responsibilities, particularly those related to notification requirements for member states.

NSA representatives were also involved in the following Work Streams within the Cooperation Groups:

- Work Stream on Notification Obligations for Essential Service Operators
- Work Stream on Large-Scale Cybersecurity Incident Response
- Work Stream on Digital Infrastructure
- Work Stream 5G – Security and Protection of 5G Networks
- Work Stream on the Healthcare Sector
- Work Stream on Elections

The EU CyberNet community, which includes national authorities and institutions involved in cybersecurity, expert groups, think tanks, and academic institutions based in EU member states, continued to develop. EU CyberNet organized numerous workshops and conferences throughout the year, focusing on current cybersecurity issues.

The regular meetings of the European External Action Security Committee (SC EEAS) included a review and implementation of the security awareness program and intensified staff training on potential cybersecurity risks.

Activities and efforts continued related to the institutionalization of the European Centre of Sectoral, Technological, and Research Competence in Cybersecurity and the network of National Coordination Centres (ECCC). The primary role of this center is the EU's strategic interest in maintaining and developing cybersecurity capacities to ensure a unified digital market, protect critical networks and information systems, and provide key services in this area.

The Cybersecurity Competence and Certification Centre actively represented the NSA on the ECCC Board, while also fulfilling the intermediary roles of the ECCC as the national coordination center. Additionally, it is positively noted that the NSA's nomination for the position of Executive Director of the ECCC was presented and submitted on behalf of Slovakia. This position will be selected by the European Commission and elected by the Board.

6.3 NATO

A major milestone in NATO's cybersecurity/defense area can be considered the July summit in Vilnius, where the Virtual Cyber Incident Support Capability (VCISC) mechanism was piloted. This represents a virtual capability that allies can use if they are unable to resolve the consequences of harmful cyber activities on their own.

Member states can request assistance through NATO. Prior to the summit, Slovakia voluntarily contributed to the VCISC, and representatives of the National Security Authority (NSA) actively participated in its pilot testing. Lessons learned from the exercise will be incorporated into setting goals for the mechanism and building the VCISC community.

Another significant event was the first annual NATO Cyber Defence Conference, held in November in Berlin, which brought together all three levels of the organization as well as all 31 allies. Slovakia was represented at the political, technical, and military levels by NSA representatives, the Slovak Ministry of Foreign and European Affairs, and the Cyber Defense Center.

The main messages of the conference included the necessity of cooperation at all levels with the private sector, the need to build shared situational awareness, timely information sharing for rapid response to harmful cyber activities, building partnerships and collaboration (primarily with the EU), keeping pace with the implementation of new technologies, greater proactivity, and potential joint attribution.

6.4 Regional Cooperation

Based on the rotation of the chairmanship among the countries that are members of the Central European Cybersecurity Platform (CECSP), the chair for this platform was held by the Czech National Cyber and Information Security Agency (NÚKIB). Representatives of the authority actively participated in the platform's discussions with colleagues from the Visegrad Group countries and Austria. The discussions focused on current topics resonating at the EU level, with partners seeking common ground and mutual support on these issues.

Some of the most important topics of the meeting included the current status of the NIS 2 directive transposition process in individual member states; research, development, and regional cooperation—such as the Czech approach to cybersecurity exer-

cises, best practices, and potential collaboration; and “The Role of Legal Advisors in GovCERT.CZ (LEGAD).” Experts agreed that an adaptive, coordinated, and innovative approach is required for approximation to achieve the widest possible harmonization across the EU.

6.5 Bilateral Relations

The National Security Authority developed bilateral relations on a daily basis across all working platforms and formats, whether through contacts during working group meetings or through ad hoc tasks at the bilateral level.

The NSA regularly communicated and exchanged information at the national level about current legal regulations, vulnerabilities, threats, and incidents. They also exchanged information on best practices and successful practices with their foreign partners both within and outside the EU. They participated in bilateral meetings and foreign receptions as well.

In November 2023, the NSA hosted its first-ever delegation from the African continent—from Kenya. The delegation included representatives from the Ministry of Defence of the Slovak Republic, the Ministry of the Interior of the Slovak Republic, and the NC4 Cybersecurity Management Committee. The meeting was initiated and organized in collaboration with the Slovak Agency for International Development Cooperation (SlovakAid) and the Embassy of the Slovak Republic in Nairobi. The Kenyan side expressed interest in closer cooperation with the authority. The agenda of the meeting was focused on cybersecurity issues.

In March and then in August 2023, meetings were initiated at the request of the Indonesian side with representatives of the Embassy of the Republic of Indonesia in the Slovak Republic and their experts to deepen cooperation in the areas of security, regional security challenges, and the development of security cooperation between the two countries. The main focus was the signing of a memorandum of understanding between both sides in March.

At the beginning of 2023, a high-level meeting was held in Brno at the headquarters of the Czech NÚKIB. The purpose of the meeting was to sign a Memorandum of Cooperation between the National Security Authority and the National Cyber and Information Security Authority, signed by both directors of the agencies. This act confirmed the active and long-term cooperation between the two authorities.

The memorandum identified 17 areas of cooperation, including but not limited to protection against active cyber threats, incidents, and attacks; support for responsible state behavior in cyberspace; cyber threat intelligence (CTI) and strategic analysis; security of the information and communication technology supply chain; capacity building, and more.

In September 2023, a liaison officer position was created at the Embassy of the Slovak Republic in Washington, with the main task of establishing close cooperation in the field of cybersecurity and developing cooperation with relevant authorities dealing with the protection of classified information in the United States.

6.6 Issuance of Warnings and Bulletins

The National Cyber Security Center regularly issues security bulletins and warnings that highlight vulnerabilities in various systems and services. These are primarily intended for Operators of Essential Services and Providers of Digital Services. However, anyone can subscribe to these bulletins for free.

The evaluation of vulnerabilities found in the bulletins and warnings follows the internationally recognized CVSS 3.1 methodology, which is used to assess vulnerabilities in software and hardware products.

Security bulletins are issued weekly and contain a list of medium and high severity vulnerabilities. Security warnings address critical vulnerabilities, and if they have a significant impact, the authority also issues warnings for vulnerabilities with lower severity.

The following overview lists the number of weekly security bulletins and security warnings issued for the year 2023:

	Total Bulletins 2023	Total Warnings 2023	Total Vulnerabilities
January	5	36	**79**
February	4	30	**61**
March	4	27	**73**
April	4	20	**64**
May	5	54	**127**
June	4	25	**86**
July	4	56	**102**
August	5	40	**117**
October	5	34	**98**
November	4	36	**83**
December	4	27	**108**
TOTAL	48	385	**998**

6.7 CyberGame

In 2023, the authority once again organized the cybersecurity competition named CyberGame, which was recognized as the IT Project of the Year in 2022. The scenarios and tasks in CyberGame are inspired by the practical experience of professionals. CyberGame lasted for ten weeks and featured over 70 tasks of varying difficulty. To participate in the game, all that was needed was a computer and freely available analytical tools, with players earning points and flags for each solved task. The National Cyber Security Center managed the communication channel for players and provided advisory support.

In CyberGame 2023, players encountered six gameplay branches: malware analysis, forensic analysis, OSINT (Open Source Intelligence), cryptography, and two new branches – a security enhancement branch, known as hardening, and a non-technical branch called processes and security management.

A new feature was that CyberGame was also played on an English-language platform. The game also addressed the current phenomenon of the availability of generative language models based on artificial intelligence.

For the second edition, 2,334 participants registered on both the Slovak and English platforms. On the Slovak platform, there were 1,788 registered participants, with 832 being active players, indicating a significant increase in both categories. The age group under 25 years was represented by 754 participants.

6.8 Raising Awareness Among the General Public

In 2023, the National Security Authority (NSA) developed several awareness campaigns to promote cybersecurity. The most extensive campaign was the Advent Cyber Calendar, which consisted of 24 posts on social media. This calendar provided practical advice on how to defend against threats in cyberspace.

NSA representatives also taught a course on “Security and Journalism in the Online Space” at the Department of Journalism at Comenius University. The course covered principles of cybersecurity hygiene, data protection, privacy, communication, and working with open sources. Students were required to integrate journalistic skills with new knowledge from the course.

The authority was also invited to a primary school in Nitra, where they spoke with students about safe online behavior. This visit concluded a week focused on cybersecurity, during which students participated in quizzes and discussions on social networks, cyberbullying, and more. The authority continues to build on similar activities from previous years and plans to engage more ministries in future initiatives.

6.9 Activities of CSCCC

The State Contribution Organization Competence and Certification Center for Cybersecurity (CSCCC) serves as the National Coordination Center (NCC-SK) within the network of European Coordination Centers and the European Center for Industrial, Technological, and Research Competences under Regulation (EU) No. 2021/887.

Accreditation from the European Commission confirms the expertise and capacity of the Competence Center to manage European financial funds for cybersecurity from directly managed EU programs. Slovakia achieved exceptional success in the Digital Europe program in 2023, leading member states in the number of successful projects. Activities by the National Coordination Center significantly contributed to Slovak companies receiving substantial financial resources for their cybersecurity needs. CSCCC, NSA, and the Ministry of Transport of the Slovak Republic signed a grant agreement with the European Commission aimed at the effective implementation of the NIS2 Directive in Slovakia. To continuously enhance expertise, applications were submitted to MIRRI for additional funding from European projects under the Recovery and Resilience Plan.

A key objective of the Competence Center was the intensive development of a professional cybersecurity community. This effort led to the creation of strong partnerships, sharing of best practices, and raising awareness of the importance of cybersecurity among businesses, academia, and the public sector. Thanks to NCC-SK, several dozen Slovak entities have become members of the European cybersecurity community under Regulation (EU) No. 2021/887.

A significant part of the Competence Center's tasks involves conformity assessment in cybersecurity according to Regulation (EU) No. 2019/881 concerning ENISA (European Union Agency for Cybersecurity) and the certification of cybersecurity for information and communication technologies (Cybersecurity Regulation). Following the adoption of the Cyber Resilience Act (CRA), the Competence Center will also apply for accreditation under this regulation.

Currently, the Competence Center is accredited for the certification of cybersecurity auditors and managers according to specific regulations and the STN EN ISO/IEC 17024 standard, as well as for integrated management systems for quality, information security, IT services, and business continuity management under the STN EN ISO/IEC 17021 standard. The number of certified individuals has increased by 5 certified auditors and 7 certified managers.

In 2022/806, the Ministry of Justice of the Slovak Republic accepted the proposal from the National Security Authority to expand the list of expert fields to include a new field of cybersecurity. This led to the amendment of the Ministry of Justice Decree No. 228/2018, which implements Act No. 382/2004 on experts, interpreters, and translators. CSCCC aims to be the first expert organization to perform expert activities in the new field of Cybersecurity.

The Competence Center also succeeded in adult education. In 2023, it received accreditation for educational programs from the Accreditation Commission of the Ministry of Education, Science, Research, and Sport of the Slovak Republic for further education in Cybersecurity Management and Cybersecurity Auditing. An updated educational scheme was issued. New specialized courses and workshops on Continuity Management and Information Security Management were added, and syllabi for several existing courses were updated.

In 2023, a total of 65 training sessions were conducted:

- 8 Introduction to Cybersecurity courses
- 10 Basics of Cybersecurity courses
- 20 Cybersecurity Management courses
- 3 Cybersecurity Auditor courses
- 9 specialized courses and workshops
- 1 Information Security Management course according to ISO/IEC 27001:2022
- 14 free webinars on raising awareness about cybersecurity

A total of 1,033 participants attended these educational activities during the year.

The Competence Center organized a successful cybersecurity awareness event, Cybersecurity Roadshow 2023, which included various expert presentations at conferences and for students at selected Slovak universities.

Every month, CSCCC issued one flyer to raise security awareness:

- 10 Ways to Protect Your Personal Data – for Data Protection Day
- 10 Steps to Cybersecurity
- Zero Trust Architecture
- Traffic Light Protocol (TLP)
- Principles of Secure Software Development
- How Strong Is Your Password?
- Principles of Secure Software Development
- 12 Steps to Protect Your Business – Cybersecurity for Small and Medium Enterprises
- Cybersecurity in Local Government
- Choosing a Cybersecurity Service Provider: A 5-Step Guide for Municipalities and Cities
- Artificial Intelligence Regulation

Annual surveys on the state of cybersecurity were prepared based on CSCCC's assignments and published as public documents. These include results from surveys of the general public and small and medium enterprises.

CSCCC also continued to expand its network of organizations through memorandum agreements. In cooperation with the National Cyber Security Center, the Competence Center assembled a team of young individuals to represent Slovakia at the European Cyber Security Challenge. This activity, overseen by the European Union Agency for Cybersecurity (ENISA), involved 34 national teams, including those from 28 EU member countries and guest teams from the USA, Canada, Costa Rica, Serbia, Georgia, and the United Arab Emirates. The competition took place from October 24 to 27 in Norway.

The Slovak team consisted of ten young talents – nine boys and one girl. The team prepared for the competition over several months, participating in an international bootcamp in Vienna in June and several bootcamps in Bratislava led by technical coaches from NSA.